## INFORMATION TO USERS

This dissertation was produced from a microfilm copy of the original document. While the most advanced technological means to photograph and reproduce this document have been used, the quality is heavily dependent upon the quality of the original submitted.

The following explanation of techniques is provided to help you understand markings or patterns which may appear on this reproduction.

1. The sign or "target" for pages apparently lacking from the document photographed is "Missing Page(s)". If it was possible to obtain the missing page(s) or section, they are spliced into the film along with adjacent pages. This may have necessitated cutting thru an image and duplicating adjacent pages to insure you complete continuity.

2. When an image on the film is obliterated with a large round black mark, it is an indication that the photographer suspected that the copy may have moved during exposure and thus cause a blurred image. You will find a good image of the page in the adjacent frame.

3. When a map, drawing or chart, etc., was part of the material being photographed the photographer followed a definite method in "sectioning" the material. It is customary to begin photoing at the upper left hand corner of a large sheet and to continue photoing from left to right in equal sections with a small overlap. If necessary, sectioning is continued again — beginning below the first row and continuing on until complete.

4. The majority of users indicate that the textual content is of greatest value, however, a somewhat higher quality reproduction could be made from "photographs" if essential to the understanding of the dissertation. Silver prints of "photographs" may be ordered at additional charge by writing the Order Department, giving the catalog number, title, author and specific pages you wish reproduced.

**University Microfilms**

300 North Zeeb Road
Ann Arbor, Michigan 48106

A Xerox Education Company

Downloaded from SHAREOK. Persistent Handle URL: https://hdl.handle.net/11244/3379

72-29,919

WIRT, B. Richard, 1943-
FINITE NON-COMMUTATIVE LOCAL RINGS.

The University of Oklahoma, Ph.D., 1972
Mathematics

University Microfilms, A XEROX Company, Ann Arbor, Michigan

THIS DISSERTATION HAS BEEN MICROFILMED EXACTLY AS RECEIVED

THE UNIVERSITY OF OKLAHOMA

GRADUATE COLLEGE

# FINITE NON-COMMUTATIVE LOCAL RINGS

A DISSERTATION

SUBMITTED TO THE GRADUATE FACULTY

in partial fulfillment of the requirements for the

degree of

DOCTOR OF PHILOSOPHY

BY

B. RICHARD WIRT

Norman, Oklahoma

1972

FINITE NON-COMMUTATIVE LOCAL RINGS

APPROVED BY

Leonard R. Rubin

Kirby C. Smith

DISSERTATION COMMITTEE

PLEASE NOTE:

Some pages may have

indistinct print.

Filmed as received.

University Microfilms, A Xerox Education Company

ACKNOWLEDGMENTS

I wish to thank Professor Bernard McDonald, my dissertation advisor for his suggestion of a topic, for his patience and encouragement while I was writing, and for his many outstanding lectures as a teacher.

I also wish to thank my wife, Lynda, and our daughters for their understanding and encouragement during my years as a student.

TABLE OF CONTENTS


| | | Page |
|---|---|---|
| INTRODUCTION | | 1 |
| Chapter | | |
| I. | SURVEY OF FINITE RINGS | 4 |
| II. | STRUCTURE OF FINITE LOCAL RINGS | 9 |
| III. | SKEW POLYNOMIAL RINGS OVER A FINITE LOCAL RING | 23 |
| IV. | APPLICATIONS OF SKEW POLYNOMIAL THEORY | 56 |
| BIBLIOGRAPHY | | 70 |

# INTRODUCTION

Finite fields and structures over finite fields have a rich and well-developed theory. There has been considerable interest in generalizing these results to finite rings and preliminary to this, to finite local rings since finite rings decompose into structures involving local rings (See Chapter I).

McDonald and Ganske [21], [9] have developed extensively the theory of commutative finite local rings and in particular a Galois theory. Clark and Drake [2] have characterized commutative finite local principal ideal rings. While Raghavendran [23], Wilson [27], [28], and others have proven several structure theorems for particular finite local rings. But a workable structure theorem for the non-commutative case has not been obtained. Thus the theory of non-commutative finite rings remains undeveloped.

In this paper we show that non-commutative local rings are homomorphic images of skew polynomial rings over a suitable "coefficient" subring. This corresponds to the Cohen Structure Theorem for commutative complete local rings so that much of the theory in the non-commutative case is a parallel to the commutative theory.

The technique often used in the study of local rings is to reduce modulo the maximal ideal and then "lift" results back to the ring. This same technique is used in the case of polynomial rings over a local ring.

The needed background and motivation for studying finite non-commutative local rings is given in Chapter I without proof. In Chapter II we prove the existence of a "coefficient" subring S of a finite local ring R. Clark [3] and Wilson [27] independently have shown $R = S \oplus Sb_1 \oplus \cdots \oplus Sb_n$ as a two-sided S-module where $b_i$ are in the Rad(R). We will extend this by showing there exist automorphisms $\sigma_i$ of S such that

$$sb_i = b_i\sigma_i(s) \quad \text{for } s \text{ in } S \text{ and } 1 \leq i \leq n.$$

This is the needed substitute for the lack of commutativity in R. Using this decomposition of R we then show that R is the homomorphic image of the skew polynomial ring $S[X_1,\cdots,X_n,\sigma_1,\cdots,\sigma_n]$ where $X_i$ are non-commuting indeterminants and $sX_1 = X_i\sigma_i(s)$ for s in S and $1 \leq i \leq n$.

In Chapter III we study in detail the skew polynomial ring $R[X,\sigma]$ for R a finite local ring. We are interested in R being finite due to the above structure theorem, but we note that most of the results of Chapter III are also valid for local or Artinian local rings with only slight modification of several proofs. Ore [22] in 1933 first considered skew polynomial rings over fields and division rings. Since Ore's work, little has been done to develop the properties of polynomials and ideals in skew polynomial rings over a more general coefficient ring. We follow the approach of Snapper [25] for polynomial rings over commutative local rings and develop an extensive theory for polynomials, ideals, and factorization in skew polynomial rings over finite local (Artinian local) rings.

Chapter IV is an application of our skew polynomial theory and the structure theorem. We first consider ring extensions of a non-commutative finite local ring. In particular our interest is in a skew simple

algebraic extension $R[\theta,\sigma]$ where $\sigma$ is an automorphism of R such that $r\theta = \theta\sigma(r)$ for r in R. Also we complete the characterization of Clark [2] of all finite chain rings R by using a skew Eisenstein extension of the coefficient subring S of R. Further we characterize the finite one-step ring of Redei [24] in terms of a particular skew polynomial ring.

# CHAPTER I

## SURVEY OF FINITE RINGS

This chapter introduces some of the definitions and notation used in studying finite rings with identity and gives several decomposition theorems of finite rings into rings involving local rings. Thus the study of finite rings involves that of local rings.

Throughout this paper "ring" will mean a finite ring with identity which is not necessarily commutative. The one exception is the polynomial ring which will not be finite but will have coefficients from a finite ring.

A ring R is called local or completely primary if R/Rad(R) is a finite field, where the radical of R is

$$\mathrm{Rad}(R) = \bigcap\{M \mid M \text{ is a maximal right ideal of } R\}.$$

We have the following well-known results concerning the radical of R and local rings, which are given without proof. The first proposition shows that for finite rings the various well-known types of radicals are equivalent. See McDonald [21] for proof.

1.1 PROPOSITION. Let R be a finite ring with identity.

(1) $\mathrm{Rad}(R) = \{r \text{ in } R \mid 1 - rs \text{ is invertible for all } s \text{ in } R\}$

$= \{r \text{ in } R \mid 1 - sr \text{ is invertible for all } s \text{ in } R\}.$

(2) Rad (R) is an ideal and is the largest ideal k such that

for all r in k, 1 - r is a unit.

(3) Rad (R) = $\bigcap\{M \mid M$ is a maximal left ideal of R$\}$.

(4) Rad (R) = $\bigcap\{P \mid P$ is a prime ideal of R$\}$.

(5) Rad (R) = $\bigcup\{B \mid B$ is a nilpotent ideal of R$\}$.

(6) Rad (R) = {r in R | r is strongly nilpotent}.

Our concern is mostly with local rings:

1.2 PROPOSITION. The following are equivalent.

(1) R is a local ring.

(2) R has exactly one maximal right (or left) ideal.

(3) The non-units of R form a right (or left) proper ideal.

(4) For every r in R, either r or 1 + r is a unit.

(5) R has only 0 and 1 as its idempotents.

(6) Every element of R is either a unit or a nilpotent element.

1.3 PROPOSITION. If R is a finite local ring with maximal ideal M, then

(1) Rad (R) = M = {r in R | r is nilpotent}; hence M is nilpotent.

(2) The units of R = {r | r is not in M}.

(3) Every non-unit is a two-sided zero divisor in R.

The following proposition from Raghavendran [20, Thm. 2, p. 199] gives the relationship of the orders of R, M, and R/M for R a finite local ring.

1.4 THEOREM. Let R be a finite local ring with unique maximal ideal M. Then there are associated with R integers p (prime), n, and r such that

$$|R| = p^{nr}, \quad |M| = p^{(n-1)r}, \quad |R/M| = p^{r}$$

where

(1) The characteristic of R is $p^k$ where $1 \leq k \leq nr$.

(2) $M^n = (0)$.

Examples of local rings are:

(1) Any finite field $GF(p^r)$, whose radical is (0) and $\chi(R) = p$.

(2) The ring $Z/Zp^n$ (p prime), whose radical is $Zp/Zp^n$ and $\chi(R) = p^n$.

(3) The ring of matrices

$$\left\{\begin{bmatrix} a & b \\ 0 & a \end{bmatrix} \mid a,b \text{ are in } Z/Zp\right\}$$

whose radical is

$$\left\{\begin{bmatrix} 0 & a \\ 0 & 0 \end{bmatrix} \mid a \text{ is in } Z/Zp\right\}$$

and $\chi(R) = p$.

(4) (Wilson [28]) The ring of matrices

$$\left\{\begin{bmatrix} a & b \\ 2c & 2d \end{bmatrix} \mid a,b,c,d \text{ are in } Z/4Z\right\}$$

whose radical is

$$\left\{\begin{bmatrix} 2a & b \\ 2c & 2d \end{bmatrix} \mid a,b,c,d \text{ are in } Z/4Z\right\}$$

and $\chi(R) = 4$.

The first three examples are commutative while the last is noncommutative.

To require that R has a unique maximal right ideal is stronger than requiring that R have a unique maximal two-sided ideal as the following illustrates.

Let $S = Z/Zp^n$ (p prime) and $R = M_n(S)$ be the $n \times n$ matrix ring over S ($n \geq 2$). Then R has a unique maximal two-sided ideal

$$M = M_n(Zp/Zp^n),$$

but

$$R/M = M_n(Z/Zp^n)/M_n(Zp/Zp^n) \simeq M_n(Z/Zp)$$

which is not a field.

We next give various structure theorems for finite rings each of which involves finite local rings. Thus the structure of finite rings may be approached from the context of the structure of finite local rings.

1.5 PROPOSITION. (Structure theorem for semi-local rings)

Let R be a semi-local ring. Then R is isomorphic to an $n \times n$ matrix ring over a local ring S. The integer n is unique and S is unique up to a ring isomorphism.

By lifting orthogonal idempotents from R/Rad(R) we obtain the following well-known result for finite rings. The proof may be found in McDonald [21].

1.6 PROPOSITION. (Standard decomposition)

Let R be a finite ring. Then

$$R = S + N$$

where (a) $S \cap N = 0$.

(b) $S = \oplus \sum_{i=1}^{n} M_{n_i}(S_i)$ is a direct sum as an additive Abelian group of $n_i \times n_i$ matrix rings over local rings $S_i$.

(c) N is a subgroup of Rad (R).

If in the above standard decomposition the characteristic of $S_i$ is $p_i$ (prime), then $S_i$ contains a subfield $k_i$ isomorphic to the residue field $S_i/\mathrm{Rad}(S_i)$. Thus we may consider $S_i$ as a finite dimensional algebra over $k_i$. Applying the Wedderburn-Malcev Theorem we have

$$S_i = k_i \oplus \mathrm{Rad}(S_i) \text{ as Abelian groups for } 1 \leq i \leq n.$$

So that the standard decomposition splits into

$$R = \oplus \sum_{i=1}^{n} M_{n_i}(k_i) + \mathrm{Rad}\ (R)$$

where

$$\sum_{i=1}^{n} M_{n_i}(k_i) \cap \text{Rad } (R) = 0.$$

In Chapter II we generalize this result to all finite rings.

In (1.6) the local rings $S_i$ are called the associated local rings of R. These local rings together with the subgroup N and the manner in which their elements combine determine the structure of R.

If $N = 0$, then $R = \oplus \sum_{i=1}^{n} M_{n_i}(S_i)$ is a direct sum of matrix rings over the associated local rings; i.e., is a direct sum of semi-local rings. It is easy to show that $N = 0$ if the radical of R is contained in the center of R or if the commutative orthogonal idempotents of R/Rad (R) lift to commutative idempotents in R. Other necessary and sufficient conditions for $N = 0$ were given recently by Courter [5].

## CHAPTER II

## STRUCTURE OF FINITE LOCAL RINGS

As shown in the first chapter every finite ring has a standard decomposition into the direct sum (as Abelian groups) of matrix rings over finite local rings plus a factor which is a subgroup of the radical R. Thus knowing the structure of finite local rings one hopes to use the properties of matrix rings to study the structure of finite rings.

In this chapter we give several structure theorems for non-commutative finite local rings. Each of the structure theorems employs the use of a commutative local principal ideal subring S of R. The ring S is a Galois ring of the form $(Z/Zp^n[X])/(f)$. (Z denotes the rational integers, p is a prime and f is irreducible modulo p). Following Krull and Janusz [16] who have shown similar results for commutative rings we will call S a "coefficient" subring of R.

As a substitute for commutativity in R we show that R has a "distinguished" independent generating set $\{1,b_2,\cdots,b_m\}$ where for each i, $1 \leq i \leq m$, there is an automorphism $\sigma_i$ of S such that $sb_i = b_i\sigma_i(s)$ for each s in S. Using this result we have our main structure theorem.

THEOREM. Let R be a finite local ring with coefficient ring S, Then R is the homomorphic image of a skew polynomial ring $S[X_1,\cdots,X_m; \sigma_1,\cdots,\sigma_m]$ where $\sigma_i$'s are automorphisms of S, $X_i$'s noncommuting indeterminants, and $sX_i = X_i\sigma_i(s)$ for s in S.

## 1. GALOIS RINGS.

Let $GR(p^n,r)$ denote the extension $(Z/Zp^n[X])/(f)$ of the ring $Z/Zp^n$ (p a prime) where f is monic of degree r and irreducible modulo $Zp/Zp^n$. Such a ring is called a Galois ring of characteristic $p^n$. We note that a Galois ring is a generalization of a Galois field $GF(p^r)$ and the ring $Z/Zp^n$. For n = 1, $GR(p,r) = GF(p^r)$ and for r = 1, $GR(p^n,1) = Z/Zp^n$.

For another characterization of $GR(p^n,r)$ we use the fact that $Z/Zp^n$ and $(Z/Zp^n)[X]/(f)$ are commutative rings to conclude from Ganske and McDonald [9, Theorems 5.6, 5.11] that $GR(p^n,r)$ is a Galois extension of $Z/Zp^n$. We include for completeness and reference their theorem which summarizes the properties of commutative Galois extensions.

2.1 PROPOSITION. Let $S = GR(p^n,r) = (Z/Zp^n[X])/(f)$ be a Galois extension of $Z/Zp^n$. Then

(i) S is unramified over $Z/Zp^n$, with unique maximal ideal Sp, and every ideal is of the form $Sp^i$.

(ii) $S = (Z/Zp^n)[a]$, where a is a root of f.

(iii) S is a splitting ring of f.

(iv) The automorphisms of S permute the roots of f.

(v) $|\text{Auto } (S)| = \dim_{Z/Zp^n}(S) = \deg f$.

(vi) Auto (S) is a cyclic group and isomorphic to Auto (S/Sp).

(vii) S is the unique Galois extension of $Z/Zp^n$ of degree r.

Further note that since each ideal of $GR(p^n,r)$ is of the form $(p^i)$, for g in $GR(p^n,r)$, $g = up^t$, where u is a unit and t a unique integer.

Next we show that if R is a finite local ring with characteristic $p^n$ and $R/Rad(R) = GF(p^r)$, then R contains the Galois ring $S = GR(p^n,r)$. Thus we may consider R as a two-sided S-module (denoted (S-S)-module).

In fact, S is a (S-S)-module direct summand of R and is called the coefficient subring of R.

2.2 THEOREM. (Coefficient Subring)

Let R be a finite local ring with unique maximal ideal M, the characteristic of R be $p^n$, and residue field $R/M = GF(p^r)$.

Then there exists a commutative local subring S of R such that

(1) $S = GR(p^n,r)$; i.e., S is a Galois ring.

(2) $S/Rad(S) = S/Sp \simeq R/Rad(R) = R/M$.

(3) S is unique up to an inner automorphism.

(4) S is an (S-S)-module direct summand of R, i.e.,

$$ {}_SR_S = {}_SS_S \oplus {}_SN_S \quad \text{where } N \subset Rad(R). $$

Proof. We construct S in R as follows. Since the finite field $R/Rad(R) = GF(p^r)$ contains the subfield Z/Zp, we have from the theory of finite fields that

$$ GF(p^r) = (Z/Zp[X])/(\bar{f}) = (Z/Zp)[\bar{\theta}] $$

for some monic irreducible $\bar{f}$ of degree r in (Z/Zp)[X] and $\bar{\theta}$ in $GF(p^r)$ a zero of $\bar{f}$. Let f in $(Z/Zp^n)[X]$ be a monic preimage of $\bar{f}$ of degree r. Then f is irreducible and hence by (2.1) $(Z/Zp^n)[X]/(f)$ is the Galois ring $GR(p^n,r)$. Further $\bar{\theta}$ has a preimage $\theta$ in $GR(p^n,r)$ such that $\theta$ satisfies f and $GR(p^n,r) = (Z/Zp^n)[\theta]$. We let $(Z/Zp^n)[X]/(f) = GR(p^n,r)$ be denoted by S, and note that S is commutative since it is a simple extension of $Z/Zp^n$.

By Raghavendran [20, Thm. 8, p. 212] we have that up to an inner automorphism of R, S is a unique subring of R. Note, if R is commutative then S is absolutely unique by (2.1).

Further $\mathrm{Rad}(S) = \mathrm{Rad}(R) \cap S$, and from the construction of S under the natural homomorphism

$$\mu : R \to R/\mathrm{Rad}(R)$$

S is mapped surjectively onto $R/\mathrm{Rad}(R)$. Thus

$$S/\mathrm{Rad}(S) \simeq S/(\mathrm{Rad}(R) \cap S) \simeq S/\ker \mu \simeq R/\mathrm{Rad}(R).$$

It remains to prove (iv). Since R and S are natural (S-S)-modules and S is commutative, R and S may be considered as left modules over their enveloping algebra $S \otimes_Z S$.

We first show that $S \otimes_Z S \simeq \oplus \sum_{i=1}^{r} S$ as rings. Now $S = (Z/Zp^n)[X]/(f)$ where f is monic of degree r and irreducible modulo Z/Zp. We have a natural ring isomorphism

$$\psi : S \otimes_Z S = (Z/Zp^n)[X]/(f) \otimes_Z S \to S[X]/(f)$$

defined by

$$\psi : \overline{X} \otimes s \to s\overline{X} \text{ where } \overline{X} = X + (f) \text{ and } s \text{ is in } S.$$

But by (2.1), S[X] is a splitting ring for f, so that $f(X) = (X - a_1) \cdots (X - a_r)$. Thus

$$\begin{aligned} S \otimes_Z S \simeq S[X]/(f) &\simeq S[X]/(X - a_1) \cdots (X - a_r) \\ &\simeq \oplus \sum_{i=1}^{r} S[X]/(X - a_i) \\ &\simeq \oplus \sum_{i=1}^{r} S \text{ as rings.} \end{aligned}$$

Therefore we consider R and S as left $(\oplus \sum_{i=1}^{r} S)$-modules.

Since S is a local principal ideal ring, by Hungerford [13] S is the homomorphic image of a principal ideal domain and hence is a quasi-Frobenius ring. Now $S \otimes_Z S$ being the direct sum of quasi-Frobenius rings is also quasi-Frobenius. The ring S being a direct summand of $S \otimes_Z S$ is

$S \otimes_Z$ S-projective and hence injective. A module is projective if and only if injective over quasi-Frobenius rings. Thus S is an injective (S-S)-module. That is, S is a (S-S)-module direct summand of R. So that there exists a (S-S)-module N such that

$$ {}_S R_S = {}_S S_S \oplus {}_S N_S . $$

By Wilson [24, Prop. 2.2] ${}_S N_S$ is contained in Rad(R).

## 2. MODULES OVER GALOIS RINGS

We show that for a Galois ring $S = GR(p^n,r)$, an (S-S)-module M decomposes into (S-S)-submodules $M_i$, where for each i there is an automorphism $\sigma_i$ of S such that $sm = m\sigma_i(s) = ms^{\sigma_i}$ for m in $M_i$ and s in S. This will be referred to as "skew commuting". Thus, when considering the structure of M as a (S-S)-module we need only consider the left S-module structure.

2.3 THEOREM. Let $S = GR(p^n,r)$ be a Galois ring, M a (S-S)-module, and $\text{Auto}(S) = \{1,\sigma_2,\cdots,\sigma_r\}$ be the ring automorphisms of S. Then

$$ M = M_1 \oplus \cdots \oplus M_r \text{ as (S-S)-modules} $$

where for each i, $1 \le i \le r$, there is an automorphism $\sigma_{k(i)}$ of S such that

$$ sm = m\sigma_{k(i)}(s) $$

for each m in $M_i$ and s in S.

Proof. Since $S = (Z/Zp^n)[X]/(f)$ is a Galois extension of $Z/Zp^n$, by (2.1) there exists a primitive element $a_1$ in S such that $S = (Z/Zp^n)[a_1]$. The element $a_1$ satisfies the monic polynomial f which is irreducible modulo Z/Zp. In S[X] f splits into $f(X) = (X - a_1) \cdots (X - a_r)$. Since f has distinct roots in $S/Sp = (Z/Zp[X])/(f)$ we have $\bar{a}_i \neq \bar{a}_j$ for $i \neq j$. Thus

$a_i - a_j$ is not in Sp and is a unit. Define

$$f_i(x) = \prod_{\substack{j=1 \\ j \neq i}}^{r} (x - a_j).$$

Then $f_i(a_i) = (a_i - a_1) \cdots (a_i - a_{i-1})(a_i - a_{i+1}) \cdots (a_i - a_r)$ is a unit in S, and we have the following identity

$$(*) \qquad \sum_{i=1}^{r} [f_i(a_i)]^{-1} f_i(x) = 1.$$

Observe that right multiplication of elements in M by $a_1$ is a left S-linear morphism. Denote it by

$$\sigma : M \to M \text{ where } \sigma(m) = ma_1.$$

Let $f(X) = X^r + t_1 X^{r-1} + \cdots + t_r$ where the $t_i$ are in $Z/Zp^n$. Then

$$\begin{aligned} f(\sigma)m &= (\sigma^r + t_1\sigma^{r-1} + \cdots + t_r)m \\ &= ma_1^r + t_1 ma_1^{r-1} + \cdots + t_r m \\ &= mf(a_1) \\ &= 0, \end{aligned}$$

since $f(a_1) = 0$ and $t_i m = mt_i$ for $t_i$ in $Z/Zp^n$. From the identity (*) we have the identity mapping

$$i_M = \sum_{i=1}^{r} [f_i(a_i)]^{-1} f_i(\sigma) : M \to M,$$

so that

$$M = M_1 + M_2 + \cdots + M_r$$

where for $1 \leq i \leq r$

$$M_i = [f_i(a_i)]^{-1} f_i(\sigma) M.$$

We show that this sum is direct. Suppose, without loss of generality, that m is in $M_1 \cap (M_2 + \cdots + M_r)$. Now, m in $M_1$ implies

$m = [f_1(a_1)]^{-1}f_1(\sigma)m_1$ for some $m_1$ in $M_1$, and thus since S[X] is commutative,

$$(\sigma - a_1)m = (\sigma - a_1)[f_1(a_1)]^{-1}f_1(\sigma)m_1$$

$$= [f_1(a_1)]^{-1}f(\sigma)m_1$$

$$= 0.$$

On the other hand, since m is in $M_2 + \cdots + M_r$,

$$m = [f_2(a_2)]^{-1}f_2(\sigma)m_2 + \cdots + [f_r(a_r)]^{-1}f_r(\sigma)m_r$$

for some $m_2, \cdots, m_r$ in M. Thus

$$(\sigma - a_2) \cdots (\sigma - a_r)m = \left[\prod_{i=2}^{r} (\sigma - a_i)\right]\left[\sum_{i=2}^{r} f_i(a_i)^{-1}f_i(\sigma)m_i\right]$$

$$= 0.$$

Thus the sum is direct.

Now for each m in $M_i$, $m = [f_i(a_i)]^{-1}f_i(\sigma)m_i$ for some $m_i$ in M, and

$$(\sigma - a_i)m = (\sigma - a_i)[f_i(a_i)]^{-1}f_i(\sigma)m_i$$

$$= [f_i(a_i)]^{-1}f(\sigma)m_i$$

$$= 0.$$

Thus $\sigma(m) = a_i m$, but also by definition of $\sigma$, $\sigma(m) = ma_1$. Consequently for m in $M_i$

$$ma_1 = a_i m.$$

Since $a_i$ and $a_1$ are roots of f(x) in S[X] there is by (2.1) an automorphism $\sigma_{k(i)}$ in Auto(S) such that

$$\sigma_{k(i)}(a_1) = a_i.$$

That is, for each m in $M_i$, $ma_1 = \sigma_{k(i)}(a_1)m$.

Since $S = Z/Zp^n[a_1]$ each s in S has the form $s = c_0 + c_1a_1^1 + \cdots c_{r-1}a_1^{r-1}$ where $c_i$ is in $Z/Zp^n$. Thus for m in $M_i$ and s in S,

$$ms = m(\sum_i c_i a_1^i) = \sum_i c_i m a_1^i$$

$$= \sum_i c_i [\sigma_{k(i)}(a_1)]^i m = \sum_i c_i \sigma_{k(i)}(a_1^i)m$$

$$= \sigma_{k(i)}(\sum_i c_i a_1^i)m = \sigma_{k(i)}(s)m.$$

We are done.

Let $S = GR(p^n,r)$ be a Galois ring. If $\{b_1,b_2,\cdots,b_n\}$ is a generating set for a (S-S)-module M, it is an <u>independent generating set</u> if whenever

$$s_1b_1 + s_2b_2 + \cdots + s_nb_n = 0$$

with $s_i$ in S, then $s_ib_i = 0$ for all i, $1 \le i \le n$. Equivalently, $\{b_1,\cdots,b_n\}$ is an <u>independent generating set</u> for M if

$$M = Sb_1 \oplus \cdots \oplus Sb_n.$$

The set $\{b_i,\sigma_i\}_{i=1}^n$ is a <u>distinguished generating set</u> for the (S-S)-module M if for each i, $1 \le i \le n$, there is an automorphism $\sigma_i$ of S such that

$$sb_i = b_i\sigma_i(s) \text{ for each } s \text{ in } S.$$

We prove that every (S-S)-module M over a Galois ring S possesses a distinguished independent generating set over S.

<u>2.4 THEOREM</u>. Let S be the Galois ring $GR(p^n,r)$ and M be a (S-S)module. Let $\{1,\sigma_2,\cdots,\sigma_r\}$ be the ring automorphisms of S. Then M is the direct sum of cyclic modules

$$M = \oplus \sum_{i=1}^{r} \sum_{j=1}^{n(i)} Sb_{ij}$$

where

$$sb_{ij} = b_{ij}\,\sigma_{k(i)}(s), \text{ for each } s \text{ in } S$$

and $1 \le j \le n(i)$.

Hence $\{b_{ij},\sigma_{k(i)}\}_{i=1,j=1}^{r,n(i)}$ is a distinguished independent generating set for M.

Proof: This follows immediately from theorem 2.3 and the fact that S is a principal ideal ring so that by Jacobson [15, Theorem 43, p. 78] the $M_i$ in (2.3) decompose into the direct sum of cyclic S-modules. That is,

$$M_i = \oplus \sum_{j=1}^{n(i)} Sb_{ij}$$

where $sb_{ij} = b_{ij}\sigma_{k(i)}(s)$ for each $\{b_{ij}\}_{j=1}^{n(i)}$ and s in S.

## 3. STRUCTURE THEOREMS.

Let R be a finite local ring with coefficient subring $S = GR(p^n,r)$. Consider R as a (S-S)-module. By theorem 2.2

$$_SR_S = {}_SS_S \oplus {}_SN_S \text{ as (S-S) modules,}$$

where ${}_SN_S \le Rad(R)$.

Let

$$\{b_{ij},\sigma_{k(i)}\}_{i=1,j=1}^{r,n(i)}$$

be a distinguished independent generating set of ${}_SN_S$ where $\sigma_{k(i)}$ is an automorphism of S. We use this set in arriving at the following main structure theorem for R.

2.5 THEOREM. (Main Structure Theorem)

Let R be a finite local ring of characteristic $p^n$ and coefficient subring $S = GR(p^n,r)$. Let $\{1,\sigma_2,\cdots,\sigma_r\}$ be the ring automorphisms of S. Then R is the homomorphic image of the skew polynomial ring

$S[X_{ij},\sigma_{k(i)}]_{i=1,j=1}^{r,n(i)}$ under the ring homomorphism

$\Phi:X_{ij} \to b_{ij}$ and $\Phi:s \to s$, where the $X_{ij}$ are noncommuting indeterminants such that $sX_{ij} = X_{ij}\,\sigma_{k(i)}(s)$ for $s$ in $S$.

Proof: Since $S = GR(p^n,r)$ we have as noted the distinguished independent generating set $\{1,b_{ij};\sigma_{k(i)}\}_{i=1,j=1}^{r,n(i)}$ for $R$ as a $(S\text{-}S)$-module. The map

$$\Phi:S[X_{ij},\sigma_{k(i)}]_{i=1,j=1}^{r,n(i)} \to R$$

defined by $\Phi(X_{ij}) = b_{ij}$ and $\Phi(s) = s$ is clearly well-defined since each polynomial in $S[X_{ij},\sigma_{k(i)}]_{i=1,j=1}^{r,n(i)}$ has a unique representation in the $X_{ij}$. Further, it is surjective since it takes generators to generators. Thus it only remains to show that $\Phi$ is a ring morphism. $\Phi$ is clearly linear and preserves products since

$$\begin{aligned}\Phi(sX_{kj} \cdot s'X_{hi}) &= \Phi(s\sigma_{k(k)}(s')X_{kj}X_{hi})\\ &= s\sigma_{k(k)}(s')b_{kj}b_{hi}\\ &= sb_{kj}s'b_{hi}\\ &= \Phi(sX_{kj})\Phi(s'X_{hi}).\end{aligned}$$

An ideal structure for $R$ would result if $N \subseteq \mathrm{Rad}(R)$ had a distinguished independent generating set of the form $\{b,b^2,\cdots,b^{m-1},\sigma\}$ where $m$ is the degree of nilpotency of $\mathrm{Rad}(R)$ and $\sigma$ an automorphism of $S$. Then $R = S \oplus Sb \oplus \cdots \oplus Sb^{m-1}$ as $(S\text{-}S)$-modules and also $R$ would be the homomorphic image of $S[X,\sigma]$. In Chapter IV we will show that a chain ring has such a structure.

A natural generalization of this is to replace the cyclic $S$-submodules $(b),\cdots,(b^{m-1})$ by finitely generated $S$-submodules

$T,\cdots,T^{m-1}$. With additional requirements on the (S-S)-submodule N we show that R is the homomorphic image of the finite ring

$$S \oplus T \oplus T^2 \oplus \cdots \oplus T^{m-1}.$$

We require that N be a subring of R such that $N^2$ can be complemented in N; that is, $N = N^2 \oplus T$. Note that to require that N be a subring of R is equivalent to requiring that N be an ideal of R, since $R = S \oplus N$ implies $rn = (s + n')n = sn + n'n$ is in N.

2.6 THEOREM. (Quasi-cyclic Structure Theorem)

Let R be a finite local ring with $\chi(R) = p^n$, the degree of nilpotency of Rad(R) be m and $S = GR(p^n,r)$ the coefficient subring of R.

If ${}_SN_S$ of the decomposition ${}_SR_S = {}_SS_S \oplus {}_SN_S$ is an ideal of R and $N = N^2 \oplus T$ as (S-S)-modules, then R is the ring homomorphic image of

$$S \oplus (N/N^2) \oplus \cdots \oplus (N/N^2)^{m-1}.$$

Proof: We have $N = N^2 \oplus T$ as (S-S)-modules. Let

$$T^{(k)} = T \otimes_S \cdots \otimes_S T \quad (k \text{ factors}) \text{ for } 1 \le k \le m-1.$$

Then $T^{(k)}$ is a natural (S-S)-module. For $1 \le k \le m-1$ we have the following (S-S)-module morphism

$$\theta_k : T^{(k)} \to N \text{ by } \theta_k(t_1 \otimes \cdots \otimes t_k) = t_1 \cdots t_k.$$

It is straight-forward to show by induction that $\theta_k$ is well-defined by showing the corresponding morphism

$$\bar{\theta}_k : T \times \cdots \times T \to N \text{ by } \bar{\theta}_k(<t_1,\cdots,t_k>) = t_1 \cdots t_k$$

is S-balanced and appealing to universal mapping property of tensor product.

Consider the (S-S)-module

$$H = T^{(1)} \oplus \cdots \oplus T^{(m-1)}.$$

The morphisms $\theta_k$ extend linearly to a unique (S-S)-module morphism

$$\sigma: H \to N.$$

Since $N = N^2 \oplus T$ and $N^m = 0$, an element n in N can be written as

$$n = t + t_{i_1} \cdot t_{i_2} + \cdots + t_{j_1} \cdots t_{j_{m-1}}$$

so that

$$\sigma(t + t_{i_1} \otimes t_{i_2} + \cdots + t_{j_1} \otimes \cdots \otimes t_{j_{m-1}}) = n$$

and $\sigma$ is a surjection.

We give $H = T^{(1)} \oplus \cdots \oplus T^{(m-1)}$ a ring structure (without identity) by defining a multiplication on the generators as follows:

For $H_{k_1}$ in $T^{(k_1)}$ and $H_{k_2}$ in $T^{(k_2)}$, define

$$H_{k_1} * H_{k_2} = H_{k_1} \otimes H_{k_2} \text{ (which is in } T^{(k_1+k_2)}) \text{ for } k_1 + k_2 \leq m-1$$

$$= 0 \quad \text{otherwise.}$$

This is clearly a well-defined operation. The associative and distributive properties of * follow since tensor product is associative and bilinear. Since

$$\begin{aligned}\sigma((t_{i_1} \otimes \cdots \otimes t_{i_{k_1}}) * (t_{j_1} \otimes \cdots \otimes t_{j_{k_2}})) &= \sigma(t_{i_1} \otimes \cdots \otimes t_{i_{k_1}} \otimes t_{j_1} \otimes \cdots \otimes t_{j_{k_2}}) \\ &= t_{i_1} \cdots t_{i_{k_1}} \cdot t_{j_1} \cdots t_{j_{k_2}} \\ &= \sigma(t_{i_1} \otimes \cdots \otimes t_{i_{k_1}}) \cdot \sigma(t_{j_1} \otimes \cdots \otimes t_{j_{k_2}})\end{aligned}$$

we have that $\sigma: H \to N$ is a ring morphism.

Let $C = S \oplus H$ as (S-S)-modules. We give C a ring structure (without identity) by defining

$$(s_1, h_1)(s_2, h_2) = (s_1 s_2, s_1 h_2 + h_1 s_2 + h_1 * h_2).$$

Using the distributive property of H as a (S-S)-module and also H as a ring the distributive property is easily verified. The key in showing that H is associative is that tensor product is S-balanced and H is a (S-S)-module, thus we have

$$h_1*(sh_2) = h_1 \otimes sh_2 = h_1 s \otimes h_2 = (h_1 s) * h_2$$

and $s(h_1 * h_2) = s(h_1 \otimes h_2) = sh_1 \otimes h_2 = (sh_1) * h_2$. It is then routine to show that

$$[(s_1,h_1)(s_2,h_2)](s_3,h_3) = (s_1,h_1)[(s_2,h_2)(s_3,h_3)],$$

so that C is a ring (without identity).

We are now in the position to show that R is the homomorphic image of $C = S \oplus H$. Consider the map

$$\gamma: C = S \oplus H \to R \text{ defined by } \gamma(s,h) = s + \sigma(h),$$

where $\sigma: H \to N$ is the ring surjection defined by

$$\sigma(t + t_{i_1} \otimes t_{i_2} + \cdots + t_{j_1} \otimes \cdots \otimes t_{j_{m-1}}) = t + t_{i_1} \cdot t_{i_2} + \cdots + t_{j_1} \cdots t_{j_{m-1}}.$$

Since $\sigma$ is a ring morphism $\gamma$ is clearly linear. Further, $\sigma$ is a (S-S)-module morphism so that

$$\begin{aligned}((s_1,h_1)(s_2,h_2)) &= s_1 s_2 + \sigma(s_1 h_2 + h_1 s_2 + h_1 * h_2) \\ &= s_1 s_2 + s_1 \sigma(h_2) + \sigma(h_1) s_2 + \sigma(h_1)\sigma(h_2) \\ &= \gamma(s_1,h_1)\gamma(s_2,h_2).\end{aligned}$$

Finally $\gamma$ is surjective since $R = S \oplus N$ and $\sigma: H \to N$ is a surjection. Thus R is the homomorphic image of the ring

$$S \oplus H = S \oplus T^{(1)} \oplus \cdots \oplus T^{(m-1)}.$$

But

$$T \simeq (N^2 + T)/N^2 \simeq N/N^2$$

and

$$T^{(k)} = T \otimes \cdots \otimes T = T * \cdots * T = (T)^k \text{ in } C.$$

Thus R is the homomorphic image of

$$S \oplus (N/N^2) \oplus \cdots \oplus (N/N^2)^{m-1}, \text{ where } m$$

is the degree of nilpotency of the ideal N.

The advantage of this theorem over (2.5) is that the ring $S \oplus (N/N^2) \oplus \cdots \oplus (N/N^2)^{m-1}$ is finite, while $S[X_1,\cdots,X_n,\sigma_1,\cdots,\sigma_n]$ is not.

The natural question that arises when considering this proposition is, will ${}_SN_S$ be an ideal of R? We give the following examples to show this may or may not be the case.

Let R be a finite local ring with characteristic p.

Then $S = GR(p,r) = Z/Zp$ is a field. Thus R is an algebra over the field S and by the Wedderburn-Malcev theorem we have $R = S + Rad(R)$ where $S \cap Rad\ R = 0$. Hence $N = Rad(R)$ is a two-sided ideal in R.

On the other hand consider example 4 on page 3. In this ring S has the form

$$\left\{\begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} \mid a \text{ is in } Z/Z4\right\}.$$

Now $N \subseteq Rad(R)$, so every element of N is of the form

$$\left\{\begin{bmatrix} 2a & b \\ 2c & 2d \end{bmatrix} \mid a,b,c \text{ are in } Z/Z4\right\}.$$

Since $\begin{bmatrix} 0 & 1 \\ 2 & 0 \end{bmatrix}$ is in R and $R = S \oplus N$, the element $\begin{bmatrix} 2a & 1 \\ 2 & 2a \end{bmatrix}$ for some a in Z/Z4 must be in N. But then

$$\begin{bmatrix} 2a & 1 \\ 2 & 2a \end{bmatrix}^2 = \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix} \in S$$

and $S \cap N = 0$, so that N cannot be a subring of R.

# CHAPTER III

## THEORY OF SKEW POLYNOMIAL RINGS OVER FINITE LOCAL RINGS

Until recently skew polynomial rings have largely been a source of counter-examples (See Jategaonkar [19]). Ore [22] in 1933 considered skew polynomial rings over fields and division rings developing results directly from the properties of the polynomials themselves. Jacobson in [2, 1943] considered skew polynomial rings over division rings as non-commutative principal ideal domains. The structure of skew polynomial rings over a more general ring was not furthered until recently; for example, see Jategaonkar [17] for structure theorems for skew polynomial rings over semi-simple rings.

We develop the theory of skew polynomial rings over finite local non-commutative rings following the approach of Snapper [25] for polynomial rings over local commutative rings. Although the results of this chapter are developed in the context of finite local rings, slight modification will yield analogous results for local or Artinian local rings.

### 1. BACKGROUND

Let R be a finite local ring with unique maximal ideal M = Rad(R). Let $R[X,\sigma]$ denote the skew polynomial ring where X is an indeterminant and $\sigma$ an automorphism of R such that

$$rX = X\sigma(r) \text{ for } r \text{ in } R.$$

The multiplication in $R[X,\sigma]$ is defined by the distributive property and

$$(aX^m)(bX^n) = a\sigma^m(b)X^{m+n}.$$

We note that since M is nilpotent, $\sigma(M) \subseteq M$ and $\sigma$ maps units to units.

Our technique in studying polynomials will be to "lift" results from $(R/M)[X,\bar{\sigma}]$ under the natural map

$$\mu: R[X,\sigma] \to (R/M)[X,\bar{\sigma}]$$

defined by

$$\mu(r) = r + M = \bar{r}$$

$$\mu(X) = X$$

$$\mu(\sigma) = \bar{\sigma} \text{ where } \bar{\sigma}(\bar{r}) = \sigma(r) + M.$$

We note that $\bar{\sigma}$ is a well-defined automorphism of R/M. Suppose $r + M = s + M$, then $r - s$ is in M. So that $\sigma(r - s) = \sigma(r) - \sigma(s)$ is in M and hence $\sigma(r) + M = \sigma(s) + M$. Further, $\bar{\sigma}(\bar{r}) = \sigma(r) + M = \bar{0}$ if and only if $\sigma(r)$ is in M. Equivalently, r is in M. Thus $\bar{r} = 0$ and we have that $\bar{\sigma}$ is injective. The ring R/M is finite so $\bar{\sigma}$ is also surjective and hence an automorphism of R/M.

Let $f(X) = \sum_{i=0}^{n} a_i X^i$ and $g(X) = \sum_{i=0}^{m} b_i X^i$ be polynomials in $R[X,\sigma]$ where $n < m$. It is clear that $\mu$ is linear. We show that $\mu$ preserves products and is thus a ring morphism.

$$\mu(f \cdot g) = \sum_{k=0}^{n+m} \left(\sum_{i+j=k} \bar{a}_i \, \bar{\sigma}^i(\bar{b}_j)\right) X^{i+j}$$

$$= \left(\sum_{i=0}^{n} \bar{a}_i \, X^i\right)\left(\sum_{j=0}^{m} \bar{b}_j \, X^j\right)$$

$$= \mu(f)\mu(g),$$

where $\sigma^0$ is the identity map of R.

Since much of the theory of $R[X,\sigma]$ depends upon that of the skew polynomial ring $(R/M)[X,\bar{\sigma}]$ where $R/M$ is a finite field we summarize its properties.

Consider the polynomials f and g above, the degree of f, $D(f)$, is n. We define the degree of 0 to be $-\infty$. Then in $(R/M)[X,\bar{\sigma}]$ we have

(1) $D[f \cdot g] = D(f) + D(g)$

(2) $D[f+g] = \max[D(f),D(g)]$.

Since equality holds in (1), $(R/M)[X,\bar{\sigma}]$ has no divisors of zero and is thus an integral domain. The units of $(R/M)[X,\bar{\sigma}]$ are the non-zero elements of $R/M$; that is, the units of R. Further $(R/M)[X,\bar{\sigma}]$ is a Euclidean domain.

Let A be a non-zero right ideal in $(R/M)[X,\bar{\sigma}]$, then a non-zero polynomial in A of least degree generates A. So that $(R/M)[X,\bar{\sigma}]$ is a non-commutative right (or left) principal ideal domain.

Concerning two-sided ideals in $(R/M)[X,\bar{\sigma}]$ we have that any two-sided ideal which is generated on the left by a polynomial f is also generated on the right by f. This follows since if $A = f(R/M)[X,\bar{\sigma}] = (R/M)[X,\bar{\sigma}]g$ then $f = ug$ and $g = fv$ for some u and v in $(R/M)[X,\bar{\sigma}]$. But since uf is in $A = f(R/M)[X,\bar{\sigma}]$ there is a u' such that $uf = fu'$. Now $f = ug = ufv = fu'v$, so that v is a unit since $(R/M)[X,\bar{\sigma}]$ is an integral domain. Similarly u is a unit and thus $g = u^{-1}f$. Hence $f(R/M)[X,\bar{\sigma}] = (R/M)[X,\bar{\sigma}]f$.

## 2. NILPOTENTS, UNITS, AND ZERO DIVISORS IN $R[X,\sigma]$.

We have the following result concerning the nilpotent polynomials in $R[X,\sigma]$.

**3.1 PROPOSITION.** Let f be a polynomial in $R[X,\sigma]$. Then

$f = a_0 + a_1X + \cdots + a_nX^n$ is nilpotent if and only if $a_0, a_1, \cdots, a_n$ are nilpotent; i.e., $a_0, \cdots, a_n$ are in M.

Proof. Suppose $(a_0 + a_1X + \cdots + a_nX^n)^\beta = 0$ for some $\beta > 0$. Then

$$0 = \mu(0) = \mu[(a_0 + \cdots + a_nX^n)^\beta]$$

$$= [\mu(a_0 + \cdots + a_nX^n)]^\beta$$

$$= [\bar{a}_0 + \cdots + \bar{a}_nX^n]^\beta.$$

Thus $\bar{a}_0 + \cdots + \bar{a}_nX^n$ is a zero divisor in $(R/M)[X,\bar{\sigma}]$ and is the zero polynomial; that is, $\bar{a}_0, \cdots, \bar{a}_n$ are zero. Hence $a_0, \cdots, a_n$ are in M.

Conversely suppose $a_0, a_1, \cdots, a_n$ are nilpotent and thus in M. Then if $M^\beta = 0$ we have

$$(a_0 + a_1X + \cdots + a_nX^n)^\beta = \sum_{\langle i_j \rangle} a_{i_1} a_{i_2}^{\sigma^{i_1}} \cdots a_{i_\beta}^{\sigma^{i_1+\cdots+i_{\beta-1}}} X^{i_1+\cdots+i_\beta}$$

where the sum ranges over all the $\beta$-tuples $\langle i_1, \cdots, i_\beta \rangle$ with $0 \le i_j \le n$. But each term of this sum has its coefficient in $M^\beta$ so that the sum is zero and f is nilpotent.

In general, this theorem is not true for a skew polynomial ring.

Example: Let $R = k \oplus k$ where k is a field, then R is not local. Let $\sigma: R \to R$ be defined by $\sigma\langle i,j \rangle = \langle j,i \rangle$. Then in $R[X,\sigma]$ we have

$$(\langle 1,0 \rangle X)^2 = \langle 1,0 \rangle X \langle 1,0 \rangle X = \langle 1,0 \rangle \langle 0,1 \rangle X^2$$

$$= \langle 0,0 \rangle X^2 = 0,$$

while $(\langle 1,0 \rangle)^n = \langle 1,0 \rangle$ for every integer n.

Concerning units in $R[X,\sigma]$ we have the following result.

3.2 PROPOSITION. The polynomial $f = a_0 + a_1X + \cdots + a_nX^n$ in $R[X,\sigma]$ is a unit if and only if $a_0$ is a unit of R and $a_1, \cdots, a_n$ are in M.

Proof. Suppose $a_1,\cdots,a_n$ are in M and $a_0$ is a unit of R. Then $a_0^{-1}a_1,\cdots,a_0^{-1}a_n$ are in M and thus by (3.1)

$$a_0^{-1}a_1x^1 + \cdots + a_0^{-1}a_nx^n$$

is nilpotent so that

$$1 + a_0^{-1}a_1x^1 + \cdots + a_0^{-1}a_nx^n$$

is a unit of $R[X,\sigma]$. Hence

$$a_0(1 + a_0^{-1}a_1x^1 + \cdots + a_0^{-1}a_nx^n) = a_0 + a_1x^1 + \cdots + a_nx^n$$

is a unit of $R[X,\sigma]$.

Conversely suppose $f = a_0 + a_1x^1 + \cdots + a_nx^n$ is a unit of $R[X,\sigma]$. Then $\mu(f) = \bar{a}_0 + \bar{a}_1x^1 + \cdots + \bar{a}_nx^n$ is a unit in $(R/M)[X,\bar{\sigma}]$ so that $\bar{a}_0 \neq 0$ and $\bar{a}_1,\cdots,\bar{a}_n$ are zero. Thus $a_0$ is not in M so a unit of R, while $a_1,\cdots,a_n$ are in M.

We have the following result due to Castillion [1, Thm. 1] which is well-known for commutative rings and generalizes to skew polynomial rings.

3.3 PROPOSITION. (Hilbert basis theorem)

If R is Noetherian, then $R[X,\sigma]$ is Noetherian.

It is well-known that in Noetherian rings nil ideals are nilpotent. (For example, see Lambek, p. 70). Let $M[X,\sigma]$ denote the ideal of $R[X,\sigma]$ consisting of polynomials whose coefficients are contained in the maximal ideal $M = \mathrm{Rad}(R)$. Then, since $M[X,\sigma]$ is a nil ideal in the Noetherian ring $R[X,\sigma]$, $M[X,\sigma]$ is nilpotent.

As is in the case of R, the various well-known radicals of $R[X,\sigma]$ are equivalent.

3.4 PROPOSITION. Let $R[X,\sigma]$ be a skew polynomial ring over a finite local ring R. Then the following sets are equal.

(1) $\cup\{B \mid B$ is a two-sided nilpotent ideal of $R[X,\sigma]\}$.

(2) $\{f$ in $R[X,\sigma] \mid f^n = 0$ for some integer $n\}$.

(3) $\{f$ in $R[X,\sigma] \mid 1 + fg$ is a unit of $R[X,\sigma]$ for each $g$ in $R[X,\sigma]\}$.

(4) $(\mathrm{Rad}(R))[X,\sigma] = M[X,\sigma]$.

We denote by $\mathrm{Rad}(R[X,\sigma])$ any of the above ideals.

Proof. From (3.1) and the preceding remarks we have that the sets (1), (2) and (3) are equivalent. If $f$ is nilpotent in $R[X,\sigma]$ then by (3.2) $1 + f$ is a unit of $R[X,\sigma]$ and thus $f$ is in set (3). If $f = a_0 + a_1X^1 + \cdots + a_nX^n$ is in set (3) then

$$1 + (a_0 + a_1X^1 + \cdots + a_nX^n)X = 1 + a_0X + \cdots + a_nX^{n+1}$$

is a unit of $R[X,\sigma]$ and thus by (3.2) $a_0,\cdots,a_n$ are in $M$. Hence $f$ is in set (4), and all are equivalent.

We will have occasion to consider the ring $R[X,\sigma]/A$ and its radical where $A$ is an ideal of $R[X,\sigma]$. Since by (3.3) $R[X,\sigma]$ is Noetherian, $A$ is finitely generated by say $f_1,\cdots,f_t$. Two cases should be noted. If one of the $f_i$ is not in $M[X,\sigma]$, then $R[X,\sigma]/A$ is a finite ring and its radical is given by (1.1). On the other hand, if each $f_i$ is in $M[X,\sigma]$ then $A$ is in $M[X,\sigma]$. In this case, $r(A) = \{f$ in $R[X,\sigma] \mid$ for some integer $n$, $f^n$ is in $A\}$ is precisely the ideal $M[X,\sigma]$ and $\mathrm{Rad}(R[X,\sigma]/A) = M[X,\sigma]$.

We show that in the case that $R[X,\sigma]/A$ is finite the

$$\mathrm{Rad}(R[X,\sigma]/A) = \{\bar{f} \text{ in } R[X,\sigma]/A \mid f^n \text{ is in } A \text{ for } f \text{ in } R[X,\sigma] \text{ with } \mu(f) = (\bar{f})\}$$

Since $R[X,\sigma]/A$ is finite, by McDonald [21]

$$S = (R[X,\sigma]/A) / \mathrm{Rad}(R[X,\sigma]/A)$$

$$\simeq \oplus \sum_{i=1}^{t} M_{n_i}(k_i)$$

where $M_{n_i}(k_i)$ is an $n_i \times n_i$ matrix ring over a finite field. But on the other hand S is the homomorphic image of the non-commutative principal ideal domain $(R/M)[X,\bar{\sigma}]$. This follows by considering the following composition of natural homomorphisms

$$\beta: R[X,\sigma] \to R[X,\sigma]/A \to S.$$

Now $\beta(\mathrm{Rad}(R[X,\sigma])) \subseteq \mathrm{Rad}(S) = 0$, and thus by the "induced homomorphism theorem" there exists a homomorphism taking $(R/M)[X,\bar{\sigma}]$ to S.

It is now clear that $n_i = 1$ for $1 \leq i \leq t$, and thus $S = \oplus \sum_{i=1}^{t} k_i$ is a direct sum of fields $k_i$. Hence S contains no nilpotent elements, so that if $\bar{f}$ in $R[X,\sigma]/A$ is nilpotent it is contained in $\mathrm{Rad}(R[X,\sigma]/A)$.

Conversely, by (1.1) if $\bar{f}$ is in $\mathrm{Rad}(R[X,\sigma]/A)$ then $\bar{f}$ is nilpotent.

Hence $\mathrm{Rad}(R[X,\sigma]/A) = \{\bar{f}$ in $R[X,\sigma]/A \mid f^n$ is in A for f in $R[X,\sigma]$ with $\mu(f) = \bar{f}\}$.

A ring R is <u>right primary</u> provided $ab = 0$ and $a \neq 0$ implies b is in $\mathrm{Rad}(R)$. We define <u>left primary</u> analogously. The ring R is <u>primary</u> if it is both left and right primary.

<u>3.5 PROPOSITION</u>. Let R be a finite local ring with $\mathrm{Rad}(R) = M$. Then

(1) R is primary.

(2) $R[X,\sigma]$ is primary.

<u>Proof</u>. (1) Suppose $ab = 0$ and $a \neq 0$. Then b is in M. For if not, b is a unit. In which case $abb^{-1} = a = 0$.

(2) Let n be the degree of nilpotency of M. The proof is by induction on the smallest integer n such that $M^n = 0$.

If $n = 1$, then $R[X,\sigma]$ is right primary. For suppose $fg = 0$ and $f \neq 0$, then $g = 0$ is in $M[X,\sigma] = \text{Rad}(R[X,\sigma])$ since $R[X,\sigma]$ is an integral domain.

Assume that all finite local rings R with M of nilpotency k; i.e., such that $M^k = 0$, have $R[X,\sigma]$ a right primary ring.

Consider a finite local ring R with $M^{k+1} = 0$ and $M^k \neq 0$. We show that $R[X,\sigma]$ is right primary. The ring $R/M^k$ is local and has radical $M/M^k$. The degree of nilpotency of $M/M^k$ is k, so by the induction hypothesis $(R/M^k)[X,\sigma]$ is right primary.

Now suppose f and g are in $R[X,\sigma]$ with $fg = 0$, $f \neq 0$ and g is not in $\text{Rad}(R[X,\sigma])$. Then, since $(R/M)[X,\sigma]$ is an integral domain and $\bar{f}\bar{g} = \bar{0}$ with $\bar{g} \neq \bar{0}$, we conclude f is in $M[X,\sigma]$. If we can show f is not in $M^k[X,\sigma]$ we are done. For if $\bar{f}\bar{g} = \bar{0}$ in $(R/M^k)[X,\sigma]$ and $f \neq 0$, then because $(R/M^k)[X,\sigma]$ is primary by above, we conclude that $\bar{g}$ is in $\text{Rad}((R/M^k)[X,\bar{\sigma}]) = (M/M^k)[X,\bar{\sigma}]$. Hence g is in $M[X,\sigma]$ which is a contradiction. Thus $R[X,\sigma]$ will be right primary.

We now show f is not in $M^k[X,\sigma]$. Suppose $f = b_r X^r + \cdots + b_0$ is in $M^k[X,\sigma]$ where $b_r \neq 0$. Since g is not in $M[X,\sigma]$, let $a_s$ be the coefficient of the highest power of X in g which is not in M. Since $M^{k+1} = 0$ and $fg = 0$ we have the term $a_s\sigma^s(b_r)X^{s+r} = 0$ in the product of f and g. But $b_r \neq 0$ so the automorphism $\sigma^s$ does not take $b_r$ to zero. Thus since R is primary by (1) and $\sigma^s(b_r) \neq 0$ we conclude $a_s$ is in $\text{Rad}(R) = M$. But this contradicts the choice of $a_s$.

Hence $R[X,\sigma]$ is right primary. In a similar fashion $R[X,\sigma]$ is left primary, thus primary.

We have the following important corollary.

3.6 COROLLARY. Let f be in $R[X,\sigma]$. Then f is a zero divisor if and only if f is in $M[X,\sigma]$.

Proof. If f is in $M[X,\sigma]$, then by (3.1) f is nilpotent of say degree n. Then $ff^{n-1} = 0$ with $f^{n-1} \neq 0$ so that f is a zero divisor.

On the other hand if $fg = 0$ and $g \neq 0$, since $R[X,\sigma]$ is primary f is in $\text{Rad}(R[X,\sigma]) = M[X,\sigma]$.

Many of the results concerning polynomials in $R[X,\sigma]$ will result from the fact that the divisors of zero are contained in the $\text{Rad}(R[X,\sigma]) = M[X,\sigma]$. The following illustrates this.

3.7 PROPOSITION. If f in $R[X,\sigma]$ is a right (or left) unit, then f is a unit of $R[X,\sigma]$.

Further, if fg is a unit, both f and g are units.

Proof. Suppose $fg = 1$, then $gfg = g$ so that $(1 - gf)g = 0$. Thus since $R[X,\sigma]$ is primary and $g \neq 0$ we conclude by (3.6) that $1 - gf$ is in $\text{Rad}(R[X,\sigma])$. Let $h = 1 - gf$, then $gf = 1 - h$ is a unit of $R[X,\sigma]$, so that $(gf)^{-1}gf = 1$. Hence f is a left unit and thus a unit of $R[X,\sigma]$.

If fg is a unit, then $(fg)h = f(gh) = 1$ and $k(fg) = (kf)g = 1$ for some h and k in $R[X,\sigma]$. Thus f is a right unit and g is a left unit and hence a unit of $R[X,\sigma]$.

3.8 PROPOSITION. Let f and g be non-zero polynomials in $R[X,\sigma]$. If $fg = f$ or $gf = f$, then g is a unit. Hence 1 is the only non-zero idempotent in $R[X,\sigma]$.

Proof. Suppose f and g are non-zero polynomials such that $fg = f$, then $f(g - 1) = 0$ so that $g - 1$ is in $\text{Rad}(R[X,\sigma])$. Thus $g = 1 + z$ for some in $\text{Rad}(R[X,\sigma])$. Hence g is a unit of $R[X,\sigma]$. Similarly if $gf = f$ we conclude g is a unit.

Further suppose f is a non-zero idempotent of $R[X,\sigma]$. Then $ff = f$ so that f is a unit. Hence,

$$f = (f^{-1}f)f = f^{-1}f^2 = f^{-1}f = 1.$$

## 2. RELATIONSHIPS BETWEEN PROPERTIES OF $(R/M)[X,\bar{\sigma}]$ AND THOSE IN $R[X,\sigma]$.

We have the following obvious relationship between the units of $R[X,\sigma]$ and the units of $(R/M)[X,\bar{\sigma}]$. Let $\mu: R[X,\sigma] \to (R/M)[X,\bar{\sigma}]$.

3.9 PROPOSITION. A polynomial f in $R[X,\sigma]$ is a unit if and only if $\bar{f} = \mu(f)$ is a unit of $(R/M)[X,\sigma]$.

Proof. By (3.2) if f is a unit then $\bar{f}$ is non-zero and hence a unit of $(R/M)[X,\bar{\sigma}]$.

Conversely suppose $fg + M[X,\sigma] = 1 + M[X,\sigma]$ then $1 - fg$ is in $M[X,\sigma] = \mathrm{Rad}(R[X,\sigma])$. Let $1 - fg = z$. Then $fg = 1 - z$ is a unit of $R[X,\sigma]$, so that by (3.7) f is a unit of $R[X,\sigma]$.

Two right ideals $Q_1$ and $Q_2$ of $R[X,\sigma]$ are relatively prime if $Q_1 + Q_2 = R[X,\sigma]$. We say two polynomials f and g of $R[X,\sigma]$ are relatively prime if as right ideals $fR[X,\sigma] + gR[X,\sigma] = R[X,\sigma]$.

By applying the preceding proposition (3.9) on units we have the following immediate result.

3.10 PROPOSITION. The right ideals $Q_1$ and $Q_2$ are relatively prime in $R[X,\sigma]$ if and only if $\bar{Q}_1$ and $\bar{Q}_2$ are relatively prime right ideals in $(R/M)[X,\bar{\sigma}]$.

The non-zero polynomials f and g of $R[X,\sigma]$ are called right associates if $fR[X,\sigma] = gR[X,\sigma]$, left associates if $R[X,\sigma]f = R[X,\sigma]g$, and associates if both left and right associates.

Since $R[X,\sigma]$ is a primary ring we have the following characterization of the associates of $R[X,\sigma]$.

3.11 PROPOSITION. The polynomials f and g in $R[X,\sigma]$ are right associates if and only if $f = gu$ where u is a unit of $R[X,\sigma]$.

Proof. If $fR[X,\sigma] = gR[X,\sigma]$, then $f = gu$ and $g = fv$ for u and v in $R[X,\sigma]$. Thus $f = fvu$ and by (3.8) and (3.7) u and v are units of $R[X,\sigma]$.

With this characterization the following is clear.

3.12 PROPOSITION. If f and g are right (left) associates in $R[X,\sigma]$, then $\bar{f}$ and $\bar{g}$ are right (left) associates in $(R/M)[X,\bar{\sigma}]$.

If f and g are non-zero polynomials in $R[X,\sigma]$, f is called a left factor or right divisor of g if $gR[X,\sigma] \subseteq fR[X,\sigma]$, that is $g = fh$ for some h in $R[X,\sigma]$. We may similarly define right factors or left divisors and proper divisors.

Again the following is immediate.

3.13 PROPOSITION. If f is a right divisor in $R[X,\sigma]$, then $\bar{f}$ is a right divisor in $(R/M)[X,\bar{\sigma}]$.

A polynomial f of $R[X,\sigma]$ is called irreducible if $f = gh$ for some g and h in $R[X,\sigma]$ implies that either g or h is a unit of $R[X,\sigma]$. The polynomial f is called a fundamental irreducible if its coset $\bar{f} = f + M[X,\sigma]$ is irreducible in $(R/M)[X,\bar{\sigma}]$.

3.14 PROPOSITION. Let f be a polynomial in $R[X,\sigma]$.

(1) If f is a unit, then f is irreducible.

(2) If $\bar{f}$ is irreducible in $(R/M)[X,\bar{\sigma}]$, then f is irreducible in $R[X,\sigma]$.

Proof. Part (1) is immediate from (3.7).

For part (2) suppose $f = gh$ is in $R[X,\sigma]$. Then $\bar{f} = \bar{g}\bar{h}$ in $(R/M)[X,\bar{\sigma}]$ and hence by hypothesis $\bar{g}$ or $\bar{h}$ is a unit. Thus by (3.9) g or h is a unit of $R[X,\sigma]$.

A polynomial f in $R[X,\sigma]$ is called regular if f is not a zero divisor. By (3.6) f is regular if f is not in $M[X,\sigma]$. An ideal I in $R[X,\sigma]$ is regular if $I \not\subseteq M[X,\sigma]$; i.e., I is not nilpotent. We show that the form of regular polynomials closely resemble units in $R[X,\sigma]$.

3.15 PROPOSITION. Let $f = a_0 + a_1X^1 + \cdots + a_nX^n$ be in $R[X,\sigma]$. The following are equivalent.

(1) f is regular.

(2) $a_i$ is a unit for some i, $1 \leq i \leq n$.

(3) $\bar{f} \neq 0$.

(4) $\bar{f}$ is regular.

Proof. This follows immediately from the fact that the non-units of R are M, R/M is a field, and $(R/M)[X,\bar{\sigma}]$ is an integral domain.

An ideal P of $R[X,\sigma]$ is prime if for f and g in $R[X,\sigma]$ with $fR[X,\sigma]g \subseteq P$, then f or g is in P. We also have the more restricted definition, that is, an ideal P of $R[X,\sigma]$ is completely prime if for f and g in $R[X,\sigma]$ with fg in P, then f or g is in P. Equivalently, P is completely prime if $R[X,\sigma]/P$ is an integral domain. An ideal P of $R[X,\sigma]$ is maximal right if $R[X,\sigma]/P$ is a finite field. Thus maximal right implies completely prime.

3.16 PROPOSITION. An ideal P in $R[X,\sigma]$ is completely prime (maximal right) if and only if

(1) $M[X,\sigma] \subseteq P$

(2) $\bar{P}$ is a completely prime (maximal right) ideal of $(R/M)[X,\bar{\sigma}]$.

Proof. Suppose P is a completely prime ideal of $R[X,\sigma]$. Then if f is in $M[X,\sigma]$, f is nilpotent and thus since $f^n = 0$ is in P for some n; we conclude that f is in P. Now if P is a maximal right then it is completely

prime so that $M[X,\sigma] \subseteq P$.

If $M[X,\sigma] \subsetneq P$, then we have

$$(R/M)[X,\bar{\sigma}]/(P/(M[X,\sigma])) \simeq (R[X,\sigma]/M[X,\sigma])/(P/(M[X,\sigma]))$$
$$\simeq R[X,\sigma]/P,$$

so that $(R/M)[X,\bar{\sigma}]/\bar{P}$ is an integral domain (finite field) if and only if $R[X,\sigma]/P$ is an integral domain (finite field).

By (3.1) we have the following corollary.

3.17 COROLLARY. If the ideal $M[X,\sigma]$ is completely prime then $M[X,\sigma]$ is the only nilpotent completely prime ideal $R[X,\sigma]$ contains.

## 3. PRIMARY IDEALS

Let A be an ideal in $R[X,\sigma]$. Then we define the radical of A denoted as $r(A)$ to be

$$r(A) = \{f \text{ in } R[X,\sigma] \mid f^n \text{ is in } A \text{ for some } n\}.$$

In general $r(A)$ need not be an ideal. (See McCoy [20, p. 31]). We will be interested only in $r(Q)$ where Q is a primary ideal. In this case $r(Q)$ is an ideal of $R[X,\sigma]$.

An ideal Q of $R[X,\sigma]$ is right primary if fg is in Q and f not in Q implies $g^n$ is in Q for some integer n. Q is left primary if fg is in Q and g not in Q implies $f^n$ is in Q for some integer n. Further, an ideal Q is primary if it is both left and right primary.

3.18 THEOREM. Let Q be a primary ideal in $R[X,\sigma]$. Then $r(Q)$ is an ideal of $R[X,\sigma]$.

Proof. Recall from comments following (3.4) that for Q an ideal of $R[X,\sigma]$

$$\text{Rad}(R[X,\sigma]/Q) = \{\bar{f} \text{ in } R[X,\sigma]/Q \mid f^n \in Q$$
$$\text{for } f \text{ in } R[X,\sigma] \text{ with } \mu(f) = \bar{f}\}.$$

Thus the natural morphism

$$\mu: R[X,\sigma] \to R[X,\sigma]/Q$$

maps $r(Q) = \{f \text{ in } R[X,\sigma] \mid f^n \text{ is in } Q \text{ for some } n\}$ onto $\text{Rad}(R[X,\sigma]/Q)$.

Let f and g be in $r(Q)$. Then $\mu(f)$ and $\mu(g)$ are in the ideal $\text{Rad}(R[X,\sigma]/Q)$. Thus $\mu(f) + \mu(g) = \mu(f+g)$ is in $\text{Rad}(R[X,\sigma]/Q)$, so there is an h in $r(Q)$ and t in Q such that

$$f + g = h + t.$$

Let m be such that $h^m$ is in Q. Then since Q is an ideal $(f+g)^m = (h+t)^m$ is in Q. Hence $f + g$ is in $r(Q)$.

Further $r(Q)$ is closed under right and left multiplication by elements of $R[X,\sigma]$, for suppose f is in $r(Q)$ and n is the least integer such that $f^n$ is in Q. Since Q is an ideal, $hf^n$ is in Q for h in $R[X,\sigma]$. If $n > 1$, then $(hf)f^{n-1}$ is in Q and $f^{n-1}$ not in Q implies $(hf)^m$ is in Q for some integer m. Thus hf is in $r(Q)$. If $n = 1$, then hf is in $Q \subseteq r(Q)$. In a similar fashion $r(Q)$ is a right ideal.

Since $r(Q)$ is an ideal when Q is primary we have

$$\text{Rad}(R[X,\sigma]/Q) = r(Q)/Q.$$

The radical of a primary ideal has the following properties. The proof of which follows the commutative case and the fact

$$r(\bar{Q}) = r(Q + M[X,\sigma]) = r(Q) + M[X,r] = \overline{r(Q)}$$

since $M[X,\sigma]$ is nilpotent.

3.19 PROPOSITION. If P and Q are primary ideals in $R[X,\sigma]$, then

(1) $r(\bar{Q}) = \overline{r(Q)}$.

(2) $r(\bar{P}) \subseteq r(\bar{Q})$ if and only if $r(P) \subseteq r(Q)$.

Further, we have the following isomorphisms which follow from the

inclusions:

$$Q \subseteq r(Q) \quad \text{and} \quad M[X,\sigma] \subseteq r(Q):$$

$$\begin{aligned}(R[X,\sigma]/Q)/\mathrm{Rad}(R[X,\sigma]/Q) &\cong (R[X,\sigma]/Q)/(r(Q)/Q)\\ &\cong R[X,\sigma]/r(Q)\\ &\cong (R[X,\sigma]/M[X,\sigma])/(r(Q)/M[X,\sigma])\\ &\cong ((R/M)[X,\bar{\sigma}])/\overline{r(Q)}.\end{aligned}$$

Thus we have immediately that if Q is a nilpotent primary ideal in $R[X,\sigma]$, then

$$(R[X,\sigma]/Q)/\mathrm{Rad}(R[X,\sigma]/Q) \cong R/M[X,\bar{\sigma}].$$

The characterization of the primary ideals of $R[X,\sigma]$ will depend largely upon the following theorem.

3.20 THEOREM. Let P be a non-trivial ideal in $(R/M)[X,\bar{\sigma}]$. Then P is completely prime if and only if P is maximal right.

Proof. If P is maximal right then $(R/M)[X,\bar{\sigma}]/P$ is a finite field and hence an integral domain.

To show the converse we again note that in $(R/M)[X,\bar{\sigma}]$ a left generator of a two-sided ideal is also a right generator. Thus assume that $P = f(R/M)[X,\bar{\sigma}] = (R/M)[X,\bar{\sigma}]f$ is a non-trivial completely prime ideal and let $I = g(R/M)[X,\bar{\sigma}]$ be a right ideal such that $P \subset I \subset (R/M)[X,\bar{\sigma}]$. Then $f = gh$ for some h in $(R/M)[X,\bar{\sigma}]$. But P is completely prime so either g or h is in P. If g is in P then $I = P$; on the other hand if h is in $P = (R/M)[X,\bar{\sigma}]f$, then $h = kf$ for some k in $(R/M)[X,\bar{\sigma}]$. Thus $f = gh = gkf$. By (3.8) $gk = 1$ and hence $I = (R/M)[X,\bar{\sigma}]$. In either case we have a contradiction so that P is a maximal right ideal.

3.21 PROPOSITION. Let Q be an ideal in $R[X,\sigma]$. If r(Q) is an ideal and

is maximal right, then Q is primary.

Proof. We have $(R[X,\sigma]/Q)/\mathrm{Rad}(R[X,\sigma]/Q) \cong (R[X,\sigma]/Q)/(r(Q)/Q) \cong R[X,\sigma]/r(Q)$ is a finite field since $r(Q)$ is maximal right. Thus $R[X,\sigma]/Q$ is a local ring, so that the divisors of zero are nilpotent. Suppose $fg$ is in Q and f not in Q, then $f \neq 0$ in $R[X,\sigma]/Q$. But $fg = 0$ and g is nilpotent. Thus $g^n$ is in Q for some integer n, and Q is right primary. Similarly Q is left primary, hence primary.

Concerning the nilpotent primary ideals in $R[X,\sigma]$ we have a primary ideal Q is nilpotent if and only if $Q \subseteq M[X,\sigma]$. Further, $r(Q) = M[X,\sigma]$. Suppose f is in $r(Q)$, then $f^n$ is in $Q \subseteq M[X,\sigma]$ for some integer n. Conversely, if f is in $M[X,\sigma]$, then $f^m = 0$ is in Q for some integer m, so that f is in $r(Q)$.

Thus if $M[X,\sigma]$ is maximal right, by the above proposition every nilpotent ideal is primary.

The following proposition characterizes the non-trivial primary ideals which are not nilpotent.

3.22 PROPOSITION. Let Q be a non-trivial non-nilpotent ideal in $R[X,\sigma]$.

(1) Q is completely prime if and only if Q is maximal right.

(2) Q is primary if and only if $r(Q)$ is completely prime.

Proof. (1) If Q is completely prime by (3.16) $M[X,\sigma] \subseteq Q$ and $\bar{Q}$ is non-trivial and completely prime in $(R/M)[X,\bar{\sigma}]$. Thus by (3.20) $\bar{Q}$ is maximal right, and by (3.16) Q is maximal right.

The converse is clear since $(R)[X,\sigma]/Q$ is a finite field.

(2) Suppose that Q is a primary ideal in $R[X,\sigma]$. Then $r(Q)$ is completely prime. For assume $fg$ is in $r(Q)$; i.e., $(fg)^n$ is in Q for some integer n. Then consider the product $fgfg\cdots fg$ (2n factors). Let

$a_{i_1},\cdots,a_{i_k}$ be the smallest subcollection of the f and g's such that $a_{i_1}\cdots a_{i_k}$ is in Q. Then since Q is primary and k minimal $a_{i_1}\cdots a_{i_{k-1}}$ is not in Q and thus $a_{i_k}$ is in $Q \subseteq r(Q)$. But $a_{i_k}$ is either f or g, so that f or g is in r(Q) whenever fg is in r(Q). Hence r(Q) is completely prime.

Conversely, suppose Q is such that r(Q) is completely prime. We may suppose $r(Q) \subset R[X,\sigma]$ for otherwise it is clear that $r(Q) = R[X,\sigma]$ implies Q is primary. Now since r(Q) is primary, $M[X,\sigma] \subset r(Q) \subset R[X,\sigma]$, and hence $\overline{r(Q)}$ is a non-trivial completely prime ideal in $(R/M)[X,\bar{\sigma}]$. Thus by (3.20) $\overline{r(Q)}$ is maximal right and by (3.16) r(Q) is maximal right, so that by (3.21) Q is primary.

We are now in a position to give the relationship between primary ideals in $R[X,\sigma]$ and their images in $(R/M)[X,\bar{\sigma}]$.

3.23 PROPOSITION.

(1) If Q is a primary ideal in $R[X,\sigma]$, then $\bar{Q}$ is primary in $(R/M)[X,\bar{\sigma}]$.

(2) The ideal Q is non-nilpotent and primary in $R[X,\sigma]$ if and only if $\bar{Q}$ is a non-zero primary ideal in $(R/M)[X,\bar{\sigma}]$.

Proof. If Q is primary and $Q \subseteq M[X,\sigma]$; i.e., Q is nilpotent, then $\bar{Q} = 0$ and is primary since $(R/M)[X,\bar{\sigma}]$ is an integral domain. Thus we only need to prove part (2).

Suppose Q is a non-nilpotent primary ideal, then $Q \not\subseteq M[X,\sigma]$ and r(Q) is completely prime by (3.22, part (2)). Thus $\overline{r(Q)} = r(\bar{Q}) \neq 0$ is a completely prime non-nilpotent ideal in $(R/M)[X,\bar{\sigma}]$ so that by (3.22) $\bar{Q}$ is primary.

Conversely, suppose $\bar{Q} \neq 0$ is primary. Then Q is not nilpotent in

$R[X,\sigma]$. Thus $r(Q)$ is either $R[X,\sigma]$ or is maximal right. In both cases by (3.22) $Q$ is primary.

As previously noted, if $f$ is a left generator of an ideal in $(R/M)[X,\bar{\sigma}]$, then $f$ is a right generator. In $(R/M)[X,\bar{\sigma}]$ we will denote the ideal $f(R/M)[X,\bar{\sigma}] = (R/M)[X,\bar{\sigma}]f$ by $(f)$.

We now characterize a generator of a primary ideal in $(R/M)[X,\bar{\sigma}]$.

3.24 PROPOSITION. If $Q = (f)$ is a primary ideal in $(R/M)[X,\bar{\sigma}]$ with $r(Q) = (g)$, then $g$ is irreducible and $f = vg^n = g^n u$ for some integer $n$ and $u,v$ units of $(R/M)[X,\sigma]$.

Proof. The polynomial $g$ is irreducible, for suppose $g = rs$. Then $r(Q) = (g)$ is completely prime by (3.22); so that $r$ or $s$ is in $(g)$. If $r$ is in $(g)$ then $r = gt$ for some $t$ in $(R/M)[X,\bar{\sigma}]$. Thus $g = gts$ and by (3.8) $s$ is a unit. Similarly if $s$ is in $(g)$ then $t$ is a unit. Therefore $g$ is irreducible.

Further, since $Q \subseteq r(Q)$ we have $(f) \subseteq (g)$ where $g$ is irreducible. Let $f = gh$ for some $h$ in $(R/M)[X,\bar{\sigma}]$. Since $(f) = Q$ is primary, if $g$ is not in $(f)$, then $h^n$ is in $(f)$ for some integer $n$. Thus $h$ is in $r((f)) = (g)$, so that $h = gk$ and $f = g^2k$ for $k$ in $(R/M)[X,\bar{\sigma}]$. Since $(R/M)[X,\bar{\sigma}]$ is a non-commutative principal ideal domain by Jacobson [15, p. 34, Thm. 5] this process finally gives an integer $n$ such that $f = g^n u$ where $g^n$ is in $(f)$. But $g^{n-1}$ is not in $(f)$. (Otherwise $f$ would not factor into a unique number of irreducible factors). Now $g^n = fd$ for some $d$ in $(R/M)[X,\bar{\sigma}]$ so that $f = fud$ and thus $u$ is a unit of $(R/M)[X,\bar{\sigma}]$. In a similar fashion $f = vg^n$ where $v$ is a unit.

This representation of the primary ideal $Q = (f)$ in $(R/M)[X,\bar{\sigma}]$ may be "lifted" to $R[X,\sigma]$.

3.25 LEMMA. If $Q$ is an ideal in $R[X,\sigma]$, then there is an $f$ in $Q$ such that

$$Q = R[X,\sigma]f + N = fR[X,\sigma] + N$$

where $N = M[X,\sigma] \cap Q$.

Proof. If $Q$ is an ideal in $R[X,\sigma]$, then $\bar{Q} = (\bar{f})$ in $(R/M)[X,\bar{\sigma}]$. Let $f$ be a preimage in $Q$ of $\bar{f}$. Clearly $fR[X,\sigma] + M[X,\sigma] \cap Q \subseteq Q$. On the other hand suppose $g$ is in $Q$. Then $\bar{g} = \bar{f}\bar{h}$ for some $\bar{h}$ in $(R/M)[X,\bar{\sigma}]$. If $h$ is a preimage of $\bar{h}$, then $g = fh + m$ where $h$ is in $R[X,\sigma]$ and $m$ in $M[X,\sigma]$. Since $m = g - fh$, $m$ is also in $Q$ and thus in $M[X,\sigma] \cap Q$. Hence we have $Q = fR[X,\sigma] + M[X,\sigma] \cap Q$ and in a similar fashion $Q = R[X,\sigma]f + M[X,\sigma] \cap Q$.

3.26 THEOREM. Let $Q$ be a non-trivial, non-nilpotent primary ideal in $R[X,\sigma]$. Then

$$Q = (ug^n + m)R[X,\sigma] + M[X,\sigma] \cap Q$$

$$= R[X,\sigma](ug^n + m) + M[X,\sigma] \cap Q$$

where $u$ is a unit, $g$ is a fundamental irreducible, and $m$ is in $M[X,\sigma]$ in the ring $R[X,\sigma]$.

Further $r(Q) = gR[X,\sigma] + M[X,\sigma]$ and $R[X,\sigma]/(r(Q))$ is a finite field.

Proof. Let $Q$ be a non-trivial, non-nilpotent primary ideal. Then by Lemma 3.25 there is a $f$ in $Q$ such that

$$Q = fR[X,\sigma] + M[X,\sigma] \cap Q = R[X,\sigma]f + M[X,\sigma] \cap Q.$$

Then $\bar{Q} = (\bar{f})$ is primary in $(R/M)[X,\bar{\sigma}]$, and by (3.24) $r(\bar{Q}) = (\bar{g})$ and $\bar{f} = \bar{u}\bar{g}^n = \bar{g}^n\bar{v}$ where $\bar{u},\bar{v}$ are units and $\bar{g}$ irreducible in $(R/M)[X,\bar{\sigma}]$. Hence $f = g^n v + m = ug^n + m$ where $g$ is a fundamental irreducible, $u,v$ units, and $m$ in $M[X,\sigma]$ in $R[X,\sigma]$.

Now $\bar{Q} = (\bar{f}) = \bar{g}^n\bar{v}(R/M)[X,\bar{\sigma}]$. But $(R/M)[X,\bar{\sigma}]$ is a right principal ideal domain and $\bar{g}$ irreducible so $\bar{g}(R/M)[X,\bar{\sigma}]$ is maximal right in

$(R/M)[X,\bar{\sigma}]$. Hence $r(\bar{Q}) \subseteq g(R/M)[X,\bar{\sigma}]$; but also it is clear that $g(R/M)[X,\bar{\sigma}] \subseteq \bar{Q} \subseteq r(\bar{Q})$. Thus $\overline{r(Q)} = r(\bar{Q}) = g(R/M)[X,\bar{\sigma}]$ and $r(Q) = gR[X,\sigma] + M[X,\sigma]$.

Since Q is a non-trivial non-nilpotent primary ideal, by (3.22) r(Q) is completely prime and hence maximal right. Thus $R[X,\sigma]/r(Q)$ is a finite field.

3.27 PROPOSITION. Let Q be a non-trivial, non-nilpotent primary ideal of $R[X,\sigma]$. Then $R[X,\sigma]/Q$ is a local ring.

Proof. From (3.26) $R[X,\sigma]/r(Q) \simeq (R[X,\sigma]/Q)/(r(Q)/Q) \simeq (R[X,\sigma]/Q)/\mathrm{Rad}(R[x,\sigma]/Q)$ is a finite field. Hence $R[X,\sigma]$ is a local ring.

## 4 PRIME, PRIMARY, and IRREDUCIBLE POLYNOMIALS

A polynomial f in $R[X,\sigma]$ is said to be prime if $R[X,\sigma]f = fR[X,\sigma]$, and $fR[X,\sigma]$ is a completely prime ideal. A polynomial f in $R[X,\sigma]$ is primary if $R[X,\sigma]f = fR[X,\sigma]$, and $fR[X,\sigma]$ is a primary ideal.

3.28 PROPOSITION. If f is an irreducible polynomial in $(R/M)[X,\bar{\sigma}]$ such that $f(R/M)[X,\bar{\sigma}] = (R/M)[X,\bar{\sigma}]f$ then f is prime hence primary.

Proof. Let f be irreducible and $(R/M)[X,\bar{\sigma}]f = f(R/M)[X,\bar{\sigma}]$. If gh is in $f(R/M)[X,\bar{\sigma}]$ then $gh = fr$ for some polynomial r in $(R/M)[X,\bar{\sigma}]$. Since f is irreducible, f must appear in either the factorization of g or h. Suppose without loss that $g = g_1 \cdots g_j f g_{j+2} \cdots f_n$. Now $g_i f = f k_i$, where $1 \leq i \leq j$ and $k_i$ is in $(R/M)[X,\bar{\sigma}]$, so that $g = f k_1 \cdots k_j g_{j+2} \cdots g_n$. Now $k_1, \cdots, k_j$ must be irreducible since the number of irreducible factors in a factorization is unique by Jacobson [15, p. 34, Thm. 5]. Thus g is in $f(R/M)[X,\bar{\sigma}]$ and we conclude $f(R/M)[X,\bar{\sigma}]$ is completely prime hence primary, so that f is a prime and thus primary polynomial.

In $(R/M)[X,\bar{\sigma}]$ irreducible polynomials generate maximal right (or left) ideals.

3.29 PROPOSITION. A polynomial f in $(R/M)[X,\bar{\sigma}]$ is irreducible if and only if $f(R/M)[X,\bar{\sigma}]$ is a maximal right ideal.

Proof. Let $g(R/M)[X,\bar{\sigma}]$ be a right ideal such that $f(R/M)[X,\bar{\sigma}] \subset g(R/M)[X,\bar{\sigma}] \subset (R/M)[X,\bar{\sigma}]$ where f is irreducible. Then $f = gh$ for some h in $g(R/M)[X,\bar{\sigma}]$ and thus g or h is a unit. If g is a unit then clearly $g(R/M)[X,\bar{\sigma}] = (R/M)[X,\bar{\sigma}]$, while if h is a unit $g = fh^{-1}$ then $f(R/M)[X,\bar{\sigma}] = g(R/M)[X,\bar{\sigma}]$. Hence $f(R/M)[X,\bar{\sigma}]$ is maximal right.

Conversely, let $f(R/M)[X,\bar{\sigma}]$ be a maximal right ideal and suppose f is not irreducible. Then $f = gh$ where neither g or h is a unit. We may suppose g is not in $f(R/M)[X,\bar{\sigma}]$ for if it is, $g = fk$ and $f = fkh$ for some k in $(R/M)[X,\bar{\sigma}]$. Thus by (3.7) and (3.8) h is a unit. Now $f(R/M)[X,\bar{\sigma}] \subset g(R/M)[x,\bar{\sigma}] \subset (R/M)[X,\bar{\sigma}]$ since g is not a unit. Hence $f(R/M)[X,\bar{\sigma}]$ is not maximal.

Note: If $f(R/M)[X,\bar{\sigma}] = (R/M)[X,\bar{\sigma}]f$ where f is irreducible then $f(R/M)[X,\bar{\sigma}]$ is maximal right; i.e., $((R/M)[X,\bar{\sigma}])/(f(R/M)[X,\bar{\sigma}])$ is a finite field.

We use (3.29) to obtain the following representation of non-trivial non-nilpotent completely prime and maximal right ideals in $R[X,\sigma]$.

3.30 PROPOSITION. In $R[X,\sigma]$ a non-trivial non-nilpotent ideal P is completely prime if and only if $P = gR[X,\sigma] + M[X,\sigma] = R[X,\sigma]g + M[X,\sigma]$ where g is a non-trivial regular fundamental irreducible in $R[X,\sigma]$.

Proof. If P is completely prime it is primary and thus by (3.26) $P = (ug^n + m)R[X,\sigma] + M[X,\sigma] \cap P = R[X,\sigma](ug^n + m) + M[X,\sigma] \cap P$ where u is is a unit, g a non-trivial fundamental irreducible and m in $M[X,\sigma]$. Further $r(P) = gR[X,\sigma] + M[X,\sigma] = R[X,\sigma]g + M[X,\sigma]$. But if P is completely prime $P = r(P)$.

Conversely, suppose $P = gR[X,\sigma] + M[X,\sigma] = R[X,\sigma]g + M[X,\sigma]$, where

g is a regular fundamental irreducible in $R[X,\sigma]$. Then $\overline{P} = \bar{g}(R/M)[X,\bar{\sigma}] = (R/M)[X,\bar{\sigma}]\bar{g}$ where $\bar{g}$ is a non-trivial irreducible in $(R/M)[X,\bar{\sigma}]$. By (3.29) $\overline{P}$ is maximal right, and hence by (3.22) $\overline{P}$ is completely prime. Now since $M[X,\sigma] \subset P$ we conclude by (3.16) that P is completely prime.

We are interested in the prime elements in $R[X,\sigma]$. The following is immediate from (3.30).

3.31 COROLLARY. A polynomial f in $R[X,\sigma]$ is a non-trivial regular prime polynomial if and only if

(1) f is a non-trivial regular fundamental irreducible.

(2) $fR[X,\sigma] = R[X,\sigma]f$.

(3) $M[X,\sigma] \subset fR[X,\sigma]$.

3.32 PROPOSITION. (Characterization of Finite Fields)

Let R be a finite local ring. Then $R[X,\sigma]$ contains a prime regular polynomial if and only if R is a finite field.

Proof. Let M be the maximal ideal of R and suppose $M \neq 0$. If $f = r + uX$ is a prime, regular polynomial where u is a unit of R, then for any $g = \sum_{i=1}^{n} a_i X^i$ in $R[X,\sigma]$, $fg = \text{lower terms} + ua_n^{\sigma} X^{n+1}$. But u is not a zero divisor in R and $\sigma(a_n) \neq 0$ so $u\sigma(a_n) \neq 0$. Thus $M \not\subset fR[X,\sigma]$ which contradicts (3.31 part 3); i.e., $M[X,\sigma] \subset fR[X,\sigma]$. Therefore $M = 0$ and R is a finite field.

The converse is clear.

## 5 FACTORIZATION IN $R[X,\sigma]$

The factorization of polynomials in $R[X,\sigma]$ is achieved from factorization in $(R/M)[X,\sigma]$ given by the following well-known theorem for factorization in non-commutative principal ideal domains. See Jacobson [15, Thm. 5, p. 34].

3.33 THEOREM Let f be a polynomial which is a non-unit and non-trivial in the non-commutative principal ideal domain $(R/M)[X,\bar{\sigma}]$. Then f factors as follows:

(1) $f = g_1 \cdots g_n$ where the $g_i$'s are non-trivial irreducibles in $(R/M)[X,\bar{\sigma}]$.

(2) If $f = h_1 \cdots h_m$ is another factorization into non-trivial irreducibles then $n = m$, and there is a permutation $\pi$ of $\{1,2,\cdots,n\}$ such that $g_i$ is similar to $h_{\pi(i)}$.

Two polynomials g and h in $R[X,\sigma]$ are said to be right similar if $R[X,\sigma]/hR[X,\sigma] \simeq R[X,\sigma]/gR[X,\sigma]$ as right $R[X,\sigma]$-modules. The notion of left similar may be defined analogously. Since $(R/M)[X,\bar{\sigma}]$ is an integral domain we have from Jacobson [15] the following result.

3.34 PROPOSITION. Let g and h be non-trivial polynomials in $(R/M)[X,\bar{\sigma}]$. Then g and h are right similar if and only if they are left similar.

Further the preimages in $R[X,\sigma]$ of regular similar polynomials are similar.

3.35 PROPOSITION. Let $\bar{g}$ and $\bar{h}$ be non-trivial regular polynomials in $(R/M)[X,\bar{\sigma}]$ which are similar. Then g and h are similar in $R[X,\sigma]$.

Proof. Since $(R/M)[X,\bar{\sigma}]/\bar{g}(R/M)[X,\bar{\sigma}] \simeq (R/M)[X,\bar{\sigma}]/\bar{h}(R/M)[X,\bar{\sigma}]$ as $(R/M)[X,\bar{\sigma}]$-modules and

$$(R/M)[X,\bar{\sigma}]/\bar{g}(R/M)[X,\bar{\sigma}] \simeq R[X,\sigma]/gR[X,\sigma]$$

as $R[X,\sigma]$-modules, we have a natural isomorphism

$$R[X,\sigma]/gR[X,\sigma] \simeq R[X,\sigma]/hR[X,\sigma]$$

as $R[X,\sigma]$-modules where g and h are preimages in $R[X,\sigma]$ of $\bar{g}$ and $\bar{h}$ in $(R/M)[X,\bar{\sigma}]$.

3.36 PROPOSITION. Let g and h in $(R/M)[X,\bar{\sigma}]$ be similar and $g(R/M)[X,\bar{\sigma}]$ and $h(R/M)[X,\bar{\sigma}]$ be ideals. Then g and h are associates.

Proof. If $g(R/M)[X,\bar{\sigma}]$ and $h(R/M)[X,\bar{\sigma}]$ are ideals, then $(R/M)[X,\bar{\sigma}]/g(R/M)[X,\bar{\sigma}] \simeq (R/M)[X,\bar{\sigma}]/h(R/M)[x,\bar{\sigma}]$ as rings. Thus $h + g(R/M)[X,\bar{\sigma}]$ maps to 0 in the isomorphism and hence h is in $g(R/M)[X,\bar{\sigma}]$ so that h and g are left associates. In an analogous manner using (3.34) we have h and g are right associates, hence associates.

Unless we put more restrictions on $R[X,\sigma]$ we only have the following factorization theorem for polynomials in $R[X,\sigma]$.

3.37 THEOREM. Let f be a regular non-unit in $R[X,\sigma]$. Then

(1) $f = f_1 \cdots f_n$ where $f_i$ are non-trivial irreducibles.

(2) If $\bar{f} = \bar{g}_1 \cdots \bar{g}_m$ then $n \leq m$.

Proof. It is clear that f factors as a product of irreducibles $f = f_1 \cdots f_n$. Now $\bar{f} = \bar{f}_1 \cdots \bar{f}_n = \bar{g}_1 \cdots \bar{g}_m$ where $\bar{g}_i$ are irreducible and $\bar{f}_i$ may or may not be irreducible. Thus by (3.33) we conclude $n \leq m$.

Note: If $f = f_1 \cdots f_n$ where $f_i$ are fundamental irreducibles, then $n = m$.

## 6 FACTORIZATION IN $S[X,\sigma]$ for S a GALOIS RING

We have shown in (2.5) that a finite local ring R with characteristic $p^n$ is the homomorphic image of the skew polynomial ring $S[X_{ij},\sigma_{k(i)}]_{i=1,j=1}^{r,n(i)}$ where S is the Galois ring $GR(p^n,r)$. Thus we now consider the factorization of polynomials in $S[X,\sigma]$ which is lifted from $(S/Sp)[X,\bar{\sigma}] \simeq (R/M)[X,\bar{\sigma}]$.

3.38 THEOREM (Hensel's Lemma)

Let $S = GR(p^n,r)$ be a Galois ring with maximal ideal Sp. Let f be in $S[X,\sigma]$ and suppose

$$\mu(f) = \bar{g}\cdot\bar{h}$$

where $\bar{g}$ and $\bar{h}$ are polynomials in $(S/Sp)[X,\bar{\sigma}]$ such that

$$\bar{g}(S/Sp)[X,\bar{\sigma}] + (S/Sp)[X,\bar{\sigma}]\bar{h} = (S/Sp)[X,\bar{\sigma}].$$

Then there exists g and h in $S[X,\sigma]$ such that

(1) $\mu(g) = \bar{g}$; $\mu(h) = \bar{h}$,

(2) $f = gh$.

Proof. As shown earlier S is a commutative local principal ideal ring and thus the maximal ideal Sp is nilpotent of degree of nilpotency n where $S = GR(p^n,r)$.

The approach follows the classical proof in that we construct two sequences $\{g_k\}$ and $\{h_k\}$ in $S[X,\sigma]$ such that

(1) $\deg h_k = r$; $\deg g_k = m - r$

(2) $h_{k+1} = h_k \bmod (Sp)^{k+1}$; $g_{k+1} = g_k \bmod (Sp)^{k+1}$

(3) $f = g_k h_k \bmod (Sp)^{k+1}$.

Then since $(Sp)^n = 0$ we use $h = h_n$ and $g = g_n$ for the desired polynomials since $h_n g_n = h = f$.

We construct the sequences $\{g_k\}$, $\{h_k\}$ inductively. For $k = 0$, since $\mu: S[X,\sigma] \to (S/Sp)[X,\bar{\sigma}]$ is surjective we have $g_0$ and $h_0$ in $S[X,\sigma]$ with $\mu(g_0) = \bar{g}$ and $\mu(h_0) = \bar{h}$.

Suppose that $g_0,\cdots,g_j$ and $h_0,\cdots,h_j$ satisfy properties 1-3.

Let

$$g_{j+1} = g_j + p^{j+1}s$$

$$h_{j+1} = h_j + p^{j+1}t$$

where s and t are in $S[X,\sigma]$ with $\deg s < r$ and $\deg t \leq m - r$. Then (1) and (2) are clear. Further,

$$f = g_{j+1}h_{j+1} \bmod (Sp)^{j+2}$$

holds if and only if

$$(*) \qquad f - g_{j+1}h_{j+1} = f - (g_j + p^{j+1}s)(h_j + p^{j+1}t)$$

$$= f - g_jh_j - (g_jp^{j+1}t + p^{j+1}sh_j + p^{j+1}sp^{j+1}t)$$

$$= 0 \bmod (Sp)^{j+2}.$$

We note that the automorphism $\sigma$ takes p to p since $p = p \cdot 1$. Further S is commutative so that $p^{j+1}sp^{j+1}t$ is in $(Sp)^{j+2}$ and thus equals zero modulo $(Sp)^{j+2}$. Also by the induction step $f - g_jh_j = p^{j+1}q$ for some q in $S[X,\sigma]$ of degree less than m. Under these simplifications we have

$$f - g_{j+1}h_{j+1} = p^{j+1}(q - g_jt + sh_j).$$

Thus our choice of s and t must be such that

$$q = g_jt + sh_j \bmod (Sp)^{j+2}.$$

But

$$g_j = g_0 \bmod (Sp) \text{ and } h_j = h_0 \bmod (Sp),$$

so that

$$q = g_0t + sh_0 \bmod (Sp).$$

By our hypothesis

$$(S/Sp)[X,\bar{\sigma}] = \bar{g}(S/Sp)[X,\bar{\sigma}] + (S/Sp)[X,\bar{\sigma}]\bar{h}.$$

Thus there exists $\bar{s}$, $\bar{t}$ in $(S/Sp)[X,\bar{\sigma}]$ such that

$$\bar{q} = \bar{g}\bar{s} + \bar{t}\bar{h} = \bar{g}_0\bar{s} + \bar{t}\bar{h}_0,$$

where deg $\bar{s} \leq$ deg $\bar{h}_0$ and deg $\bar{t} \leq$ deg $\bar{g}_0$. Let s and t be preimages of $\bar{s}$ and $\bar{t}$. Then

$$q = g_js + th_j \bmod (Sp),$$

and thus

$$q = g_j s + t h_j \bmod (Sp)^{j+2}.$$

Hence we have shown there exist s and t such that

$$f = g_{j+1} h_{j+1} \bmod (Sp)^{j+2},$$

so by induction the sequences $\{g_k\}$ and $\{h_k\}$ exists for all k.

Thus for $h = h_n$ $g = g_n$ we have $f = g_n h_n = g \cdot h$.

3.39 COROLLARY. Let f be a polynomial in $S[X,\sigma]$. Suppose

$$\mu(f) = \bar{g}_1 \cdots \bar{g}_n$$

where $\bar{g}_1, \cdots, \bar{g}_n$ are polynomials in $(S/Sp)[X,\bar{\sigma}]$ such that

$$\bar{g}_i (S/Sp)[X,\bar{\sigma}] = (S/Sp)[X,\bar{\sigma}]\bar{g}_i$$

and the $\bar{g}_i$ are pairwise relatively prime. Then there exist $h_1, \cdots, h_n$ in $S[X,\sigma]$ such that

(1) $\mu(h_i) = \bar{g}_i$.

(2) $f = h_1 \cdots h_n$.

(3) $h_1, \cdots, h_n$ are pairwise relatively prime.

Proof. The proof is by induction on n, using Hensel's Lemma (3.38) and the fact that if $\bar{g}_i (S/Sp)[X,\bar{\sigma}] = (S/Sp)[X,\bar{\sigma}]\bar{g}_i$ where the $\bar{g}_i$'s are pairwise relatively prime then $\bar{g}_1$ and $\bar{g}_2 \cdots \bar{g}_n$ are relatively prime. The polynomials $h_1, \cdots, h_n$ are pairwise relatively prime by (3.10).

A ring R is said to be duo if every right ideal is also a left ideal and every left ideal is also a right ideal. We note that $S[X,\sigma]$ is duo if $\sigma$ is the identity automorphism of S. For duo skew polynomial rings over Galois rings $S = GR(p^n,r)$ we have the following classical primary factorization.

3.40 THEOREM. Let $S = GR(p^n,r)$ be a Galois ring, and $S[X,\sigma]$ a duo skew

polynomial ring. Then,

(1) Every regular polynomial f in $S[X,\sigma]$ can be factored as $f = uf_1 \cdots f_n$ where u is a unit and $f_1,\cdots,f_n$ are pairwise relatively prime, primary, non-units in $S[X,\sigma]$.

(2) If $f = uf_1 \cdots f_n = vg_1 \cdots, g_m$ where $u,v,f_i,g_i$ are as in (1), then n = m and there is a permutation $\pi$ of $\{1,\cdots,n\}$ where $f_i$ and $g_{\pi(i)}$ are associates.

Proof. (2) The proof of this is standard in the case of duo rings. See Feller [7, p. 87].

To prove (1) let f be a regular polynomial in $S[X,\sigma]$. Then $\bar{f}$ is a non-zero polynomial in $(S/Sp)[X,\bar{\sigma}]$ and hence by (3.33) can be factored as

$$\bar{f} = \bar{u}\bar{f}_1^{k_1} \cdots \bar{f}_n^{k_n}$$

where $\bar{u}$ is a unit and $\bar{f}_1,\cdots,\bar{f}_n$ are irreducible non-associated non-units in $(S/Sp)[X,\bar{\sigma}]$ which are relatively prime in pairs. Then $\bar{f}_1^{k_1},\cdots,\bar{f}_n^{k_n}$ are regular primary polynomials which are also pairwise relatively prime in $(S/Sp)[X,\bar{\sigma}]$. By (3.39) there are pairwise relatively prime polynomials $f_1,\cdots,f_n$ in $S[X,\sigma]$ such that

$$f = uf_1 \cdots f_n$$

and

$$\mu(f_i) = \bar{f}_i^{k_i}.$$

By (3.9) u is a unit in $S[X,\sigma]$ and by (3.23) $f_1,\cdots,f_n$ are primary, non-units in $S[X,\sigma]$.

## 7 S-AUTOMORPHISMS OF $S[X,\sigma]$ FOR S A GALOIS RING

Let $S = GR(p^n,r)$ be a Galois ring with maximal ideal Sp. We consider in this section the automorphisms of $S[X,\sigma]$ which leave S fixed.

Let f be an S-automorphism of $S[X,\sigma]$, then since f fixes S we have that f is completely determined by its action on the indeterminant X. If f takes X to the polynomial $t = s_0 + s_1X + \cdots + s_nX^n$ we denote f by $f_t$. Thus

$$f_t : S[X,\sigma] \to S[X,\sigma]$$

is defined by

$$f_t(g(X)) = g(t)$$

$$f_t(s) = s.$$

In showing that $f_t$ is an endomorphism of $S[X,\sigma]$ we find that t must be restricted to t = sX as the following illustrates. Suppose $t = sX^m$. Then

$$\begin{aligned} f_t((aX^i)(bX^j)) &= f_t(ab^{\sigma^i}X^{i+j}) = ab^{\sigma^i}(sX^m)^i(sX^m)^j \\ &= a(sX^m)^i b^{\sigma^{i-mi}}(sX^m)^j \\ &= a(t)^i b^{\sigma^{i-mi}}(t)^j \\ &= f_t(aX^i)f_t(bX^j) \end{aligned}$$

if and only if m = 1 and $\sigma^0$ is identity map. We also note that the above required that S be commutative or S to be in the center of the ring. Restricting t to t = sX it is then clear that $f_t$ is an S-endomorphism of $S[X,\sigma]$. We assume throughout that $\sigma$ is not the identity.

3.41 LEMMA Let t = sX be in $S[X,\sigma]$ and u be a unit of S. Then

(1) $f_t$ is onto if and only if $f_{ut}$ is onto.

(2) $f_t$ is 1-1 if and only if $f_{ut}$ is 1-1. (1-1 denotes injective)

Proof. We note that the units of S form a group under multiplication and $\sigma$ being an automorphism of S maps units to units. We have that $f_t[S[X,\sigma]] = S[t,\sigma]$. Thus part (1) follows by showing $S[t,\sigma] = S[ut,\sigma]$.

Suppose $g(t) = \sum_i s_i t^i$ is a polynomial in $S[t,\sigma]$. Then we have

$$\sum_i s_i t^i = \sum_i s_i (uu \cdots u^{\sigma^{i-1}})^{-1} (uu \cdots u^{\sigma^{i-1}}) t^i$$

$$= \sum_i s_i (uu^{\sigma} \cdots u^{\sigma^{i-1}})^{-1} (ut)^i$$

is a polynomial in $S[ut,\sigma]$. While conversely if $\sum_i s_i (ut)^i$ is in $S[ut,\sigma]$ then

$$\sum_i s_i (ut)^i = \sum_i s_i uu^{\sigma} \cdots u^{\sigma^{i-1}} t^i$$

is in $S[t,\sigma]$.

To show part (2), suppose $f_t$ is not 1-1. Then for some non-zero $g(X) = \sum_i s_i X^i$, we have

$$f_t(g(X)) = \sum_i s_i t^i = 0.$$

Hence

$$\sum_i s_i (uu^{\sigma} \cdots u^{\sigma^{i-1}})^{-1} (ut)^i = \sum_i s_i t^i = 0.$$

That is $f_{ut}(h(X)) = 0$, but

$$h(X) = \sum_i s_i (uu^{\sigma} \cdots u^{\sigma^{i-1}})^{-1} X^i \neq 0.$$

Since $(uu^{\sigma} \cdots u^{\sigma^{i-1}})^{-1}$ is not a zero divisor and $s_i$ are not all zero. Thus $f_{ut}$ is not 1-1.

The converse follows similarly.

3.42 PROPOSITION. Let $t = sX$ be in $S[X,\sigma]$. Then,

(1) $f_t$ is onto if and only if $s$ is a unit of $S$.

(2) $f_t$ is 1-1 if and only if $s$ is a unit of $S$.

(3) $f_t$ is an $S$-automorphism if and only if $s$ is a unit of $S$.

Proof. We use the fact that $f_t$ induces a natural $S/Sp$-endomorphism of

$(S/Sp)[X,\sigma]$; i.e. $\bar{f}_t(\overline{g(X)}) = \overline{f_t(g(X))} = \overline{g(t)}$.

Suppose $f_t$ is onto and $t = sX$. Then for $g(X) = \sum_{i=1}^{n} s_i X^i$ in $S[X,\sigma]$ where $s_i$ is a unit, there is some polynomial $h(X) = \sum_{i=1}^{n} r_i X^i$ such that $f_t(h(X)) = g(X)$. Thus $\overline{f_t(h(X))} = \overline{g(X)} \neq 0$; that is,

$$\sum_{i=1}^{n} \overline{r_i (sX)^i} = \sum_{i=1}^{n} \overline{r_i s s^{\sigma} \cdots s^{\sigma^{i-1}}} X^i = \sum_{i=1}^{n} \bar{s}_i X^i \neq 0.$$

So that for some $j$, $1 < j < n$,

$$\overline{r_j s s^{\sigma} \cdots s^{\sigma^{j-1}}} \neq 0$$

and thus $\bar{s} \neq 0$; i.e., $s$ is a unit in $S/Sp$ and hence a unit in $S$ by (3.9).

The converse follows immediately from Lemma (3.41) using the fact that for $t = X$ in $S[X,\sigma]$, $f_t$ is onto. Then if $s$ is a unit $f_{sX}$ is onto.

For part (2) suppose $t = sX$ where $s$ is not a unit of $S$. Then $S$ is a zero divisor so that for some non-zero $c$ in $S$, $c \cdot s = 0$. Now take $g(X) = cX \neq 0$. Then

$$f_t(g(X)) = csX = 0$$

so that $f_t$ is not 1-1.

The converse follows as in part (1).

Part (3) is immediate since $f_t$ fixes $S$.

We next characterize the automorphisms of $S[X,\sigma]$ which are extensions of automorphisms of $S$ to an automorphism of $S[X,\sigma]$. Suppose $\phi$ is an automorphism of $S$. Let

$$\phi_t : S[X,\sigma] \to S[X,\sigma]$$

be defined for $g(X) = s_0 + s_1 X + \cdots + s_n X^n$ by

$$\phi_t(g(X)) = \phi(s_0) + \phi(s_1)t^1 + \cdots + \phi(s_n)t^n$$

where $t = sX$.

Since by (2.1 vi) the automorphisms of S form a commutative group, $\phi \cdot \sigma^i = \sigma^i \cdot \phi$. Using this we have that $\phi_t$ is an endomorphism of $S[X,\sigma]$. Clearly $\phi_t$ is additive, and the following extends linearly to show that $\phi_t$ is multiplicative.

$$\begin{aligned}\phi_t((aX^i)(bX^j)) &= \phi(ab^{\sigma^i}t^{i+j}) = \phi(a)\phi(b^{\sigma^i})t^{i+j} \\ &= \phi(a)(\phi(b))^{\sigma^i}t^it^j = \phi(a)t^i\phi(b)t^j \\ &= \phi_t(aX^i)\phi_t(bX^j).\end{aligned}$$

It is clear that $\phi_t$ extends $\phi$ to $S[X,\sigma]$. The following theorem gives necessary and sufficient conditions for $\phi_t$ and $f_t$ to be automorphisms of $S[X,\sigma]$.

3.43 THEOREM. Let $f_t$ and $\phi_t: S[X,\sigma] \to S[X,\sigma]$ be as described. Then,

(1) $\phi_t$ is 1-1 if and only if $f_t$ is 1-1 if and only if $t = sX$ for s a unit of S.

(2) $\phi_t$ is onto if and only if $f_t$ is onto if and only if $t = sX$ for s a unit of S.

Proof. Part (1) follows from (3.42) by showing $\phi_t$ is 1-1 if and only if $f_t$ is 1-1. Suppose $g(X) = \sum_i s_iX^i$ is such that

$$f_t(g(X)) = \sum_i s_it^i = 0,$$

and $\phi_t$ is 1-1. Now

$$\sum_i s_it^i = \phi_t(\sum_i \phi^{-1}(s_i)X^i) = 0,$$

so that $\sum_i \phi^{-1}(s_i)X^i = 0$ since $\phi_t$ is 1-1. Hence $\phi^{-1}(s_i) = 0$ and $s_i = 0$ since $\phi^{-1}$ is 1-1. Thus $g(X) = 0$ and $f_t$ is 1-1.

Conversely, if $g(X) = \sum_i s_i X^i$ is such that

$$\phi_t(g(X)) = \sum_i \phi(s_i)t^i = f_t(\sum_i \phi(s_i)X^i) = 0$$

and $f_t$ is 1-1, then

$$\sum_i \phi(s_i)X^i = 0$$

or $\phi(s_i) = 0$ and thus $s_i = 0$ since $\phi$ is 1-1. Hence $\phi_t$ is 1-1.

Part (2) follows immediately since $\phi$ is an automorphism of S and thus the range of $\phi_t$ is $S[t,\sigma]$ which is precisely the range of $f_t$.

# CHAPTER IV

## APPLICATIONS OF SKEW POLYNOMIAL THEORY

In this chapter we use the polynomial theory of Chapter 3 in the development of simple and unramified extensions of a finite local ring. Further we characterize finite chain rings and finite one-step rings.

### 1 EXTENSIONS

Let R be a finite local ring. A ring T is said to be an extension of R if $R \subseteq T$. We will be interested in rings T which are finite local extensions of R, but on occasion we take T to be $R[X,\sigma]$. In either case the only non-zero idempotent is 1, thus R and T share the same identity.

Since $R \subseteq T$ we may consider T to be an R-module. If T is finitely generated over R we take the degree of T over R, denoted by [T:R], to be the rank of T over R; i.e. the cardinality of a minimal generating set of T over R. Observe this is well-defined.

Further note that T/(T Rad(R)) is a natural R/Rad(R)-vector space since Rad(R) annihilates T/(T Rad(R)). We use this to "lift" the R/Rad(R)-basis of T/(T Rad(R)) to R-minimal generating sets of S.

We begin a somewhat more general setting with the following lemmas.

**4.1 LEMMA.** (Nakayama's Lemma)

Let R be a ring, J an ideal of R contained in Rad(R), M an R-module, N an arbitrary submodule of M, and F a finitely generated submodule of M.

Then $M = N + JF$ implies $M = N$.

4.2 LEMMA. Let R be a ring, J an ideal of R contained in Rad(R), M an R-module, N and $N'$ arbitrary submodules of M, and F a submodule of M such that M/F is a finitely generated R-module.

Then $M = N + F + JN'$ implies $M = N + F$.

Proof. Let $x_1 + F, \cdots, x_n + F$ generate M/F, Then $M = Rx_1 + \cdots + Rx_n + F$. Since F is a submodule of M we have

$$\begin{aligned} M &= N + F + JN' = N + F + JM \\ &= N + F + J(Rx_1 + \cdots + Rx_n + F) \\ &= N + F + J(Rx_1 + \cdots + Rx_n) \end{aligned}$$

and thus, by (4.1), $M = N + F$.

Let R be a finite local ring with maximal ideal M and T a ring extension of R. Let Q be an ideal of T such that T/Q is a finitely generated R-module. We say that a subset B of T is a R-generating set modulo Q of T if $T = Q + RB$.

Let "—" denote the image under the natural homomorphisms

$$\mu: T \to T/MT \quad \text{and} \quad \mu: R \to R/M.$$

Since M annihilates $T/MT = \bar{T}$, the R-module structure of $\bar{T}$ induces a natural $R/M = \bar{R}$ structure on $\bar{T}$; i.e.,

$$(r + M)(t + MT) = r(t + MT) = rt + MT.$$

4.3 THEOREM. (Lifting of generating sets)

Consider the above setting, Then

(1) If B is a subset of T,

$$T = Q + RB \text{ if and only if } \bar{T} = \bar{Q} + \bar{R}\bar{B}.$$

(2) $\operatorname{rank}(T/Q) = \operatorname{rank}(\bar{T}/\bar{Q})$.

(3) If T is a finite extension and Q = 0,

$$[T:R] = [\bar{T}:\bar{R}]$$

where $\bar{T}$ is a $\bar{R}$-vector space.

Proof. If B is a subset of T and T = Q + RB then clearly $\bar{T} = \bar{Q} + \bar{R}\bar{B}$ as R-modules and thus from above remark, $\bar{T} = \bar{Q} + \bar{R}\bar{B}$ as $\bar{R}$-modules. Conversely, if $\bar{T} = \bar{Q} + \bar{R}\bar{B}$ as $\bar{R}$-modules then $\bar{T} = \bar{Q} + \bar{R}\bar{B}$ as R-modules and thus $T = Q + RB + MT$. Since T/Q is finitely generated by hypothesis we conclude from (4.2) that T = Q + RB.

From (1) we have $T/Q \simeq RB$ if and only if $T/Q \simeq RB$ so that the rank (T/Q) equals the rank $(\bar{T}/\bar{Q})$. Thus if Q = 0 we conclude $[T:R] = [\bar{T}:\bar{R}]$.

If R and T are rings with $R \subseteq T$, then the contraction $I_*$ of an ideal I in T is $I_* = I \cap R$; while the extension $I^*$ of an ideal I in R is $I^* = TIT$, that is, the smallest two-sided ideal of T containing I. We have shown that for T local or $T = R[X,\sigma]$ that Rad(T) is a two-sided ideal. We are interested in extensions T of R such that Rad(T) = T(Rad(R)) = $(\text{Rad}(R))^*$. Such a ring T is called an unramified extension of R.

4.4 PROPOSITION. Let T be a local extension of R. Then R = T if and only if [T:R] = 1.

Proof. Clearly R = T implies [T:R] = 1. Conversely, if [T:R] = 1 and {b} is a generating set of T, then since 1 is in T, rb = 1 for some r in R. Thus b is a unit of T and thus $b^2 \neq 0$. Now there exists an $r^1$ in R with $r^1 b = b^2$, so that $(r^1 - b)b = 0$ and hence $r^1 = b$ is in R. That is, T = R.

4.5 COROLLARY. Let T be an unramified local extension of R. If $\bar{T} = \bar{R}$ then T = R.

Proof. If $\bar{T} = \bar{R}$ then since $\bar{T}$ is an $\bar{R}$-vector space ($\bar{T} = T/MT = T/\text{Rad}(T)$

is a finite field) we have $1 = [\bar{T}:\bar{R}] = [T:R]$ by (4.3). Thus by (4.4) $T = R$.

In general if $R = T_0 \subsetneq T_1 \subsetneq \cdots \subseteq T_n$ where $T_i$ is a finite extension of $T_{i-1}$ of degree $[T_i:T_{i-1}] = r_i$ then

$$[T_n:R] \leq r_1 \cdots r_n.$$

We now show in the case of unramified extensions equality holds.

4.6 PROPOSITION. Let $R = T_0 \subseteq \cdots \subseteq T_n$ where $T_i$ is an unramified finite local extension of $T_{i-1}$ of degree $[T_i:T_{i-1}] = r_i$. Then

$$[T_n:R] = r_1 \cdots r_n.$$

Proof. Since $\mathrm{Rad}(T_i) = T_i\mathrm{Rad}(T_{i-1})$ is a two-sided ideal, we have $\mathrm{Rad}(T_n) = T_1 \cdots T_n \mathrm{Rad}(R) = T_n \mathrm{Rad}(R)$ so that $T_n$ is unramified over R. Thus by (4.5) $[T_n:R] = [\bar{T}_n:\bar{R}]$ and $[\bar{T}_i:\bar{T}_{i-1}] = [T_i:T_{i-1}] = r_i$. But $\bar{R}, \cdots, \bar{T}_{n-1}$ are finite subspaces of $\bar{T}_n$, so that

$$[T_n:R] = [\bar{T}_n:\bar{R}] = [\bar{T}_n:\bar{T}_{n-1}] \cdots [\bar{T}_1:\bar{R}] = r_1 \cdots r_n.$$

## 2 DEGREE OF IDEALS IN $R[X,\sigma]$.

We have from (3.4) that $\mathrm{Rad}(R[X,\sigma]) = (\mathrm{Rad}(R))[X,\sigma]$ so that $R[X,\sigma]$ is an unramified extension of R. We say that an ideal Q of $R[X,\sigma]$ has finite degree if the rank of the R-module $R[X,\sigma]/Q$ is finite, in which case, we define

$$\deg(Q) = \mathrm{rank}(R[X,\sigma]/Q) = [R[X,\sigma]/Q:R/Q_*].$$

By (4.3) if Q has finite degree then

$$\deg(Q) = \deg(\bar{Q}).$$

4.7 THEOREM. Let Q be an ideal of $R[X,\sigma]$. Then the following are equivalent.

(1) $Q$ has finite degree

(2) $Q$ contains a monic polynomial.

(3) $Q$ is regular.

(4) $\bar{Q}$ has finite degree in $(R/M)[X,\bar{\sigma}]$.

Proof. We first show (1) and (2) are equivalent. Suppose $Q$ has finite degree, then $R[X,\sigma]/Q$ has a R-generating set say $\{f_1,\cdots,f_t\}$. Let m be the maximal degree of the polynomials $f_1,\cdots,f_t$. Then for $n > m$ there exists $r_1,\cdots,r_t$ in R and g in $Q$ such that $X^n = r_1f_1 + \cdots + r_tf_t + g$. Now $X^n - r_1f_1 - \cdots - r_tf_t = g$ is a monic polynomial in $Q$.

Conversely, let f be a monic polynomial of degree n in $Q$. Then since the division algorithm holds in $R[X,\sigma]$ for monic polynomials as divisors (proof same as for $R[X]$ with appropriate consideration for skewing), for g in $R[X,\sigma]$ there exists h and k in $R[X,\sigma]$ such that $g = hf + k$ where $k = 0$ or the degree of f is less than n. Thus $\{1,X,\cdots,X^{n-1}\}$ is an R-generating set of $R[X,\sigma]/Q$, and $Q$ has finite degree less than or equal to n.

It is immediate that (2) implies (3). Further we have noted (1) implies (4). We show (4) implies (1).

Suppose $\bar{Q}$ has finite degree in $(R/M)[X,\bar{\sigma}]$. Then since $(R/M)[X,\bar{\sigma}]$ is a skew polynomial ring over a finite local ring R/M, by (2) $\bar{Q}$ contains a monic polynomial $\bar{f} = X^n + \bar{r}_{n-1}X^{n-1} + \cdots + \bar{r}_0$ where $\bar{r}_i$ is in R/M. Thus $Q$ contains $f = X^n + r_{n-1}X^{n-1} + \cdots + r_0 + m(X)$ where $m(X)$ is a polynomial in $M[X,\sigma]$. Since $M[X,\sigma]$ is nilpotent, $M[X,\sigma] \leq r(Q)$ and hence f is in $r(Q)$. Thus $f - m(X) = X^n + r_{n-1}X^{n-1} + \cdots + r_0$ is in $r(Q)$ so that $(X^n + r_{n-1}X^{n-1} + \cdots + r_0)^k$ is in $Q$ for some integer k. Hence $Q$ has degree less than or equal to nk.

If Q is regular, then $\bar{Q} \neq 0$ and thus since R/M is a finite field $(R/M)[X,\bar{\sigma}]/\bar{Q}$ is finitely generated as a (R/M)-module; i.e., $\bar{Q}$ has finite degree. Hence (3) implies (4).

We denote the <u>degree of a polynomial f by D(f)</u>. Since $R[X,\sigma]$ contains zero divisors for polynomials f and g in $R[X,\sigma]$,

$$D(f \cdot g) \leq D(f) + D(g)$$

while in the integral domain $(R/M)[X,\bar{\sigma}]$

$$D(\bar{f} \cdot \bar{g}) = D(\bar{f}) + D(\bar{g}).$$

Thus we define the <u>order</u> of a regular polynomial f in $R[X,\sigma]$ to be the minimal degree of the non-zero polynomials of the right ideal $fR[X,\sigma]$. Note that in $(R/M)[X,\bar{\sigma}]$ if $\bar{Q} = \bar{f}(R/M)[X,\bar{\sigma}] = (R/M)[X,\bar{\sigma}]\bar{f}$ then from above we have

$$\deg(\bar{Q}) = D(\bar{f}) = \text{order}(\bar{f}).$$

<u>4.8 LEMMA</u>. Let f be a regular polynomial in $R[X,\sigma]$. Then the order(f) equals the maximum exponent of X in the polynomial f whose coefficient is a unit of R.

<u>Proof</u>. Let $f = r_s X^s + \cdots + r_m X^m + \cdots + r_0$ where $r_s, \cdots, r_{m+1}$ are in M and $r_m$ is a unit of R. Then clearly order(f) < m since $r_s, \cdots, r_{m+1}$ are zero divisors in $R[X,\sigma]$. For example, if we choose $r^1$ such that $r_s \sigma^s(r^1) = 0$ then $(r_s X^s + \cdots + r_0)r^1$ is a polynomial in $fR[X,\sigma]$ of degree less than or equal to s - 1.

Let $\beta$ denote the degree of nilpotency of M = Rad(R). We show by induction on $\beta$ that order(f) = m. The result is obvious if $M^1 = 0$. Assume inductively that the theorem is true for all local rings with $M^r = 0$ for $r \leq \beta$. We show the result holds for all local rings R with

$M^{\beta} \neq 0$ and $M^{\beta+1} = 0$. Suppose for $g = a_t X^t + \cdots + a_0$ where $a_t \neq 0$ that $D(fg) < m$, then $D(\bar{f}\cdot\bar{g}) < m$. But $D(\bar{f}\cdot\bar{g}) = D(\bar{f}) + D(\bar{g}) = m + D(\bar{g})$ implies that $\bar{g} = 0$ or $g$ is in $M[X,\sigma]$. Now since $R$ is local with maximal ideal $M^{\beta} \neq 0$ and $M^{\beta+1} = 0$, we have $R/M^{\beta}$ is a local ring with maximal ideal $M/M^{\beta}$. But $(M/M^{\beta})^{\beta} = 0$, thus if $g$ is not in $(M^{\beta})[X,\sigma]$ by the induction hypothesis $D(f\cdot g) \geq m$ in $R[X,\sigma]$. If on the other hand, $g$ is in $(M^{\beta})[X,\sigma]$ and $D(f\cdot g) < m$ then $a_m \sigma^m(b_s) = 0$ which is contradictory since $a_m$ is a unit of $R$ and thus not a zero divisor. In either case the assumption that $D(f\cdot g) < m$ leads to a contradiction so that order$(f) = m$.

4.9 PROPOSITION. Let $R$ be a finite local ring with maximal ideal $M$. Let $f$ be a polynomial in $R[X,\sigma]$ which generates a two-sided ideal $fR[X,\sigma] = R[X,\sigma]f = (f)$. Then $(f)$ is generated by a monic polynomial of degree $m$ if and only if $f = r_t X^t + \cdots + r_m X^m + \cdots + r_0$ where $r_t, \cdots, r_{m+1}$ are in $M$ and $r_m$ is a unit of $R$.

Proof. Suppose $fR[X,\sigma] = R[X,\sigma]f$ and $f$ is as above. Let $B = \{1, X, \cdots, X^{m-1}\}$ in $R[X,\sigma]$. Then since $\bar{f} = \bar{r}_m X^m + \bar{r}_{m-1} X^{m-1} + \cdots + \bar{r}_0$ where $\bar{r}_m \neq 0$ we have by the division algorithm that

$$(R/M)[X,\bar{\sigma}] = (\bar{f}) + \bar{R}\bar{B} \text{ and hence by (4.3) } R[X,\sigma] = (f) + RB.$$

Thus for $X^m$ in $R[X,\sigma]$,

$$X^m = a_{m-1}X^{m-1} + \cdots + a_0 + f_0$$

where $a_{m-1}, \cdots, a_0$ are in $R$ and $f_0$ in $(f)$, so that

$$X^m - a_{m-1}X^{m-1} - \cdots - a_0 = f_0 \text{ is monic and in } (f).$$

It remains to show $(f_0) = (f)$. This follows since $f_0 \neq 0$ and $f_0$ has leading coefficient a unit so by the division algorithm there exists $h$ and $k$ in $R[X,\sigma]$ such that

$$f = hf_0 + k \text{ where } k = 0 \text{ or } D(k) < m.$$

Since order(f) = m by (4.8) $D(k) \geq m$ and hence $k = 0$; i.e., $(f) = R[X,\sigma]f_0$. Similarly $f_0R[X,\sigma] = (f)$ so that $(f) = (f_0)$.

Conversely suppose $(f) = (f_0)$ where $f_0$ is monic of degree m. Then order(f) = order($f_0$), but order($f_0$) = m by (4.8). Thus order(f) = m and f is of the form

$$f = r_t X^t + \cdots + r_m X^m + \cdots + r_0$$

where $r_t, \cdots, r_m$ are in M and $r_m$ is a unit of R.

We conclude this section with the following summary.

4.10 THEOREM. Let Q be a regular ideal in $R[X,\sigma]$ with form as in (3.26); i.e.,

$$Q = (ug^k + m)R[X,\sigma] + M[X,\sigma] \cap Q$$

where u is a unit, g a fundamental irreducible and m in $M[X,\sigma]$ in $R[X,\sigma]$. Further, let $\bar{Q} = \bar{f}(R/M)[X,\bar{\sigma}] = (R/M)[X,\bar{\sigma}]\bar{f}$. Then,

$$\deg(Q) = \deg(\bar{Q}) = \text{order}(\bar{f}) = D(\bar{f}) = kD(\bar{g}).$$

## 3 SIMPLE ALGEBRAIC EXTENSIONS.

Let R and T be finite rings with $R \subseteq T$. If $\theta$ is an element in T such that $r\theta = \theta\sigma(r)$ for some automorphism $\sigma$ of R and all r's in R, then we denote by $R[\theta,\sigma]$ the smallest subring of T containing R and $\theta$. We denote by $R(\theta,\sigma)$ the smallest local subring of T containing R and $\theta$, and call $R(\theta,\sigma)$ a simple extension of R and $\theta$.

Suppose that R is local. The ring $R[\theta,\sigma]$ is the homomorphic image of $R[X,\sigma]$ under the natural substitution map taking f(X) to $f(\theta)$. Let Q be the kernel of the substitution map. Then

$$R[X,\sigma]/Q \simeq R[\theta,\sigma].$$

Since $R[\theta,\sigma]$ is a homomorphic image of the primary ring $R[X,\sigma]$, $R[\theta,\sigma]$ is also primary; that is, (0) is a primary ideal in $R[\theta,\sigma]$. We use this in showing that Q is primary. Suppose $f(X)g(X)$ is in Q, then $f(\theta)g(\theta) = 0$. Thus $f(X)$ is in Q or $(g(X))^n$ is in Q.

Further since $Q = \{f \text{ in } R[X,\sigma] \mid f(\theta) = 0\}$ it is clear that $R \cap Q = 0$ and thus $R[X,\sigma]/Q$ is a finite ring.

We now show that Q is a regular non-trivial ideal so that by (3.27)

$$R[X,\sigma]/Q \simeq R[\theta,\sigma]$$

is a local ring. Hence $R[\theta,\sigma] = R(\theta,\sigma)$.

4.11 PROPOSITION. Let $R \subseteq T$ be finite rings. If $\theta$ in T is such that for some automorphism $\sigma$ of R, $r\theta = \theta\sigma(r)$ for all r in R, then there exists a monic polynomial f in $R[X,\sigma]$ such that $f(\theta) = 0$.

Proof. Let $\theta$ be in T and such that $r\theta = \theta\sigma(r)$ for r in R. Consider $R_0 = \{\Sigma\, r_i\theta^i \mid r_i \text{ is in } R\}$. Then $R \subseteq R_0 \subseteq T$. For each element in $R_0$ select a representative with least degree as a polynomial in $\theta$. Let B denote the set of these representatives. Then B is finite and thus contains a polynomial of greatest degree, say m. Since $\theta^{m+1}$ is in $R_0$, $\theta^{m+1} = p(\theta)$ for some $p(\theta)$ in B. That is, $\theta$ satisfies the monic polynomial $X^{m+1} - p(X)$ in $R[X,\sigma]$.

The kernel $Q = \{f \text{ in } R[X,\sigma] \mid f(\theta) = 0\}$ of the substitution map is called the defining ideal of $\theta$. The element $\theta$ is called skew algebraic and $R(\theta,\sigma)$ is called a simple skew algebraic extension or simply a simple algebraic extension if $\theta$ is algebraic.

4.12 THEOREM. If $T = R(\theta,\sigma)$ is a simple algebraic extension of R, then

the defining ideal Q of $\theta$ is a regular primary ideal and has the form

$$Q = (ug^k + m)R[X,\sigma] + M[X,\sigma] \cap Q,$$

where u is a unit, g a fundamental irreducible and m in $M[X,\sigma]$ in $R[X,\sigma]$.

Further, $T = R(\theta,\sigma) = R[\theta,\sigma]$ and T is a finite local extension of R with

$$[T:R] = kD(\bar{g}).$$

The finite field $\bar{T} = T/\mathrm{Rad}(T) = (R/M)[X,\bar{\sigma}]/(\bar{g}) = (R/M)(\bar{\theta},\bar{\sigma})$ is obtained from (R/M) by the adjunction of $\bar{\theta}$ the zero of $\bar{g}$ to (R/M).

Hence $[T:R] = k[\bar{T}:\bar{R}]$.

Proof. In the preceding discussion we have already noted that Q is a non-trivial regular primary ideal. Thus by (3.26) Q has the given form. By definition and (4.10) the $\deg(Q) = [R[X,\sigma]/Q:R] = [T:R] = kD(\bar{g})$. Now from (3.26), (3.19) and following comments we have the isomorphisms

$$\begin{aligned}\bar{T} = T/\mathrm{Rad}(T) &\simeq (R[X,\sigma]/Q)/\mathrm{Rad}(R[X,\sigma]/Q)\\ &\simeq (R/M)[X,\bar{\sigma}]/\overrightarrow{r(Q)}\\ &\simeq (R/M)[X,\bar{\sigma}]/(\bar{g}).\end{aligned}$$

Thus $\bar{T}$ is a finite field extension of $\bar{R}$, and hence by McDonald [21, Thm. II.1] $\bar{T}$ is the adjunction of $\bar{R}$ and $\bar{\theta}$ the zero of the irreducible polynomial $\bar{g}$ in $(R/M)[X,\bar{\sigma}]$. Hence $[\bar{T}:\bar{R}] = D(\bar{g})$, so that $[T:R] = k[\bar{T}:\bar{R}]$.

## 4 FINITE CHAIN RINGS AND ONE-STEP NON-COMMUTATIVE RINGS

In this section we apply the main structure theorem (2.5) to the results of Clark and Drake [2] to characterize finite non-commutative chain rings.

A ring R is a left (right) chain ring if its lattice of left (right) ideals forms a chain.

The following lemma from [2] summarizes the properties of finite chain rings.

4.13 LEMMA If R is a finite ring with $\mathrm{Rad}(R) = M \neq 0$, then the following are equivalent.

(1) R is a left chain ring.

(2) R is a right chain ring.

(3) R is a local ring with $M = R\theta$ for any $\theta$ in $M - M^2$.

(4) The principal left ideals of R form a chain.

Thus the ideals of R are

$$R \supset R\theta \supset R\theta^2 \supset \cdots \supset R\theta^{\beta} = 0$$

where $\beta$ is the index of nilpotency of $\mathrm{Rad}(R) = M$. Further, for $1 \leq i \leq \beta$ $R\theta^i = \theta^i R$.

Since a finite chain ring R is local by (2.2) R contains the coefficient subring $S = GR(p^n,r)$ where the characteristic of R is $p^n$ and $R/\mathrm{Rad}(R) = GF(p^r)$. Now $R = S \oplus N$ as (S-S)-modules where N is a (S-S)-submodule of R contained in $\mathrm{Rad}(R) = M$. Since N is an (S-S)-module by (2.4) it has a distinguished independent generating set $\{b_1,\cdots,b_m; \sigma_1,\cdots,\sigma_m\}$ where $sb_i = b_i\sigma_i(s)$ for s in S. Thus $R = S \oplus Sb_1 \oplus \cdots \oplus Sb_m$. We now show that some $b_i$ is in $M - M^2$. For suppose $b_1,\cdots,b_m$ are in $M^2$. Then since p is also in $M^2$ (otherwise $Rp = M$ and R would be an unramified extension of $Z/Zp^n$ which contradicts (2.1)) we conclude that

$$Sp \oplus Sb_1 \oplus \cdots \oplus Sb_m \subset M^2.$$

But S is an unramified extension of $Z/Zp^n$ so that $M \cap S = Sp$. Thus since $M \subseteq R$ it is clear that

$$Sp \oplus Sb_1 \oplus \cdots \oplus Sb_m = M.$$

But this contradicts the above inclusion so that for some i, $1 \leq i \leq m$, $b_i$ is in $M - M^2$. Denote $b_i$ by $\theta$, then $s\theta = \theta\sigma_i(s)$ and $\theta$ generates M.

Using this we have an improved version of Clark and Drake's principal result in [2].

4.14 THEOREM Let R be a finite chain ring with characteristic $p^n$, maximal ideal $M = R\theta$ ($\theta$ as above), and $S = GR(p^n,r)$ the coefficient subring of R.

Let m denote the degree of nilpotency of M. Then there exist integers k and t such that

(1) $R = S \oplus S\theta \oplus \cdots \oplus S\theta^{k-1}$ as an (S-S)-module direct sum, where $s\theta^i = \theta^i\sigma^i(s)$ for some fixed automorphism of S and each s in S.

(2) $\theta^k = p(s_{k-1}\theta^{k-1} + \cdots + s_1\theta + s_0)$ where $s_i$ is in S and $s_0$ is a unit of S.

(3) There are (S-S)-module isomorphisms

$$S\theta^i \simeq S \quad \text{for } i = 1,\cdots,t-1$$

$$S\theta^i \simeq Sp \quad \text{for } i = t,\cdots,k-1.$$

(4) $m = (n-1)k + t$, $1 \leq t \leq k$, where k is the greatest integer $i \leq m$ such that p is in $M^i$.

Let R be a finite chain ring as described above in (4.14) with coefficient subring $S = GR(p^n,r)$, and integer k being the greatest integer $i \leq m$ such that p is in $M^i = R\theta^i$.

A skew polynomial $g(X) = X^k + p(s_{k-1}X^{k-1} + \cdots + s_1X + s_0)$ in $S[X,\sigma]$ where $s_0$ is a unit in S is called a skew Eisenstein polynomial over S.

The ring $S[X,\sigma]/(g(X))$ is called an Eisenstein extension of S of degree k.

By using a skew Eisenstein extension we are able to extend Krull's characterization of commutative finite chain rings to that of non-commutative finite chain rings.

4.15 THEOREM (Characterization of chain rings)

Let R be a finite chain ring with maximal ideal M of degree of nilpotency m, $R/M = GF(p^r)$, and coefficient ring $S = GR(p^n,r)$.

Then there exists integers t and k such that

$$R \simeq S[X,\sigma]/(g(X),p^{n-1}X^t)$$

where $t = m - (n-1)k > 0$ and g(X) is an Eisenstein polynomial of degree k over S.

Conversely, such a quotient is a finite chain ring.

Proof. It is clear from the proof of (4.14) that the above quotient ring has the properties given in (4.14). Thus we map the generator of $S[X,\sigma]/(g(X),p^{n-1}X^t)$ to the generator of R and achieve the desired isomorphism.

A one-step non-commutative ring is a non-commutative ring for which every proper subring is commutative.

In [24; p. 753, Thm. 447 Ring $R_{II}$] Redei has characterized finite one-step non-commutative rings. From this theorem and our theory of skew polynomial rings we have the following characterization of finite non-nilpotent one-step rings with identity.

Let p and q be primes and m, e, n positive integers with $n < q$. Let f be a fundamental irreducible in $(Z/Zp^m)[X]$ of degree $q^e$. Consider the Galois ring $S = (Z/Zp^m)[X]/(f)$. Select a separable generator $\rho$ of S over $Z/Zp^m$ such that $Auto_{Z/Zp^m}(S)$ are given by power maps of this generator

(See Ganske and McDonald [9, Thm. 5.11]). Define an automorphism

$$\tau : S \to S \text{ by } \tau : \rho \to \rho^{t}$$

where $t = \rho^{nq^{e-1}}$. For this automorphism consider $S[X,\tau]$.

4.16 THEOREM (In the above setting) The ring

$$S[X,\tau]/(X^2)$$

is a one-step non-commutative ring with identity. Further, every non-nilpotent one-step non-commutative ring with identity has the above form.

Proof. It is clear that $S[X,\tau]/(X^2)$ is generated by $\rho$ and $X$ where $\rho$ and $X$ have the properties of the ring $R_{II}$ in [24, p. 753, Thm. 447]. Hence $S[X,\tau]/(X^2)$ is a one-step non-commutative ring. Further, for any non-nilpotent one-step ring with identity we may construct $S[X,\tau]/(X^2)$ as above. Then mapping generators to generators we have the desired isomorphism.

BIBLIOGRAPHY


1. Castillion, J. B., "Sur Une classe d'anneaux presque commutative," C. R. Acad. Sc. Paris, Vol. 260 (1965), pp. 379-382.

2. Clark, W. E. and Drake, D. A., "Finite Chain Rings," Submitted.

3. Clark, W. E. and Drake, D. A., "A Coefficient Ring for Noncommutative Finite Local Rings," Submitted.

4. Cohn, P. M., "Noncommutative Unique Factorization Domains," Trans. A.M.S., Vol. 109 (1963), pp. 313-331.

5. Courter, R. C., "Finite Direct Sums of Complete Matrix Rings Over Perfect Completely Primary Rings," Canad. J. Math., Vol. 21 (1969), pp. 430-446.

6. Curtis, C. W. and Reiner, I., Representation Theory of Finite Groups and Associative Algebras, Interscience (1966).

7. Feller, E. H., "Properties of Primary Non-commutative Rings," Trans. A.M.S., 89 (1958), pp. 130-138.

8. Feller, E. H. and Swokowski, E. W., "On Ring Extensions for Completely Primary Non-commutative Rings," Trans. A.M.S., 105 (1962), pp. 251-263.

9. Ganske, G. and McDonald, B. R., "Structure and Galois Theory for Finite Local Rings," Accepted: Rocky Mountain J.

10. Gilmer, Robert W. Jr., "R-Automorphism of R[X]," Proc. London Math. Soc., (3) 18 (1968), pp. 328-36.

11. Herstein, I. N., Noncommutative Rings, M.A.A. Carus Monograph., No. 15.

12. Hochshild, G., "On Structure of Algebras with Non-zero Radical," Bulletin American Mathematical Society, Number 53 (1947), pp. 369-377.

13. Hungerford, T. W., "On Structure of Principal Ideal Rings," Pac. J. Math., 25 (1968), pp. 543-547.

14. Jacobson, N., Structure of Rings, A.M.S. Colloq. Publ. XXXVII (1964).

15. Jacobson, N., The Theory of Rings, A.M.S. Math. Surveys II (1943),

16. Janusz, G. J., "Separable Algebras over Commutative Rings," Transactions of the American Mathematical Society, 122 Number 2 (1966), pp. 461-479.

17. Jategaonkar, A. V., "Skew Polynomial Rings over Semisimple Rings," J. of Algebra, 19 (1971), pp. 315-328.

18. Jategaonkar, A. V., "Skew Polynomial Rings over Orders in Artinian Rings," Submitted.

19. Jategaonkar, A. V., "A Counter-Example in Ring Theory and Homological Algebra," J. of Algebra, 12 (1969), 418-440.

20. McCoy, N. H., The Theory of Rings, Mac Millan (1964).

21. McDonald, B. R., Lecture Notes on Finite Rings, Univ. of Oklahoma.

22. Ore, O., "Theory of Non-commutative Polynomials," Ann. Math, 34 (1933), 480-508.

23. Raghavendran, R., "Finite Associative Rings," Composito Math., 21 (1969), pp. 195-229.

24. Redei, L., Algebra Vol. I, Pergamon Press, (1967),

25. Snapper, E., "Completely Primary Rings I, "Annals of Math. 52 (1950), pp. 666-693.

26. Snapper, E., "Completely Primary Rings II, "Annals of Math. 53 (1951), pp. 125-142.

27. Wilson, R. S., "On the Structure of Finite Rings, I," Submitted.

28. Wilson, R. S., "On the Structure of Finite Rings, II," Submitted.