The Structure Of Chain Rings

By

HANAN ABDUL AZIZ AL – OLAYAN

A Dissertation submitted to the Graduate School in partial

fulfillment of the requirements for the degree

Doctor of Philosophy

Department of Mathematics

College of Science

King Saud University

1422A. H.–2001A. D

ACKNOWLEDGEMENT

♡♡♡♡♡♡♡

All great and abundant thanks to the Glorious Almighty **Allah**, the Omniscient, and the sole nourisher and sustainer of the universe, who taught me and guided my steps in this humble effort.

My heartfelt thanks and deep gratitude to my thesis supervisor *Prof. Y. Alkhamees* and co-supervisor *Prof. S. Singh*. They both exerted their utmost in encouraging and in offering me their valuable advice without which such accomplishment would never have been possible.

My endless thanks to my beloved *mother* who inculcated in me the respect of scholars and the love of knowledge. As well as, I wish to extend my sincere thanks to my *husband* and my *brother* who saved no effort in helping and encouraging me.

I take this opportunity to acknowledge my indebtedness to King Saud University for providing necessary support and facilities. Also I wish to thank all my teachers and colleagues in the Department of Mathematics for their cooperation and kind help.

Table of Contents

=30pt

INTRODUCTION

Let R be a finite local ring . It was proved by Clark and Drake [8] that R has a Galois subring R_0 such that $R = R_0 + J(R)$, $J(R_0) = R_0 \cap J(R) = pR_0$, where p is a prime number such that *char* $R = p^n$ for some positive integer n; such a subring of R is called a *coefficient subring*, Clark [7] proved that any two such subrings of R are conjugates in R and hence they are isomorphic. On the other hand Wirt [26] gave the concept of a distinguished basis of a bimodule over a Galois ring. He proved the existence of such a distinguished basis. Let R be a finite chain ring. So R as a bimodule over its coefficient subring R_0 has a distinguished basis. This distinguished basis is used by Wirt to prove that R is a quotient of some skew polynomial ring over R_0. The centralizer of R_0 in R is investigated by Alkhamees [2] and he showed that the centralizer of R_0 is a commutative chain ring, independent of the choice of a coefficient subring of R and determines R up to isomorphism.

This thesis is an attempt to generalize these results to rings that need not be finite. In chapter 2, the concept of a generalized Galois ring is introduced. A ring R is called a generalized Galois ring, if there exists a family $\{R_\alpha\}_{\alpha\in\Lambda}$ of Galois subrings such that for any $\alpha,\ \beta \in \Lambda$, there exists $\gamma \in \Lambda$ such that $R_\alpha \cup R_\beta \subseteq R_\gamma$ and R is the union of the members of this family. Let R be a generalized Galois ring. Indeed R is a union of an ascending chain of Galois subrings of R. Then for some prime number p and a positive integer n, *char* $R = p^n$, $J(R) = pR$ and $\overline{R} = R/J(R)$ is an algebraic field extension of $\mathbb{Z}_p$. This ring R is a commutative artinian local principal ideal ring ($i.e.$, a special primary ring). Among several results the followings are a noteworthy generalizations of the results on Galois rings. (i) The groups of automorphisms of R and of $\overline{R}$ are isomorphic. (ii) Two generalized Galois rings R and R' are isomorphic if and only if $\overline{R}$ and $\overline{R'}$ are isomorphic and they have same characteristic. Given a local ring R and commutative local subring T of R such that $J(T) = T \cap J(R)$, the concepts of lift algebraic elements of R over T is given by Alkhamees and Singh [1]. By using Hensel Lemma, some basic properties of lift algebraic elements are discussed. These properties of lift algebraic elements play a fundamental role in chapter 2 and the subsequent chapters.

The concept of coefficient subring of a local ring R is discussed in sections 1 and 2 of chapter 3. Given an artinian local duo ring R with $\overline{R}$ an absolutely algebraic field, it is shown in section 1 that R has a coefficient subring R_0, which is a field or a generalized Galois subring according as *char* $\overline{R}$ is zero or a prime number. Suppose now that R is an artinian local duo ring such that $\overline{R}$ is a field but need not be absolutely algebraic. Does R admit a coefficient subring? This question is examined in section 2. A complete answer to this question is not yet known. Let F the maximal absolutely algebraic subfield of $\overline{R}$. In case $\overline{R}$ is a simple transcendental extension of F, the answer is given in affirmative.

Let R_0 be a generalized Galois ring. Following Wirt, the concept of a distinguished basis of an $(R_0, R_0) - bimodule\ \mathfrak{M}$ is introduced in section 1 of chapter 4. In case $d({}_{R_0}\mathfrak{M})$ is finite, the existence of a distinguished basis of $\mathfrak{M}$ is established. Some invariants of this distinguished basis in terms of the automorphism group of R_0 are given. Let R be an artinian local duo ring such that $\overline{R}$ is an absolutely algebraic field of non-zero characteristic. As given in chapter 3, R admits a coefficient subring R_0. By using the results on distinguished basis, it is shown that $R = R_0 \oplus \mathfrak{N}$ as an (R_0, R_0) $-bimodule$ with $\mathfrak{N} \subseteq J(R)$.

Let R be a chain ring with $\overline{R}$ an absolutely algebraic field of non-zero characteristic and R_0 be its coefficient subring. Given an $(R_0, R_0) - bimodule\ \mathfrak{M}$, a pair (s, σ), where s is a non-zero element of $\mathfrak{M}$ and $\sigma \in Aut\ R_0$ is called a *distinguished element* of $\mathfrak{M}$ if $sa = \sigma(a)s$ for every $a \in R_0$. As in Wirt, it is proved that R has a distinguished element (θ, σ) such that $J(R) = \theta R = R\theta$. For some prime number p and some positive integer n, *char* $R = p^n$. To avoid the trivial case, we take $n > 1$.

Let k be the positive integer such that the ideal $\langle \theta^k \rangle = pR$. Then as proved by Clark, Drake and Wirt for finite chain rings, we prove in chapter 5 that

$$R = R_0 \oplus R_0\theta \oplus R_0\theta^2 \oplus \ldots \oplus R_0\theta^{k-1}.$$

Using this, the centre of R, the centralizer of R_0 in R are determined, generalizing some results known for finite chain rings. If m is the index of nilpotency of $J(R)$, it is finally proved that R is isomorphic to $R_0[x,\sigma]/\langle g(x), x^m \rangle$ for a suitably defined Eisenstein polynomial $g(x)$.

The Structure Of Chain Rings

By

HANAN ABDUL AZIZ AL – OLAYAN

This Thesis was examined on 15/10/1422 - 30/12/2001
and it has been approved

Member of Committee: Prof. S. K. Jain

Prof. Yousef A. Alkhamees

Dr. Ahmad H. Sharary

CHAPTER 1

Preliminaries

In this chapter we give some notations used in this thesis and recall some known definitions and results required for the following chapters. Most results are stated without proofs. For the proof of some results we mention some references while the proof of other results in rings theory can be found in many references like [5], [16] and [19] and the proof of the results in fields theory can be found in [16].

1.1 General results on rings

All rings considered in this thesis are with identity $1(\neq 0)$ and any subring of a ring contains the identity of the ring. An ideal I of a ring R is called a *nil ideal* if all its elements are nilpotents; if for some positive integer m, $I^m = \{0\}$, then I is called a *nilpotent ideal* of R. The ring of polynomials over a commutative ring R is denoted by $R[x]$ and $I[x]$ denote the set of all polynomials in $R[x]$ of the form $\sum_{i=0}^{t} a_i x^i$, $a_i \in I$. A polynomial $f(x) \in R[x]$ is called *monic* if the coefficient of highest power of x in $f(x)$ is equal to 1, the identity of R. Let R be a ring and T be a subring of R. The *centralizer* of T

in R is the set $\{r \in R : rt = tr \text{ for all } t \in T\}$ and is denoted by $Z_R(T)$. The *centre* of R is the set $\{r \in R : r'r = rr' \text{ for all } r' \in R\}$ and is denoted by $C(R)$. Also $Aut\ R$ will denote the group of automorphisms of R and $Aut_T\ R$ will denote the subgroup of $Aut\ R$ which fixes T elementwise. A ring R is called *left* [*right*] *artinian* if any descending chain of left [right] ideals of R has a minimal element and R is said to be *artinian* if R is both left and right artinian. While R is called *left* [*right*] *notherian* if any ascending chain of left [right] ideals of R has a maximal element and R is said to be *notherian* if R is both left and right notherian. The *Jacobson radical* $J(R)$ of a ring R is the intersection of all maximal left [right] ideals of R. Indeed, $J(R)$ contains all [left, right] nil ideals of R and if $r \in J(R)$, then $1 - r$ is a unit in R. By $(J(R))^0$ we mean the ring R, by $\overline{R}$ we mean $R/J(R)$, for any element $r \in R$, $\bar{r}$ will means $r + J(R)$ and characteristic of R will be denoted by *char* R. Recall that for a ring R, if $\overline{R}$ is a division ring, then *char* $R = q$, where $q = 0$ or p^n for some prime number p and hence R has a copy of $\mathbb{Z}$ or $\mathbb{Z}_{p^n}$ respectively, where $\mathbb{Z}$ is the ring of integers and $\mathbb{Z}_{p^n}$ is the ring of integers modulo p^n. An element x of a ring R is *quasi − regular* if $1 + x$ is a unit or equivalently there exists $x' \in R$ such that $x + x' + x'x = 0$ and $x + x' + xx' = 0$. A one sided ideal I is *quasi − regular* provided that it consist of quasi-regular elements. By an R *− module* we mean a left R *− module* and by an (R,R) *− bimodule* we mean a left and right R *− module* $\mathfrak{M}$ such that $(as)b = a(sb)$ for all $a, b \in R$ and $s \in \mathfrak{M}$. If R^{op} denote the opposite ring of R, an (R,R) *− bimodule* is an $R \otimes_{\mathbb{Z}} R^{op}$ *− module*. For a ring R, all R *− modules* are unitary; *i.e.*, if $\mathfrak{M}$ is an R *− module*, $1s = s$ for all $s \in \mathfrak{M}$. A chain of submodules of an R *− module* $\mathfrak{M}$

$$\mathfrak{M} = \mathfrak{M}_0 \supset \mathfrak{M}_1 \supset \cdots \supset \mathfrak{M}_h = \{0\}$$

is called a *composition series* of R *− submodules* of $\mathfrak{M}$ if the factor $\mathfrak{M}_i/\mathfrak{M}_{i+1}$ has no proper submodule.

Definition 1. Let R be a ring, $m \geq 1$. Then m is called *the index of nilpotency* of $J(R)$ if $(J(R))^m = \{0\}$ and $(J(R))^{m-1} \neq \{0\}$.

Theorem 2. *Let R be a left or right artinian ring. Then $J(R)$ is nilpotent.* ♣

Proposition 3. *Let R be a ring and I a quasi−regular ideal of R. Then $a \in R$ is a unit if and only if $a + I$ is a unit in R/I.* ♣

Proof : It is clear that if a is a unit in R then $a + I$ is a unit in R/I. Conversely, let $a + I$ be a unit in R/I. Then there exists an element $b + I \in R/I$ such that $(a + I)(b + I) = (b + I)(a + I) = 1 + I$. So $ab - 1, ba - 1 \in I$. As I is a quasi−regular ideal of R, $ab = 1 + (ab - 1), ba = 1 + (ba - 1)$ are units in R. So there exist $c, d \in R$ such that

$$(ab)c = d(ba) = 1.$$

Let $bc = b'$ and $d' = db$. Then

$$d' = d'1 = d'(ab') = (d'a)b' = 1b' = b',$$

which implies that a is a unit. ♣

Lemma 4 [5]$\big[$Nakayama's lemma$\big]$**.** *If I is a left ideal of a ring R, then the following conditions are equivalent :*
(i) $I \subseteq J(R)$;
(ii) $1 - i$ is a unit for every $i \in I$;
(iii) If A is finitely generated R − module such that $IA = A$, then $A = \{0\}$;
(iv) If B is a submodule of a finitely generated R − module A such that $A = IA + B$, then $A = B$. ♣

Definition 5. A ring R is called a *duo ring* if every right or left ideal of R is a two-sided ideal of R.

Definition 6. Let R be a ring and $\mathfrak{M}$ an R *− module* which has a composition series of

$R-$ submodules

$$\mathfrak{M} = \mathfrak{M}_0 \supset \mathfrak{M}_1 \supset \cdots \supset \mathfrak{M}_n = \{0\}.$$

Then the length n is called *the length of* $\mathfrak{M}$ as an $R-$ *module* and is denoted by $d({}_R\mathfrak{M})$ or simply by $d(\mathfrak{M})$.

Theorem 7. *Let R be a ring and $\mathfrak{M}$ an $R-$ module. If*

$$\mathfrak{M} = \mathfrak{M}_0 \oplus \mathfrak{M}_1 \oplus \cdots \oplus \mathfrak{M}_n,\ \mathfrak{M}_i \neq \{0\} \ \textit{for all } i,\ 0 \leq i \leq n$$

and

$$\mathfrak{M} = \mathfrak{N}_0 \oplus \mathfrak{N}_1 \oplus \cdots \oplus \mathfrak{N}_t,\ \mathfrak{N}_j \neq \{0\} \ \textit{for all } j,\ 0 \leq j \leq t,$$

such that $n \leq t$ and $\mathfrak{M}_i \subseteq \mathfrak{N}_i$ for each i, $0 \leq i \leq n$, then $\mathfrak{M}_i = \mathfrak{N}_i$ and $n = t$.

Proof : Since $\mathfrak{M}_i \subseteq \mathfrak{N}_i$ *for each* i,

$$\begin{aligned}\mathfrak{M} &= \mathfrak{M}_0 \oplus \mathfrak{M}_1 \oplus \cdots \oplus \mathfrak{M}_n \\ &\subseteq \mathfrak{N}_0 \oplus \mathfrak{N}_1 \oplus \cdots \oplus \mathfrak{N}_n \\ &\subseteq \mathfrak{M}.\end{aligned}$$

So

$$\mathfrak{M} = \mathfrak{N}_0 \oplus \mathfrak{N}_1 \oplus \cdots \oplus \mathfrak{N}_n,$$

and $n = t$. Let $s \in \mathfrak{N}_i$ for some $i,\ 0 \leq i \leq n$. Then

$$\begin{aligned}s &= s_0 + s_1 + \cdots + s_n, \text{ where } s_j \in \mathfrak{M}_j \text{ for each } j, 0 \leq j \leq n \\ s - s_i &= s_0 + \cdots + s_{i-1} + s_{i+1} + \cdots + s_n \\ &\in \bigoplus_{\substack{j=0 \\ j\neq i}}^{n} \mathfrak{M}_j \cap \mathfrak{N}_i \\ &\subseteq \bigoplus_{\substack{j=0 \\ j\neq i}}^{n} \mathfrak{N}_j \cap \mathfrak{N}_i = \{0\}.\end{aligned}$$

Therefore $s = s_i \in \mathfrak{M}_i$ and hence $\mathfrak{M}_i = \mathfrak{N}_i$ for all i. ♣

Remark 1. *Let R be a ring, $\mathfrak{M}$ an $R-$ module and I an ideal of R such that $I\mathfrak{M} = \{0\}$. Then it is easy to check that $\mathfrak{M}$ is an $R/I-$module such that for any $a + I \in R/I$ and $s \in \mathfrak{M}$,*

$$(a + I)s = as. \quad \clubsuit$$

Definition 8. A module $\mathfrak{M}$ over a ring R is said to be *injective* if given any diagram of $R-$ *module* homomorphisms

$$\begin{array}{ccccc} \{0\} & \to & A & \xrightarrow{g} & B \\ & {\scriptstyle f}\downarrow & & & \\ & \mathfrak{M} & & & \end{array}$$

with g a monomorphism, there exists an $R-$ *module* homomorphism $h : B \to \mathfrak{M}$ such that the diagram

$$\begin{array}{ccccc} \{0\} & \to & A & \xrightarrow{g} & B \\ & & {\scriptstyle f}\downarrow & \swarrow & \\ & & \mathfrak{M} & {\scriptstyle h} & \end{array}$$

is commutative, that is $hg = f$.

Proposition 9. *Let R be a ring and $\mathfrak{M}$ an $R-$module. Then $\mathfrak{M}$ is injective if and only if $\mathfrak{M}$ is a direct summand of any module of which it is a submodule.* ♣

Lemma 10. *Let R be a ring with $d({}_RR)$ finite and T a subring of R such that*

$$R = T + J(R).$$

Then $d({}_TR) = d({}_RR)$. ♣

Proof : Let $\mathfrak{M}$ be a simple $R-$*module*. Then $\mathfrak{M} = Rs$ for all $s(\neq 0) \in \mathfrak{M}$. By Nakayama's lemma, $J(R)s \subset \mathfrak{M}$, so $J(R)s = \{0\}$,

$$\mathfrak{M} = Rs = [T + J(R)]s = Ts.$$

Hence $\mathfrak{M}$ is simple $T-$*module*. Let $d({}_RR) = n$,

$$R = A_0 \supset A_1 \supset \cdots \supset A_n = \{0\}$$

be a composition series of R as an $R-$*moodule*. Then A_i/A_{i+1} is a simple $R-$*module*. Hence A_i/A_{i+1} is a simple $T-$*module* for each i, $0 \leq i \leq n-1$. Thus

$$R = A_0 \supset A_1 \supset \cdots \supset A_n = \{0\}$$

is a composition series of R as a $T-$*moodule*. This proves that $d({}_TR) = n$. ♣

Theorem 11 [17]**.** *If R is a left [right] artinian principal ideal ring, then any finitely generated $R-$module $\left[\text{right } R-\text{module}\right]$ is a direct sum of cyclic $R-$modules $\left[\text{right } R-\text{modules}\right]$.* ♣

Definition 12. Let R be a commutative ring, σ an automorphism of R and S the set of all left polynomials $\sum_{i=0}^{t} a_i x^i$ over R. Then S can be made into a ring by usual addition, and the multiplication defined by the rule

$$xa = \sigma(a)x$$

for any $a \in R$. This ring is called *the skew polynomial ring* over R given by σ and it is denoted by $R[x,\sigma]$. If σ has finite order k', then $R[x,\sigma]$ is denoted by $R[x,\sigma,k']$.

Proposition 13. *Let $R[x,\sigma]$ be a skew polynomial ring over R and $g(x) \in R[x,\sigma]$ a monic polynomial. Then for any $f(x) \in R[x,\sigma]$ there exists unique $q(x)$, $r(x) \in R[x,\sigma]$ such that*

$$f(x) = q(x)g(x) + r(x),$$

deg $r(x) <$ deg $g(x)$ or $r(x) = 0$.

Proof : We first show the existence of $q(x)$, $r(x)$. If *deg* $g(x) >$ *deg* $f(x)$, then $q(x) = 0$, $r(x) = f(x)$. Let *deg* $g(x) = l$ and *deg* $f(x) = t \geq l$. We apply induction on t. Suppose that the result holds for all polynomials of degree $< t$. Let a_t be the leading coefficient of $f(x)$, and

$$h_1(x) = f(x) - a_t x^{t-l} g(x).$$

Then *deg* $h_1(x) <$ *deg* $f(x)$. By the induction hypothesis there exists $q_1(x)$, $r_1(x) \in R[x,\sigma]$ such that

$$h_1(x) = q_1(x)g(x) + r_1(x),$$

deg $r_1(x) < deg\ g(x)$ *or* $r_1(x) = 0$. Let $q(x) = a_t x^{t-l} + q_1(x)$ and $r(x) = r_1(x)$. Then

$$f(x) = q(x)g(x) + r(x).$$

To show the uniqueness, suppose that there are another $q_0(x)$, $r_0(x) \in R[x,\sigma]$ with *deg* $r_0(x) < deg$ $g(x)$ or $r_0(x) = 0$ such that

$$f(x) = q_0(x)g(x) + r_0(x).$$

So

$$(q_0(x) - q(x))g(x) = r(x) - r_0(x).$$

Suppose that $q_0(x) - q(x) \neq 0$. As $g(x)$ is monic,

$$\deg\ ((q_0(x) - q(x))g(x)) \geq \deg\ g(x) > deg\ (r(x) - r_0(x)).$$

This is a contradiction. Thus $q_0(x) = q(x)$ and hence $r_0(x) = r(x)$. ♣

Remark 2. *Let* $F[x,\sigma]$ *be a skew polynomial ring over a field* F. *Then it is easy to see that* $F[x,\sigma]$ *is a principal ideal domain.*

Proposition 14. *Let* $R[x,\sigma]$ *be a skew polynomial ring over* R *and* $f(x) \in R[x,\sigma]$ *a monic polynomial of degree* t. *Then*

$$R[x,\sigma]/\langle f(x)\rangle \cong \underbrace{R \oplus R \oplus \cdots \oplus R}_{t \text{ times}},$$

as an $R-$*module and hence*

$$d({}_R(R[x,\sigma]/\langle f(x)\rangle)) = d({}_R R) \cdot \deg f(x). \quad ♣$$

1.2 Local and chain rings

Definition 15 [19]**.** Let R be a ring. Then R is called a *local* [or *completely primary*] *ring* if the set of non-units of R is closed under addition.

By (R,M) we mean R is a local ring with maximal ideal M; if $M = \pi R = R\pi$ for some $\pi \in R$, then we will denote the local ring by (R,π).

We have the following characterization of local rings.

Proposition 16 [19]**.** *For a ring* R *the following statements are equivalent:*
(i) R *is a local ring;*
(ii) R *has a unique maximal left ideal;*
(iii) $J(R)$ *is a maximal left ideal;*
(iv) *The set of elements of* R *without left inverses is closed under addition;*
(v) $J(R) = \{x \in R : Rx \neq R\}$;
(vi) $R/J(R)$ *is a division ring;*
(vii) $J(R) = \{x \in R : x \text{ is not a unit}\}$;
$(viii)$ *If* $x \in R$, *then either* x *or* $1 - x$ *is a unit.* ♣

Example 1. Localization at $\mathcal{P}$. Let R be a commutative ring and C a multiplicatively closed subset of R which does not contain zero element. In the set $Q = \{(a,u) : a \in R, u \in C\}$, we introduce an equivalence relation such that (a,u) is equivalent to (b,v) if and only if $avw = buw$ for some $w \in C$. We denote the equivalence class of (a,u) by a/u. The set $R_C = \{a/u : a \in R, u \in C\}$

is called *the ring of quotients of R with respect to C*. If C is the set of all regular elements of R, then R_C is called *the total quotient ring* of R. Let $\mathcal{P}$ be a prime ideal of R and $C = R\backslash\mathcal{P}$. In this case we use different notation; R_C is called *the ring of quotients of R with respect to* $\mathcal{P}$, and is denoted by $R_{\mathcal{P}}$. The elements a/u with $a \in \mathcal{P}$ form an ideal M in $R_{\mathcal{P}}$. If $b/v \notin M$, then $b \notin \mathcal{P}$, hence $b \in C$ and therefor b/v is a unit in $R_{\mathcal{P}}$. It follows that if I is an ideal of $R_{\mathcal{P}}$ with $I \not\subseteq M$, then I contain a unit and therefore I is the whole ring. Hence M is the only maximal ideal in $R_{\mathcal{P}}$; in the other words, $R_{\mathcal{P}}$ is a local ring.

The process of passing from R to $R_{\mathcal{P}}$ is called *Localization at* $\mathcal{P}$ [21].

Proposition 17. Let R be an artinian ring which has no non-trivial idempotent. Then R is local ring. ♣

This is a direct result of (3.6.3) page 74 and (3.7.2) page 76 in [19].

Definition 18. Let R be a ring. Then the smallest subring P of R containing the identity $1 \neq 0$ such that for any integer n, if $n1$ is a unit in R, then $(n1)^{-1} \in P$, is called *the prime subring* of R. If the prime subring P is a field, then P is called *the prime subfield* of R.

Example 2. The ring $\mathbb{Z}[x]$ of all polynomials with coefficient in $\mathbb{Z}$, has $\mathbb{Z}$ as its prime subring.

Proposition 19. *Let R be a local ring with J(R) a nil ideal and P the prime subring of R.*
(*i*) *If char* $R = 0$, *then* $P \cong \mathbb{Q}$.
(*ii*) *If char* $R = p^n$, *then* $P \cong \mathbb{Z}_{p^n}$.

Proof : Now $P = \{(n1)(m1)^{-1} : n, m \in \mathbb{Z}, (m1)^{-1} \text{ exists in } R\}$.
(*i*) *Char* $R = 0$. Then *char* $(\overline{R}) = 0$. For $m(\neq 0) \in \mathbb{Z}$, $m1 \in P$, $m1 \notin J(R)$, gives $(m1)^{-1}$ exists. Also $\mathbb{Z}1 = \{n1 : n \in \mathbb{Z}\} \cong \mathbb{Z}$. So $P = \{(n1)(m1)^{-1} : n, m \in \mathbb{Z} \text{ with } m \neq 0\} \cong \mathbb{Q}$.
(*ii*) *Char* $R = p^n$. Then $\mathbb{Z}1 = \{m1 : m \in \mathbb{Z}\} \cong \mathbb{Z}_{p^n}$. Here $m1$ has inverse in R if and only if *gcd* $(m, p^n) = 1$; *i.e.*, *gcd* $(m, p) = 1$. But any $m + (p^n) \in \mathbb{Z}_{p^n}$ has inverse in $\mathbb{Z}_{p^n}$, whenever *gcd* $(m, p) = 1$. So

$$P = \{m1 : m \in \mathbb{Z}\} \cong \mathbb{Z}_{p^n}. \quad ♣$$

Proposition 20. *Let R be a local ring with J(R) a nil ideal and P the prime subring of R. Then* $\overline{P} = (P + J(R))/J(R)$ *is the prime subfield of* $\overline{R}$.

Proof : *Case I : char* $R = 0$. Then $P \cong \mathbb{Q}$, $P \cap J(R) = 0$. So $P \cong P/(P \cap J(R)) \cong (P + J(R))/J(R) = \overline{P}$ and hence $\overline{P} \cong \mathbb{Q}$. Thus $\overline{P}$ is the prime subfield of $\overline{R}$.
Case II : char $R = p^n$. Then $P \cong \mathbb{Z}_{p^n}$, $J(P) = pP = P \cap J(R)$. So

$$\mathbb{Z}/p\mathbb{Z} \cong P/pP \cong [P + J(R)]/J(R) = \overline{P}.$$

But the prime subfield of $\overline{R}$ is isomorphic to $\mathbb{Z}/p\mathbb{Z} = \mathbb{Z}_p$. Hence $\overline{P}$ is the prime subfield of $\overline{R}$. ♣

Throughout this thesis, for any local ring R, P will denote the prime subring of R and $\overline{P}$ will denote the prime subfield of $\overline{R}$. For any $f(x) = \sum_{i=0}^{t} a_i x^i \in R[x]$, $\bar{f}(x)$ will denote the polynomial $\sum_{i=0}^{t} \overline{a_i} x^i \in \overline{R}[x]$.

Definition 21. Let R be a commutative local ring and $f(x) \in R[x]$. Then $f(x)$ is called a *regular polynomial* if $f(x)$ is not a zero divisor in $R[x]$.

Theorem 22 [20]**.** *Let R be a commutative local ring with J(R) a nil ideal and* $f(x) = \sum_{i=0}^{t} a_i x^i \in R[x]$. *Then f(x) is nilpotent if and only if* $a_0, a_1, \cdots, a_t$ *are nilpotent.* ♣

Following Macdonald [20, (xx.9)], we define :

Definition 23. Let R be a ring. Then R is called a *left [right] chain ring* if its left [right] ideals

form a finite chain.

It is known that R is a chain ring if and only if R is an artinian local principal ideal ring.

Lemma 24 [20]**.** *Let R be a ring with J(R) a nilpotent ideal. Then R is a chain ring if and only if R is a local ring and* $J(R) = R\pi = \pi R$*, for some* $\pi \in J(R)$. ♣

If R is a chain ring, then R has a unique composition series of finite length, say

$$R \supset \langle \pi \rangle \supset \langle \pi^2 \rangle \supset \cdots \supset \langle \pi^m \rangle = \{0\},$$

for some $\pi \in J(R)$.

Definition 25 [13, p.200]**.** A local ring R is called a *special primary ring* if it is commutative artinian principal ideal ring. In other words, a commutative chain ring is called a *special primary ring*.

1.3 Field extensions and Galois rings

Let F, L be two fields such that $F \subseteq L$. Then L is said to be an *algebraic extension* of F if every element in L is algebraic over F. Otherwise L is said to be a *transcendental extension* of F. By a finite extension L of F we mean that L has a finite basis as a $F-$*vector space*. If for some $a \in L$, $L = F(a)$ the smallest subfield containing F and a, then L is called a *simple extension* of F. If $f(x)$ is a monic irreducible polynomial in $F[x]$ such that $f(a) = 0$, then $f(x)$ is called the *minimal polynomial* of a over F. If $\deg f(x) = r$ then we say that degree $a = r$. If a is algebraic over F, then $F(a)$ is an algebraic extension of F and $F(a) = F[a]$ the smallest subring containing F and a. Given field extensions $F \subseteq L \subseteq K$ such that L is an algebraic extension of F, then $a \in K$ is transcendental element over F if and only if a is transcendental element over L. We call L a *splitting field* of a polynomial $f(x)$ over a field F if it is the smallest field containing F and all the roots of $f(x)$. If F is a finite field, then F is of order p^n; such a field is denoted by $GF(p^n)$. The group of automorphisms $Aut\ F$ of $F = GF(p^n)$ is cyclic of order n. Let F be a field of the form $GF(p^n)$. Then every subfield of F is of the form $GF(p^t)$, where $t \mid n$. Moreover F has a unique subfield of the form $GF(p^t)$ if and only if $t \mid n$. It is obvious that if $a \in L$ is a root of a polynomial $g(x) \in F[x]$ and $\sigma \in Aut_F\ L$ then $\sigma(a)$ is also a root of $g(x)$. If L is a finite extension of the field $F = GF(p^n)$, $L = GF(p^{nt})$; if $g(x)$ is a monic irreducible polynomial over F of degree r and $g(a) = 0$ for some $a \in L$, then $r \leq t$ and $g(x)$ has exactly r roots in L. Finally, $Aut_F\ L$ is a cyclic group of order t.

Theorem 26. *Let F be a field and* $f(x) \in F[x]$ *an irreducible polynomial over F. Then* $F[x]/\langle f(x) \rangle$ *is a field.* ♣

Definition 27. An algebraic extension L of a field F is called *a normal extension* of F if every irreducible polynomial in $F[x]$ that has a root in L splits in L.

Proposition 28. *If F is a finite field and L is a finite extension of F, then L is a normal extension of F.* ♣

Definition 29. A polynomial $f(x) \in F[x]$, where F is a field, is said to be *separable* if every irreducible factor of $f(x)$ has no multiple roots in its splitting field.

Let L be an algebraic extension of a field F. Then an element a in L is *separable* if its minimal polynomial over F is separable. Moreover L is *separable extension* of F if every element in L is separable over F.

Proposition 30. *Let L be a separable extension of a field F,* $\alpha \in L$ *and* $f(x)$ *an irreducible polynomial over F such that* $f(\alpha) = 0$*. Then* α *is not a root of the derivative* $f'(x)$ *of* $f(x)$. ♣

Theorem 31. *Let F be a field such that* $char\ F = 0$ *or F is a finite field. Then any algebraic extension of F is a separable extension of F.* ♣

Theorem 32 [The primitive element Theorem]**.** *If L is a finite separable extension of F, then L is a simple extension.* ♣

Definition 33. Let L be an extension field of a field F such that the fixed subfield under the

group $Aut_F\ L$ is F itself. Then L is called a *Galois extension* of F.

Theorem 34. *Let L be a finite extension of a field F. Then L is a separable normal extension of F if and only if L is a Galois extension of F.* ♣

Corollary 35. *Let L be a finite extension of a finite field F. Then L is a Galois extension of F.* ♣

Definition 36. A field F is called an *absolutely algebraic field* if it is an algebraic extension of its prime subfield.

Let F by an absolutely algebraic field. Then by (5.3.5) [16], $|F| \leq |\mathbb{Z}^+||\overline{P}|$, where $\overline{P}$ is the prime subfield of F and $\mathbb{Z}^+$ is the set of positive integers. So $|F|$ is countable and

$$F = \overline{P}[a_1, a_2, \cdots].$$

Then for any integer n there exists b_n in F such that

$$\overline{P}[b_n] = \overline{P}[a_1, \cdots, a_n].$$

Thus $\overline{P}[b_n] \subseteq \overline{P}[b_{n+1}]$ and $F = \bigcup_{i-1}^{\infty} \overline{P}[b_i]$ a union of ascending chain of simple field extensions over its prime subfield.

GALOIS RINGS. It is well known that if R is a finite local ring, then $|R| = p^{mr}$, $|J(R)| = p^{(m-1)r}$, $\overline{R} \cong GF(p^r)$ and $char\ R = p^n$, where $1 \leq n \leq m$ for some prime p and positive integers m, n, r [24]. Of special interest is the case $m = n$; in this case R is commutative and isomorphic to $\mathbb{Z}_{p^n}[x]/\langle g(x)\rangle$, where $g(x) \in \mathbb{Z}_{p^n}[x]$ is a monic irreducible polynomial modulo p and of degree r. These rings were first considered by Krull (1924) [18] and since then rediscovered by others. Following the general trend, we call such a ring a Galois ring and denote it by $GR(p^n, r)$.

We need the following results :

Proposition 37 [24]**.** *Let R be a Galois ring of the form $GR(p^n, r)$. Then $R = \mathbb{Z}_{p^n}[b]$, where $b \in R$ is a root of monic polynomial $g(x)$ over $\mathbb{Z}_{p^n}$ which is irreducible modulo p and of degree r.* ♣

Proposition 38 [8]**.** *Let R be a finite local ring. Then R is a Galois ring if and only if $J(R) = pR$ for some prime number p.* ♣

Proposition 39 [24]**.** *Let R be a Galois ring. Then Aut $R \cong$ Aut $\overline{R}$.* ♣

Lemma 40 [24]**.** *Let R be a Galois ring of the form $GR(p^n, r)$. Then R has a unique Galois subring of the form $GR(p^n, s)$ if and only if $s \mid r$.* ♣

Remark 3 [4]**.** A subring of a Galois ring is not necessary Galois and it is Galois if and only if it is principal ideal ring.

Proposition 41 [7]. *Let R, R' be two Galois rings of the same characteristic. Then $R \cong R'$ if and only if $\overline{R} \cong \overline{R'}$.* ♣

Unless otherwise stated all symbols introduced in this chapter will retain their meanings throughout this thesis.

CHAPTER 2

Generalized Galois Rings

Given a local ring R and a commutative local subring T of R such that $J(T) = T \cap J(R)$. The concept of lift algebraic element of R over T is given by Alkhmees and Singh [1]. By using Hensel lemma, some basic properties of lift algebraic elements are discussed in the first section of this chapter. These properties of lift algebraic elements play a fundamental role in chapters 2 and 3. Also certain special primary rings are studied in the second section. Finally in the last section the generalized Galois ring is introduced. This ring is a union of ascending chain of Galois rings. We manage to generalize some properties of Galois rings. For instance we prove that if R is a generalized Galois ring, then R is commutative chain ring with $J(R) = pR$, $Aut\ R \cong Aut\ \overline{R}$ and if R, R' are generalized Galois rings of the same characteristic then $R \cong R'$ if and only if $\overline{R} \cong \overline{R'}$.

Conclusion

We end this thesis by giving a few open questions

(i) Does there exist chain rings that do not have coefficient subring ?

(ii) Let R be an artinian local ring with $\overline{R} = R/J(R)$ an absolutely algebraic field of non-zero characteristic. If R is a duo ring, it has a coefficient subring. Does R have a coefficient subring, if R is not duo ring ?

(iii) Give a suitable generalization of the theorems on existence of coefficient subrings of local rings, to rings that need not be local.

(iv) Study the possibility of the existence of coefficient subring of an artinian local duo ring R for which $\overline{R}$ need not be an absolutely algebraic field.

(v) Let R_0 be a special primary ring with $J(R_0) = pR_0$, where p is a prime number such that $char\ R_0 = p^n$ for some $n \geq 1$. Let $\mathfrak{M}$ be an $(R_0, R_0) - bimodule$.

(1) In case $d({}_{R_0}\mathfrak{M})$ is infinite, does $\mathfrak{M}$ have a distinguished basis ?

(2) In case $\overline{R_0}$ is not an absolutely algebraic field and $d({}_{R_0}\mathfrak{M}) < \infty$, does $\mathfrak{M}$ have a distinguished basis ?

(vi) Let R be a chain ring such that $\overline{R}$ is a simple transcendental extension of an absolutely algebraic field of non-zero characteristic knowing that R has a coefficient subring, try to generalize the structure theorem for chain rings, proved in Chapter 5 of this thesis.

(vii) Let R be a generalized Galois ring. Then $Aut\ R \cong Aut\ \overline{R}$, which is an abelian group. Does the converse true; $i.e.$, given any abelian group G, does there exists a generalized Galois ring R such that $Aut\ R \cong G$?

♣♣♣♣♣♣♣

List of symbols

symbol	**Meaning**	**Page Reference**
I^m	$\left\{ \sum a_1 a_2 \cdots a_m : a_1, \cdots, a_m \in I \right\}$	1
$R[x]$	the ring of polynomials over a ring R	1
$Z_R(T)$	the centralizer of T in a ring R	2
$C(R)$	the centre of R	2
$Aut\ R$	the group of automorphisms of R	2
$Aut_T\ R$	the subgroup of $Aut\ R$ that fixes T elementwise	2
$J(R)$	the Jacobson radical of R	2
$(J(R))^0$	R	2
$\overline{R}$	$R/J(R)$	2
$\bar{r}$	$r + J(R)$	2
$char\ R$	the characteristic of R	2
$\mathbb{Z}$	the ring of integers	2
$\mathbb{Z}_p$	the ring of integers modulo p	2
$R - module$	left $R - module$	2
$(R,R) - bimodule$	left and right $R - module$	2
$\subset$	is a proper subset of	3

symbol	**Meaning**	**Page Reference**
$d({}_R\mathfrak{M}), d(\mathfrak{M})$	the length of $\mathfrak{M}$ as an $R-module$	4
$\mathfrak{M}_1 \oplus \mathfrak{M}_2$	direct sum of *modules* $\mathfrak{M}_1$ and $\mathfrak{M}_2$	4
$\bigoplus_{i=0}^{n} \mathfrak{M}_i$	direct sum of a family of *modules* $\mathfrak{M}_i$	5
$R[x,\sigma]$	a skew polynomial ring over R	7
$R[x,\sigma,k']$	$R[x,\sigma]$ with k' the order of σ	7
deg $f(x)$	degree of $f(x)$	8
$\cong$	is isomorphic to	9
$\langle a \rangle$	the ideal generated by the element a	9
R_C	the ring of quotients of R with respect to a multiplicative set C	10
$R \backslash T$	$\{r \in R : r \notin T\}$	10
$R_{\mathcal{P}}$	the ring of quotients of R with respect to a prime ideal $\mathcal{P}$	10
$\mathbb{Q}$	the set of rational numbers	11
gcd(a,b)	the greatest common divisor of a and b	12
P	the prime subring of the given ring	12
$\overline{P}$	the prime subfield of the given field	12

symbol	**Meaning**	**Page Reference**
$\mathbb{Z}^+$	the set of positive integers	16
$GR(p^n, r)$	the Galois ring R with $char\ R = p^n$ and $\|R\| = p^{nr}$	16
$a \equiv b (\mathrm{mod}\, T)$	a is congruent to b modulo T	22
R_0	a generalized Galois ring	40
(R, θ, m, p^n, k)	a chain ring with $J(R) = \theta R = R\theta$, $\overline{R}$ an absolutely algebraic field, m the index of nilpotency of $J(R)$, $char\ R = p^n$ and k is the largest positive integer such that $p \in \theta^k R$	93
$(R_0, \theta, m, p^n, k, \sigma, k')$	the distinguished set of a given chain ring	100
R^σ	$\{r \in R : \sigma(r) = r\}$	106

REFERENCES

[1] **Y. Alkhamees and S. Singh**, Inertial subrings of a locally finite algebra, Colloq. Math., *Institute of Mathematics Polish Academy of Sciences*, *Warsaw*, (to appear).

[2] **Y. Alkhamees**, The enumeration of finite chain rings, *Panamerican Math. J.,* 5 (1995), 75 – 81.

[3]————————**-,** On the structure of finite completely primary rings, *J. Coll. Sci., King Saud Uni.* 13 (1982), 149 – 153.

[4]————————, The intersection of distinct Galois subrings is not necessarily Galois, *Compositio Math.,* 40 (1980)**,** 283 – 286.

[5] **F.W. Anderson and K.R. Fuller,** Rings and Categories of Modules**,** Graduate Texts in Mathematics 13, *Springer-Verlag,* 1974.

[6] **G. Azumaya,** On maximally central algebras, *Nagoya Math. J.*, 2 (1951), 119 – 150.

[7] **W.E. Clark,** A coefficient ring for finite non-commutative rings. *Proc. Amer. Math. Soc.*, 33 (1972), 25 – 28.

[8] ————————**and D. A. Drake,** Finite chain rings, *Abhandlungen Math. Sem. Uni. Hamburg, 29* (1973), 147 – 153.

[9] **I. S. Cohen,** On the structure and ideal theory of complete local rings, *Trans. Amer. Math. Soc.,* 59 (1946), 54 – 106.

[10] **B. Corbas**, Distinguished basis for finite local ring over it's coefficient subring, unpublished notes.

[11] **B. Corbas**, A coefficient subring of finite rings, unpublished notes.

[12] **G. Ganske and B. R. Mcdonald**, Finite local rings, *Rocky Mountain J. Math.*, 3 (1973), 521 – 540.

[13] **R. Gilmer**, Multiplicative Ideal Theory, Pure and Applied Mathematics Series 12, *Marcel Dekker*, 1972.

[14] **C. Faith,** Algebra II, Ring Theory, Grundlehren der mathematischen Wissenschaften 191, *Springer-Verlag***,** 1976.

[15] **J.L. Fisher**, Finite principal ideal rings, *Canad. Math. Bull.* 19(1976), 277 – 283.

[16] **T.W. Hungerford,** Algebra, *Holt, Rinehart and Winston Inc.,* 1974.

[17] **N. Jacobson,** The Theory of Rings, Amer. Math. Soc*., Math. Surveys II,* 1943.

[18] **W. Krull,** Algebraische theoie der ringe 11, *Math. Ann.*, 91 (1924), 1 – 46.

[19] **J. Lambek**, Lectures on Rings and Modules, *Chelsea Publishing Com.,* 1976.

[20] **B.R. Macdonald,** Finite Rings with Identity, Pure and Applied Mathematics Series, *Marcel Dekker,* 1974.

[21] **M. Nagata,** Local Rings**,** *Robert E. Krieger Publishing Company,* 1975**.**

[22] **A.A. Nechaev**, Finite rings of principal ideals, *Mat. Sb. 91*(1973), 350 – 366.

[23] **R.S. Pierce,** Associative Algebras, Graduate Texts in Mathematics 88, *Springer-Verlag,* (1982).

[24] **R. Raghavendran,** Finite associative rings, *Compositio Math.*, 21 (1969), 195 – 229.

[25] **R.S. Wilson,** On the structure of finite rings. *Compositio Math.*, 26 (1973), 79 – 93.

[26] **B.R. Wirt,** Finite non-commutative local rings, *Ph.D. thesis,* University of Oklahoma, 1972.

♣♣♣♣♣♣♣