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 it's 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 $r \in R$, $\overline{r}$ 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 and 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] [Nakayama's lemma]**.** *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 $R-module$ has a composition series of an $R-submodules$

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

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*

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

and

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

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* $s \in \mathfrak{M}$,

$$(a + I)\, s = as. \quad ♣$$

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

$$\{0\} \underset{f}{\longrightarrow} A \underset{\mathfrak{M}}{\downarrow} \xrightarrow{g} B$$

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

$$\{0\} \underset{f}{\longrightarrow} A \underset{\mathfrak{M}}{\downarrow} \xrightarrow{g} \underset{h}{\swarrow} B$$

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* $d({}_R R)$ *finite and* T *a subring of* R *such that*

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

Then $d({}_T R) = d({}_R R)$. ♣

Proof : Let $\mathfrak{M}$ be a simple $R-module$. Then $\mathfrak{M} = Rs$ for some $s\,(\neq 0) \in \mathfrak{M}$. 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 $R - module$ [right $R - module$] is a direct sum of cyclic $R - modules$ [right $R - modules$].* ♣

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,

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

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 principle 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) $J(R) = \{x \in R : x$ is not a unit$\}$;
(viii) If $x \in R$, then either x or $1 - x$ is a unit. ♣

Example 1. Localization at $\mathcal{P}$. If R is 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 (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 $b \notin M$, 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 $I \nsubseteq M$, 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 $f(x) = \sum_{i=0}^{t} a_i x^i \in R[x]$, $\overline{f}(x)$ 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 *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 a local principal ideal ring such that it is artinian.

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

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

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 an $F-$*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 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 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] , $|F| = |\mathbb{Z}^+|\,|\overline{P}|$, 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 $F = \underset{i-1}{\overset{\infty}{\cup}} \overline{P}[b_i]$ 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.*

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 except otherwise stated.

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 $\overline{R} \cong \overline{R'}$.

2.1 Unique lifting of a root and related results

The following theorem is a generalization of Theorem (3.2.6), in [24].

Theorem 1. *Let R be a ring and T a subring of R such that $T \subseteq C(R)$. Let I be a nil ideal of R, $f(x) \in T[x]$. If $\overline{f}(x) \in ((T+I)/I)[x]$ has a root $\overline{\alpha} \in \overline{R} = R/I$ such that $\overline{f'(\alpha)}$ is an invertible element in $\overline{R}$, where $f'(x)$ is the derivative of $f(x)$, then there exists a root $\beta \in \overline{\alpha}$ of f(x) in R.*

Proof : By (1.3), $\alpha \in R$ is invertible if and only if $\overline{\alpha} \in R/I$ is invertible. Let $u \in R$ be such that $\overline{f}(\overline{u}) = 0$ and $\overline{f'(u)}$ is invertible. Keeping u fixed, let $R_0 = T[u]$ and R_1 be the subring generated by R_0 and the inverses of those elements of R_0 that are units in R. As $T \subseteq C(R)$, R_1 is a commutative ring. Also $\overline{f(u)} = 0$ implies that $f(u) \in I \cap R_0 \subseteq I \cap R_1$. We wish to find an element $y \in I \cap R_1$ such that $f(u+y) = 0$. If we assume the existence of such an element y and write $\alpha = u + y$, then we get $f(\alpha) = 0$ and $\overline{\alpha} = \overline{u}$. So we proceed to consider the element $f(u+y)$, where y ranges over the ring R_1. As u belongs to the commutative ring R_1, we can expand $f(u+y)$ as follows:

$$f(u+y) = a + yf_1(u) + ... + y^r f_r(u), \qquad \cdots(1)$$

for all $y \in R_1$, where $f_i(u) \in R_0$, $i = 1, ..., r$, are independent of y, and $a = f(u) \in I \cap R_0$, and $f_1(u) = f'(u)$, where $f'(u)$ is the derivative of $f(x)$ at u. By the hypothesis, $\overline{f_1}(\overline{u})$ is an invertible element in $\overline{R_1}$, so $f_1(u)$ is invertible in R_1. On multiplying by $(f_1(u))^{-1}$, which is an element of R_1, the equation (1) becomes

$$(f_1(u))^{-1} f(u+y) = -b + y + a_2 y^2 + ... + a_r y^r, \qquad \cdots(2)$$

for all $y \in R_1$, $-b = (f_1(u))^{-1} a \in I \cap R_1$, for all $i = 2, \cdots, r$, $a_i = (f_1(u))^{-1} f_i(u) \in R_1$ are all independent of y. As I is a nil ideal, $b^{n+1} = 0$, for some n.

For $\alpha_2, ..., \alpha_s \in R_1$, let us substitute the element

$$b + \alpha_2 b^2 + ... + \alpha_n b^n, \qquad \cdots (3)$$

of $I \cap R_1$ for y in the relation (2). As $b^{n+1} = 0$, the equation (2) becomes

$$(f_1(u))^{-1} f(u + y) = \beta_2 b^2 + \beta_3 b^3 + ... + \beta_n b^n, \qquad \cdots (4)$$

where

$$\beta_2 = \alpha_2 + a_2,$$

and

$$\beta_s = \alpha_s + c_s, \ for \ s \geq 3,$$

where each c_s is a well defined polynomial in the elements $a_2, ..., a_s$ and $\alpha_2, ..., \alpha_{s-1}$ with integer coefficients. We now choose α_s in such a way that $\beta_s = 0$ for $s \geq 2$. For this $\alpha_2 = -a_2 \in R_1$. Suppose, for some $i \geq 2$, we have already chosen $\alpha_2, ..., \alpha_i$ such that $\beta_j = 0$ and $\alpha_j \in R_1$ for $2 \leq j \leq i$. As c_{i+1} is a polynomial in $a_2, ..., a_{i+1}$ and $\alpha_2, ..., \alpha_i$ with integers coefficients, clearly $c_{i+1} \in R_1$. Then $\alpha_{i+1} = -c_{i+1} \in R_1$. This shows that all the $\alpha_i \in R_1$. Let

$$y = b + \alpha_2 b^2 + ... + \alpha_n b^n.$$

As $b \in I \cap R_1$, $y \in I \cap R_1$ and $f(u + y) = 0$. ♣

Definition 2 [6] [Hensel ring]**.** Let (R, M) be a commutative local ring. Then R is called a *Hensel ring* if it satisfies the following condition:

Let $f(x) \in R[x]$ be any monic polynomial. If for some monic polynomials $g_0(x)$, $h_0(x) \in R[x]$,

$$\overline{f}(x) = \overline{g_0}(x)\overline{h_0}(x)$$

with $\langle g_0(x) \rangle + \langle h_0(x) \rangle + M[x] = R[x]$, then there exist monic polynomials $g(x)$, $h(x) \in R[x]$ such that

$$f(x) = g(x)h(x),$$

$\overline{g}(x) = \overline{g_0}(x)$, $\overline{h}(x) = \overline{h_0}(x)$.

It is well known that any complete commutative local noetherian ring is a Hensel ring [9]. We prove a special case of this result.

Theorem 3 [Hensel lemma]**.** *Let (R, M) be a commutative local ring with M nilpotent. Then R is a Hensel ring.*

Proof: Let $f(x) \in R[x]$ be a monic polynomial such that

$$\overline{f}(x) = \overline{g_0}(x)\overline{h_0}(x),$$

where $g_0(x)$, $h_0(x) \in R[x]$, $\langle g_0(x) \rangle + \langle h_0(x) \rangle + M[x] = R[x]$, so

$$f(x) = g_0(x)h_0(x) + \nu(x), \ \nu(x) \in M[x].$$

Now $\langle g_0(x) \rangle + \langle h_0(x) \rangle + M[x] = R[x]$ gives that there exists $\alpha_0(x)$, $\alpha_0'(x) \in R[x]$, and $\nu_0(x) \in M[x]$ such that

$$\alpha_0(x)g_0(x) + \alpha_0'(x)h_0(x) = 1 + \nu_0(x),$$

$1 + \nu_0(x)$ is a unit in $R[x]$. We prove by induction on k that there exist monic polynomials $g_k(x)$, $h_k(x) \in R[x]$ such that

$$\overline{g_k}(x) = \overline{g_0}(x),$$

$$\overline{h_k}(x) = \overline{h_0}(x),$$

$$f(x) \equiv g_k(x)h_k(x) \ (mod\ M^{k+1}[x]),$$

and

$$\langle g_k(x)\rangle + \langle h_k(x)\rangle + M[x] = R[x].$$

The result holds for $k = 0$. Suppose the result holds for $k = r$. Then there exist monic polynomials $g_r(x)$, $h_r(x) \in R[x]$ such that

$$\overline{g_r}(x) = \overline{g_0}(x),$$

$$\overline{h_r}(x) = \overline{h_0}(x),$$

$$f(x) \equiv g_r(x)h_r(x) \ (mod\ M^{r+1}[x]),$$

and

$$\langle g_r(x)\rangle + \langle h_r(x)\rangle + M[x] = R[x].$$

As M is nilpotent, by Nakayama's lemma (1.4), we have

$$\langle g_r(x)\rangle + \langle h_r(x)\rangle = R[x],$$

$$1 = \alpha_r(x)g_r(x) + \beta_r(x)\ h_r(x).$$

Consider $g_{r+1}(x) = g_r(x) + \beta_r(x)\ \nu_r(x)$, $h_{r+1}(x) = h_r(x) + \alpha_r(x)\ \nu_r(x)$, where $\nu_r(x) \in M^{r+1}[x]$ is such that $f(x) = g_r(x)\ h_r(x) + \nu_r(x)$. Then

$$g_{r+1}(x)h_{r+1}(x) = f(x) + \alpha_r(x)\beta_r(x)\nu_r^2(x),$$

clearly $\nu_r^2(x) \in M^{r+2}[x]$. Hence

$$f(x) \equiv g_{r+1}(x)h_{r+1}(x) \ (mod\ M^{r+2}[x]).$$

As $M^l = \{0\}$ for some l, let $t = l - 1$. Then we get

$$f(x) = g_t(x)h_t(x),$$

$$\overline{g_t}(x) = \overline{g_0}(x),$$

$$\overline{h_t}(x) = \overline{h_0}(x). \quad \clubsuit$$

Let (R, M) be a local ring such that $\overline{R}$ is a field, $\overline{f}(x)$ be an irreducible polynomial over $\overline{R}$. Then by (1.26), $\overline{R}[x]/\left\langle \overline{f}(x)\right\rangle$ is a field. But $R[x]/\left\langle f(x), M[x]\right\rangle \cong \overline{R}[x]/\left\langle \overline{f}(x)\right\rangle$. Hence $\langle f(x), M[x]\rangle = \langle f(x)\rangle + M[x]$ is a maximal ideal of $R[x]$.

Theorem 4. *Let R be a Hensel ring and $f(x)$ a monic polynomial over R. Then every non-multiple root of $\overline{f}(x)$ in $\overline{R}$ can be lifted to a unique root of $f(x)$ in R.*

Proof : Let $\overline{a}$ be a non-multiple root of $\overline{f}(x)$ in $\overline{R}$. Then

$$\overline{f}(x) = (x - \overline{a})\ \overline{g}(x),$$

such that $\overline{g}(\overline{a}) \neq 0$. Therefor $g(a) \notin J(R)$ and hence $g(x) \notin \langle (x-a) \rangle + J(R)[x]$. As $\langle (x - \overline{a}) \rangle$ is irreducible polynomial over $\overline{R}$, $\langle (x-a) \rangle + J(R)[x]$ is a maximal ideal in $R[x]/J(R)[x]$. So $\langle g(x) \rangle + \langle (x-a) \rangle + J(R)[x] = R[x]$. By Hensel lemma, there exist monic polynomials $h_1(x)$, $g_1(x) \in R[x]$ such that

$$f(x) = h_1(x)g_1(x),$$

$$\overline{h_1}(x) = (x - \overline{a}),$$

$$\overline{g_1}(x) = \overline{g}(x).$$

As $h_1(x)$ is monic, $deg\ h_1(x) = 1$. So we have $h_1(x) = x - a_1$, $\overline{a_1} = \overline{a}$. Suppose that $b\,(\neq a_1) \in \overline{a}$ is another root of $f(x)$. Then

$$0 = f(b) = (b - a_1)g(b).$$

As $(b - a_1) \neq 0$, $g(b) \in J(R)$. Hence

$$\overline{g}(\overline{a}) = \overline{g}(\overline{b}) = 0.$$

This is a contradiction because $\overline{a} = \overline{b}$ is not a multiple root of $\overline{f}$ in $\overline{R}$. Thus $b = a_1$ and a_1 is the unique lift algebraic element in $\overline{a}$. ♣

Proposition 5. *If R is a local ring with $J(R)$ a nil ideal and T is a subring of R such that $T/(T \cap J(R))$ is a division ring, then T is a local ring with $J(T) = T \cap J(R)$.*

Proof : Suppose that $T/(T \cap J(R))$ is a division ring. Then $T \cap J(R)$ is a maximal ideal, and hence $J(T) \subseteq T \cap J(R)$. As R is a local ring with $J(R)$ a nil ideal and consequently $T \cap J(R)$ is a nil ideal in T, $T \cap J(R) \subseteq J(T)$. Hence $J(T) = T \cap J(R)$ is a maximal ideal of T. Hence T is a local ring. ♣

Lemma 6. *Let R be a local ring such that $J(R)$ is nilpotent and $\overline{R}$ an algebraic field extension of a field F. Then any subring T of R such that $\overline{T} = (T + J(R))/J(R)$ contains F, is a local subring with $J(T) = T \cap J(R)$ a nilpotent ideal.*

Proof : As $F \subseteq \overline{T} = (T + J(R))/J(R) \subseteq \overline{R}$ and $\overline{R}$ is an algebraic field extension of F, $\overline{T}$ is a subfield of $\overline{R}$. Since

$$T/(T \cap J(R)) \cong (T + J(R))/J(R),$$

$T/(T \cap J(R))$ is a field and $J(T) = T \cap J(R)$. By Proposition 5, T is a local subring. As $J(R)$ is a nilpotent ideal, $J(T)$ is also nilpotent. ♣

Definition 7. Let R be a commutative local ring. Then a monic polynomial $f(x) = \sum_{i=0}^{r} a_i x^i \in R[x]$ is said to be *separable* [*partially irreducible*] polynomial over R if $f(x)$ is separable [irreducible] modulo $J(R)$, in the since that $\overline{f}(x) = \sum_{i=0}^{r} \overline{a_i} x^i \in \overline{R}[x]$ is separable [irreducible] over $\overline{R}$.

Definition 8. Let R be a local ring and T a commutative local subring of R such that $J(T) = J(R) \cap T$. Then
(i) An element a in R is said to be a *lift algebraic element* over T if there exists a partially irreducible polynomial $f(x)$ over T such that $f(a) = 0$; $f(x)$ is called a *minimal polynomial* of a over T. If *deg* $f(x) = r$, then a is said to be of *degree* r over T.
(ii) A lift algebraic element a in R over T is said to be *separable* over T if its minimal polynomial over T is separable.

Example 1. Let $f(x) = x^2 + x + 3 \in \mathbb{Z}_4[x]$ and $R = \mathbb{Z}_4[y]/\langle f(y)\rangle$. Then $\overline{f}(x) = x^2 + x + \overline{1} \in \overline{\mathbb{Z}_4}[x]$ is irreducible over $\overline{\mathbb{Z}_4} = \mathbb{Z}_4/2\mathbb{Z}_4$. So $f(x)$ is partially irreducible polynomial over $\mathbb{Z}_4$ and hence R is a Galois ring of the form $GR\left(2^2, 2\right)$. Now

$$\overline{\mathbb{Z}_4} \subseteq T = \overline{\mathbb{Z}_4}[y]/\langle y^2 + y + 1\rangle \cong GF\left(2^2\right)$$

and $\overline{y} = y + \langle y^2 + y + 1\rangle \in T$ is a root of $\overline{f}(x)$. As

$$\overline{R} = \overline{\mathbb{Z}_4[y]}/\langle \overline{y^2 + y + 3}\rangle \cong T,$$

Clearly $y + \langle y^2 + y + 3\rangle \in R$ is a lift algebraic element over $\mathbb{Z}_4$.

Corollary 9. *Let T be a commutative local ring with $J(T)$ nilpotent, and T' a local subring of T such that $J(T') = T' \cap J(T)$. Let $\overline{a} \in \overline{T}$ be separable over $\overline{T'}$ and $f(x)$ a monic polynomial over T' such that $\overline{f}(x)$ the minimal polynomial of $\overline{a}$. Then there exist unique $b \in \overline{a}$ such that $f(b) = 0$.*

Proof : As $\overline{f}(\overline{a}) = 0$ and $\overline{f}(x)$ has no multiple root in $\overline{T}$. By Theorem 4, there exist a unique lift algebraic element b in $a + J(T)$ such that $f(b) = 0$. ♣

Definition 10. Let R be any ring and T a subring of R. Then R is called an *unramified extension* of T if $J(R) = J(T)R$.

Proposition 11 [1]**.** *Let T be any commutative local ring with $J(T)$ a nilpotent and $f(x)$ a partially irreducible polynomial over T. Then $R = T[x]/\langle f(x)\rangle$ is a local ring and an unramified extension of T. Also the indices of nilpotencies of $J(R)$ and $J(T)$ are the same.*

Proof : Let $R = T[x]/\langle f(x)\rangle$, then $\lambda : T \longrightarrow R$ such that $\lambda(a) = a + \langle f(x)\rangle$, $a \in T$, is an embedding of T in R. Consider

$$A = (J(T)[x] + \langle f(x)\rangle)/\langle f(x)\rangle.$$

As $J(T)^n = \{0\}$ for some n, $A^n = \{0\}$, so $A \subseteq J(R)$. But

$$R/A \cong T[x]/\langle J(T)[x] + \langle f(x)\rangle\rangle \cong \overline{T}[x]/\left\langle \overline{f}(x)\right\rangle.$$

As $\overline{f}(x) \in \overline{T}[x]$ is an irreducible polynomial over the field $\overline{T}$, $\overline{T}[x]/\left\langle \overline{f}(x)\right\rangle$ is a field. Therefore A is a maximal ideal of R and subsequently $J(R) \subseteq A$. Thus $J(R) = A = \lambda(J(T))R$. This shows that R is an unramified extension of T and R is a local ring. If n is the index of nilpotency of $J(T)$, then $J(T)^n = \{0\}$ and this implies $A^n = \{0\}$. Also if $A^t = \{0\}$ for some t, then $\{0\} = A^t = (\lambda(J(T))R)^t$ and consequently $J(T)^t = \{0\}$. Hence the indices of nilpotencies of $J(R)$ and $J(T)$ are the same. ♣

2.2 Extensions of a special primary ring

Definition 12. Let R be a commutative local ring and T a special primary subring of R. Then R is said to be a $T-$*separable ring* if $J(R)=J(T)R$ and $\overline{R}$ is a finite separable field extension of $(T+J(R))/J(R)$. If, in addition, $\overline{R}$ is a Galois extension of $(T+J(R))/J(R)$, R is called a $T-$*Galois ring*.

Theorem 13 [1]**.** *Let R be any local ring, (T,π) a special primary subring of R and $\pi R=R\pi$. Then*
(i) $J(T)=\pi T=J(R)\cap T$;
(ii) Let $a\in Z_R(T)$ be a lift algebraic element over T. Then

$$T[a]\cong T[x]/\langle f(x)\rangle .$$

and

$$d({}_TT[a])=\deg f(x)\cdot d({}_TT),$$

where $f(x)$ is a minimal polynomial of a over T.

Proof : *(i)* As π is nilpotent, and $\pi R=R\pi$, πR is nilpotent. So $\pi R\subseteq J(R)$, consequently $\pi T\subseteq J(R)\cap T$. As $1\notin J(R)\cap T$, $J(R)\cap T\neq T$. But πT is the unique maximal ideal of T. Thus $\pi T=J(R)\cap T$.
(ii) Define $\lambda: T[x]\longrightarrow T[a]$ such that $\lambda(g(x))=g(a)$ for $g(x)\in T[x]$. Since $\lambda(f(x))=f(a)=0$, $\langle f(x)\rangle\subseteq Ker\ \lambda$. Suppose some $g(x)\in Ker\ \lambda$ with $g(x)\notin\langle f(x)\rangle$. By the division algorithm, $g(x)=f(x)q(x)+h(x)$ for some $q(x),h(x)\in T[x]$ with $h(x)=0$ or $\deg h(x)<\deg g(x)$. As $f(x)$ does not divide $g(x)$, $h(x)\neq 0$ and hence $0=g(a)=f(a)\underline{q(a)}+h(a)$, gives $h(x)\in Ker\ \lambda$. Also $\overline{f}(x)$ is the minimal polynomial of $\overline{a}$. So $\overline{h(a)}=0$ implies that $h(x)\in J(T)[x]$. But $J(T)=\pi T$. So $h(x)=\pi^s h_1(x)$, for some $s\geq 0$ and $h_1(x)\in T[x]\setminus J(T)[x]$ with $\deg h_1(x)=\deg h(x)<\deg f(x)$. Then $0=h(a)=\underline{\pi^s h_1(a)}$ and $\pi^s\neq 0$, gives $h_1(a)\in J(R)$; *i.e.*, $\overline{h_1(a)}=0$. This implies that $\overline{h_1}(x)=0$ and hence $h_1(x)\in J(T)[x]$. This is a contradiction. Therefore there does not exist any $g(x)\in Ker\ \lambda$ such that $g(x)\notin\langle f(x)\rangle$. Hence $Ker\ \lambda=\langle f(x)\rangle$, and

$$T[x]/\langle f(x)\rangle\cong T[a].$$

Since $f(x)$ is a monic polynomial over T, by (1.14),

$$d({}_T(T[a]))=d({}_T(T[x]/\langle f(x)\rangle))=d({}_TT)\cdot\deg f(x).\quad\clubsuit$$

Theorem 14 [1]**.** *Let $(T,\pi),(R,\pi)$ be special primary rings such that $T\subseteq R$ and $\overline{R}=\overline{T}[\overline{a}]$, where $\overline{T}=(T+\pi R)/\pi R$ and $\overline{a}$ is an algebraic element in $\overline{R}$ over $\overline{T}$. Then there exists a lift algebraic element $b\in\overline{a}$ over T such that $R=T[b]$.*

Proof : As R is a Hensel ring, by Theorem 4, there exists $b\in\overline{a}$ a lift algebraic element in R over T. Let $f(x)\in T[x]$ be a minimal polynomial of b over T of degree r. Since R is an unramified extension of T, by Proposition 11, they have the same index of nilpotencies, say m. Now $d(\overline{T}\overline{R})=r$ and $d(\overline{T}\pi^iR/\pi^{i+1}R)=r$, for all $1\leq i\leq m-1$. So

$$d\,({}_TR)=d(\overline{T}\overline{R})\cdot d({}_TT)=rm.$$

By Theorem 13, $d\,({}_TT[b]) = rm$. But $T[b] \subseteq R$; hence $R = T[b]$. ♣

Remark 1. Let R be a commutative artinian local ring with $\overline{R}$ an absolutely algebraic field, and let (T, π) be a special primary subring of R. Suppose that $\overline{a}$ is a separable element in $\overline{R}$ over $\overline{T} = (T + J(R))/J(R)$ and $f(x)$ a partially irreducible polynomial over T such that $\overline{f}(\overline{a}) = 0$. By Corollary 9, there exist a unique lift algebraic element $a' \in R$ over T such that $f(a') = 0$ and $\overline{a'} = \overline{a}$. By Theorem 13$(ii)$, we have

$$T[a'] \cong T[x]/\langle f(x)\rangle .$$

Then by Proposition 11, $T[a']$ is a local and an unramified extension of T and hence $T[a']$ is a special primary subring of R. Let $\overline{b} \in \overline{T}[\overline{a}]$ such that $\overline{T}[\overline{b}] = \overline{T}[\overline{a}]$ and $g(x)$ a partially irreducible polynomial over T satisfying $\overline{g}(\overline{b}) = 0$. By Corollary 9, there exist a unique $b' \in T[a']$ such that $g(b') = 0$ and $b' + J(T[a']) = b + J(T[a'])$. Thus $T[b'] \subseteq T[a']$. By Theorem 13(ii),

$$d({}_TT[b']) = \deg\ g(x) \cdot d({}_TT) = d({}_TT[a']).$$

Therefore $T[b'] = T[a']$. Hence $T[a']$ is determined by the field $\overline{T}[\overline{a}]$ in the sense that it does not depend up on the choice of $\overline{a}$. Let us call two partially irreducible polynomials $f(x)$, $g(x) \in T[x]$ to be equivalent if $T[x]/\langle f(x)\rangle$ and $T[x]/\langle g(x)\rangle$ are $T-$*isomorphic*. From above we have

$$T[x]/\langle f(x)\rangle \cong T[a'] = T[b'] \cong T[x]/\langle g(x)\rangle .$$

Then the minimal polynomials of a' and b' are equivalent.

Theorem 15 [1]**.** *Let R be a local ring and (T, π) a special primary subring of R. Also let a, $b \in Z_R(T)$ be lift algebraic elements over T and $f(x)$ a minimal polynomial of a over T. Then the followings hold :*
(i) *If $f(b) = 0$, then there exists a $T-$isomorphism $\lambda : T[a] \longrightarrow T[b]$ such that $\lambda(a) = b$;*
(ii) *If $\overline{a}$ is separable over $\overline{T}$, then $T[a]$ is a T-separable ring;*
(iii) *If $\overline{a}$ is separable over $\overline{T}$, then $T[a] \subseteq T[b]$ if and only if $ab = ba$ and $\overline{T}[\overline{a}] \subseteq \overline{T}[\overline{b}]$ in $\overline{R}$, where $\overline{T} = (T + J(R))/J(R)$.*

Proof : (i) Suppose that $f(b) = 0$, then by Theorem 13(ii), $T[b] \cong T[x]/\langle f(x)\rangle$ with $T-$isomorphism γ defined by $\gamma(g(x) + \langle f(x)\rangle) = g(b)$, for all $g(x) \in T[x]$. Also there is an isomorphism $\delta : T[x]/\langle f(x)\rangle \longrightarrow T[a]$ such that $\delta(g(x) + \langle f(x)\rangle) = g(a)$, for all $g(x) \in T[x]$. Take $\lambda : R[a] \longrightarrow R[b]$ such that $\lambda = \gamma\delta^{-1}$. Then $\lambda(a) = \gamma\delta^{-1}(a) = \gamma(x + \langle f(x)\rangle) = b$.
(ii) Suppose that $\overline{a}$ is separable over $\overline{T}$, then $f(x)$ is separable polynomial over T. Hence $\overline{T}[\overline{a}] \cong \overline{T}[x]/\langle \overline{f}(x)\rangle$ is a finite separable extension. By Proposition 11, $T[a]$ is an unramified extension of T. Hence $T[a]$ is a T-separable ring.
(iii) Suppose that $T[a] \subseteq T[b]$, then it is clear that $\overline{T}[\overline{a}] \subseteq \overline{T}[\overline{b}]$ in $\overline{R}$ and $ab = ba$. Conversely, let $\overline{T}[\overline{a}] \subseteq \overline{T}[\overline{b}]$ and $ab = ba$. As $T[a]$ and $T[b]$ are finitely generated as $T-$*module*, $T' = T[a, b]$ is also finitely generated as $T-$*module*, so T' is a commutative artinian ring. As $T' \subseteq R$ and R has no non-trivial idempotent,

we get T' has no non-trivial idempotent. Hence by (1.17), T' is a local ring. Now

$$T'/(T' \cap J(R)) \cong (T' + J(R))/J(R) = \overline{T}[\overline{a}, \overline{b}] = \overline{T}[\overline{b}],$$

is a field. So $T' \cap J(R) = J(T')$ a nilpotent ideal. Therefore T' is a Hensel ring. Since $f(a) \in T' \cap J(R) = J(T')$ and $\overline{a}$ is separable over $\overline{T}$, by Theorem 4, there exists a unique $a' \in T'$ such that $a' \in a + J(T')$ and $f(a') = 0$. But $a \in T'$ and $f(a) = 0$, so we get $a = a' \in T[b]$. Hence $T[a] \subseteq T[b]$. ♣

Remark 2. Let R be an artinian local ring such that $\overline{R}$ is an absolutely algebraic field. Suppose that $f_1(x)$, $f_2(x) \in P[x]$ are partially irreducible polynomials over P such that

$$\overline{f_1}(x) = \overline{f_2}(x).$$

Let $\overline{a} \in \overline{R}$ such that $\overline{f_2}(\overline{a}) = \overline{f_1}(\overline{a}) = 0$. Then by Theorem 1, $\overline{a}$ has a lift algebraic element $a_1 \in R$ over P such that $f_1(a_1) = 0$. Now $\overline{a} = \overline{a_1} \in \overline{P}[\overline{a_1}]$. By Lemma 6, $P[a_1]$ is a commutative local subring of R with $J(P[a_1]) = J(R) \cap P[a_1]$ a nilpotent ideal of R. By Corollary 9, there exist a unique lift algebraic element $a_2 \in \overline{a}$ in $P[a_1]$ over P such that $f_2(a_2) = 0$. As $\overline{P}[\overline{a_1}] = \overline{P}[\overline{a_2}]$ and $a_1 a_2 = a_2 a_1$, by Theorem 15 (iii), $P[a_1] = P[a_2]$. Thus a lifting subring $P[a_1]$ of $\overline{P}[\overline{a}]$ is determined by the polynomial $\overline{f_1}(x)$ in the sense that it does not depend up on the choice of $f_i(x) \in P[x]$, $i = 1, 2$.

Proposition 16. *Let R be a local ring with $J(R)$ a nil ideal and $a \in R$ a lift algebraic element over P.*
(i) If char $R = 0$, then $P[a]$ is a field;
(ii) If char $R = p^n$, then $P[a]$ is a Galois ring of the form $GR(p^n, r)$, where r is the degree of a over P.

Proof : As a is a lift algebraic element over P, there exists a partially irreducible polynomial $f(x)$ over P such that $f(a) = 0$. Let deg $f(x) = r$.
(i) If *char* $R = 0$, then $P \cong \mathbb{Q}$; hence $f(x)$ is an irreducible over P and

$$P[a] \cong \mathbb{Q}[x]/\langle f(x) \rangle$$

is a field.
(ii) If *char* $R = p^n$, then $P \cong \mathbb{Z}_{p^n}$. By Theorem 13 (ii),

$$P[a] \cong P[x]/\langle f(x) \rangle \cong \mathbb{Z}_{p^n}[x]/\langle f(x) \rangle .$$

Hence $P[a]$ is the Galois ring of the form $GR(p^n, r)$. ♣

Proposition 17. *Let R be a commutative local ring such that $\overline{R}$ is an absolutely algebraic field, $J(R)$ a nilpotent ideal.*
(i) If char $R = 0$, T a subfield of R and $b \in R$ a lift algebraic element over P. Then $T[b]$ is a subfield of R;
(ii) If char $R = p^n$, T a Galois subring in R and $b \in R$ a lift algebraic element over P. Then $T[b]$ is a Galois subring in R .

Proof : (i) In this case $P = \mathbb{Q}$, and b is an algebraic element over T. So $T[b]$ is a subfield of R.

(ii) Let $f(x)$ be a partially irreducible polynomial over P such that $f(b) = 0$. Now $f(b) = 0$ gives $\overline{f}(\overline{b}) = 0$. Then $\overline{f}(x) = \overline{g}(x)\overline{h}(x)$, where $g(x)$, $h(x) \in T[x]$, $g(x)$ is partially irreducible polynomial over T and $\overline{g}(\overline{b}) = 0$. Now $f(x) - g(x)h(x) \in J(R)[x] \cap T[x] = J(T)[x] = pT[x]$,

$$f(x) \equiv g(x)h(x) \pmod{pT[x]}.$$

As T is a Hensel ring, we can get $g'(x)$, $h'(x) \in T[x]$ such that

$$f(x) = g'(x)h'(x),$$

$$g'(x) \equiv g(x) \pmod{pT[x]},$$

$$h'(x) \equiv h(x) \pmod{pT[x]},$$

$$\overline{g'(b)} = \overline{g(b)} = 0.$$

By Corollary 9, there exist a unique lift algebraic element $b' \in b + J(T[b])$ over T such that $g'(b') = 0$. As $f(b') = 0$ and $\overline{b} = \overline{b'}$, $b = b'$. By Proposition 11, $T[x]/\langle g'(x)\rangle$ is an unramified extension of T. Then

$$\begin{aligned} J(T[x]/\langle g'(x)\rangle) &= J(T)(T[x]/\langle g'(x)\rangle) \\ &= pT(T[x]/\langle g'(x)\rangle) \\ &= p(T[x]/\langle g'(x)\rangle), \end{aligned}$$

By (1.38), $T[x]/\langle g'(x)\rangle$ is a Galois ring. By Theorem 13 (ii),

$$T[b] \cong T[x]/\langle g'(x)\rangle.$$

Therefore $T[b]$ is a Galois subring of R. ♣

Theorem 18 [1]**.** *Let T be a special primary ring. Then two $T-$Galois rings R, R' are $T-$isomorphic if and only if $\overline{R}$ and $\overline{R'}$ are $\overline{T}-$isomorphic.*

Proof : By Theorem 14, R, R' are simple extensions of T by lift algebraic element and hence they are special primary rings. Suppose that R and R' are $T-isomorphic$ and $\sigma : R \to R'$ a $T-isomorphism$. Then we get that $\overline{\sigma} : \overline{R} \to \overline{R'}$ is $\overline{T}-isomorphism$. Conversely, suppose that $\overline{R} \cong \overline{R'}$. Let $\overline{R} = \overline{T}[\overline{b}]$, where $\overline{T} = T + J(R)/J(R)$. Then by Theorem 14, there exists $b' \in \overline{b}$ such that $R = T[b']$ and b' is lift algebraic element over T. Let $g(x)$ be a minimal polynomial of b' over T. Then by Theorem 13(ii),

$$R = T[b'] \cong T[x]/\langle g(x)\rangle.$$

As $\overline{R} \cong \overline{R'}$, $\overline{g}(x) \in \overline{T}[x]$, has a root $\overline{a} \in \overline{R'}$, $\overline{R'} = \overline{T}[\overline{a}]$. As R is a Hensel ring, by Theorem 4, there exists a unique lift algebraic element $a' \in \overline{a}$ over T such that $g(a') = 0$. By Theorems 13(ii), $R' \cong T[x]/\langle g(x)\rangle$. Hence $\overline{R}$ *and* $\overline{R'}$ *are* $\overline{T}-isomorphic$. ♣

Definition 19. Let R be a local ring. Then $\eta \in Aut\ R$ is said to be a *lifting* of $\sigma \in Aut\ \overline{R}$ if for all $\overline{a} \in \overline{R}$, $\sigma(\overline{a}) = \eta(a) + J(R) = \overline{\eta(a)}$.

Theorem 20. *Let T be a special primary ring, R a $T-$Galois ring and $\sigma \in Aut_{\overline{T}}\overline{R}$, where $\overline{T} = (T + J(R))/J(R)$. Then σ has a unique lifting η in $Aut_T R$.*

Proof : Let $\sigma : \overline{R} \longrightarrow \overline{R}$ be a $\overline{T} - isomorphism$. As $\overline{R}$ is a finite Galois extension of $\overline{T}$, we can find $\overline{a} \in \overline{R}$ separable over $\overline{T}$ such that $\overline{R} = \overline{T}[\overline{a}]$. Let $f(x) \in T[x]$ be a partially irreducible polynomial such that $\overline{f}(\overline{a}) = 0$. As R is a special primary ring and hence a Hensel ring, by Theorem 4, there exists a unique lift algebraic element $a' \in \overline{a}$ in R such that $f(a') = 0$. By using Theorem 14, one can deduce that $R = T[a']$. As

$$\overline{f}(\sigma(\overline{a'})) = \sigma(\overline{f}(\overline{a'})) = 0,$$

again by Theorem 4, there exists a unique lift algebraic element $b \in \sigma(\overline{a'})$ in R over T such that $f(b) = 0$. By Theorem 15 (i), we get an $T - isomorphism$ $\eta : T[a'] \longrightarrow T[b]$ such that $\eta(a') = b$. As $\overline{T}[\overline{a}] = \overline{T}[\sigma(\overline{a})]$, $\sigma(\overline{a})$, $\overline{a}$ are separable, by Theorem 15 (iii), $T[a'] = T[b]$. Hence η is a lifting of σ. Suppose there is another $T - automorphism$ $\eta' : R \longrightarrow R$ a lifting of σ. Then $f(a') = 0$ implies that $f(\eta'(a')) = 0$. But

$$\overline{\eta'(a')} = \sigma(\overline{a}) = \overline{b},$$

with $f(b) = 0$. By the uniqueness of b, $b = \eta'(a')$. Hence $\eta = \eta'$. ♣

2.3 Generalized Galois rings

Definition 21. Let $\{R_i\}_{i\in\Lambda}$ be countable set of Galois rings of the same characteristic such that for any α, $\beta \in \Lambda$ there exists $\gamma \in \Lambda$ such that $R_\alpha \cup R_\beta \subseteq R_\gamma$. Let $R = \underset{i\in\Lambda}{\cup} R_i$. Then clearly R is a ring; such a ring is called a *generalized Galois ring.*

Proposition 22. *If $R = \underset{i\in\Lambda}{\cup} R_i$ is a generalized Galois ring, then R is a special primary ring.*

Proof : There exists a prime number p and a positive integer n such that each Galois ring R_i has characteristic p^n. Now $J(R_i) = pR_i \subseteq pR$ gives $\underset{i\in\Lambda}{\cup} J(R_i) \subseteq pR$. Consider $px \in pR$. For some $i \in \Lambda$, $x \in R_i$ and so $px \in pR_i \subseteq \underset{i\in\Lambda}{\cup} pR_i$. Hence $pR = \underset{i\in\Lambda}{\cup} pR_i$. Clearly $pR \subseteq J(R)$. Consider any $y \in R\backslash pR$. Then for some $i \in \Lambda$, $y \in R_i\backslash pR_i$, so y is a unit and consequently R is a local ring. Hence $J(R) = pR$. As $p^n = 0$, and $p^{n-1} \neq 0$, R is an artinian. By (1.24), R is a chain ring and n is the index of nilpotency of $J(R)$. Thus R is a special primary ring . ♣

Proposition 23. *Let R be a local ring with char $R = p^n$ and for each i, let a_i be a lift algebraic element in R over P such that $\underset{i\in\Lambda}{\cup} \overline{P}[\overline{a_i}]$ is the maximal absolutely algebraic subfield of $\overline{R}$ and $a_i a_j = a_j a_i$ for all $i, j \in \Lambda$. Then $\underset{i\in\Lambda}{\cup} P[a_i]$ is a generalized Galois ring.*

Proof : Let $P[a_k]$, $P[a_j] \subseteq \underset{i\in\Lambda}{\cup} P[a_i]$. Then the subfield generated by $\overline{P}[\overline{a_k}] \cup \overline{P}[\overline{a_j}]$ is $\overline{P}[\overline{a_k}, \overline{a_j}] = \overline{P}[\overline{c}]$ for some $\overline{c} \in \overline{R}$. Thus $\overline{c} \in \overline{P}[\overline{a_\gamma}]$ for some γ and hence $\overline{P}[\overline{a_k}] \cup \overline{P}[\overline{a_j}] \subseteq \overline{P}[\overline{a_\gamma}]$. As a_γ is a lift algebraic element over P, $\overline{a_\gamma}$ is separable over $\overline{P}$. Since $a_k a_\gamma = a_\gamma a_k$, $a_\gamma a_j = a_j a_\gamma$, Theorem 15 (iii) implies that $P[a_k] \cup P[a_j] \subseteq P[a_\gamma]$. Therefore $\underset{i\in\Lambda}{\cup} P[a_i]$ is a generalized Galois ring. ♣

Corollary 24. *Any generalized Galois ring can be written as a union of ascending chain of Galois subrings.*

Proof : Let $R = \underset{i\in\Lambda}{\cup} P[a_i]$ be a generalized Galois ring such that $P[a_i] = GR(p^n, r_i)$ is a Galois subring for each i. Then $\overline{R} = \underset{i\in\Lambda}{\cup} \overline{P}[\overline{a_i}]$ is an absolutely algebraic field. Hence $\overline{R}$ can be written as a union of ascending chain of simple field extensions over the prime subfield of $\overline{R}$, say $\overline{R} = \overset{\infty}{\underset{i=1}{\cup}} \overline{P}[\overline{b_i}]$. As R is a Hensel ring, by Theorem 4, for each i, there exist a lift algebraic element $b_i' \in \overline{b_i}$ over P. Let $T = \overset{\infty}{\underset{i=1}{\cup}} P[b_i'] \subseteq R$. For $i \leq j$,

$$\overline{P}[\overline{b_i'}] = \overline{P}[\overline{b_i}] \subseteq \overline{P}[\overline{b_j}] = \overline{P}[\overline{b_j'}].$$

Also $\overline{b_i'}$ and $\overline{b_j'}$ are separable over $\overline{P}$. By Theorem 15(iii), $P[b_i] \subseteq P[b_j]$. Hence $T = \overset{\infty}{\underset{i=1}{\cup}} P[b_i']$ is a union of an ascending chain of Galois subrings. Now

$$\overline{T} = \overset{\infty}{\underset{i=1}{\cup}} \overline{P}[\overline{b_i'}] = \overset{\infty}{\underset{i=1}{\cup}} \overline{P}[\overline{b_i}] = \overline{R},$$

so $R = T + J(R) = T + pR$. As p is nilpotent element in T, $R = T$. Hence R is a union of an ascending chain of Galois subrings. ♣

Henceforth, if we write a generalized Galois ring $R = \overset{\infty}{\underset{i=1}{\cup}} P[a_i]$, then we mean R is a union of ascending chain of Galois subrings $P[a_i]$, $1 \leq i < \infty$. It is clear that if $char\ R = p$, then R is an absolutely algebraic field.

Theorem 25. *Let R, R' be two generalized Galois rings such that $char\ R = char\ R' = p^n$. Then R, R' are isomorphic if and only if*

$$\overline{R} \cong \overline{R'}.$$

Proof : It is clear that if $R \cong R'$, then $\overline{R} \cong \overline{R'}$. As $char\ R = char\ R' = p^n$, $P \cong \mathbb{Z}_{p^n}$ and $\overline{P} \cong \mathbb{Z}_p$. Suppose that $\overline{R} \cong \overline{R'}$, $R = \overset{\infty}{\underset{i=1}{\cup}} P[a_i]$. Let $\overline{\eta} : \overline{R} \longrightarrow \overline{R'}$ be an isomorphism. For each i, let $f_i(x)$ be a partially irreducible polynomial over P of degree r_i such that $\overline{f_i}(\overline{a_i}) = 0$. So $\overline{f_i}(\overline{\eta}(\overline{a_i})) = 0$. As R, R' are Hensel rings, there exist unique lift algebraic elements $a_i' \in \overline{a_i}$, $b_i' \in \overline{\eta}(\overline{a_i})$ over P in R, R' respectively having the same minimal polynomial $f_i(x)$. By Proposition 16(ii), $P[a_i']$, $P[b_i']$ are Galois subrings in R, R' respectively of the form $GR(p^n, r_i)$. Then by the proof of Theorem 18, there exists an isomorphism $\Psi_i : P[a_i'] \longrightarrow P[b_i']$ such that $\Psi_i(a_i') = b_i'$. We have $P[a_{i-1}'] \subseteq P[a_i']$ and

subsequently $P[b'_{i-1}] \subseteq P[b'_i]$. Let $a'_{i-1} = v\,(a'_i)$, where $v(x) \in P[x]$. Then

$$\begin{aligned}
\overline{\Psi_i(a'_{i-1})} &= \overline{\Psi_i(v\,(a'_i))} \\
&= \overline{v(\Psi_i(a'_i))} \\
&= \overline{v(b'_i)} \\
&= \overline{v}(\overline{b_i}) \\
&= \overline{v}\left(\overline{\eta}\left(\overline{a'_i}\right)\right) \\
&= \overline{\eta}\left(\overline{v}\left(\overline{a'_i}\right)\right) \\
&= \overline{\eta}\left(\overline{a'_{i-1}}\right) \\
&= \overline{b_{i-1}}.
\end{aligned}$$

As $f_{i-1}(x) \in P[x]$ is a minimal polynomial of a'_{i-1} over P. Then $f_{i-1}(\Psi_i\left(a'_{i-1}\right)) = 0$. Also $f_{i-1}(b'_{i-1}) = 0$. By Theorem 4,

$$\Psi_i\left(a'_{i-1}\right) = b'_{i-1}.$$

This proves that Ψ_i is an extension of Ψ_{i-1}. Then we can define $\Psi : R \longrightarrow R'$ such that $\Psi(c) = \Psi_j(c)$ if $c \in P[a'_j]$, and hence Ψ is an isomorphism. ♣

Theorem 26. *Let R_0 be a generalized Galois ring with char $R = p^n$ and $\sigma \in Aut\ \overline{R_0}$. Then σ has unique lifting in Aut R_0.*

Proof : Let $R_0 = \overset{\infty}{\underset{i=1}{\cup}} P[a_i]$ be a union of ascending chain of Galois subrings $P[a_i]$. For each a_i, there exists a partially irreducible polynomial $f_i(x) \in P[x]$ such that $f_i(a_i) = 0$. Let $\sigma \in Aut\ \overline{R_0}$. Then $\overline{f_i}(\overline{a_i}) = 0$ in $\overline{R_0}$ gives $\overline{f_i}(\sigma(\overline{a_i})) = 0$. As $\overline{R_0}$ is an absolutely algebraic field and R_0 is a Hensel ring, by Theorem 4, there exists a unique element $b_i \in R_0$ such that $\overline{b_i} = \sigma(\overline{a_i})$ and $f_i(b_i) = 0$. Now $P[a_i] \subseteq P[a_{i+1}]$ implies $\overline{P}[\overline{a_i}] \subseteq \overline{P}[\overline{a_{i+1}}]$ and subsequently $\overline{P}[\sigma(\overline{a_i})] \subseteq \overline{P}[\sigma(\overline{a_{i+1}})]$. Then by Theorem 15$(iii)$, $P[b_i] \subseteq P[b_{i+1}]$. Also by Theorem 15$(i)$, for each i, we have an isomorphism $\eta_i : P[a_i] \longrightarrow P[b_i]$ such that $\eta_i(a_i) = b_i$. As seen in the proof of Theorem 25, η_{i+1} extends η_i for every i. Define $\eta : R_0 \longrightarrow R_0$ such that $\eta(b) = \eta_i(b)$ if $b \in P[a_i]$. Then η is a monomorphism. As $\overline{\eta(R_0)} = \sigma(\overline{R_0}) = \overline{R_0}$,

$$\begin{aligned}
R_0 &= \eta(R_0) + J(R_0) \\
&= \eta(R_0) + pR_0.
\end{aligned}$$

Since p is nilpotent in $\eta(R_0)$, we deduce

$$R_0 = \eta(R_0).$$

Hence η is an automorphism of R_0 and it is a lifting of σ. Suppose there is another automorphism η' of R_0 and it is a lifting of σ. Consider any a_i, as $f_i(a_i) = 0$, $f_i(\eta'(a_i)) = 0$. But $\overline{\eta'(a_i)} = \sigma(\overline{a_i}) = \overline{b_i}$, by Theorem 4, $\eta'(a_i) = b_i$. This gives η' restricted to $P[a_i]$ is η_i for each i. Hence $\eta' = \eta$. ♣

Theorem 27. *Let R_0 be a generalized Galois ring. Then*

$$Aut\ \overline{R_0} \cong Aut\ R_0.$$

Proof : Let $\sigma \in Aut\ \overline{R_0}$. By Theorem 26, there exists a unique automorphism η_σ of R_0 such that $\overline{\eta_\sigma(a)} = \sigma(\overline{a})$, $\overline{\eta_\sigma(a)} = \eta_\sigma(a) + pR_0$ for all $a \in R_0$. So we can define

$$\Psi : Aut\ \overline{R_0} \longrightarrow Aut\ R_0$$

such that $\Psi(\sigma) = \eta_\sigma$. For $\sigma, \delta \in Aut\ \overline{R_0}$, $a \in R_0$, $\Psi(\sigma\delta) = \eta_{\sigma\delta}$, $\overline{\eta_{\sigma\delta}(a)} = \sigma\delta(\overline{a})$, but $\sigma\delta(\overline{a}) = \sigma(\delta(\overline{a})) = \sigma(\overline{\eta_\delta(a)}) = \overline{\eta_\sigma\eta_\delta(a)}$. By Theorem 26, $\sigma\delta$ has unique lifting $\eta_{\sigma\delta}$. Then $\eta_{\sigma\delta} = \eta_\sigma\eta_\delta$, and $\Psi(\sigma\delta) = \eta_{\sigma\delta} = \eta_\sigma\eta_\delta = \Psi(\sigma)\Psi(\delta)$. Hence Ψ is a group homomorphism, if $\sigma \in \ker\Psi$, then $\eta_\sigma = \Psi(\sigma) = I_{R_0}$, $\sigma(\overline{a}) = \overline{\eta_\sigma(a)} = \overline{I_{R_0}(a)} = \overline{a}$, for all $a \in R_0$, so $\sigma = I_{\overline{R_0}}$ the identity on $\overline{R_0}$. Therefore Ψ is a monomorphism. Let $\eta \in Aut\ R_0$, and let $\sigma : R_0 \longrightarrow R_0$ such that $\sigma(\overline{a}) = \overline{\eta(a)}$. Then $\sigma \in Aut\ \overline{R_0}$ and $\Psi(\sigma) = \eta$. Thus Ψ is an isomorphism. ♣

CHAPTER 3

Coefficient Subring

It is a consequence of Cohen's structure Theorem for complete local rings [21, $p.106$] that every finite commutative ring R of characteristic p^n contains a unique special primary subring R_0 satisfying $R/J(R) \cong R_0/pR_0$. Cohen called R_0 the coefficient subring of R. Actually the existence and structure of R_0 for finite commutative local ring R was known to Krull as early as 1924 [18, $p.20$]. For finite commutative local ring it turns out that R_0 is a Galois ring. Clark (1972) [7] proved that a coefficient subring of finite $p-ring$ R is a direct sum of full matrix rings over Galois rings. Finally Corbas [11] manages to characterize coefficient subring of a finite ring as a direct sum of full matrix rings over Galois rings.

Let R be an artinian local duo ring such that $\overline{R}$ is an absolutely algebraic field. In the first section of this chapter, we prove that R has a coefficient subring R_0, which is either a field or a generalized Galois ring. As a direct consequence of this result we get that if R is a local ring of characteristic p^n then R is a generalized Galois ring if and only if $J(R) = pR$ and $\overline{R}$ is an absolutely algebraic field, which generalized a similar result for finite local ring [7].

In the second section of this chapter, we prove that if R is an artinian local duo ring such that $\overline{R}$ is a simple transcendental field extension of an absolutely algebraic field of non-zero characteristic, then the coefficient subring of R is a simple transcendental extension of a generalized Galois subring K_0 which is a coefficient subring of the ring of all algebraic elements in R over P. Moreover any two coefficient subrings of R are isomorphic.

3.1 Absolutely algebraic fields

Lemma 1. *Let R be a commutative local ring with $J(R)$ a nilpotent ideal. Let*

$$f(x) = \sum_{i=0}^{t} a_i x^i \in R[x] \ .$$

Then the following are equivalent :
(i) $f(x)$ is regular;
(ii) a_i is a unit for some i, $0 \leq i \leq t$;
(iii) $f(x) + J(R)[x] \neq J(R)[x]$;
(iv) $\langle a_0, a_1, \cdots, a_t \rangle = R$.

Proof : We need only to show that $(i) \Leftrightarrow (ii)$ and the rest is clear. Let $f(x)$ be a regular polynomial in $R[x]$. Suppose on the contrary that for all i, $0 \leq i \leq t$, a_i are not units. As R is local ring, $f(x) \in J(R)[x]$. Let m be the index of nilpotency of $J(R)$. Let $g(x)$ be a non-zero polynomial over $(J(R))^{m-1}$.

Then $g(x)J(R) = 0$ and hence $g(x)f(x) = 0$ which implies that $f(x)$ is not a regular polynomial. This is a contradiction. Hence $f(x) \notin J(R)[x]$ and there exists i, $0 \leq i \leq t$ such that a_i is a unit in R. Conversely, let a_i be a unit in R, for some i, $0 \leq i \leq t$. Suppose that there exists a non-zero polynomial $g(x) \in R[x]$ such that $g(x)f(x) = 0$, then $\overline{f}(x)\overline{g}(x) = 0$. Since $\overline{f}(x) \neq 0$ and $\overline{R}[x]$ is an integral domain, $\overline{g}(x) = 0$. Therefore $g(x) \in J(R)[x]$. Let $j \in \{0, \cdots, t\}$ be the largest integer such that a_j is a unit in R. Then $a_j^{-1}f(x) = h(x) + u(x)$, where $h(x) \in J(R)[x]$ and $u(x) \in R[x]$ is a monic polynomial. Now

$$\begin{aligned} 0 &= g(x)f(x) \\ &= g(x)\left(h(x) + u(x)\right) \\ &= g(x)h(x) + g(x)u(x). \qquad \cdots(1) \end{aligned}$$

As $g(x) \in J(R)[x]$, there exists a non-negative integer l such that $\left(J(R)\right)^{l+1} g(x) = 0$ and $\left(J(R)\right)^{l} g(x) \neq 0$. Let $a\,(\neq 0) \in \left(J(R)\right)^{l}$ such that $ag(x) \neq 0$. Then $ag(x)h(x) = 0$ and $ag(x)f(x) = 0$. So (1) gives $0 = ag(x)u(x)$. As $u(x)$ is a monic polynomial and $ag(x) \neq 0$, $ag(x)u(x) \neq 0$. This is a contradiction. Hence $f(x)$ is a regular polynomial. ♣

Definition 2. Let R be a local ring and T a subring of R such that $\overline{R}$ is a field. Then
(i) $a \in R$ is called an *algebraic element* over T if it is satisfies a regular polynomial over T.
(ii) $a \in R$ is called a *transcendental element* over T if it is not algebraic element over T.

Lemma 3. *Let R be a local ring with $J(R)$ a nil ideal such that $\overline{R}$ is a field. Then $a \in R$ is a transcendental element over $P \subseteq R$ if and only if $\overline{a}$ is a transcendental element over $\overline{P} \subseteq \overline{R}$.*

Proof : Let $\overline{a}$ be a transcendental element over $\overline{P}$. Suppose on the contrary that a is an algebraic element over P. Then there exists a regular polynomial $f(x) \in P[x]$ such that $f(a) = 0$. Then

$$0 = \overline{f(a)} = \overline{f}(\overline{a}).$$

As $\overline{a}$ is a transcendental element over $\overline{P}$, we get $\overline{f}(x) = 0$; *i.e.*, $f(x) \in J(R)[x] \cap P[x] = J(P)[x]$. As $J(P)$ nilpotent, this contradicts Lemma 1. Thus a is a transcendental element over P. Conversely, let a be a transcendental element over P. Suppose that there is a regular polynomial $f(x) \in P[x]$ such that $\overline{f(a)} = 0$, so $f(a) \in J(R)$. For some positive integer l, $\left(f(a)\right)^{l} = 0$. As $f(x)$ is a regular polynomial, $\left(f(x)\right)^{l}$ is also a regular polynomial. Hence a is algebraic over P. This is a contradiction. Thus $\overline{a}$ is a transcendental element over $\overline{P}$. ♣

Proposition 4. *Let R be an artinian local ring such that $\overline{R}$ is a field. If $a \in R$ is an algebraic element over P, then there exists a monic polynomial $f(x) \in P[x]$ such that $f(a) = 0$.*

Proof : Let a be an algebraic element over P. Then there exists a regular polynomial $g(x) = \sum_{i=0}^{t} a_i x^i \in P[x]$, $a_t \neq 0$ such that $g(a) = 0$. Let $j \in \{0, \cdots, t\}$

be the largest integer such that a_j is a unit. Then

$$a_j^{-1}g(x) = h(x) + u(x),$$

where $h(x) \in J(P)[x]$ and $u(x)$ is a monic polynomial in $P[x]$. As

$$u(x) = a_j^{-1}g(x) - h(x),$$

$$\begin{aligned} u(a) &= a_j^{-1}g(a) - h(a) \\ &= h(a) \in J(R). \end{aligned}$$

So $(u(a))^l = 0$, for some positive integer l. As $u(x)$ is a monic polynomial, $(u(x))^l$ is a monic polynomial. Then $f(x) = (u(x))^l$ is a monic polynomial such that $f(a) = 0$. ♣

Suppose that R is a local ring such that for some $\theta \in R$, $\theta R = R\theta$ is a minimal ideal of R. Then $\theta^2 = 0$, otherwise $\theta R = \theta^2 R$ and hence $\theta = \theta^2 r$ for some $r \in R$ which implies that $\theta(1 - \theta r) = 0$, as $1 - \theta r$ is a unit, $\theta = 0$. So if $J(R) = qR + \theta R$, where q is nilpotent, then $J(R)$ is nilpotent.

Proposition 5. *Let R be a local ring such that for some $\theta \in R$, $\theta R = R\theta$ is a minimal ideal of R, $R/\theta R$ a field or a commutative ring of characteristic p^n and $J(R) = pR + \theta R$. Also suppose $a \in R$ is a lift algebraic element over P such that*

$$ah = ha,$$

for some $h(\neq 0) \in \theta R$. Then $a \in C(R)$.

Proof : Suppose $\theta R = \theta J(R)$. Then $\theta = \theta h$, $h \in J(R)$, $\theta(1 - h) = 0$, which implies that $\theta = 0$. Hence $\theta R \neq \theta J(R)$. But θR is a minimal ideal, so $\theta J(R) = 0$. Similarly $J(R)\theta = 0$. So θR is an $R/\theta R - module$. For the given a, there exists $a' \in R$ such that $a\theta = \theta a'$. For any $c \in R$, let $\overline{c} = c + \theta R$. As $ah = ha$ for some $h = \theta r \in \theta R$, r a unit,

$$a\theta r = \theta ra = \theta\overline{ra} = \theta\overline{ar} = \theta ar.$$

Hence

$$a\theta = \theta a.$$

Case I : $R/\theta R$ is a field. So $J(R) = \theta R$. Let $h' = \theta t \in J(R)$. Then

$$ah' = a\theta t = \theta at = \theta\overline{at} = \theta\overline{ta} = \theta ta = h'a.$$

So for any $h' \in J(R)$, $ah' = h'a$.
Case II : $R/\theta R$ is a commutative ring of characteristic p^n with $J(R) = pR + \theta R$.

As $p \in J(R)$, pR is an $R/\theta R - module$. Thus for any $h_0 = pt_1 + \theta t_2 \in J(R)$,

$$\begin{aligned} ah_0 &= pat_1 + a\theta t_2 \\ &= pat_1 + \theta at_2 \\ &= p\overline{at_1} + \theta\overline{at_2} \\ &= p\overline{t_1 a} + \theta\overline{t_2 a} \\ &= pt_1 a + \theta t_2 a \\ &= (pt_1 + \theta t_2)a \\ &= h_0 a. \end{aligned}$$

Hence $ah_0 = h_0 a$ for all $h_0 \in J(R)$. So in the two cases $a \in Z_R(J(R))$. Let b be a unit in R. Then by the commutativity of $R/\theta R$, we have $\overline{ab} = \overline{ba}$, hence $\overline{bab^{-1}} = \overline{a}$ and subsequently $bab^{-1} - a \in \theta R$. Let $bab^{-1} - a = \theta t$. Then

$$\begin{aligned} a(bab^{-1}) &= a(a + \theta t) \\ &= a^2 + a\theta t \\ &= a^2 + (\theta t)a \\ &= (a + \theta t)a \\ &= (bab^{-1})a. \end{aligned}$$

Since $T/(J(R) \cap T) \cong (T + J(R))/J(R) = \overline{P}[\overline{a}]$ a field, by (2.5), $T = P[a, bab^{-1}]$ is a commutative local ring with $J(T) = T \cap J(R)$ a nilpotent ideal. Let $g(x)$ be a minimal polynomial of a over P. Then

$$g(bab^{-1}) = bg(a)b^{-1} = 0.$$

But T is a Hensel ring, so (2.4) implies that $\overline{a}$ has unique lift algebraic element a in T over P such that $g(a) = 0$. Thus $bab^{-1} = a$ and hence $a \in C(R)$. ♣

Proposition 6. *Let R be a local ring such that for some $\theta \in R$, $\theta R = R\theta$ is a minimal ideal of R, $R/\theta R$ a field or a commutative ring of characteristic p^n and $J(R) = pR + \theta R$. Also suppose that $a \in R$ is a lift algebraic element over P and $b \in R$. Then there exists $h \in \theta R$ such that*

$$a(b + h) = (b + h)a.$$

Proof : For the given a, there exists $a' \in R$ such that $a\theta = \theta a'$. For any $c \in R$, let $\overline{c} = c + \theta R$. As θR is a minimal ideal, θR is an $R/\theta R - module$. So for any $c \in R$, $\theta c = \theta\overline{c}$. We want to show that there exists $h = \theta t \in \theta R$ such that

$$a(b + h) = (b + h)a.$$

Suppose there is an $h \in R$ such that $a(b+h) = (b+h)a$. Then

$$\begin{aligned} ab - ba &= ha - ah \\ &= \theta ta - a\theta t \\ &= \theta ta - \theta a' t \\ &= \theta\overline{ta} - \theta\overline{a't} \\ &= \theta\overline{ta} - \theta\overline{ta'} \\ &= \theta ta - \theta ta' \\ &= \theta t(a - a') \\ &= h(a - a'). \end{aligned}$$

Case I : $(a - a')$ is a unit. Since $\overline{ab} = \overline{ba}$, $ab - ba \in \theta R$ and hence $h = (ab - ba)(a - a')^{-1} \in \theta R$. Thus such an h exists.
Case II : $(a - a') \in J(R)$. As θR is a minimal ideal, $\theta J(R) = J(R)\theta = 0$, so $\theta(a - a') = 0$. Thus

$$\theta a = \theta a' = a\theta.$$

By Proposition 5, $a \in C(R)$ and we can choose h to be any element in θR. ♣

Proposition 7. *Let R be a local ring such that for some $\theta \in R$, $\theta R = R\theta$ is a minimal ideal of R, $R/\theta R$ a field or a commutative ring of characteristic p^n and $J(R) = pR + \theta R$. Also suppose that $a \in R$ is a lift algebraic element over P and $\overline{b}$ is an algebraic element over $\overline{P}$. Then there exists $c \in \overline{b}$ a lift algebraic element over P such that*

$$ac = ca,$$

(i) if char $R = 0$, then $T = P[a, c]$ is a subfield,
(ii) if char $R = p^n$, then $T = P[a, c]$ is a Galois subring.

Proof : (i) Let *char* $R = 0$. Then $P \cong \mathbb{Q} \cong \overline{P}$. Let $a \in R$ be a lift algebraic element over P. Then by $(2.16)\,(i)$, $P[a]$ is a subfield of R. Suppose that $\overline{b}$ is an algebraic element over $\overline{P}$. By Proposition 6, there exists $h \in \theta R$ such that

$$a(b+h) = (b+h)a.$$

Let $b_0 = b+h$. Then $T = P[a, b_0]$ is a commutative subring of R with $T/(T \cap J(R)) \cong \overline{P}[\overline{a}, \overline{b_0}]$ a subfield of $\overline{R}$, hence by (2.5), T is a local subring with $J(T) = T \cap J(R)$ nilpotent. Let $f(x) \in P[a][x]$ be a partially irreducible polynomial over $P[a]$ such that $\overline{f}(\overline{b_0}) = 0$. Then $f(b_0) \in J(R) \cap T = J(T)$. So $f(b_0) + J(T) = J(T)$. By (2.9), $\overline{b}$ has a unique lift algebraic element $b' \in T$ over the field $P[a]$ such that $f(b') = 0$. Thus by $(2.17)\,(i)$, $P[a, b']$ is a field.
(ii) Let *char* $R = p^n$. Then $P \cong \mathbb{Z}_{p^n}$, $\overline{P} \cong \mathbb{Z}_p$. Let $a \in R$ be a lift algebraic element over P. Then by $(2.16)\,(ii)$, $P[a]$ is a Galois subring of R. Suppose that $\overline{b}$ is an algebraic element over $\overline{P}$. By Proposition 6, there exists $h \in \theta R$ such that

$$a(b+h) = (b+h)a.$$

Let $b_0 = b+h$. Then $T' = P[a, b_0]$ is a commutative subring with $T'/(T' \cap J(R)) \cong P[\overline{a}, \overline{b_0}]$ a subfield of $\overline{R}$, hence by (2.5), T' is a local ring with $J(T') = T' \cap J(R)$

nilpotent. Let $g(x) \in P[x]$ be a partially irreducible polynomial over P such that $\overline{g}(\overline{b_0}) = 0$. Then $g(b_0) \in J(R) \cap T' = J(T')$. So $g(b_0) + J(T') = J(T')$. By (2.4), $\overline{b}$ has a unique lift algebraic element $b' \in T'$ over P such that $g(b') = 0$. By $(2.17)\,(ii)$, $P[a, b']$ is a Galois subring of R. ♣

Definition 8. A subring [subfield] T of a ring R is called a *coefficient subring* [*subfield*] if $\overline{T} = (T + J(R))/J(R) = \overline{R}$; *i.e.*, $R = T + J(R)$ and $J(T) = T \cap J(R) = qT$, where $q = char\ \overline{R}$.

Definition 9. Let R be a local ring with $J(R)$ a nil ideal. Then R is called *an absolutely algebraic ring* if every element in R is algebraic over the prime subring P of R.

Remark 1. Let R be a local ring with $J(R)$ a nil ideal such that $\overline{R}$ is a field. Let K be the set of all algebraic elements in R over P. By Lemma 3, it is clear that $a - b, ab \in K$ for any algebraic elements $a, b \in R$ over P. Hence K is an absolutely algebraic ring. As $J(R)$ is a nil ideal, $J(R) \subseteq K$. Since $\overline{K} = K/J(R)$ is an absolutely algebraic subfield of $\overline{R}$. Then by (2.5), K is a local ring with $J(K) = J(R)$ a nil ideal.

Proposition 10. *Let R be a local duo ring such that char $R = 0$, $d(R) = 2$ and $\overline{R}$ is a field. Let K be the subring of all algebraic elements in R over P. Then K has a coefficient subfield.*

Proof : By Remark 1, $\overline{K}$ is an absolutely algebraic subfield of $\overline{R}$,

$$\overline{K} = \bigcup_{i=1}^{\infty} \overline{P}[\overline{a_i}]$$

a union of ascending chain of simple field extensions of $\overline{P}$, where $\overline{a_i}$ is algebraic element over $\overline{P}$ for each i. By (2.1), there exists a lift algebraic element $c_i \in \overline{a_i}$ in R over P. As K is the set of all algebraic elements in R over P, $c_i \in K$. From Remark 1 and $(2.16)\,(i)$, we get $P[c_i]$ is a subfield of K. Since R is a local ring and $d(R) = 2$, there exists an element $\theta \in R$ such that $J(R) = \theta R = R\theta$ is a minimal ideal. Suppose for some n, we have chosen $b_1, b_2, \cdots, b_n$ in K such that $\overline{b_i} = \overline{a_i}$ for each i, $1 \leq i \leq n$, where each b_i is algebraic over P and $P[b_i] \subseteq P[b_{i+1}]$. By Proposition 7$(i)$, there exists a lift algebraic element $b_{n+1} \in \overline{a_{n+1}}$ in R over P such that

$$b_n b_{n+1} = b_{n+1} b_n$$

and $P[b_{n+1}]$ is a subfield of R. As $b_{n+1} \in K$, $P[b_{n+1}] \subseteq K$. Since

$$\overline{P}[\overline{b_n}] = \overline{P}[\overline{a_n}] \subseteq \overline{P}[\overline{a_{n+1}}] = \overline{P}[\overline{b_{n+1}}],$$

by $(2.15)\,(iii)$,

$$P[b_n] \subseteq P[b_{n+1}].$$

This gives an ascending sequence $\{P[b_n]\}_{n=1}^{\infty}$ of subfields of K such that $\overline{P}[\overline{b_n}] = \overline{P}[\overline{a_n}]$. Then $K_0 = \bigcup_{n=1}^{\infty} P[b_n]$ is a union of an ascending chain of subfields of K. So K_0 is a subfield of K. From Remark 1, $J(K) = J(R)$ and hence

$$\overline{K_0} = (K_0 + J(K))/J(K) = \bigcup_{n=1}^{\infty} \overline{P}[\overline{a_n}] = \overline{K},$$

$$K = K_0 + J(K).$$

Thus K_0 is a coefficient subfield of K. ♣

Proposition 11. *Let R be a local duo ring such that char $R = p^n$, $d(R) = 2$ and $\overline{R}$ a field. Let K be the subring of all algebraic elements in R over P. Then K has a coefficient subring.*

Proof : By Remark 1, $\overline{K}$ is an absolutely algebraic subfield of $\overline{R}$,

$$\overline{K} = \bigcup_{i=1}^{\infty} \overline{P}[\overline{a_i}]$$

a union of ascending chain of simple field extensions of $\overline{P}$, where $\overline{a_i}$ is algebraic element over $\overline{P}$ for each i. By (2.1), there exists a lift algebraic element $c_i \in \overline{a_i}$ in R over P. As K is the set of all algebraic elements in R over P, $c_i \in K$. From Remark 1 and (2.16) (ii), we get $P[c_i]$ is a Galois subring of K. Since R is a local ring and $d(R) = 2$, there exists an element $\theta \in R$ such that $J(R) = \theta R = R\theta$ is a minimal ideal. Suppose for some n, we have found lift algebraic elements $b_1, b_2, \cdots, b_n$ in K over P such that $\overline{b_i} = \overline{a_i}$ for each i, $1 \leq i \leq n$, and $P[b_i] \subseteq P[b_{i+1}]$. By Proposition 7$(ii)$, there exists a lift algebraic element $b_{n+1} \in \overline{a_{n+1}}$ in R over P such that

$$b_n b_{n+1} = b_{n+1} b_n$$

and $P[b_{n+1}]$ is a Galois subring of R. As $b_{n+1} \in K$, $P[b_{n+1}] \subseteq K$. Since

$$\overline{P}[\overline{b_n}] = \overline{P}[\overline{a_n}] \subseteq \overline{P}[\overline{a_{n+1}}] = \overline{P}[\overline{b_{n+1}}],$$

by (2.15) (iii),

$$P[b_n] \subseteq P[b_{n+1}].$$

This gives an ascending sequence $\{P[b_n]\}_{n=1}^{\infty}$ of Galois subrings of K such that $\overline{P}[\overline{b_n}] = \overline{P}[\overline{a_n}]$. Then $K_0 = \bigcup_{n=1}^{\infty} P[b_n]$ is a union of an ascending chain of Galois subrings of K. So K_0 is a generalized Galois ring. By Remark 1, $J(K) = J(R)$ and hence

$$\overline{K_0} = (K_0 + J(K))/J(K) = \bigcup_{n=1}^{\infty} \overline{P}[\overline{a_n}] = \overline{K},$$

so

$$K = K_0 + J(K).$$

As K_0 is a generalized Galois ring,

$$J(K_0) = pK_0 = K_0 \cap J(K).$$

Thus K_0 is a coefficient subring of K. ♣

Theorem 12. *Let R be an arinian local duo ring such that char $R = 0$ and $\overline{R}$ is an absolutely algebraic field. Then R has a coefficient subfield.*

Proof : Since $\overline{R}$ is an absolutely algebraic field, by Lemma 3, R is an absolutely algebraic ring. We will prove the result by induction on $d(R)$. Let $d(R) = 2$. Then by Proposition 10, R has a coefficient subfield. Let $d(R) = m$,

$m \geq 3$ and suppose that R has a coefficient subfield for $d(R) \leq m-1$. Let N be a minimal right ideal of R. So $N = \theta R$ for some $\theta \in J(R)$. Also R is a duo ring, $N = \theta R = R\theta$. Let $R' = R/N$. Then $d(R') = m-1$. Since R' is a homomorphic image of R, R' is an artinian local duo ring and hence R' has a coefficient subfield $L = T/N$, where T a subring of R containing N.

$$\begin{aligned} R/N &= T/N + J(R/N), \\ &= T/N + J(R)/N. \end{aligned}$$

So

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

$$\theta R = \theta[T + J(R)] = \theta T,$$

$$R\theta = [T + J(R)]\theta = T\theta.$$

Thus θ generates N as an $R-$*module* if and only if θ generates N as a $T-$*module*. This shows that $\theta T = T\theta$ is a minimal two-sided ideal of T. Since L is a field, $J(T) = \theta T = T\theta$ and hence T is an artinian local duo ring with $d(T) = 2$ and *char* $T = 0$. By Proposition 10, T has a coefficient subfield H. Then

$$\begin{aligned} T &= H + J(T) \\ &= H + \theta T \\ &= H + \theta R, \end{aligned}$$

$$\begin{aligned} R &= T + J(R) \\ &= H + \theta R + J(R) \\ &= H + J(R). \end{aligned}$$

Since $H \cap J(R) = 0$, H is a coefficient subfield of R. ♣

Theorem 13. *Let R be an arinian local duo ring such that char $R = p^n$ and $\overline{R}$ is an absolutely algebraic field. Then R has a coefficient subring.*

Proof : Since $\overline{R}$ is an absolutely algebraic field, by Lemma 3, R is an absolutely algebraic ring. We will prove the result by induction on $d(R)$. Let $d(R) = 2$. Then by Proposition 12, R has a coefficient subring. Let $d(R) = m$, $m \geq 3$ and suppose that the result holds for artinian local duo rings with $d(R) \leq m-1$. Let $N = \theta R$ be a minimal right ideal of R. As R is a duo ring, N is an ideal. Consider $R' = R/N$, then R' is an artinian local duo ring. By the induction hypothesis, R' has a coefficient subring A. Now $A = T/N$, $J(A) = pA$, where T is a subring of R containing N. Since *char* $T = p^n$, $P \cong \mathbb{Z}_{p^n}$ and $\overline{P} \cong \mathbb{Z}_p$. Then

$$R' = A + J(R'),$$

$$R/N = T/N + J(R)/N,$$

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

This gives

$$\theta R = \theta[T + J(R)] = \theta T,$$
$$R\theta = [T + J(R)]\theta = T\theta.$$

So θT is an ideal of T and it is minimal as a right ideal and as a left ideal. Now

$$T/(T \cap J(R)) \cong (T + J(R))/J(R) = \overline{R}$$

is a field. By (2.5), T is a local ring with $J(T) = T \cap J(R)$ a nilpotent ideal. Consider $\overline{a} \in \overline{R}\backslash\overline{P}$ and $f(x) \in P[x]$ be a partially irreducible polynomial such that $\overline{f}(\overline{a}) = 0$. Since $\overline{R} = (T + J(R))/J(R)$, there exists an element $h \in J(R)$ such that $a+h \in T$ and $f(a+h) \in T \cap J(R) = J(T)$. So $f(a+h)+J(T) = J(T)$. By (2.1), we can find a lift algebraic element $a' \in a+h+J(T)$ in T over P with $\overline{a'} = \overline{a}$. By (2.16 (ii)), $P[a']$ is a Galois subring of T. If there is $\overline{b} \in \overline{R}\backslash\overline{P}[\overline{a}]$, then as we have done above, we can find an $h' \in J(R)$ such that $b_1 = b+h' \in T$. Now $J(T/N) = p(T/N)$, gives $J(T) = pT + N = pT + \theta T$. By Proposition 7$(ii)$, we can find $c \in b_1 + J(T)$ lift algebraic element over P such that $ac = ca$ and $P[a, c]$ is a Galois subring of T. Clearly $\overline{c} = \overline{b}$ and $P[a] \subseteq P[a, c]$. As

$$\overline{T} \cong \overline{R},$$

$\overline{T}$ is an absolutely algebraic field and hence $\overline{T} = \bigcup_{i=1}^{\infty} \overline{P_T}[a_i + J(T)]$, where $\overline{P_T} = (P + J(T))/J(T)$. Suppose that for some n, $1 \leq n < \infty$, we have found a Galois subring $T_n = P[b_n]$ of T, where b_n a lift algebraic element over P such that

$$\overline{P_T}[a_n + J(T)] = \overline{T_n} = (T_n + J(T))/J(T).$$

Since

$$\overline{P_T}[a_n + J(T)] \subseteq \overline{P_T}[a_{n+1} + J(T)].$$

By the result given above we can find an element c_{n+1} in T such that $P[b_n, c_{n+1}]$ is a Galois subring of T with $c_{n+1} + J(T) = a_{n+1} + J(T)$. So $P[b_n, c_{n+1}] = P[b_{n+1}]$ for some lift algebraic element $b_{n+1} \in T$ over P. Put $T_{n+1} = P[b_{n+1}]$. Then

$$\overline{P_T}[a_{n+1} + J(T)] = \overline{T_{n+1}}$$

and $T_n \subseteq T_{n+1}$. Hence by induction, we get ascending chain $\{T_n\}_{n=1}^{\infty}$ of Galois subrings of T such that

$$\overline{T_n} = \overline{P_T}[a_n + J(T)]$$

for every n. Consequently

$$\overline{T} = \bigcup_{n=1}^{\infty} \overline{T_n}.$$

Let $T_0 = \bigcup_{n=1}^{\infty} T_n$. Then T_0 is a generalized Galois subring of T and $T = T_0 + J(T)$. Therefore

$$\begin{aligned} R &= T + J(R) \\ &= T_0 + J(T) + J(R) \\ &= T_0 + J(R), \end{aligned}$$

and $J(T_0) = pT_0 = T_0 \cap J(R)$. Thus T_0 is a coefficient subring of R. ♣

The following Theorem is a generalization of Lemma 3, in [7].

Theorem 14. *Let R be a local ring with char $R = p^n$. Then R is a generalized Galois ring if and only if $J(R) = pR$ and $\overline{R}$ is an absolutely algebraic field.*

Proof : Let R be a local ring with $J(R) = pR$ and $\overline{R}$ an absolutely algebraic field. Then $J(R)$ is a nilpotent ideal and R has a finite composition length and all its one sided ideals are of the form p^iR, $0 \leq i \leq n$. Hence R is an artinian duo ring. By Theorem 13, R has a generalized Galois subring R_0 as its coefficient subring. Then $R = R_0 + J(R) = R_0 + pR = R_0$, as p is a nilpotent element in R_0. Thus R is a generalized Galois ring. The converse is trivial. ♣

Remark 2. Let R be an artinian local duo ring such that *char* $R = 0$ and $\overline{R}$ is an absolutely algebraic field. Then $\overline{R} = \overset{\infty}{\underset{i=1}{\cup}} \overline{P}[\overline{a_i}]$ for some $\overline{a_i}$ algebraic elements in $\overline{R}$ over $\overline{P}$. By Theorem 12, R has a coefficient subfield H of the form $\overset{\infty}{\underset{i=1}{\cup}} P[a_i']$, where $a_i' \in \overline{a_i}$ is a lift algebraic element over P. So

$$H = \overset{\infty}{\underset{i=1}{\cup}} P[a_i'] \cong \overset{\infty}{\underset{i=1}{\cup}} \overline{P}[\overline{a_i}] = \overline{R}.$$

Suppose that T is another coefficient subfield of R. Then $R = T + J(R)$, $T \cap J(R) = \{0\}$ and

$$T \cong \overline{R} \cong H.$$

Thus the coefficient subfields of R are isomorphic.

In the following theorem we prove that the above statement is also true if *char* $R = p^n$.

Theorem 15. *Let R be an arinian local duo ring with char $R = p^n$ and $\overline{R}$ an absolutely algebraic field. Then any coefficient subring of R is a generalized Galois ring. Moreover any two coefficient subrings of R are isomorphic.*

Proof : By Theorem 13, R has a coefficient subring R_0 which is a generalized Galois subring of R. Let T be another coefficient subring of R. Then $R = T + J(R)$, $J(T) = J(R) \cap T = pT$. By (2.5), T is a local ring, and by Theorem 14, T is a generalized Galois ring. As

$$\overline{R_0} \cong \overline{R} \cong \overline{T},$$

by (2.25), $R_0 \cong T$. ♣

3.2 Transcendental extensions

Proposition 16. *Let (R, π) be a special primary ring. Then*
(i) $\pi R[x]$ is a prime ideal.
(ii) $f(x) \in R[x]$ is regular if and only if $f(x) \in R[x] \backslash \pi R[x]$.
(iii) The ring of quotients of $R[x]$ with respect to $P' = \pi R[x]$ is $L = R[x]_{P'} = R[x]_S$ with $J(L) = \pi L$, where $S = R[x] \backslash \pi R[x]$. In fact L is the total quotient ring of $R[x]$.

Proof : (i) As $R[x]/\pi R[x] \cong \overline{R}[x]$ is an integral domain, $\pi R[x]$ is a prime ideal.
(ii) Follows from Lemma 1.
(iii) Let $S = R[x]\backslash\pi R[x]$. Then S is the set of all regular elements of $R[x]$. So S is a multiplicative subset of R. By the definition of the ring of qoutients $R[x]_S$ of $R[x]$ with respect to S, $L = R[x]_S$. But $S = R[x]\backslash P'$. So by definition of $R[x]_{P'}$,

$$R[x]_{P'} = R[x]_S = L$$

is a local ring with

$$J\left(R[x]_{P'}\right) = P'R[x]_{P'} = \pi R[x]R[x]_{P'} = \pi L. \quad \clubsuit$$

Proposition 17. *Let R be a local ring such that for some $\theta \in R$, $\theta R = R\theta$ is a minimal ideal of R, $R/\theta R$ a field or a commutative ring of characteristic p^n and $J(R) = pR + \theta R$. Also, let $K_0 = \overset{\infty}{\underset{i=1}{\cup}} P[a_i]$ be a subfield or a generalized Galois subring of R according as char $\overline{R} = 0$ or char $\overline{R} = p$, a prime number, and let $b \in R$. Then there exists $h \in \theta R$ such that $K_0[b+h]$ is a commutative subring of R.*

Proof : By Proposition 6, for each a_i there exists an element $h_i \in \theta R$ such that

$$a_i(b + h_i) = (b + h_i)a_i$$

If $a_i \in C(R)$ for all i, $1 \leq i < \infty$, then we can take $h = 0$, so $K_0[b]$ is a commutative subring of R. Suppose that $K_0 \nsubseteq C(R)$. Then there exists smallest positive integer j such that $a_j \notin C\left(R\right)$. Consider a_i, $i \geq j$. Suppose that $h_i \neq h_j$. Then $a_j \in P[a_i]$ implies that

$$a_j\left(b + h_i\right) = (b + h_i)a_j$$

and

$$a_j(b + h_j) = (b + h_j)a_j.$$

Let $h' = h_j - h_i$. Then

$$\begin{aligned}(b + h_i)a_j + h'a_j &= (b + h_i + h')a_j \\ &= (b + h_j)a_j \\ &= a_j(b + h_j) \\ &= a_j(b + h_i + h') \\ &= (b + h_i)a_j + a_jh'.\end{aligned}$$

So $h'a_j = a_jh'$. Since $h' \neq 0, h' = \theta r$, where r is a unit in R. By Proposition 5, $a_j \in C(R)$. This is a contradiction. Thus $h_j = h_i$ for all $i \geq j$. So we can find $h = h_j \in \theta R$ such that

$$a_i(b + h) = (b + h)a_i$$

for all i, $1 \leq i < \infty$. Hence $K_0[b+h]$ is a commutative subring of R. ♣

Theorem 18. *Let R be a local duo ring with char $R = 0$, $d(R) = 2$ and $\overline{R}$ a simple transcendental extension of an absolutely algebraic field. Then R has a coefficient subfield .*

Proof : Let K be the subring of all algebraic elements in R over P. By Proposition 10, we can find a subfield $H = \bigcup_{i=1}^{\infty} P[a_i]$ of K with each a_i an algebraic element over $P = \mathbb{Q}$ such that

$$K = H + J(R).$$

Suppose that $\overline{R} = \overline{K}(\overline{\alpha})$, for some element $\alpha \in R$ transcendental over P. Then by Lemma 17, there exists $h \in J(R)$ such that $H[\alpha + h]$ is a commutative subring of R. As α is transcendental over H, $\alpha + h$ is also transcendental over H. Then $H[\alpha + h] \cong H[x]$, where x is an indeterminate. So $H[\alpha + h]$ is an integral domain. Since R is a local ring, R contains the inverses of all non-zero elements in $H[\alpha + h]$. So R contains the quotient field $H(\alpha + h)$ of $H[\alpha + h]$. Now

$$\left(H(\alpha + h) + J(R)\right)/J(R)$$

contains $\overline{K}$ and $\overline{\alpha}$. Hence

$$\begin{aligned} \overline{R} &= \left(H(\alpha + h) + J(R)\right)/J(R), \\ R &= H(\alpha + h) + J(R) \end{aligned}$$

Thus $H(\alpha + h)$ is a coefficient subfield of R.

Theorem 19. *Let R be an artinian local duo ring with char $R = 0$ and $\overline{R}$ a simple transcendental extension of an absolutely algebraic field. Then R has a coefficient subfield .*

Proof : We will prove the result by induction on $d(R)$. Let $d(R) = 2$. Then by Theorem 18, R has a coefficient subfield. Suppose that for $d(R) \leq m - 1$, $m \geq 3$, R has a coefficient subfield. Let $d(R) = m$, $R' = R/\theta R$, where θR is a minimal right ideal of R. Hence $\theta R = R\theta$, θR is an ideal of R. Let K be the subring of all algebraic elements in R over P and suppose that $\overline{R} = \overline{K}(\overline{\alpha})$, for some transcendental element α in R over P. As R is an artinian local duo ring, R' is an artinian local duo ring with $d(R') = m - 1$. So R' has a coefficient subfield, say $T/\theta R$, where T is a subring of R containing some $\alpha' \in \overline{\alpha}$. Since $T/\theta R$ is a field, $J(T) = \theta R$ and hence

$$\begin{aligned} R/\theta R &= T/\theta R + J\left(R/\theta R\right) \\ &= T/\theta R + J(R)/\theta R. \end{aligned}$$

So

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

As θR is a minimal ideal of R, $\theta J(R) = J(R)\theta = 0$. Thus

$$\theta R = \theta[T + J(R)] = \theta T,$$

and

$$R\theta = [T + J(R)]\theta = T\theta.$$

Therefore $\theta T = T\theta$ is a minimal ideal of T and hence T is an artinian local duo ring such that $J^2(T) = (\theta T)^2 = 0$. So $d(T) = 2$. By Proposition 18, T has a coefficient subfield, say F. Now

$$T = F + J(T),$$

$$\begin{aligned} R &= T + J(R) \\ &= F + J(T) + J(R) \\ &= F + J(R). \end{aligned}$$

Hence F is a coefficient subfield of R. ♣

Proposition 20. *Let R be a local duo ring with char $R = p^n$, $d(R) = 2$ and $\overline{R}$ a simple transcendental extension of an absolutely algebraic field. Then R has a coefficient subring.*

Proof : Let K be the subring of all algebraic elements in R over P. By Proposition 11, we can find a generalized Galois ring $K_0 = \overset{\infty}{\underset{i=1}{\cup}} P[a_i]$ such that

$$K = K_0 + J(R).$$

Suppose that $\overline{R} = \overline{K}(\overline{\alpha})$, for some transcendental element α in R over P. By Proposition 7, there exists an element $h \in J(R)$ such that $K_0[\alpha + h]$ is a commutative subring of R. As α is a transcendental element over K_0, $\alpha + h$ is also transcendental element over K_0 and hence

$$K_0[\alpha + h] \cong K_0[x]$$

where x is an indeterminate. Now K_0 is a special primary ring. Since R is an artinian local ring, by (1.3) and (1.16), the non-zero divisor elements in $K_0[\alpha+h]$ are units in R. So by Proposition 16, R contains the ring of quotients of $K_0[\alpha+h]$ with respect to $pK_0[\alpha+h]$; *i.e.*, the total qoutient ring of $K_0[\alpha+h]$, say

$$R_0 = K_0[\alpha + h]_{\mathcal{P}},$$

where $\mathcal{P} = pK_0[\alpha + h]$. Now

$$\begin{aligned} J(R_0) &= R_0 \cap J(R) \\ &= pR_0 \end{aligned}$$

and $(R_0 + J(R))/J(R)$ contains $\overline{K}$ and $\overline{\alpha}$. Therefore

$$\begin{aligned} (R_0 + J(R))/J(R) &= \overline{K}(\overline{\alpha}) \\ &= \overline{R}, \end{aligned}$$

$$R = R_0 + J(R).$$

Thus R_0 is a coefficient subring of R. ♣

Theorem 21. *Let R be an artinian local duo ring with char $R = p^n$ and $\overline{R}$ a simple transcendental extension of an absolutely algebraic field. Then R has a coefficient subring.*

Proof : We will prove the result by induction on $d(R)$. Let $d(R) = 2$. Then by Proposition 20, R has a coefficient subring. Suppose that for $d(R) = m-1$, $m \geq 3$, R has a coefficient subring. Let $d(R) = m$. Let $R' = R/N$, where N is a minimal right ideal of R. Then $N = \theta R$ for some $\theta \in R$. As R is a duo ring, $N = R\theta = \theta R$. Let K be the subring of all algebraic elements in R over P and suppose that $\overline{R} = \overline{K}(\overline{\alpha})$, for some transcendental element $\alpha \in R$. Now R' is an artinian local duo ring with *char* $R' = p^{n'}$, where $n' \leq n$ and $d(R') = m-1$. Hence R' has a coefficient subring, say T/N, where T is a subring of R containing some $\alpha' \in \overline{\alpha}$. Therefore

$$\begin{aligned} R/N &= T/N + J(R/N) \\ &= T/N + J(R)/N, \end{aligned}$$

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

As

$$J(T/N) = p(T/N),$$

$$\begin{aligned} J(T) &= pT + N \\ &= pT + R\theta \end{aligned}$$

Since $R\theta$ is a minimal ideal, $\theta J(R) = J(R)\theta = 0$,

$$\theta R = \theta[T + J(R)] = \theta T$$

$$R\theta = [T + J(R)]\theta = T\theta.$$

So $\theta T = T\theta$ is a minimal ideal of T,

$$\overline{T} = T/\left(T \cap J(R)\right) \cong \left(T + J(R)\right)/J(R) = \overline{R}$$

is a field. Thus T is a local ring with $J(T) = T \cap J(R)$ a nilpotent ideal. Let $\overline{P} = \left(P + J(T)\right)/J(T)$ and consider an element $a + J(T) \in \overline{T} \backslash \overline{P}$ algebraic over $\overline{P}$. Then by (2.1), there exists a lift algebraic element $a' \in a + J(T)$ in T over P. By (2.16) (ii), $P[a']$ is a Galois subring of R. If $b + J(T) \in \overline{T} \backslash \overline{P}[a + J(T)]$ is an algebraic element over $\overline{P}$, then by Proposition 7(ii), there exist an element $b' \in b + J(T)$ in T such that $L = P[a', b']$ is a Galois subring of T. By Remark 1, $J(K) = J(R)$,

$$\begin{aligned} \overline{T} &\cong \overline{R} \\ &= \overline{K}\left(\overline{\alpha}\right). \end{aligned}$$

Since α is a transcendental element over P and T is a local ring with $J(T)$ a nilpotent ideal, by Lemma 3, $\alpha + J(T)$ is a transcendental element over $\overline{P}$. As $\overline{K}$ is an absolutely algebraic field,

$$\overline{T} = \left(\overset{\infty}{\underset{i=1}{\cup}} \overline{P}[a_i + J(T)]\right)(\alpha' + J(T)),$$

for each $i, a_i + J(T)$ is an algebraic element over $\overline{P}$. Now $P[a_1]$ contains a lift algebraic element b_1 such that $\overline{b_1} = \overline{a_1}$. Suppose for some n, $1 \leq n < \infty$, we found a lift algebraic elements $b_1, \cdots, b_n$, $b_i \in \overline{a_i}$ such that $P[b_i] \subseteq P[b_{i+1}]$ for $1 \leq i \leq n-1$. Put $T_n = P[b_n]$. Then

$$\overline{P}[a_n + J(T)] = \overline{T_n} = (T_n + J(T))/J(T).$$

Since

$$\overline{P}[a_n + J(T)] \subseteq \overline{P}[a_{n+1} + J(T)],$$

then as seen above there exists $c_{n+1} \in T$ such that $P[b_n, c_{n+1}]$ is a Galois subring of T, $c_{n+1} + J(T) = a_{n+1} + J(T)$. So $P[b_n, c_{n+1}] = P[b_{n+1}]$ for some lift algebraic element $b_{n+1} \in T$ over P. Put $T_{n+1} = P[b_{n+1}]$. Then

$$\overline{P}[a_{n+1} + J(T)] = \overline{T_{n+1}},$$

and $T_n \subseteq T_{n+1}$. Hence by induction, we get ascending chain $\{T_n\}_{n=1}^{\infty}$ of Galois subrings of T such that

$$\overline{T_n} = \overline{P}[a_n + J(T)],$$

for every n. Let $T_0 = \bigcup_{n=1}^{\infty} T_n$. Then T_0 is a generalized Galois subring of T. By Proposition 17, there exists $h \in \theta T$ such that $T_0[\alpha' + h]$ is a commutative subring of T. Then $T_0[\alpha' + h] \cong T_0[x]$, where x is an indeterminate. As T is a local ring with $J(T) = T \cap J(R)$ nilpotent, every non-zero divisor element is a unit in T. Thus T contains the ring of quotients R_0 of $T_0[\alpha' + h]$ with respect to $\mathcal{P} = pT_0[\alpha' + h]$; *i.e.*, the total qoutients ring of $T_0[\alpha' + h]$. Now

$$R_0 = T_0[\alpha' + h]_{\mathcal{P}},$$

$$\begin{aligned} J(R_0) &= pR_0 \\ &= R_0 \cap J(T). \end{aligned}$$

As $\alpha' + J(T)$ and $(T_0 + J(T))/J(T)$ are in $(R_0 + J(T))/J(T)$,

$$(R_0 + J(T))/J(T) = \overline{T},$$

$$T = R_0 + J(T).$$

Now

$$\begin{aligned} R &= T + J(R) \\ &= R_0 + J(T) + J(R) \\ &= R_0 + J(R), \end{aligned}$$

$$\begin{aligned} J(R_0) &= pR_0 \\ &= R_0 \cap J(T) \\ &= R_0 \cap T \cap J(R) \\ &= R_0 \cap J(R). \end{aligned}$$

Thus R_0 is a coefficient subring of R. ♣

Definition 22. Let R be a commutative local ring and K a generalized Galois subring of R with *char* $K = p^n$. Then R is called *a simple transcendental extension of* K if R is the ring of qoutients $K[\alpha]_{\mathcal{P}}$, where α is transcendental element over K and $\mathcal{P} = pK[\alpha]$.

Theorem 23. *Let R be a local ring with char $R = p^n$. Then R is a simple transcendental extension of a generalized Galois ring if and only if $J(R) = pR$ and $\overline{R}$ is a simple transcendental field extension of an absolutely algebraic field.*

Proof : Let R be a local ring with $J(R) = pR$ and $\overline{R}$ a simple transcendental field extension of an absolutely algebraic field. Then R has a finite composition length and all one sided ideals are of the form $p^i R$, $0 \leq i \leq n$. Hence R is an artinian duo ring. By Theorem 21, R has a simple transcendental extension of a generalized Galois subring R_0 as its coefficient subring. Then $R = R_0 + J(R) = R_0 + pR = R_0$, as p is nilpotent in R_0. Thus R is a simple transcendental extension of a generalized Galois ring. The converse is trivial. ♣

Remark 3. Let R be an artinian local duo ring with *char* $R = 0$ and $\overline{R}$ a simple transcendental field extension of an absolutely algebraic field $\overline{K}$. Then $\overline{R} = \overline{K}(\overline{\alpha})$ for some $\overline{\alpha}$ transcendental elements in $\overline{R}$ over $\overline{P}$. By Theorem 19, R has a coefficient subfield $H(\alpha + h)$, where H is an absolutely algebraic subfield of R and $h \in J(R)$. So

$$H(\alpha + h) \cong \overline{R}.$$

Suppose that T is another coefficient subfield of R. Then $R = T + J(R)$, $T \cap J(R) = \{0\}$ and

$$T \cong \overline{R} \cong H(\alpha + h).$$

Thus T is a simple transcendental field extension of an absolutely algebraic field and the coefficient subfields of R are isomorphic.

Theorem 24. *Let R be an artinian local duo ring with char $R = p^n$ and $\overline{R}$ a simple transcendental field extension of an absolutely algebraic field. Then any coefficient subring of R is a simple transcendental extension of a generalized Galois subring. Moreover any two coefficient subrings of R are isomorphic.*

Proof : Let T be coefficient subring of R. Then $R = T + J(R)$, $J(T) = J(R) \cap T = pT$ and hence $\overline{T} \cong \overline{R}$ is a simple transcendental field extension of an absolutely algebraic field. By Theorem 23, T is a simple transcendental extension of a generalized Galois subring in R. Moreover, let us suppose that $T = K[\alpha]_{\mathcal{P}}$ and $T' = K'[\alpha']_{\mathcal{P}'}$ are two coefficient subrings of R, where K, K' are generalized Galois subrings of R. Then it is clear that $\overline{K} \cong \overline{K'}$ and by (2.25), we get $K \cong K'$. Let $\eta : K \longrightarrow K'$ be an isomorphism. This gives an isomorphism $\eta' : K[\alpha] \longrightarrow K'[\alpha']$ that extends η, and for which $\eta'(\alpha) = \alpha'$. Let $\mathcal{P} = pK[\alpha]$. Then $\eta(pK[\alpha]) = pK'[\alpha'] = \mathcal{P}'$. Then η' extends to an isomorphism $\overline{\eta'} : K[\alpha]_{\mathcal{P}} \longrightarrow K[\alpha']_{\mathcal{P}'}$. This proves the result. ♣

CHAPTER 4

Distinguished Basis

Corbas [10] and Wirt [26] proved that if R is a finite local ring and R_0 its coefficient subring then there exist $\pi_1, \pi_2, \cdots, \pi_n$ in $J(R)$ and $\sigma_1, \sigma_2, \cdots, \sigma_n$ in *Aut* R_0 such that

$$R = R_0 \oplus \sum_{i=1}^{n} R_0 \pi_i$$

and

$$\pi_i r = \sigma_i (r) \pi_i,$$

for each $r \in R_0$ and for all $i = 1, \cdots, n$. Alkhamees [3] proved that these automorphisms are uniquely determined by R and R_0.

In this chapter, we manage to generalize these results to the case where R is an artinian local duo ring with $\overline{R}$ an absolutely algebraic field.

4.1 Distinguished basis

Definition 1. Let R be a ring, $\mathfrak{M}$ an $(R, R) - bimodule$.
(i) An element $s \in \mathfrak{M}$ is called a *distinguished element of* $\mathfrak{M}$ over R if there exists an automorphism σ of the ring R such that

$$sr = \sigma (r) s$$

for all $r \in R$ and it is denoted by (s, σ).
(ii) A set $\{(s_1, \sigma_1), \cdots, (s_h, \sigma_h)\}$ of distinguished elements of $\mathfrak{M}$ over R is called a *distinguished* $R - basis$ of $\mathfrak{M}$ if

$$\mathfrak{M} = \overset{h}{\underset{i=1}{\oplus}} R s_i.$$

Theorem 2 [26]. *Let* $R_0 = GR(p^n, r)$ *be a Galois ring,* $\mathfrak{M}$ *an* $(R_0, R_0) -$ *bimodule, and Aut* $R_0 = \{\sigma_1, \sigma_2, \cdots, \sigma_r\}$. *Then*

$$\mathfrak{M} = \mathfrak{M}_1 \oplus \cdots \oplus \mathfrak{M}_r$$

as an $(R_0, R_0)-$*bimodule, where for each* i, $1 \leq i \leq r$, *there is an automorphism* $\sigma_{k(i)}$ *of* R_0 *such that*

$$sr = \sigma_{k(i)} (r) s$$

for each $s \in \mathfrak{M}_i$, $r \in R_0$, $\sigma_{k(1)} = I_{R_0}$ *and for* $i \neq j$, $1 \leq i, j \leq r$, $\sigma_{k(i)} \neq \sigma_{k(j)}$.

Proposition 3. *Let* R_0 *be a generalized Galois ring,* $\mathbb{Z}_{p^n}[a]$ *a Galois subring of* R_0 *and* $\sigma \in$ *Aut* R_0. *Then*

$$\sigma \mid_{\mathbb{Z}_{p^n}[a]} \in \text{ Aut } \mathbb{Z}_{p^n}[a].$$

Proof : As $\mathbb{Z}_{p^n}[a]$ is a Galois ring,

$$\mathbb{Z}_{p^n}[a] \cong \mathbb{Z}_{p^n}[x]/\langle f(x)\rangle,$$

where $f(x) \in \mathbb{Z}_{p^n}[x]$ is a minimal polynomial of a over $\mathbb{Z}_{p^n}$. Since σ is a $\mathbb{Z}_{p^n} - automorphism$, $\sigma(a)$ is a root of $f(x)$. So $\overline{a}$, $\overline{\sigma(a)}$ are roots of the irreducible polynomial $\overline{f}(x)$. As $\overline{\mathbb{Z}_{p^n}}[\overline{a}]$ is a normal extension of $\overline{\mathbb{Z}_{p^n}}$ $(\cong \mathbb{Z}_p)$,

$$\overline{\mathbb{Z}_{p^n}}[\overline{\sigma(a)}] = \overline{\mathbb{Z}_{p^n}}[\overline{a}].$$

By $(2.15)\,(iii)$,

$$\mathbb{Z}_{p^n}[\sigma(a)] = \mathbb{Z}_{p^n}[a].$$

So $\sigma(a) \in \mathbb{Z}_{p^n}[a]$ and $\sigma(\mathbb{Z}_{p^n}[a]) = \mathbb{Z}_{p^n}[a]$. Thus

$$\sigma\,|_{\mathbb{Z}_{p^n}[a]} \in Aut\ \mathbb{Z}_{p^n}[a]. \quad \clubsuit$$

Henceforth, R_0 is a generalized Galois ring and $\mathfrak{M}$ is an $(R_0, R_0)-bimodule$. If $b \in R_0$, is a lift algebraic element over $\mathbb{Z}_{p^n}$, then $r(b)$ denotes its degree over $\mathbb{Z}_{p^n}$. So $Aut\ \mathbb{Z}_{p^n}[b] = \{\sigma_{1,b}, \cdots, \sigma_{r(b),b}\}$, and

$$\mathfrak{M} = \mathfrak{M}_{1,b} \oplus \cdots \oplus \mathfrak{M}_{r(b),b},$$

is a decomposition of $\mathfrak{M}$ as a $(\mathbb{Z}_{p^n}[b], \mathbb{Z}_{p^n}[b]) - bimodule$ such that

$$sb = \sigma_{i,b}(b)\, s,$$

for all $s \in \mathfrak{M}_{i,b}$, $1 \le i \le r(b)$.

Proposition 4. *Let $\mathbb{Z}_{p^n}[b]$ be a Galois subring of R_0 and $\sigma, \delta \in Aut\ \mathbb{Z}_{p^n}[b]$ such that*

$$(\sigma(a) - \delta(a))\, s = 0,$$

for all $a \in \mathbb{Z}_{p^n}[b]$ and some $s\,(\neq 0) \in \mathfrak{M}$ an $(R_0, R_0) - bimodule$. Then $\sigma = \delta$.

Proof : Suppose that for all $a \in \mathbb{Z}_{p^n}[b]$ and some $s\,(\neq 0) \in \mathfrak{M}$ we have

$$(\sigma(a) - \delta(a))\, s = 0.$$

Then $\sigma(a) - \delta(a) \in J(\mathbb{Z}_{p^n}[b])$,

$$\overline{\sigma(a)} - \overline{\delta(a)} = 0.$$

Since we have an isomorphism $\varphi : Aut\ \mathbb{Z}_{p^n}[b] \longrightarrow Aut\ \overline{\mathbb{Z}_{p^n}[b]}$ with

$$\varphi(\eta) = \overline{\eta},$$

where $\overline{\eta}(\overline{a}) = \overline{\eta(a)}$ for all $\eta \in Aut\ \mathbb{Z}_{p^n}[b]$. Then

$$\overline{\sigma}(\overline{a}) = \overline{\sigma(a)} = \overline{\delta(a)} = \overline{\delta}(\overline{a}),$$

for all $\overline{a} \in \overline{\mathbb{Z}_{p^n}[b]}$ gives $\overline{\sigma} = \overline{\delta}$. Thus $\sigma = \delta$. $\clubsuit$

Proposition 5. *Let $\mathbb{Z}_{p^n}[b]$ be a Galois subring of R_0 and $s \in \mathfrak{M}$. Then for an i, $1 \leq i \leq r(b)$, $s \in \mathfrak{M}_{i,b}$ if and only if $sb = \sigma_{i,b}(b)\, s$.*

Proof : It is clear that if $s \in \mathfrak{M}_{i,b}$ then $sb = \sigma_{i,b}(b)\, s$. Suppose that $s = \sum_{j=1}^{r(b)} s_j \in \mathfrak{M}$ with $s_j \in \mathfrak{M}_j$ such that $sb = \sigma_{i,b}(b)\, s$. Then

$$\begin{aligned} \sum_{j=1}^{r(b)} \sigma_{i,b}(b)\, s_j &= \sigma_{i,b}(b)\, s \\ &= sb \\ &= \sum_{j=1}^{r(b)} s_j b \\ &= \sum_{j=1}^{r(b)} \sigma_{j,b}(b)\, s_j. \end{aligned}$$

As the sum is direct, for each j, $1 \leq j \leq r(b)$, $(\sigma_{i,b}(b) - \sigma_{j,b}(b))\, s_j = 0$. By Proposition 4,

$$\sigma_{i,b} = \sigma_{j,b}$$

whenever $s_j \neq 0$. But we know that if $i \neq j$, then $\sigma_{i,b} \neq \sigma_{j,b}$. Thus $s_j = 0$ for $i \neq j$, and hence $s = s_i \in \mathfrak{M}_{i,b}$. ♣

Proposition 6. *Let $\mathbb{Z}_{p^n}[a]$, $\mathbb{Z}_{p^n}[b]$ be two Galois subrings of R_0 such that $\mathbb{Z}_{p^n}[a] \subseteq \mathbb{Z}_{p^n}[b]$. For each $\sigma_{j,a} \in Aut\ \mathbb{Z}_{p^n}[a]$, $1 \leq j \leq r(a)$, let*

$$S_j = \{i : \sigma_{i,b} \mid_{\mathbb{Z}_{p^n}[a]} = \sigma_{j,a}\}.$$

Then

$$\mathfrak{M}_{j,a} = \bigoplus_{i \in S_j} \mathfrak{M}_{i,b}.$$

Proof : Now

$$\begin{aligned} \mathfrak{M} &= \mathfrak{M}_{1,b} \oplus \cdots \oplus \mathfrak{M}_{r(b),b}, \\ &= \mathfrak{M}_{1,a} \oplus \cdots \oplus \mathfrak{M}_{r(a),a}. \end{aligned}$$

For any element $s \in \mathfrak{M}_{i,b}, 1 \leq i \leq r(b)$,

$$sr = \sigma_{i,b}(r)\, s,$$

for every $r \in \mathbb{Z}_{p^n}[b]$; in particular as $a \in \mathbb{Z}_{p^n}[b]$,

$$sa = \sigma_{i,b}(a)\, s.$$

Also we have

$$sa = \sigma_{j,a}(a)\, s,$$

for each $s \in \mathfrak{M}_{j,a}$. Let $s\,(\neq 0) \in \mathfrak{M}_{j,a}$. Then $s = \sum_{i=1}^{r(b)} s_i$, $s_i \in \mathfrak{M}_{i,b}$ and

$$\begin{aligned} \sigma_{j,a}(a)\, s &= sa \\ &= \sum_{i=1}^{r(b)} s_i a \\ &= \sum_{i=1}^{r(b)} \sigma_{i,b}(a)\, s_i. \end{aligned}$$

Therefore

$$\sum_{i=1}^{r(b)} \sigma_{j,a}(a)\, s_i = \sum_{i=1}^{r(b)} \sigma_{i,b}(a)\, s_i.$$

As the sum is direct,

$$\sigma_{j,a}(a)\, s_i = \sigma_{i,b}(a)\, s_i.$$

Suppose that for some i, $s_i \neq 0$. Then

$$(\sigma_{i,b}(a) - \sigma_{j,a}(a))\, s_i = 0$$

gives $(\sigma_{i,b}(a) - \sigma_{j,a}(a)) \in p\mathbb{Z}_{p^n}[b]$. But by Proposition 3, $\sigma_{i,b} \mid_{\mathbb{Z}_{p^n}[a]} \in Aut\ \mathbb{Z}_{p^n}[a]$, so $(\sigma_{i,b}(a) - \sigma_{j,a}(a)) \in p\mathbb{Z}_{p^n}[a]$. Let $\sigma'_{i,b} = \sigma_{i,b} \mid_{\mathbb{Z}_{p^n}[a]}$. Then by Proposition 4,

$$\sigma'_{i,b} = \sigma_{j,a},$$

and $i \in S_j$. Hence

$$\mathfrak{M}_{j,a} \subseteq \underset{i \in S_j}{\oplus} \mathfrak{M}_{i,b}.$$

By Proposition 5, $s \in \mathfrak{M}_{i,b}$ if and only if $sb = \sigma_{i,b}(b)\, s$. Consider any $i \in S_j$. Then

$$\sigma_{j,a} = \sigma_{i,b} \mid_{\mathbb{Z}_{p^n}[a]}.$$

For $s \in \mathfrak{M}_{i,b}$,

$$sa = \sigma_{i,b}(a)\, s = \sigma_{j,a}(a)\, s.$$

So $\mathfrak{M}_{i,b} \subseteq \mathfrak{M}_{j,a}$. Hence

$$\mathfrak{M}_{j,a} = \underset{i \in S_j}{\oplus} \mathfrak{M}_{i,b}. \quad \clubsuit$$

Lemma 7. *Let $\mathbb{Z}_{p^n}[a]$ be a Galois subring of R_0. Then the decomposition*

$$\mathfrak{M} = \overset{r(a)}{\underset{j=1}{\oplus}} \mathfrak{M}_{j,a}$$

is a decomposition of $\mathfrak{M}$ as an $(R_0, R_0) - bimodule$.

Proof : We have

$$\mathfrak{M} = \overset{r(a)}{\underset{j=1}{\oplus}} \mathfrak{M}_{j,a}$$

as a $(\mathbb{Z}_{p^n}[a], \mathbb{Z}_{p^n}[a]) - bimodule$. Let $c \in R_0$ such that $c \notin \mathbb{Z}_{p^n}[a]$. Then there exists a Galois subring $\mathbb{Z}_{p^n}[b] \subseteq R_0$ such that $c \in \mathbb{Z}_{p^n}[b]$ and $\mathbb{Z}_{p^n}[a] \subset \mathbb{Z}_{p^n}[b]$. Now

$$\mathfrak{M} = \overset{r(b)}{\underset{i=1}{\oplus}} \mathfrak{M}_{i,b}$$

as a $(\mathbb{Z}_{p^n}[b], \mathbb{Z}_{p^n}[b]) - bimodule$. For $1 \leq j \leq r(a)$, let S_j be the set of those i such that $\sigma_{i,b} \mid_{\mathbb{Z}_{p^n}[a]} = \sigma_{j,a}$. By Proposition 6,

$$\mathfrak{M}_{j,a} = \underset{i \in S_j}{\oplus} \mathfrak{M}_{i,b}$$

Let $s \in \mathfrak{M}_{j,a}$. Then $s = \sum\limits_{i \in S_j} s_i$, where $s_i \in \mathfrak{M}_{i,b}$. Therefore

$$\begin{aligned} sc &= \sum_{i \in S_j} s_i c \\ &= \sum_{i \in S_j} \sigma_{i,b}(c)\, s_i \\ &\in \underset{i \in S_j}{\oplus} \mathfrak{M}_{i,b} = \mathfrak{M}_{j,a}. \end{aligned}$$

Hence $\mathfrak{M}_{j,a} R_0 \subseteq \mathfrak{M}_{j,a}$. Similarly $R_0 \mathfrak{M}_{j,a} \subseteq \mathfrak{M}_{j,a}$. Thus

$$\mathfrak{M} = \overset{r(a)}{\underset{j=1}{\oplus}} \mathfrak{M}_{j,a}$$

as an $(R_0, R_0) - bimodule$. ♣

Theorem 8. *Let R_0 be a generalized Galois ring, $\mathfrak{M}$ an $(R_0, R_0) -$ bimodule having a finite composition length as an $R_0 -$ module. Then $\mathfrak{M}$ has a distinguished $R_0 -$ basis.*

Proof : For any lift algebraic element $a \in R_0$, we have

$$\mathfrak{M} = \overset{r(a)}{\underset{j=1}{\oplus}} \mathfrak{M}_{j,a}.$$

This is a $(\mathbb{Z}_{p^n}[a], \mathbb{Z}_{p^n}[a]) - bimodule$ decomposition. By Lemma 7, it is also an $(R_0, R_0) - bimodule$ decomposition. If $d({}_{R_0}\mathfrak{M}) = n$, then the number $\mathfrak{t}_a$ of non-zero $\mathfrak{M}_{j,a}$ can not be more than n. So we can find a lift algebraic element d in R_0 over $\mathbb{Z}_{p^n}$ such that $\mathfrak{t}_d$ is the largest. Let $c \in R_0$ be any lift algebraic element over $\mathbb{Z}_{p^n}$ with $\mathbb{Z}_{p^n}[d] \subseteq \mathbb{Z}_{p^n}[c]$. Consider the decomposition

$$\mathfrak{M} = \overset{r(c)}{\underset{i=1}{\oplus}} \mathfrak{M}_{i,c}.$$

For $1 \leq j \leq r(d)$, let $S_j = \{i : \sigma_{i,c} \mid_{\mathbb{Z}_{p^n}[d]} = \sigma_{j,d}\}$. Then

$$\mathfrak{M}_{j,d} = \underset{i \in S_j}{\oplus} \mathfrak{M}_{i,c}.$$

So $\mathfrak{t}_c \geq \mathfrak{t}_d$. Hence $\mathfrak{t}_c = \mathfrak{t}_d$. If for some j, $\mathfrak{M}_{j,d} \neq \{0\}$, then S_j is a singletion set. So given $\sigma_{j,d}$, with $\mathfrak{M}_{j,d} \neq \{0\}$, there exists a unique $\eta(j)$ such that $\sigma_{\eta(j),c} \mid_{\mathbb{Z}_{p^n}[d]} = \sigma_{j,d}$. Then $\mathfrak{M}_{j,d} = \mathfrak{M}_{\eta(j),c}$. Conversely, consider an i such that $\mathfrak{M}_{i,c} \neq \{0\}$, then there exists $\sigma_{j,d} \in Aut\ \mathbb{Z}_{p^n}[d]$ such that $\sigma_{i,c} \mid_{\mathbb{Z}_{p^n}[d]} = \sigma_{j,d}$. So $\mathfrak{M}_{i,c} \subseteq \mathfrak{M}_{j,d}$ and hence by (1.7), $\mathfrak{M}_{j,d} = \mathfrak{M}_{i,c}$. Let $\mathfrak{X}_d = \{j : \mathfrak{M}_{j,d} \neq \{0\}\}$ and $\mathfrak{X}_c = \{i : \mathfrak{M}_{i,c} \neq \{0\}\}$. As above, we have shown that there exists a one-to-one correspondence η between $\mathfrak{X}_d$ and $\mathfrak{X}_c$ such that

$$\mathfrak{M}_{j,d} = \mathfrak{M}_{\eta(j),c},$$

for all $j \in \mathfrak{X}_d$. By reindexing, we suppose that $\mathfrak{X}_d = \{1, 2, \cdots, \mathfrak{t}_d\}$ and for any lift algebraic element c with $\mathbb{Z}_{p^n}[d] \subseteq \mathbb{Z}_{p^n}[c]$, we can take $\mathfrak{X}_c = \{1, 2, \cdots, \mathfrak{t}_d\}$ such that each $\sigma_{i,c}$ is an extension of $\sigma_{i,d}$, $i \in \mathfrak{X}_d$. As

$$R_0 = \cup\{\mathbb{Z}_{p^n}[c] : \mathbb{Z}_{p^n}[d] \subseteq \mathbb{Z}_{p^n}[c]\},$$

for each $i \in \mathfrak{X}_d$, we get an automorphism $\sigma_i : R_0 \longrightarrow R_0$ such that given $a \in R_0$, $\sigma_i(a) = \sigma_{i,c}(a)$, whenever $a \in \mathbb{Z}_{p^n}[c]$ such that $\mathbb{Z}_{p^n}[d] \subseteq \mathbb{Z}_{p^n}[c]$. Then for any $s \in \mathfrak{M}_{i,d}$

$$sa = \sigma_i(a)\, s.$$

As R_0 is a chain ring, by (1.11),

$$\mathfrak{M}_{i,d} = \overset{n(i)}{\underset{j=1}{\oplus}} R_0 s_{i,j},$$

for some non-zero cyclic $R_0 - modules\ R_0 s_{i,j}$. For any $a \in R$, $s_{i,j}a = \sigma_i(a)\, s_{i,j} \in R_0 s_{i,j}$. This shows that $R_0 s_{i,j}$ is an $(R_0, R_0) - bimodule$. So

$$\mathfrak{M} = \overset{\mathfrak{t}_d}{\underset{i=1}{\oplus}} \left(\overset{n(i)}{\underset{j=1}{\oplus}} R_0 s_{i,j} \right)$$

is a decomposition of $\mathfrak{M}$ as an $(R_0, R_0) - bimodule$ such that for any $s \in R_0 s_{i,j}$ and $a \in R_0$,

$$sa = \sigma_i(a)\, s.$$

Thus

$$\{(s_{i,j}, \sigma_i) : 1 \leq i \leq \mathfrak{t}_d, 1 \leq j \leq n(i)\}$$

is a distinguished $R_0 - basis$ of $\mathfrak{M}$. ♣

Henceforth, d will be a lift algebraic element in R_0 having the property as in the proof of Theorem 8 and $\mathfrak{t}_d = |\mathfrak{X}_d|$, where $\mathfrak{X}_d = \{j : \mathfrak{M}_{j,d} \neq \{0\}\} = .$

Definition 9. Let R_0 be a generalized Galois ring and $\mathfrak{M}$ an $(R_0, R_0) - bimodule$ having a finite composition length as an $R_0 - module$. According to the last theorem $\mathfrak{M}$ has $\{(s_{i,j}, \sigma_i) : 1 \leq i \leq \mathfrak{t}_d,\ 1 \leq j \leq n(i)\}$ a distinguished $R_0 - basis$ of $\mathfrak{M}$. We shall prove in the following theorem that the automorphisms of R_0 $\{\sigma_i : 1 \leq i \leq \mathfrak{t}_d\}$ are uniquely determined by $\mathfrak{M}$. Thus we call such automorphisms *the associated automorphisms with* $\mathfrak{M}$.

Corollary 10. *Let R_0 be a generalized Galois ring and $\sigma, \delta \in Aut\ R_0$ such that*

$$(\sigma(a) - \delta(a))\, s = 0,$$

for all $a \in R_0$ and some $s\,(\neq 0) \in \mathfrak{M}$ an $(R_0, R_0) - bimodule$. Then $\sigma = \delta$.

Proof : By using (2.27), we can repeat the same steps as in the proof of Proposition 4 to get the result. ♣

Theorem 11. *Let R_0 be a generalized Galois ring and $\mathfrak{M}$ an $(R_0, R_0) - bimodule$ with $d({}_{R_0}\mathfrak{M})$ finite. Then the associated automorphisms with $\mathfrak{M}$ are uniquely determined by $\mathfrak{M}$.*

Proof : Suppose that $T = \{(s_{i,j}, \sigma_i) : 1 \leq i \leq \mathfrak{t}_d,\ 1 \leq j \leq n(i)\}$, $N = \{(u_{l,k}, \delta_l) : 1 \leq l \leq \mathfrak{h},\ 1 \leq k \leq m(l)\}$ be two distinguished $R_0 - basis$ of $\mathfrak{M}$. Let

$$\mathfrak{M}_i = \overset{n(i)}{\underset{j=1}{\oplus}} R_0 s_{i,j},$$

$$\mathfrak{N}_l = \overset{m(l)}{\underset{k=1}{\oplus}} R_0 u_{l,k}.$$

Then

$$\mathfrak{M} = \overset{\mathfrak{t}_d}{\underset{i=1}{\oplus}} \mathfrak{M}_i$$

and

$$\mathfrak{M} = \overset{\mathfrak{h}}{\underset{l=1}{\oplus}} \mathfrak{N}_l$$

Let $s \in \mathfrak{M}_i$. As $s \in \mathfrak{M} = \overset{\mathfrak{h}}{\underset{l=1}{\oplus}} \mathfrak{N}_l$, $s = \sum_{l=1}^{\mathfrak{h}} v_l$, $v_l \in \mathfrak{N}_l$. For any $a \in R_0$,

$$\begin{aligned} \sigma_i(a) \left(\sum_{l=1}^{\mathfrak{h}} v_l \right) &= \sigma_i(a)\, s \\ &= sa \\ &= \left(\sum_{l=1}^{\mathfrak{h}} v_l \right) a \\ &= \sum_{l=1}^{\mathfrak{h}} \delta_l(a)\, v_l. \end{aligned}$$

So $(\sigma_i(a) - \delta_l(a))\, v_l = 0$. If $v_l \neq 0$, then by Corollary 10, $\sigma_i = \delta_l$. Since $\delta_1, \cdots, \delta_{\mathfrak{h}}$ are all distinct, we get $\mathfrak{t}_d \leq \mathfrak{h}$. Similarly $\mathfrak{h} \leq \mathfrak{t}_d$. Hence $\{\sigma_1, \cdots, \sigma_{\mathfrak{t}_d}\} = \{\delta_1, \cdots, \delta_{\mathfrak{t}_d}\}$. Thus $\sigma_1, \cdots, \sigma_{\mathfrak{t}_d}$ are uniquely determined by $\mathfrak{M}$. ♣

Theorem 12. *(i) Let R_0 be a generalized Galois ring and $\mathfrak{M}$ an $(R_0, R_0) -$ bimodule with $d({}_{R_0}\mathfrak{M})$ finite. Let $\sigma_1, \cdots, \sigma_h$ be the associated automorpisms with $\mathfrak{M}$ and*

$$\mathfrak{M} = \mathfrak{M}_1 \oplus \cdots \oplus \mathfrak{M}_h$$

such that for any $s \in \mathfrak{M}_i$, $1 \leq i \leq h$ and $a \in R_0$, $sa = \sigma_i(a)\, s$. Then any $s \in \mathfrak{M}$ is in $\mathfrak{M}_i$ if and only if $sa = \sigma_i(a)\, s$ for all $a \in R_0$.

(ii) Let $T = \{(s_{i,j}, \sigma_i) : 1 \leq i \leq h,\ 1 \leq j \leq n(i)\}$ *and* $N = \{(u_{i,j}, \delta_i) : 1 \leq i \leq h,\ 1 \leq j \leq m(i)\}$ *be two distinguished* $R_0 - basis$ *of* $\mathfrak{M}$. *Then* $n(i) = m(i)$ *for all* $1 \leq i \leq h$.

Proof : Let $s \in \mathfrak{M}_i$. Then $sa = \sigma_i(a)\, s$ for all $a \in R_0$. Conversely, let $s \in \mathfrak{M}$ such that $sa = \sigma_i(a)\, s$ for all $a \in R_0$. Now $s = \sum_{j=1}^{h} s_j$, $s_j \in \mathfrak{M}_j$. This gives

$$sa = \sum_{j=1}^{h} s_j a = \sum_{j=1}^{h} \sigma_j(a)\, s_j,$$

so

$$\sum_{j=1}^{h} \sigma_i(a)\, s_j = \sum_{j=1}^{h} \sigma_j(a)\, s_j.$$

Thus $(\sigma_i(a) - \sigma_j(a))\, s_j = 0$ for every j. By Corollary 10, $\sigma_i = \sigma_j$ whenever $s_j \neq 0$. But $\sigma_i \neq \sigma_j$ for $j \neq i$. So $s_j = 0$ for all $j \neq i$, $s = s_i \in \mathfrak{M}_i$.
(ii) Now

$$\mathfrak{M} = \bigoplus_{i=1}^{h} \left(\bigoplus_{j=1}^{n(i)} R_0 s_{i,j} \right).$$

As $s_{i,j} a = \sigma_i(a)\, s_{i,j}$ for all $a \in R_0$, by the first part $s_{i,j} \in \mathfrak{M}_i$. So

$$\mathfrak{M}'_i = \bigoplus_{j=1}^{n(i)} R_0 s_{i,j} \subseteq \mathfrak{M}_i.$$

Similarly $\mathfrak{M}_i \subseteq \mathfrak{M}'_i$. Hence

$$\begin{aligned} \mathfrak{M}_i &= \bigoplus_{j=1}^{n(i)} R_0 s_{i,j} \\ &= \bigoplus_{j=1}^{m(i)} R_0 u_{i,j}. \end{aligned}$$

Now $d({}_{R_0}\mathfrak{M}_i)$ is finite. As R_0 is local, $R_0 s_{i,j}$, $R_0 u_{i,j}$ are local $R_0 - modules$, so they are indecomposable. By Krull-Schmidt Theorem [5, (12.9)] $n(i) = m(i)$ for all $1 \leq i \leq h$. ♣

4.2 Distinguished basis for a local ring over its coefficient subring

Proposition 13. *Let* R *be an artinian local duo ring such that* $\overline{R}$ *is an absolutely algebraic field of non-zero characteristic and* R_0 *a coefficient subring of* R. *Then*

$$R = \bigoplus_{i=1}^{\mathfrak{t}_d} \left(\bigoplus_{j=1}^{n(i)} R_0 s_{i,j} \right)$$

such that $\{(s_{i,j},\sigma_i) : 1 \leq i \leq \mathfrak{t}_d,\ 1 \leq j \leq n(i)\}$ *is a distinguished* $R_0 - basis$ *of* R *and* $\sigma_1 = I_{R_0}$. *Further,*

$$Z_R(R_0) = \overset{n(1)}{\underset{j=1}{\oplus}} R_0 s_{1,j}.$$

Proof : By (1.10), $d({}_{R_0}R) = d({}_RR)$. As R is an artinian local ring and $d({}_{R_0}R)$ is finite, by Theorem 8,

$$R = \overset{\mathfrak{t}_d}{\underset{i=1}{\oplus}} \left(\overset{n(i)}{\underset{j=1}{\oplus}} R_0 s_{i,j} \right),$$

where $\{(s_{i,j},\sigma_i) : 1 \leq i \leq \mathfrak{t}_d,\ 1 \leq j \leq n(i)\}$ is a distinguished $R_0 - basis$ of R. Consider $s\,(\neq 0) \in Z_R(R_0)$. For any $a \in R_0$, $sa = as = \sigma_1(a)s$. By Theorem 12, $s \in \overset{n(1)}{\underset{j=1}{\oplus}} R_0 s_{1,j}$. Hence $Z_R(R_0) \subseteq \overset{n(1)}{\underset{j=1}{\oplus}} R_0 s_{1,j}$. Obviously $\overset{n(1)}{\underset{j=1}{\oplus}} R_0 s_{1,j} \subseteq Z_R(R_0)$. Thus

$$Z_R(R_0) = \overset{n(1)}{\underset{j=1}{\oplus}} R_0 s_{1,j}. \quad \clubsuit$$

Theorem 14. *Let* R *be an artinian local duo ring such that* $\overline{R}$ *is an absolutely algebraic field of non-zero characteristic. Then*

$$R = R_0 \oplus \mathfrak{T}$$

as an $(R_0, R_0)-$*bimodule, where* R_0 *is a coefficient subring of* R *and* $\mathfrak{T} \subseteq J(R)$.

Proof : By Proposition 13,

$$R = \overset{\mathfrak{t}_d}{\underset{i=1}{\oplus}} \left(\overset{n(i)}{\underset{j=1}{\oplus}} R_0 s_{i,j} \right),$$

$$Z_R(R_0) = \overset{n(1)}{\underset{j=1}{\oplus}} R_0 s_{1,j},$$

where $\{(s_{i,j},\sigma_i) : 1 \leq i \leq \mathfrak{t}_d,\ 1 \leq j \leq n(i)\}$ is a distinguished $R_0 - basis$ of R and $\sigma_1 = I_{R_0}$. Since R_0 is an injective $R_0 - module$ and $R_0 \subseteq Z_R(R_0)$, by (1.9)

$$Z_R(R_0) = R_0 \oplus \mathfrak{N}$$

as an $(R_0, R_0) - bimodule$. Now $d({}_{R_0}\mathfrak{N}) = d({}_{R_0}Z_R(R_0)) - d({}_{R_0}R_0)$, hence $\mathfrak{N}$ has a distinguished $R_0 - basis$, say $\{(v_j, I_{R_0}) : 2 \leq j \leq n(1)\}$. Suppose that for some i, j, with $2 \leq i \leq \mathfrak{t}_d$, $1 \leq j \leq n(i)$, $s_{i,j}$ is a unit. Then

$$s_{i,j}a = \sigma_i(a)\, s_{i,j}$$

for all $a \in R_0$. So

$$\begin{aligned} \overline{as_{i,j}} &= \overline{s_{i,j}a} \\ &= \overline{\sigma_i(a)\, s_{i,j}}, \end{aligned}$$

$$\left(\overline{a} - \overline{\sigma_i(a)}\right)\overline{s_{i,j}} = 0.$$

As $\overline{s_{i,j}} \neq 0$. By Corollary 10, $\sigma_i = I_{R_0}$. Hence $i = 1$. This is a contradiction. This shows that $s_{i,j}$ is a non-unit for $2 \leq i \leq \mathfrak{t}_d$, $1 \leq j \leq n(i)$. Thus

$$\mathfrak{K} = \overset{\mathfrak{t}_d}{\underset{i=2}{\oplus}} \left(\overset{n(i)}{\underset{j=1}{\oplus}} R_0 s_{i,j} \right) \subseteq J(R).$$

Now $\{(1, I_{R_0}), (v_j, I_{R_0}) : 2 \leq j \leq n(1)\}$ is a distinguished $R_0-basis$ for $Z_R(R_0)$. As $v_j \in R = R_0 + J(R)$, there exist $r_j \in R_0$ and $t_j \in J(R)$ such that

$$t_j = v_j - r_j.$$

Let some v_i be a unit. Then r_i is a unit in R_0. Clearly

$$R_0 \oplus R_0 v_i = R_0 \oplus R_0 t_i.$$

Hence for $2 \leq i \leq n(1)$ we can find an element $t_i \in J(R)$ such that $R_0 \oplus R_0 v_i = R_0 \oplus R_0 t_i$. Therefore

$$\begin{aligned} Z_R(R_0) &= R_0 \oplus R_0 v_1 \oplus \cdots \oplus R_0 v_{n(1)} \\ &= R_0 \oplus R_0 t_1 \oplus \cdots \oplus R_0 t_{n(1)}. \end{aligned}$$

Let

$$\mathfrak{T} = \left(\overset{n(1)}{\underset{j=2}{\oplus}} R_0 t_j \right) \oplus \mathfrak{K}.$$

Then

$$R = R_0 \oplus \mathfrak{T}$$

as an $(R_0, R_0) - bimodule$, where $\mathfrak{T} \subseteq J(R)$. ♣

Definition 15. Let R be an artinian local duo ring such that $\overline{R}$ is an absolutely algebraic field of non-zero characteristic. Then

$$R = R_0 \oplus \mathfrak{T}$$

as an $(R_0, R_0) - bimodule$, where R_0 is a coefficient subring of R and $\mathfrak{T} \subseteq J(R)$. Suppose

$$T = \{(\pi_{i,j}, \sigma_i) : 1 \leq i \leq \mathfrak{t}_d,\ 1 \leq j \leq n(i)\}$$

is a distinguished $R_0 - basis$ of $\mathfrak{T}$. We call T *a distinguished basis of R over R_0* and we call $\sigma_1, \cdots, \sigma_{\mathfrak{t}_d}$ *the distinct associated automorphisms of R with respect to R_0*.

Theorem 16. *Let R be an artinian local duo ring such that $\overline{R}$ is an absolutely algebraic field of non-zero characteristic. Then R has a distinguished basis over its coefficient subring R_0 and the distinct associated automorphisms of R with respect to R_0 are uniquely determined by R and R_0.*

Proof : By (3.13), R has a coefficient subring R_0. Now using Theorems 8, 11 and 14, the result follows. ♣

CHAPTER 5

The Structure Of Chain Rings

Finite chain rings have been studied by quite many mathematicians. As regards to the construction of finite chain rings, Wirt [26] had shown that a finite chain ring is a quotient of a skew polynomial ring over a Galois ring by an ideal of special form depending upon an Eisenstein polynomial; this construction was also almost achieved by Nechaev [22]. Also, Fisher [15] gave the structure of a finite chain ring as a quotient of a skew power series ring over a certain complete discrete commutative valuation domain by an ideal of special form, similar to the ideal involved in the construction by Wirt [26]. Alkhamees [2] proved that the centralizer of a coefficient subring R_0 of a finite chain ring is a maximal commutative chain subring $Z_{R_0}(R)$ and it determines R up to isomorphism.

In this chapter, we manage to generalize Alkhamees results involving the centralizer of a coefficient subring and the centre of finite chain ring to the case of a chain ring R such that $\overline{R}$ is an absolutely algebraic field. We also manage to determine the structure of such chain rings as quotients of skew polynomial ring over generalized Galois ring by an ideal of special form depending upon an Eisenstein polynomial. This construction is a generalization of the one given by Wirt for finite chain rings.

5.1 The centralizer of a coefficient subring

By (R, θ, m, p^n, k) we mean a chain ring R with $J(R) = \theta R = R\theta$, $\overline{R}$ an absolutely algebraic field, $m\,(>1)$ is the index of nilpotency of $J(R)$, *char* $R = p^n$, where p is a prime number and $n > 0$, and k is the smallest positive integer such that $p \in (J(R))^k$. In case $n \neq 1$, $\theta^k = pw$ for some unit $w \in R$. In the other case $k = m$.

Lemma 1. *Let (R, θ, m, p^n, k) be a chain ring with R_0 a coefficient subring of R. Then*

$$R = R_0 + R_0\theta + \cdots + R_0\theta^{k-1}.$$

Proof : We have

$$\begin{aligned} R &= R_0 + R\theta \\ &= R_0 + (R_0 + R\theta)\,\theta \\ &= R_0 + R_0\theta + R\theta^2 \\ &\;\;\vdots \\ &= T + R\theta^k, \end{aligned}$$

where $T = \sum_{i=0}^{k-1} R_0\theta^i$. If $n = 1$, then $\theta^k = 0$ and hence $R = T$. Let $n > 1$. Then $\theta^k = pw$ with w a unit in R, which gives $R\theta^k = Rp$. Hence $R = T + Rp = T = \sum_{i=0}^{k-1} R_0\theta^i$, as p is nilpotent in T. ♣

Proposition 2. *Let (R, θ, m, p^n, k) be a chain ring with R_0 a coefficient subring of R. Let*

$$0 \neq r = \sum_{i=0}^{k-1} r_i \theta^i \in R,$$

*with $r_i \in R_0$. If for some i and $s < m$, $r_i\theta^i \in J(R)^s \backslash J(R)^{s+1}$, then for any $j \neq i$, $r_j\theta^j \notin J(R)^s \backslash J(R)^{s+1}$. Moreover, if l is the smallest non-*negative *integer such that $r_i\theta^i \in J(R)^l \backslash J(R)^{l+1}$ for some i, $0 \leq i \leq k-1$, then $r \in J(R)^l \backslash J(R)^{l+1}$.*

Proof : Let $0 \neq r = \sum_{i=0}^{k-1} r_i \theta^i \in R$. Suppose on the contrary that there exists $i \neq j$, $0 \leq i, j \leq k-1$ such that $r_i\theta^i, r_j\theta^j \in J(R)^s \backslash J(R)^{s+1}$ for some $s < m$. If $n = 1$, then R_0 is a field and hence r_i, r_j are units. So $i = s = j$. This is a contradiction. Let $n > 1$. Then

$$\begin{aligned} r_i\theta^i &= v_i p^l \theta^i, \\ r_j\theta^j &= v_j p^h \theta^j, \end{aligned}$$

where $0 \leq l, h \leq n-1$ and v_i, v_j are units in R_0. As $\theta^k = pw$ with w a unit in R, $p = \theta^k w^{-1} = w^{-1}\theta^k$ and hence

$$\begin{aligned} r_i\theta^i &= v_i w^{-l} \theta^{lk} \theta^i, \\ r_j\theta^j &= v_j w^{-h} \theta^{hk} \theta^j. \end{aligned}$$

Since $r_i\theta^i, r_j\theta^j \in J(R)^s \backslash J(R)^{s+1}$,

$$\begin{aligned} lk + i &= s = hk + j \\ j - i &= (l-h)\, k. \end{aligned}$$

Hence $k \mid (j-i)$, but $0 \leq i, j \leq k-1$, so $|j-i| < k$. This is a contradiction. Thus $r_j\theta^j \notin J(R)^s \backslash J(R)^{s+1}$. Let l be the smallest non-negative integer such that $r_i\theta^i \in J(R)^l \backslash J(R)^{l+1}$ for some i, $0 \leq i \leq k-1$. Since $r \neq 0$, $J(R)^l \neq 0$. Let $a \in J(R)^i \backslash J(R)^{i+1}$, $b \in J(R)^j \backslash J(R)^{j+1}$ such that $i < j$. Then $a = v\theta^i$, $b = u\theta^j$, where v, u are units in R. So

$$\begin{aligned} a + b &= v\theta^i + u\theta^j \\ &= \left(v + u\theta^{j-i}\right) \theta^i \\ &\in J(R)^i \backslash J(R)^{i+1}. \end{aligned}$$

Since $0 \neq r = \sum_{i=0}^{k-1} r_i \theta^i \in R$ with each $r_i\theta^i$ belong to distinct power of $J(R)$, $r \in J(R)^l \backslash J(R)^{l+1}$. ♣

Theorem 3. *Let (R, θ, m, p^n, k) be a chain ring with R_0 a coefficient subring of R. Then*

$$R = R_0 \oplus R_0\theta \oplus \cdots \oplus R_0\theta^{k-1},$$

and

$$J(R) = J(R_0) \oplus R_0\theta \oplus \cdots \oplus R_0\theta^{k-1}$$

as an $R_0 - module.$

Proof : By Lemma 1, we have

$$R = R_0 + R_0\theta + \cdots + R_0\theta^{k-1}.$$

So we need only to show that this sum is direct. Suppose on the contrary that

$$0 = r_0 + r_1\theta + \cdots + r_{k-1}\theta^{k-1},$$

$r_i \neq 0$ for some $0 \leq i \leq k-1$. Let l be the smallest non-negative integer such that $r_i\theta^i \in J(R)^l \backslash J(R)^{l+1}$ for some $0 \leq i \leq k-1$. Then $J(R)^l \neq 0$ and by Proposition 2,

$$0 = r_0 + r_1\theta + \cdots + r_{k-1}\theta^{k-1} \in J(R)^l \backslash J(R)^{l+1}.$$

This is a contradiction. Thus $r_j\theta^j = 0$ for all $0 \leq j \leq k-1$ and the sum is direct. Also

$$\begin{aligned} J(R) &= (R_0 \cap J(R)) \oplus R_0\theta \oplus \cdots \oplus R_0\theta^{k-1} \\ &= J(R_0) \oplus R_0\theta \oplus \cdots \oplus R_0\theta^{k-1}. \quad \clubsuit \end{aligned}$$

Theorem 4. *Let* (R, θ, m, p^n, k) *be a chain ring with* R_0 *a coefficient subring of* R. *Then*
(i) $\theta^k = p\left(u_0 + u_1\theta + \cdots + u_{k-1}\theta^{k-1}\right)$, *where* $u_i \in R_0$ *for* $0 \leq i \leq k-1$ *and* u_0 *is a unit.*
(ii) $m = (n-1)k + t$, $1 \leq t \leq k$.
(iii) *There are* $R_0 - module$ *isomorphisms,*

$$\begin{aligned} R_0\theta^i &\cong R_0, \ \textit{for } i = 1, \cdots, t-1 \\ R_0\theta^i &\cong R_0 p, \textit{ for } i = t, \cdots, k. \end{aligned}$$

Proof : (i) As $\theta^k = pw$ with w a unit in R,

$$w = u_0 + u_1\theta + \cdots + u_{k-1}\theta^{k-1},$$

where u_0 is a unit in R_0.
(ii) We have

$$\theta^{nk} = p^n w^n = 0.$$

Hence $m \leq nk$. As $p^{n-1} \neq 0$ and w^{n-1} is a unit,

$$\theta^{(n-1)k} = p^{n-1}w^{n-1} \neq 0.$$

Thus

$$m = (n-1)k + t, \ 1 \leq t \leq k.$$

(*iii*) Let $\delta_i : R_0 \longrightarrow R_0\theta^i$ be a map such that $\delta_i(r) = r\theta^i$ for all $r \in R_0$. Then for $s, r, v, u \in R_0$,

$$\begin{aligned}\delta_i(sr+vu) &= (sr+vu)\theta^i \\ &= s\left(r\theta^i\right) + v\left(u\theta^i\right) \\ &= s\delta_i(r) + v\delta_i(u).\end{aligned}$$

So δ_i is an $R_0 - module$ homomorphism.
Case I : $i = 1, \cdots, t-1$. Suppose that $p^{n-1}\theta^i = 0$. As $p = \theta^k w^{-1} = w^{-1}\theta^k$,

$$0 = \left(w^{-1}\theta^k\right)^{n-1}\theta^i = w^{-(n-1)}\theta^{(n-1)k+i}.$$

This is a contradiction, since $i < t$. Hence $R_0p^{n-1} \nsubseteq \ker \delta_i$. As R_0p^{n-1} is the minimal ideal of R_0, $\ker \delta_i = 0$ and δ_i is a monomorphism. It is clear that δ_i is onto. Thus

$$R_0 \cong R_0\theta^i, \text{ for } i = 1, \cdots, t-1.$$

Case II : $i = t, \cdots, k$. As

$$p^{n-1}\theta^i = \left(w^{-1}\theta^k\right)^{n-1}\theta^i = w^{-(n-1)}\theta^{(n-1)k+i} = 0,$$

$R_0p^{n-1} \subseteq \ker \delta_i$. But $(n-2)k + i < m$. So

$$p^{n-2}\theta^i = \left(w^{-1}\theta^k\right)^{n-2}\theta^i = w^{-(n-2)}\theta^{(n-2)k+i} \neq 0$$

and hence $R_0p^{n-2} \nsubseteq \ker \delta_i$. Since there is no ideal in R_0 between R_0p^{n-1} and R_0p^{n-2}, $\ker \delta_i = R_0p^{n-1}$. Thus

$$R_0/R_0p^{n-1} \cong R_0\theta^i.$$

But $R_0/R_0p^{n-1} \cong R_0p$ by the isomorphism ρ defined by $\rho\left(r + R_0p^{n-1}\right) = pr$. Hence

$$R_0p \cong R_0\theta^i, \quad \text{for } i = t, \cdots, k. \quad \clubsuit$$

Lemma 5. *Let (R, π, m, p^n, k) be a chain ring with R_0 a coefficient subring of R. Then there exist $\theta \in J(R)\backslash\left(J(R)\right)^2$ and $\sigma \in Aut\ R_0$ such that (θ, σ) is a distinguished element in R over R_0. Furthermore $\sigma, \sigma^2, \cdots, \sigma^{k'-1}$ are the distinct associated automorphisms of R with respect to R_0, where k' is the order of σ.*

Proof : By (1.10), $d\left({}_{R_0}J(R)\right) = d\left({}_RJ(R)\right) = m$ and hence $J(R)$ has finite composition length as an $R_0 - module$. Hence by (4.8), $J(R)$ has a distinguished $R_0 - basis$, say $\{(t_1, \sigma_1), , \cdots, (t_h, \sigma_h)\}$. So

$$J(R) = R_0t_1 \oplus \cdots \oplus R_0t_h.$$

Now there is an element $t_i \in \{t_1, t_2, \cdots, t_h\}$ such that $t_i \in J(R)\backslash\left(J(R)\right)^2$, otherwise

$$J(R) = R_0t_1 \oplus \cdots \oplus R_0t_h \subseteq \left(J(R)\right)^2.$$

Let $\theta = t_i \in J(R) \backslash (J(R))^2$ and $\sigma = \sigma_i$. Then clearly $J(R) = \theta R = R\theta$ and

$$\theta a = \sigma(a)\theta,$$

for all $a \in R_0$. Hence (θ, σ) is a distinguished element in R over R_0. By Theorem 3,

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

So $\sigma, \sigma^2, \cdots, \sigma^{k'-1}$ are the distinct associated automorphisms of R with respect to R_0.

Definition 6. Let R be a chain ring. Then $(R_0, \theta, m, p^n, k, \sigma, k')$ is called a *distinguished set of* R if (R, θ, m, p^n, k) is a chain ring, where R_0 is a coefficient subring of R, (θ, σ) is a distinguished element of R over R_0 and k' is the order of σ.

Theorem 7. *Let R be a chain ring and $(R_0, \theta, m, p^n, k, \sigma, k')$ a distinguished set of R. Then*

$$R = R_0 \oplus R_0\theta \oplus \cdots \oplus R_0\theta^{k-1},$$

and

$$J(R) = J(R_0) \oplus R_0\theta \oplus \cdots \oplus R_0\theta^{k-1}$$

as an $(R_0, R_0) - bimodule$.

Proof : As (θ, σ) is a distinguished element in R over R_0, $\left(R_0\theta^i\right) R_0 \subseteq R_0\theta^i$ for all $1 \leq i \leq k-1$. From Theorem 3, we get

$$R = R_0 \oplus R_0\theta \oplus \cdots \oplus R_0\theta^{k-1}$$

and

$$J(R) = J(R_0) \oplus R_0\theta \oplus \cdots \oplus R_0\theta^{k-1}$$

as an $(R_0, R_0) - bimodule$.

Proposition 8. *Let k, k' be two positive integers and*

$$\begin{aligned} k_1 &= k/k', \quad \textit{if } k' \mid k, \\ k_1 &= [k/k'] + 1, \quad \textit{otherwise.} \end{aligned}$$

Then

$$\begin{aligned} (k_1 - 1)k' &\leq k - 1, \\ k_1 k' &\geq k. \end{aligned}$$

Proof : *Case I :* Let $k' \mid k$. Then

$$\begin{aligned} (k_1 - 1)k' &= (k/k' - 1)k' = k - k' \leq k - 1, \\ k_1 k' &= (k/k')k' = k. \end{aligned}$$

Case II : Let $k' \nmid k$, then $k = ik' + s$, $1 \leq s < k'$ and hence $[k/k'] = [(ik' + s)/k'] = i$,

$$\begin{aligned}(k_1 - 1)\,k' &= ([k/k'] + 1 - 1)\,k' \\ &= ik' \\ &= k - s \\ &\leq k - 1,\end{aligned}$$

and

$$\begin{aligned}k_1 k' &= ([k/k'] + 1)\,k' \\ &= (i + 1)\,k' \\ &= ik' + k' \\ &> k. \quad \clubsuit\end{aligned}$$

Henceforth, R is a chain ring and $(R_0, \theta, m, p^n, k, \sigma, k')$ is a distinguished set of R. If $k' \mid k$, then $k_1 = k/k'$ and $k_1 = [k/k'] + 1$ otherwise.

Proposition 9. *Let R be a chain ring and $(R_0, \theta, m, p^n, k, \sigma, k')$ a distinguished set of R. Then $n = 1$ whenever $k' \nmid k$.*

Proof : Suppose that $n \neq 1$. We have $\theta^k = p\left(u_0 + u_1\theta + \cdots + u_{k-1}\theta^{k-1}\right)$, where $u_i \in R_0$, $0 \leq i \leq k - 1$ and u_0 is a unit. Let $b \in R_0$. Then

$$\begin{aligned}\theta^k b &= p\left(u_0 + u_1\theta + \cdots + u_{k-1}\theta^{k-1}\right) b \\ &= p\left(bu_0 + \sigma(b)\,u_1\theta + \cdots + \sigma^{k-1}(b)\,u_{k-1}\theta^{k-1}\right) \qquad \cdots (1)\end{aligned}$$

Also

$$\begin{aligned}\theta^k b &= \sigma^k(b)\,\theta^k \\ &= p\sigma^k(b)\left(u_0 + u_1\theta + \cdots + u_{k-1}\theta^{k-1}\right) \\ &= p\left(\sigma^k(b)\,u_0 + \sigma^k(b)\,u_1\theta + \cdots + \sigma^k(b)\,u_{k-1}\theta^{k-1}\right) \qquad \cdots (2)\end{aligned}$$

As L.H.S's of (1) and (2) are equal and the sum is direct, we get

$$pbu_0 = p\sigma^k(b)\,u_0,$$

$$\left(b - \sigma^k(b)\right) pu_0 = 0.$$

Since *char* $R \neq p$ and u_0 is a unit in R_0, by (4.10), $\sigma^k = I_{R_0}$ and hence $k' \mid k$. Thus $k' \nmid k$ implies that $n = 1$. $\clubsuit$

Corollary 10. *Let R be a chain ring and $(R_0, \theta, m, p^n, k, \sigma, k')$ a distinguished set of R. Then $k' \nmid k$ implies that R_0 is a field.*

Proof : By Proposition 9, for $k' \nmid k$, $n = 1$ and hence R_0 is a field. $\clubsuit$

Proposition 11. *Let R be a chain ring and $(R_0, \theta, m, p^n, k, \sigma, k')$ a distinguished set of R. If $\theta^k = pw$, then we can choose*

$$w = \sum_{i=0}^{k_1-1} u_{ik'}\theta^{ik'},$$

for some $u_{ik'} \in R_0$.

Proof : Let

$$w = \sum_{j=0}^{k-1} u_j\theta^j,$$

u_0 a unit in R_0, $u_j \in R_0$ for all $1 \leq j \leq k-1$. Consider $b \in R_0$.
Case I : $k' \mid k$. Then

$$\begin{aligned} pwb &= \theta^k b \\ &= \sigma^k(b)\,\theta^k \\ &= b\theta^k \\ &= bpw \\ &= pbw. \end{aligned}$$

So

$$\begin{aligned} p\left(\sum_{j=0}^{k-1} u_j\theta^j\right) b &= pb\left(\sum_{j=0}^{k-1} u_j\theta^j\right), \\ p\left(\sum_{j=0}^{k-1} \sigma^j(b)\, u_j\theta^j\right) &= p\left(\sum_{j=0}^{k-1} bu_j\theta^j\right). \end{aligned}$$

But the sum is direct, hence

$$\left(\sigma^j(b) - b\right) pu_j\theta^j = 0,$$

if $pu_j\theta^j \neq 0$, by (4.10), $\sigma^j = I_{R_0}$ and hence $k' \mid j$. As $k_1 = k/k'$, by Proposition 8, $(k_1 - 1)\,k' \leq k-1$ and $k_1k' \geq k$. So we can write

$$w = \sum_{i=0}^{k_1-1} u_{ik'}\theta^{ik'}.$$

Case II : $k' \nmid k$. Then by Proposition 9, $n = 1$. Hence $\theta^k = pw = 0$. In this case $w = 1$ is of desired type. ♣

Proposition 12. *Let R be a chain ring and $(R_0, \theta, m, p^n, k, \sigma, k')$ a distinguished set of R. Then the centralizer of R_0 in R*

$$Z_R(R_0) = \bigoplus_{i=0}^{k_1-1} R_0\theta^{ik'}.$$

Proof : For any $r \in R_0$,

$$\begin{aligned} \theta^{ik'} r &= \sigma^{ik'}(r)\,\theta^{ik'} \\ &= r\theta^{ik'}. \end{aligned}$$

So $\overset{k_1-1}{\underset{i=0}{\oplus}} R_0\theta^{ik'} \subseteq Z_R(R_0)$. Conversely, let $a = \sum_{j=0}^{k-1} a_j\theta^j \in Z_R(R_0)$, $b \in R_0$. Then

$$\begin{aligned} \sum_{j=0}^{k-1} b a_j\theta^j &= b\sum_{j=0}^{k-1} a_j\theta^j \\ &= \left(\sum_{j=0}^{k-1} a_j\theta^j\right) b \\ &= \sum_{j=0}^{k-1} \sigma^j(b)\, a_j\theta^j. \end{aligned}$$

Since the sum is direct, $\left(b - \sigma^j(b)\right) a_j\theta^j = 0$ and hence by (4.10), for $a_j\theta^j \neq 0$, $\sigma^j = I_{R_0}$, so $k' \mid j$. We get $j = ik'$, $0 \leq i \leq k_1 - 1$, whenever $a_j\theta^j \neq 0$. By Proposition 8, $(k_1 - 1)\,k' \leq k - 1$ and $k_1k' \geq k$. So

$$a = \sum_{i=0}^{k_1-1} a_{ik'}\theta^{ik'} \in \overset{k_1-1}{\underset{i=0}{\oplus}} R_0\theta^{ik'}.$$

Therefore $Z_R(R_0) \subseteq \overset{k_1-1}{\underset{i=0}{\oplus}} R_0\theta^{ik'}$. Thus

$$Z_R(R_0) = \overset{k_1-1}{\underset{i=0}{\oplus}} R_0\theta^{ik'}. \quad \clubsuit$$

Theorem 13. *Let R be a chain ring and $(R_0, \theta, m, p^n, k, \sigma, k')$ a distinguished set of R. Then the centralizer $Z_R(R_0)$ of R_0 in R is a commutative chain ring of the form $\left(Z_R(R_0), \theta^{k'}, m_1, p^n, k_1\right)$, where $m_1 = m/k'$ if $k' \mid m$, $m_1 = [m/k'] + 1$ otherwise.*

Proof : Let $a, b \in Z_R(R_0)$ such that $a = \sum_{i=0}^{k_1-1} a_i\theta^{ik'}$ and $b = \sum_{j=0}^{k_1-1} b_j\theta^{jk'}$.

Then

$$\begin{aligned} ab &= \left(\sum_{i=0}^{k_1-1} a_i\theta^{ik'}\right)\left(\sum_{j=0}^{k_1-1} b_j\theta^{jk'}\right) \\ &= \sum_{l=0}^{k_1-1}\left(\sum_{l=i+j} a_ib_j\right)\theta^{lk'} \\ &= \sum_{l=0}^{k_1-1}\left(\sum_{l=i+j} b_ja_i\right)\theta^{lk'} \\ &= \left(\sum_{j=0}^{k_1-1} b_j\theta^{jk'}\right)\left(\sum_{i=0}^{k_1-1} a_i\theta^{ik'}\right) \\ &= ba. \end{aligned}$$

Thus $Z_R(R_0)$ is a commutative subring of R. As $J(R_0) \oplus \left(\overset{k_1-1}{\underset{i=1}{\oplus}} R_0\theta^{ik'}\right) \subseteq Z_R(R_0) \cap J(R) \subseteq J(Z_R(R_0))$ and

$$\left(\overset{k_1-1}{\underset{i=0}{\oplus}} R_0\theta^{ik'}\right) / \left(J(R_0) \oplus \left(\overset{k_1-1}{\underset{i=1}{\oplus}} R_0\theta^{ik'}\right)\right) \cong \overline{R_0}$$

is a field, $Z_R(R_0)$ is a local ring with

$$J(Z_R(R_0)) = J(R_0) \oplus \left(\overset{k_1-1}{\underset{i=1}{\oplus}} R_0\theta^{ik'}\right) \qquad \cdots(1)$$

Now we have $\theta^{k'} \in J(Z_R(R_0))$ and consequently $\left\langle \theta^{k'} \right\rangle \subseteq J(Z_R(R_0))$. Also $\overset{k_1-1}{\underset{i=1}{\oplus}} R_0\theta^{ik'} \subseteq Z_R(R_0)\theta^{k'} = \left\langle \theta^{k'} \right\rangle$. If $n = 1$, then $J(R_0) = 0$, and (1) gives $J(Z_R(R_0)) = \overset{k_1-1}{\underset{i=1}{\oplus}} R_0\theta^{ik'} \subseteq \left\langle \theta^{k'} \right\rangle$. Hence in this case $J(Z_R(R_0)) = \left\langle \theta^{k'} \right\rangle$. Suppose $n > 1$. By Proposition 9, $k' \mid k$. Assume that $\theta^k = pw$ with w a unit, by Proposition 11, we can get $w = \sum_{i=0}^{k_1-1} u_i\theta^{ik'}$ a unit in $Z_R(R_0)$. So once again $p = w^{-1}\theta^k \in \left\langle \theta^{k'} \right\rangle$ and (1) gives $J(Z_R(R_0)) \subseteq \left\langle \theta^{k'} \right\rangle$. Hence $J(Z_R(R_0)) = \left\langle \theta^{k'} \right\rangle$ a nilpotent ideal with m_1 the index of nilpotency, where $m_1 = m/k'$ if $k' \mid m$, $m_1 = [m/k'] + 1$ otherwise . By (1.24) , $Z_R(R_0)$ is a commutative chain ring. ♣

5.2 The centre of a chain ring

Definition 14. Let R be a ring and $\sigma \in Aut\ R$. Then the subring

$$R^\sigma = \{r \in R : \sigma(r) = r\}$$

of R is called a *fixed subring of R under σ*. Indeed if R is a field, then R^{σ} is a subfield of R.

Proposition 15. *Let R be a chain ring and $(R_0, \theta, m, p^n, k, \sigma, k')$ a distinguished set of R with $R_0 = \overset{\infty}{\underset{i=1}{\cup}} P[a_i]$. Then*

$$R_0^{\sigma} = \overset{\infty}{\underset{i=1}{\cup}} P[b_i],$$

where $P[b_i] = (P[a_i])^{\sigma}$ for each i.

Proof : Let $R_0 = \overset{\infty}{\underset{i=1}{\cup}} P[a_i]$ and $\overline{\sigma}$ the image of σ under the isomorphism $\gamma : Aut\ R_0 \longrightarrow Aut\ \overline{R_0}$. As $\overline{P} \cong \mathbb{Z}_p$, $\overline{P}[\overline{a_i}]$ is a finite normal extension of $\overline{P}$ and hence

$$\overline{\sigma}\left(\overline{P}[\overline{a_i}]\right) = \overline{P}[\overline{a_i}].$$

Also the fixed subfield of $\overline{P}[\overline{a_i}]$ under $\overline{\sigma}$ is a simple extension of $\overline{P}$, say $\overline{P}[\overline{c_i}]$. So $\overline{R_0}^{\overline{\sigma}} = \overset{\infty}{\underset{i=1}{\cup}} \overline{P}[\overline{c_i}]$. Let $f(x) \in P[x]$ be such that $\overline{f}(x)$ is the minimal polynomial of $\overline{c_i}$. As $\overline{c_i}$ is separable over $\overline{P}$, by (2.9), there exists a unique lift algebraic element $b_i \in \overline{c_i}$ in $P[a_i]$ such that $f(b_i) = 0$. Then $f(\sigma(b_i)) = 0$. Therefore $\overline{b_i} = \overline{c_i} = \overline{\sigma}(\overline{c_i}) = \overline{\sigma}\left(\overline{b_i}\right) = \overline{\sigma(b_i)}$. Since R_0 is a Hensel ring, by (2.4), $\sigma(b_i) = b_i$ and hence $b_i \in R_0^{\sigma}$. So $\overset{\infty}{\underset{i=1}{\cup}} P[b_i] \subseteq R_0^{\sigma}$. Conversely, let $d \in R_0^{\sigma}$. Then $d \in P[a_i]$ for some i such that $\sigma(d) = d$. So $\overline{\sigma}\left(\overline{d}\right) = \overline{\sigma(d)} = \overline{d}$ and $\overline{d} \in \overline{R_0}^{\overline{\sigma}}$, hence $\overline{d} \in \overline{P}\left[\overline{b_i}\right] \subseteq \overline{P}[\overline{a_i}]$. As $P[b_i]$ is a Galois ring and $\overline{d}$ is separable over $\overline{P}$, again by (2.9), there exists a lift algebraic element $d_1 \in \overline{d}$ in $P[b_i]$. If P is a field then $d = d_1 \in P[b_i] \subseteq R_0^{\sigma}$. Suppose that $n > 1$. Then $d - d_1 \in J(P[b_i]) = pP[b_i]$ and

$$d = d_1 + v_1 p^{s_1},$$

for some unit $v_1 \in P[a_i]$ and $s_1 \geq 1$.

$$\begin{aligned} d_1 + v_1 p^{s_1} &= d \\ &= \sigma(d) \\ &= \sigma(d_1) + \sigma(v_1) p^{s_1} \\ &= d_1 + \sigma(v_1) p^{s_1}. \end{aligned}$$

So $(v_1 - \sigma(v_1)) p^{s_1} = 0$. If $p^{s_1} = 0$, then $d = d_1 \in R_0^{\sigma}$. Suppose that $p^{s_1} \neq 0$. Then $\overline{v_1} = \overline{\sigma}(\overline{v_1})$ with $\overline{v_1} \in \overline{P}[\overline{a_i}]$ and hence $\overline{v_1} \in \overline{P}\left[\overline{b_i}\right]$. Therefore there exists an element $d_2 \in P[b_i]$ such that $v_1 = d_2 + v_2 p^{s_2}$, v_2 is a unit in $P[a_i]$ and

$$d = d_1 + d_2 p^{s_1} + v_2 p^{s_2}, \quad s_1 < s_2.$$

Continuing in this way, we get

$$d = d_1 + d_2 p^{s_1} + d_3 p^{s_2} + \cdots + d_h p^{s_{h-1}},$$

where $d_1, d_2, \cdots, d_h \in P[b_i]$ and $s_1 < s_2 < \cdots < s_{h-1} < n$. Thus $d \in P[b_i] \subseteq R_0^\sigma$ and

$$R_0^\sigma = \overset{\infty}{\underset{i=1}{\cup}} P[b_i]. \quad \clubsuit$$

Lemma 16. *Let R be a chain ring and $(R_0, \theta, m, p^n, k, \sigma, k')$ a distinguished set of R. Then $\overset{k_1-1}{\underset{i=0}{\oplus}} R_0^\sigma \theta^{ik'} \subseteq C(R)$ the centre of R. Moreover if $k' \mid m-1$, then also $(J(R))^{m-1} \subseteq C(R)$.*

Proof : Let $r = \sum_{i=0}^{k-1} r_i \theta^i \in R$. Then

$$\theta^{k'} r = \theta^{k'} \left(\sum_{i=0}^{k-1} r_i \theta^i \right) = \sum_{i=0}^{k-1} \theta^{k'} r_i \theta^i = \sum_{i=0}^{k-1} \sigma^{k'}(r_i) \theta^{k'+i} = \sum_{i=0}^{k-1} r_i \theta^{k'+i} = \left(\sum_{i=0}^{k-1} r_i \theta^i \right) \theta^{k'}.$$

Hence $\theta^{k'} \in C(R)$. Let $s \in R_0^\sigma$. Then

$$sr = s \left(\sum_{i=0}^{k-1} r_i \theta^i \right) = \sum_{i=0}^{k-1} s r_i \theta^i = \sum_{i=0}^{k-1} r_i s \theta^i = \left(\sum_{i=0}^{k-1} r_i \theta^i \right) s = rs.$$

So $\overset{k_1-1}{\underset{i=0}{\oplus}} R_0^\sigma \theta^{ik'} \subseteq C(R)$. Suppose that $k' \mid m-1$. Let $c\,(\neq 0) \in (J(R))^{m-1}$. Then there exists a unit $d \in R$ such that $c = d\theta^{m-1}$. As $d = d_0 + h$ with d_0 a unit in R_0 and $h \in J(R)$, $c = (d_0 + h)\theta^{m-1} = d_0 \theta^{m-1}$. So

$$\begin{aligned} cr &= d_0 \theta^{m-1} \left(\sum_{i=0}^{k-1} r_i \theta^i \right) \\ &= d_0 \theta^{m-1} r_0 \\ &= d_0 \sigma^{m-1}(r_0) \theta^{m-1} \\ &= d_0 r_0 \theta^{m-1} \\ &= r_0 d_0 \theta^{m-1} \\ &= \left(\sum_{i=0}^{k-1} r_i \theta^i \right) c \\ &= rc. \end{aligned}$$

Thus $k' \mid m-1$ implies that $(J(R))^{m-1} \subseteq C(R)$. $\clubsuit$

Proposition 17. *Let R be a chain ring and $(R_0, \theta, m, p^n, k, \sigma, k')$ a distinguished set of R, with $n > 1$. Let $r \in Z_R(R_0)$ such that*

$$p^l r \theta = p^l \theta r,$$

for some l, $0 \leq l < n$. Then there exist $s \in \mathfrak{S} = \overset{k_1-1}{\underset{i=0}{\oplus}} R_0^\sigma \theta^{ik'}$ and $v \in (J(R))^{m-lk-1}$ such that

$$r = s + v.$$

Proof : If $p^l\theta = 0$; *i.e.*, $m = lk + 1$, then we can choose $s = 0$, $r = v \in (J(R))^0$. Suppose that $p^l\theta \neq 0$ and $r = \sum_{i=0}^{k_1-1} r_i\theta^{ik'} \in Z_R(R_0)$. Then

$$\begin{aligned} p^l \sum_{i=0}^{k_1-1} r_i\theta^{ik'+1} &= p^l r\theta \\ &= p^l\theta r \\ &= p^l\theta\left(\sum_{i=0}^{k_1-1} r_i\theta^{ik'}\right) \\ &= p^l\left(\sum_{i=0}^{k_1-1} \theta r_i\theta^{ik'}\right) \\ &= p^l \sum_{i=0}^{k_1-1} \sigma(r_i)\,\theta^{ik'+1}. \quad \cdots(1) \end{aligned}$$

By Proposition 8, $(k_1 - 1)k' + 1 \leq k$. Suppose $(k_1 - 1)k' + 1 = k$. Then $k - k' + 1 = k$ and hence $k' = 1$. In this case $\sigma = I_{R_0}$ and $Z_R(R_0) = \mathfrak{S} = R$. So we can take $s = r \in \mathfrak{S}$, $v = 0 \in (J(R))^{m-1}$ and hence the result holds. Assume that $(k_1 - 1)k' + 1 < k$. First, we will prove that for each i,

$$r_i = s_i + u_i,$$

where $s_i \in \mathfrak{S}$ and $u_i\theta^{ik'} \in (J(R))^{m-lk-1}$. As the sum in (1) is direct, for each i,

$$(r_i - \sigma(r_i))\,p^l\theta^{ik'+1} = 0.$$

If $r_ip^l\theta^{ik'+1} = 0$, then $r_i\theta^{ik'} \in (J(R))^{m-lk-1}$ and we can take $s_i = 0$, $u_i = r_i$. Suppose that $r_ip^l\theta^{ik'+1} \neq 0$. Then $\overline{\sigma}(\overline{r_i}) = \overline{\sigma(r_i)} = \overline{r_i}$, so $\overline{r_i} \in \overline{R_0}^{\overline{\sigma}}$ and there exists $d_0 \in R_0^{\sigma}$ such that

$$r_i = d_0 + v_0p^{s_1}, \quad v_0 \text{ a unit in } R_0,\ s_1 > 0.$$

If $v_0p^{s_1+l}\theta^{ik'+1} = 0$, then $v_0p^{s_1}\theta^{ik'} \in (J(R))^{m-lk-1}$ and we stop. Suppose $v_0p^{s_1+l}\theta^{ik'+1} \neq 0$. Then $p^{s_1}\theta^{ik'} \neq 0$. As

$$\sigma(r_i) = d_0 + \sigma(v_0)\,p^{s_1},$$

$$(v_0 - \sigma(v_0))\,p^{l+s_1}\theta^{ik'+1} = (r_i - \sigma(r_i))\,p^l\theta^{ik'+1} = 0.$$

Then $\overline{\sigma}(\overline{v_0}) = \overline{\sigma(v_0)} = \overline{v_0}$. So $\overline{v_0} \in \overline{R_0}^{\overline{\sigma}}$ and there exists $d_1 \in R_0^{\sigma}$ such that

$$v_0 = d_1 + v_1p^{s_2'}, \quad v_1 \text{ a unit in } R_0,\ s_2' > 0.$$

Hence

$$r_i = d_0 + d_1p^{s_1} + v_1p^{s_2}, \quad s_2 = s_1 + s_2' > s_1.$$

If $v_1 p^{s_2+l}\theta^{ik'+1} = 0$, then $v_1 p^{s_1}\theta^{ik'} \in (J(R))^{m-lk-1}$ and we stop. Otherwise we continue in this way until we get

$$r_i = d_0 + d_1 p^{s_1} + \cdots + d_{j-1} p^{s_{j-1}} + v_j p^{s_j},$$

with $d_h \in R_0^\sigma$ for each h, $0 \leq h < j$, $v_j p^{s_j+l}\theta^{ik'+1} = 0$; *i.e.*, $v_j p^{s_j}\theta^{ik'} \in (J(R))^{m-lk-1}$. By taking $s_i = d_0 + d_1 p^{s_1} + \cdots + d_{j-1} p^{s_{j-1}}$, $u_i = v_j p^{s_j}$, we get

$$r_i = s_i + u_i, \quad \text{for each } i$$

where $s_i \in R_0^\sigma$ and $u_i\theta^{ik'} \in (J(R))^{m-lk-1}$. Now, let

$$s = \sum_{i=0}^{k_1-1} s_i\theta^{ik'},\ v = \sum_{i=0}^{k_1-1} u_i\theta^{ik'}.$$

Then

$$r = s + v$$

with $s \in \mathfrak{S} = \bigoplus_{i=0}^{k_1-1} R_0^\sigma\theta^{ik'}$ and $v \in (J(R))^{m-lk-1}$. ♣

Theorem 18. *Let R be a chain ring and $(R_0, \theta, m, p^n, k, \sigma, k')$ a distinguished set of R, with $n > 1$. Then*

$$C(R) = \mathfrak{S} + \Omega,$$

where $\mathfrak{S} = \bigoplus_{i=0}^{k_1-1} R_0^\sigma\theta^{ik'}$ and $\Omega = (J(R))^{m-1}$ if $k \mid m-1$, otherwise $\Omega = 0$.

Proof : Let $r \in C(R)$. Then $\theta r = r\theta$. As $C(R) \subseteq Z_R(R_0)$, $r \in Z_R(R_0)$ and by Proposition 17, there exists $s \in \mathfrak{S} = \bigoplus_{i=0}^{k_1-1} R_0^\sigma\theta^{ik'}$ and $v \in (J(R))^{m-1}$ such that

$$r = s + v \qquad \cdots(1).$$

Case I : $k' \nmid m-1$. Suppose on the contrary that $v = v'\theta^{m-1} \neq 0$ which implies that v' is a unit in R_0. Now $v = r - s \in Z_R(R_0)$. For any $a \in R_0$, $va = av$ and

$$\begin{aligned} av'\theta^{m-1} &= v'\theta^{m-1}a \\ &= v'\sigma^{m-1}(a)\,\theta^{m-1} \\ &= \overline{v'}\overline{\sigma^{m-1}(a)}\theta^{m-1} \\ &= \overline{\sigma^{m-1}(a)}\overline{v'}\theta^{m-1} \\ &= \sigma^{m-1}(a)\,v'\theta^{m-1}. \end{aligned}$$

So $\left(a - \sigma^{m-1}(a)\right)v'\theta^{m-1} = 0$. As $v'\theta^{m-1} \neq 0$, by (4.10), we get $\sigma^{m-1} = I_{R_0}$ and hence $k' \mid m-1$. This is a contradiction. Hence $v = 0$ and $r = s \in \mathfrak{S}$. So $C(R) \subseteq \mathfrak{S}$. But by Lemma 16, $\mathfrak{S} \subseteq C(R)$. Thus

$$C(R) = \mathfrak{S}.$$

Case II : $k' \mid m-1$. Then (1) shows that $C(R) \subseteq \mathfrak{S} + (J(R))^{m-1}$. By Lemma 16, $\mathfrak{S} + (J(R))^{m-1} \subseteq C(R)$. So in this case

$$C(R) = \mathfrak{S} + (J(R))^{m-1}. \quad \clubsuit$$

Corollary 19. *Let R be a chain ring and $(R_0, \theta, m, p^n, k, \sigma, k')$ a distinguished set of R, with $n > 1$. If $\theta^k = pw$ with $w \in Z_R(R_0)$, then there exist $w' \in \mathfrak{S} = \overset{k_1-1}{\underset{i=0}{\oplus}} R_0^{\sigma}\theta^{ik'}$ and $v \in (J(R))^{m-k-1}$ such that*

$$w = w' + v.$$

Furthermore, if $k' \nmid m-1$, then we can take $w \in \mathfrak{S}$.

Proof : By Propositions 11 and 12, if $\theta^k = pw$, then we can choose w such that $w \in Z_R(R_0)$. As

$$pw\theta = \theta^k\theta = \theta\theta^k = \theta pw = p\theta w,$$

by Proposition 17, there exists $w' \in \mathfrak{S}$ and $v \in (J(R))^{m-k-1}$ such that

$$w = w' + v.$$

If $k' \nmid m-1$, then as in Theorem 18, $v = 0$, $w = w' \in \mathfrak{S} = C(R)$. In this case $\theta^k = pw$ with $w \in C(R)$. $\clubsuit$

5.3 The structure of chain rings

Lemma 20. *Let F be an absolutely algebraic field and $F[x, \sigma, k']$ a skew polynomial ring. Then for any positive integer m*

$$F[x,\sigma,k']/\langle x^m\rangle$$

is a chain ring with distinguished set $\left(\widetilde{F}, \widetilde{x}, m, p, k, \widetilde{\sigma}, k'\right)$, where $k = m$, $\widetilde{a} = a + \langle x^m\rangle$ for all $a \in F[x,\sigma,k']$ and $\widetilde{\sigma}(\widetilde{r}) = \sigma(r) + \langle x^m\rangle$ for all $\widetilde{r} \in \widetilde{F}$.

Proof : As F is a field, $F[x, \sigma, k']$ is a right and left principle ideal domain. Let $R' = F[x, \sigma, k']/\langle x^m\rangle$. Then

$$R'/\langle \widetilde{x}\rangle \cong F$$

is a field. So $\langle \widetilde{x}\rangle$ is a maximal ideal. As $\langle \widetilde{x}\rangle$ is nilpotent with index of nilpotency m, $J(R') = \langle \widetilde{x}\rangle$ and R' is a local ring. By (1.24), R' is a chain ring. Since $R' = \widetilde{F} + J(R')$, $\widetilde{F}$ is a coefficient subfield of R'. It is clear that $\widetilde{\sigma} \in Aut\ \widetilde{F}$ and hence $(\widetilde{x}, \widetilde{\sigma})$ is a distinguished element in R' over $\widetilde{F}$. Suppose that l is the order of $\widetilde{\sigma}$ and $l < k'$. Then $l \mid k'$ and for any $r \in F$, $\widetilde{\sigma}^l(\widetilde{r}) = \widetilde{r}$. So $\sigma^l(r) - r = v(x)x^m$. If $v(x) \neq 0$, then $deg\ v(x)x^m \geq m > 0$. But $deg\left(\sigma^l(r) - r\right) \leq 0$.So $v(x)x^m = 0$, $\sigma^l(r) = r$. Therefore $k' \mid l$. This is a contradiction. Thus $l = k'$ and $\left(\widetilde{F}, \widetilde{x}, m, p, k, \widetilde{\sigma}, k'\right)$ is a distinguished set of R' with $k = m$. $\clubsuit$

Theorem 21. *Let R be a chain ring and $(F, \theta, m, p, k, \sigma, k')$ a distinguished set of R, where F is a field. Then*

$$R \cong F[x, \sigma, k'] / \langle x^m \rangle .$$

Proof : Let $R' = F[x, \sigma, k'] / \langle x^m \rangle$. Then by Lemma 20, R' is a chain ring. Now by (1.14),

$$d\left({}_F\left(F[x, \sigma, k'] / \langle x^m \rangle\right)\right) = d\left({}_F F\right) \cdot \deg\ x^m = m.$$

As $k = m$, $R = \overset{m-1}{\underset{i=0}{\oplus}} F\theta^i$ and the mapping

$$\lambda : F[x, \sigma, k'] \longrightarrow R$$

such that for any $f(x) \in F[x, \sigma, k']$, $\lambda(f(x)) = f(\theta)$ is an epimorphism. By (1.10), $d\left({}_F R\right) = d\left({}_R R\right) = m$. As $\theta^m = 0$, $\langle x^m \rangle \subseteq \ker \lambda$ and

$$d\left({}_F\left(F[x, \sigma, k'] / \langle x^m \rangle\right)\right) = m = d\left({}_F R\right)$$

implies that λ induces an isomorphism from $F[x, \sigma, k'] / \langle x^m \rangle$ onto R. ♣

Definition 22. Let $h(x) \in C(R_0[x, \sigma, k'])$ with R_0 a generalized Galois ring and $f(x) = x^k - ph(x)$, where the constant term of $h(x)$ is a unit in R_0, $k > deg\ h(x)$ and $k' \mid k$. Then the skew polynomial

$$g(x) = f(x) - \beta x^{m-1},$$

where $m - 1 \geq k$ is called an *Eisenstein polynomial* if the following hold :
(i) If $k' \nmid m - 1$, then $\beta = 0$.
(ii) If $k' \mid m - 1$, then $\beta = 0$ or a unit.
(iii) If $k' \mid m - 1$ and $m - 1 = k$, Then either $\beta = 0$ or β, $(1 - \beta)$ both are units in R.

Theorem 23. *Let $R_0[x, \sigma, k']$ be a skew polynomial ring such that R_0 is a generalized Galois ring. Then $C(R_0[x, \sigma, k']) = R_0^{\sigma}[x^{k'}]$.*

Proof : Let $f(x) = \sum_{i=0}^{h} r_i x^i \in C(R_0[x, \sigma, k'])$ and $a\,(\neq 0) \in R_0$. Then $af(x) = f(x)a$, gives $\sum_{i=0}^{h} a r_i x^i = \sum_{i=0}^{h} \sigma^i(a) r_i x^i$ so $\left(a - \sigma^i(a)\right) r_i = 0$ for $0 \leq i \leq h$. Let for some i, $r_i \neq 0$. By (4.10), $\sigma^i = I$ and hence $k' \mid i$. Therefore $f(x) \in R_0[x^{k'}]$. Again $xf(x) = f(x)x$, gives

$$\sum_{i=0}^{h} \left(\sigma(r_i) - r_i\right) x^{i+1} = 0.$$

So $\sigma(r_i) = r_i$ and $r_i \in R_0^{\sigma}$ for all i and hence $f(x) \in R_0^{\sigma}[x^{k'}]$. Thus $C(R_0[x, \sigma, k']) \subseteq R_0^{\sigma}[x^{k'}]$. Obviously $R_0^{\sigma}[x^{k'}] \subseteq C(R_0[x, \sigma, k']$. This proves the result. ♣

From Proposition 8 and Theorem 23 we get The following :

Corollary 24. *Let $R_0[x,\sigma,k']$ be a skew polynomial ring such that R_0 is a generalized Galois ring. If $g(x) \in R_0[x,\sigma,k']$ is an Eisenstein polynomial, then $g(x)$ is of the form*

$$g(x) = x^k - ph(x) - \beta x^{m-1},$$

where $h(x) = \sum_{i=0}^{k_1-1} u_i x^{ik'}$, $u_i \in R_0^{\sigma}$, u_0 is a unit, $k_1 = k/k'$. ♣

Lemma 25. *Let $R_0[x,\sigma,k']$ be a skew polynomial ring such that R_0 is a generalized Galois ring. If $g(x) = x^k - ph(x) - \beta x^{m-1} \in R_0[x,\sigma,k']$ is an Eisenstein polynomial, then*

$$\begin{aligned} \langle g(x), x^m \rangle &= g(x)R_0[x,\sigma,k'] + \langle x^m \rangle \\ &= R_0[x,\sigma,k']g(x) + \langle x^m \rangle . \end{aligned}$$

Proof : Now $k' \mid k$ and $h(x) \in C(R_0[x,\sigma,k'])$. Let $a \in R_0$. Then

$$a\left(x^k - ph(x)\right) = \left(x^k - ph(x)\right)a.$$

If $k' \nmid m-1$, then $\beta = 0$, so $a\left(\beta x^{m-1}\right) = \left(\beta x^{m-1}\right)a$. Suppose that $k' \mid m-1$, then $ax^{m-1} = x^{m-1}a$, gives $a\left(\beta x^{m-1}\right) = \left(\beta x^{m-1}\right)a$. Thus $ag(x) = g(x)a \in g(x)R_0[x,\sigma,k'] + \langle x^m \rangle$. Also

$$\begin{aligned} xg(x) &= x\left(x^k - ph(x)\right) - x\beta x^{m-1} \\ &= \left(x^k - ph(x)\right)x - \sigma(\beta)x^m \\ &= g(x)x + (\beta - \sigma(\beta))x^m \\ &\in g(x)R_0[x,\sigma,k'] + \langle x^m \rangle . \end{aligned}$$

By induction on i, we get

$$x^i g(x) \in g(x)R_0[x,\sigma,k'] + \langle x^m \rangle .$$

Thus $\langle g(x), x^m \rangle \subseteq g(x)R_0[x,\sigma,k'] + \langle x^m \rangle \subseteq \langle g(x), x^m \rangle$. Hence $\langle g(x), x^m \rangle = g(x)R_0[x,\sigma,k'] + \langle x^m \rangle$. Similarly $\langle g(x), x^m \rangle = R_0[x,\sigma,k']g(x) + \langle x^m \rangle$. ♣

Theorem 26. *Let $R_0[x,\sigma,k']$ be a skew polynomial ring such that R_0 is a generalized Galois ring. If $g(x) \in R_0[x,\sigma,k']$ is an Eisenstein polynomial, then*

$$R' = R_0[x,\sigma,k'] / \langle g(x), x^m \rangle$$

is a chain ring with distinguished set $\left(\widetilde{R_0}, \widetilde{x}, m', p^n, k, \widetilde{\sigma}, k'\right)$, where $m' \leq m$, $\widetilde{a} = a + \langle g(x), x^m \rangle$ for all $a \in R_0[x,\sigma,k']$ and $\widetilde{\sigma}(\widetilde{r}) = \sigma(r) + \langle g(x), x^m \rangle$ for all $\widetilde{r} \in \widetilde{R_0}$.

Proof : We have

$$R' / \langle \widetilde{x}, \widetilde{p} \rangle \cong R[x,\sigma,k'] / \langle x, p \rangle \cong \overline{R}$$

is a field. So $\langle \widetilde{x}, \widetilde{p} \rangle$ is a maximal ideal. As $\widetilde{x}^m = 0$, $\langle \widetilde{x} \rangle$ is nilpotent. Hence $J(R') = \langle \widetilde{x}, \widetilde{p} \rangle$ and R' is a local ring. As $\widetilde{h(x)} + \langle \widetilde{x} \rangle$ and $\left(\widetilde{1} - \widetilde{\beta x^{m-1-k}}\right) + \langle \widetilde{x} \rangle$

are units in $R'/\langle\widetilde{x}\rangle$, by (1.3), $\widetilde{h(x)}$ and $\widetilde{1}-\widetilde{\beta x}^{m-1-k}$ are units in R'. Since $g(x)=x^k-ph(x)-\beta x^{m-1}$, $k\leq m-1$. Then

$$\widetilde{p}=\widetilde{(h(x))}^{-1}\left(\widetilde{x}^k-\widetilde{\beta x}^{m-1}\right)=\widetilde{(h(x))}^{-1}\left(\widetilde{1}-\widetilde{\beta x}^{m-1-k}\right)\widetilde{x}^k\in\left\langle\widetilde{x}^k\right\rangle\subseteq\langle\widetilde{x}\rangle.$$

If $m-1>k$, obviously $\widetilde{1}-\widetilde{\beta x}^{m-1-k}$ is a unit in R', so $\langle\widetilde{p}\rangle=\langle\widetilde{x}\rangle$. If $m-1=k$, then $\widetilde{p}=\widetilde{(h(x))}^{-1}\left(\widetilde{1}-\widetilde{\beta}\right)\widetilde{x}^k$. But by the hypothesis, $1-\beta$ is a unit. Once again, $\langle\widetilde{p}\rangle=\langle\widetilde{x}\rangle$. By (1.24), we get R' is a chain ring. Suppose that l is the order of $\widetilde{\sigma}$ and $l<k'$. Then $l\mid k'$ and for any $r\in R_0$, $\widetilde{\sigma}^l(\widetilde{r})=\widetilde{r}$. So by Lemma 25, $\sigma^l(r)-r=u(x)\left(x^k-ph(x)-\beta x^{m-1}\right)+v(x)x^m$, hence $\sigma^l(r)-r=pa\in J(R_0)$, for some $a\in R_0$ and hence $\left(\sigma^l(r)-r\right)p^{n-1}=0$. By (4.10), $\sigma^l=I_{R_0}$. Therefore $k'\mid l$. This is a contradiction. Thus $l=k'$ and $\left(\widetilde{R_0},\widetilde{x},m',p^n,k,\widetilde{\sigma},k'\right)$ is a distinguished set of R', where $m'\leq m$. ♣

Henceforth, by a chain ring (R,θ,m,p^n,k) we mean $n>1$ and hence $k'\mid k$ and $k_1=k/k'$.

Lemma 27. *Let R be a chain ring and $(R_0,\theta,m,p^n,k,\sigma,k')$ a distinguished set of R. Then there exist an Eisenstein polynomial*

$$\omega(x)=x^k-ph(x)-\beta x^{m-1}\in R_0[x,\sigma,k'],$$

such that

$$\omega(\theta)=0.$$

Proof : By Corollary 19, $\theta^k=pw$, where $w=w'+v$ with $w'=\sum_{i=0}^{k_1-1}u_i\theta^{ik'}\in\bigoplus_{i=0}^{k_1-1}R_0^{\sigma}\theta^{ik'}$, u_0 a unit and $v=\beta'\theta^{m-k-1}$. Further, we take $w=w'$ if $k'\nmid m-1$.

Case I : $k'\nmid m-1$. Then $v=0$, $\omega(x)=x^k-p\left(\sum_{i=0}^{k_1-1}u_ix^{ik'}\right)$ is an Eisenstein polynomial such that $\omega(\theta)=0$.

Case II : $k'\mid m-1$. Then $\theta^k=pw'+pv$ with $pv\in(J(R))^{m-1}$. So $pv=v'\theta^{m-1}$. If $pv=0$, $\omega(x)=x^k-p\left(\sum_{i=0}^{k_1-1}u_ix^{ik'}\right)$ is the desired Eisenstein polynomial. Suppose that $pv\neq0$. As $\theta^m=0$ and v' is a unit, $v'=\sum_{i=0}^{k-1}\beta_i\theta^i$, where $\beta_i\in R_0$ and β_0 a unit. Then $pv=v'\theta^{m-1}=\beta\theta^{m-1}$, where $\beta=\beta_0\in R_0$ is a unit. So $\theta^k=p\left(\sum_{i=0}^{k_1-1}u_i\theta^{ik'}\right)-\beta\theta^{m-1}$. Thus $\omega(x)=x^k-p\left(\sum_{i=0}^{k_1-1}u_ix^{ik'}\right)-\beta x^{m-1}$ is such that $\omega(\theta)=0$. If $m-1>k$, obviously $\omega(x)$ is an Eisenstein polynomial. Let $m-1=k$. Then $(1-\beta)\theta^k=ph(\theta)$ with $h(\theta)=\sum_{i=0}^{k_1-1}u_i\theta^{ik'}$ a unit in R since u_0 is a unit. If $1-\beta$ is not a unit, we get $p\in\left\langle\theta^{k+1}\right\rangle$. This is a contradiction. Hence $1-\beta$ is a unit. This proves that $\omega(x)$ is an Eisenstein polynomial. ♣

Henceforth, if $\theta^k = pw$, then $w = \sum_{i=0}^{k_1-1} u_i \theta^{ik'} - \beta\theta^{m-k-1}$ and

$$\omega(x) = x^k - p\left(\sum_{i=0}^{k_1-1} u_i x^{ik'}\right) - \beta x^{m-1}$$

is an Eisenstein polynomial related with w.

Theorem 28. *Let R be a chain ring and $(R_0, \theta, m, p^n, k, \sigma, k')$ a distinguished set of R. If $\omega(x)$ is the Eisenstein polynomial in $R_0[x, \sigma, k']$ related with w, then*

$$R \cong R_0[x, \sigma, k'] / \langle \omega(x), x^m \rangle .$$

Proof : As $R = \sum_{i=0}^{m-1} R_0\theta^i$ with $\theta a = \sigma(a)\theta$ for all $a \in R_0$, it is clear that the mapping

$$\lambda : R_0[x, \sigma, k'] \longrightarrow R,$$

such that for any $f(x) = \sum_{i=0}^{h} a_i x^i \in R_0[x, \sigma, k']$, $\lambda(f(x)) = f(\theta) = \sum_{i=0}^{h} a_i\theta^i$ is a ring and $R_0 - module$ epimorphism. Now $\omega(\theta) = 0$, gives $\omega(x) \in \ker \lambda$. As $\theta^m = 0$, $x^m \in \ker \lambda$. So $A = \langle \omega(x), x^m \rangle \subseteq \ker \lambda$. By Theorem 26, $T = R_0[x, \sigma, k']/A$ is a chain ring such that $\overline{T} \cong \overline{R_0}$ and $(J(T))^m = 0$. So by (1.10), $d({}_{R_0}T) = d({}_T T) \leq m$. But λ induces an epimorphism $\overline{\lambda}$ from T onto R. As $d({}_{R_0}R) = m$, $d({}_{R_0}T) \geq m$. Hence $d({}_{R_0}T) = m$. As $R_0[x, \sigma, k']/\ker \lambda \cong R$, $d({}_{R_0}(R_0[x, \sigma, k']/\ker \lambda)) = d({}_{R_0}R) = m = d({}_{R_0}(R_0[x, \sigma, k']/A))$ with $A \subseteq \ker \lambda$. This gives $A = \ker \lambda$. Thus

$$R \cong R_0[x, \sigma, k'] / \langle \omega(x), x^m \rangle .$$

This proves the Theorem. ♣

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	$\{ \sum a_1 a_2 \cdots a_m : a_1, \cdots, a_m \in I\}$	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
$Aut_T\ R$	$\left\{ \begin{array}{c} \text{the subgroup of } Aut\ R \\ \text{that fixes } T \text{ elementwise} \end{array} \right\}$	2
$J(R)$	the Jacobson radical of R	2
$(J(R))^0$	R	2
$\overline{R}$	$R/J(R)$	2
$\overline{r}$	$r + J(R)$	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
$\subseteq$	is a subset of	4

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
$F(a)$	the smallest subfield containing F and a	14
$F[a]$	the smallest subring containing F and a	14
$GF(p^n)$	the field of order p^n	14
$\|R\|$	the order of R	16

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
$a \equiv b \pmod{T}$	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*, *Warsow*, (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. Survys 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.

♣♣♣♣♣♣♣

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 Gloroius 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

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 α, $\beta \in \Lambda$, 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

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

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 $g(x)$.

i ii iii iv v vi vii viii

CHAPTER 1

Preliminaries

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. By using Hensel lemma some basic properties of lift algebraic elements are discussed in the first section of this chapter.

2.1 Unique lifting of a root and related results

Theorem I. *Let R be a ring and T a subring of R such that $T \subseteq C(R)$. Let I be a nil ideal of R, $f(x) \in T[x]$. If $\overline{f}(x) \in ((T+I)/I)[x]$ has a root $\overline{\alpha} \in \overline{R} = R/I$ such that $\overline{f'(\alpha)}$ is an invertible element in $\overline{R}$, where $f'(x)$ is the derivative of $f(x)$, then there exists a root $\beta \in \overline{\alpha}$ of f(x) in R.*

Theorem II. *Let R be a Hensel ring and $f(x)$ a monic polynomial over R. Then every non-multiple root of $\overline{f}(x)$ in $\overline{R}$ can be lifted to a unique root of $f(x)$ in R.*

Corollary III. *Let T be a commutative local ring with $J(T)$ nilpotent, and T' a local subring of T such that $J(T') = T' \cap J(T)$. Let $\overline{a} \in \overline{T}$ be separable over $\overline{T'}$ and $f(x)$ a monic polynomial over T' such that $\overline{f}(x)$ the minimal polynomial of $\overline{a}$. Then there exist unique $b \in \overline{a}$ such that $f(b) = 0$.*

2.2 Extensions of a special primary ring

Certain special primary rings are studied in this section.

Proposition IV. *Let R be a local ring with $J(R)$ a nil ideal and $a \in R$ a lift algebraic element over P.*

(i) If char $R = 0$, then $P[a]$ is a field;

(ii) If char $R = p^n$, then $P[a]$ is a Galois ring of the form $GR(p^n, r)$, where r is the degree of a over P.

Proposition V. *Let R be a commutative local ring such that $\overline{R}$ is an absolutely algebraic field, $J(R)$ a nilpotent ideal.*

(i) If char $R = 0$, T a subfield of R and $b \in R$ a lift algebraic element over P. Then $T[b]$ is a subfield of R

(ii) If char $R = p^n$, T a Galois subring in R and $b \in R$ a lift algebraic element over P. Then $T[b]$ is a Galois subring in R .

2.3 Generalized Galois rings

in this 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 :

Theorem VI. *Let R, R' be two generalized Galois rings such that char R = char $R' = p^n$. Then R, R' are isomorphic if and only if*

$$\overline{R} \cong \overline{R'}.$$

Theorem VII. *Let R_0 be a generalized Galois ring. Then*

$$Aut\ \overline{R_0} \cong Aut\ R_0.$$

CHAPTER 3

Coefficient Subring

It is a consequence of Cohen's structure Theorem for complete local rings that every finite commutative ring R of characteristic p^n contains a unique special primary subring R_0 satisfying $R/J(R) \cong R_0/pR_0$. Cohen called R_0 the coefficient ring of R. Actually the existence and structure of R_0 for finite commutative local ring R was known to Krull as early as 1924. For finite commutative local ring it turns out that R_0 is a Galois ring. Clark (1972) proved that a coefficient subring of finite $p-ring$ R is a direct sum of full matrix rings over Galois rings. Finally Corbas manages to characterize coefficient subring of a finite ring as a direct sum of full matrix rings over Galois rings.

Let R be an artinian local duo ring such that $\overline{R}$ is an absolutely algebraic field.

3.1 Absolutely algebraic fields

In this section of this chapter, we prove the following :

Theorem I. *Let R be an arinian local duo ring such that $\overline{R}$ is an absolutely algebraic field. Then R has a coefficient subring, which is a field if char $R = 0$ and a generalized Galois ringaccording otherwise.*

Theorem II*Let R be a local ring with char $R = p^n$. Then R is a generalized Galois ring if and only if $J(R) = pR$ and $\overline{R}$ is an absolutely algebraic field.*

Theorem III. *Let R be an arinian local duo ring with char $R = p^n$ and $\overline{R}$ an absolutely algebraic field. Then any coefficient subring of R is a generalized Galois ring. Moreover any two coefficient subrings of R are isomorphic.*

3.2 Transcendental extensions

In this section, we prove the following :

Theorem IV. *Let R be an artinian local duo ring with $\overline{R}$ a simple transcendental extension of an absolutely algebraic field. Then R has a coefficient subfield .*

Definition V. Let R be a commutative local ring and K a generalized Galois subring of R. Then R is called *a simple transcendental extension of K*

if R is the ring of qoutients $K[\alpha]_{\mathcal{P}}$, where α is transcendental element over K and $\mathcal{P} = pK[\alpha]$, where *char* $K = p^n$.

Theorem VI. *Let R be a local ring with char $R = p^n$. Then R is a simple transcendental extension of a generalized Galois ring if and only if $J(R) = pR$ and $\overline{R}$ is a simple transcendental field extension of an absolutely algebraic field.*

Theorem VII. *Let R be an artinian local duo ring with char $R = p^n$ and $\overline{R}$ a simple transcendental field extension of an absolutely algebraic field. Then any coefficient subring of R is a simple transcendental extension of a generalized Galois subring. Moreover any two coefficient subrings of R are isomorphic.*

CHAPTER 4

Distinguished Basis

Corbas, and Wirt proved that if R is a finite local ring and R_0 its coefficient subring then there exist $\pi_1, \pi_2, \cdots, \pi_n$ in $J(R)$ and $\sigma_1, \sigma_2, \cdots, \sigma_n$ in $Aut\ R_0$ such that

$$R = R_0 \oplus \sum_{i=1}^{n} R_0 \pi_i$$

and

$$\pi_i r = \sigma_i (r) \pi_i,$$

for each $r \in R_0$ and for all $i = 1, \cdots, n$. Alkhamees proved that these automorphisms are uniquely determined by R and R_0.

In this chapter, we manage to generalize these results to the case where R is an artinian local duo ring with $\overline{R}$ an absolutely algebraic field.

4.1 Distinguished basis

Definition I. Let R be a ring, $\mathfrak{M}$ an $(R, R) - bimodule$.

(i) An element $s \in \mathfrak{M}$ is called a *distinguished element of* $\mathfrak{M}$ over R if there exists an automorphism σ of the ring R such that

$$sr = \sigma(r)\, s$$

for all $r \in R$ and it is denoted by (s, σ).

(ii) A set $\{(s_1, \sigma_1), \cdots, (s_h, \sigma_h)\}$ of distinguished elements of $\mathfrak{M}$ over R is called a *distinguished* $R-basis$ of $\mathfrak{M}$ if

$$\mathfrak{M} = \overset{h}{\underset{i=1}{\oplus}} Rs_i.$$

Theorem II. *Let* R_0 *be a generalized Galois ring,* $\mathfrak{M}$ *an* $(R_0, R_0)-$ *bimodule having a finite composition length as an* R_0-*module. Then* $\mathfrak{M}$ *has a distinguished* R_0-*basis.*

Definition III. Let R_0 be a generalized Galois ring and $\mathfrak{M}$ an $(R_0, R_0)-$ *bimodule* having a finite composition length as an R_0-*module.* According to the last theorem $\mathfrak{M}$ has $\{(s_{i,j}, \sigma_i) : 1 \leq i \leq \mathfrak{X}_d,\ 1 \leq j \leq n(i)\}$ a distinguished R_0-*basis* of $\mathfrak{M}$. We shall prove in the following theorem that the automorphisms of R_0 $\{\sigma_i : 1 \leq i \leq \mathfrak{X}_d\}$ are uniquely determined by $\mathfrak{M}$. Thus we call such automorphisms *the associated automorphisms with* $\mathfrak{M}$.

Theorem IV. *Let* R_0 *be a generalized Galois ring and* $\mathfrak{M}$ *an* $(R_0, R_0)-$ *bimodule with* $d({}_{R_0}\mathfrak{M})$ *finite. Then the associated automorphisms with* $\mathfrak{M}$ *are*

uniquely determined by $\mathfrak{M}$.

Theorem V. (i) *Let* R_0 *be a generalized Galois ring and* $\mathfrak{M}$ *an* $(R_0, R_0)-$ *bimodule with* $d({}_{R_0}\mathfrak{M})$ *finite. Let* $\sigma_1, \cdots, \sigma_h$ *be the associated automorpisms with* $\mathfrak{M}$ *and*

$$\mathfrak{M} = \mathfrak{M}_1 \oplus \cdots \oplus \mathfrak{M}_h$$

such that for any $s \in \mathfrak{M}_i$, $1 \leq i \leq h$ *and* $a \in R_0$, $sa = \sigma_i(a)\, s$. *Then any* $s \in \mathfrak{M}$ *is in* $\mathfrak{M}_i$ *if and only if* $sa = \sigma_i(a)\, s$ *for all* $a \in R_0$.

(ii) *Let* $T = \{(s_{i,j}, \sigma_i) : 1 \leq i \leq h,\ 1 \leq j \leq n(i)\}$ *and* $N = \{(u_{i,j}, \delta_i) : 1 \leq i \leq h,\ 1 \leq j \leq m(i)\}$ *be two distinguished* $R_0 -$ *basis of* $\mathfrak{M}$. *Then* $n(i) = m(i)$ *for all* $1 \leq i \leq h$.

4.2 Distinguished basis for a local ring over its coefficient subring

Proposition VI. *Let* R *be an artinian local duo ring such that* $\overline{R}$ *is an absolutely algebraic field of non-zero characteristic and* R_0 *a coefficient subring of* R. *Then*

$$R = \bigoplus_{i=1}^{\mathfrak{X}_d} \left(\bigoplus_{j=1}^{n(i)} R_0 s_{i,j} \right)$$

such that $\{(s_{i,j}, \sigma_i) : 1 \leq i \leq \mathfrak{X}_d,\ 1 \leq j \leq n(i)\}$ *is a distinguished* $R_0 -$ *basis*

of R and $\sigma_1 = I_{R_0}$. Further,

$$Z_R(R_0) = \overset{n(1)}{\underset{j=1}{\oplus}} R_0 s_{1,j}.$$

Theorem VII. *Let R be an artinian local duo ring such that $\overline{R}$ is an absolutely algebraic field of non-zero characteristic. Then*

$$R = R_0 \oplus \mathfrak{T}$$

as an $(R_0, R_0)-$bimodule, where R_0 is a coefficient subring of R and $\mathfrak{T} \subseteq J(R)$.

Definition VIII. Let R be an artinian local duo ring such that $\overline{R}$ is an absolutely algebraic field of non-zero characteristic. Then

$$R = R_0 \oplus \mathfrak{T}$$

as an $(R_0, R_0) - bimodule$, where R_0 is a coefficient subring of R and $\mathfrak{T} \subseteq J(R)$. Suppose

$$T = \{(\pi_{i,j}, \sigma_i) : 1 \leq i \leq \mathfrak{X}_d,\ 1 \leq j \leq n\,(i)\}$$

is a distinguished $R_0 - basis$ of $\mathfrak{T}$. We call T *a distinguished basis of R over R_0* and we call $\sigma_1, \cdots, \sigma_{\mathfrak{X}_d}$ *the distinct associated automorphisms of R with respect to R_0.*

Theorem IX. *Let R be an artinian local duo ring such that $\overline{R}$ is an absolutely algebraic field of non-zero characteristic. Then R has a distinguished*

basis over its coefficient subring R_0 and the distinct associated automorphisms of R with respect to R_0 are uniquely determined by R and R_0.

CHAPTER 5

The Structure Of Chain Rings

Finite chain rings have been studied by quite many mathematicians. As regards to the construction of finite chain rings, Wirt had shown that a finite chain ring is a quotient of a skew polynomial ring over a Galois ring by an ideal of special form depending upon an Eisenstein polynomial; this construction was also almost achieved by Nechaev. Alkhamees proved that the centralizer of a coefficient subring R_0 of a finite chain ring is a maximal commutative chain subring $Z_{R_0}(R)$ and he managed to determine the structure of finite chain rings in terms of a quotient of skew polynomial ring over its centralizer.

In this chapter, we manage to generalize Alkhamees results involving the centralizer of a coefficient subring and the centre of finite chain ring to the case of a chain ring R such that $\overline{R}$ is absolutely algebraic. We also manage to determine the structure of such chain rings as quotients of skew polynomial ring over generalized Galois ring by an ideal of special form depending upon an Eisenstein polynomial. This construction is a generalization of the one given by Wirt for finite chain rings.

5.1 The centralizer of a coefficient subring

Theorem I. *Let (R, θ, m, p^n, k) be a chain ring with R_0 a coefficient subring of R. Then*

(i) $\theta^k = p\left(u_0 + u_1\theta + \cdots + u_{k-1}\theta^{k-1}\right)$, *where* $u_i \in R_0$ *for* $0 \leq i \leq k-1$ *and* u_0 *is a unit.*

(ii) $m = (n-1)\,k + t$, $1 \leq t \leq k$.

(iii) There are $R_0 -$ *module isomorphisms,*

$$R_0\theta^i \cong R_0, \text{ for } i = 1, \cdots, t-1$$

$$R_0\theta^i \cong R_0 p, \text{ for } i = t, \cdots, k.$$

Lemma II. *Let (R, π, m, p^n, k) be a chain ring with R_0 a coefficient subring of R. Then there exist $\theta \in J(R) \setminus (J(R))^2$ and $\sigma \in$ Aut R_0 such that (θ, σ) is a distinguished element in R over R_0. Furthermore $\sigma, \sigma^2, \cdots, \sigma^{k'-1}$ are the distinct associated automorphisms of R with respect to R_0, where k' is the order of σ.*

Definition III. Let R be a chain ring. Then $(R_0, \theta, m, p^n, k, \sigma, k')$ is called a *distinguished set of* R if (R, θ, m, p^n, k) is a chain ring, where R_0 is a coefficient subring of R, (θ, σ) is a distinguished element of R over R_0 and k' is

the order of σ.

Theorem IV. *Let R be a chain ring and $(R_0, \theta, m, p^n, k, \sigma, k')$ a distinguished set of R. Then*

$$R = R_0 \oplus R_0\theta \oplus \cdots \oplus R_0\theta^{k-1},$$

and

$$J(R) = J(R_0) \oplus R_0\theta \oplus \cdots \oplus R_0\theta^{k-1}$$

as an $(R_0, R_0) - bimodule$.

Proposition V. *Let R be a chain ring and $(R_0, \theta, m, p^n, k, \sigma, k')$ a distinguished set of R. If $\theta^k = pw$, then we can choose*

$$w = \sum_{i=0}^{k_1-1} u_{ik'}\theta^{ik'},$$

for some $u_{ik'} \in R_0$.

Proposition VI. *Let R be a chain ring and $(R_0, \theta, m, p^n, k, \sigma, k')$ a distinguished set of R. Then the centralizer of R_0 in R*

$$Z_R(R_0) = \overset{k_1-1}{\underset{i=0}{\oplus}} R_0\theta^{ik'}.$$

Theorem VII. *Let R be a chain ring and $(R_0, \theta, m, p^n, k, \sigma, k')$ a distinguished set of R. Then the centralizer $Z_R(R_0)$ of R_0 in R is a commutative*

chain ring of the form $\left(Z_R(R_0), \theta^{k'}, m_1, p^n, k_1\right)$, *where* $m_1 = m/k'$ *if* $k' \mid m$, $m_1 = [m/k'] + 1$ *otherwise.*

5.2 The centre of a chain ring

Theorem VIII . *Let* R *be a chain ring and* $(R_0, \theta, m, p^n, k, \sigma, k')$ *a distinguished set of* R, *with* $n > 1$. *Then*

$$C(R) = \mathfrak{S} + \Omega,$$

where $\mathfrak{S} = \bigoplus_{i=0}^{k_1-1} R_0^{\sigma}\theta^{ik'}$ *and* $\Omega = (J(R))^{m-1}$ *if* $k \mid m-1$, *otherwise* $\Omega = 0$.

Corollary IX. *Let* R *be a chain ring and* $(R_0, \theta, m, p^n, k, \sigma, k')$ *a distinguished set of* R, *with* $n > 1$. *If* $\theta^k = pw$ *with* $w \in Z_R(R_0)$, *then there exist* $w' \in \mathfrak{S} = \bigoplus_{i=0}^{k_1-1} R_0^{\sigma}\theta^{ik'}$ *and* $v \in (J(R))^{m-k-1}$ *such that*

$$w = w' + v.$$

Furthermore, if $k' \nmid m-1$, *then we can take* $w \in \mathfrak{S}$.

5.3 The structure of chain rings

Theorem X. *Let* R *be a chain ring and* $(F, \theta, m, p, k, \sigma, k')$ *a distinguished*

set of R, where F is a field. Then

$$R \cong F[x, \sigma, k'] / \langle x^m \rangle .$$

Conversely, if $F[x, \sigma, k']$ is a skew polynomial ring over an absolutely algebraic field F. Then for any positive integer m

$$F[x,\sigma, k'] / \langle x^m \rangle$$

is a chain ring with distinguished set $\left(\widetilde{F}, \widetilde{x}, m, p, k, \widetilde{\sigma}, k'\right)$, where $k = m$, $\widetilde{a} = a + \langle x^m \rangle$ for all $a \in F[x, \sigma, k']$ and $\widetilde{\sigma}(\widetilde{r}) = \sigma(r) + \langle x^m \rangle$ for all $\widetilde{r} \in \widetilde{F}$.

Definition XI. Let $h(x) \in C(R_0[x, \sigma, k'])$ with R_0 a generalized Galois ring, where the constant term of $h(x)$ is a unit in R_0, . Then the skew polynomial

$$g(x) = x^k - ph(x) - \beta x^{m-1},$$

where $k > deg\ h(x)$, $k' \mid k$ and $m - 1 \geq k$ is called an *Eisenstein polynomial* if the following hold :

(i) If $k' \nmid m - 1$, then $\beta = 0$.

(ii) If $k' \mid m - 1$, then $\beta = 0$ or a unit.

(iii) If $k' \mid m - 1$ and $m - 1 = k$, Then either $\beta = 0$ or β, $(1 - \beta)$ both are units in R.

Theorem XII. *Let $R_0[x, \sigma, k']$ be a skew polynomial ring such that R_0 is a generalized Galois ring. If $g(x) \in R_0[x, \sigma, k']$ is an Eisenstein polynomial,*

then

$$R' = R_0[x, \sigma, k'] / \langle g(x), x^m \rangle$$

is a chain ring with distinguished set $\left(\widetilde{R_0}, \widetilde{x}, m', p^n, k, \widetilde{\sigma}, k'\right)$, *where* $m' \leq m$, $\widetilde{a} = a + \langle g(x), x^m \rangle$ *for all* $a \in R_0[x, \sigma, k']$ *and* $\widetilde{\sigma}(\widetilde{r}) = \sigma(r) + \langle g(x), x^m \rangle$ *for all* $\widetilde{r} \in \widetilde{R_0}$.

Lemma XIII. *Let* R *be a chain ring and* $(R_0, \theta, m, p^n, k, \sigma, k')$ *a distinguished set of* R *with* $n > 1$. *Then there exist an Eisenstein polynomial*

$$\omega(x) = x^k - ph(x) - \beta x^{m-1} \in R_0[x, \sigma, k'],$$

such that

$$\omega(\theta) = 0.$$

Theorem XIV. *Let* R *be a chain ring and* $(R_0, \theta, m, p^n, k, \sigma, k')$ *a distinguished set of* R. *If* $\omega(x)$ *is the Eisenstein polynomial in* $R_0[x, \sigma, k']$ *such that* $\omega(\theta) = 0$, *then*

$$R \cong R_0[x, \sigma, k'] / \langle \omega(x), x^m \rangle .$$

Recently bilt classifying interest role aim particular