AIMS Mathematics, 7(4): 5106–5116.
DOI:10.3934/math.2022284
Received: 21 October 2021
Revised: 09 December 2021
Accepted: 13 December 2021
Published: 30 December 2021

http://www.aimspress.com/journal/Math

Research article

Classification of chain rings

Yousef Alkhamees and Sami Alabiad*

Department of Mathematics, King Saud University, Riyadh 11451, Saudi Arabia

* **Correspondence:** Email: ssaif1@ksu.edu.sa.

Abstract: An associative Artinian ring with an identity is a chain ring if its lattice of left (right) ideals forms a unique chain. In this article, we first prove that for every chain ring, there exists a certain finite commutative chain subring which characterizes it. Using this fact, we classify chain rings with invariants p, n, r, k, k', m up to isomorphism by finite commutative chain rings ($k' = 1$). Thus the classification of chain rings is reduced to that of finite commutative chain rings.

Keywords: local ring; chain ring; Galois ring; p-adic field; isomorphism class
Mathematics Subject Classification: 16L30, 16P20, 16P30

1. Introduction

We consider only associative Artinian rings with identity. A chain ring is a ring whose left (right) ideals form a unique chain under inclusion. It turned out that a ring is a chain ring if and only if it is a principal local ring. Finite chain rings arise naturally in at least four different places: in algebraic number theory [17]; in commutative algebra [10]; in geometry [15]; in coding theory [11,19]. One remarkable class that nicely exemplifies this applicability is the class of the commutative rings $\mathbb{Z}_{p^n}[x]/(g(x))$, where $g(x)$ is a monic polynomial of degree r over $\mathbb{Z}_{p^n}$ irreducible modulo p. Such rings are uniquely determined by p, n, r and their groups of automorphisms are cyclic of order r. Moreover, these rings have a lot in common with Galois fields, and thus they are called Galois rings and denoted by $GR(p^n, r)$ (see Krull [16]).

For a general review of chain rings, we refer to [2, 4, 5, 7, 9, 10, 16, 20]. Let R denote a finite chain ring of characteristic p^n with nonzero (Jacobson) radical $J(R)$ of nilpotency index m, i.e., $| R |= p^{mr}$ and $R/J(R)$ is a field of order p^r. R contains a subring (coefficient subring) R_0 of the form $R_0 = GR(p^n, r) \cong \mathbb{Z}_{p^n}[a]$, where a is an element of R_0 of multiplicative order $p^r - 1$. Additionally, there exist $\pi \in J(R) \setminus J^2(R)$ and $\sigma \in Aut\ R_0$ such that $J(R) = \pi R$ and $\pi u = \sigma(u)\pi$, for each $u \in R_0$. The automorphism σ is uniquely determined by R and R_0, and it is called the associated automorphism of

R with respect to R_0. If k is the greatest integer i, $i \leq m$, such that $p \in J^i(R)$, then R is expressed as:

$$R = \oplus_{i=0}^{k-1} R_0 \pi^i$$

(as R_0-module). It follows that $\pi^k = p\sum_{i=0}^{k-1} u_i \pi^i$, where $u_i \in R_0$ and u_0 is a unit. This means, π is a root of an Eisenstein polynomial over R_0 of the form $g(x) = x^k - p\sum_{i=0}^{k-1} u_i x^i$. If $n > 1$, then $\sigma^k = Id$ and $k' \mid k$, where k' is the order of σ. Furthermore, $m = (n-1)k + t$ for some t, $1 \leq t \leq k$. The integers p, n, r, k, k', m are called the *invariants* of R. The case when $k' = 1$, R is commutative.

Clark and Liang [8] determined the enumeration of finite chain rings with given invariants when $k' = 1$ and $p \nmid k$. This enumeration was generalized by Alkhamees [5] to finite chain rings with $k' \geq 1$ and $p \nmid k$. Moreover, Hou [13] classified finite pure chain rings up to isomorphism in case of $k' = 1$, $p - 1 \nmid k$ and $p \parallel k$ ($p \mid k$ but $p^2 \nmid k$). Recently, Alabiad and Alkhamees [1] investigated generally the number of isomorphism classes of finite commutative chain rings with the same invariants, and gave their number in case $(p-1) \nmid k$. That motivates us to classify chain rings with invariants p, n, r, k, k', m up to isomorphism. We first demonstrate that there exists a certain finite commutative chain subring of any finite chain ring which characterizes it. Using this, we determine the number of isomorphism classes of finite chain rings with fixed invariants p, n, r, k, k', m. Furthermore, we give a classification of chain rings in which their residue fields are absolutely algebraic.

2. Preliminaries

In this section, we state some facts and introduce notations used in the subsequent discussions. In the sequel, R is a finite chain ring with invariants p, n, r, k, k', m. Let R_1 be the centralizer of R_0 in R, then from [5],

$$R_1 = \oplus_{i=0}^{k_1-1} R_0 \pi^{ik'}, \tag{2.1}$$

where $k_1 = \frac{k}{k'}$ and $m_1 = \lfloor \frac{m}{k'} \rfloor + 1$. By (2.1), the radical of R_1, $J(R_1) = \pi^{k'} R_1$. However, it turned out that R_1 is a commutative chain ring with invariants p, n, r, k_1, m_1. In addition, R_1 is the only maximal commutative subring of R containing R_0 and it is unique up to inner automorphisms of R.

Denote $Z(R)$ the center of R, then

$$Z(R) = \oplus_{i=0}^{k_1-1} S \pi^{k'i} + \Omega, \tag{2.2}$$

where $S = R_0^{\sigma}$ is the fixed subring by σ, $\Omega = J^{m_1-1}(R_1) = J^{m-1}(R)$ if $k' \mid (m-1)$ and $\Omega = 0$ otherwise. It is clear that $S = GR(p^n, s) = \mathbb{Z}_{p^n}[b]$, b is an element of $< a >$ of multiplicative order $p^s - 1$ and $s = r/k'$ (cf. [5]).

Let

$$R_2 = \oplus_{i=0}^{k_1-1} S \pi^{k'i}. \tag{2.3}$$

It is easy to check that $R_2 = Z(R)$ when $k' \nmid (m-1)$, and consequently $Z(R)$ is a commutative chain ring with invariants p, n, s, k_1, m_1. The case when $k' \mid (m-1)$, $Z(R) = R_2 + \Omega$ which is not a chain subring of R. However, $Z(R)/\Omega$ is a commutative chain ring with invariants p, n, s, k_1, $m_1 - 1$.

Note that $\pi^k \in Z(R)$, i.e., π^k can be written as:

$$\pi^k = \sum_{i=0}^{k_1-1} u_i \pi^{k'i} + u_{m-1}\pi^{m-1} = p\beta_1 h_1 + u_{m-1}\pi^{m-1}, \tag{2.4}$$

where $\beta_1 \in < b >$, $h_1 = 1 + \sum_{i=1}^{k_1-1} u_i' \pi^{k'i}$, $pu_i' = \beta_1^{-1} u_i$, $u_i \in S$ for $0 \le i \le k_1 - 1$ and $u_{m-1} \in < a >$ [4]. If there exists π in R such that $\pi^k = p\beta h$ for $\beta \in < a >$ and $h \in 1 + pR_0$, R is called a *pure* chain ring, and it is called *very pure* if $h = 1$.

The following statements are related to commutative chain rings ($k' = 1$) [12, 14, 18]. These rings are known to have close connections to the p-adic fields as factor-rings of the rings of integers of finite extensions of $\mathbb{Q}_p$ (the field of p-adic numbers). Indeed, the classification of finite extensions over $\mathbb{Q}_p$ is essentially equivalent to that of finite commutative chain rings. Moreover, if $U(R)$ represents the group of units of R, then $U(R) =< a > \otimes H$, where $H = 1 + J(R)$ is the p-Sylow subgroup of $U(R)$. Let $H_i = 1 + J^i(R)$, $i \in P_m = \{1, 2, \ldots, m\}$ and consider

$$H = H_1 > H_2 > H_3 > \cdots > H_m =< 1 >, \tag{2.5}$$

joined with the function j defined by:

$$j(i) = \begin{cases} \min(pi, m), & i \le k_0, \\ \min(i + k, m), & i > k_0, \end{cases} \tag{2.6}$$

where $k_0 = \lfloor \frac{k}{p-1} \rfloor$. We refer to the series (2.5) when we mention j-diagram. We call R an *incomplete* chain ring if H has an incomplete j-diagram, and R is called *complete* if H acquires a complete j-diagram in the sense that given by Ayoub [6].

All symbols shall retain their meanings throughout the article as stated above, in addition, for a given finite chain ring R, we denote T_R all pairs (R_0, π) which fulfill the above conditions.

3. Classification of finite chain rings

It is already known from [5] that the number of non-isomorphic classes of finite chain rings of characteristic p ($n = 1$) is r. Thus, from now onwards, we assume that $n > 1$.

Proposition 3.1. *Let R be a finite chain ring with invariants p, n, r, k, k', m. Then,*

$$\pi^k = p\beta h, \tag{3.1}$$

$$\begin{cases} \beta \in < a >, h = 1, & \text{if } m - 1 = k, \\ \beta \in < b >, h = h_1 + \alpha_0 \pi^{m-k-1}, & \text{otherwise}, \end{cases}$$

where $h_1 \in R_2 \cap H(R_1)$ and $\alpha_0 \in R_0$.

Proof. First, if $m - 1 = k$, i.e., $n = 2$ and $t = 1$. Since $p^{n-1}\pi^t = 0$, then $p\pi = 0$ and

$$p\beta_1 h_1 = p\beta_1 (1 + \sum_{i=1}^{k_1-1} u_i' \pi^{k'i}) = p\beta_1.$$

This means, by (2.4), $\pi^k = p\beta_1 + u_{m-1}\pi^k$ and hence, $(1 - u_{m-1})\pi^k = p\beta_1$. Thus, $\pi^k = p\beta$, where $\beta = \beta_1(1 - u_{m-1})^{-1} \in < a >$. On the other hand, if $m - 1 > k$, we consider two cases. The case when $k' \nmid (m - 1)$, the result can easily be proved since $Z(R) = R_2$. Now, assume that $k' \mid (m - 1)$, then $k' \mid (t - 1)$ because $m - 1 = (n - 1)k + t - 1$. Let $t - 1 = t_1 k'$ for some t_1 positive integer. Then,

$$u_{m-1}\pi^{m-1} = u_{m-1}\pi^{(n-1)k}\pi^{t_1 k'}$$

$$= u_{m-1}(p\beta_1 h_1 + u_{m-1}\pi^{m-1})^{n-1}\pi^{t_1 k'}$$
$$= u_{m-1}(p^{n-1}\beta_1^{n-1}h_1^{n-1})\pi^{t_1 k'}$$
$$= u_{m-1}p^{n-1}\beta_1^{n-1}\pi^{t_1 k'},$$

where $\beta_1 \in < b >$. Now, since $t_1 < k$,

$$\pi^k = p\beta_1 h_1 + u_{m-1}p^{n-1}\beta_1^{n-1}\pi^{t_1 k'}$$
$$= p\beta(h_1 + p^{n-2}u_{m-1}\beta^{n-1}\beta^{-1}\pi^{t_1 k'}) \ (n > 2)$$
$$= p\beta h,$$

where $\beta = \beta_1$, $h = h_1 + \alpha_0\pi^{m-k-1}$ and $\alpha_0 = u_{m-1}\beta^{n-1}\beta^{-1}$. □

Remark 3.1. *By the proof of the previous proposition, we can write*

$$Z(R) = R_2 + p^{n-1}R_0\pi^{t_1 k'}. \tag{3.2}$$

Remark 3.2. *Note that if $k \neq m-1$, then by the proof of Proposition 3.1,*

$$h = 1 + \sum_{i=1}^{k_1-1} u_i\pi^{ik'}, \tag{3.3}$$

where $u_i \in S$ if $i \neq t_1$ and $u_{t_1} \in R_0$. However, if $k = m-1$, ($n = 2$ and $t = 1$), in this case, take $u_{t_1} = \beta$. Let S_0 be the extension of $S = \mathbb{Z}_{p^n}[b]$ by the element u_{t_1}, and let e be its degree over S. Then, for some $c \in S_0$, $S_0 = \mathbb{Z}_{p^n}[c] = GR(p^n, r_1)$ and $r_1 = se$. Let

$$R_3 = \oplus_{i=0}^{k_1-1} S_0\pi^{ik'}. \tag{3.4}$$

It is clear that $\pi^k \in R_3$, and then R_3 is a finite commutative chain subring of R_1 with invariants p, n, r_1, k_1, m_1.

Proposition 3.2. *The following statements are equivalent:*

(i) R_2 is a subring.

(ii) σ can be extended to an automorphism of R fixing $\pi^{k'}$.

(iii) β and h can be chosen in R_2.

Proof. It is enough to prove that (i) and (ii) are equivalent. First, assume that R_2 is a subring of R. Then, it is clear that $\pi^k \in R_2$. Consider the correspondence α_σ, defined by:

$$\alpha_\sigma(\sum_{i=0}^{k-1} u_i\pi^i) = \sum_{i=0}^{k-1} \sigma(u_i)\pi^i. \tag{3.5}$$

It is obvious that α_σ is an automorphism of R with $\alpha_\sigma(\pi^{k'}) = \pi^{k'}$. Conversely, if there is an extension of σ to an automorphism ψ of R fixing $\pi^{k'}$, then

$$p\beta h = \pi^k = \psi(\pi^k) = p\sigma(\beta)\psi(h). \tag{3.6}$$

This means, $\sigma(\beta) = \beta$ and $\psi(h) = h \bmod \pi^{m-k}$. Now, if $m-1 = k$, then $h = 1$. Also if $m-1 > k$, then from (3.3), $\psi(u_{t_1}) = \sigma(u_{t_1}) = u_{t_1}$. Therefore, in either case, we have $\pi^k \in R_2$, and hence R_2 is a subring of R. □

Corollary 3.1. *$\alpha_\sigma \in Aut\ R$ if and only if R_2 is a subring of R.*

The proof of the following lemma is easy.

Lemma 3.1. *$R_3 = R_2$ if and only if $r_1 = s$.*

Definition 3.1. *Let G be a group of automorphisms of a commutative ring E. A function $f : G \to U(E)$ is called a crossed homomorphism if $f(\eta\tau) = f(\eta)\eta(f(\tau))$, where $\eta, \tau \in G$.*

Lemma 3.2. *Assume that E_1 is a commutative chain ring which is Galois extension over a commutative chain ring E_2. If f is a crossed function from G, the Galois group, into $U(E_1)$. Then, for every $\tau \in G$, there is $\delta \in U(E_1)$ such that $f(\tau) = \tau(\delta)\delta^{-1}$.*

Proof. First, we prove that if $\sum_{i=1}^{q} a_i\eta_i = 0$, then all $a_i = 0$ for distinct $\eta_i \in G$. Assume that there is minimal e such that $\sum_{i=1}^{e} a_i\eta_i = 0$ with all $a_i \neq 0$. Note that $e > 1$ since $a_i \neq 0$. Now, since $\eta_1 \neq \eta_e$, then there is $u \in E_1$ such that $\eta_1(u) \neq \eta_e(u)$. Let x be an arbitrary in E_1, then

$$\sum_{i=1}^{e} a_i\eta_i(ux) = \sum_{i=1}^{e} a_i\eta_i(u)\eta_i(x) = \sum_{i=1}^{e} a_i\eta_i(x) = 0. \tag{3.7}$$

Hence,

$$\sum_{i=1}^{e} a_i(\eta_i(u) - \eta_e(u))\eta_i(x) = \sum_{i=1}^{e-1} a_i(\eta_i(u) - \eta_e(u))\eta_i(x) = 0. \tag{3.8}$$

This contradicts the fact that e is minimal because $a_1(\eta_1(u) - \eta_e(u)) \neq 0$. To prove the lemma, we now assume f is a crossed homomorphism. Since $\sum_{\eta\in G} f(\eta)\eta \neq 0$, then if we reduce this sum to $\overline{E_1} = E_1/J(E_1)$, we obtain $\sum_{\eta\in G} f(\eta)\eta \neq 0$ since $G \cong Aut_{\overline{E_2}}\ \overline{E_1}$. This means, there is $\zeta \in U(E_1)$ such that

$$\sum_{\eta\in G} f(\eta)\eta(\zeta) = \epsilon. \tag{3.9}$$

Then, for $\tau \in G$,

$$\begin{aligned}
\tau(\epsilon) &= \tau(\sum_{\eta\in G} f(\eta)\eta(\zeta)) \\
&= \sum_{\eta\in G} \tau(f(\eta))\tau\eta(\zeta) \\
&= \sum_{\eta\in G} \tau(f(\eta))\tau\eta(\zeta) \\
&= f(\tau)^{-1} \sum_{\eta\in G} (f(\tau\eta))\tau\eta(\zeta) \\
&= f(\tau)^{-1}\epsilon.
\end{aligned}$$

Therefore, $f(\tau) = \tau(\delta)\delta^{-1}$, where $\delta = \epsilon^{-1}$. □

Definition 3.2. *Let E_1 be a commutative chain ring which is cyclic Galois over a commutative chain ring E_2. Let $G =< \chi >$ be the group of all E_2-automorphisms of E_1. Define $N_\chi(y) : U(E_1) \to U(E_2)$ as:*

$$N_\chi(y) = \prod_{\eta\in G} \eta(y), \tag{3.10}$$

N_χ is called the norm function.

Proposition 3.3. *Let E_1 be a commutative chain ring which is cyclic Galois over a commutative chain ring E_2. Let $G =< \chi >$ be the Galois group of order k'. Then,*

$$ker\ N_\chi = \{\chi(\delta)\delta^{-1} : \delta \in U(E_1)\}. \tag{3.11}$$

Proof. If $\zeta \in ker\ N_\chi$, then $N_\chi(\zeta) = 1$. Let $f(\chi^i) = N_i(\zeta) = \zeta\chi(\zeta)\ldots\chi^{i-1}(\zeta)$, then clearly f is a crossed homomorphism. By Lemma 3.2, there exists $\delta \in U(E_1)$ such that $f(\chi) = \zeta = \chi(\delta)\delta^{-1}$. Note that $N_\chi(\zeta) = N_{k'-1}(\zeta)$. □

Corollary 3.2. *With the same hypothesis of Proposition 3.3, $ker\ N_\chi \cong U(E_1)/U(E_2)$.*

Proof. Consider the map $\psi : U(E_1) \to ker\ N_\chi$ defined by: $\psi(w) = \chi(w)w^{-1}$. It is easy to check that ψ is a surjective homomorphism and $\ker\psi = U(E_2)$. □

Lemma 3.3. *Let R be a finite chain ring. Then, the homomorphism ϕ defined from $U(E_1)$ into $U(E_2)$ by: $\phi(\omega) = N_\sigma(\omega)$ is surjective, where $E_1 = R_1/J^{m_1-1}(R_1)$ and $E_2 = Z(R)/\Omega$.*

Proof. Proposition 3.3 and its corollary give $|\ U(E_1)/U(E_2)\ | = |\ ker\ N_\sigma\ |$. Thus,

$$|\ U(E_1)/ker\ N_\sigma\ | = |\ U(E_2)\ |\ . \tag{3.12}$$

This implies N_σ is surjective. □

Proposition 3.4. *A finite chain ring R is very pure if and only if its R_3 is very pure.*

Proof. Let R_3 be very pure, and let (R_0, π_1) be an element of T_{R_3} such that $\pi_1^{k_1} = p\beta$, where $\beta \in< c >$. As $(\pi_1) = (\pi^{k'}) = J^{k'}(R)$, then $\pi_1 = \beta_1\delta\pi^{k'}$, for $\beta_1 \in< b >$ and $\delta \in H(R_3) \cap Z(R)$. By Lemma 3.3, there are $\beta_2 \in< a >$ and $\zeta \in H(R_1)$ such that $\beta_1 = N_\sigma(\beta_2)$ and $\delta = N_\sigma(\zeta)$. Now, let $\theta = \beta_2\zeta\pi$, then it is easy to verify that (R_0, θ) is an element of T_R. Therefore, R is very pure. The converse is obvious. □

Remark 3.3. *If $m - 1 > k$ and R is very pure, then $R_2 = R_3$.*

Proposition 3.5. *Let R and T be two finite chain rings with invariants p, n, r, k, k', m. Then, $R \cong T$ if and only if $\sigma = \tau$ and $R_3 \cong T_3$.*

Proof. Assume that $\sigma = \tau$ and ϕ is an isomorphism from R_3 into T_3. Thus, $\phi(\pi^{k'}) = p\delta\zeta\theta^{k'}$, where $\delta \in< c >$ and $\zeta \in H(T_3)$. Moreover, $\phi(\pi^{k'}) \in Z(T)$, and then by using Lemma 3.3, there exist $\epsilon \in< a >$ and $\xi \in H(T_1)$ mod $J^{m_1-1}(T_1)$ such that $N_\sigma(\epsilon) = \delta$ and $N_\sigma(\xi) = \zeta$. Now, let η be the restriction of ϕ to S_0, and $\psi : R \to T$ defined by:

$$\psi(\sum_{i=0}^{k-1} u_i\pi^i) = \sum_{i=0}^{k-1} \mu(u_i)(\epsilon\xi\theta)^i,$$

where μ is an extension of η to R_0 which exists since S_0 is Galois subring of R_0. Then, it is easy to see that ψ is an isomorphism. The other direction is trivial. □

Corollary 3.3. *With the same assumption as in Proposition 3.5, $R_1 \cong T_1$ if and only if $R_3 \cong T_3$.*

Theorem 3.1. *If N is the number of non-isomorphic classes of finite chain rings with invariants p, n, r, k, k', m. Then,*

$$N = \phi(k')N_c, \tag{3.13}$$

where ϕ is the Euler function and N_c is the number of finite commutative chain rings with invariants p, n, r_1, k_1, m_1.

Proof. Since we have $\phi(k')$ automorphisms in $Aut\ R_0$ generate $< \sigma >$, i.e., of order k', then the result follows immediately from Proposition 3.5. □

Remark 3.4. *Let $N(r_1, k_1)$ be the number of $\mathbb{Q}_p$-isomorphic of finite extensions of $\mathbb{Q}_p$ with residue degree r_1 and ramification index k_1. Then from [1],*

$$N(r_1, k_1) = \frac{1}{\phi(k')}N, \tag{3.14}$$

where N is the number of non-isomorphic classes of finite chain rings with invariants p, n, r, k, k', m.

Next, set $d = (p^{r_1} - 1, k_1)$ and $k_1 = p^l k_2$, where $l \geq 0$ and $(p, k_2) = 1$.

Corollary 3.4 (Theorem 1, [5])**.** *Assume that $(p, k_1) = 1$, then*

$$N = \phi(k') \sum_{z|d} \frac{\phi(z)}{\tau(z)}, \tag{3.15}$$

where $\tau(z)$ is the order of p in the group of units of $\mathbb{Z}_z$.

If $(p, k_1) \neq 1$, the classification of finite commutative chain rings with invariants p, n, r_1, k_1, m_1 depends strongly on the structure of their groups of units [1].

Definition 3.3. *Let R be a finite chain ring, then we call R complete (incomplete) if its R_3 is complete (incomplete).*

The following Corollaries 3.5-3.7 depend on results from [1].

Remark 3.5. *Let U_i be the subgroup of H generated by $1 + \alpha_z \pi^i$, $1 \leq z \leq r$, where $\{\alpha_z\}_{1 \leq z \leq r}$ is a representatives system in R for a basis of the residue field over $\mathbb{Z}_p$. If R is complete, then [6],*

$$H(R_3) = \otimes_{i \notin R(j)} U_i.$$

Moreover, for each i, U_i is a homogeneous group of rank r_1 and of order $p^{\nu(i)}$, where $\nu(i)$ is the least positive integer satisfying $j^{\nu(i)}(i) = m$.

Corollary 3.5. *The number N of isomophrism classes of complete chain rings with invariants p, n, r, k, k', m is*

$$N = \phi(k')[\frac{1}{r_1} \sum_{i=0}^{r_1 - 1} (p^i - 1, d)p^{(i, r_1)\iota}], \tag{3.16}$$

where $\iota = \sum_{i \notin R(j)} l_i$ and $l_i = min\{\nu(i), l\}$.

Remark 3.6. *If R is an incomplete chain ring, the structure of $H(R_3)$ can be written [3] as:*

$$H(R_3) = \otimes_{i=1}^{i_1-1} U_i \otimes G,$$

where G is a subgroup of $H(R_3)$ and $i_1 = \frac{k_0}{p^l}$. We call R an almost complete chain ring if there exists $\pi \in R$ such that $\pi^k = p\beta h$, where $h \in \otimes_{i=1}^{i_1-1} U_i$.

Corollary 3.6. *Let N be the number of non-isomorphic classes of almost complete chain rings with invariants p, n, r, k, k', m. Then,*

$$N = \phi(k')[\frac{1}{r_1}\sum_{i=0}^{r_1-1}(p^i - 1, d)p^{(i,r_1)l(i_1-1)}]. \tag{3.17}$$

Corollary 3.7. *If N is the number of isomophrism classes of incomplete chain rings with invariants p, n, r, k, k', m. Then,*

$$\phi(k')\frac{p^{r_1}}{r_1} \leq N \leq \phi(k')(p^{r_1} - 1)p^{(m_1-k_1-1)r_1}. \tag{3.18}$$

4. The classification of chain rings whose residue fields are absolutely algebraic

Let R be a chain ring of characteristic p^n with absolutely algebraic residue field. Then [4], R has a commutative chain subring R_0 as its coefficient subring. Actually, R_0 is a union of ascending chain of Galois subrings of R of characteristic p^n, its maximal ideal generated by p, and $Aut\, R_0 \cong Aut\, (R_0/pR_0)$. Thus, in this case, we call R_0 a generalized Galois ring.

Remark 4.1. *We refer to [4], for the following facts concerning R. Let m be the index of nilpotency of J(R). There exists a pair (π, σ) such that $J(R) = R\pi$ and $\pi u = \sigma(u)\pi$ for each u in R_0, where π is an element of J(R) and $\sigma \in Aut\, R_0$. Also σ is uniquely determined by R and R_0. Thus, we call σ the associated automorphism of R with respect to R_0. Moreover, $\sigma^k = Id_{R_0}$ if $n > 1$; thus, if k' is the order σ then k' divides k. In this case, $R = \oplus_{i=0}^{k-1} R_0\pi^i$ (as R_0-module). This implies, $\pi^k = p\Sigma_{i=0}^{k-1} u_i\pi^i$, where $u_i \in R_0$ and u_0 is a unit, i.e., π is a root of Eisenstein polynomial $g(x) = x^k - p\Sigma_{i=0}^{k-1} u_i x^i$ over R_0. Assume R' is the subring of R generated by $\mathbb{Z}_{p^n}$ and π. Then it is easy to check that R' is a finite chain subring of R with invariants p, n, r, k, k', m where $R'_0 \cong GR(p^n, r) = \mathbb{Z}_{p^n}[a]$ is a coefficient subring of R' and a is an element of R'_0 of multiplicative order $p^r - 1$. We call R' the associated finite chain ring of R and the integers p, n, r, k, k', m are called invariants of R. Now, as in the finite case, $\pi^k = p\beta h$, where $\beta \in < a >$ and $h \in H(R'_1)$, R'_1 is the centralizer of R'_0 in R'.*

Proposition 4.1. *([5]) Let R be a finite local ring. Then, R is a chain ring if and only if J(R) has the maximal index of nilpotency.*

Lemma 4.1. *Let R be a finite local ring. Then, R is a chain ring if and only if there exists an element in J(R) which has the maximal index of nilpotency.*

Proof. Let R be a chain ring. Then $J(R) = R\pi$ has the maximal index of nilpotency, and thus π is the required element. Conversely, let π be an element of $J(R)$ which has the maximal index of nilpotency, say m, and let $J = \{\sum_{i=1}^{m-1} \alpha_i\pi^i : \alpha_i \in < a > \cup\{0\}\}$, then $J = J(R)$ and $| J | = | J(R) | = p^{(m-1)r}$, and subsequently $J = J(R) = R\pi$. Thus, by Proposition 4.1, R is a chain ring. □

Proposition 4.2. *Let R be an Artinian local ring of characteristic p^n in which its residue field is absolutely algebraic. Then the followings are equivalent:*

(i) R is a chain ring.

(ii) $J(R)$ has the maximal index of nilpotency.

(iii) There exists an element in $J(R)$ which has the maximal index of nilpotency.

Proof. By Remark 4.1, it follows that $J(R)$ and $J(R')$ have the same generator. Now, the proof follows from Proposition 4.1 and Lemma 4.1. □

By considering the last proposition, it is easy to check the following result.

Proposition 4.3. *Let R and T be chain rings with the same invariants p, n, r, k, k', m with $n > 1$ and in which their residue fields are absolutely algebraic. Also let R', T' be their associated finite chain subrings and K, K' be their residue fields, respectively. Then, $R \cong T$ if and only if $R' \cong T'$ and $K \cong K'$.*

By Remark 4.1 and Proposition 4.3, one can easily prove the following theorem.

Theorem 4.1. *The number of non-isomorphic chain rings with the same invariants p, n, r, k, k', m with $n > 1$ and in which their residue fields are absolutely algebraic and isomorphic is the same as the number of finite chain rings with the same invariants p, n, r, k, k', m .*

Corollary 4.1. *The number of non-isomorphic commutative chain rings with the same invariants p, n, r, k, m with $n > 1$ and in which their residue fields are absolutely algebraic and isomorphic is the same as the number of finite commutative chain rings with the same invariants p, n, r, k, m.*

Remark 4.2. *Let R be a chain ring with invariants $p, n = 1, r, k, k', m$ and its residue field F is absolutely algebraic. Then [4],*

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

Corollary 4.2. *If R is a chain ring with invariants $p, n = 1, r, k, k', m$ and in which its residue field is absolutely algebraic. Then, R is uniquely determined by its invaraints and the residue field.*

5. Conclusions

In this paper, the classification (up to isomorphism) of chain rings with same invariants is investigated. Every chain ring is characterized by a certain finite commutative chain subring. Therefore the classification of chain rings has been reduced to the classification of finite commutative chain rings.

Acknowledgments

The authors would like to thank Deanship of scientific research in King Saud University for funding and supporting this research through the initiative of DSR Graduate Students Research Support (GSR).

Conflict of interest

The authors declare that they have no conflict of interest.

References

1. S. Alabiad, Y. Alkhamees, On classification of finite commutative chain rings, *AIMS Mathematics*, **7** (2022), 1742–1757. http://dx.doi.org/10.3934/math.2022100
2. S. Alabiad, Y. Alkhamees, On automorphism groups of finite chain rings, *Symmetry*, **13** (2021), 681. http://dx.doi.org/10.3390/sym13040681
3. S. Alabiad, Y. Alkhamees, Recapturing the structure of group of units of any finite commutative chain ring, *Symmetry*, **13** (2021), 307. http://dx.doi.org/10.3390/sym13020307
4. Y. Alkhamees, H. Alolayan, S. Singh, A representation theorem for chain rings, *Collog. Math.*, **96** (2003), 103–119. http://dx.doi.org/10.4064/cm96-1-10
5. Y. Al-Khamees, The enumeration of finite principal completely primary rings, *Abh. Math. Semin. Univ. Hambg.*, **51** (1981), 226. http://dx.doi.org/10.1007/BF02941222
6. C. Ayoub, On the group of units of certain rings, *J. Number Theory*, **4** (1972), 383–403. http://dx.doi.org/10.1016/0022-314X(72)90070-4
7. W. Clark, D. Drake, Finite chain rings, *Abh.Math.Semin.Univ.Hambg.*, **39** (1973), 147–153. http://dx.doi.org/10.1007/BF02992827
8. W. Clark, J. Liang, Enumeration of finite chain rings, *J. Algebra*, **27** (1973), 445–453. http://dx.doi.org/10.1016/0021-8693(73)90055-0
9. W. Clark, A coefficient ring for finite non-commutative rings, *Proc. Amer. Math. Soc.*, **33** (1972), 25–28. http://dx.doi.org/10.2307/2038164
10. J. Fisher, Finite principal ideal rings, *Can. Math. Bull.*, **19** (1976), 277–283. http://dx.doi.org/10.4153/CMB-1976-043-1
11. M. Greferath, Cyclic codes over finite rings, *Discrete Math.*, **177** (1997), 273–277. http://dx.doi.org/10.1016/S0012-365X(97)00006-X
12. X. Hou, K. Leung, S. Ma, On the groups of units of finite commutative chain rings, *Finite Fields Appl.*, **9** (2003), 20–38. http://dx.doi.org/10.1016/S1071-5797(02)00003-5
13. X. Hou, Finite commutative chain rings, *Finite Fields Appl.*, **7** (2001), 382–396. http://dx.doi.org/10.1006/ta.2000.0317
14. K. Iwasawa, *Local class field theory*, New York: Oxford Univ Press, 1986.
15. W. Klingenberg, Projective und affine Ebenen mit Nachbarelementen, *Math. Z.*, **60** (1954), 384–406. http://dx.doi.org/10.1007/BF01187385
16. W. Krull, Algebraische theorie der ringe. II., *Math. Ann.*, **91** (1924), 1–46. http://dx.doi.org/10.1007/BF01498378
17. W. Krull, *Grundlagen und ausgangspunkte*, Berlin: Springer, 1968. http://dx.doi.org/10.1007/978-3-642-87033-0_1
18. S. Lang, *Algebraic number theory*, New York: Springer-Verlag, 1986. http://dx.doi.org/10.1007/978-1-4612-0853-2
19. X. Lui, H. Lui, LCD codes over finite chain rings, *Finite Fields Appl.*, **34** (2015), 1–19. http://dx.doi.org/10.1016/j.ffa.2015.01.004

20. B. Wirt, Finite non-commutative local rings, Ph.D Thesis, University of Oklahoma, 1972. Available from: https://shareok.org/handle/11244/3379.

AIMS Press