Mathematics

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

AIMS Mathematics, 7(2): 1742–1757.
DOI: 10.3934/math.2022100
Received: 19 February 2021
Accepted: 18 September 2021
Published: 02 November 2021

Research article

On classification of finite commutative chain rings

Sami Alabiad* **and Yousef Alkhamees**

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

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

Abstract: Let R be a finite commutative chain ring with invariants p, n, r, k, m. It is known that R is an extension over a Galois ring $GR(p^n, r)$ by an Eisenstein polynomial of some degree k. If $p \nmid k$, the enumeration of such rings is known. However, when $p \mid k$, relatively little is known about the classification of these rings. The main purpose of this article is to investigate the classification of all finite commutative chain rings with given invariants p, n, r, k, m up to isomorphism when $p \mid k$. Based on the notion of j-diagram initiated by Ayoub, the number of isomorphism classes of finite (complete) chain rings with $(p-1) \nmid k$ is determined. In addition, we study the case $(p-1) \mid k$, and show that the classification is strongly dependent on Eisenstein polynomials not only on p, n, r, k, m. In this case, we classify finite (incomplete) chain rings under some conditions concerning the Eisenstein polynomials. These results yield immediate corollaries for p-adic fields, coding theory and geometry.

Keywords: finite chain rings; p-adic fields; Galois rings; j-diagram; isomorphism class
Mathematics Subject Classification: 12J12, 13B05, 13E10

1. Introduction

We consider only commutative rings which have an identity. An associative Artinian ring with an identity whose lattice of ideals forms a unique chain is called a chain ring. It is not hard to show that a finite ring R is a chain ring if and only if its (Jacobson) radical $J(R)$ is principal and the quotient $F = R/J(R)$ is a field of order p^r, p is prime, i.e., R is a local ring. There are known positive integers p, n, r, k, m associted with R called the *invariants* of R. Ayoub [3] dubbed these rings "homogenous rings". Finite chain rings appear in various areas, for details see [4]. In particular, finite chain rings have been increasingly used in coding theory [5, 11, 14] and in geometry as coordinatizing rings of Pappian Hjelmslev planes [9]. An interesting class of finite chain rings is that contains Galois rings, i.e.,

$$GR(p^n, r) = Z_{p^n}[x]/(f(x)), \tag{1.1}$$

where $f(x)$ is a monic polynomial of degree r and irreducible modulo p. However, there are different algebraic ways to construct finite chain rings.

Let R denote a finite chain ring with invariants p, n, r, k and m, then R is an Eisenstein extension of a Galois ring $GR(p^n, r)$

$$R = GR(p^n, r)[x]/(g(x), x^m), \tag{1.2}$$

where $g(x)$ is an Eisenstein polynomial of degree k over $GR(p^n, r)$, i.e.,

$$g(x) = x^k - p\sum_{i=0}^{k-1} s_i x^i, \ \text{ where } s_0 \text{ is a unit of } GR(p^n, r). \tag{1.3}$$

However, the case when $g(x) = x^k - ps_0$, R is called a *pure* chain ring.

Another construction of R is that connected to p-adic fields; R is a factor-ring of the ring of integers of a suitable finite extension of $\mathbb{Q}_p$, the field of p-adic numbers. Let K be an extension of $\mathbb{Q}_p$ with ramification index k and residue degree r, and let L be the unramified subextension of degree r over $\mathbb{Q}_p$. Let O_K denote the ring of integers of K, and let π be a prime element of O_K. Then,

$$R \cong O_K/(\pi^m) \cong O_L/(p^n)[x]/(\overline{g}(x), x^m) \cong GR(p^n, r)[x]/(\overline{g}(x), x^m), \tag{1.4}$$

where $g(x)$ is the minimal polynomial of π over L whose image $\overline{g}(x)$ in $O_L/(p^n)[x] \cong GR(p^n, r)[x]$ is Eisenstein of degree k. We shall see later that when m is sufficiently large, the classification of $\mathbb{Q}_p$-isomorphism finite extensions of $\mathbb{Q}_p$ coincides with that of finite commutative chain rings. For the basic of p-adic fields, we refer to [8, 10].

Let $U(R)$ be the group of units of R, then

$$U(R) =< a > \otimes H, \tag{1.5}$$

where a is an element of order $p^r - 1$, and $H = 1 + J(R)$ (Ayoub [3]). The structure of H is introduced in [3] when $(p-1) \nmid k$, and given in [1] if $(p-1) \mid k$. However, it turned out that if $p \mid k$, H plays a paramount role in the enumeration of finite chain rings. Let $k = k_1 p^l$, $(p, k_1) = 1$, Hou [7] classified pure chain rings when $l = 1$ and $(p-1) \nmid k$. Moreover, if $l = 0$, the classification is independent of H, and the enumeration, in this case, was determined by Clark and Liang [4]. Our main aim in this article is to classify, in case of $p \mid k$, finite chain rings with fixed invariants p, n, r, k, m up to ismorphism by using ideas from [1, 3].

The present manuscript is organized as follows. Section 2 involves notations and known statements that will appear in the sequel. In Section 3, we consider the classification problem of finite chain rings with the same invariants p, n, r, k, m. First, we classify them when $(p-1) \nmid k$. Next, the case $(p-1) \mid k$ is investigated under certain conditions. Section 4 is devoted to apply our results in p-adic number fields.

2. Preliminaries

This section collects some facts and states notations required in our subsequent discussions.

Let R be a finite chain ring with invariants p, n, r, k and m, and nonzero radical $J(R)$ with nilpotency index m. The residue field $F = R/J(R)$ is of order p^r. We refer to [1, 3, 4, 12, 13] for the verification of the statements given here.

The ring R has a coefficient subring $S = GR(p^n, r) \cong \mathbb{Z}_{p^n}[a]$ for some a of multiplicative order $p^r - 1$. If $x \in J^i(R) \setminus J^{i+1}(R) = J_i$, we define $wt(x) = i$. Let $wt(\pi) = 1$, then, $J(R) = (\pi)$ and

$$R = \oplus_{i=0}^{k-1} S\pi^i, \tag{2.1}$$

(as $S-$module). There exists t, $1 \le t \le k$ with $m = (n-1)k + t$ such that

$$\begin{cases} S \cong S\pi^i, & \text{if } 0 \le i < t, \\ S/p^{n-1}S \cong S\pi^i, & \text{if } t \le i \le k. \end{cases} \tag{2.2}$$

Let $\pi \in J_1$ be fixed, and let $U(R)$ denote the group of units of R, then

$$U(R) = C_{p^r-1} \otimes H, \tag{2.3}$$

where $C_{p^r-1} =< a >$ is a cyclic group of order $p^r - 1$, and $H = 1 + J(R)$ is the p-Sylow subgroup of $U(R)$. Moreover, π is a root of an Eisenstein polynomial $g(x)$ (1.3), then, from (2.3),

$$\pi^k = p\beta h,\ \beta \in < a > \text{ and } h \in H. \tag{2.4}$$

Let $u = \lfloor \frac{k}{p-1} \rfloor$, where $\lfloor x \rfloor$ means the greatest positive integer less than or equal x, and let $H_s = 1 + J^s(R)$, $s \in P_m = \{1, 2, \ldots, m\}$. Consider the following filtering and (admissible) function:

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

$$j(s) = \begin{cases} \min(ps, m), & s \le u, \\ \min(s + k, m), & s > u. \end{cases} \tag{2.6}$$

The series (2.5) with j and the p-th power homomorphisms η_s from H_s/H_{s+1} into $H_{j(s)}/H_{j(s)+1}$ form the so called j-diagram, however, we refer to (2.5) when we mention j-diagram. We call the j-diagram in (2.5) incomplete at s' if $\eta_{s'}$ is not an isomorphism, and complete if all η_s are isomorphisms.

Definition 2.1. *We call R incomplete (complete) chain ring if the series (2.5) is incomplete at u (complete).*

Now, let $\{\alpha_i\}_{1\le i\le r}$ be a representatives system in R for a basis of F over $\mathbb{Z}_p$. Furthermore, let f be the homomorphism $f : F \to F$, defined by: $f(\alpha) = \alpha^p + \beta\alpha$. Let $k = k_1 p^l$ $((k_1, p) = 1)$, $\lambda = l + 1$ and $R(j)$ be the range of j, then H is generated by:

$$\begin{cases} w_{is} = 1 + \alpha_i \pi^s, \quad (i, s) \in B = \{(i, s) : 1 \le i \le r \text{ and } s \notin R(j)\}, \\ \left.\begin{cases} \gamma = 1 + \alpha_0 \pi^{up}, \\ \text{where } \alpha_1^{p^\lambda} - \beta\alpha_1^{p^{\lambda-1}} = 0 \text{ and } \alpha_0 \notin \operatorname{Im} f. \end{cases}\right\} \text{(incomplete case)} \end{cases} \tag{2.7}$$

For each $s \in P_m$, let U_s and U_s^* be subgroups of H generated by $\{w_{is}\}_{1\le i\le r}$ and $\{w_{is}\}_{2\le i\le r}$, respectively. Hence, U_s and U_s^* are homogeneous groups of rank r and $r-1$, respectively, and of order $p^{\nu(s)}$, where $\nu(s)$ is the least positive integer satisfying $j^{\nu(s)}(s) = m$. In particular,

$$U(GR(p^n, r)) = \begin{cases} U_k, & \text{if } p > 2 \text{ or } p = 2 \text{ and } n \le 2, \\ C_{2^{n-1}}^{r-1} \otimes C_{2^{n-2}} \otimes C_2, & \text{otherwise.} \end{cases} \tag{2.8}$$

Denote $c =\mid P_m \setminus R(j) \mid$, then by using j-diagram,

$$c = \begin{cases} m - \lfloor \frac{m}{p} \rfloor, & \text{if } m < k + u, \\ k, & \text{otherwise.} \end{cases} \tag{2.9}$$

Lemma 2.1 ([6]). *Let q and z be positive integers such that $q \geq z - 1$. Then, for $0 \leq b \leq p^q$,*

$$C(p^q, b) \equiv \begin{cases} 0, & \textit{if } v_p(b) \leq q - z, \\ C(p^{z-1}, i), & \textit{if } b = ip^{q-z+1}, \end{cases} \quad (mod\ p^z)$$

where v_p is the p-adic valuation.

All notations mentioned above have the same meanings throughout; in addition, we denote $l_s = min\{l, v(s)\}$.

3. Classification of finite chain rings

If $n = 1$, then $R \cong S[x]/(x^k)$, where $S = GF(p^r) = F$, i.e., R is completely determined by its invariants. Hence, in the sequel, we assume $n > 1$. Now, let

$$E(p, k) = \{\sum_{i=0}^{k-1} s_i x^i : s_i \in S, s_0 \in U(S)\}. \tag{3.1}$$

For every $\theta \in J_1$, there exists a unique defined $f(x) \in E(p, k)$ such that θ is a root of $g(x) = x^k - pf(x)$. Let $E(R)$ be the set of all such polynomials $g(x)$ (Eisenstein polynomials) corresponding to the set J_1. If $\sigma \in Aut\ S$, we denote $\sigma(E(R))$ by:

$$\sigma(E(R)) = \{\sigma(g(x)) : \sigma \text{ is applied to the coefficients of } g(x)\}. \tag{3.2}$$

The group of automorphisms of S, Aut S, is cyclic of order r generated by ρ (Frobenius map) defined as:

$$\rho(\sum_{i=0}^{n-1} \zeta_i p^i) = \sum_{i=0}^{n-1} \zeta_i{}^p p^i, \tag{3.3}$$

where $\zeta_i \in \Gamma(r)$, the Teichmüller set of S. Furthermore, Aut $(S/p^i S) \cong$ Aut S (by the natural isomorphism).

If $g(x) \in E(R)$, we denote R_g by:

$$R_g = S[x]/(g(x), x^m). \tag{3.4}$$

Remark 3.1. *If $g(x) \in E(R)$, then $R \cong R_g$.*

Proposition 3.1. *Let R and T be two finite chain rings with the same invariants and same coefficient subring S. Then, $R \cong T$ if and only if $\sigma(E(R)) \cap E(T) \neq \phi$ for some $\sigma \in Aut\ S$.*

Proof. Assume that $R \cong T$ and ψ is the isomorphism. Let $\psi\ |_S = \sigma$ and π be a root of $g(x) \in E(R)$. Then, it is easy to justify that $\psi(\pi)$ is a root of $\sigma(g(x))$ in T. Thus, $\sigma(g(x)) \in E(T)$, and so $\sigma(E(R)) \cap E(T) \neq \phi$. Conversely, if $\sigma(g(x))$ has a root θ in T for some $\sigma \in Aut\ S$ and $g(x) \in E(R)$. Then, the corresponding $\psi(\sum s_i \pi^i) = \sum \sigma(s_i)\theta^i$ is obviously an isomorphism. □

Corollary 3.1. *$\sigma(E(R)) \subseteq E(R)$ for every $\sigma \in Aut\ S$.*

Proposition 3.2. *For any finite chain rings R and T, either $E(R) \cap E(T) = \phi$ or $E(R) = E(T)$.*

Proof. If $E(R) \cap E(T) \neq \phi$, then Proposition 3.1 concludes that $R \cong T$ and, hence, $E(R) = E(T)$. □

Corollary 3.2. *$R \cong T$ (not isomorphic) if and only if $E(R) = E(T)$ ($E(R) \cap E(T) = \phi$).*

3.1. Complete chain rings

Let R be a complete chain ring, then (cf. [1]) the system $\{w_{is}\}$ in (2.7) forms a basis for H, and by (Theorem 3, [3]),

$$H = \otimes_{s \notin R(j)} U_s. \tag{3.5}$$

Let R and T be two complete chain rings with the same invariants p, n, r, k, m. Assume that $\pi^k = p\beta_1 h_1$ and $\theta^k = p\beta_2 h_2$ for R and T, respectively. If $R \cong T$, then via Proposition 3.1, there is $\sigma \in Aut\ S$ such that $\sigma(g(x)) = x^k - p\sigma(f(x))$ has a root in R, where $g(x) \in E(T)$. This means, there is $\zeta = \pi\beta\delta$, where $\delta \in H_R$ and $\beta \in < a >$ such that

$$p\sigma(\beta_2)\sigma(h_2) = \zeta^k = (\pi\beta\delta)^k = p\beta_1 h_1 \beta^k \delta^k. \tag{3.6}$$

Observe that, σ can be considered isomorphism maps θ to ζ (proof of Proposition 3.1). Therefore,

$$\beta^{k_1} = \beta_1^{-1}\sigma(\beta_2), \tag{3.7}$$

$$\delta^{p^l} = h_1^{-1}\sigma(h_2) \quad mod\, \pi^{m-k}. \tag{3.8}$$

Thus, we consider the invariants, $p, n-1, r, k, m$. From Eq (3.8), $h_1 = \sigma(h_2)\ mod\, H^{p^l}$, i.e., in H/H^{p^l}, we have

$$h_1 = \sigma(h_2). \tag{3.9}$$

Since we have the same structure for H_R and H_T, then

$$u_s = \sigma(w_s), \tag{3.10}$$

where $h_1 = \prod_{s \notin R(j)} u_s$ and $h_2 = \prod_{s \notin R(j)} w_s$. By (2.9), there are exactly c equations of the form (3.10). Moreover, since $u_s, w_s \in U_s$, then $u_s = \prod_{i=1}^{r} w_{is}^{a_i}$ and $w_s = \prod_{i=1}^{r} (1 + \alpha_i \theta^s)^{m_i}$, where a_i and m_i are considered $mod\ p^l$, i.e., $a_i, m_i \in \mathbb{Z}_{p^l}$. For the converse, assume (3.7) and (3.10) hold for all $s \in P_m \setminus R(j)$ and some $\sigma \in Aut\ S$. Then, there exist $\beta \in < a >$ and $\delta \in H_R$ such that

$$\psi(\theta^k) = p\psi(\beta_2 h_2) = p\beta_1 h_1 \beta^k \delta^k = (\pi\beta\delta)^k = \pi_1^k, \tag{3.11}$$

where ψ is the corresponding:

$$\sum_{i=0}^{k-1} s_i \theta^i \mapsto \sum_{i=0}^{k-1} \sigma(s_i){\pi_1}^i. \tag{3.12}$$

Clearly, π_1 is a root of $\sigma(g(x))$ in R and, hence, ψ is an isomorphism. Thus, the following theorem is proved.

Theorem 3.1. *Let R and T be two complete chain rings with the same invariants p, n, r, k, m. Then, $R \cong T$ if and only if (3.7) and (3.10) hold for all $s \in P_m \setminus R(j)$.*

Corollary 3.3. *If R is associated with $p, 2, r, k, k+1$ such that $(p^r - 1, k_1) = 1$. Then, R is uniquely determined up to isomorphism by its invariants.*

Proof. Since $(p^r - 1, k_1) = 1$ and $n = 2, t = 1$, then clearly $x^k - p \in E(R)$; thus, $\beta = 1$ and $h = 1$. This means, the classification does not depend on (3.7) and (3.10). Therefore, Theorem 3.1 implies that there is only one ring (up to isomorphism) with such invariants. □

Example 3.1. *If R and T are two finite chain rings with the same invariants such that $l \geq 1$ and $n > 2$ or $n = 2$ and $t > 1$. Assume $x^k - p(x+1) \in E(R)$ and $x^k - p \in E(T)$. Since $(\pi + 1) = h_1 \neq \sigma(h_2) = \sigma(1) = 1$ for any $\sigma \in Aut\ S$. Hence, from Theorem 3.1, R and T are not isomorphic. By similar argument one can show $R \cong T$ when $x^k - p(1 + x^2) \in E(T)$, where $k > 2$.*

Theorem 3.2. *Let N be the number of complete chain rings with invariants p, n, r, k, m such that $n \geq 3$ or $n = 2, t > 1$. Then,*

$$N = \frac{1}{r} \sum_{i=0}^{r-1} (p^i - 1, z) p^{(i,r)\iota}, \tag{3.13}$$

where $z = (p^r - 1, k_1)$ and $\iota = \sum_{s \notin R(j)} l_s$.

Proof. For $s \notin R(j)$, U_s is a homogeneous group of order $p^{\nu(s)}$ and of rank r, and thus $U_s/U_s^{p^l}$ is also a homogeneous group of order p^{l_s} and of the same rank. It follows that every u_s of $U_s/U_s^{p^l}$ can be written as $u_s = \prod_{i=1}^{r} w_{is}^{a_i}$, where the exponents taken modulo p^{l_s}. Now, to simplify notations, we can identify $U_s/U_s^{p^l}$, as a set, as $\Gamma^*(r)^{l_s}$. Since there are c direct summands of H, i.e., c equations of the form (3.10), we identify H/H^{p^l} as $\Gamma^*(r)^{l_{s_1}} \times \Gamma^*(r)^{l_{s_2}} \times \cdots \times \Gamma^*(r)^{l_{s_c}}$. Moreover, replace $< a > / < a^{k_1} >$ by the additive group $\mathbb{Z}_z$ of integers modulo z, where $z = (p^r - 1, k_1)$. Let $Aut\ S =< \rho >$ acts on the set $\mathbb{Z}_z \times \Gamma^*(r)^{l_{s_1}} \times \Gamma^*(r)^{l_{s_2}} \times \cdots \times \Gamma^*(r)^{l_{s_c}}$ by:

$$\rho^i(a, x_{s_1}, \ldots, x_{s_c}) = (p^i a, x_{s_1}^{p^i}, \ldots, x_{s_c}^{p^i}). \tag{3.14}$$

According to Theorem 3.1, it suffices to verify that N given in (3.13) is the number of equivalence classes. The number of elements fixed by ρ^i is $(p^i - 1, z) \prod_{s \notin R(j)} [(p^i - 1, p^r - 1) + 1]^{l_s}$, but $[(p^i - 1, p^r - 1) + 1] = p^{(i,r)}$, hence,

$$(p^i - 1, z) \prod_{s \notin R(j)} [(p^i - 1, p^r - 1) + 1]^{l_s} = (p^i - 1, z) p^{(i,r) \sum_{s \notin R(j)} l_s}. \tag{3.15}$$

Therefore, Burnside Lemma computes the total number of equivalence classes. □

Corollary 3.4. *If $l < n - 1$, then $l_s = l$, thus,*

$$N = \frac{1}{r} \sum_{i=0}^{r-1} (p^i - 1, z) p^{(i,r)cl}. \tag{3.16}$$

Corollary 3.5. *If $n = 2$ and $t > 1$ or $n = 3$ and $t = 1$. Then, $l_s = \nu(s)$ in Theorem 3.2.*

Example 3.2. *Assume that $\mathfrak{I}$ is the class of finite chain rings R with the same invariants and with associated Eisenstein polynomials $g(x) = x^k - p\beta(x+1) \in E(R)$. If R and T in $\mathfrak{I}$, then by Theorem 3.1,*

$R \cong T$ if and only if the Equation (3.7) holds. Thus, from Theorem 3.2, there are N_0 of non-isomorphic classes of such rings in $\mathfrak{I}$,

$$N_0 = \frac{1}{r}\sum_{i=0}^{r-1}(p^i - 1, z) = \sum_{a|z}\frac{\phi(a)}{\tau(a)}, \tag{3.17}$$

where ϕ is Euler function and $\tau(a)$ is the order of p in $\mathbb{Z}_a$. Note that the right-hand side of (3.17) represents the number of finite chain rings when $p \nmid k$, and it was given by Clark [4].

Next, we consider a subclass which consists of all pure chain rings with the same invariants. First, we determine $H^{p^l} \cap 1 + pS$. By Lemma 2.1, one can directly prove

$$(1 + \pi^s\epsilon)^{p^e} = 1 + \sum_{i=0}^{e}\pi^{k(e-i)+sp^i}\epsilon_i, \tag{3.18}$$

where ϵ and ϵ_i are units of R. Let

$$\begin{aligned} j(s,i,e) &= k(e-i) + sp^i, \\ j(s,e) &= \min\{j(s,i,e) : 0 \le i \le e\}. \end{aligned}$$

Then [1],

$$j(s,e) = j^e(s) = \begin{cases} sp^e, & \text{if } e \le b_s, \\ sp^{b_s} + (e - b_s)k, & \text{if } e > b_s, \end{cases} \tag{3.19}$$

where $b_s = \lceil \log_p \frac{u}{s} \rceil$ and $\lceil x \rceil$ is the smallest positive integer greater that or equal to x. Moreover,

$$v(s) = \begin{cases} b_s + n - 1, & \text{if } t \ge u, \\ b_s + n - 2, & \text{if } t < u. \end{cases} \tag{3.20}$$

Lemma 3.1. *Let R be a pure finite chain ring with $l \ge 1$, and $n > 2$ or $n = 2$ and $t > k_1p^{l-1} + \cdots + k_1$. If $0 \le i \le l-1$ and $\epsilon \in U(R)$, then there exists s, $k \nmid s$ such that*

$$(1 + \pi^{k_1p^i}\epsilon)^{p^{l-i}} \in U_k \times U_s \times H_{s+1}. \tag{3.21}$$

Proof. First, if $\epsilon \in \Gamma^*(r)$, then by using (3.18),

$$\begin{aligned} (1 + \pi^{p^ik_1}\alpha)^{p^{l-i}} &= (1 + \alpha^{p^{l-i}}\pi^k + \pi^{k+p^{l-i-1}k_1}\epsilon) \\ &= (1 + \alpha^{p^{l-i}}\pi^k)(1 + \pi^{k+p^{l-1}k_1}\epsilon_1), \end{aligned}$$

where ϵ, ϵ_1 are units of R. Take $s = k + k_1p^{l-1}$, and the proof is complete. Now, if $\epsilon \notin \Gamma^*(r)$ and i is fixed, then by successive application of (3.18) and (3.19),

$$(1 + \pi^{k_1p^i}\epsilon)^{p^{l-i}} = 1 + \xi_0\pi^k + \xi_1\pi^{s_1} + \xi_2\pi^{s_2} + \cdots + \xi_{s_{i+1}}\pi^{s_{i+1}} + \xi'_{a_{i+1}}\pi^{a_{i+1}} + \pi^q\epsilon_0, \tag{3.22}$$

where

$$\begin{cases} s_b = k + k_1p^{l-1} + \cdots + k_1p^{l-b}, \\ s_{i+1} = s_b + j^{l-i}(s'), \\ a_{i+1} = s_b + k_1p^{l-(i+1)}, \\ q > \max\{s_{i+1}, a_{i+1}\}, \\ \xi_0, \xi_{s_{i+1}}, \xi'_{a_{i+1}} \in \Gamma^*(r) \text{ and } \xi_b, \xi'_b \in \Gamma(r), \end{cases}$$

$1 \leq b \leq i$ and ϵ_0 is a unit of R. Note that $s_{i+1} \neq a_{i+1}$ because otherwise yields $j^{l-i}(s') = k_1 p^{l-(i+1)}$, thus, $k_1 = j(s')$ which is contradiction since $k_1 < k$ and $(k_1, p) = 1$. Assume

$$s = \min\{s_b, s_{i+1}, a_{i+1} : \xi_b \neq 0\}, \tag{3.23}$$

then the proof is complete. □

Proposition 3.3. *Assume that R is a pure finite chain ring with p, n, r, k, m. Then,*

$$H^{p^l} \cap 1 + pS = \begin{cases} (1+pS)^{p^l}, & \text{if } n > 2 \text{ or } n = 2 \text{ and } t > k_1 p^{l-1}, \\ 1 + pS, & \text{if } n = 2 \text{ and } t \leq k_1 p^{l-1}. \end{cases} \tag{3.24}$$

Proof. First, if $n = 2$ and $t \leq k_1 p^{l-1}$, then it is easy to see that every element of $1 + pS$ is given by $1 + \pi^k \delta^{p^l}$, for some $\delta \in \Gamma^*(r)$. This yields $(1 + \pi^{k_1}\delta)^{p^l} = 1 + \pi^k \delta^{p^l}$, hence,

$$H^{p^l} \cap 1 + pS = 1 + pS. \tag{3.25}$$

Next, let $n > 2$ or $n = 2$ and $t > k_1 p^{l-1}$. If $h \in H$, there is $s \in P_m$ such that $h \in H_s \setminus H_{s+1}$ and $h = 1 + \pi^s \epsilon$, where $\epsilon \in U(R)$. We consider different cases for s.

(**a**) If $s \geq k$ and $h^{p^l} \in 1 + pS$. Then,

$$h^{p^l} = (1 + \pi^s \epsilon)^{p^l} = 1 + \pi^{j^l(s)} \epsilon_1, \tag{3.26}$$

where ϵ_1 is a unit in R. Since any element of $1 + pS$ is of the form $1 + \sum \pi^{ak} \alpha_a$, where $\alpha_a \in \Gamma^*(r)$, thus, $\pi^{j^l(s)} \epsilon_1 = 0$ or $j^l(s) = lk + s = qk$ and $\epsilon_1 \in U(S)$ for some positive integer $q \geq l + 1$, i.e., $k \mid s$. In either case, we obtain

$$h^{p^l} \in 1 + p^{l+1} S = (1 + pS)^{p^l}. \tag{3.27}$$

(**b**) When $s < k$. If $s \neq k_1 p^i$, then similarly $k \nmid j^l(s)$; thus, $\pi^{j^l(s)} \epsilon_1 = 0$. On the other hand, if $s = k_1 p^i$, $0 \leq i \leq l - 1$. Consider the filtering:

$$H_k > H_{k+1} > \cdots > H_m =< 1 > . \tag{3.28}$$

This series is complete, hence, satisfies all related results in [1,3]. The set $\{w_{ik} = 1 + \alpha_i \pi^k : 1 \leq i \leq r\}$ generates U_k, then, $U_k = 1 + pS$. Notably, Lemma 3.1 implies

$$h^{p^l} = (1 + \pi^s \epsilon)^{p^l} = ((1 + \pi^s \epsilon)^{p^{l-i}})^{p^i} = (1 + \zeta \pi^k)^{p^i} \cdot \vartheta^{p^i}, \tag{3.29}$$

where $\zeta \in \Gamma^*(r)$, $\vartheta \in H_s$ and $k \nmid s$. Since $h^{p^l} \in 1 + pS$, then

$$h^{p^l} \cdot ((1 + \zeta \pi^k)^{-1})^{p^i} \in 1 + pS, \tag{3.30}$$

and, thus, $\vartheta^{p^i} \in 1 + pS$ which is impossible since the generators of H_k are linearly independent. Finally, consider the particular case $n = 2$ and $k_1 p^{l-1} < t \leq k_1 p^{l-1} + \cdots + k_1$. Since $n = 2$, $h^{p^l} = (1 + \pi^{k_1 p^i} \epsilon)^{p^l} = 1$ for $1 \leq i \leq l - 1$. If $i = 0$, then

$$h^{p^l} = (1 + \pi^{k_1} \epsilon)^{p^l} = 1 + \delta \pi^k + \delta_1 \pi^{k + j^l(s)} + \delta_2 \pi^{k + k_1 p^{l-1}} + \epsilon_0 \pi^s, \tag{3.31}$$

for $\delta, \delta_1, \delta_2 \in \Gamma^*(r)$, $\epsilon_0 \in U(R)$, $s \in P_m$ and $s > k + k_1 p^{l-1}$. Since $k + k_1 p^{l-1} \neq k + j^l(s)$, hence $h^{p^l} \notin 1 + pS$. In this case, we have

$$H^{p^l} \cap 1 + pS =< 1 > \subseteq (1 + pS)^{p^l}. \tag{3.32}$$

□

Note that if $n = 2$, then $x^k - p\beta \in E(R)$ for every pure chain ring R, thus, N is given by (3.17). The following theorem gives N when $n \geq 3$.

Theorem 3.3. *The number N of pure finite chain rings with same invariants p, n, r, k, m such that $n \geq 3$ is precisely*

$$N = \frac{1}{r} \sum_{i=0}^{r-1} (p^i - 1, z) p^{(i,r)\iota}, \tag{3.33}$$

where

$$\iota = \begin{cases} l, & \text{if } l < n - 2, \\ n - 2, & \text{if } l \geq n - 2. \end{cases}$$

Proof. The proof follows directly from Proposition 3.3 and Theorem 3.2. □

Remark 3.2. *Note that N in Theorem 3.3 is dependent on n.*

The following corollary illustrates that the result in [7] is just a special case of Theorem 3.3.

Corollary 3.6. *If $l = 1$, then $N = \frac{1}{r} \sum_{i=0}^{i-1} (p^i - 1, z) p^{(i,r)}$.*

3.2. Incomplete chain rings

In this section, we investigate the incomplete case. If R is a finite chain ring with invariants p, n, r, k and m, and $\pi^k = p\beta h$. The incomplete situation happens when (cf. [1]),

$$p - 1 \mid k, \;\; -\beta \in F^{*p-1} \text{ and } m > k + u, \tag{3.34}$$

($k = (p-1)u$). However, if R is incomplete, the system (2.7) and $\xi = w_{1s_0} = 1 + \alpha_1 \pi^{s_0}$ are subjected to

$$\xi^{p^\lambda} = \prod_{(1,s_0) \neq (i,s) \in B} w_{is}^{a_{is}} \cdot \gamma^{a_0}, \tag{3.35}$$

where a_{is}, a_0 are positive integers divisible by p. Denote $\mu = \mu_1 = \min\{a_{is}, a_0 : (i, s) \in B \setminus \{(1, s_0)\}\}$.

Proposition 3.4 (Theorem 2, [1])**.** *Let R be incomplete chain ring, then there are $d \geq 0$, $\Omega = \{s_0, s_1, \ldots, s_d\} \subseteq P_m$ and $\{\mu_i\}_{0 \leq i \leq d}$ such that*

$$H = \otimes_{s \in \Lambda} U_s \otimes_{i=0}^{d} (U_{s_i}^* \otimes C_{p^{\mu_i}}) \otimes C, \tag{3.36}$$

where $\Lambda = \{P_m \setminus R(j)\} \setminus \Omega$ and $C =< \gamma >$ if $k + u \notin \Omega$ or $C =< 1 >$, otherwise.

If R and T are two incomplete chain rings with same invariants p, n, r, k, m. Then, H_R and H_T may not have the same structure [1]. This situation makes the enumeration much harder than the complete case.

3.2.1. Special incomplete chain rings

If we write H_R (3.36) as $H_R = G_R \otimes \prod_{s\geq u_1} U_s \otimes G_2$, where $G_R = \prod_{1\leq s\leq u_1-1} U_s$ and $u_1 = \frac{u}{p^l}$. Thus, H_R and H_T have the same summand G_R; $G_T \cong G_R$.

We state the following theorem without proof because it involves the same ideas to that ones of Theorem 3.2. Note that l_s, in this case, equal l for $1 \leq s \leq u_1 - 1$.

Theorem 3.4. *Let Σ be the class of all finite incomplete chain rings R which have the same invariants p, n, r, k and m, and associated with $\pi^k = p\beta h$, where $h \in G_R$. If N is the cardinality (up to isomorphism) of Σ, then*

$$N = \frac{1}{r}\sum_{i=0}^{r-1}(p^i - 1, z)p^{(i,r)l(u_1-1)}. \tag{3.37}$$

Remark 3.3. *The conditions in (3.34) guarantee the existence of a root of $x^{p-1} + p$ in R (see [1]). Assume that $R_0 = S[\pi_0]$, where π_0 is a root of $x^{p-1} + p$, then R_0 is a finite (complete) chain suring of R with $p, n, r, p-1, m_1$, where $m_1 = (n-1)(p-1) + t_1$ and $1 \leq t_1 \leq p-1$. Consider the class $\Im$ of all finite incomplete chain rings with p, n, r, k, m which are associated with $\pi^k = p\beta h$, where $h \in H(R_0)$. If $\beta_1^{p-1} = \beta$ and $h_1^{p-1} = h$ for $\beta_1 \in < a >$ and $h_1 \in H(R_0)$, then one can check that*

$$\pi_0 = \beta_1 h_1 \pi^u, \tag{3.38}$$

is a root of $x^{p-1} + p$.

Next, we aim to obtain the number of non-isomorphic rings in $\Im$. First, we introduce some useful information about R_0.

Lemma 3.2. *$\phi \in Aut\ R_0$ if and only if*

$$\phi(\sum_{i=0}^{p-2} s_i{\pi_0}^i) = \sum_{i=0}^{p-2}\sigma(s_i)(\alpha\zeta\pi_0)^i, \tag{3.39}$$

where $\alpha \in < a >$ is a $(p-1)$-th root of unity and $\zeta \in H_{m_1-(p-1)}(R_0)$ for some $\sigma \in Aut\ S$.

Proof. Let $\phi \in Aut\ R_0$, then $\phi(\pi_0) = \alpha\zeta\pi_0$ where $\alpha \in < a >$ and $\zeta \in H(R_0)$. Note that

$$-p = \phi(\pi_0^{p-1}) = \phi(\pi_0)^{p-1} = -p\alpha^{p-1}\zeta^{p-1}. \tag{3.40}$$

Thus, $\alpha^{p-1} = 1$ and $\zeta^{p-1} = 1 \bmod H_{m_1-(p-1)}(R_0)$. Since $(p-1, p) = 1$, then $\zeta \in H_{m_1-(p-1)}(R_0)$. On the other hand, if α and ζ satisfy the condition, then one can see that $\phi(\pi_0^{p-1}) = \phi(\pi_0)^{p-1}$. Thus, ϕ is an automorphism of R_0. □

Corollary 3.7. *Every $\sigma \in Aut\ S$ can be extended to an automorphism $\phi \in Aut\ R_0$.*

Proposition 3.5. *If R and T are two rings in $\Im$ with the same R_0. Then, $R \cong T$ if and only if there is $\phi \in Aut\ R_0$ such that $\phi(g(x))$ (applies to the coefficients) has a root in R, where $g(x)$ is an Eisenstein polynomial of T over R_0.*

The proof involves argument similar to that of Proposition 3.1 with help from Corollary 3.7.

Lemma 3.3. *Assume the admissible function j satisfies: if $j(s) \geq p$, then $s \in R(j)$ for all s. Then, $H_s^{p^i} = H_{j^i(s)}$, in particular, $H^{p^i} = H_{j^i(1)}$.*

Proof. The proof is conducted by induction on i. First, let $i = 1$, and note that $H_s^p \subseteq H_{j(s)}$. If $y \in H_{j(s)}$, then $y = u_{j(s)}y_1$, where $u_{j(s)} \in U_{j(s)}$ and $y_1 \in H_{j(s)+1}$. Moreover, $u_{j(s)} = u_s^p$ for some $u_s \in U_s$, and $y_1 = u_{j(s)+1}y_2$, where $u_{j(s)+1} \in U_{j(s)+1}$ and $y_1 \in H_{j(s)+2}$. Since

$$j(j(s) + 2) \geq j(j(s) + 1) \geq j(1) = p, \tag{3.41}$$

then $j(s) + 2$ and $j(s) + 1 \in R(j)$. Which follows that $u_{j(s)+1} = u_{s_1}^p$. Continuing in this way, we obtain $y = y_0^p$, and hence $H_{j(s)} \subseteq H_s^p$. Thus, $H_{j(s)} = H_s^p$. For $i > 1$, note that $H_s^{p^i} = (H_s^{p^{i-1}})^p$, and by the induction step, the result follows. □

Lemma 3.4. *Let R be in $\Im$. Then,*

$$H^{p^l} \cap H(R_0) = \begin{cases} (H(R_0))^{p^l}, & \text{if } n > 2 \text{ or } n = 2 \text{ and } t > k_1p^{l-1}, \\ H(R_0), & \text{if } n = 2 \text{ and } t \leq k_1p^{l-1}. \end{cases} \tag{3.42}$$

The proof follows by slightly modifying the proofs of Lemma 3.1 and Proposition 3.3, that is, consider u instead of k, and the Eq (3.35) as illustrated in (Example 2, [1]).

Theorem 3.5. *Assume that $l < n - 2$, the number N of incomplete chain rings exist in the class $\Im$ is*

$$N = N_0[\frac{1}{r}\sum_{i=0}^{r-1}(p-1)(p^i-1, d_1)p^{(i,r)l(p-2)}], \tag{3.43}$$

where $d_1 = (k, \frac{p^r-1}{p-1})$ and N_0 is the number of finite chain rings R_0 given in (3.17).

Proof. If R and T are in $\Im$, and if $R \cong T$, then by Proposition 3.5, there exists $\phi \in Aut\ R_0$ such that $\phi(g(x))$ has a root in R, where $g(x) = x^u - \pi_0\beta_1h_1$, $h_1 \in H(R_0)$. Let $\pi_1 = \delta\zeta\pi$ be a root of $\phi(g(x))$ in R, note that

$$\pi_0\beta h\delta^u\zeta^u = \pi_1^u = \phi(\pi_0)\sigma(\beta_1)\phi(h_1) = \pi_0\alpha\vartheta\sigma(\beta_1)\phi(h_1).$$

Thus,

$$\begin{aligned} \beta\delta^u &= \alpha\sigma(\beta_1) \\ h\zeta^u &= \vartheta\phi(h_1) \mod H_{m_1-1}(R_0). \end{aligned}$$

Since $l \leq n-3$, then $j^l(1) \leq m_1 - (p-1)$, and since $\vartheta \in H_{m_1-(p-1)}(R_0)$ (Lemma 3.2), then $\vartheta = 1 \bmod H(R_0)^{p^l} = 1 \bmod H_{j^l(1)}(R_0)$ (Lemma 3.3). This implies $h = \phi(h_1) \bmod H_{j^l(1)}(R_0)$. Let $G = Aut\ S$ acts on $\Gamma^*(r)^{l(p-2)}$, then there are $p^{(i,r)l(p-2)}$ elements fixed by ρ^i (see proof of Theorem 3.2). On the other hand, the equation $\beta\delta^u = \alpha\sigma(\beta_1)$ implies that $\beta^{p-1}\delta^k = \sigma(\beta_1^{p-1})$ (Lemma 3.2). Moreover, if $\sigma = \rho^i$, then we have $(p^i - 1, d_1)$ elements in $\mathbb{Z}_{d_1}$ fixed by ρ^i, and since there are $p - 1$ different roots α of unity, then, there are $(p-1)(p^i-1, d_1)$ elements fixed by ρ^i. Therefore, by an argument similar to the proof of Theorem 3.2, the number of finite chain rings in $\Im$ which have the same invariants and same R_0 is

$$N_1 = \frac{1}{r}\sum_{i=0}^{r-1}(p-1)(p^i-1, d_1)p^{(i,r)l(p-2)}.$$

Furthermore, there are $N_0 = \frac{1}{r}\sum_{i=0}^{r-1}(p^i - 1, z)$ (Example 3.2) of non-isomorphic types of R_0. Thus, the proof of the theorem follows. □

Corollary 3.8. *The number N of pure chain rings with p, n, r, k, m is precisely given in (3.33)*

Proof. In the case $l < n - 2$, the proof is just a direct application to the previous Theorem 3.5 when $\alpha = 1$, $\zeta = 1$ and $N_0 = 1$. If $l \geq n - 2$, the proof follows from Proposition 3.4 and the proof of Theorem 3.2. □

3.2.2. General incomplete chain rings

The general case of incomplete chain rings when $n \geq 4$ or $n = 3, t > 1$ is still complicated to determine N. For the moment, the best we can do is to approximate N by finding upper and lower bounds. First, we derive a relation between Aut R and N.

Lemma 3.5. *Let $g_1(x)$ and $g_2(x)$ be in $E(R)$ corresponding to π_1 and π_2 respectively. If $\phi \in Aut\ R$, then $\phi(\pi_1) = \pi_2$ if and only if there exists $\sigma \in Aut\ S$ such that $\sigma(g_1(x)) = g_2(x)$.*

Proof. Let $\phi \in Aut\ R$ maps π_1 to π_2, and let σ be its restriction on S. Observe that

$$\phi(g_1(\pi_1)) = (\phi(\pi_1))^k - p\sigma(f(\phi(\pi_1))) = (\pi_2)^k - p\sigma(f(\pi_2)) = 0 = g_2(\pi_2). \tag{3.44}$$

Hence, $g_2(x) = \sigma(g_1(x))$. The other direction is analogous to that of Proposition 3.1. □

Corollary 3.9. *Assume the hypotheses of Lemma 3.5, then $g_1(x) = g_2(x)$ if and only if $\phi \in Aut_S\ R$ (fixing S).*

Corollary 3.10. *If $\phi \in Aut_S\ R$ such that $\phi(\pi) = \pi$ for some $\pi \in J_1$, then ϕ is the identity automorphism.*

Define a relation $\sim$ on $E(R)$ by: $g_1 \sim g_2$ if and only if $g_2 = \sigma(g_1)$; that is, $G = Aut\ S$ acts on $E(R)$. This relation is well defined since $\sigma(E(R)) \subseteq E(R)$ (Corollary 3.1). Let $orb(g)$ denotes the orbit of g and G_g is the stabilizer of g in G. Hence, $\mid orb(g) \mid = r / \mid G_g \mid$.

Proposition 3.6. *Let R runs over all non-ismorphic classes of finite chain rings with the same invariants p, n, r, k, m. Then,*

$$\sum_R \frac{1}{\mid G_{g_R} \mid\mid Aut\ R \mid} = \frac{1}{rp^{(k-1)r}}. \tag{3.45}$$

Proof. Let $Aut_S\ R$ acts on J_1 in the natural way, i.e., $\phi\pi = \phi(\pi)$. Let $\sim$ be the induced equivalence relation. Thus, J_1 splits into classes of elements, and Corollary 3.10 implies that each class has $\mid Aut_S\ R \mid$ elements. Also Lemma 3.5 emphasizes that the number of the equivalent classes is $\mid E(R) \mid$. Hence,

$$\mid J_1 \mid = \mid Aut_S\ R \mid\mid E(R) \mid . \tag{3.46}$$

Moreover, $\mid J_1 \mid = \mid \Gamma^*(r) \mid\mid \Gamma(r) \mid^{m-2} = (p^r - 1)p^{(m-2)r}$, then

$$\mid E(R) \mid = \frac{(p^r - 1)p^{(m-2)r}}{\mid Aut_S\ R \mid}. \tag{3.47}$$

On the other hand, $E(p, k)$ splits into non-intersecting by Proposition 3.2. Thus,

$$\mid E(p, k) \mid = \sum_R \mid E(R) \mid, \tag{3.48}$$

where R represents the classes of finite chain rings with same invariants p, n, r, k, m. Simple calculations imply that there exist $(p^r - 1)p^{(m-k-1)r}$ of all possible polynomials in $E(p, k)$. Furthermore, in the light of Lemma 3.5, for each polynomial exists in $orb(g)$, there are $\mid Aut_S\ R \mid$ different automorphisms of R, i.e.,

$$\mid Aut\ R \mid = \mid orb(g) \mid\mid Aut_S\ R \mid . \tag{3.49}$$

This leads to

$$\mid E(R) \mid = \frac{(p^r - 1)p^{(m-2)r} \mid orb(g) \mid}{\mid Aut\ R \mid}, \tag{3.50}$$

thus,

$$\sum_R \frac{(p^r - 1)p^{(m-2)r} \mid orb(g) \mid}{\mid Aut\ R \mid} = (p^r - 1)p^{(m-k-1)r}. \tag{3.51}$$

Now, $\mid orb(g) \mid = r / \mid G_g \mid$ which follows that

$$\sum_R \frac{1}{\mid G_{g_R} \mid\mid Aut\ R \mid} = \frac{1}{rp^{(k-1)r}}. \tag{3.52}$$

□

Corollary 3.11. *If $g(x) \in E(R)$, then the number of roots of $g(x)$ in R is $\mid Aut_S\ R \mid$.*

Theorem 3.6. *Let N be the number of all non-isomorphic finite incomplete chain rings with invariants p, n, r, k, m. Then,*

$$\frac{p^r}{r} \leq N \leq (p^r - 1)p^{(m-k-1)r}. \tag{3.53}$$

Proof. By the proof of Proposition 3.6,

$$\begin{aligned} \mid Aut\ R \mid &= \mid orb(g) \mid\mid Aut_S\ R \mid \\ &= \frac{r}{\mid G_{g_R} \mid} \frac{\mid J_1 \mid}{\mid E(R) \mid} \\ &\leq \frac{r}{\mid G_{g_R} \mid} (p^r - 1)p^{(m-2)r}. \end{aligned}$$

Hence,

$$\frac{1}{\mid Aut\ R \mid} \geq \frac{\mid G_{g_R} \mid}{r} \frac{1}{(p^r - 1)p^{(m-2)r}}.$$

This implies

$$\frac{1}{\mid G_{g_R} \mid\mid Aut\ R \mid} \geq \frac{1}{r(p^r - 1)p^{(m-2)r}}.$$

Now, also from Proposition 3.6,

$$\frac{N}{r(p^r - 1)p^{(m-2)r}} \leq \frac{1}{p^{r(k-1)}}.$$

Thus, $N \leq (p^r - 1)p^{(m-k-1)r}$. On the other hand,

$$\mid Aut\ R \mid = \frac{r}{\mid G_{g_R} \mid} \frac{\mid J_1 \mid}{\mid E(R) \mid}$$

$$\begin{aligned}&\geq \frac{r}{\mid G_{g_R}\mid}\frac{p^{(m-2)r}}{p^{(m-k-1)r}}\\&\geq p^{r}\frac{p^{(m-2)r}}{p^{(m-k-1)r}}\\&=p^{kr}.\end{aligned}$$

Moreover, from Proposition 3.6,

$$\frac{1}{rp^{(k-1)r}}=\sum_{R}\frac{1}{\mid G_{g_R}\mid\mid Aut\ R\mid}\leq Np^{-kr}.$$

Therefore, $N\geq\frac{p^r}{r}$. □

Corollary 3.12. *$N=1$ if and only if $\mid Aut_S\ R\mid=p^{(k-1)r}$.*

Remark 3.4. *The lower and upper bounds in (3.53) are attained when $p=k=n=m=2$ and $r=1$. In this case, they coincide.*

The following result is easy to check so we skip the proof.

Proposition 3.7. *Assume that R is a finite chain ring with invariants p,n,r,k,m. Then, R is uniquely determined if and only if one of these conditions holds:*
(i) $k=m$; (ii) $m=k+1$ and $(k,p^r-1)=1$; (iii) $m>k+1$, $(k,p)=1$ and $(k,p^r-1)=1$.

Corollary 3.13. *$\mid Aut_S\ R\mid=p^{(k-1)r}$ if and only if $(k,p)=1$ and $(k,p^r-1)=1$ or $m-1=k$ and $(k,p^r-1)=1$.*

Proof. Forward from Proposition 3.7 and Corollary 3.12. □

4. Finite chain rings and p-adic fields

In this section, we apply the above-mentioned results to the p-adic number fields. Any finite extension of $\mathbb{Q}_p$ is called a p-adic number field where $\mathbb{Q}_p$ is a completion of $\mathbb{Q}$ using p-adic norm $|\ .\ |$ generated from p-adic valuation v_p, defined as: $|a|=p^{-v_p(a)}$. Let K be a p-adic number field with ramification index k and residue degree r. There is a unique extension v of v_p normalized such that $v(\pi)=1$, where π is the unique prime element (uniformizer) of O_K ring of integers of K.

Lemma 4.1. *If L is unramified extension of degree r over $\mathbb{Q}_p$ and K is a totally ramified extension of degree k over L. Let $g(x)$ be an Eisenstein polynomial over O_L of degree k such that its image in $O_L/(p^n)$ has a root in $O_K/(\pi^m)$, then if $m>2[(l+1)k-1]$, $g(x)$ has a root in O_K.*

Proof. Assume that $\overline{g}(x)$ (mod p^n) has a root θ in $O_K/(\pi^m)$. If $\zeta\in O_K$ is a lifting of θ, then $g(\zeta)\in(\pi^m)$, and thus

$$\mid g(\xi)\mid\leq\frac{1}{p^m}.\tag{4.1}$$

Consider the formal derivative of g,

$$g'(\zeta)=k\xi^{k-1}-p[a_1+2a_2\zeta+\cdots+(k-1)a_{k-2}\zeta^{k-2}].\tag{4.2}$$

Now, let v be the extension of p-adic evaluation v_p to K which is complete and nonarchimedean. Thus, we have $v(\theta) = v(\xi) = 1$ since ζ is lifting of θ. Hence, $e = v(g'(\xi)) \leq (l+1)k - 1$, and

$$| g'(\zeta) |= \frac{1}{p^e},$$
$$| g'(\zeta) |^2= \frac{1}{p^{2e}}.$$

Then,

$$\frac{1}{p^m} \leq \frac{1}{p^{2(l+1)k-1}} \leq \frac{1}{p^{2e}}.$$

This implies

$$| g(\zeta) |<| g'(\zeta) |^2 .$$

Therefore, by Hensel's Lemma ([2]), $g(x)$ has a root in O_K. □

Theorem 4.1. *Let N be the number of isomorphism classes of finite commutative chain rings associated with the same p, n, r, k and m, with $m > 2[(l+1)k - 1]$. Then, N is the number of $\mathbb{Q}_p$–isomorphism finite extension of $\mathbb{Q}_p$ with ramification index k and residue degree r.*

Proof. Let K_1 and K_2 be both extensions over $\mathbb{Q}_p$ with ramification index k and residue degree r. Then, K_1 and K_2 have the same maximal unramified extension L over $\mathbb{Q}_p$. Assume $R = O_1/(\pi^m)$ and $T = O_2/(\theta^m)$, where O_1 and O_2 are the rings of integers of K_1 and K_2, respectively. Now, if $R \cong T$, then by Proposition 3.1, there is $\sigma \in Aut\ S$ such that $\sigma(\overline{g}(x))$ has a root in T, where $g(x)$ is an Eisenstein polynomial over L. Assume $\overline{\theta}$ is the root of $\sigma(\overline{g}(x))$, and let $\zeta \in O_2$ be a lifting of $\overline{\theta}$. Note that $\sigma(\overline{g}(\overline{\theta})) = 0$ and so $\tau(g(\zeta)) \in (\theta^m)$, where $\tau \in Aut_{\mathbb{Q}_p} L$ is the corresponding to σ since $Aut_{\mathbb{Q}_p} L \cong Aut\ S$ (L is unramified over $\mathbb{Q}_p$). Since $m > 2[(l+1)k - 1]$, then by Lemma 4.1, $f(x) = \tau(g(x))$ has a root π_2 in K_2. Thus,

$$K_1 = L(\pi_1) \cong L(\pi_2) = K_2, \tag{4.3}$$

where π_1 is a root of $g(x)$ in K_1. Also note that $\pi_2 \cong \zeta \bmod \theta$. This ends the proof. □

The following example shows that the condition on m in Theorem 4.1 is necessary.

Example 4.1. *Consider $K_1 = \mathbb{Q}_2(\sqrt{2})$ and $K_2 = \mathbb{Q}_2(\sqrt{6})$. Now, let O_1 and O_2 be the rings of integers of K_1 and K_2, respectively. Assume that*

$$R = O_1/(\pi^4) \cong \mathbb{Z}_4[x]/(g_1(x)),$$
$$T = O_2/(\theta^4) \cong \mathbb{Z}_4[x]/(g_2(x)),$$

where $g_1(x) = x^2 - 2$ and $g_2(x) = x^2 - 6$ (mod 4), i.e., $g_2(x) = x^2 - 2$. Then, clearly R and T are finite chain rings with invariants $2, 2, 1, 2, 4$ which are isomorphic. While K_1 and K_2 are not isomorphic. Note that $m = 4 < 6 = 2(l+1)k - 1$.

5. Conclusions

In this paper, we have investigated the classification of finite commutative chain rings with the same invaraints p, n, r, k, m. If $(p-1) \nmid k$, the full classification of these rings is given. While if $(p-1) \mid k$, we showed that the number of non-isomorphic classes of finite commutative chain rings depends not only on their invariants but also on their Eisenstein polynomials. In this case, we classified such rings up to isomorphism under some conditions concerning the Eisenstein polynomials.

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 no conflict of interest.

References

1. S. Alabiad, Y. Alkhamees, Recapturing the structure of group of units of any finite commutative chain ring, *Symmetry*, **13** (2021), 307. doi: 10.3390/sym13020307.
2. J. W. S. Cassels, *Local fields*, Cambridge University Press, 1986. doi: 10.1017/CBO9781139171885.
3. C. W. Ayoub, On the group of units of certain rings, *J. Number Theory*, **4** (1972), 383–403.
4. W. E. Clark, J. J. Liang, Enumeration of finite chain rings, *J. Algebra*, **27** (1973), 445–453. doi: 10.1016/0021-8693(73)90055-0.
5. M. Greferath, Cyclic codes over finite rings, *Discrete Math.*, **177** (1997), 273–277. doi: 10.1016/S0012-365X(97)00006-X.
6. P. W. Haggard, J. O. Kiltenin, Binomial expansion modulo prime powers, *Int. J. Math. Math. Sci.*, **3** (1980), 985261. doi: 10.1155/S0161171280000270.
7. X. D. Hou, Finite commutative chain rings, *Finite Fields Appl.*, **7** (2001), 382–396. doi: 10.1006/ffta.2000.0317.
8. J. Neukirch, *Local class field theory*, Berlin: Springer, 1986.
9. W. Klingenberg, Projective und affine Ebenen mit Nachbarelementen, *Math. Z.*, **60** (1954), 384–406. doi: 10.1007/BF01187385.
10. S. Lang, *Algebraic number theory*, New York: Springer, 1994. doi: 10.1007/978-1-4612-0853-2.
11. X. S. Lui, H. L. Lui, LCD codes over finite chain rings, *Finite Fields Appl.*, **34** (2015), 1–19. doi: 10.1016/j.ffa.2015.01.004.
12. B. R. McDonald, *Finite rings with identity*, New York: Marcel Dekker, 1974.
13. R. Raghavendran, Finite associative rings, *Compos. Math.*, **21** (1969), 195–229.
14. M. J. Shi, S. X. Zhu, S. L. Yang, A class of optimal p-ary codes from one-weight codes over $F_p[u]/ < u^m >$, *J. Franklin I.*, **350** (2013), 929–937. doi: 10.1016/j.jfranklin.2012.05.014.