symmetry

MDPI

Article

On J-Diagrams for the One Groups of Finite Chain Rings

Sami Alabiad * and Yousef Alkhamees

Department of Mathematics, College of Sciences, King Saud University, Riyadh 11451, Saudi Arabia; ykhamees@ksu.edu.sa
* Correspondence: ssaif1@ksu.edu.sa

Abstract: Let R be a finite commutative chain ring with invariants p, n, r, k, m. The purpose of this article is to study j-diagrams for the one group $H = 1 + J(R)$ of R, where $J(R) = (\pi)$ is Jacobson radical of R. In particular, we prove the existence and uniqueness of j-diagrams for such one group. These j-diagrams help us to solve several problems related to chain rings such as the structure of their unit groups and a group of all symmetries of $\{\pi^{k'}\}$, where $k' \mid k$. The invariants p, n, r, k, m and the Eisenstein polynomial by which R is constructed over its Galois subring determine fully the j-diagram for H.

Keywords: chain rings; j-diagrams; p-groups; Galois rings

Citation: Alabiad, S.; Alkhamees, Y. On J-Diagrams for the One Groups of Finite Chain Rings. *Symmetry* **2023**, *15*, 720. https://doi.org/10.3390/sym15030720

Academic Editor: Alexei Kanel-Belov

Received: 3 February 2023
Revised: 9 March 2023
Accepted: 10 March 2023
Published: 14 March 2023

1. Introduction

Suppose that $P_m = \{1, 3, \ldots, m\}$, the function $j : P_m \to P_m$ is said to be admissible if $s < j(s)$ and if $j(s) = j(i)$, then $s = i$. Admissible functions have been used as a significant tool to determine the structure of abelian p-groups which have certain types of j-diagram series [1–3]. Moreover, j-diagrams are used in classifying chain rings and in determining their groups of automorphisms [4]. Motivated by the important role of j-diagrams in group and ring theory, this article is aimed to investigate the existence and uniqueness of such j-diagrams. We focus our attention on j-diagrams for finite abelian p-groups, and particularly groups of units of finite commutative chain rings. Chain rings are associative rings that have a lattice of ideals that creates a unique chain. A finite ring R can easily be shown to be a chain ring if and only if its (Jacobson) radical $J(R) = J$ is principal and $\overline{R} = R/J$ is a field of order p^r, p is prime. Every finite chain ring has five positive integers p, n, r, k, m named the *invariants*. These rings occur in several applications, for details see [1,5–12]. For instance, they have widely appeared in coding theory [13–17]. However, the class of Galois rings is a distinguished class of finite chain rings, and every Galois ring is represented as:

$$GR(p^n, r) = \mathbb{Z}_{p^n}[x]/(f(x)), \tag{1}$$

where $f(x)$ is a monic irreducible polynomial of degree r.

Finite chain rings are constructed in at least two different ways. Suppose that R is a finite chain ring that has the invariants p, n, r, k, m. First, R can be viewed as an Eisenstein extension of $GR(p^n, r)$

$$R = GR(p^n, r)[x]/(g(x), x^m), \tag{2}$$

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

$$g(x) = x^k - p\sum_{i=0}^{k-1} s_i x^i, \tag{3}$$

where s_0 is a unit of $GR(p^n, r)$. Another way to construct R involves $\mathbb{Q}_p$, the field of p-adic numbers. Every chain ring R is a quotient ring of the integers ring of a certain finite extension of $\mathbb{Q}_p$, for more details see [6] and the references therein. The symmetry of invariants of various chain rings injects more choice and flexibility into the theory of ring construction.

The group of units (multiplicative group) $U(R)$ of R is defined by $U(R) = R \setminus J$, i.e., the set of all non-nilpotent elements of R. From Ayoub (1972) [2], $U(R) \cong U \otimes H$, where $U \cong (R/J)^*$ is cyclic of order $p^r - 1$ and $H = 1 + J$ which is a p-group. Thus, the structure problem of $U(R)$ is reduced to that of H. After Ayoub, we call H the ***one group***. If $p - 1$ does not divide k, the structure of H is given by Ayoub [2] based on the results in [3]. However, the case when $(p-1) \mid k$, the full structure of H is given by Alabiad and Alkhamees [1]. In this paper, we aim to study the existence and uniqueness of j-diagrams for the one group H of R.

In Section 2, we introduce the concept of j-diagrams, some notations and examples. In Section 3, we study the existence and uniqueness of complete and incomplete j-diagrams for the series $H = H_1 > H_2 > H_3 > \cdots > H_m = 1$ of the one group H, for any finite commutative chain ring R with invariants p, n, r, k, m, where $H_s = 1 + J^s$. Moreover, among other results, we find an explanation of j-diagrams from a ring-theoretic point of view, see Theorem 5.

2. Preliminaries

Unless otherwise mentioned, all considered groups are multiplicative abelian groups, p denotes a fixed prime. See [2,3,18] for the details of this section.

Definition 1. *If $P_m = \{1, 2, \cdots, m\}$, $j : P_m \to P_m$ is called an admissible function if j satisfies the following conditions:*

$$(i)\ s < j(s), s \neq m;$$
$$(ii)\ If\ j(i) = j(s) \neq m,\ then\ i = s.$$

The following example is direct.

Example 1. *Let $j : P_m \to P_m$ be an admissible function and let $1 \le m' \le m$. Define*
(i) $j_1 : P_{m'} \to P_{m'}$, given by $j_1(i) = j(m - m' + i) - (m - m')$;
(ii) $j_2 : P_{m'} \to P_{m'}$, given by:

$$j_2(i) = \begin{cases} j(i), & \text{if } j(i) < m', \\ m', & \text{if } j(i) \ge m'. \end{cases}$$

Then, j_1 and j_2 are admissible functions.

Definition 2. *Let p be a fixed prime and A an abelian p-group. Then, the series*

$$A = A_1 > A_2 > \cdots > A_m = 1, \tag{4}$$

is called a complete $j-$diagram for A of length m with respect to p if $j : P_m \to P_m$ is admissible and
(i) If $j(s) = m$, $A_s^p = 1$.
(ii) If $j(s) \neq m$, $\eta_s : A_s/A_{s+1} \longrightarrow A_{j(s)}/A_{j(s)+1}$, given by:

$$\eta_s(xA_{s+1}) = x^p A_{j(s)+1}, \tag{5}$$

defines an isomorphism.

In case when η_s, for some $s \in P_m$, is only homomorphism, the series is called incomplete $j-$diagram at $i = s$.

Example 2. *Let $A =< a >$, where $o(a) = p^{m-1}$. Then,*

$$A =< a >= A_1 > A_2 =< a^p > \cdots > A_m = 1,$$

is a $j-$diagram of length m if j defined by:

$$j(i) = \begin{cases} i+1, & \text{if } 1 \le i < m, \\ m, & \text{if } i = m. \end{cases}$$

Example 3. *Let A be an elementary abelian $p-$group and let*

$$A = A_1 > A_2 \cdots > A_m = 1, \tag{6}$$

be a chain of subgroups of A. Then if $j(i) = m, 1 \le i \le m$, the chain (6) is a $j-$diagram of length m since $A_i^p = 1, 1 \le i \le m$. Thus, clearly a group need not have a unique j-diagram.

Notations and Terminologies

1. $\nu(s)$ is the smallest positive integer such that $j^{\nu(s)}(s) = m$.
2. $\mathrm{o}(x)$ means the multiplicative order of x.
3. $R(j)$ denotes the range of j.
4. β is always associated with Eisenstine polynomial $g(x)$,, i.e., $\pi^k = p\beta h$.
5. If $a \in A_i \setminus A_{i+1}$, we denote $wt(a) = i$.
6. $rank(A)$ is the smallest number of generators of A.
7. $dim(A)$ is the dimension of A as a vector space over $\mathbb{Z}_p$.

3. The J-Diagrams for One Group H

In what follows, R is a finite commutative chain ring with invariants p, n, r, k, m. We focus on the following series of $H = 1 + J$ ($J = J(R)$),

$$H = H_1 > H_2 > H_3 > \cdots > H_m = 1, \tag{7}$$

where $H_s = 1 + J^s$.

Definition 3. *We call R a complete (incomplete) chain ring if H has complete (incomplete at s^*) $j-$diagram, where $s^* = \lfloor \frac{k}{p-1} \rfloor$.*

Lemma 1. *If x is a unit in R. Then, $x = y \bmod H_i$ if and only if $x = y \bmod J^i$.*

Proof. This is true because

$$y - x \in J^i \Leftrightarrow x^{-1}y - 1 \in J^i \Leftrightarrow x^{-1}y \in H_i.$$

□

The following lemma is easy to prove.

Lemma 2. *Let $1 \le s \le m$.*

(1) The map $\gamma_s : H_s/H_{s+1} \longrightarrow J^s/J^{s+1}$ defined by:

$$\gamma_s(1+x)H_{s+1} = x + J^{s+1} \tag{8}$$

is an isomorphism.

(2) Let $\delta_s : J^s/J^{s+1} \longrightarrow J^{s+k}/J^{s+k+1}$ defined by:

$$\delta_s(x + J^{s+1}) = px + J^{s+k+1}. \tag{9}$$

Then, δ_s is an isomorphism.

Remark 1. *Note that J^s/J^{s+1} is an elementary p-group.*

Theorem 1. *Let R be complete, and let $j(i) \neq m$ for some i.*

(i) *If $k+i < pi$, then $j(i) = k+i$.*
(ii) *If $k+i = pi$ and $j(i+1) < m$, then $j(i) = k+i$.*
(iii) *If $pi < k+i$, then $j(i) = pi$.*

Proof. Consider $1+x \in H_i \setminus H_{i+1}$. Then, $(1+x)^p \in H_{j(i)} \setminus H_{j(i)+1}$. Moreover, $(1+x)^p = 1+py+x^p$ with $wt(y) = wt(x) = i$. Suppose $k+i < pi$, then $k+i = wt(py) < pi$. As $wt(x^p) = \min\{m, pi\} > k+i$, we get $(1+x)^p \in H_{k+i} \setminus H_{k+i+1}$. Hence, $j(i) = k+i$ and this ends (i). For (ii), assume that $k+i = pi$ and $j(i) < m$. Then, $k+(i+1) < p(i+1)$. Now $1+py+x^p \in H_{k+i}$. So $j(i) \geq k+i$. However, $k+i+1 < p(i+1)$. If $j(i+1) < m$, then $j(i+1) = k+i+1 > j(i)$ gives $j(i) = k+i$. Similarly, one can prove (iii). □

Lemma 3. *Let R be complete.*

(i) *Let e be the smallest positive integer such that $j(e) = m$. Then either $k+e = pe$ or $k+e \geq m$, $pe \geq m$.*
(ii) *Any homomorphic image of R is complete.*

Proof. (i) As $j(e) = m$, by definition $H_e^p = 1$. For any $x \in J$, $(1+x)^p = 1+py+x^p$ for some $y \in R$ with $wt(y) = wt(x)$. Consider any $0 \neq x \in J^e$, then $1 = (1+x)^p = 1+py+x^p$, $py+x^p = 0$. If $py = 0$, then $x^p = 0, k+e \geq m, pe \geq m$. Suppose that $py \neq 0$. Then, $py = -x^p$ gives $k+wt(x) = pwt(x)$. (ii) Let I be a non-zero ideal of R, $I = J^s$ for some $1 \leq s \leq m$. For $T = R/I$, $J(T) = J/J^s$, $H_i(T) = 1+J^i(T)$ and $H_i(T)/H_{i+1}(T) \cong H_i/H_{i+1}$ for $1 \leq i \leq s$. Thus, whenever $i < s$ and $j(i) < s$,

$$H_i(T)/H_{i+1}(T) \cong H_{j(i)}(T)/H_{j(i)+1}(T).$$

For some $i < s$ suppose that $j(i) \geq s$. Then, $H_{j(i)} \subseteq H_s$. However, either $H_i^p = 1$ or $H_i/H_{i+1} \cong H_{j(i)}/H_{j(i)+1}$ under the mapping $(1+x)H_{i+1} \to (1+x)^p H_{j(i)+1}$. Hence, $H_i^p \subseteq 1+J^s$. This shows that $H_i^p(T) = 1$, and thus T is complete with the admissible function j' defined on P_s as follows: $j'(i) = j(i)$ if $j(i) < s$, otherwise $j'(i) = s$. □

Lemma 4. *Let R be complete, and let $(p-1) \mid k$, i.e., $k+s = ps < m$. If $j(s) > k+s$, then the followings hold*

(i) $m = k+s+1$.
(ii) $|\overline{R}| = p$.
(iii) *There exists a unit $v \in R$ such that $px_0 = x_0^p v$ and $1+v \in J$, where $wt(x_0) = s$.*

Conversely, if there exists $x_0 \in J$ with $wt(x_0) = s$, $k+s = ps < m$, and if R satisfies (i), (ii) and (iii), then there exists an admissible function j on P_m for which R is complete.

Proof. Now $k+s+1 < p(s+1)$. If $k+s+1 < m$, by Theorem 1, $j(s+1) = k+s+1$. As $j(s) < j(s+1)$, we get $j(s) = k+s$. This is a contradiction. Hence, $m = k+s+1$ and $j(s) = m$. For any $x \in R$, the binomial expansion gives $(1+x)^p = 1+px+x^p+pz$ for some $z \in R$ with $wt(z) \geq \min\{m, 2wt(x)\}$. Consider any unit $u \in R$. As $px_0^2 = 0$, then,

$$(1+ux_0)^p = 1+pux_0+u^p x_0^p = 1.$$

So, $pux_0 + u^p x_0^p = 0$, and in particular $px_0 + x_0^p = 0$. It follows that $p(u-u^p)x_0 = 0$, and hence $u - u^p \in J$. This proves $|\overline{R}| = p$. The hypothesis gives that $px_0 = x_0^p v$ for some unit $v \in R$. Then, $px_0 + x_0^p = 0$ gives that $1+v \in J$.

For the converse, define j such that $j(i) = pi$ for $i < s$, and $j(i) = m$ for $i \geq s$. Then for any unit $u \in R$, $(1+ux_0)^p = 1+pux_0+u^p x_0^p$. As $u-u^p \in J, 1+u \in J$,

$$pux_0 + u^p x_0^p = p(u-u^p)x_0 + u^p x_0^p(1+u) = 0.$$

Hence, $(1+ux_0)^p = 1$. By using this, and the argument in [2], it can be easily verified that j is an admissible function and that R is complete. □

Theorem 2. *Let R be a finite commutative chain ring with invariants p, n, r, k, m, $\pi^k = p\beta h$, and for some $s \in P_m$, $k + s = ps < m$. Then there exists an admissible function j on P_m such that $j(s) > k + s$, and R is complete if and only if R satisfies the following conditions:*

(i) $m = k + s + 1$.
(ii) $\mid \overline{R} \mid = p$.
(iii) $\beta = -1$ *in* $\overline{R}$.

Proof. Let R be complete and $j(s) > k+s$. Let $x_0 \in J$ such that $wt(x_0) = s$. By Lemma 4, (i) and (ii) hold, and there exists a unit $u \in R$ such that $px_0 = x_0^p u$ and $1 + u \in J$. Now $x_0 = \pi^s w$ for some unit w. Then,

$$p\pi^s w = \pi^{ps} w^p u = \pi^{k+s} w^p u = p\pi^s w^p uy.$$

It follows that $w - w^p uy \in J^{m-k-s} = J$. In $\overline{R}$, $\overline{u} = -1$, by (ii), $\overline{w}^{p-1} = 1$, so $\overline{y} = -1$,, i.e., $\beta = -1$. Conversely, let R satisfy (i), (ii) and (iii). By (iii), $-y^{-1} \in H = H^{p-1}$. Hence, $-y^{-1} = w^{p-1}$ for some $w \in H$. Consider $x = \pi^s w, u = -1$. Then, $px = x^p u$ and $1 + u = 0 \in J$. By Lemma 4, the desired j exists. □

Theorem 3. *Let R be a finite commutative chain ring with invariants p, n, r, k, m, and for some $s \in P_m$, $k + s = ps < m$. Then there exists an admissible function j on P_m such that $j(s) = k + s$ and R is complete if and only if $-\beta \notin \overline{R}^{p-1}$.*

Proof. Suppose that R is complete and $j(s) = k + s$. For any $0 \neq y \in J$, $(1+y)^p = 1 + py + y^p + pz$ for some $z \in R$ with $wt(z) \geq \min\{m, 2wt(y)\}$. Fix an $x \in H_s \setminus H_{s+1}$. As $(1+x)^p \in H_{k+s} \setminus H_{k+s+1}$, then we get $wt(px + x^p) = k + s$. Moreover, $px = x^p u$ for some unit $u \in R$. So $x^p(u+1) \in J^{k+s} \setminus J^{k+s+1}$, and thus $1 + u$ is a unit. For any $c \in R$, as $(1+cx)^p \in H_{k+s} \setminus H_{k+s+1}$, $pcx + c^p x^p = x^p(cu + c^p)$ has weight $k + s$, so $u + c^{p-1}$ is a unit. Thus, in $\overline{R}$, $u \notin \overline{R}^{p-1}$. Now, $x = \pi^s w$ for some unit w. Then, $x^p u = \pi^{k+s} w^p u$, and $px = \pi^{k+s} w y^{-1}$, so $w^{p-1} - (yu)^{-1} \in J^{m-k-s}$. Thus, $\overline{yu} \in \overline{R}^{p-1}$. As $\overline{u} \notin \overline{R}^{p-1,}$ we get $\overline{y} \notin \overline{R}^{p-1}$. Consequently, $-\beta \notin \overline{R}^{p-1}$. Conversely, let $-\beta \notin \overline{R}^{p-1}$. Consider $u = -y^{-1}$, then for any unit $c \in R$, $c^{p-1} + u$ is a unit. It follows that for $x = \pi^s$, $px = x^p u$, $pcx + c^p x^p = x^p(cu + c^p)$ has weight $k + s$, $(1+cx)^p \in H^{k+s} \setminus H^{k+s+1}$, and thus

$$H_s / H_{s+1} \cong H_{s+k} / H_{s+k+1}.$$

For $i < s$, $pi < k + i$, define $j(i) = pi$, and for $i \geq s$, define $j(i) = \min\{m, k+i\}$. By using ([2], Propositions 1 and 2), it follows that j is the desired admissible function. □

Theorem 4. *Let R be a finite commutative chain ring with invariants p, n, r, k, m. If R is complete, then there exists only one admissible function j on P_m.*

Proof. Suppose that $k = m$. Then, *char* $R = p$, $(x+y)^p = x^p + y^p$. Using this it follows that any finite chain ring R of characteristic p is complete and the underlying admissible function j on P_m is such that $j(i) = pi$, whenever $pi < m$, and $j(i) = m$ otherwise. Suppose $k < m$, and j, j' are two different admissible functions on P_m such that R is complete with respect to j as well as j'. It follows from the proof of Theorem 1 that if for some $i < m$, $k + i \neq pi$ and $\min\{k+i, pi\} < m$, then $j(i) = \min\{k + i.pi\} = j'(i)$. If for some $i < m$ and $\min\{k + i.pi\} \geq m$, then $j(i) = m = j'(i)$. So, there exists an $s < m$ such that $k + s = ps < m$ and $j(s) \neq j'(s)$. It follows from Lemma 4 that $\mid \overline{R} \mid = p$, and we can take $j(s) = s + k$, $j'(s) = s + k + 1 = m$. Let J_1 and J_2 be the restriction of j and j', respectively, to $L_s = \{i : s \leq i \leq m\}$. Set $X = \{i : s \leq i \leq s + k\}$. By applying (Theorem 1 (4) [3]), we get two sets of cyclic $p-$subgroups $\{U_i : 1 \leq i \leq m\}$, $\{U'_i : 1 \leq i \leq m\}$ of H corresponding to j and j', respectively. By Proposition 6, $H_s = \oplus_{i \in X} U_i$, so $rank(H_s) = k$. Furthermore, $H_s = \oplus_{i \in Y} U'_i$ gives $rank(H_s) = k + 1$. This is a contradiction, and thus proves the result. □

Remark 2. *By a similar discussion, the above results hold if we assume that R is incomplete.*

Remark 3. *Consider a finite commutative chain ring R with p, n, r, k, m. Let $\pi^k = p\beta h$ be an Eisenstein polynomial of R. By looking at the invariants p, k and the element β, one knows whether a given R is complete or incomplete using Theorems 2 and 3. In any case, the form of the underlying admissible function j on P_m is well defined by:*

$$j(i) = \begin{cases} min\{pi, m\}, & if\ i \leq s^*, \\ min\{i + k, m\}, & if\ i > s^*, \end{cases} \tag{10}$$

where $k = (p-1)s^* + q$, where $0 \leq q < p - 1$.

Example 4. *Let R be a chain ring with invariants $2, 3, 5, 1, 3$ and suppose that $j(1) = 2, j(2) = 3$ and $j(3) = 3$. Then, R is clearly a complete j-diagram with unique admissible function j. This means if there is another admissible function j' such that R is also a complete j'-diagram, then $j = j'$. For the converse, note that if $j_1(1) = j_1(2) = j_1(3) = 3$ which is an admissible function but R is not j_1-diagram. This means the existence of an admissible function j on P_m is not enough to say R is j-diagram (either complete or not), see Definition 2. Thus, in general, the converse is not true.*

Proposition 1. *Let R be a finite commutative chain ring with p, n, r, k, m. If $(p-1) \nmid k$ or $m \leq k + s^*$, then R is complete.*

Proof. Note that for $x \in U(R)$,

$$(1 + \pi^{s^*} x)^p = \begin{cases} 1 + p\pi^{s^*} u + \pi^{s^* p} x^p, & \text{if } m > k + s^*, \\ 1, & \text{if } m \leq k + s^*, \end{cases} \tag{11}$$

where $u \in U(R)$. Thus, if $m \leq k + s^*$, then clearly the series (7) is a complete j-diagram, and hence R is complete. Now, assume that $m > k + s^*$. If $(p-1) \nmid k$, $q \neq 0$, and hence $s^* p < k + s^*$. It follows from Equation (11) that

$$(1 + \pi^{s^*} x)^p = 1 + \pi^{s^* p} x_1 \bmod H_{s^* p + 1},$$

for some $x_1 \in U(R)$. Furthermore, when $s > s^*$, $\eta_s = \gamma_{s+k}^{-1} \cdot \delta_s \cdot \gamma_s$, where γ_s and δ_s are defined in Lemma 2 Thus, η_s is an isomorphism. In case of $s \leq s^*$, consider the map

$$\begin{aligned} \beta_s : J^s / J^{s+1} &\longrightarrow J^{sp} / J^{sp+1} \\ x + J^{s+1} &\longmapsto x^p + J^{sp+1} \end{aligned}$$

One can prove easily that β_s is well-defined, and moreover, is a monomorphism. For epimorphism, note that since $\overline{R}$ is a finite field, then $\overline{R}^p = \overline{R}$, a basic field. That is, if $y \in J^{sp} \setminus J^{sp+1}$, then $y = \pi^{sp} y_0 \bmod J^{sp+1}$ where $y_1 \in \overline{R}^*$. Then, there is y_2 such that $y_1 = y_2^p$ and then $\beta(x^s y_2) = y \bmod N^{ps+1}$. Therefore, β_s is an isomorphism and $\eta_s = \gamma_{sp}^{-1} \cdot \beta_s \cdot \gamma_s$, which means η_s is an isomorphism. □

Corollary 1. *Any finite commutative chain ring R with characteristic p is complete.*

Proof. Since $n = 1$, then $k = m$ which means that $m < k + s^*$, and by Proposition 1, R is complete. □

Remark 4. *By Proposition 1, when $q \neq 0$ ($(p-1) \nmid k$) the j-diagram for H is independent of the Eisenstein polynomial $\pi^k = p\beta h$. However, this is not true when $q = 0$, i.e., $k + s^* = ps^*$. Let $x \in U(R)$, by Equation (11),*

$$(1+\pi^{s^*}x)^p = 1 + p\pi^{s^*}x + \pi^{s^*p}x^p \ mod\ H_{j(s^*)+1}$$
$$= 1 + \pi^{s^*+k}((\beta h)^{-1}x + x^p) \ mod\ H_{j(s^*)+1}.$$

Thus, $(1+\pi^{s^*}x)^p = 1$ mod $H_{j(s^*)+1}$ if and only if $(\beta h)^{-1}x + x^p = 0$ mod J, i.e., $x^{p-1} + \beta = 0$ in $\overline{R}^*$.

Proposition 2. *If $m > k + s^*$, then η_{s^*} is an isomorphism if and only if $-\beta \notin \overline{R}^{*\,p-1}$.*

Proof. If η_{s^*} is an isomorphism, then $\ker \eta_{s^*} = \{H_{s^*+1}\}$, which means that $(1+\pi^{s^*}a)^p \neq 1$ mod $H_{j(s^*)+1}$, for any $a \in \overline{R}^*$. Hence, $x^{p-1} + \beta$ has no zeros in $\overline{R}^*$ and thus $-\beta \notin \overline{R}^{*\,p-1}$. The converse is direct by Theorem 3. □

The following theorem gives a characterization of incomplete chain rings.

Theorem 5. *Suppose that R has invaraints p, n, r, k, m with $m > k + s^*$. Therefore, the subsequent hypotheses are equivalent:*

(i) R is incomplete.
(ii) There is $\alpha \in R$ such that $\alpha^{p-1} + p = 0$.
(iii) $p - 1$ divides k and there exists $\alpha \in \overline{R}^*$ such that $-\beta = \alpha^{(p-1)}$.

Proof. Let (i) be satisfied, thus $\ker \eta_{s^*} \neq 1$ because η_{s^*} is surjective. In this case, there is $1 + \alpha\pi^{s^*}$ in $\ker \eta_{s^*}$ with

$$(1+\alpha\pi^{s^*})^p = 1 + \alpha^p\pi^{s^*p} - \beta\alpha\pi^{s^*+k}\xi = 1$$

mod H_{s^*p+1}, where $\xi \in H$. However, the above equation holds when $ps^* = s^* + k$ and $\alpha^p + \beta\alpha = 0$ mod π. Now, assume that $(p-1) \mid k$, then $\ker \eta_{s^*} \cong \ker f$, where f is a homomorphism; $f : \overline{R} \to \overline{R}$ and $f(\alpha) = \alpha^p + \beta\alpha$. Moreover, $\ker f = 1$ if and only if $x^p + \beta x$ has only zero solution. Thus, $(\beta_1 h_1 \pi)^{s^*}$ is a root of $x^{p-1} + p$ in R, where $\beta_1 = \alpha^{-1}$ and $h_1^{p-1} = h$. The remaining hypotheses follow immediately by Proposition 2 and Theorem 3. □

Corollary 2. *If R is an incomplete chain ring, then $\ker \eta_{s^*}$ is of rank p.*

Proof. Since any element in $\ker \eta_{s_1}$ is of the form $1 + \alpha\pi^{s^*}$, where α is a zero of the polynomial $x^p + \beta x$. Thus, the order of $\ker \eta_{s^*}$ is exactly p since there are p distinct zeros of $x^p + \beta x$ in $\overline{R}$. □

Lemma 5. *Let R be a finite commutative chain ring with invaraints p, n, r, k, m.*

(a) If $n > 2$ or $n = 2$ and $t > s^*$. Then, $m > k + s^*$.
(b) If $n \leq 2$, $t \leq s^*$. Then, $m \leq k + s^*$.

Proof. Part (b) is obvious; note that if $n = 1$, then $m = k = t$. For part (a),

$$
\begin{aligned}
m &= (n-1)k + t = (n-1)((p-1)s^* + q) + t \\
&= (n-1)(ps^* - s^* + q) + t \\
&= (n-1)(ps^* + q)) - (n-1)s^* + t \\
&= (n-1)(k + s^*) + t - (n-1)s^* \\
&= (k + s^*) + (n-2)k + t - (n-1)s^* \\
&= (k + s^*) + (n-2)k + +(n-2-n+1)s^* \\
&= (k + s^*) + (n-2)k + t - s^*.
\end{aligned}
$$

However, $s^* < k$ and $n > 2$, then $(n-2)k - s^* > 0$, thus, $m > k + s^*$. □

Proposition 3. *If $s > k + s^*$, then $s \in R(j)$. Furthermore,*

$$c_0 =\mid P_m \setminus R(j) \mid = \begin{cases} m - \lfloor \frac{m}{p} \rfloor, & \text{if } m < k + s^*, \\ k, & \text{otherwise}, \end{cases} \tag{12}$$

where $\lfloor x \rfloor$ means the greatest integer that is less than or equal to x.

Proof. Let$s = k + s^* + e$, for some $e > 0$, then clearly $s = j(s^* + e)$, which means $s \in R(j)$. If $m \geq k + s^*$, then it is clear that $P_m \setminus R(j) = \{s \in P_m : p \nmid s, 1 \leq s \leq k + s^*\}$. Thus,

$$c_0 = k + s^* - \lfloor \frac{k + s^*}{p} \rfloor = \lfloor \frac{(p-1)s^* + q + s^*}{p} \rfloor = \lfloor \frac{ps^* + q}{p} \rfloor = k + s^* - s^* = k.$$

For the case $m < k + s^*$, $P_m \setminus R(j) = \{s \in P_m : p \nmid s, s < m\}$, and thus,

$$c_0 = m - \lfloor \frac{m}{p} \rfloor.$$

□

Proposition 4. *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

$$j(j(s) + 2) \geq j(j(s) + 1) \geq j(1) = p, \tag{13}$$

it follows that $j(s) + 2, j(s) + 1$ are elements of $R(j)$. This means $u_{j(s)+1} = u_{s_1}^p$. As we proceed, we get $y = y_0^p$, and thus $H_{j(s)} \subseteq H_s^p$. Therefore, $H_{j(s)} = H_s^p$. If $i > 1$, observe that $H_s^{p^i} = (H_s^{p^{i-1}})^p$, and hence the conclusion is drawn from the induction step. □

Next, we give an important result; that is useful in capturing the structure of the subgroups H_s of H via the following j-subdiagram:

$$H_s > H_{s+1} > \cdots > H_m = 1.$$

Which in turn helps us to investigate the group of automorphisms of R, for more details see Remark 4.2.10 in [4].

The following result for finite abelian groups can be easily proved.

Lemma 6. *Let G be a finite direct product of cyclic groups, each of order p^e for some $e \geq 1$. Let U' be a subgroup of G which is a direct product of cyclic groups B_i, each of order $p^{e'}$, and* *for which $rank(U') = rank(G)$. Then, $G = A_1 \otimes A_2 \otimes \cdots \otimes A_s$ such that each A_i is a cyclic group and $B_i = U' \cap A_i$. Moreover, for any $s \geq 1$, $G^{p^{e-e'-c}} = \{g \in G : g^{p^s} \in U'\}$, where $c = min\{e - e', s\}$.*

Theorem 6. *Let $A = A_1 > A_2 > \cdots > A_m = 1$ be a complete $j-$diagram for an abelian p-group A, $0 \leq s < m$ and $L_{m-s} = \{i : m - s \leq i \leq m\}$. Let $j' = j \mid_{L_{m-s}}$ and $X_s = \{i \in L_{m-s} : i \notin R(j')\}$. Then,*

(a) $A_{m-s} = \otimes_{i \in X_s} U_i$.

(b) $X_s = B \cup C$ *satisfying the following conditions:*

- *(i)* $B \cap R(j) = \phi$,
- *(ii)* *There exists a subset D of $P_m \setminus R(j)$ disjoint form B and a one to one mapping $j_1 : D \to C$ such that for any $i \in D, j_1(i) = j^{e_i}(i)$ for some $e_i \geq 1$. Suppose $P' = (P_m \setminus R(j)) \setminus (D \cup B)$, $E = \otimes_{i \in P'} U_i$ and $F' = \otimes_{i \in (B \cup D)} U_i$.*
- *(iii)* *$A = E \otimes F'$, $A_{m-s} = (\otimes_{i \in B} U_i) \otimes (\otimes_{i \in D} U_i{}^{p^{e_i}}) \subseteq F$ and $rank(A_{m-s}) = rank(F')$.*
- *(iv)* *Let $c \geq 0$ and $P_1 = \{i \in P' : \nu(i) \leq c\}$. Then,*

$$G = \{x \in A : x^{p^c} \in A_{m-s}\} = (\otimes_{i \in P_1} U_i) \otimes (\otimes_{i \in B} U_i) \otimes (\otimes_{i \in D} U_i^{p^{e_i - min\{e_i, c\}}}). \quad (14)$$

Proof. (a) Put $K_i = A_{m+i-s-1}, 1 \leq i \leq s+1$. Then, $A_{m-s} = K_1 > K_2 > \cdots > K_{s+1} = 1$ is a complete j^*-diagram, where $j^* : P_{s+1} \to P_{s+1}$ is given by $j^*(i) = j(m - s - 1 - i) - (m - s - 1)$. Note that $K_i = K_{i+1} \times U_{m-s-1+1}$. By [Theorem 1 [3]],

$$A_{m-s} = \otimes_{i \notin R(j^*)} U_{m-s-1+i} = \otimes_{i \in X_s} U_i. \quad (15)$$

(b) Write $X_k = B \cup C$ with $B \subseteq P_m \setminus R(j)$ and $C \subseteq R(j)$. It is clear that $m \notin C$. Suppose that all U_i have the same rank. For each $i \in C$, there exists a positive integer e_i, and a unique i' such that $i = j^{e_i}(i')$. Thus, $U_i = U_{j^{e_i}(i')} = U_{i'}^{p^{e_i}} \subseteq U_{i'}$. It follows that from the definition of j, $D = \{i' : i \in C\}$ is disjoint from B and there exists a bijection $j_1 : D \to C$, such that $j_1(i) = j^{e_i}(i)$. This proves (ii). Hence,

$$A_{m-s} = \otimes_{i \in B} U_i \otimes_{i \in D} p^{e_i} U_i \subseteq F'.$$

This proves (iii). Finally, consider $c \geq 0$ and $G = \{x \in A : x^{p^c} \in A_{m-s}\}$. Observe that any $x \in A$ is in G if and only if each of its components in the decomposition $A = E \otimes F'$ is in G. For any $x \in E$, $x^{p^c} \in A_{m-s}$ implies $x^{p^c} = 1$. For any $i \in P'$, $U_i^{p^c} = 1$, whenever $\nu(i) \leq c$. So $E \cap G = \times_{i \in P_1} U_i$. Consider any $i \in D$. Now, $U_i \cap G = \{x \in U_i : x^{p^c} \in U_i^{p^{e_i}}\}$. As the order of U_i is $p^{\nu(i)}$ and the order of $U_i^{p^{e_i}}$ is $p^{\nu(i)-e_i}$, then by Lemma 6,

$$U_i \cap G = U_i^{p^{e_i - \min\{e_i, c\}}}.$$

Thus,

$$G = (\otimes_{i \in P_1} U_i) \otimes (\otimes_{i \in B} U_i) \otimes (\otimes_{i \in D} U_i^{p^{e_i - \min\{e_i, c\}}}).$$

□

4. Conclusions

In this article, we have investigated j-diagrams for one group of finite commutative chain rings. Under certain conditions concerning the invariants p, n, r, k, m and Eisenstein polynomials, we proved the existence and uniqueness of such j-diagrams. These j-diagrams have been found helpful tools in investigating finite chain rings.

Author Contributions: Conceptualization, S.A. and Y.A.; Methodology, S.A. and Y.A.; Formal analysis, S.A.; Investigation, S.A.; Writing–original draft, S.A.; Writing–review and editing, S.A. and Y.A.; Supervision, Y.A. All authors have read and agreed to the published version of the manuscript.

Funding: This research was supported by the Researchers Supporting Project number (RSPD2023R545), King Saud University, Riyadh, Saudi Arabia.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: The authors would like to acknowledge the Researchers Supporting Project number (RSPD2023R545), King Saud University, Riyadh, Saudi Arabia.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Alabiad, S.; Alkhamees Y. Recapturing the structure of group of units of any finite commutative chain rings. *Symmetry* **2021**, *13*, 307. [CrossRef]
2. Ayoub, C. On the group of units for certain rings. *J. Number Theory* **1972**, *4*, 383-403. [CrossRef]
3. Ayoub, C. On diagrams for abelian groups. *J. Number Theory* **1970**, *2*, 442–458. [CrossRef]
4. Alabiad, S.; Alkhamees, Y. On automorphism groups of finite chain rings. *Symmetry* **2021**, **13**, 681. [CrossRef]
5. Hou, X. Finite commutative chain rings. *Finite Fields Appl.* **2001**, *7*, 382–396. [CrossRef]
6. Clark, W.; Liang, J. Enumeration of finite commutative chain rings. *J. Algebra* **1973**, *27*, 445–453. [CrossRef]
7. Clark, W.; Drake, D. Finite chain rings. *Abh. Math. Sem .Uni. Hambg.* **1973**, *29*, 147–153. [CrossRef]
8. Clark, W. A coefficient ring for finite non-commutative rings. *Proc. Amer. Math. Soc.* **1972**, *33*, 25–28. [CrossRef]
9. Hou, X. Bent functions, partial difference sets and quasi-Frobenius local rings. *Des. Codes Cryptogr.* **2000** , *20*, 251–268. [CrossRef]
10. Klingenberg, W. Projective und affine Ebenen mit Nachbarelementen. *Math. Z.* **1960**, *60*, 384–406. [CrossRef]
11. Ma, S.; Schmidt, B. Relative (p^a, p^b, p^a, p^{a-b})-relative difference sets: a unified exponent bound and a local ring construction. *Finite Fields Appl.* **2000**, *6* 1–22. [CrossRef]
12. Artman, B.; Dorn, G.; Drake, D.; Törner, G. Hjelmslev'sche Inzidenzgeometrie und verwandte Gebiete—Literaturverzeichnis. *J. Geom.* **1976**, *7*, 175–191. [CrossRef]
13. Sălăgean, A. Repeated-root cyclic and negacyclic codes over finite chain rings. *Discret. Appl. Math.* **2006**, *154*, 413–419. [CrossRef]
14. Dinh, H.; López-Permouth, S. Cyclic and negacyclic codes over finite chain rings. *IEEE Trans. Inform. Theory* **2004**, *50*, 1728–1744. [CrossRef]
15. Dinh, H. Negacyclic codes of length 2^s over Galois rings. *IEEE Trans. Inform. Theory* **2005**, *51*, 4252–4262. [CrossRef]
16. Lui, X.; Lui, H. LCD codes over finite chain rings. *Finite Fields Appl.* **2015**, *43*, 1–19.
17. Greferath, M. Cyclic codes over finite rings. *Discret. Math.* **1997**, *177*, 273–277. [CrossRef]
18. Luis, M. Incomplete j-diagrams fail to capture group structure. *J. Algebra* **1991**, *144*, 88–93. [CrossRef]