symmetry

MDPI

Article

Recapturing the Structure of Group of Units of Any Finite Commutative Chain Ring

Sami Alabiad *,† **and Yousef Alkhamees** †

Department of Mathematics, College of Science, King Saud University, Riyadh 11451, Saudi Arabia; ykhamees@ksu.edu.sa

* Correspondence: ssaif1@ksu.edu.sa

† These authors contributed equally to this work.

Abstract: A finite ring with an identity whose lattice of ideals forms a unique chain is called a finite chain ring. Let R be a commutative chain ring with invariants p, n, r, k, m. It is known that R is an Eisenstein extension of degree k of a Galois ring $S = GR(p^n, r)$. If $p-1$ does not divide k, the structure of the unit group $U(R)$ is known. The case $(p-1) \mid k$ was partially considered by M. Luis (1991) by providing counterexamples demonstrated that the results of Ayoub failed to capture the direct decomposition of $U(R)$. In this article, we manage to determine the structure of $U(R)$ when $(p-1) \mid k$ by fixing Ayoub's approach. We also sharpen our results by introducing a system of generators for the unit group and enumerating the generators of the same order.

Keywords: finite chain rings; group of units; Galois rings; j-diagrams

1. Introduction

In this article, we consider finite commuative chain rings, although some results still correct under more general situation. Ayoub called these rings (cf. [1]) primary homogeneous rings. Such rings arise in various places; in Coding Theory (cf. for example [2,3]); in Geometry (cf. [4]). It is well-known that every finite chain ring R is an Eisenstein extension of some degree k over a Galois ring of the form $S = GR(p^n, r)$. There are positive integers p, n, r, k and m associated with R, called invariants of R. Our main aim in this study is to obtain the structure of the multiplicative group $U(R)$ of R. In (1972) (cf. [1]), Ayoub obtained various results based on ideas (cf. [5]) regarding j-diagrams for abelian p-groups.

One major result claims that the factorization of an abelian $p-$group with incomplete j-diagram can be completely obtained by the mentioned diagram. This idea was then used to find the structure of $U(R)$ when R is not necessarily finite (Theorem 3, Section 4 [1]). However, later, it turned out that incomplete j-diagrams failed to determine the exact decomposition of multiplicative groups of some examples introduced by Luis [6]. On the other hand, Hou [7] by different approach gave the structure of $U(R)$ in a special case; $p \nmid k$. This sudy demonstrates that the result (Theorem 3, [1]) is still valid in some cases, for instance the case studied in [7]. Additionally, we enhance the idea that incomplete j-diagrams are generally not enough to obtain the decomposition of bounded p-groups. That is, there is a relation amongst the generators which plays essential role in determining the structure. That relation depends not only on the related incomplete j-diagram, but also on the Eisenstein polynomial by which R is constructed over its coefficient subring $GR(p^n, r)$. However, with this relation being taken into consideration, we manage to make incomplete j-diagrams succeed in recapturing the structure of multiplcative groups of finite chain rings. In addition, a set of linearly independent generators for $U(R)$ is provided and, further, the number of such generators is computed for each possible order. Finally, we give the correct version of ([5], p. 458).

check for updates

Citation: Alabiad, S.; Alkhamees, Y. Recapturing the Structure of Group of Units of Any Finite Commutative Chain Ring. *Symmetry* **2021**, *13*, 307. https://doi.org/10.3390/sym13020307

Academic Editor: José Carlos R. Alcantud

Received: 12 January 2021

Accepted: 8 February 2021

Published: 11 February 2021

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

2. Preliminaries and Notations

In what follows, R will denote a finite commutative chain ring of characteristic p^n and nonzero radical N (the case when $N = 0$, R is a field) with index of nilpotency m. The residue field $F = R/N$ is a finite field of order p^r. We now state some facts and introduce notations that we shall use throughout. For the details, we refer the reader to [8] for finite chain rings and [1,5] for j-diagrams.

The ring R contains a subring (coefficient subring) S of the form $S = GR(p^n, r) \cong Z_{p^n}[a]$, where a is an element of S of multiplicative order $p^r - 1$. If $\pi \in N \setminus N^2$, it is easy to see that $N = (\pi)$, since N/N^2 is of 1 dimension over F. In this case, R is expressed as:

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

(as $S-$module) where k is the greatest integer $i \leq m$ such that $p \in N^i$. It follows that

$$\pi^k = p \sum_{i=0}^{k-1} s_i \pi^i, \tag{2}$$

where $s_i \in S$. This means that π is a root of an Eisenstein polynomial over S of the form:

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

The positive integers p, n, r, k and m are called invariants of R. Furthermore, $m = (n-1)k + t$, for some $1 \leq t \leq k$. Let $H_s = 1 + N^s$, $s \in P_m = \{1, 2, \ldots, m\}$ and consider the following filtering:

$$H = H_1 > H_2 > H_3 > \cdots > H_m =< 1 >, \tag{4}$$

joined with a function j defined as:

$$j(s) = \begin{cases} \min(ps, m), & s \leq u, \\ \min(s + k, m), & s > u, \end{cases} \tag{5}$$

where $k = (p-1)u + v$, $0 \leq v < p - 1$. Note that if $\mathrm{Char}(R) = p$, i.e., $n = 1$, put $k = m$. The series (4) with j defined in (5) and the p-th power homomorphisms η_s from H_s/H_{s+1} into $H_{j(s)}/H_{j(s)+1}$ form what we call j-diagram. However, we refer to the series (4) when we mention j-diagram. If there exists $m \neq s' \in P_m$, such that $\eta_{s'}$ is not an isomorphism, we then call the series (4) incomplete j-diagram at s' and complete j-diagram otherwise (all η_s are isomorphisms).

We denote, by $U(R)$, the units group of R, and so one can verify that

$$U(R) =< a > \otimes H, \tag{6}$$

where $< a >$ is a cyclic group of order $p^r - 1$ and $H = 1 + \pi R$ is the p-Sylow subgroup of $U(R)$. The structure problem of $U(R)$ is then reduced to that of H. After Ayoub [1] we call H the One Group of $U(R)$. If $N_m(e)$ is the number of basis elements in H whose orders p^e, then H is decomposed as:

$$H \cong \otimes_e (C_{p^e})^{N_m(e)}, \tag{7}$$

where C_{p^e} is a cyclic group of order p^e. We define p-rank N_m of H as

$$p^{N_m} = [H : H^p]. \tag{8}$$

If $\pi \in \mathrm{N} \backslash N^2$ fixed, then from Eisenstein polynomial (3)

$$\pi^k = -p\beta h, \tag{9}$$

where $\beta \in < a >$ and $h \in H$. Now, let $\{\alpha_i\}_{1\leq i\leq r}$ be a representatives system in R for a basis of F over its prime field ($\mathbb{Z}_p$). Set

$$w_{is} = 1 + \alpha_i \pi^s (1 \leq i \leq r \text{ and } s \notin R(j)), \qquad (*)$$

where $R(j)$ is the range of j. For each $s \in P_m$, let U_s be a subgroup of H generated by $\{w_{is}\}_{1\leq i\leq r}$. Hence one can easily show that $H_s = U_s \times H_{s+1}$. Now, if (4) is a complete $j-$diagram, then, from (cf. [1]), the system $\{w_{is}\}$ $(*)$ forms a basis for H.

Proposition 1 (Theorem 3, [1]). *Assume that (4) is a complete j-diagram. Then,*

$$H = \otimes_{s\notin R(j)} U_s. \qquad (10)$$

The purpose of the present paper is to establish a basis for H when (4) is an incomplete j-diagram at u. Moreover, $N_m(e)$ and N_m are determined in both cases (complete and incomplete) in Theorems 3 and 4.

Unless otherwise mentioned, all of the symbols stated above will retain their meanings throughout and, additionally, if $s \in P_m$, $\nu_m(s)$ is the least positive number fulfilling $j^{\nu_m(s)}(s) = m$.

3. The Determination of the Structure of *H*

Throughout this section, $k = k_1 p^l$, where $(k_1, p) = 1$ and $l \geq 0$. The following proposition is useful and it will be needed later.

Proposition 2. *If $m > k + u$, then the following conditions are equivalent:*
(i) The series (4) is an incomplete j-diagram at u.
(ii) The polynomial $x^{p-1} + p$ has a root in R.
(iii) $p - 1 \mid k$ and $\beta \in F^{*p-1}$.

Proof. Assume that (i) holds, then $\ker \eta_u \neq 1$ since η_u is onto. Then there is $1 + \alpha\pi^u \in \ker \eta_u$, such that $(1 + \alpha\pi^u)^p = 1 + \alpha^p \pi^{up} - \beta\alpha\pi^{u+k}\xi = 1 \bmod H_{up+1}$, where $\xi \in H$. This only happens when $pu = u + k$ and $\alpha^p - \beta\alpha = 0 \bmod p$. Hence, if $(p - 1) \mid k$, $\ker \eta_u$ is isomorhpic to that of the homomorphism, $f : F \to F$ defined by: $f(\alpha) = \alpha^p - \beta\alpha$. However, $\ker f \neq 1$ if and only if $x^p - \beta x$ has nonzero solutions in F. The remaining hypotheses follow immediately. □

Definition 1. *We call R incomplete (complete) chain ring if one of the equivalent conditions in Proposition 2 holds (otherwise).*

Corollary 1. *If R is an incomplete chain ring, then $\ker \eta_u$ is of rank p.*

Remark 1. *In the light of Proposition 2 and its corollary, $v = 0$ and $k_1 = (p-1)s_0$, i.e., $u = s_0 p^l$. Furthermore, if η is the composition of $\eta_{s_0}, \ldots, \eta_u$ then $\ker \eta$ is of rank p. Let*

$$\xi = 1 + \alpha_1 \pi^{s_0} \qquad (11)$$

be a generator of $\ker \eta$.

Assume that f is as mentioned in the proof of Proposition 2 and $\lambda = l + 1$. Construct the following system:

$$\begin{cases} w_{is} = 1 + \alpha_i \pi^s, \quad \text{for } 1 \leq i \leq r \text{ and } s \notin R(j), \\ \gamma = 1 + \alpha_0 \pi^{up}, \\ \text{where } \alpha_1^{p^\lambda} - \beta\alpha_1^{p^{\lambda-1}} = 0 \text{ and } \alpha_0 \notin \operatorname{Im} f. \end{cases} \qquad (**)$$

The following proposition is stated without proof, since it involves the same ideas of that in the complete case.

Proposition 3. *The set* $\{w_{is}, \gamma\}$ $(**)$ *represents a system of generators for* H.

Put

$$B = \{(i,s) : 1 \leq i \leq r \text{ and } s \notin R(j)\} \setminus \{(1, s_0)\}. \tag{12}$$

Observe that $\xi = w_{1s_0} \in \ker \eta$ and then

$$\xi^{p^\lambda} = \prod_{(i,s)\in B} w_{is}^{a_{is}} \cdot \gamma^{a_0} = y^{p^\mu}, \tag{13}$$

where a_{is} and a_0 are positive integers that are divisible by p, i.e., $\mu \geq 1$. Note that μ will keep its meaning throughout the paper, as described here. Let H_0 be a subgroup of H that is generated by $\{\gamma, w_{is}\}_{(i,s)\in B}$. Thus, by (cf. [1]), H_0 has a direct decomposition,

$$H_0 = \otimes_{(i,s)\in B} < w_{is} > \otimes < \gamma > . \tag{14}$$

Theorem 1. *Let* R *be an incomplete chain ring and* $\lambda \leq \mu$, *then*

$$H \cong H_0 \otimes D, \tag{15}$$

where D *is a cyclic group of order* p^λ.

Proof. By Equation (13), it is clear that $H_0 \cap < \xi > = < \xi^{p^\lambda} >$ and also H_0 is a p-pure subgroup of H; every element is not of a smaller p-height in H_0 than in H. Thus, by the results from (cf. [9]), H_0 is a direct summand of H. This finishes the proof. □

Corollary 2. *If* $\zeta = \xi y^{p^{\mu-\lambda}}$, *then* $\{\gamma, \zeta, w_{is}\}_{(i,s)\in B}$ *is a basis for* H.

Corollary 3. *The system* $\{\gamma, \xi, w_{is}\}_{(i,s)\in B}$ *is a basis for* H *if and only if* $o(\xi) = \lambda$ *(the order of* ξ*).*

Remark 2.

(1) It is worthy to mention that Theorem 1 coincides with Ayoub's results (Theorem 3 Section 4, [1]). That means in such case, incomplete j-diagrams succeed in retrieving the structure of H.
(2) If $p \nmid k$, *then obviously* $\lambda = 1 \leq \mu$ *and, thus, the result that is given in* [7] *is just a particular case of Theorem 1.*

From now on, we assume $\lambda > \mu$. Consider Equation (13) and let

$$\begin{cases} A = \{(i,s) \in B\} \cup \{(i',s')\}, \\ w_{i's'} = \gamma \text{ and } a'_{i's'} = a_0. \end{cases} \tag{16}$$

Lemma 1. *If* R *is an incomplete chain ring and* $\lambda > \mu$, *then there is a positive integer* d *and p-pure subgroups* G_i *of* H, *such that* $G_{i+1} \subseteq G_i$, $1 \leq i \leq d-1$.

Proof. For $(i,s) \in A$, let $a_{is} = v_p(a'_{is})$, where v_p is the p-adic valuation. Subsequently, it is clear that $\mu \leq a_{is}$ for all $(i,s) \in A$. Choose $(i_1, s_1) \in A$ such that $a_{i_1 s_1} = \mu$. If there are more than one of s satisfying $a_{is} = \mu$, choose the smallest one. Let h_{is} be defined as $a'_{is} = h_{is} p^{a_{is}}$, $(h_{is}, p) = 1$. If $B_1 = A \setminus \{(i_1, s_1)\}$, $h_1 = h_{i_1 s_1}$ and $w_1 = w_{i_1 s_1}^{h_1}$, then Equation (13) can be rewritten as:

$$w_1^{p^\mu} = (\xi^{p^{\lambda-\mu}} \tau)^{p^{f_1}}, \tag{17}$$

where $\tau = \prod_{(i,s)\in B_1} w_{is}^{\delta_{is}}$, $\delta_{is} = -h_{is} p^{a_{is}-\mu_1}$ and $f_1 = \min\{a_{is} : (i,s) \in B_1\}$. Define G_1 to be the subgroup of H that is generated by $\{w_{is}, \xi\}_{(i,s)\in B_1}$. Thus, from (17), $G_1 \cap \{w_1\} = <$

$w_1^{p^\mu} >$. Because $\mu \leq f_1$, then the p-height of w_1 in G_1 is not lesser than that in H and thus G_1 is a p-pure subgroup of H. Now, if we raise Equation (17) to $p^{\nu(s_1)-\mu}$, we obtain a new relation among the generators of G_1,

$$\xi^{p^{\lambda+\nu(s_1)-\mu}} = \prod_{(i,s)\in B_1'} {w_{is}}^{b_{is}'}, \tag{18}$$

where $b_{is}' = c_{is}p^{a_{is}+\nu(s_1)-\mu}$, and $B_1' \subseteq B_1$, because some generators might disappear due to raising (17) to a power of p. Note that since the generators on the right side of Equation (18) are linearly independent, thus the left side cannot vanish. Again, there is (i_2, s_2) such that $a_{i_2s_2} = a_2 \geq \mu$ is the smallest a_{is} ($(i,s) \in B_1'$) and then

$$\mu_2 = b_{i_2s_2} = v_p(b_{i_2s_2}') = a_2 + \nu(s_1) - \mu \tag{19}$$

is the smallest $b_{is} = v_p(b_{is}')$, $(i,s) \in B_1'$. Assume that $w_2 = w_{i_2s_2}^{h_{i_2s_2}}$, then we have a similar situation to that of w_1. Let $B_2 = B_1' \setminus \{(i_2, s_2)\}$ and G_2 be a subgroup of G_1 generated by ξ and all w_{is} with $(i,s) \in B_2$. By a similar arguement, G_2 is a p-pure subgroup of G_1 and, thus, transitively (Lemma 26.1, [9]) G_2 is a p-pure subgroup of H. Therefore, after a finite number d of similar processes, we obtain:

$$\begin{cases} I = \{(i_1,s_1),\ldots,(i_d,s_d)\} \subseteq A; \\ J = \{w_1,\ldots,w_d\},\ w_q = w_{i_qs_q}^{h_{i_qs_q}} \text{ and } (i_q,s_q) \in I; \\ G_d \subseteq G_{d-1} \subseteq \cdots \subseteq G_1 \subseteq H,\ G_i = G_{i+1} \times < w_i >; \\ \mu_1 = \mu \leq \mu_2 \leq \cdots \leq \mu_d \text{ subjected to} \begin{cases} w_i^{p^{\mu_i}} = y_i^{p^{f_i}}, \\ y_i \in G_i \text{ and } \mu_i \leq f_i; \end{cases} \\ \xi^{p^{\lambda_0}} = 1,\ \lambda_0 = \lambda + \sum_{i=1}^{d}(\nu(s_i) - \mu_i). \end{cases} \tag{20}$$

□

Remark 3. *Based on notations that were introduced in Lemma 1, put* $\Omega = \{s_1,\ldots,s_d\}$ *and let*

$$G_d = \begin{cases} \prod_{s\in\Lambda} U_s \times \prod_{s\in\Omega'} U_s^* \times < \xi >, & \text{if } (i',s') \in I, \\ \prod_{s\in\Lambda} U_s \times \prod_{s\in\Omega'} U_s^* \times < \xi > \times < \gamma >, & \text{if } (i',s') \notin I, \end{cases} \tag{21}$$

where $\Lambda = \{P_m \setminus R(j)\} \setminus \Omega'$ *and* $\Omega' = \Omega \cup \{s_0\}$.

Theorem 2. *Let R be an incomplete finite chain ring with invariants p, n, r, k, m such that $\lambda > \mu$. Then,*

$$H = \otimes_{s\in\Lambda} U_s \otimes_{i=1}^{d} (U_{s_i}^* \otimes D_i) \otimes D \otimes C, \tag{22}$$

(i) U_s is a direct product of r cyclic groups of order $p^{\nu(s)}$.
(ii) $U_{s_i}^*$ is a direct product of $r-1$ cyclic groups of order $p^{\nu(s_i)}$, and D_i is a cyclic group of order p^{μ_i}.
(iii) D is a cyclic group of order $\lambda_0 = \lambda + \sum_{i=1}^{d}(\nu(s_i) - \mu_i)$.
(iv) C is a cyclic group of order $p^{\nu(u)-1}$ if $(i',s') \notin I$ and $C =< 1 >$ otherwise.

Proof. Because, for each $1 \leq i \leq d-1$, G_{i+1} is a p-pure subgroup of G_i (Lemma 1) and also a bounded p-group, then (Theorem 27.5, [9]) G_{i+1} is a direct summand of G_i; there is a subgroup $L \subseteq G_i$, such that $G_i = G_{i+1} \otimes L$. Thus, based on (20) and Remark 3,

$$L \cong G_i/G_{i+1} = G_{i+1} \times < w_i > /G_{i+1} =< w_i > /G_{i+1} \cap < w_i > .$$

By the argument of the proof of Lemma 1, $G_{i+1} \cap < w_i >=< w_i^{p^{\mu_i}} >$. Hence, $G_i = G_{i+1} \otimes D_i$, where D_i is a cyclic group of order p^{μ_i}. Therefore, the decomposition (22) is just a result of successive application to the above argument. Note that $D =< \xi >$. □

Corollary 4. *With the same assumption in Theorem 2, $N_m = cr + 1$.*

Corollary 5. *$\{w_{is}\}$ $((i,s) \in B \setminus I)$, $\{w_i y_i^{-p^{f_i-\mu_i}}\}$ $(1 \le i \le d)$, ξ and η if $(i',s') \notin I$ form a basis of H.*

The following example demonstrates the failure of Ayoub's results (Theorem 3, [1]); non-isomorphic abelian p-groups may have the same incomplete j-diagrams. Furthermore, it shows how Eisenstein polynomials play a key role in factorizing H.

Example 1. *Let R be a finite chain ring with invariants $2,3,1,2,6$ and $\pi^2 = 2$. Forward computation leads to*

$$\xi^{2^2} = 1 + \pi^5 = (1 + \pi^3)^2, \tag{23}$$

where $\xi = 1 + \pi$. Note that H_0 here is not p-pure subgroup of H_R. Since $3 \notin R(j)$, $(1,3) \in I$, $w_1 \neq \gamma$ and $\mu = 1$, thus from Theorem 2

$$H_R = C_{2^3} \otimes C_2 \otimes C_2. \tag{24}$$

Now, if we consider T is a finite chain ring with same invariants $2,3,1,2,6$ (same incomplete j-diagram) and different Eisenstein polynomial $x^2 - 2(1+x)$. Let $\xi = 1 + \theta$, where $\theta = 1 + a$ (root of $x^2 - 2(1+x)$) and a is a root of $x^2 - 3$. Then, $\xi^{2^2} = 1$ and, hence, from Theorem 1,

$$H_T = C_{2^2} \otimes C_2 \otimes C_{2^2}. \tag{25}$$

Next, we state the correct version of (cf. p. 458, [1]).

Corollary 6. *Let R and T be two incomplete chain rings with same invariants p,n,r,k,m and same Ω and $\{\mu_i\}_{1 \le i \le d}$. Then, $H_R \cong H_T$.*

In general, Lemma 1 gives an algorithm for calculating Ω and μ_i's. The following example illustrates that algorithm.

Example 2. *Let R be an incomplete chain ring with invariants p,n,r,k,m and $\pi^k = p\beta h$, where $h \in H(R_0)$ and $R_0 \subset R$ is an Eisenstein extension over S by $x^{p-1} + p$, i.e., $R_0 = S[\pi_0]$, π_0 is a root of $x^{p-1} + p$ (Proposition 2). Clearly, R_0 is an incomplete chain ring with $p,n,r,p-1,m_1$, where $m_1 = (n-1)(p-1) + t_1$ and $t_1 = \lceil \frac{t}{k_1 p^l} \rceil$. Consider the (admissible) function j_0 with*

$$H_1(R_0) > H_2(R_0) > ... > H_{m_1}(R_0) = 1.$$

A similar equation of that in (13),

$$\xi_0^p = \prod_{(i,s) \in A} \omega_{is}^{a_{is}} = y^p, \tag{26}$$

where $\xi_0 = 1 + \pi_0$. Let $R_1 = R_0[\pi_1]$ be an Eisenstein extension over R_0 by $x^p - \pi_0 h_1$, where $h_1^{p-1} = h$. R_1 is an incomplete chain ring with invariants p,n,r,p,m_2, such that $m_2 = pm_1$. Now, put $\pi_0 = \pi_1^p h_1^{-1}$ in (26) and after forward computations we get

$$\xi_1^{p^2} = x_{s_1}^p \dot{y}, \tag{27}$$

where $\xi_1 = 1 + \pi_1$, $y \in H_s(R_1)^p$ and $s > s_1 = p(p-1) + 1$. If $j(s_1) < m_1$, then based on Lemma 1 $\Omega_1 = \{s_1\}$. Continuing in this way and after l steps ($k = s_0(p-1)p^l$), R is an Eisenstein

extension over R_l by $x^{s_0} - \pi_l\alpha$, where $\alpha^{(p-1)p^l} = \beta$. Thus, as a result $\Omega = \{s_0s_1, \ldots, s_0s_l\}$, where $s_i = (p-1)(p^i + p^{i-1} + \cdots + 1) + 1$ for $1 \leq i \leq l$.

4. Enumeration of Generators of the Same Order

In this section, we compute p-rank N_m and $N_m(e)$ for the decomposition that is given in (15) and (22). However, first we determine N_m and $N_m(e)$ for the complete case (10). If we denote $c = \mid P_m \setminus R(j) \mid$, then using the j-diagram it is not hard to prove the following:

$$c = \begin{cases} m - \lfloor \frac{m}{p} \rfloor, & \text{if } m < k + u, \\ k, & \text{otherwise,} \end{cases} \tag{28}$$

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

$$m_0 = \begin{cases} k + t, & \text{if } t < u, \\ t, & \text{if } t \geq u. \end{cases} \quad (n > 1) \tag{29}$$

Note that, if $n = 1$, $m = m_0 = k$. By the j-diagram, one can easily prove that $\nu_m(s) = \nu_{m_0}(s) + n - 2$ when $t < u$, and $\nu_m(s) = \nu_{m_0}(s) + n - 1$ when $t \geq u$. Thus, for $e \geq 1$, $N_m(e + (n-2)) = N_{m_0}(e)$ if $t \leq u$ and $N_m(e + (n-1)) = N_{m_0}(e)$ otherwise. Hence, it suffices to obtain $N_{m_0}(e)$.

Theorem 3. *Assume that R is a complete chain ring, then $N_m = cr$ and if $e \geq 1$,*

$$N_{m_0}(e) = (\lfloor \frac{m_0 - 1}{p^{e-1}} \rfloor - 2\lfloor \frac{m_0 - 1}{p^e} \rfloor + \lfloor \frac{m_0 - 1}{p^{e+1}} \rfloor)r. \tag{30}$$

Proof. The first claim is easy. Note that $N_{m_0}(e)$ is exactly the cardinality of $A = \{s \notin R(j) : v_{m_0}(s) = e\}$. For each s, there is a positive integer b_s, such $sp^{b_s - 1} \leq u < sp^{b_s}$ and, hence,

$$j^b(s) = \begin{cases} sp^b, & \text{if } b \leq b_s, \\ sp^{b_s} + (b - b_s)k, & \text{if } b > b_s. \end{cases}$$

However, since $m_0 = k + t$ or $m_0 = t$, then, if $s \in A$, either $b_s = e$ or $b_s = e - 1$. Consider two cases: (i) let $m_0 \geq pu$, then clearly $b_s = e - 1$ for all $s \in A$ and, thus, by the definition of b_s, $sp^{e-1} \leq pu \leq m_0$. However, we know that $m_0 \leq sp^e$ and, hence, $\frac{m_0}{p^e} \leq s < \frac{m_0}{p^{e-1}}$. (ii) Assume $m_0 < pu$, then if $b_s = e$, by definition of b_s, $sp^{e-1} \leq u < m_0$. Also if $b_s = e - 1$, which means that $sp^{e-1} > u$, hence

$$sp^e \geq j(sp^{e-1}) = sp^{e-1} + k = j^e(s) > m_0. \tag{31}$$

On the other hand, $sp^{e-1} < m_0$. Thus, in this case $\frac{m_0}{p^e} < s < \frac{m_0}{p^{e-1}}$. From (i) and (ii), we conclude that, for every $s \in A$, $\frac{m_0}{p^e} \leq s < \frac{m_0}{p^{e-1}}$. That implies A is the set of all positive integers in the interval $(\lfloor \frac{m_0 - 1}{p^{e-1}} \rfloor, \lfloor \frac{m_0 - 1}{p^e} \rfloor]$ except those in $R(j)$, i.e., $s \equiv 0 \bmod p$. Therefore, the proof follows. □

Corollary 7. *Based on the assumptions of Theorem 3,*

$$\begin{cases} N_m(n-2) = u - t + 1 - \lfloor \frac{u - t + 1}{p} \rfloor, & \text{if } t \leq u \text{ and } n > 2, \\ N_m(n-1) = k + u - t + 1 - \lfloor \frac{k + u - t + 1}{p} \rfloor, & \text{if } t > u. \end{cases}$$

We now compute $N_m(e)$ for the incomplete case. In this case, $m > k+u$, which means either $n = 2$ and $t > u$ or $n > 2$. Put

$$m_0 = \begin{cases} \iota k + t, & \text{if } u \le t, \\ (\iota+1)k + t, & \text{if } u > t, \end{cases} \quad n_0 = \begin{cases} n-1-\iota, & \text{if } t \ge u, \\ n-2-\iota, & \text{if } t < u, \end{cases} \tag{32}$$

where

$$\iota = \begin{cases} 1, & \text{if } \mu \ge \lambda, \\ \mu, & \text{if } \mu < \lambda. \end{cases}$$

Proposition 4. *Let $e \ge \iota$ and $\mu < n-1$. Then with same notations mentioned above,*

$$\begin{cases} N_m(\mu) = 1 + N_{m_0}(\mu - n_0), \\ N_m(\mu + n_0) = N_{m_0}(\mu) - 1, \\ N_m(e + n_0) = N_{m_0}(e), \text{ if } e \ne \mu \text{ and } e \ne \mu + n_0. \end{cases} \tag{33}$$

Proof. By the j-diagram, one can check that H_{m_0} is a subgroup of H^{p^μ}. Because there is an element in H with p^μ (Theorem 2), then clearly $N_m(\mu) = 1 + N_{m_0}(\mu - n_0)$ and $N_m(\mu + n_0) = N_{m_0}(\mu) - 1$. On the other hand, the proof of Lemma 1 implies $\mu_i \ge n-1$ for all $i \ge 2$ (since $\nu(s_i) \ge n-1$) and, hence, we only consider $N_{m_0}(e)$, $e \ge \mu$. This immediately implies $N_m(e + n_0) = N_{m_0}(e)$ for all e other than μ and $\mu + n_0$. □

Remark 4. *By Proposition 4, when $\mu < n-1$, it suffices to compute $N_{m_0}(e)$. However, in case of $\mu \ge n-1$ nothing can be said since $N_{m_0}(e) = N_m(e)$.*

Note that, in the case when $\lambda > \mu$, once we determine (13) and $N_{m_0}(e)$ for the part $\otimes_{s\in\Lambda} U_s \otimes_{i=1}^{d} U_{s_i}^*$, we then completely obtain H. Denote $z_e = \mid \Omega' \cap P_e \mid$, where $P_e = \{w \in H_s : o(w) = e, s \notin R(j)\}$.

Theorem 4. *Let R be an incomplete chain ring, then*
(i) $N_{m_0} = N_m = cr + 1$
(ii)

$$N_{m_0}(e) = \begin{cases} (2k - m_0 + \lfloor \frac{m_0 - k}{p} \rfloor)r + \delta, & \text{if } e = 1, \\ (\lfloor \frac{m_0 - ak - 1}{p^{e-1-a}} \rfloor - 2\lfloor \frac{m_0 - ak - 1}{p^{e-a}} \rfloor + \lfloor \frac{m_0 - ak - 1}{p^{e-a+1}} \rfloor)r + z, & \text{if } e > \iota, \end{cases}$$

where

$$\delta = \begin{cases} 2, & \text{if } \lambda = 1, \\ 1, & \text{if } \lambda \ne 1, \end{cases} \qquad z = \begin{cases} \begin{cases} 1, & \text{if } e = \lambda \ge 2, \\ -1, & \text{if } e = \lambda + 1, \quad (\iota = 1) \\ 0, & \text{otherwise,} \end{cases} \\ -z_e, \quad \text{if } \iota = \mu, \end{cases}$$

$$a = \begin{cases} \iota - 1, & \text{if } t = u, \\ \iota, & \text{otherwise.} \end{cases}$$

Proof. (i) is obvious. For (ii), we first let $e = 1$. Note that $o(\gamma) = 1$ and $o(\xi) = 1$ if $\lambda = 1$, thus we have δ. Now, consider two cases: (a) when $u \le t$, then $m_0 = k + t$ and clearly $\nu_{m_0}(s) = 1$ if and only if $s \ge t$. Consequently, there are $k + u - t -$ $\mid \{s \ge t : s \equiv 0 \bmod p\} \mid$ of such s and, thus

$$N_{m_0}(1) = (k + u - t - (u - \lfloor \frac{t}{p} \rfloor))r + \delta = (2k - m_0 + \lfloor \frac{m_0 - k}{p} \rfloor)r + \delta. \tag{34}$$

(b) In the case when $u > t$. Firstly, observe that $\nu_{m_0}(s) = 1 = e$ if and only if $s \geq k + t$. By the same reasoning of Case (a), we obtain the results. Secondly, when $e > \iota$, in this case all s satisfying $\nu_{m_0}(s) > 1$ occur in the interval $s < t$ if $u \leq t$ or $s < k + t$ when $t < u$. Therefore, we return to a similar situation of Theorem 3 with $m_0 - ak$ and $e - a$ instead of m_0 and e, respectively. Observe that, if $\iota = 1$ and $e = \lambda + 1$, then there exist $r - 1$ generators of U_{s_0} and then put $z = -1$. When $e = \lambda$, we have to add $z = 1$, since $o(\xi) = \lambda$. On the other hand, if $\iota = \mu$, there are z_e of U_s each having $r - 1$ elements of basis of the same order, so put $z = -z_e$. □

In conclusion, this article considered the multiplicative groups of finite commutative chain rings. The case when $(p - 1) \mid k$ was completed for every incomplete chain ring. Moreover, a set of linearly independent generators for H was established by connecting those generators to a basis of F over its prime field.

Recently, there has been increasing interest in using finite commutative chain rings in Coding Theory. Researchers may wish to further apply this knowledge about finite commutative chain rings to Coding Theory.

Author Contributions: Conceptualization, S.A. and Y.A.; Methodology, S.A. and Y.A.; Investigation, S.A. and Y.A.; Writing—original draft preparation, S.A.; Supervision, Y.A.; Funding acquisition, Y.A. All authors have read and agreed to the published version of the manuscript.

Funding: This project was supported by King Saud University, Deanship of Scientific Research, College of Science Research Center.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: The authors express their sincere thanks to the referees for their valuable comments and suggestions. This project was supported by King Saud University, Deanship of Scientific Research, College of Science Research Center.

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

References

1. Ayoub, C. On the group of units of certain rings. *J. Number Theory* **1972**, *4*, 383–403. [CrossRef]
2. Greferath, M. Cyclic codes over finite rings. *Discret. Math.* **1997**, *177*, 273–277. [CrossRef]
3. Lui, X.; Lui, H. LCD codes over finite chain rings. *Finite Fields Appl.* **2015**, *43*, 1–19.
4. Klingenberg, W. Projective und affine Ebenen mit Nachbarelementen. *Math. Z.* **1960**, *60*, 384–406. [CrossRef]
5. Ayoub, C. On diagrams for abelian groups. *J. Number Theory* **1970**, *2*, 442–458. [CrossRef]
6. Luis, M. Incomplete j-diagrams fail to capture group structure. *J. Algebra* **1991**, *144*, 88–93. [CrossRef]
7. Hou, X.; Leung, K.; Ma, S. On the groups of units of finite commutative chain rings. *Finite Fields Their Appl.* **2003**, *9*, 20–38. [CrossRef]
8. Clark, W.; Liang, J. Enumeration of finite chain rings. *J. Algebra* **1973**, *27*, 445–453. [CrossRef]
9. Fuchs, L. *Infinite Abelian Groups*; Academic Press, Inc.: Orlando, FL, USA, 1970.