AIMS Mathematics, 7(9): 15824–15833.
DOI: 10.3934/math.2022866
Received: 16 February 2022
Revised: 24 May 2022
Accepted: 12 June 2022
Published: 27 June 2022

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

Research article

Structure of a chain ring as a ring of matrices over a Galois ring

Yousef Alkhamees* **and Badr Alhajouj**

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

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

Abstract: The structure of a finite chain ring has already been described by Wirt in 1972 and others later. The purpose of this article is to describe another structure of a finite chain ring as a ring of square matrices over Galois ring using the companion matrix of a certain Eisenstein polynomial over Galois ring. Such a companion matrix generates the unique maximal ideal of the corresponding matrix chain ring.

Keywords: local ring; chain ring; Galois ring; companion matrix
Mathematics Subject Classification: 16L30, 16P20, 16P30

1. Introduction

We only consider associative Artinian rings with identity. A chain ring is a ring whose left (right) ideals form a chain. A ring is a chain ring if and only if it is a principal local ring. Because commutative principal ring is a direct sum of chain rings, the study of commutative principal rings is reduced to that of chain rings. Finite commutative chain rings occur naturally in at least three different areas; in Algebraic Number Theory (cf. p. 86 in [11]); in Commutative Algebra (cf. [6]); and in Geometry (cf. [9]).

A good example of finite chain rings are the commutative rings $Z_{p^n}[x]/(g(x))$, where $g(x)$ is a monic polynomial of degree r over Z_{p^n} irreducible mod p. The maximal ideal of such a ring is the ideal generated by p, where p is the characteristic of its residue field. Such a ring is uniquely determined by p, n, and r, and its group of automorphisms is cyclic of order r. These rings have a lot in common with Galois fields and are thus called Galois rings and denoted by $GR(p^n, r)$. They were first observed by Krull (1924) (cf. p. 20 in [10]).

A commutative chain subring R_0 of a local ring R is called a coefficient subring of R if $R = R_0 + J(R)$ and $R/J(R) \cong R_0/pR_0$, where $J(R)$ is the maximal ideal of R. The subring R_0 plays an important role in the structure of the local ring R. The coefficient subring of a finite local ring is its maximal Galois subring (cf. [4]).

Chain rings have been studied by several mathematicians. Wirt [17] describes the structure of a finite chain ring as the quotient of a skew polynomial ring over a Galois ring by an ideal of special form generated using Eisenstein polynomial; this conclusion was almost achieved by Nechaev [14], who called them Galois-Eisenstein-Ore rings. Further, Fisher [6] described the structure of such a ring as the quotient of a skew power series ring over a certain commutative complete discrete valuation domain by an ideal of special form similar to the ideal involved in the construction in the study by Wirt. Finally, Alkhamees, Singh, and Alolayan [1] generalize the construction of Wirt to the situation of an Artinian chain ring in which the residue field is absolutely algebraic (algebraic over its prime subfield).

The use of finite chain rings in coding theory may be traced back to the seminal work of Preparata [15] in 1968; afterward, there was an increased interest in using finite chain rings in getting more compact codes with higher capabilities of error-correction (see for example [12]). The role of different types of matrices in coding theory is well known (for instance, cf. [3,7,16,18]). They are used during the decoding process to expose and correct errors during transmission.

This paper aimed to describe the structure of a chain ring as a ring of square matrices over a Galois ring using the companion matrix of a certain Eisenstein polynomial over a Galois ring (for the definition of the companion matrix of a monic polynomial over a field, see Definition, p. 307 and problem 4, p. 312 in [8]). Such a companion matrix generates the unique maximal ideal of the corresponding matrix chain ring.

The use of matrices in coding theory mentioned above indicates that this construction may be useful in the recent applications of finite chain rings in coding theory. This construction may also help in implementing finite chain rings in coding theoretic environments.

2. Construction of a finite chain ring

Let R be a finite chain ring of characteristic p^n, m the index of nilpotency of $J(R)$, and $R_0 = GR(p^n, r) = Z_{p^n}[\eta]$ a coefficient subring of R, where η is an element of R_0 of multiplicative order $p^r - 1$. Then [5]:

(i) There exists a pair (π, σ) such that $J(R) = R\pi$ and $\pi a = a^\sigma \pi$ for each a in R_0, where π is an element of $J(R)$ and σ is an automorphism of R_0. Additionally, σ is uniquely determined by R and R_0 [1]. Thus, we call σ the associated automorphism of R with respect to R_0. Let $S_0 = GR(p^n, s)$ be the Galois subring of R_0, where $s = r\ /k'$; i.e., $S_0 = (R_0)^\sigma$.

(ii) $R = \oplus_{i=0}^{k-1} R_0\pi^i$ as R_0- modules.

(iii) $\pi^k = p\Sigma_{i=0}^{k-1} u_i\pi^i$, where u_0 is a unit in R_0 and the other u_i are elements of R_0; i.e., π is a root of Eisenstein polynomial $g(x) = x^k - p\Sigma_{i=0}^{k-1} u_i x^i$ over R_0.

(iv) There are R_0-module isomorphisms:

$$R_0\pi^i \cong R_0 \text{ for } i = 1, 2, ..., t-1 \text{ and}$$

$$R_0\pi^i \cong R_0/p^{n-1}R_0 \text{ for } i = t, t+1, ..., k-1,$$

where $1 \le t \le k$.

(v) $\sigma^k = Id_{R_0}$ if $n > 1$ and hence if k' is the order σ then k' divides k.

(vi) $m = (n-1)k + t$.

(vii) We call the integers p, n, r, k, k', m invariants of R.

In the case that R is a finite chain ring, let R_0, S_0, π, η, u_0, u_1, ..., u_{k-1}, p, n, r, s, t, k, k', m and σ retain their meanings throughout the paper.

Proposition 2.1. *Let R be a finite local ring. Then, R is a chain ring if and only if $J(R)$ has the maximal index of nilpotency.*

This is Proposition 1 in [2].

Construction A:

Notation: Let R_0 be a Galois ring of the form $GR(p^n, r)$, t , k be positive integers with $1 \leq t \leq k$, and σ be an automorphism of R_0 of order k' with k' divides k if $n > 1$. Suppose that S_0 is a Galois subring of R_0 of the form $GR(p^n, s)$, u_0, u_1, ..., u_{k-2}, u_{k-1} are certain elements of R_0 such that u_0, u_1, ..., u_{k-2} are elements of S_0 with u_0 is a unit and u_{k-1} is either an element of R_0 if $p^2u_{k-1} = 0$ or an element of S_0 otherwise, where $s = r \,/\, k'$. Next, assume that $CM_k(R_0)$ is the additive matrix group of all $k \times k$ matrices of the form $A = \left[\alpha_{ij}\right]$, where $[a_0 \;\; a_1 \; ... \; a_{t-1} \; a_t \; ... \; a_{k-1}]$ is the first row of A, $a_0, a_1, ..., a_{t-1} \in R_0$ & a_t, ..., $a_{k-1} \in R_0/p^{n-1}R_0$, $\alpha_{i1} = pu_0\alpha_{i-1k}$ for $i > 1$ and α_{ij} is a function of α_{i-1j-1} and α_{i-1k} defined by $\alpha_{ij} = \alpha_{i-1j-1} + p\, u_{j-1}\, \alpha_{i-1k}$for $i, j > 1$. Clearly, there is a certain pattern of matrices in $CM_k(R_0)$ makes all the rows of them depend on their first row and the certain elements pu_0, pu_1, ..., pu_{k-1}; thus each matrix A in $CM_k(R_0)$ is induced (derived) from the first row $[a_0 \; a_1 \; ... \; a_{t-1} \; a_t \; ... \; a_{k-1}]$ and hence let us denote an arbitrary element A of $CM_k(R_0)$ by $A = D[a_0 \; a_1 \; ... \; a_{k-1}]$, where a_0, a_1, ..., a_{k-1} are the elements of the first row of A (see Example 2.1 below).

Let R_0, S_0, $CM_k(R_0)$, $D[a_0 \; a_1 \; ... \; a_{k-1}]$, u_0, u_1, ..., u_{k-1}, p, n, r, s, t, k, k' and σ retain their meanings as in the last notation. Suppose that $A = D[a_0 \; a_1 \; ... \; a_{k-1}]$ and $B = D[b_0 \; b_1 \; ... \; b_{k-1}]$ are elements of $CM_k(R_0)$ and let us define the σ- skew multiplication $A * B$ in $CM_k(R_0)$ in the same way as the usual matrix multiplication AB except we put $a_ib_j^{\sigma^i}$ in stead of a_ib_j for all $i, j = 0, 1, ..., k-1$. The multiplication $A*B$ makes sense by taking into consideration that pR_0 may be considered as $R_0/p^{n-1}R_0$-module (in the case that the elements of the first t columns are involved in the multiplication when it is needed) and $R_0/p^{n-1}R_0$ may be considered as R_0-module (in the case that the elements of the last $k-t$ columns are involved in the multiplication).

To make it easier to understand construction A, let us introduce the following example:

Example 2.1. *Let R_0 be a Galois ring of the form $GR(p^n, r)$ with $n > 1$, r an even positive number, σ an automorphism of R_0 of order $k' = 2$, u_0 and u_1 are certain elements of R_0 such that u_0 is a unit in the subring $S_0 = GR(p^n, s)$ of R_0 and u_1 is either an element of R_0 or an element of S_0 according to wether p^2u_1 is zero or not, where $s = r/k' = r/2$. Assume*

$CM_2(R_0) = \left\{ \begin{pmatrix} a_0 & a_1 \\ pu_0a_1 & a_0+pu_1a_1 \end{pmatrix} : a_0 \in R_0 \text{ and } a_1 \in R_0/p^{n-1}R_0 \right\}$. *Then, there is a certain pattern of matrices in $CM_2(R_0)$ such that the second row of them depends on their first row and the certain elements pu_0, pu_1 and so any matrix $A = \begin{pmatrix} a_0 & a_1 \\ pu_0a_1 & a_0+pu_1a_1 \end{pmatrix}$ of $CM_2(R_0)$ is induced (derived) from the first row $[a_0 \; a_1]$; thus, let us denote an arbitrary element A of $CM_2(R_0)$ by $A = D[a_0 \; a_1]$, where a_0 and a_1 are the elements of the first row of A. Suppose that $A = D[a_0 \; a_1]$ and $B = D[b_0 \; b_1]$ are arbitrary elements of the additive matrix group $CM_2(R_0)$ and let us define the σ-skew multiplication $A * B$ in $CM_2(R_0)$ in the same way as the usual matrix multiplication AB except we put $a_ib_j^{\sigma}$ instead of a_ib_j for $i = 1$ and for all $j = 0, 1$. Thus,*

$$A * B = D[a_0\ a_1] * D[b_0 b_1]$$
$$= \begin{pmatrix} a_0b_0 + pu_0a_1b_1^{\sigma} & a_0b_1 + a_1b_0^{\sigma} + pu_1a_1b_1^{\sigma} \\ pu_0(a_0b_1 + a_1b_0^{\sigma} + pu_1a_1b_1^{\sigma}) & a_0b_0 + pu_0a_1b_1^{\sigma} + pu_1(a_0b_1 + a_1b_0^{\sigma} + pu_1a_1b_1^{\sigma}) \end{pmatrix}$$
$$= D[a_0b_0 + pu_0a_1b_1^{\sigma} a_0b_1 + a_1b_0^{\sigma} + pu_1a_1b_1^{\sigma}].$$

The multiplication $A * B$ makes sense by taking into consideration that pR_0 may be considered as $R_0/p^{n-1}R_0$-module (in the case that the elements of the first column are involved in the multiplication when it is needed) and $R_0/p^{n-1}R_0$ may be considered as R_0-module (in the case that the elements of the second column are involved in the multiplication). Thus, $A * B \in CM_2(R_0)$. Now, it is trivial to see that that $CM_2(R_0)$ is a ring. Let $J = \{D[pa_0\ a_1] : a_0 \in R_0$ and $a_1 \in R_0/p^{n-1}R_0\}$. It is easy to see that $CM_2(R_0)/J \cong GF(p^r)$ and $CM_2(R_0)$ is a local ring of order p^{mr}, where $m = 2(n-1)+1$. Suppose that $\Pi = D[0\ 1] = \begin{pmatrix} 0 & 1 \\ pu_0 & pu_1 \end{pmatrix}$, then $\Pi^2 = pD[u_0\ u_1]$. This implies that $\Pi^m = \Pi^{2(n-1)+1} = p^{n-1}\Pi N_2^{(n-1)} = 0$ $N_2^{(n-1)} = 0$ and $\Pi^{m-1} = \Pi^{2(n-1)} = p^{n-1}N_2^{(n-1)} \neq 0$, where $N_2 = D[u_0\ u_1]$ is a unit in $CM_2(R_0)$. Therefore, Π has the maximal index of nilpotency and thus according to the last proposition $CM_2(R_0)$ is a chain ring with invariants p, n, r, $k = k' = 2$, m.

Assume that R is a finite chain ring with invariants $p, n, r, k = k' = 2, m = 2(n-1)+1 (t = 1)$ with $n > 1$, r is even number, $R_0 = GR(p^n, r)$ is a coefficient subring of R, σ is the associated automorphism of R with respect to R_0 of order $k' = 2$ and $J(R) = R\pi$ with $\pi^2 = pu_0 + pu_1\pi$; i.e., π is a root of Eisenstein polynomial $g(x) = x^2 - pu_1x - pu_0$ over R_0. Using $\pi\pi^2 = \pi^2\pi$ and $\pi^2 = pu_0 + pu_1\pi$, we get that u_0 is a unit in the subring $S_0 = GR(p^n, s)$ of R_0 and u_1 is either an element of R_0 or an element of S_0 according to whether p^2u_1 is zero or not.

Let ϕ be a mapping from R to $CM_2(R_0)$ defined by $\phi(a_0 + a_1\pi) = D[a_0\ a_1]$. Let $a = a_0 + a_1\pi$ and $b = b_0 + b_1\pi$ be elements of R. Then,

$\phi(a+b) = \phi((a_0 + a_1\pi) + (b_0 + b_1\pi)) = \phi((a_0 + b_0) + (a_1 + b_1)\pi)) = D[a_0 + b_0\ \ a_1 + b_1] = D[a_0\ a_1] + D[b_0\ b_1] = \phi(a) + \phi(b)$,

$\phi(ab) = \phi((a_0 + a_1\pi)(b_0 + b_1\pi)) = \phi(a_0b_0 + pu_0a_1b_1^{\sigma} + (a_0b_1 + a_1b_0^{\sigma} + pu_1a_1b_1^{\sigma})\pi) = D[a_0b_0 + pu_0a_1b_1^{\sigma}\ a_0b_1 + a_1b_0^{\sigma} + pu_1a_1b_1^{\sigma}] = D[a_0\ a_1] * D[b_0\ b_1] = \phi(a)\phi(b)$.

Therefore, ϕ is a ring homomorphism. Now, it is easy to check that ϕ is an isomorphism. It is worth noting that $\phi(\pi) = \Pi = D[0\ 1] = \begin{pmatrix} 0 & 1 \\ pu_0 & pu_1 \end{pmatrix}$, which is the companion matrix of a certain Eisenstein polynomial $g(x) = x^2 - pu_1x - pu_0$ over R_0 mentioned above and has π in $J(R)$ as its root.

Let us denote $CM_k(R_0)$ with $\sigma = Id_{R_0}$ by $CCM_k(R_0)$. In such a case, we notice that the σ-skew multiplication $A * B$ in $CCM_k(R_0)$ is the same as the usual matrix multiplication AB because $\sigma = Id_{R_0}$.

Proposition 2.2. *$CCM_k(R_0)$ is a finite commutative chain ring with invariants p, n, r, k, m.*

Proof. Assume that $A = D[a_0\ a_1\ ...\ a_{k-1}] = [\alpha_{ij}]$, $B = D[b_0\ b_1\ ...\ b_{k-1}] = [\beta_{ij}]$ are arbitrary elements of $CCM_k(R_0)$ and $C = AB = \left[c_{ij}\right]$. We want to prove that:

$$c_{i1} = pu_0c_{i-1k} \text{ for } i > 1 \text{ and } c_{ij} = c_{i-1j-1} + pu_{j-1}c_{i-1k} \text{ for } i, j > 1. \tag{2.1}$$

For the 1*st* column, we notice that

$$\begin{aligned}
c_{i1} &= \sum_{e=1}^{k} \alpha_{ie}\beta_{e1} = \alpha_{i1}\beta_{11} + \sum_{e=2}^{k} \alpha_{ie}\beta_{e1} = pu_0\alpha_{i-1k}\beta_{11} + \sum_{e=2}^{k}(\alpha_{i-1e-1} + pu_{e-1}\alpha_{i-1k})pu_0\beta_{e-1k} \\
&= pu_0 \sum_{e=2}^{k} \alpha_{i-1e-1}\beta_{e-1k} + pu_0\ \alpha_{i-1k}(\beta_{11} + \sum_{e=2}^{k} pu_{e-1}\beta_{e-1k}) \\
&= pu_0(c_{i-1k} - \alpha_{i-1k}\beta_{kk}) + pu_0\ \alpha_{i-1k}(\beta_{11} + \sum_{e=2}^{k} pu_{e-1}\beta_{e-1k}) \\
&= pu_0c_{i-1k} + pu_0\ \alpha_{i-1k}(\beta_{11} + \sum_{e=2}^{k}(\beta_{ee} - \beta_{e-1e-1}) - \beta_{kk}) = pu_0c_{i-1k}.
\end{aligned}$$

Now, let us find c_{ij} for $i, j > 1$:

$$\begin{aligned}
c_{ij} = \sum_{e=1}^{k} \alpha_{ie}\beta_{ej} = \alpha_{i1}\beta_{1j} + \sum_{e=2}^{k} \alpha_{ie}\beta_{ej} &= \alpha_{i1}\beta_{1j} + \sum_{e=2}^{k}(\alpha_{i-1e-1} + pu_{e-1}\alpha_{i-1k})(\beta_{e-1j-1} + pu_{j-1}\beta_{e-1k}) \\
&= \alpha_{i1}\beta_{1j} + \sum_{e=2}^{k} \alpha_{i-1e-1}\beta_{e-1j-1} + p\alpha_{i-1k} \sum_{e=2}^{k} u_{e-1}\beta_{e-1j-1} \\
&\quad + pu_{j-1} \sum_{e=2}^{k} \alpha_{i-1e-1}\beta_{e-1k} + p^2u_{j-1}\alpha_{i-1k} \sum_{e=2}^{k} u_{e-1}\beta_{e-1k}.
\end{aligned}$$

But

$$\begin{aligned}
&\sum_{e=2}^{k} \alpha_{i-1e-1}\beta_{e-1j-1} = c_{i-1j-1} - \alpha_{i-1k}\beta_{k\ j-1}, \\
&pu_{j-1} \sum_{e=2}^{k} \alpha_{i-1e-1}\beta_{e-1k} = pu_{j-1}(c_{i-1k} - \alpha_{i-1k}\beta_{kk}), \\
&p^2u_{j-1}\alpha_{i-1k} \sum_{e=2}^{k} u_{e-1}\beta_{e-1k} = \ pu_{j-1}\alpha_{i-1k} \sum_{e=2}^{k} pu_{e-1}\beta_{e-1k} \ = pu_{j-1}\alpha_{i-1k}(\beta_{kk} - \beta_{11})
\end{aligned}$$

Thus,

$$\begin{aligned}
c_{ij} =& \alpha_{i1}\beta_{1j} + (c_{i-1j-1} - \alpha_{i-1k}\beta_{kj-1}) + pu_{j-1}(c_{i-1k} - \alpha_{i-1k}\beta_{kk}) + pu_{j-1}\alpha_{i-1k}(\beta_{kk} - \beta_{11}) \\
&+ \alpha_{i-1k} \sum_{e=2}^{k} pu_{e-1}\beta_{e-1j-1} = c_{i-1j-1} + pu_{j-1}c_{i-1k} + pu_0\alpha_{i-1k}\beta_{1j} - \alpha_{i-1k}\beta_{kj-1} - pu_{j-1}\alpha_{i-1k}\beta_{11} \\
&+ \alpha_{i-1k} \sum_{e=2}^{k} pu_{e-1}\beta_{e-1j-1} = c_{i-1j-1} + pu_{j-1}c_{i-1k} + \alpha_{i-1k}(pu_0\beta_{1j} - \beta_{kj-1} - pu_{j-1}\beta_{11} \\
&+ \sum_{e=2}^{k} pu_{e-1}\beta_{e-1j-1}).
\end{aligned}$$

Using the following relations: $\beta_{i1} = pu_0\beta_{i-1k}$ for $i > 1$ and $\beta_{ij} = \beta_{i-1\ j-1} + pu_{j-1}\ \beta_{i-1\ k}$ for $i, j > 1$ which make all the rows of $B = [\beta_{ij}]$ depend on their first row and certain elements pu_0, pu_1, ..., pu_{k-1}. It is a matter of routine calculations to deduce that $pu_0\beta_{1j} - \beta_{kj-1} - pu_{j-1}\beta_{11} + \sum_{e=2}^{k} pu_{e-1}\beta_{e-1j-1} = 0$. Hence,

$$c_{ij} = c_{i-1j-1} + pu_{j-1}c_{i-1k}$$

Now, it is easy to see that $CCM_k(R_0)$ is a commutative ring with identity. Assume that $M = \{D[pa_0\ a_1\ ...\ a_{t-1}\ a_t\ ...\ a_{k-1}] : a_0, a_1, ..., a_{t-1} \in R_0\ \&\ a_t, ..., a_{k-1} \in R_0/p^{n-1}R_0\}$. Then, it is easy to see that M is an ideal in $CCM_k(R_0)$, $|M| = p^{(m-1)r}$, whereas $|CCM_k(R_0)| = p^{mr}$. Clearly, $CCM_k(R_0)\ /M \cong GF(p^r)$; subsequently, $CCM_k(R_0)$ is a local ring. Suppose that

$$\Pi = D[0, 1, 0, ..., 0, 0] = \begin{pmatrix} 0 & 1 & 0 & 0 & . & . & . & 0 \\ 0 & 0 & 1 & 0 & . & . & . & 0 \\ 0 & 0 & 0 & 1 & 0 & . & . & 0 \\ . & . & . & . & . & . & . & . \\ . & . & . & . & . & . & . & . \\ 0 & 0 & . & . & . & 0 & 1 & 0 \\ 0 & 0 & . & . & . & 0 & 0 & 1 \\ pu_0 & pu_1 & pu_2 & . & . & . & pu_{k-2} & pu_{k-1} \end{pmatrix}$$

is an element of $CCM_k(R_0)$ in which the first superdiagonal consists entirely of ones and all other elements above the last row of the matrix Π are zeros. Then, obviously $\Pi^2 = D[0, 0, 1, 0, ..., 0, 0]$, $\Pi^3 = D[0, 0, 0, 1, ..., 0, 0]$ and so on $\Pi^k = pD[u_0, u_1, ..., u_{k-1}]$. Using $\Pi^k = pD[u_0, u_1, ..., u_{k-1}]$, then one can deduce that $\Pi^m = \Pi^{(n-1)k+t} = p^{n-1}\Pi^t N_k^{(n-1)} = 0\ N_k^{(n-1)} = 0$ and $\Pi^{m-1} = \Pi^{(n-1)k+t-1} = p^{n-1}\Pi^{t-1}N_k^{(n-1)} \neq 0$, where $N_k = D\ [u_0, u_1, ..., u_{k-1}]$ is a unit in $CCM_k(R_0)$. Thus, Π has the maximal index of nilpotency in $CCM_k(R_0)$. Using Proposition 2.1, one deduce that $CCM_k(R_0)$ is a chain ring with invariants p, n, r, k, m. □

Proposition 2.3. *$CM_k(R_0)$ is a finite chain ring with invariants p, n, r, k, k′,m.*

Proof. Assume that $A = D[a_0\ a_1\ ...\ a_{k-1}] = [\alpha_{ij}]$, $B = D[b_0\ b_1\ ...\ b_{k-1}] = [\beta_{ij}]$ are elements of $CM_k(R_0)$. Then, we define σ- multiplication in $CM_k(R_0)$ as $A * B = C^* = [c_{ij}^*]$, where c_{ij}^* in $CM_k(R_0)$ has the same expression as c_{ij} in $CCM_k(R_0)$, except we put $a_i b_j^{\sigma^i}$ instead of $a_i b_j$ for all $i, j = 0, 1, ..., k-1$. Now, using $c_{i1} = pu_0c_{i-1k}$ for $i > 1$ and $c_{ij} = c_{i-1j-1} + pu_{j-1}c_{i-1k}$ for $i, j > 1$, we deduce that $c_{i1}^* = pu_0c_{i-1k}^*$ for $i > 1$ and $c_{ij}^* = c_{i-1j-1}^* + pu_{j-1}c_{i-1k}^*$ for $i, j > 1$.

Let $M = \{D[pa_0\ a_1\ ...\ a_{t-1}\ a_t\ ...\ a_{k-1}] : a_0, a_1, ..., a_{t-1} \in R_0\ \&\ a_t, ..., a_{k-1} \in R_0/p^{n-1}R_0\}$. Then, it is easy to see (as above) that M is the unique maximal ideal in $CM_k(R_0)$; subsequently, $CM_k(R_0)$ is a local ring. Further, assume that $\Pi = D[0, 1, 0, ..., 0, 0]$. Then, obviously as above $\Pi^m = 0$ and $\Pi^{m-1} \neq 0$. Thus, Π has the maximal index of nilpotency in $CM_k(R_0)$. Using Proposition 2.1, one deduce that $CM_k(R_0)$ is a chain ring with invariants p, n, r, k, k', m. □

Theorem 2.1. *A finite ring is a chain ring with invariants p, n, r, k, k′,m if and only if it is isomorphic to one of the rings given by construction A.*

Proof. Let R be a finite chain ring with invariants p, n, r, k, k', m, $R_0 = GR(p^n, r)$ be a coefficient subring of R, $J(R) = R\pi$ such that π is a root of Eisenstein polynomial $g(x) = x^k - p\Sigma_{i=0}^{k-1}u_i x^i$ over R_0

and σ be the associated automorphism of R with respect to R_0. Using $\pi\pi^k = \pi^k\pi$ and $\pi^k = p\Sigma_{i=0}^{k-1}u_i\pi^i$, we deduce that u_0, u_1, ..., u_{k-2} are elements of the subring $S_0 = GR(p^n, s)$ of R_0 such that u_0 is a unit and u_{k-1} is either an element of R_0 or an element of S_0 according to whether p^2u_{k-1} is zero or not (see Example 2.1).

Let ϕ be a mapping from R to $CM_k(R_0)$ defined by $\phi((a_0 + a_1\pi + ... + a_{k-1}\pi^{k-1}) = D[a_0\ a_1\ ...\ a_{k-1}]$. Assume that $a = a_0 + a_1\pi + ... + a_{k-1}\pi^{k-1}$ and $b = b_0 + b_1\pi + ... + b_{k-1}\pi^{k-1}$ are elements of R. Then:

$\phi(a+b) = \phi((a_0 + a_1\pi + ... + a_{k-1}\pi^{k-1}) + (b_0 + b_1\pi + ... + b_{k-1}\pi^{k-1})) = \phi((a_0+b_0) + (a_1+b_1)\pi + ... + (a_{k-1}+b_{k-1})\pi^{k-1})) = D[a_0+b_0\ \ a_1+b_1\ ...\ a_{k-1}+b_{k-1}] = D[a_0a_1...a_{k-1}] + D[b_0\ b_1\ ...\ \ b_{k-1}] = \phi(a) + \phi(b)$. Also $ab = (a_0 + a_1\pi + ... + a_{k-1}\pi^{k-1})(b_0 + b_1\pi + ... + b_{k-1}\pi^{k-1}) = \zeta_0 + \zeta_1\pi + ... + \zeta_{k-1}\pi^{k-1}$ and $\phi(ab) = [c_{ij}^*]$. According to the last proposition $[c_{ij}^*]$ is determined completely by $[c_{1j}]$. Thus, to check that $\phi(ab) = \phi(a) * \phi(b)$ it is enough to prove that $[c_{1j}^*] = [\zeta_0\ \zeta_1\ ...\ \zeta_{k-1}]$, which can be proved using similar technique as the one used in the proof of Proposition 2.2. Therefore, ϕ is a ring homomorphism. Now, it is easy to check that ϕ is an isomorphism. Actually, $\phi(\pi) = \Pi = D[0\ 1\ 0\ ...\ 0\ 0]$ is the $k \times k$ companion matrix of Eisenstein polynomial $g(x) = x^k - p\Sigma_{i=0}^{k-1}u_ix^i$ over R_0 in which π is its root. □

Remark 2.1. *Suppose that*

$$C'M_k(R_0) = \left\{\sum_{i=0}^{k-1} a_i\Pi^i :\ a_0,\ a_1,\ ...,\ a_{k-1} \in R_0\right\} = \sum_{i=0}^{k-1} R_0\Pi^i,$$

where Π *is the matrix given in the proof of the last proposition and* $\Pi^0 = I_k = \left[e_{ij}\right]$ *is the diagonal matrix of degree k, the elements* e_{ij} *of* Π^0 *in the first t columns are in* R_0*, whereas they are in* $R_0/p^{n-1}R_0$ *otherwise and* $e_{ii} = 1$ *for all* $i = 1, 2; ..., k$*; this means that* $\Pi^0 = I_k = [1, 0, ..., 0]$ *in* $C'M_k(R_0)$ *according to the notation used above. Clearly,* $C'M_k(R_0)$ *is additive matrix group. Let us define that* $\Pi^i a = a^{\sigma^i}\Pi^i$ *for each* $a \in R_0$*. It is a direct check to see that this multiplication transfers the additive group* $C'M_k(R_0) = \sum_{i=0}^{k-1} R_0\Pi^i$ *into a ring; i.e., it is the ring of all* $k \times k$ *matrices* $\sum_{i=0}^{k-1} a_i\Pi^i$*, where* a_i *are elements of* R_0*. Further,* $C'M_k(R_0)$ *is commutative if and only if* $\sigma = Id_{R_0}$*. Now, it is evident that* $C'M_k(R_0)$ *is the same as the ring* $CM_k(R_0)$ *given in construction A. This can be considered as another matrix construction of a finite chain ring.*

3. Construction of Artinian chain ring with absolutely algebraic residue field

Let R be an Artinian local duo (every left ideal is a right ideal and vice versa) ring of characteristic p^n with absolutely algebraic residue field, where p is the characteristic of $R/J(R)$; it is already known [1] that R in sucha case has a commutative chain subring R_0 as its coefficient subring. In fact, R_0 is a union of ascending chains of Galois subrings of R of characteristic p^n, with its maximal ideal generated by p and $Aut\ R_0 \cong Aut\ (R_0/pR_0)$. Thus, we call R_0 in this case a generalized Galois ring.

Now assume that R is an Artinian chain ring with m as the index of nilpotency of $J(R)$. Then [1]:

(i) There exists a pair (π, σ) such that $J(R) = R\pi$ and $\pi a = a^\sigma\pi$ for each a in R_0, where π an element of $J(R)$ and σ is an automorphism of R_0. Further, σ is uniquely determined by R and R_0. Thus, we call σ the associated automorphism of R with respect to R_0.

(ii) $R = \oplus_{i=0}^{k-1}R_0\pi^i$ as R_0- modules and thus one can deduce that R is a duo ring.

(iii) $\pi^k = p\Sigma_{i=0}^{k-1}u_i\pi^i$, where u_0 is a unit in R_0 and the other u_i are elements of R_0; i.e., π is a root of Eisenstein polynomial $g(x) = x^k - p\Sigma_{i=0}^{k-1}u_ix^i$ over R_0.

(iv) There are R_0-module isomorphisms:

$$R_0\pi^i \cong R_0 \text{ for } i = 1, 2, ..., t-1 \text{ and}$$

$$R_0\pi^i \cong R_0/p^{n-1}R_0 \text{ for } i = t, t+1, ..., k-1,$$

where $1 \leq t \leq k$.

(v) $\sigma^k = Id_{R_0}$ if $n > 1$ and hence if k' is the order σ then k' divides k.

(vi) $m = (n-1)k + t$.

(vii) Assume R' is the subring of R generated by Z_{p^n} and π. Then, it is easy to check that R' is a finite chain subring of R with invariants p, n, r', k, k', m, where $R'_0 = GR(p^n, r')$ is a coefficient subring of R'. We call R' the associated finite chain ring of R.

(viii) We call the integers p, n, r', k, k', m invariants of R.

Proposition 3.1. *Let R be an Artinian duo local ring of characteristic p^n in which its residue field is absolutely algebraic. Then, the following are equivalent:*

(i) R is a chain ring
(ii) $J(R)$ has the maximal index of nilpotency
(iii) There exists an element in $J(R)$ that has the maximal index of nilpotency.

Proof. Let R_0 be a coefficient subring of R. Then, R_0 is a generalized Galois ring. Assume R'_0 is a maximal Galois subring of R_0 and $R'_0 \cong GR(p^n, r') = Z_{p^n}[\eta]$, where η is an element of R'_0 of multiplicative order $p^{r'} - 1$.

(i) $\Longrightarrow$ (ii): Let R be a chain ring and R' the associated finite chain ring of R. Then, $J(R) = R\pi$ and hence $J(R') = R'\pi$. Thus, using Proposition 2.1, one can deduce that $J(R')$ has the maximal index of nilpotency and subsequently $J(R)$ has the maximal index of nilpotency.

(ii) $\Longrightarrow$ (iii): Assume $J(R)$ has the maximal index of nilpotency, say m, and $T = \{\Sigma_{i=0}^{m-1} \lambda_i\eta^i : \lambda_i \in R_0\}$. It is easy to check that T is a finite local ring and $J(T) = T\pi$. Hence, T is a chain ring; consequently, π is an element of $J(R)$, which has the maximal index of nilpotency.

(iii) $\Longrightarrow$ (i): Let π be an element of $J(R)$ of maximal index of nilpotency, say m, and $T = \{\Sigma_{i=0}^{m-1} \lambda_i\eta^i : \lambda_i \in R_0\}$. Since R_0 is a coefficient subring of R; $R = R_0 + J(R)$ and $R/J(R) \cong R_0/pR_0$. Additionally, as above T is a chain ring with invariants p, n, r', k, k', m with $T/T\pi \cong R_0/pR_0$. Hence, $R/J(R) \cong T/T\pi$. But $T \subseteq R$. Therefore, $R = T$; thus, R is a chain ring. □

Using the fact that if R is an Artinian chain ring with absolutely algebraic field and R' is the associated finite chain ring of R, then $J(R)$ and $J(R')$ have the same generator, one can prove the following theorem.

Theorem 3.1. *Let R and T be Artinian chain rings with absolutely algebraic residue fields and constructed over the same generalized Galois subring and with the same invariants p, n, r', k, k', m and R', T' be their associated finite chain subrings respectively. Then, $R \cong T$ if and only if $R' \cong T'$.*

Construction B:

Assume that R_0 is a generalized Galois ring of characteristic p^n, t , k are positive integers with $1 \leq t \leq k$, σ is an automorphism of R_0 of order k' with k' divides k if $n > 1$, R'_0 is a Galois subring of R_0 of the form $GR(p^n, r')$, S_0 is a Galois subring of R'_0 of the form $GR(p^n, s)$, u_0, u_1, ..., u_{k-1} are certain

elements or R_0' such that u_0, u_1, ..., u_{k-2} are elements of S_0 with u_0 is a unit and u_{k-1} is either an element of R_0' if $p^2u_{k-1} = 0$ or an element of S_0 otherwise, where $s = r' / k'$. Further, in such a (Artinian) case, suppose that $ACM_k(R_0)$ is the additive matrix group of all k x k matrices of the form $[\alpha_{ij}]$, $[a_0 \ \ a_1 \ ... \ a_{t-1} \ a_t \ ... \ a_{k-1}]$ is the first row of A, $a_0, a_1, ..., a_{t-1} \in R_0$ & a_t, ..., $a_{k-1} \in R_0/p^{n-1}R_0$, $\alpha_{i1} = pu_0\alpha_{i-1k}$ for $i > 1$ and α_{ij} is a function of α_{i-1j-1} and α_{i-1k} defined by $\alpha_{ij} = \alpha_{i-1j-1} + pu_{j-1} \ \alpha_{i-1k}$ for $i, j > 1$. As in the last construction, let us denote an arbitrary element A of $ACM_k(R_0)$ by $D[a_0 \ a_1 \ ... \ a_{k-1}]$, where a_0, a_1, ..., a_{k-1} are the elements of the first row of A. Let $A = D[a_0 \ a_1 \ ... \ a_{k-1}]$ and $B = D[b_0 \ b_1 \ ... \ b_{k-1}]$ be elements of $ACM_k(R_0)$ and let us define the σ-skew multiplication $A * B$ in $ACM_k(R_0)$ as in the last construction and such multiplication make sense for the same reason as in the finite case. Now, using a similar technique as in a finite case and using Proposition 3.1, one can prove that $ACM_k(R_0)$ is a chain ring and $J(ACM_k(R_0))$ is generated by Π, where Π is the one given in the finite case.

Using Theorems 2.1 and 3.1 and taking into consideration that the associated finite chain ring of $ACM_k(R_0)$ is $CM_k(R_0') = \{D[a_0 \ a_1 \ ... \ a_{k-1}] : a_0, a_1, ..., a_{t-1} \in R_0' \ \& \ a_t, \ ..., \ a_{k-1} \in R_0'/p^{n-1}R_0'\}$, we can prove the following theorem.

Theorem 3.2. *An Artinian duo local ring of characteristic p^n in which its residue field is absolutely algebraic is a chain ring with invariants p, n, r′, k, k′, m if and only if it is isomorphic to one of the rings given by construction B.*

4. Conclusions

The structure of a finite chain ring has already been described by Wirt in 1972 and others later. We managed to describe the structure of a finite chain ring as a ring of square matrices over a Galois ring using the companion matrix of a certain Eisenstein polynomial over Galois ring. Such a companion matrix generates the unique maximal ideal of the corresponding matrix chain ring. The given construction may help in implementing finite chain rings in coding theoretic environments.

Acknowledgments

This project was supported by King Saud University, Deanship of Scientific Research, College of Science Research Center. The authors would also like to express their gratitude to the referees for their valuable comments. Finally, we would like to thank Al-Thukair, Alabaid, Balfagih, and Bazfour for reading an earlier version of this article.

Conflict of interest

The authors declare that they have no conflict of interest.

References

1. Y. Alkhamees, S. Singh, H. Alolayan, A representation theorem for chain rings, *Colloq. Math.*, **96** (2003), 103–119. https://doi.org/10.4064/cm96-1-10
2. Y. Alkhamees, The enumeration of finite principal completely primary rings, *Abh. Math. Sem. Hamburg*, **51** (1981), 226–231.

3. B. J. Chathely, Hadamard matrix and its application in coding theory and combinatorial design theory, *Int. J. Math. Trend. Technol.*, **59** (2018), 218–227.
4. W. E. Clark, A coefficient ring for finite non-commutative rings, *Proc. Amer. Math. Soc.*, **33** (1972), 25–27. https://doi.org/10.1090/S0002-9939-1972-0294411-8
5. W. E. Clark, D. A. Drake, Finite chain rings, *Abh. Math. Sem. Hamburg*, **39** (1973), 147–153. https://doi.org/10.1007/BF02992827
6. J. L. Fisher, Finite principal rings, *Can. Math. Bull.*, **19** (1976), 277–283.
7. M. Greferath, S. E. Schmidt, *Linear codes and rings of matrices*, Springer, Berlin, 2003, 160–169.
8. I. N. Herstein, *Topics in algebra*, 2 Eds., John Wiley & Sons, New York, 1975.
9. W. Klingenberg, Projective and affine Ebene mit Nachbarelementen, *Math. Z.*, **60** (1960), 384–406.
10. W. Krull, Algebraische theorie der ringe II, *Math. Ann.*, **91** (1924), 1–46. https://doi.org/10.1007/BF01498378
11. W. Krull, *Ideal theorie*, 2 Eds., Spring Verlag, Berlin, New York, 1968.
12. X. Liu, H. Liu, LCD codes over finite chain rings, *Finite Fields Th. App.*, **34** (2015), 1–19. https://doi.org/10.1016/j.ffa.2015.01.004
13. B. R. Macdonald, *Finite rings with identity*, Marcel Dekker, New York, 1974.
14. A. A. Nechaev, Finite rings of principal ideals, *Mat. Sb.*, **91** (1973), 350–366.
15. F. P. Preparata, A class of optimum nonlinear double-error-correcting codes, *Inform. Control*, **13** (1968), 378–400. https://doi.org/10.1016/S0019-9958(68)90874-7
16. A. Stakhov, *A new coding theory based on matrix approach*, The Harmony of Mathematics, Series of Knots and Every Thing, World Scientific Publishing Co. Pte. Ltd., Singapore, **22** (2009), 569–614.
17. B. R. Wirt, *Finite non-commutative local rings*, Ph. D. Thesis, University of Oklahoma, 1972.
18. C. P. Xing, *Coding theory: A first course*, Cambridge University Press, 2004.

AIMS Press