A review of the theory of completely primary finite rings

Chiteng'a J. Chikunji
Department of Basic Sciences, Botswana College of Agriculture,
Private Bag 0027, Gaborone, BOTSWANA.
E-mail: jchikunj@bca.bw

Abstract

We give a review of recent developments in the theory of finite rings with identity and pay special attention to a class of finite rings whose sets of all zero divisors form additive groups. We further describe the structure of such rings and provide a general representation for these rings as additive direct sums of cyclic modules over their maximal Galois subrings.
Keywords: finite rings, completely primary, galois subrings, cyclic modules.
Classification (MSC2010): Primary 16P10; Secondary 20K01.[1]

Our main aim is to prove the following results:

Theorem. *Let R be a CPF ring of order p^{nr}, with unique maximal ideal $\mathcal{J}$, $|R/\mathcal{J}| = p^r$, $charR = p^k$, and let R_o be a maximal Galois subring of R. Then, there exist $x_1,\ ...,\ x_h \in \mathcal{J}$ and $\sigma_1,\ ...,\ \sigma_h \in Aut(R_o)$ such that*

$$R = R_o \oplus R_o x_1 \oplus \cdots \oplus R_o x_h \text{ and } x_i r = r^{\sigma_i} x_i,$$

for ever $r \in R_o$ and each $i = 1,\ ...,\ h$. Moreover, the automorphisms $\sigma_1,\ ...,\ \sigma_h \in Aut(R_o)$ are uniqely determined by R_o and R.

[1]Paper presented at Strathmore University International Mathematics Research Meeting, Nairobi, Kenya, July 23-27, 2012

1 Introduction

Throughout this work we will assume that all rings are finite, associative (not necessarily commutative) and with identities denoted by $1 \neq 0$, that ring homomorphisms preserve 1, a ring and its subrings have the same 1 and modules are unital.

Most of our notation is standard and will usually not be repeated here. Basic definitions and results on completely primary finite rings can be found in [3] (respectively in [18]). For more details on these concepts we refer the reader to [18].

Although finite rings have been studied extensively in recent years by Raghavendran [18], and Wilson [19], [20], [21], and the tools necessary for describing completely primary finite rings have been available for some time, their classification into well known structures (which is essentially given in Chikunji [3] and [4], Clark & Liang [7], Corbas [8] and [9], and Raghavendran [18]) is not complete.

Much of the recent work on completely primary rings has demonstrated the fundamental importance of these rings in the structure theory of finite rings with identity.

Let R be a finite ring. It turns out that R has a unique maximal ideal if and only if it is a full matrix ring over a completely primary ring. In particular, rings with a unique maximal ideal are not necessarily completely primary. Therefore, the study of rings with a unique maximal ideal (i.e. local rings) reduces to the study of completely primary rings.

More evidence for the importance of these rings comes from the fact that any finite commutative ring is a direct sum of completely primary rings. Moreover, any finite ring R is of the form $S + N$, where $S \cap N = (0)$ with N a subgroup of the Jacobson radical of R and S a direct sum as an additive abelian group of certain matrix rings over completely primary rings.

Perhaps because of the feeling that completely primary rings play an important role in the classification of all finite rings with identity, they have been the subject of a good deal of research in recent years.

1.1 Motivation

Research on finite fields and their applications has been notably extensive, producing rich and deep results in finite geometries, algebraic coding theory, linear groups and other areas. Similar results are obtainable over arbitrary finite commutative rings. Some results on finite rings are being utilized on questions in the theory of algebraic

cryptography and matrix theory here-to-now formulated only for finite fields and occasionally quotient rings of rational integers.

While the algebraic theory of error-correcting codes originally took place in the setting of vector spaces over finite fields, the study of linear codes over finite rings has continued to be increasingly more important since the realization, some years ago, that many seemingly nonlinear codes are actually related to linear codes over the ring of integers modulo four.

Work on linear codes over finite chain rings from a geometric viewpoint has also been developed. Because of the existence of noncommutative finite chain rings, one is forced to distinguish between left and right linear codes, between the left and right orthogonal of the given code, and so on. More recently, finite commutative chain rings have found interesting applications in combinatorics where they are used in various constructions of partial difference sets, relative difference sets and bent functions.

Finite noncommutative rings may be considered as algebras over Galois extensions of $\mathbb{Z}/\mathbb{Z}_{p^n}$ (called *Galois Rings*) and it now appears that much of the classical theory of algebras over fields may be extended to finite rings with identity ([3], [4], [7], [8], [9] and [18]).

The purpose of this work is to give a review of recent developments in the theory of finite rings with identity and pay special attention to a class of finite rings whose sets of all zero divisors form additive groups. We further describe the structure of such rings and provide a general representation of these rings as additive direct sums of cyclic modules over their maximal Galois subrings.

The author would like to thank the organizing committee for the Strathmore University International Mathematics Research Meeting for the rare opportunity of requesting me to be one of the Key Note Speakers.

2 Some general properties of finite rings

We start with the following lemma and its corollary (see Corbas [8]).

Lemma 2.1 *Let R be a finite ring with identity $1 \neq 0$. Then, there is no distinction between left and right zero-divisors (units) in R. Moreover, every element of R is either a zero-divisor or a unit.*

Proof. Let $x \in R$ and assume x is not a left zero-divisor. Consider the map $\theta : R^+ \longrightarrow R^+$ defined by $\theta(r) = xr$. Clearly, θ is an additive group homomorphism of R^+ with $Ker\theta = \{r \in R : xr = 0\}$, which is equal to $\{0\}$ since x is not a left zero-divisor and so θ is injective. Since R is finite, θ is also surjective. In particular, $xy = 1$, for some $y \in R$, and therefore, x is a left unit.

Now, suppose that $sx = 0$, for some element s in R. Then

$$0 = (sx)y = s(xy) = s.1 = s,$$

and therefore, x is not a right zero-divisor.

A similar argument shows that if x is not a right zero-divisor, then it is a right unit, and hence, not a left zero-divisor.

Thus, if x is a left zero divisor, it is a right zero divisor; and if x is a left unit, it is also a right unit. Hence, x is either a unit or a zero divisor. ■

Corollary 2.2 *Let R be a finite ring with identity $1 \neq 0$. Then every non-trivial ideal of R consists entirely of zero-divisors.*

The following result demonstrates the importance of the set of zero-divisors in any ring.

Theorem 2.3 ([11]&[15]) *Let R be any ring containing a finite number $n \geq 2$ of left zero-divisors. Then, R is finite and $|R| \leq n^2$.*

Proof. Suppose a is a non-zero left zero-divisor of R and consider the right ideal Ra of R. Since a is a left zero-divisor of R, there exists a non-zero element $x \in R$ such that $ax = 0$, so that, for all $r \in R$, $r(ax) = (ra)x = 0$, and thus Ra consists entirely of left zero divisors. Thus, $|Ra| \leq n$.

Now, consider the surjective additive group homomorphism

$$\begin{array}{rccc} \psi : & R & \longrightarrow & Ra \\ & r & \longmapsto & ra \end{array}$$

with $ker\psi = \{y \in R : ya = 0\}$. We have $R/ker\psi \cong Ra$, and every element of $ker\psi$ is a left zero-divisor of R (since $a \neq 0$) so that $|ker\psi| \leq n$. Thus, $ker\psi$ and Ra are finite, and hence, R is finite. Moreover,

$$|R| = |ker\psi|.|Ra| \leq n^2.$$

■

From now onwards (following Lemma 2.1), an element of a finite ring R which is a left or right zero-divisor will be called simply as a *zero-divisor*. Similarly, a left or right unit will be called simply as a *unit*.

3 Completely primary finite rings

In view of Theorem 2.3, the set of zero-divisors of a finite ring obviously plays an important role, and in this work we shall restrict our attention to those rings in which the zero-divisor set has a certain property, namely, that of forming an additive group.

A finite ring R with identity $1 \neq 0$ is *completely primary* if the set $\mathcal{J}$ of all its zero-divisors forms an additive group.

It is not always true that if x and y are zero-divisors, $x+y$ is too (for example, in $\mathbb{Z}_{10}$, 2 and 5 are zero-divisors but 7 is not), but when this property does hold in a finite ring, the zero-divisors can easily be seen to form an ideal.

Since $\mathcal{J}$ is the unique maximal ideal of R, it follows that R is in fact a finite local ring, for a ring R is called *local* if it has a unique maximal ideal. However, not all local rings are completely primary, although completely primary rings play an important role in the study of finite local rings. For instance, the full 2×2 matrix ring $\mathbf{M}_2(\mathbb{F})$ over a finite field $\mathbb{F}$ is a local ring with unique maximal ideal $\left\{\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}\right\}$ and yet $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ is a zero-divisor in $\mathbf{M}_2(\mathbb{F})$.

Completely primary finite (CPF) rings have been studied in some detail by Raghavendran in [18], and here we give a list of their basic properties.

3.1 Basic Properties of CPF rings

Proposition 3.1 *Let R be a CPF ring and let $\mathcal{J}$ be its set of zero-divisors. Then $\mathcal{J}$ is the unique maximal ideal of R and $R/\mathcal{J} \cong GF(p^r)$, for some prime p and positive integer r.*

Proof. [sketch] $\mathcal{J}$ is certainly an ideal of R, all the elements of $R-\mathcal{J}$ are invertible and hence $\mathcal{J}$ is the unique maximal ideal of R. Moreover, $R/\mathcal{J}$ is a finite division ring, and hence, $R/\mathcal{J} \cong GF(p^r)$. ■

Proposition 3.2 *Let R be a CPF ring and let $\mathcal{J}$ be its unique maximal ideal. Then $\mathcal{J}^n = (0)$, $|R| = p^{nr}$ and $|\mathcal{J}| = p^{(n-1)r}$ for some prime p and positive integers n, r.*

Proof. [sketch] Let $x \in \mathcal{J}$. Since R is finite, $x^i = x^j$ for $i < j$. Hence, $x^i(x^{j-i}-1) = 0$ and $x^{j-i}-1$ is invertible since $x^{j-i}-1 \notin \mathcal{J}$. Hence, $x^i = 0$; i.e. $\mathcal{J}$ is a nil ideal. But again, finiteness of R implies that $\mathcal{J}$ is nilpotent, say, $\mathcal{J}^n = (0)$, for some positive integer n.

On the other hand, we can consider $\mathcal{J}^i/\mathcal{J}^{i+1}$ as a vector space over $R/\mathcal{J}$ with respect to

$$(r+\mathcal{J})(x+\mathcal{J}^{i+1}) = rx+\mathcal{J}^{i+1}.$$

Hence, $|\mathcal{J}^i/\mathcal{J}^{i+1}| = p^{c_i r}$, for some positive integer c_i.

Taking into account that $\mathcal{J}^n = (0)$, we have

$$|R| = |R/\mathcal{J}| \cdot |\mathcal{J}/\mathcal{J}^2| \cdot \cdots \cdot |\mathcal{J}^{h-2}/\mathcal{J}^{h-1}| \cdot |\mathcal{J}^{h-1}| = p^{rn},$$

where $n = 1 + c_1 + \cdots + c_{h-1}$, for some positive integer h.

Notice that since $c_i \geq 1$, we have $h \leq n$. By Proposition 3.1, $R/\mathcal{J} \cong GF(p^r)$, and hence, $|\mathcal{J}| = |R|/|\mathbb{F}_{p^r}| = p^{rn}/p^r = p^{r(n-1)}$. ■

Proposition 3.3 *Let R be a CPF ring with maximal ideal $\mathcal{J}$. Then $charR = p^k$ for some k with $1 \leq k \leq n$.*

Proof. Since $R/\mathcal{J}$ has characteristic p, we have $p \in \mathcal{J}$ and so, $p^n = 0$. Hence, the characteristic of R is p^k with $k \leq n$. ■

Lemma 3.4 *Let R be a CPF ring of characteristic p^k and order p^{nr}, with maximal ideal $\mathcal{J}$ of index of nilpotency i. Then $1 \leq k \leq i \leq n$.*

Proof. We have only to prove that $k \leq i$. We know that $\mathcal{J} \neq 0$ so that $i \geq 2$. Since $p^k = 0$, it follows that $p \in \mathcal{J}$ and $i \geq k$. ■

Proposition 3.5 *Let R be a CPF ring and let $\mathcal{J}$ be its unique maximal ideal. Then there exists an element $b \in R$ of multiplicative order $p^r - 1$ such that if $\psi : R \longrightarrow R/\mathcal{J}$ is the canonical homomorphism, then $\psi(b)$ is a primitive element of $R/\mathcal{J}$ and*

$$K = < b > \cup \{0\}$$

forms a complete system of coset representatives of $\mathcal{J}$ in R. Further, if ν, $\mu \in K$ with $\nu - \mu \in \mathcal{J}$, then $\nu = \mu$.

Proof. Obviously, the group of units G_R of R is $R - \mathcal{J}$, and $\phi : R \longrightarrow R/\mathcal{J}$ induces a surjective multiplicative group homomorphism

$$\tilde{\phi} : G_R \longrightarrow G_{(R/\mathcal{J})}.$$

Since $Ker\phi = \mathcal{J}$, we have $Ker\tilde{\phi} = 1 + \mathcal{J}$. In particular, $1 + \mathcal{J}$ is normal in G_R.

Let $< \beta >= G_{(R/\mathcal{J})}$ and let $b_o \in \tilde{\phi}^{-1}(\beta)$. Then, the multiplicative order of b_o must be a multiple of $p^r - 1$ and a divisor of

$$\begin{aligned} |R - \mathcal{J}| &= p^{nr} - p^{(n-1)r} \\ &= p^{(n-1)r}(p^r - 1); \end{aligned}$$

hence of the form $p^\lambda(p^r - 1)$. But then $b = b_o^{p^\lambda}$ has multiplicative order $p^r - 1$ and $\tilde{\phi}(b_o^{p^\lambda}) = \beta^{p^\lambda}$ which is still a generator of $G_{(R/\mathcal{J})}$, since $(p^\lambda,\ p^r - 1) = 1$.

Further, $\phi(K) = R/\mathcal{J}$, and hence, K is a complete set of coset representatives of $\mathcal{J}$ in R. Hence, ν, $\mu \in K$ with $\nu - \mu \in \mathcal{J}$ implies that $\nu = \mu$. ■

We collect the above properties of b in the following:

Remark 3.6 *Let R be a CPF ring with maximal ideal $\mathcal{J}$. Then R contains an element b such that*

(i) $b + \mathcal{J}$ is a primitive element of $R/\mathcal{J}$;

(ii) b has multiplicative order $p^r - 1$; and

(iii) if ν, $\mu \in K$ with $\nu - \mu \in \mathcal{J}$, then $\nu = \mu$, where $K =< b > \cup\{0\}$.

Corollary 3.7 *Let R be a CPF ring with maximal ideal $\mathcal{J}$. Then every element of R can be expressed uniquely in the form $\nu + m$, with $\nu \in K$ and $m \in \mathcal{J}$, where $K =< b > \cup\{0\}$.*

Proposition 3.8 *Let R be a CPF ring with maximal ideal $\mathcal{J}$. If $|R| = p^{nr}$, $\mathcal{J}^n = (0)$ and $charR = p^n$, then R is commutative.*

Proof. [sketch] Consider the equation

$$\sum_{j=0}^{n-1} p^j \alpha_j = \sum_{j=0}^{n-1} p^j \beta_j,$$

where $\alpha_j, \beta_j \in K$. If

$$(\alpha_0,\ \alpha_1,\ \ldots,\ \alpha_{n-1}) \neq (\beta_0,\ \beta_1,\ \ldots,\ \beta_{n-1}),$$

let i be the least index with $\alpha_i \neq \beta_i$. Then, multiplying by p^{n-1-i}, we obtain $p^{n-1}(\alpha_i - \beta_i) = 0$ and hence, $p^{n-1} = 0$ since $\alpha_i - \beta_i \in \mathcal{J}$, a contradiction. So, $\alpha_j = \beta_j$ (by Proposition 3.5), for all $j = 0,\ 1,\ ...,\ n - 1$. ■

Proposition 3.9 *Let R be a CPF ring. Then, any subring R_1 of R is a CPF ring with maximal ideal $\mathcal{J}_1 = \mathcal{J} \cap R_1$. Furthermore, there are integers n_1, r_1 such that $|R_1| = p^{n_1 r_1}, |\mathcal{J}_1| = p^{(n_1-1)r_1}$, where $r_1 | r$.*

Proof. [sketch] Clearly, $\mathcal{J} \cap R_1$ is the set of all zero-divisors of R_1 and $\mathcal{J} \cap R_1$ is a subgroup of R^+ (by Lemma 2.1), hence R_1 is a CPF ring with maximal ideal $\mathcal{J} \cap R_1$. ■

Proposition 3.10 *Let R be a CPF ring. Then, any quotient of R (by a two sided-ideal) and any homomorphic image of R is a CPF ring.*

Proof. Let $f : R \longrightarrow R_1$ be a surjective ring homomorphism. Since $\mathcal{J}$ is the unique maximal ideal of R, $Kerf \subset \mathcal{J}$. Also, clearly, $\{x + Kerf : x \in \mathcal{J}\}$ is the set of all zero-divisors in $R/Kerf$, and hence it is a subgroup of $(R/Kerf)^+$. So, $R/Kerf$ is a CPF ring and hence, R_1 is completely primary too. ■

Proposition 3.11 *Let R be a CPF ring. Then, the set K forms a subfield of R if and only if $charR = p$.*

Proof. [sketch] Use the Binomial Theorem to show that K is closed under addition, every element in K has a negative in K.

Since $K \subset R$ and addition is associative in R, it follows that K is a group under addition. Obviously, $\alpha + \beta = \beta + \alpha$, for all α, $\beta \in K$. The distributive laws follow trivially since $K \subset R$.

But the non-zero elements of K form a multiplicative group, hence, K is a subfield of R.

Conversely, if K is a subfield of R, then $\text{char}K = \text{char}R = p$, since the identity element in R is that in K. ■

Proposition 3.12 *Let R be a CPF ring. Then R contains a subfield of order p^r if and only if $charR = p$. Also, if $\mathbb{F}_1$, $\mathbb{F}_2$ are any subfields of R of order p^r, then there exists an element $x \in G_R$ such that $x\mathbb{F}_1x^{-1} = \mathbb{F}_2$.*

Proof. We can consider the set K in R, and the proof of the first part will be the same as that for Proposition 3.11. The second part follows easily. ■

Proposition 3.13 *Let R be a CPF ring of order p^{nr}, characteristic p^k and maximal ideal $\mathcal{J}$ such that $R/\mathcal{J} \cong GF(p^r)$. Let $R_o = \mathbb{Z}_{p^k}[b]$, where b is as in Remark 3.6. Then, R_o is a commutative subring of R with $R_o/(R_o \cap \mathcal{J}) \cong R/\mathcal{J}$, and minimal with respect to $R_o/(R_o \cap \mathcal{J}) \cong R/\mathcal{J}$. Further, a subring S_o of R is minimal with respect to $S_o/(S_o \cap \mathcal{J}) \cong R/\mathcal{J}$ if and only if it is conjugate to R_o in R.*

Proof. It is obvious that R_o is a commutative subring of R. By Proposition 3.9, R_o is a completely primary ring with maximal ideal $R_o \cap \mathcal{J}$ and residue order p^{r_1}, where $r_1|r$. But R_o contains $< b >$, and its residue field therefore contains at least p^r elements. Hence, R_o is a commutative completely primary ring with residue field isomorphic to $R/\mathcal{J} \cong GF(p^r)$.

Let S_o be a subring of R minimal with respect to $S_o/(S_o \cap \mathcal{J}) \cong R/\mathcal{J}$ and let $\psi : R \longrightarrow R/\mathcal{J}$ be the canonical homomorphism. Since $S_o \cap \mathcal{J}$ is the unique maximal ideal of S_o, the restriction of ψ to S_o is surjective. Hence, S_o contains an element b_o of multiplicative order $p^r - 1$ and hence, $\mathbb{Z}_{p^k}[b_o] \subset S_o$. However, ψ has also a surjective restriction to $\mathbb{Z}_{p^k}[b_o]$ and so

$$\mathbb{Z}_{p^k}[b_o]/(\mathbb{Z}_{p^k}[b_o] \cap \mathcal{J}) \cong R/\mathcal{J}.$$

But then, by the minimality of S_o, we have that $S_o = \mathbb{Z}_{p^k}[b_o]$. By Proposition 3.12, $< b >= a < b_o > a^{-1}$, for some element $a \in G_R$, and hence, $\mathbb{Z}_{p^k}[b_o]$ is conjugate to $\mathbb{Z}_{p^k}[b]$.

That R_o is minimal with respect to $R_o/(R_o \cap \mathcal{J}) \cong R/\mathcal{J}$ is essentially contained in the above argument. ■

Lemma 3.14 *Let R be a CPF ring, not necessarily commutative. Then, the group of units G_R of R is $R - \mathcal{J}$.*

Proof. This is a direct consequence of Lemma 2.1, since every non-unit in R lies in $\mathcal{J}$. ■

Lemma 3.15 *Let R be a CPF ring and let G_R be its group of units. Then $|G_R| = p^{(n-1)r}(p^r - 1)$.*

Proof. Since $|R| = p^{nr}$, $|\mathcal{J}| = p^{(n-1)r}$, and $G_R = R - \mathcal{J}$ (by Lemma 3.14), it is easy to see that

$$|G_R| = |R - \mathcal{J}| = |R| - |\mathcal{J}| = p^{nr} - p^{(n-1)r} = p^{(n-1)r}(p^r - 1).$$

■

Lemma 3.16 *The group G_R contains a maximal subgroup of order $p^{(n-1)r}$ and a subgroup of order $(p^r - 1)$.*

Proof. This is a variation of Sylow's Theorem since the prime power $p^{(n-1)r}$ is the highest power of p which divides the order of G_R, and $(p^{(n-1)r},\ (p^r - 1)) = 1$. ■

Lemma 3.17 *The subgroup $1+\mathcal{J}$ is normal in G_R.*

Proof. This follows because, for any $x \in G_R$,

$$x(1+\mathcal{J}) = x+\mathcal{J} = (1+\mathcal{J})x,$$

since $\mathcal{J}$ is the set of all the zero-divisors in R. ■

Here, $1+\mathcal{J}$ is the maximal normal $p-$subgroup of G_R and $< b >$ is the cyclic subgroup of G_R of order p^r-1. Moreover, $1+\mathcal{J}$ is a solvable group since every $p-$group is solvable.

Proposition 3.18 *Let R be a CPF ring. Then, the group of units G_R is soluble.*

Proof. Since $1+\mathcal{J}$ is a normal p-subgroup of G_R and $G_R/(1+\mathcal{J})$ is cyclic, it follows that G_R is solvable. ■

Proposition 3.19 *Let R be a CPF ring. Then, if G is any subgroup of G_R of order p^r-1, then G is conjugate to $< b >$ in G_R.*

Proof. This follows from key properties of p-solvable groups contained in the variation of Sylow's theorem, since the order of G is prime to its index in G_R. ■

Proposition 3.20 *Let R be a CPF ring. Then, if G_R contains a normal subgroup of order p^r-1, then the set K is contained in the center of the ring R.*

Proof. By Proposition 3.19 above, $< b > \lhd G_R$ and since

$$1+\mathcal{J} \lhd G_R \quad \text{with } | < b > \cap (1+\mathcal{J})| = 1,$$

it follows that $< b >$ and $1+\mathcal{J}$ commute element-wise. Hence, by Corollary 3.7, b is in the center of R. ■

Proposition 3.21 *Let R be a CPF ring. Then*

(i) $G_R = (1+\mathcal{J}) \times_\theta < b >$, a semi-direct product;

(ii) $(1+\mathcal{J}^i)/(1+\mathcal{J}^{i+1}) \cong \mathcal{J}^i/\mathcal{J}^{i+1}$ (the right hand side as an additive group, and the left hand side as a multiplicative group).

Proof.

(i) We know that $1+\mathcal{J} \lhd G_R$. Since $|G_R| = |1+\mathcal{J}|.|< b >|$ and $(1+\mathcal{J}) \cap < b >= 1$ (by Lagrange's Theorem), we have $G_R = (1+\mathcal{J}) \cdot < b >$. Hence, $G_R = (1+\mathcal{J}) \times_\theta < b >$, a semi-direct product.

(ii) Consider the map

$$\begin{array}{rccc} \eta: & (1+\mathcal{J}^i)/(1+\mathcal{J}^{i+1}) & \longrightarrow & \mathcal{J}^i/\mathcal{J}^{i+1} \\ & (1+x)(1+\mathcal{J}^{i+1}) & \longmapsto & x+\mathcal{J}^{i+1} \end{array}$$

Then, it is easy to see that η is an isomorphism. ■

Lemma 3.22 *Let R be a CPF ring. Then $R = \mathbb{Z}_{p^k}[G_R]$.*

Proof. Clearly, $1+\mathcal{J}$ and K are in $\mathbb{Z}_{p^k}[G_R]$. But $R = K + \mathcal{J}$, by Proposition 3.5. Hence, $R \subseteq \mathbb{Z}_{p^k}[G_R]$. ■

Corollary 3.23 *Let R be a CPF ring. Then R is commutative if and only if G_R is Abelian.*

Lemma 3.24 *If R is commutative, then $1+\mathcal{J}$ is isomorphic to a direct product of cyclic $p-$groups.*

4 Representation of CPF rings

Before we prove our main result, we consider the following class of finite rings.

4.1 Galois rings

Galois rings are a generalization of Galois fields and have been used widely in the past two decades to construct various optimal families of $q-$ary polyphase sequences; error correcting codes over Galois rings. These rings are important in the structure theory of finite commutative rings. Any finite commutative ring has a unique decomposition as a direct sum of finite local commutative rings. If R is a finite local commutative ring of characteristic p^n, then R contains a largest Galois extension S of $\mathbb{Z}_{p^n}$, called the coefficient subring, and R is a homomorphic image of a multivariable polynomial ring over S. See McDonald [17] for proofs of these statements.

In this article, the Galois rings serve as building blocks in our study of completely primary finite rings. Let $q = p^r$ be a prime power and $h(X) \in \mathbb{Z}_{p^n}[X]$ a monic

polynomial of degree r which is irreducible modulo p (a so-called *basic irreducible polynomial* or *Galois polynomial*).

The quotient ring $GR(p^{nr},\ p^n) \cong \mathbb{Z}_{p^n}[X]/(h(X))$ is called a *Galois ring* of order p^{nr} and characteristic p^n. Moreover, the integers $p,\ n$ and r chosen above determine uniquely (up to isomorphism) the Galois ring $GR(p^{nr},\ p^n)$ [18]. For instance, $GR(p^n,\ p^n)$ is the ring $\mathbb{Z}_{p^n}$ and $GR(p^r,\ p)$ is the field $\mathbb{F}_{p^r}$.

In this article the symbol R_o will denote the Galois ring $GR(p^{nr},\ p^n)$ or a commutative subring of a finite ring R.

4.1.1 Properties of Galois rings

It is well known that, for any prime integer p and any positive integers r and n, there exists (up to isomorphism) a unique ring $R_o = GR(p^{nr},\ p^n)$ with the following properties:

(i) R_o is a commutative local/chain ring with maximal ideal pR_o, invariants $(q,\ n)$ and characteristic p^n;

(ii) The isomorphism type of R_o does not depend on the particular choice of the polynomial $h(X)$;

(iii) A finite chain ring with invariants $(q,\ n)$ and characteristic p^n is isomorphic to R_o;

(iv) Every automorphism of R_o/pR_o can be lifted in a unique way to an automorphism of R_o. Thus, $Aut(R_o) \cong Aut(\mathbb{F}_q)$.

Moreover, all the ideals of R_o are given by

$$(0) = p^n R_o \subset p^{n-1}R_o \subset \cdots \subset pR \subset p^0 R_o = R_o$$

and that the ideal $p^i R_o$, $0 \leq i \leq n$, has cardinality $p^{(n-i)r}$.

An arbitrary element α of the Galois ring R_o can be expressed (uniquely) either in *additive formalism* as

$$\alpha = \sum_{i=0}^{r-1} a_i \xi^i, \quad a_i \in \mathbb{Z}_{p^n},$$

where ξ is a root of a monic basic irreducible polynomial

$$h(X) = h_0 + h_1 X + \cdots + h_{r-1}X^{r-1} + X^r \in \mathbb{Z}_{p^n}[X]$$

of degree r over $\mathbb{Z}_{p^n}$; or in $p-adic\ formalism$ as

$$\alpha = \sum_{i=0}^{n-1} t_i p^i, \quad t_i \in T_{p^r} = \{0,\ 1,\ \xi,\ \ \ldots\ , \xi^{p^r-2}\}, \tag{4.1}$$

where the set T_{p^r} is referred to as the *Teichmuller set*. In the $p-$adic formalism (4.1), α is a unit if and only if $t_0 \neq 0$, and it is a zero divisor or 0 if and only if $t_0 = 0$ or $t_i = 0$ for every i.

Notice that in $p-$adic formalism, an arbitrary zero divisor $\alpha \in R_o$ has a unique form

$$\alpha = t_j p^j + \cdots + t_{n-1} p^{n-1} = p^j \alpha', \quad t_j \neq 0, \quad 1 \leq j \leq n-1,$$

where $\alpha' = t_j + \cdots + t_{n-1} p^{n-j-1}$ is a unit of R_o.

4.2 Further properties of CPF rings

We start with the following:

Proposition 4.1 [Compare this with Propositions 3.12 & Lemma 4.3] *Let R be a CPF ring of order p^{nr} and maximal ideal $\mathcal{J}$ such that $R/\mathcal{J} \cong GF(p^r)$.*

(i) Then, R contains a subring isomorphic to $GR(p^{kr},\ p^k)$ if and only if $charR = p^k$;

(ii) If R_2 and R_3 are subrings of R having the same residue order as R, then $R_2 = a^{-1} R_3 a$, for some $a \in G_R$.

Proof

(i) Suppose R contains a subring R_1 isomorphic to $GR(p^{kr},\ p^k)$. Then, $charR = charR_1 = p^k$ since the identity element in R is that in R_1.

Conversely, suppose $charR = p^k$. Then $R \supseteq \mathbf{Z}_{p^k}$. Let f be a monic polynomial of degree r in $\mathbf{Z}_{p^k}[X]$, irreducible over $\mathbf{Z}_p$. Then, f has a root α in R, and therefore $\mathbf{Z}_{p^k}[\alpha]$ is a subring of R. Let ψ be the canonical map

$$\mathbf{Z}_{p^k}[X] \longrightarrow \mathbf{Z}_{p^k}[\alpha],$$

so that

$$\mathbf{Z}_{p^k}[\alpha] \cong \mathbf{Z}_{p^k}[X]/Ker(\psi).$$

Then, $f \in Ker\psi$, and in fact, $|\mathbf{Z}_{p^k}[X]/(f)| = p^{kr}$, so that $|\mathbf{Z}_{p^k}[X]/Ker\psi| \leq p^{kr}$. But again, we can show that $|\mathbf{Z}_{p^k}[\alpha]| \geq p^{kr}$, so that

$$|\mathbf{Z}_{p^k}[X]/Ker\psi| = p^{kr} = |\mathbf{Z}_{p^k}[X]/(f)|.$$

Thus, $Ker\psi = (f)$, and therefore,

$$\mathbf{Z}_{p^k}[\alpha] \cong \mathbf{Z}_{p^k}[X]/(f) \cong GR(p^k,\ p^{kr}).$$

So, R contains a subring isomorphic to the Galois ring $GR(p^{kr},\ p^k)$.

(ii) We have $charR_2 = charR_3 = charR = p^k$, and therefore,

$$R_2 \cong GR(p^{kr},\ p^k) \cong R_3.$$

Also, each R_i $(i = 2,\ 3)$ contains an element b_i of order $p^r - 1$ with the usual properties. Thus, $R_2 = \mathbf{Z}_{p^k}[b_2]$ and $R_3 = \mathbf{Z}_{p^k}[b_3]$. Now, $< b_2 >$ and $< b_3 >$ are both multiplicative subgroups of G_R of order $p^r - 1$, so, as in Proposition 3.12, $< b_2 >= a^{-1} < b_3 > a$, for some $a \in G_R$. Hence, $R_2 = \mathbf{Z}_{p^k}[b_2] = a^{-1}\mathbf{Z}_{p^k}[b_3]a = a^{-1}R_3a$. ■

Notice that Proposition 4.1 shows that every completely primary finite ring contains a Galois subring, but we can in fact be more specific than this. The following lemma, taken in conjunction with Proposition 4.1, shows that all the Galois subrings of a completely primary finite ring R having the same residue field as R are conjugates of $\mathbf{Z}_{p^k}[b]$.

Lemma 4.2 *Let R be a CPF ring of order p^{nr} and characteristic p^k, and let b be the element of R as in Remark* 3.6. *Then, the subring $\mathbf{Z}_{p^k}[b]$ of R is isomorphic to the Galois ring $GR(p^{kr},\ p^k)$.*

Proof. By Proposition 4.1(i), R contains a subring R_1 isomorphic to $GR(p^{kr},\ p^k)$. But, by Remark 3.6, R_1 contains an element b_1 with the usual properties, and of order $p^r - 1$, so that, by Proposition 3.13, $R_1 = \mathbf{Z}_{p^k}[b_1]$. But $< b_1 >$ is a subgroup of G_R of order $p^r - 1$, so, by Proposition 3.12, $< b_1 >= a^{-1} < b > a$, where $a \in G_R$. Thus,

$$\mathbf{Z}_{p^k}[b] = a\mathbf{Z}_{p^k}[b_1]a^{-1} = aR_1a^{-1} \cong R_1,$$

and therefore,

$$\mathbf{Z}_{p^k}[b] \cong GR(p^{kr},\ p^k).$$

■

Observe that part (ii) of Proposition 4.1 states only that Galois subrings of R having the *same residue field as R* are conjugate. In fact, we can weaken this statement to give the following:

Lemma 4.3 *Let R be a CPF ring of order p^{nr} and characteristic p^k, and let R_2, R_3 be Galois subrings of R having residue field $GF(p^s)$ for some $s|r$. Then, there exists $a \in G_R$ such that $R_3 = aR_2a^{-1}$.*

Proof. By Remark 3.6, R_i $(i = 2, 3)$ contains an element b_i of order $p^s - 1$ with the usual properties, so that, by Proposition 3.13, $R_i = \mathbf{Z}_{p^k}[b_i]$.

Consider $< b_i >$. Then, $< b_i > \leq G_R$, so that $p^s - 1|p^{(n-1)r} \cdot (p^r - 1)$. But $(p^s - 1,\ p^{(n-1)r}) = 1$, so that $p^s - 1|p^r - 1$. Now, G_R is solvable (see Proposition 3.18),

and furthermore, $(p^r - 1,\ p^{(n-1)r}) = 1$. Therefore, $< b_i >$ is contained in a subgroup H_i of G_R of order $p^r - 1$. But again, by the same Proposition 3.13, there exists $a \in G_R$ such that $H_3 = aH_2a^{-1}$. Furthermore, H_2 and H_3 are conjugate with $< b >$ (where b is the usual element of R), and therefore, both cyclic. Thus $< b_3 >$ and $a < b_2 > a^{-1}$ are both subgroups of order $p^s - 1$ in the cyclic group H_3, and therefore, $< b_3 >= a < b_2 > a^{-1}$. Hence,

$$R_3 = \mathbf{Z}_{p^k}[b_3] = a\mathbf{Z}_{p^k}[b_2]a^{-1} = aR_2a^{-1}. \qquad \blacksquare$$

4.3 Modules over Galois rings

There is a way of representing finite local rings as rings of matrix-like objects, called Szele matrices, due to Wilson [19]. This representation uses Galois rings. However, we do not find this representation to be very suitable in the study of isomorphism classes, automorphism groups and unit groups of completely primary finite rings. We, instead, use a module-like representation of such rings.

We start with the following:

Proposition 4.4 *Let R_o be the Galois ring $GR(p^{nr},\ p^n)$ and let M be a finite R_o-bimodule. Then, there exist $x_1,\ ...,\ x_k \in M$ such that*

$$M = R_ox_1 \oplus \cdots \oplus R_ox_k.$$

Moreover, if $M = R_oy_1 \oplus \cdots \oplus R_oy_l$ is another such decomposition of M, then $l = k$ and the order ideals of the y_j are (after possible re-indexing) the order ideals of the x_i.

This is essentially Corollary 2 of Proposition 1.1 in Wilson [19].

Proposition 4.5 *Let R_o be the Galois ring $GR(p^{nr},\ p^n)$ and let M be a finite R_o-bimodule. Then,*

$$M = M_1 \oplus \cdots \oplus M_r, \quad (as R_o - modules)$$

where for each i, $1 \leq i \leq r$, there exist $\sigma_i \in Aut(R_o)$ such that $mr_o = \sigma_i(r_o)m$, for every $m \in M_i$ and every $r_o \in R_o$.

Proof. [very long] Left out

$\blacksquare$

Corollary 4.6 *Let R_o be the Galois ring $GR(p^{nr},\ p^n)$ and let M be a finite R_o-bimodule. Then, there exist $x_1,\ ...,\ x_k \in M$ and $\sigma_1,\ ...,\ \sigma_h \in Aut(R_o)$ such that*

$$M = R_o \oplus R_ox_1 \oplus \cdots \oplus R_ox_h \text{ and } x_ir = \sigma_i(r)x_i,$$

for every $r \in R_o$ and for each $i = 1,\ ...,\ h$.

From now on, we shall denote $\sigma(r)$ by r^σ, for any $\sigma \in Aut(R_o)$ and r in any subset of R.

Proposition 4.7 *Let R_o be the Galois ring $GR(p^{nr},\ p^n)$ and let M be a finite R_o-bimodule. Let $m \in M$ and p^t be the additive order of m. Then, $|R_o m| = p^{tr}$.*

Proof. Consider the map

$$\begin{array}{rccc} \phi: & R_o & \longrightarrow & R_o m \\ & r & \longmapsto & rm. \end{array}$$

Then, it is easy to see that ϕ is an R_o-homomorphism and $Ker\phi = p^t R_o$. Therefore, $R_o m \cong R_o/p^t R_o$ and hence, $|R_o m| = p^{tr}$. ■

4.4 Representation Theorem

Theorem 4.8 *Let R be a CPF ring of order p^{nr}, $|R/\mathcal{J}| = p^r$, $charR = p^k$, and let R_o be a maximal Galois subring of R. Then, there exist $x_1,\ ...,\ x_h \in \mathcal{J}$ and $\sigma_1,\ ...,\ \sigma_h \in Aut(R_o)$ such that*

$$R = R_o \oplus R_o x_1 \oplus \cdots \oplus R_o x_h \text{ and } x_i r = r^{\sigma_i} x_i,$$

for ever $r \in R_o$ and each $i = 1,\ ...,\ h$.

Proof. Consider $\mathcal{J}/pR_o$. This is clearly an R_o-bimodule. Hence, by Corollary 4.6, there exist $m_1 + pR_o,\ ...,\ m_h + pR_o \in \mathcal{J}/pR_o$ and $\sigma_1,\ ...,\ \sigma_h \in Aut(R_o)$ such that $\mathcal{J}/pR_o = \oplus \sum_{i=1}^{h} R_o(m_i + pR_o)$ and $(m_i + pR_o)r = r^{\sigma_i}(m_i + pR_o)$, for every $r \in R_o$ and for each $i = 1,\ ...,\ h$. Suppose that $p^{n_1},\ ...,\ p^{n_h}$ are the additive orders of $m_1 + pR_o,\ ...,\ m_h + pR_o$, respectively.

Let $R_o = \mathbf{Z}_{p^k}[b]$, where b is as in Remark 3.6, and let $m_i b = b^{\sigma_i} m_i + r_i$, where $r_i \in pR_o$. If $\sigma_i \neq id_{R_o}$, put $s_i = (b^{\sigma_i} - b)^{-1} r_i$, where $(b^{\sigma_i} - b)$ is a unit in R_o (because its image under the canonical homomorphism $R_o \longrightarrow R_o/pR_o$ is not zero), and put $x_i = m_i + s_i$. Then,

$$\begin{aligned} x_i b &= (m_i + s_i)b \\ &= m_i b + s_i b \\ &= b^{\sigma_i} m_i + r_i + s_i b \\ &= b^{\sigma_i} m_i + (b^{\sigma_i} - b)s_i + s_i b \\ &= b^{\sigma_i} m_i + b^{\sigma_i} s_i \\ &= b^{\sigma_i} x_i. \end{aligned}$$

Next, since p^{n_i} is the additive order of $m_i + pR_o$, $p^{n_i}x_i \in pR_o$ and hence $p^{n_i}bx_i = p^{n_i}x_ib$. But $p^{n_i}x_ib = p^{n_i}b^{\sigma_i}x_i$; so $p^{n_i}bx_i = p^{n_i}b^{\sigma_i}x_i$. This implies that $p^{n_i}(b-b^{\sigma_i})x_i = 0$ and hence, if $p^{n_i}x_i \neq 0$, then $b = b^{\sigma_i}$, a contradiction, because $\sigma_i \neq id_{R_o}$. Therefore, $p^{n_i}x_i = 0$.

If $\sigma_i = id_{R_o}$, then

$$\begin{aligned} m_i &= m_ib^{p^r-1} = m_ibb^{p^r-2} = (bm_i + r_i)b^{p^r-2} = (bm_ib + r_ib)b^{p^r-3} \\ &= (b^2m_i + r_ib + r_ib)b^{p^r-3} = \\ &\quad \cdots \\ &= b^{p^r-1}m_i + (p^r-1)r_ib^{p^r-2} = m_i + (p^r-1)r_ib^{p^r-2}; \end{aligned}$$

and hence, $(p^r-1)r_i = 0$, which implies that $r_i = 0$, since $p^r - 1$ is a unit. Hence, $m_ib = bm_i$.

Let $p^{n_i}m_i = p^{t_i}u_i$, where u_i is a unit in R_o. If $n_i \geq t_i$, then, $p^{t_i}(p^{n_i-t_i}m_i - u_i) = 0$ and hence, $p^{n_i-t_i}m_i - u_i$ is a zero-divisor in R_o; a contradiction. Hence, $n_i < t_i$. Put $x_i = m_i - p^{t_i-n_i}u_i$. In this case, it is clear that the additive order of x_i is p^{n_i}.

Thus, the additive orders of x_1, ..., x_h are p^{n_1}, ..., p^{n_h}, respectively.

Now, clearly, $\mathcal{J} = pR_o + \sum_{i=1}^{h} R_ox_i$. But, by Proposition 4.7,

$$|R_ox_i| = |R_o(m_i + pR_o)|.$$

Now, by comparing orders, we deduce that

$$\mathcal{J} = pR_o \oplus R_ox_1 \oplus \cdots \oplus R_ox_h$$

and hence,

$$R = R_o \oplus R_ox_1 \oplus \cdots \oplus R_ox_h.$$

Also, $x_ib = b^{\sigma_i}x_i$.

Since every element of R_o can be written uniquely as $\sum_{j=0}^{k-1} p^j\lambda_j$ where $\lambda_j \in K$, then for every $r \in R_o$,

$$\begin{aligned} x_ir &= x_i[\sum_{j=0}^{k-1} p^j\lambda_j] = \sum_{j=0}^{k-1} p^jx_i\lambda_j \\ &= [\sum_{j=0}^{k-1} p^j\lambda_j^{\sigma_i}]x_i = [\sum_{j=0}^{k-1} p^j\lambda_j]^{\sigma_i}x_i \\ &= r^{\sigma_i}x_i. \end{aligned}$$

■

Proposition 4.9 *Let R be a CPF ring of order p^{nr}, $|R/\mathcal{J}| = p^r$, $charR = p^k$, and let R_o be a maximal Galois subring of R. Let $\sigma_1,\ ...,\ \sigma_h \in Aut(R_o)$ be as defined in Theorem* 4.8. *Then, $\sigma_1,\ ...,\ \sigma_h$ are uniquely determined by R and R_o.*

Proof. Let $R_o = \mathbb{Z}_{p^k}[b]$, with b as in Remark 3.6 and suppose that

$$R = R_o \oplus R_o x_1 \oplus \cdots \oplus R_o x_h = R_o \oplus R_o y_1 \oplus \cdots \oplus R_o y_h,$$

such that $x_i r = r^{\sigma_i} x_i$; $y_i r = r^{\theta_i} y_i$, for every $r \in R_o$ and each $i = 1,\ ...,\ h$; where $x_i, y_i \in \mathcal{J}$ and $\sigma_i, \theta_i \in Aut(R_o)$. Also, assume that σ_i and θ_i occur with multiplicity n_i and $n_i^{'}$, respectively. We want to prove (after possible re-indexing) that $\{\sigma_1,\ ...,\ \sigma_h\} = \{\theta_1,\ ...,\ \theta_h\}$ and $n_i = n_i^{'}$, for each $i = 1,\ ...,\ h$.

Since for each $i = 1,\ ...,\ h$; $y_i \in \mathcal{J} = pR_o \oplus R_o x_1 \oplus \cdots \oplus R_o x_h$ and $y_i \notin pR_o$, $y_i = pr_i + \sum_j r_{ij} x_j$, where $r_{ij} x_j \neq 0$ for at least one j. Now,

$$\begin{aligned} pb^{\theta_i} r_i + \sum_j b^{\theta_i} r_{ij} x_j &= b^{\theta_i} y_i = y_i b = pr_i b + \sum_j r_{ij} x_j b \\ &= pbr_i + \sum_j b^{\sigma_j} r_{ij} x_j. \end{aligned} \tag{4.2}$$

Since the sums are direct, it follows, for all j, that

$$b^{\theta_i} r_{ij} x_j = b^{\sigma_j} r_{ij} x_j, \text{and hence } (b^{\theta_i} - b^{\sigma_j}) r_{ij} x_j = 0.$$

If now $r_{ij} x_j \neq 0$, then $b^{\theta_i} - b^{\sigma_j} = 0$ and so $\theta_i = \sigma_j$. This shows two things. On the one hand, since $r_{ij} x_j \neq 0$ for at least one j, it follows that $\theta_i \in \{\sigma_1,\ ...,\ \sigma_h\}$ and by symmetry $\{\sigma_1,\ ...,\ \sigma_h\} = \{\theta_1,\ ...,\ \theta_h\}$. On the other hand, if $\sigma_j \neq \theta_i$ then $r_{ij} x_j = 0$ and so

$y_i = pr_i + \sum_{\sigma_j = \theta_i} r_{ij} x_j \in pR_o \oplus \sum^{\oplus}_{\sigma_j = \theta_i} R_o x_j$.

Hence, $R_o \oplus \sum^{\oplus}_{\theta_\lambda = \theta_i} R_o y_\lambda \subset R_o \oplus \sum^{\oplus}_{\sigma_j = \theta_i} R_o x_j$.

By symmetry $R_o \oplus \sum^{\oplus}_{\theta_\lambda = \theta_i} R_o y_\lambda = R_o \oplus \sum^{\oplus}_{\sigma_j = \theta_i} R_o x_j$. By Proposition 4.4, the number of summands is the same. Hence, if $\sigma_j = \theta_i$ the multiplicities of σ_j and θ_i are the same. ■

Definition We call $\sigma_1,\ ...,\ \sigma_h$ defined above, the *associated automorphisms* of R with respect to R_o.

Let $B = \{x_1,\ ...,\ x_h\}$ be as above and let $\tau \in Aut(R_o)$. Put

$$B_\tau = \{x \in B : xb = b^\tau x\}$$

and let $\mathcal{J}_\tau = \sum^{\oplus}_{x_i \in B_\tau} R_o x_i$.

Then, obviously, $\mathcal{J}_\tau$ is an R_o-submodule of $\mathcal{J}$.

Corollary 4.10 *Let R be a completely primary finite ring with maximal ideal $\mathcal{J}$. Then, $\mathcal{J} = pR_o \oplus \sum_{\tau \in Aut R_o}^{\oplus} \mathcal{J}_\tau$ as $R_o -$ modules.*

Acknowledgements: The author is grateful for the support he received from the Centre for Applied Research in Mathematical Sciences (CARMS), Strathmore University, Nairobi, Kenya; the Botswana College of Agriculture (BCA), Gaborone, Botswana; and for the invitation and kind hospitality from the Strathmore University International Mathematics Research Meeting Organizing Committee.

References

[1] **Y. A. Al-Khamees**, *Finite completely primary rings*, Ph.D thesis, University of Reading (1977).

[2] **G. L. C. Bond**, *On the automorphism groups of finite completely primary rings*, Ph.D thesis, University of Reading (1978).

[3] **C. J. Chikunji**, *On a class of finite rings*, Comm. Algebra, **27**(1999), 5049-5081.

[4] **C. J. Chikunji**, *A classification of cube radical zero completely primary finite rings*, Demonstratio Math., **XXXVIII**(2005), 7-20.

[5] **W. E. Clark**, *A coefficient ring for finite non-commutative rings*, Proc. Amer. Math. Soc. **33**(1972), 25-28.

[6] **W. E. Clark & D. A. Drake**, *Finite chain rings*, Abhandlungen, Math. Sem. Uni. Hamburg **39**(1973), 147-153.

[7] **W. E. Clark & J. J. Liang**, *Enumeration of finite commutative chain rings*, J. Algebra **27**(1973), 445-453.

[8] **B. Corbas**, *Rings with few zero divisors*, Math. Ann. **181**(1969), 1-7.

[9] **B. Corbas**, *Finite rings in which the product of any two zero divisors is zero*, Arch. Math. **XXI**(1970), 466-469.

[10] **N. Ganesan**, *Properties of rings with a finite number of zero divisors*, Math. Ann. **157**(1964), 215-218.

[11] **N. Ganesan**, *Properties of rings with a finite number of zero divisors II*, Math. Ann. **161**(1965), 241-246.

[12] **D. Gorenstein, R.Lyons, & R. Solomon**, The Classification of the Finite Simple Groups, Math. Surveys and Monographs, Vol. 40, No.1 (1994).

[13] **N. Jacobson**, Structure of rings, Amer. Math. Soc. Colloq. publ. (1943).

[14] **A. V. Jategaonkar**, Left principal ideal rings, Springer (1970).

[15] **K. Koh**, *On properties of rings with a finite number of zero divisors*, Math. Ann. **171**(1967), 79-80.

[16] **W. Krull**, *Algebraisce theorie der ringe II*, Math. Ann. **91**(1924), 1-46.

[17] **R. B. McDonald**, Finite rings with identity, Pure and Applied Math. **28**, Marcel Dekker, New York, (1973).

[18] **R. Raghavendran**, *Finite associative rings*, Compositio Math. **21**(1969), 195-229.

[19] **R. S. Wilson**, *On the structure of finite rings*, Compositio Math. Vol**26**(1973), 79-93.

[20] **R. S. Wilson**, *On the structure of finite rings II*, Pacific J. Math. **51**(1974), 317-325.

[21] **R. S. Wilson**, *Representations of finite rings*, Pacific J. Math. **51**(1974), 643-649.

[22] **B. R. Wirt**, Finite non-commutative rings, Ph.D. Thesis. University of Oklahoma (1972).