# AUTOMORPHISMS OF THE UNIT GROUPS OF SQUARE RADICAL ZERO, CUBE RADICAL ZERO AND POWER FOUR RADICAL ZERO FINITE COMMUTATIVE COMPLETELY PRIMARY RINGS

BY

MICHAEL ONYANGO OJIEMA

A THESIS SUBMITTED IN FULFILMENT OF THE REQUIREMENTS
FOR THE DEGREE OF
DOCTOR OF PHILOSOPHY IN PURE MATHEMATICS

SCHOOL OF MATHEMATICS, STATISTICS AND ACTUARIAL SCIENCE

MASENO UNIVERSITY

## DECLARATION

This thesis is my own work and has not been presented for a degree award in any other institution.

Signature:........................................Date.............................

Michael Onyango Ojiema

PHD/MAT/00062/2014.

This thesis has been submitted for examination with our approval as the university supervisors.

Signature:........................................Date.............................

Dr. Maurice Owino Oduor, Supervisor

Signature:........................................Date.............................

Prof. Paul Odhiambo Oleche, Supervisor.

Maseno University

2016

## ACKNOWLEDGEMENTS

I would like to express my sincere gratitude to: Masinde Muliro University of Science and Technology for their financial support and for granting me a study leave to pursue this graduate study. The National Commission for Science, Technology and Innovation (NACOSTI), for funding my research. My supervisors: Dr. Maurice Owino who encouraged me to attempt this study. He has proved to be a mentor, teacher, supervisor and friend. He has been a core figure in my mathematical development as well as the central resource for this thesis. Through his suggestions and invaluable guidance, I was able to draft this document. I am highly indebted to Prof. Paul Oleche for his constant availability and accessibility. I highly appreciate his patience, suggestions and criticisms. Special thanks to Prof. Fortuné Massamba of the University of Kwazulu Natal South Africa. He provided homage for me, encouraged me and allowed me to pursue my dream. To my family, you are the building blocks of this success. My spouse Brenda, thank you so much for your endurance, presence and support. You played the roles of both a father and a mother many times I was out of the country, in the course of this research. To our sons Garvin and Brighton, you are the true soldiers of my heart. To my father and mother, your prayers, struggles and support in the way you imagined as though small, propelled me to this big dream. May God grant you much more years. I would like to extend my gratitude to my colleagues in the Department of mathematics, Masinde Muliro University of Science and Technology. In particular, I would like to heartily thank Dr. Lawi George for his encouragements and direction. He built a dyke around my life. Special thanks to Keli Robert for being a true brother and teacher. He prepared lunch on several occasions for both of us at Pietermaritzburg. Much thanks to Dr. Everlyne Akoth for being my classmate true sister and friend. We have had common energies and veracity towards this course. Finally to the Almighty God, thank you for revealing to me these fascinating mathematical insights.

## DEDICATION

To my beloved spouse Brenda, our sons Garvin Brayden and Ryan Brightone. They are the driving force that propelled my hard work and success.

To my parents Pius Ojiema and Margret Ojiema for their relentless prayers. They believed in me throughout my academic journey .

## ABSTRACT

The study of automorphisms of algebraic structures has contributed immensely to many important findings in mathematics. For example, Galois characterized the general degree five single variable polynomials $f$ over $\mathbb{Q}$, by showing that the roots of such polynomials cannot be expressed in terms of radicals, through the automorphism groups of the splitting field of $f$. On the other hand, the symmetries of any algebraic structure are captured by their automorphism groups. The study of completely primary finite rings has shown their fundamental importance in the structure theory of finite rings with identity. Quite reasonable research has been done towards characterization of the unit groups, $R^*$ of certain classes of finite commutative completely primary rings. Much less known however, is whether there is a complete description of $R^*$, up to isomorphism. The existing literature is still scanty on the characterization of $Aut(R^*)$, the automorphism groups of the unit groups of these classes of rings. Therefore, in this thesis, we have characterized the structures and orders of the automorphisms of the unit groups of three classes of commutative completely primary finite rings, that is, Square radical zero, Cube radical zero and power Four radical zero finite commutative completely primary rings. The unit groups of the classes of rings studied are expressible as $R^* \cong \mathbb{Z}_{p^r-1} \times (1+J)$ such that, $\mathbb{Z}_{p^r-1}$ and $(1+J)$ are of relatively prime orders, where $(1+J)$ is a normal subgroup of $R^*$ and $J$ is the Jacobson radical of $R$. We have expressed the structures of $Aut(R^*)$ as direct products of $(\mathbb{Z}_{p^r-1})^*$ and $GL_{rk(1+J)}(\mathbb{F}_p)$. We have made use of the invertible matrix approach, the properties of diagonal matrices and determinants to count the number of automorphisms of $(1+J)$. We have then adjoined the counted $Aut(1+J)$ to $\varphi((\mathbb{Z}_{p^r-1})^*)$, where $\varphi$ is the Euler's phi-function, in order to completely characterize the order $Aut(R^*)$. Moreover, we have made use of the First Isomorphism Theorem to establish the relationship between $\mid GL_{rk(1+J)}(\mathbb{F}_p) \mid$ and $\mid SL_{rk(1+J)}(\mathbb{F}_p) \mid$. We noticed that our automorphisms yielded very unique structure and order formulae, distinct from the well known structures and order formulae of the automorphisms of the cyclic groups $C_n$. The results obtained in this thesis contribute significantly to the existing literature on the structure theory of finite rings with identity, thereby providing a much needed, accessible modern treatment and a complete characterization of these classes of rings up to isomorphism.

**TABLE OF CONTENTS**

## INDEX OF NOTATIONS

$[x, y]$ ..... The commutator of $x$ and $y$.

$G'$...... The commutator subgroup of $G$.

$G' = [G, G] = < [x, y]; x, y \in G >$ .

$Z(G)$ ..... The center of a group $G$.

$\varphi$ ..... Euler's phi-function/ totient function.

$\Phi(G)$ ..... Frattini subgroup of a group $G$.

$Aut(G)$ ..... The set of Automorphism group of $G$.

$Inn(G)$ ..... Inner Automorphism of $G$.

$Out(G)$ ..... The group of outer automorphisms of $G$.

$C_n$ ..... The cyclic group of $n-$ elements.

$\mathbb{Z}_n$ ..... The cyclic group of integers modulo $n$.

$d(G)$.....Minimum cardinality of the generating set of $G$.

$GL(d, \mathbb{F}_p)$..... The General Linear Group of dimension $d$ over the finite field $\mathbb{F}_p$.

$\left( \begin{array}{c} n \\ k \end{array} \right)_q$.....Gaussian (q-binomial) coefficient.

$\mathcal{G}_n(q)$.....The Galois number. The total number of subspaces of an $\mathbb{F}_q$- vector space.

$\mid G \mid$.....Order of $G$.

$< x >$.....Cyclic group generated by $x$.

$Hom(G, H)$.....The set of group homomorphisms $G \mapsto H$.

$Syl_p(G)$.....The Sylow $p-$subgroup of $G$.

$S_n$..... The Symmetric group of degree $n$.

$H \wr W$.....The wreath product of $H$ and $W$ where $W < S_n$ and $H$ is any group.

$R$ .....A finite ring.

$R^*$..... A group of units of $R$.

$ann(I)$..... annihilator of $I$.

$R_0 = GR(p^{kr}, p^k)$..... Galois ring of order $p^{kr}$ and characteristic $p^k$.

$GF(p^r)$..... Galois field of order $p^r$.

$H \rtimes K$...... The semi direct product of $H$ by $K$.

$R/N$ .....$R$ mod $N$.

$char(R)$..... Characteristic of $R$.

$ker\ \phi$..... kernel of $\phi$.

$_0(X)$ ...... order of $X$.

$Sym(G)$..... Symmetric group of $G$.

$J$..... The Jacobson radical of $R$.

$\mid R \mid$ ..... The order of $R$.

$R_p$..... The set of matrices of endomorphisms.

$E_p$...... The endomorphism ring.

$C_{p^r}^n$..... The Homocyclic abelian $p-$group.

$Q_8$..... The quaternion group

$Sp(2n, \mathbb{F}_p)$..... Symplectic group of dimension $2n$ whose entries are drawn from a field of order $p$.

$C_G(H)$...... The centralizer of $H$ over $G$.

$M(Q)$..... The Schur's multiplier.

$H^2(G)$...... The second cohomology group.

$(a, b)$..... The gcd of $a$ and $b$

$rk(1 + J)$..... The rank of $1 + J$

$M_n(\mathbb{Z}_p)$..... $n \times n$ matrix with integers mod $p$ entries.

$id_{R_o}$..... The identity element in $R_o$

$p \mid a$...... $p$ divides $a$.

$dim_{R_0}U$...... The dimension of $U$ in $R_0$.

# CHAPTER 1

# INTRODUCTION

## 1.1 Background information

Automorphisms of algebraic structures has been an active area of research for a quite a long time now. For instance, enormous number of papers have been devoted to studying the automorphisms of associative rings (cf. in [21, 29, 60, 86] ). This has been evident for quite some time, the central aim of these studies being, finding out and investigating those ring properties that are preserved under a transformation to a fixed ring and under the fixed ring to the initial ring (cf [13]). The methods which emerged in these studies proved their value for investigating arbitrary automorphisms of groups, rings and derivations basically from the point of view of their algebraic dependencies. They proved so effective that they made it possible to prove the Galois correspondence theorems in the class of semi prime rings both for the automorphism groups and for Lie Algebras of derivations.

Galois theory deals with the action of a finite group of automorphisms on a field. The power and usefulness of the theory is great, and therefore, for a long time there has been a noticeable interest in more general Galois theory. This has turned out to be a long and involved quest. The theory has also led to the modern theory of automorphisms and derivations of associative rings and algebras. To a greater extent, many technical and conceptual advances were needed to bring Galois theory to its present rich state. A few expositions worth mentioning are essentially given by Kharchenko in [61] concerning rings with generalized identities, non-standard algebras and the powerful logic algebraic meta-theorem.

The automorphism group of $R^*$ denoted as $Aut(R^*)$ is a set whose elements are automorphisms $\sigma : R^* \to R^*$ and where the group operation is composition of automorphisms. Thus, its group structure is obtained as a subgroup of the $Sym(R^*)$, the group of all permutations on $R^*$. Given an arbitrary finite group $G$, the computation of its automorphism group $Aut(G)$ is not a very easy task. Pioneer work in this regard was carried out by Felsch and Neubuser [36, 37] who developed an algorithm which made use of their subgroup lattice program. In the early 1970s, Neubuser independently developed a technique to determine the automorphism groups by considering its action on the union of certain conjugacy classes of $G$. Similar methods were used by Hulpke [5], Cannon and Holt [57] who presented a new algorithm to answer this problem.

A few efficient approaches to determine the automorphism groups of the groups satisfying certain properties are available. Following the work of Shoda [87], Hulpke in 1997 implemented a practical method for finite abelian groups. Wursthorn [71] adapted modular group algebra techniques to compute the automorphism group of a $p-$group. Smith [75] introduced for finite soluble groups. The $p-$group generation algorithm of Newman [80] and O'Brien [84] can be modified to compute the automorphism group of a finite $p-$group as outlined in [85]. The algorithm proceeds by induction down the lower exponent-$p-$central series of a given $p-$group $P$; that is, it successively computes $Aut(P_i)$ for the quotients $P_i = P/(\mathcal{P}_i(P))$ where $(\mathcal{P}_i(P))$ is the descending sequence of subgroups defined recursively by $(\mathcal{P}_1(P)) = P$ and $(\mathcal{P}_{i+1}(P)) = [(\mathcal{P}_i(P)), P](\mathcal{P}_i(P))^p$ for $i \geq 1$. The exponent-$p$ class of $P$ is the length of its lower exponent-$p$ central series.

Despite these fruitful and numerous attempts to develop algorithms that compute the automorphism groups of finite groups, no success has been achieved in developing a universal algorithm that computes these automorphisms for all the various types of groups. The researchers have so far concentrated in developing algorithms for specific types of groups. Similarly, these algorithms are simply used in counting the number of automorphisms, a given finite group satisfying certain properties has. As such is the case, characterization of groups of automorphisms is still an open problem.

The limitations encountered with the algorithms which are basically computer coded, have invigorated and shifted research towards order and structure formulae for automorphism groups. Menengazzo [72] has given a systematic account of the order and structure of the automorphism group of a finite non-abelian 2-generated $p-$groups with cyclic commutator subgroup. Special cases of the same problem have also been solved by Caranti and Scoppola [20], Miech [73], Davitt [33] and Cheng [22]. Bidwell, Curran and McCaughan [16] have shown that if $H$ and $K$ are groups with no common direct factors and $G = H \times K$, then the $Aut(G)$ can be expressed in terms of $Aut(H)$ and $Aut(K)$. Bidwell and Curran [15] have dealt with two complications not encountered in [16] by working with matrices $M_{n\times n}$, taking account of those automorphisms that permute the direct factors. They have also given automorphisms for semi-direct products of 2 cyclic $p-$groups.

Shoda [87] has characterized automorphisms of finite abelian groups by employing a matrix representation for the Sylow subgroups of an abelian group $A$. A more elegant version of Bidwell, Curran and Shoda's formulae, where a much more involved argument is used has been given by Hillar and Rhea [48]. They gave a useful description of the automorphisms of an arbitrary abelian $p-$group by computing the size of this automorphism group. In spite of these numerous attempts and the existence of such elegant order formulae, the automorphisms of the unit groups $R^*$ of completely primary finite rings have not been characterized.

The study of completely primary finite rings has shown the fundamental importance of these rings in the structure theory of finite rings with identity. A finite ring has a unique maximal ideal if and only if it is a full matrix ring over a completely primary finite ring. Moreover, any finite commutative ring is a direct sum of completely primary ring. Further, any finite ring is a direct sum of rings of prime power order. This follows from the fact that when one decomposes the additive group of a finite ring into its prime power components, the components subgroups are ideals. Thus, because completely primary finite 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.

Given a completely primary finite ring $R$. Let $R_0$ be the Galois subring of $R$ and $J$ be its Jacobson radical which is the unique maximal ideal of $R$, then, several authors have constructed such finite rings whose Jacobson radical or group of units yield particular structures. For instance, in [26], Chikunji has obtained the structures of the unit groups of classes of completely primary finite rings in which the product of any three zero divisors is zero, Oduor, Ojiema and Mmasi [82] have obtained the structures of units of a class of completely primary finite rings in which the product of any two zero divisors is zero while in [83], we characterized the unit groups of some classes of power four radical zero completely primary finite rings. It is well known that if $R$ is a finite field, then its group of units is cyclic. In [41], Gilmer has characterized some classes of finite rings whose groups of units are cyclic.

Suppose $R$ is a ring and $R^*$ is its multiplicative group of units, then, all such local rings with cyclic groups of units were determined by Ayoub [10] and the same case was also considered by Gilmer [41]. Gilmer showed that it is sufficient to consider finite primary rings. Ayoub [10] restricted attention to finite primary rings and showed some connections between the additive group $N$, the radical of the ring $R$ and the multiplicative group $1 + N$. Clark [21] investigated $R^*$ where the ideals form a chain and has shown that if $p \geq 3, n \geq 2$ and $r \geq 2$ then the units of the Galois ring $GR(p^{nr}, p^n)$ are a direct sum of cyclic groups of order $p^r - 1$ and $r$ cyclic groups of order $p^n - 1$ (This was also done independently by Raghavandran in [86]. Much less known however, is whether there is a complete description of $Aut(R^*)$, the automorphism groups of the unit groups of commutative completely primary finite rings.

In this thesis we have discovered the structures and orders of $Aut(R^*)$, the automorphisms of the unit groups of three classes of commutative completely primary finite rings, namely; Square Radical Zero, Cube Radical Zero and Power Four Radical Zero finite commutative completely primary rings. Since $R$ is of order $p^{nr}$, $n, r \in \mathbb{Z}$ and $R^* = R - J$, the order of $R^*$, that is $\mid R^* \mid= p^{(n-1)r}(p^r - 1)$ and $\mid 1 + J \mid= p^{(n-1)r}$, so that $1 + J$ is an abelian $p-$group. In [48], Hillar and Rhea gave a useful description of the automorphism groups of an arbitrary abelian $p-$group and they computed the size of this automorphism group. We extend their work by characterizing $Aut(R^*)$ in a general setting.

## 1.2 Basic Concepts

In this section, we give basic terminologies, definitions, and results that are useful in this study.

**Definition 1.2.1.** *(i) A mapping $\theta$ of a group $G$ onto a group $G'$ is called a* **homomorphism** *if $\theta(xy) = \theta(x)\theta(y)$, $G'$ being a homomorphic image of $G$.*

*(ii)A homomorphism $\theta : G \to G$ is called an* **endomorphism**. *If the homomorphism defined is $1-1$, then it is called an* **isomorphism**.

*(iii) An isomorphism $\theta : G \to G$ is called an* **automorphism**.

**Definition 1.2.2.** *Let $\theta_x : G \to G$, then, $\theta_x(y) = xyx^{-1} \in G$ is called conjugation map. An automorphism of $G$ that corresponds to conjugation by some $x \in G$ is called an* **inner automorphism** *denoted by $Inn(G)$. Any automorphism that is not inner, that is, $Aut(G)/Inn(G)$ is called outer automorphism.*

**Proposition 1.2.1.** *The set $Inn(G)$ of inner automorphisms of an arbitrary group $G$ is an invariant subgroup of the group of automorphisms and $Inn(G) \cong G/C$ where $C$ is the center of the group*

**Definition 1.2.3.** *A homocyclic abelian group is a direct product of one or more pairwise isomorphic cyclic groups.*

**Definition 1.2.4.** *A completely primary finite ring is a ring $R$ with identity $1 \neq 0$ whose subset of all the zero divisors forms a unique maximal ideal $J$.*

**Definition 1.2.5.** *A unit in a unital ring $R$ refers to any element $u$ that has got an inverse element $v$ in the multiplicative monoid of $R$. It satisfies $uv = vu = 1_R$ where $1_R$ is the identity element in $R$. The set of units of any ring is closed under multiplication and forms an abelian group $R^*$ with respect to this operation.*

**Definition 1.2.6.** *The Jacobson radical $J$ of a ring $R$ is the intersection of all the maximal ideals of $R$. Since all maximal ideals are prime, the Nilradical is contained in the Jacobson radical.*

**Definition 1.2.7.** *Let $G$ be a group and $\Gamma(Aut(G))$ be a graph of automorphisms of $G$. Then, the proportions of $\Gamma(Aut(G))$ on $n$ vertices that tend to $1$ as $n$ tends to infinity are called $Z-$graphs.*

**Theorem 1.2.1.** *(cf. [82] ) If a ring $R$ has $n \geq 2$ zero divisors (including zero),then $R$ is a finite ring and $|R| \leq n^2$.*

**Theorem 1.2.2.** *Let $R$ be a finite ring with identity $1 \neq 0$. Then every nontrivial ideal of $R$ consists entirely of zero divisors.*

**Theorem 1.2.3.** *If $G$ is a cyclic group of order $n$, then $G \cong \mathbb{Z}_n$.*

**Theorem 1.2.4.** *(cf. [34]) Let $G$ be a finite abelian group. Then $G$ is isomorphic to a product of groups of the form:*

$$H_p = \mathbb{Z}/p^{e_1}\mathbb{Z} \times \mathbb{Z}/p^{e_2}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{e_n}\mathbb{Z},$$

*in which $p$ is a prime number and $1 \leq e_1 \leq \cdots \leq e_n$.*

## 1.3 Statement of the problem

The symmetries of a group are captured in its group of automorphisms. Given a completely primary finite ring $R$, with a Jacobson radical $J$, various researchers have presented characterizations of the unit groups, $R^*$ of certain classes of $R$. For instance, local rings with cyclic groups of units were determined by Ayoub [10] and the same case was also considered by Gilmer [41]. Gilmer showed that it is sufficient to consider finite primary rings. Ayoub [10] restricted attention to finite primary rings and showed some connections between the additive group $N$, the radical of the ring $R$ and the multiplicative group $1+N$. Clark [21] investigated $R^*$ where the ideals form a chain. This was also done independently by Raghavandran in [86]. Oduor, Ojiema and Mmasi [82] determined the units of completely primary finite rings of characteristic $p^n$. Chikunji [25] determined $R^*$ for the cube radical zero completely primary finite rings, while Oduor and Ojiema [83] determined $R^*$ for some classes of power four radical zero commutative completely primary finite rings. Much less known however, is whether there is a complete description of $Aut(R^*)$, the automorphism groups of the unit groups of commutative completely primary finite rings. The documented literature shows that, no attempts have been previously made to characterize $Aut(R^*)$ in terms of its structures and order. Since $R$ is of order $p^{nr}$, $n, r \in \mathbb{Z}$ and $R^* = R - J$, and $R^* \cong < b > \times(1 + J)$, then, $\mid R^* \mid= p^{(n-1)r}(p^r - 1)$ and $\mid 1+J \mid= p^{(n-1)r}$, so that $1+J$ is an abelian $p-$group. We therefore characterize $Aut(R^*)$, where $R$ is either square radical zero, cube radical zero or power four radical zero.

## 1.4 Objective of the study

### 1.4.1 General objective

To characterize the automorphism groups of the unit groups of square radical zero, cube radical zero and power four radical zero commutative completely primary finite rings.

### 1.4.2 Specific objectives

(1) To characterize the automorphisms of the unit groups of square radical zero commutative completely primary finite rings .

(2) To characterize the automorphism groups of the unit groups of cube radical zero commutative completely primary finite rings.

(3) To characterize the automorphism groups of the unit groups of power four radical zero commutative completely primary finite rings.

## 1.5 Methodology

The following methods of study have been used in this thesis:

(1) The method of idealization of $R_o-$module has been used in identification and classification of completely primary finite rings of interest based on their constructions.

(2) We counted the number of invertible $M_2(\mathbb{Z}_p) \in GL_{rk(1+J)}(\mathbb{F}_p)$ by inspection and found it to be a tedious exercise. We therefore used the invertible matrix approach, the properties of diagonal matrices and general properties of determinants to count and generalize the number of automorphisms of $1 + J$.

(3) We employed the First Isomorphism Theorem in establishing the relationship between $\mid GL_{rk(1+J)}(\mathbb{F}_p) \mid$ and $\mid SL_{rk(1+J)}(\mathbb{F}_p) \mid$ .

## 1.6 Significance of the study

A successful characterization of automorphisms of the unit groups of these classes of commutative completely primary finite rings provide a better understanding of the groups, thereby providing a much needed, accessible modern treatment of finite rings with identity. The results obtained in the thesis mark an important step in the structure theory of finite rings with identity. This is a significant contribution of knowledge towards the pursuit of the classification of finite rings.

## 1.7 Structure of the thesis

The thesis has been presented in this fashion: In Chapter Two, we have given detailed literature review on the automorphism groups of finite groups and rings that have been studied by different researchers. In Chapter Three, we have given detailed account of the unit groups of the various classes of the finite rings studied and characterized their automorphisms in the respective sections. In Chapter Four, we have given summary of our results, conclusion and provided a raft of recommendations.

# CHAPTER 2

# LITERATURE REVIEW

## 2.1 Introduction

In this chapter, we give detailed literature and related studies concerning finite rings and their representations, a survey on the theory of automorphisms, detailing the automorphisms of $p-$groups, direct products and finite rings.

## 2.2 Representations of Rings and Morphisms

A representation of a ring $R$ is a ring homomorphism $R \to End_{\mathbb{Z}}(M)$, where $M$ is an abelian group. The theory of ring representation has been considered by various researchers to be of great interest in many facets of mathematics. For instance, the theory of sectional representation of rings which has its origin, both in the characterizations of rings of functions of various kinds occurring in analysis and geometry, and in the structure theorem of algebra which expresses certain rings in terms of direct and sub-direct product of other rings is a development that has the link between representations of rings and applications of intuitionistic mathematics, which has led to the introduction of different techniques for determining representations and a settling of its foundation in the topological algebra.

Wilson [92], studied the representation of finite rings by extending the concept of Szele's representation of finite rings from the case where the coefficient ring is cyclic to the case where the coefficient ring is Galois. Accordingly, he characterized completely primary finite rings and nilpotent rings as those rings whose Szele's representations satisfy the same conditions. Of the two classes of finite rings studied, completely primary finite rings are always of prime power order therefore, there is no loss of generality up to direct sum formation. Finite commutative rings can be represented in a number of ways. Among them given by Agrawal [3] are the following:

(i) **Table Representation**; This is the simplest representation. It involves listing all the elements of the ring and their addition and multiplication tables. This representation has size $n = \mathbf{o}(|R|^2)$. It is a highly redundant representation and the problem of finding automorphisms can be solved in $n^{\mathbf{o}(\log n)}$ times since any minimal set of generators for the additive group has size $\mathbf{o}(\log n)$.

(ii) **Basis Representation**; It is specified by a set of generators of the additive group $R$. Let $CharR = n$, then, the additive group $(R, +)$ can be expressed as the direct sum $\oplus_{i=1}^{m} \mathbb{Z}_{n_i} b_i$ where $b_1, ..., b_m$ are elements of $R$ and $n_i | n$ for each $i$. The elements $b_i$ are called basis elements for $(R, +)$ therefore, the ring $R$ can be expressed as $(n_1, ..., n_m A_1, ..., A_m)$ where the matrix $A_i = (a_{i,j,k})$ describes the effect of multiplication on $b_i$ viz; $b_i.b_i = \sum_{k=1}^{m} a_{i,j,k}.b_k, a_{i,j,k} \in \mathbb{Z}_{nk}$. The size of this representation is $\mathbf{o}(m^3)$. This in general is exponentially smaller than the size of the ring $|R| = \prod_{i=1}^{m} n_i$. The problem of finding automorphism or isomorphism becomes harder for this representation. As shown in [4], these problems belong to a complexity class and can be as complicated as factoring integers.

(iii) **Polynomial Representation**; A third and even more compact representation of $R$ is obtained by starting with the basis representation and then selecting the smallest sets of $b_i$s, that is, $b_1, ..., b_m$. The representation can be specified by $m$ basis elements and generators of the ideal of polynomials satisfied by these. Each polynomial is represented by an arithmetic circuit. Such a ring can be written as

$$R = \mathbb{Z}_n[x_1, ..., x_m]/f_1(x_1, ..., x_m), ..., f_k(x_1, ..., x_m),$$

where $x_1, ..., x_m$ are basis elements and $f_1(x_1, ..., x_m), ..., f_k(x_1, ..., x_m)$ is the ideal generated by the polynomial $f_1, ..., f_k$ describing all polynomials satisfied by $x_1, ..., x_m$. More often, this representation is succinct than the previous ones.

Suppose $f(x) \in \mathbb{Z}_{p^k}[x]$ is a monic polynomial of degree $r$ irreducible modulo $p$, then, it is well known (cf. [26]) that $\mathbb{Z}_{p^k}/(f(x))$ is the Galois ring of order $p^{kr}$ and characteristic

$p^k$ denoted as $R_0$ . Therefore, a Galois ring is an irreducible algebraic extension of degree $r$ of the ring $\mathbb{Z}/(p^k)$, and, any two irreducible algebraic extensions of $\mathbb{Z}/(p^k)$ of degree $r$ are isomorphic. This class of ring was first studied by Krull [62] and later rediscovered by Raghavendran [86] and Janusz [56] among other researchers in subsequent studies. In deed, Raghavendran described the structure of the multiplicative group of every Galois ring. The importance of Galois rings is that if $R$ is a completely primary finite ring of characteristic $p^k$, with Jacobson radical $J$ such that $R/J \cong GF(p^k)$, then, $R$ contains a unique copy up-to inner isomorphism, of $GR(p^{kr}, p^r)$. Thus, a completely primary finite ring is a $GR(p^{kr}, p^r)$-bi-module whose structural theory was developed by Wilson [92].

### 2.3 A survey of the Theory of Automorphism Groups

#### 2.3.1 Automorphisms of $p$-groups with cyclic commutator subgroup

In [72], Menengazzo gave a systematic account of the automorphism groups of finite, non-abelian, 2-generated $p-$groups with cyclic commutator subgroup, for odd prime $p$. Special cases of this problem, have also been studied by Caranti, Miech, Davitt and Cheng in [20, 22, 33, 73] in connection with many questions, with the aim of providing examples and counterexamples. However, the general information available is still remarkably scarce. It was remarked by Cheng [22], that in such groups $G$, the central factor group $G/2(G)$ is metacyclic, hence modular. It therefore follows that $\mid G \mid$ divides $\mid Aut(G) \mid$.

Another known fact (cf. [72]) is that in any metabelian two-generated $p-$group $G =< a, b >$, for all choices of $x, y \in G^{'}$, there is an automorphism $\alpha$ mapping $a \mapsto ax$ and $b \mapsto by$. Moreover, if $G^{'}$ is cyclic and $p$ is odd, such automorphisms are inner. This implies that $\mid Inn(G) \mid= (\mid G^{'} \mid)^2$. The automorphism of $G$ naturally induces a group of linear transformations of the $\mathbb{Z}/p\mathbb{Z}-$vector space $G/\Phi(G)$, where $\Phi(G)$ is the Frattini subgroup which is $GL(2, \mathbb{Z}/p\mathbb{Z})$ denoted in [72] by $Aut_l(G)$, such that $l$ is the reminder of linearity. The kernel of this action; i.e; $\{\alpha \in G | g^{\alpha}\Phi(G) = \Phi(G), \forall g \in G\}$ is sometimes denoted as $Aut^{\Phi}(G)$; for every $p-$group $Inn(G) \leq Aut^{\Phi}(G) \leq O_pAut(G)$, where $O_pAut(G)$ is the outer automorphism.

A finite $p-$group $G$ is called *metacyclic* where $p$ is a prime, if the presentation of $G$ can be written as, $G =< x, y \mid x^{p^m} = 1, y^{p^t} = x^{p^q}, yxy^{-1} = x^{1+p^n} >$ where the parameters $m, t, q, n$ satisfy the conditions in [16]. Menengazzo gave the following results:

**Lemma 2.3.1.** *(cf. [72]) Let $G =< a, b >$ be a metacyclic group. Suppose $G$ has a cyclic normal subgroup $N =< b >$ of order $p^m$, say with cyclic factor group $G/N =< aN >$ of order $p^l$, then, there exists an automorphism mapping $a \mapsto \overline{a}$ and $b \mapsto \overline{b}$ if and only if $a$ is of order $p^l$ and $\overline{b}^{\overline{a}} = \overline{b^a}$.*

**Theorem 2.3.1.** *(cf. [72]) Let $G =< a, b \mid a^{p^l} = b^{p^m} = 1, b^a = b^{1+p^s} >$ where $1 \leq s \leq m$ and $m - s \leq l$. The effect of $Aut(G)$ on the generators $a, b$ is*

$$\begin{cases} b \mapsto a^z b^w, \\ a \mapsto a a^{\lambda p^{m-s}} (a^z b^w)^{\mu}, \end{cases}$$

*where $zp^s \equiv 0(p^l)$, $w \not\equiv 0(p)$, $\mu^{p^l} \equiv 0(p^m)$.*

*(i) If $l \geq m$*

$$\begin{cases} \mid Aut(G) \mid = (p-1)p^{l+m+2s-1}, \\ \mid Inn(G) \mid = p^{2(m-s)}, \\ \mid O_p(Aut(G)) \mid = p^{l+m+2s-1}, \\ \mid Aut_l(G) \mid = p(p-1). \end{cases}$$

*(ii) If $m > l > s$*

$$\begin{cases} \mid Aut(G) \mid = (p-1)p^{2l+2s-1}, \\ \mid Inn(G) \mid = p^{2(m-s)}, \\ \mid O_p(Aut(G)) \mid = p^{2l+2s-1}, \\ \mid Aut_l(G) \mid = (p-1). \end{cases}$$

*(iii) If $s \geq l$*

$$\begin{cases} \mid Aut(G) \mid = (p-1)p^{3l+s-1}, \\ \mid Inn(G) \mid = p^{2(m-s)}, \\ \mid O_p(Aut(G)) \mid = p^{3l+s-1}, \\ \mid Aut_l(G) \mid = p(p-1). \end{cases}$$

As a consequence of the Lemma (2.3.1) and theorem (2.3.1) above, one clearly sees that the order and presentation for the automorphism group of a finite non-abelian split metacyclic $p-$group for odd prime $p$ can be found in [72]. Similarly, an extension of the same problem was considered by Bidwell and Curran [15]. They showed that if $G = H \rtimes K$ is a semi-direct product of two cyclic $p-$groups $H$ and $K$, $Aut(G)$ has cyclic subgroups $A \approx Aut(H)$, $B \approx \times Hom(K, H)$, the crossed homomorphism from $K$ to $H$, $C \approx Hom(H/[H, K], K)$, $D \approx \{\delta \in Aut(K); k^{-1}\delta(k) \in C_k(H)\ \forall k \in K\}$ such that $Aut(G) = ABCD$ where $AD = A \times D$ normalizes $B$ and $C$. Particularly, in [15], the case when the prime $p = 2$, has been examined, that is, they considered the automorphism groups of any finite split metacyclic $2-$group. Although a few of these automorphisms existed in ad hoc way, Bidwell and Curran [15] gave a unified approach to all such groups. Moreover, the method used in [72] where $p$ is odd does not exploit the regularity of $p-$groups, therefore, similar approaches have been employed in [15]. However, there are more cases considered and extra subtleties when the prime is 2. Nevertheless, the structure of $Aut(G) = ABCD$ where $A, B, C, D$ are the same subgroups as identified in [72], for $p-$odd prime. For example, Bidwell and Curran[15] considered a group $G = H \rtimes K$, a semi direct product of $H$ and $K$. That is $H \trianglelefteq G$, $K \leq G$, $H \cap K = 1$, and $\forall\ h_1, h_2 \in H$ and $k_1, k_2 \in K$, $h_1k_1h_2k_2 = h_1h_2^{k_1}k_1k_2$ where $h^k = khk^{-1}$. As in [72], Biddwel and Curran [15] associated with $\theta \in Aut(G)$ a $2 \times 2$ matrix of maps. That is;

**Lemma 2.3.2.** *(cf. [15]) Let $G = H \rtimes K$ be a semi direct product where $K$ is abelian and let*

$$M = \left\{ \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} : \begin{pmatrix} \alpha \in Map(H, H) & \beta \in Map(K, H) \\ \gamma \in Hom(H, K) & \delta \in Hom(K, K) \end{pmatrix} \right\}$$

*where $\alpha, \beta, \gamma, \delta$ satisfy the following properties:*

*(i) $\forall\ h, h' \in H, \alpha(hh') = \alpha(h)\alpha(h')^{\gamma(h)}$,*

*(ii)$\forall\ k, k' \in K, \beta(k, k') = \beta(k)\beta(k')^{\delta(k)}$,*

*(iii)$[H, k] \leq ker\ \gamma$ ,so, $\gamma \in Hom(H/[H, K], K)$,*

*(iv) $\forall\ h \in H, \forall k \in K, \alpha(h^k)\beta(k)^{\gamma(h)} = \beta(k)\alpha(h)^{\delta(k)}$,*

*(v) For any $h', k' \in G$, there exists unique $h, k \in G$ such that $\alpha(h)\beta(k)^{\delta(h)} = h', \gamma(h)\delta(k) = k'$.*

*Then, there is a one-one correspondence between* $Aut(G)$ *and* $M$ *given by* $\theta \leftrightarrow \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ *where* $\theta(h) = \alpha(h)\gamma(h)$ *and* $\theta(k) = \beta(k)\delta(k)$*. Further, if* $\theta' \leftrightarrow \begin{pmatrix} \alpha' & \beta' \\ \gamma' & \delta' \end{pmatrix}$*, then*

$$\theta'\theta \leftrightarrow \begin{pmatrix} \alpha'\alpha + \beta'\gamma^{\gamma'\alpha} & \alpha'\beta + \beta'\delta^{\gamma'\beta} \\ \gamma'\alpha + \delta'\gamma & \gamma'\beta + \delta'\delta \end{pmatrix}$$

Despite the complications for the prime 2, the order of $Aut(G)$ remains the same as taking $p = 2$ in the analogous odd prime case. Bidwell and Curran therefore easily specified the order of $Aut(G)$ for $2-$groups:

**Theorem 2.3.2.** *[16] Let* $G = H \rtimes K =< x, y : x^{2m} = y^{2n} = 1, x^y = x^{1+2^{m-r}} >$ *where* $m \geq 3, n \geq 1$ *and* $1 \leq r \leq min\{m-2, n\}$*. Then* $\mid Aut(G) \mid = 2^{m-1+min\{m,n\}+min\{m-r,n\}+n-r}$. *In particular,* $Aut(G)$ *is a* $2-$*group and its order in the three cases are ; (i.)* $2^{3m+n-2r-1}$, *(ii.)* $2^{m+3n-r-1}$, *(iii.)* $2^{2(m+n-r)-1}$.

### 2.3.2 Automorphisms of direct products of finite groups

Fitting [38] noted that if $\theta, \phi \in Hom(G, H)$, the maps $\theta + \phi : G \to H$ defined by $(\theta + \phi)g = \theta(g)\phi(g)$ is again a homomorphism if and only if $Im(\theta)$ and $Im(\phi)$ commute. Bidwell, Curran and McCaughan [16], showed that if $H$ and $K$ are groups with no common direct factors and $G = H \times K$, then, the structure and order of $Aut(G)$ can simply be expressed in terms of $Aut(H)$ and $Aut(K)$ and the central homomorphism groups $Hom(H, Z(K))$ and $Hom((K), Z(H))$. Thus we have:

**Theorem 2.3.3.** *(cf. [38]) If* $G$ *is any group and* $\phi \in End(G)$*, there is a positive integer* $r$ *such that* $Ker(\phi^r) = Ker(\phi^{r+n})$*, for every positive integer* $n$*. Further if* $\sigma = \phi^r$ *and* $Im(\sigma) \lhd G$*, then* $G \cong Ker(\sigma) \times Im(\sigma)$.

Now if

$$M = \left\{ \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} : \begin{pmatrix} \alpha \in End(H) & \beta \in Hom(K, H) : [Im(\alpha), Im(\beta)] = 1 \\ \gamma \in Hom(H, K) & \delta \in End(K) : [Im(\gamma), Im(\delta)] = 1 \end{pmatrix} \right\},$$

because of the commuting properties of the images of the given maps, one can verify that

$M$ is a monoid under matrix multiplication

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}\begin{pmatrix} \alpha' & \beta' \\ \gamma' & \delta' \end{pmatrix} = \begin{pmatrix} \alpha\alpha' + \beta\gamma' & \alpha\beta' + \beta\delta' \\ \gamma\alpha' + \delta\gamma' & \gamma\beta' + \delta\delta' \end{pmatrix}$$

and the following monoid isomorphism follows:

**Theorem 2.3.4.** *[16] If $G = H \times K$, then $End(G) \cong M$ where $M$ is the matrix of endomorphism given above,*

Therefore, by the above theorem, it is possible to find the order formulae for the full automorphism groups of the direct product $G = H \times K$ in the case where $H$ and $K$ have no common direct factors in terms of the endomorphism rings. One such a formula is given by Biswell, Curran and McCaughan [16] as follows:

**Theorem 2.3.5.** *(cf. [16]) Let $G = H \times K$ where $H$ and $K$ have no common direct factors. Then $AutG \cong A \subseteq M$. In particular,*

$$\mid Aut(G) \mid = \mid Aut(H) \mid\mid Aut(K) \mid\mid Hom(H, Z(K)) \mid\mid Hom(K, Z(H)) \mid .$$

Similar descriptions of the order of $Aut(G)$ can be found in [15]. Here, $G = H^n; n > 1$ is the direct product of $n-$copies of an indecomposable non-abelian group $H$. The case $n = 2$ arises by setting $K = H$ for the groups studied in [16]. In this case, $Aut(G)$ is an extension of $A$ in the above by $C_2-$the surplus due to the new automorphisms which swaps the two direct factors.

For a general $n$, Bidwell and Curran [15] dealt with two complications not encountered in [16] by working with $n \times n$ matrices and taking account of those automorphisms which permute the direct factors. In this regard, their main result showed that $Aut(G)$ is a semi direct product of a matrix group similar to the $2 \times 2$ case, by the symmetric group $S_n$ and $\mid Aut(G) \mid = \mid Aut(H) \mid^n \mid Hom(H, Z(H)) \mid^{n^2-n} n!$. Also, as an extension of the results of Menengazzo [72], the main result in [15] described the automorphism group of an arbitrary finite direct product $G = H_1^{\beta_1} \times \cdots \times H_n^{\beta_n}$ where the $H_i$ are all distinct and indecomposable and $\beta_i \geq 1, (1 \leq i \leq n)$. However, it is well known (cf. [87] ) that here, since $H_i$ is abelian and indecomposable (i.e, $H_i$ is a cyclic $p-$group, $p-$ prime) that $Aut(H^n) \cong GL(n, \mathbb{Z}_{p^r})$, where $H \cong \mathbb{Z}_{p^r}$ and $r$ is a positive integer. Therefore, the matrix of endomorphism rings given below is immediate;

**Lemma 2.3.3.** *Let $G = H_1 \times \cdots \times H_n$. Then, $End(G) \cong M$ where*

$$M = \begin{pmatrix} \alpha_{11} & \dots & \alpha_{1n} \\ \vdots & \ddots & \vdots \\ \alpha_{n1} & \dots & \alpha_{nn} \end{pmatrix} : \alpha_{ij} \in Hom(H_j, H_i), [Im(\alpha_{ij_1}), Im(\alpha_{ij_2})] = 1 \forall\, i, j_1, j_2; j_1 \neq j_2$$

*and multiplication in $M$ is just the usual matrix multiplication, with addition of two homomorphisms $\alpha, \beta \in Hom(H_j, H_i)$ defined by $(\alpha+\beta)(x) = \alpha(x)\beta(x)$ and multiplication of $\alpha$ and $\gamma \in Hom(H_k, H_j)$ defined by the composition $\alpha\gamma$.*

We can deduce that, any finite group $G$ has a direct product decomposition of the form $G = A \times H_1^{\beta_1} \times \cdots \times H_n^{\beta_n}$ where $A$ is abelian, the $H_i (1 \leq i \leq 1)$ are distinct, indecomposable and non-abelian and $\beta_i$ are positive integers. A characterization of the automorphisms of finite abelian groups has been given by Shoda [87]. There, a similar matrix representation was employed for the automorphisms of the Sylow subgroups of an abelian group $A$, and it follows that $Aut(A)$ is a direct product of these. Using Shoda's results, it can be seen that $Aut(C_{p^r}^n) \cong GL(n, \mathbb{Z}_{p^r})$, where $C_{p^r}^n$ is the homocyclic abelian $p-$group. The order of this group is however well known as it has been described by Han [45].

**Lemma 2.3.4.** *([45]) Let $n$ and $r$ be integers and $p$ a prime. Then*

$$\mid GL(n, \mathbb{Z}_{p^r}) \mid = p^{n^2(r-1)} \prod_{i=1}^{n} (p^n - p^{n-i}).$$

The description above is similar to the one given by Bidwell and Curran [15] in the following theorem;

**Theorem 2.3.6.** *([15]) Let $A = A_1^{\gamma_1} \times \cdots \times A_m^{\gamma_m}$ where $A_i \cong \mathbb{Z}_{p_i}^{r_i}$ $1 \leq i \leq m$ are distinct, $p_i$ prime and $r_i > 0$. Then*

$$\mid Aut(H) \mid = \prod_{i=1}^{m} \{ p_i^{\gamma_i^2 (r_i - 1)} \prod_{j=1}^{\gamma_i} (p_i^{\gamma_i} - p_i^{\gamma_i - j}) \} \prod_{i,j=1, i\neq j}^{m} \gcd(p_i^{r_i}, p_j^{r_j})^{\gamma_i \gamma_j}.$$

A more elegant version of these formulae can be seen in Hillar and Rhea [48], where a much more involved argument is used.

**Theorem 2.3.7.** *([48]) The Abelian group $H_p = \mathbb{Z}/p^{e_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{e_n}\mathbb{Z}$ has*

$$\mid Aut(H_p) \mid = \prod_{k=1}^{n}(p^{d_k} - p^{k-1}) \prod_{j=1}^{n}(p^{e_j})^{n-d_j} \prod_{i=1}^{n}(p^{e_i-1})^{n-c_i+1},$$

*where $d_k$ and $c_k$ are the maximum and minimum entries of the block upper triangular matrix of endomorphisms of $H$.*

### 2.3.3 The Automorphisms of some common $p-$Groups

There are several familiar families of finite $p-$groups for which, some information regarding their automorphism groups is well known. In particular, for a number of these families, the order of the automorphisms of these groups have been described in a reasonably extensive manner. We give a clear account of a couple of such descriptions;

A finite $p-$group $G$ is *special* if either $G$ is elementary abelian or $Z(G) = G^{'} = \Phi(G)$. Furthermore, a non-abelian special $p-$group $G$ is *extraspecial* if $Z(G) = G^{'} = \Phi(G) \cong C_p$. The order of an extraspecial $p-$group is always an odd power of $p$, and there are two isomorphism classes of extraspecial $p-$groups of order $p^{2n+1}$ for each prime $p$ and a positive integer $n$, as proved in Gorenstein [43]. When $p = 2$, both isomorphism classes have exponent 4. When $p$ is odd, one of these isomorphism classes has exponent $p$ and the other has exponent $p^2$.

Winter [93] gave a nearly complete description of the automorphism groups of an extraspecial $p-$group. Griess [44] stated many of these results without proof. Winter stated the following theorem on the automorphism groups of the extra-special $p-$groups for all primes $p$.

**Theorem 2.3.8.** *(cf.[93]) Let $G$ be an extraspecial $p-$group of order $p^{2n+1}$. Let $I = Inn(G)$ and let $H$ be the normal subgroup of $Aut(G)$ which acts trivially on $Z(G)$. Then,*

*(i)* $I \cong (C_p)^{2n}$.

*(ii) $Aut(G) \cong H \rtimes < \theta >$, where $\theta$ is an automorphism of order $p-1$.*

*(iii) If $p$ is odd and $G$ has exponent $p$, then, $H/I \cong Sp(2n, \mathbb{F}_p)$ and the order of $H/I$ is $p^{n^2}\prod_{i=1}^{n}(p^{2i}-1)$.*

*(iv) If $p$ is odd and $G$ has exponent $p^2$, then, $H/I \cong Q \rtimes Sp(2n-2, \mathbb{F}_p)$ where $Q$ is a normal extraspecial $p-$group of order $p^{2n-1}$, and the order of $H/I$ is $p^{n^2}\prod_{i=1}^{n-1}(p^{2i}-1)$. The group $(Q \rtimes Sp(2n-2, \mathbb{F}_p)$ is isomorphic to the subgroup $(Sp(2n, \mathbb{F}_p)$ consisting of elements whose matrix $(a_{ij})$ with respect to a fixed basis satisfies $a_{11} = 1$, $a_{1i} = 0$, for $i \leq 1$.*

*(v) If $p = 2$, and $G$ is isomorphic to the central product of $n-$copies of $D_8$, then, $H/I$ is isomorphic to the orthogonal group of order $(2^{n(n-1)+1})(2^n-1)\prod_{i=1}^{n-1}(p^{2i}-1)$ that preserves the quadratic form $\psi_1\psi_2 + \psi_3\psi_4 + \cdots + \psi_{2n-1}\psi_{2n}$ over $\mathbb{F}_2$.*

*(vi) If $p = 2$ and $G$ is isomorphic to the central product of $n-1$ copies of $D_8$ and one copy of $Q_8$, then $H/I$ is isomorphic to the orthogonal group of order $(2^{n(n-1)+1})(2^n+1)\prod_{i=1}^{n-1}(p^{2i}-1)$ that preserves the quadratic form $\psi_1\psi_2 + \psi_3\psi_4 + \cdots + \psi_{2n-1}^2 + \psi_{2n-1}\psi_{2n} + \psi_{2n}^2$ over $\mathbb{F}_2$.*

The set of automorphisms $\theta$ does not necessarily constitute a subgroup of $H$, and so, it is not obvious that $H$ splits over $I$. Winter did not address this issue. However, as Griess proved in [44], when $p = 2$, $H$ splits if $n \leq 2$ and does not split if $n \geq 3$. Griess also stated, but did not prove, that when $p$ is odd, $H$ always splits over $I$. This observation can also be made in, and can be deduced from Isaacs [53, 54] and Glasby and Howlett [42].

The automorphism groups of Sylow $p-$subgroups of the symmetric group for $p > 2$ were examined independently by Bondarchuk [17] and Lentoudis [65, 66, 67]. Their results are reasonably technical and apparently non-conclusive. They showed that the order of the automorphism group of the Sylow $p-$subgroup of $S_{p^m}$ is

$$(p-1)^m p^{n(m)},$$

where

$$n(m) = p^{m-1} + p^{m-2} + \cdots + p^2 + \frac{1}{2}(m^2 - m + 2)p - 1.$$

Note that the Sylow $p-$subgroup of $S_{p^m}$ is isomorphic to the $m-$fold iterated wreath product of $C_p$.

A $p-$group of order $p^n$ is of *maximal class* if it has nilpotence class $n-1$. Many examples can be found in [64], with the most familiar being the dihedral and the quaternion groups of order $2^n$ when $n > 4$. It is not too cumbersome to prove some basic results about the automorphism group of an arbitrary $p-$ group of maximal class. The presentation below follows Baartmans and Woeppel [11].

**Theorem 2.3.9.** *(cf. [11]) Let $G$ be a $p-$group of maximal class of order $p^n$, where $n \geq 4$ and $p$ is odd. Then, $Aut(G)$ has a normal Sylow $p-$subgroup $P$ a $P'-$complement $H$, so that $Aut(G) \cong H \rtimes P$. Furthermore, $H$ is isomorphic to a subgroup of $C_{p-1} \times C_{p-1}$.*

From the result above, it can be observed that $G$ has a characteristic cyclic series $G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_n = 1$; that is, each $G_i$ is characteristic and $G_i/G_{i+1}$ is cyclic (cf. [52]). By a result of Durbin and McDonald [35], $Aut(G)$ is supersolvable and so has a normal Sylow $p-$group $P$ with $p'-$complement $H$, and the exponent of $Aut(G)$ divides $p^t(p-1)$ for some $t > 0$. The additional result about the structure of $H$ comes from examining the actions of $H$ on the characteristic cyclic series and on the $G/\Phi(G)$. Baartmans and Woeppel remark that the above theorem holds for any $p-$group $G$ with a characteristic cyclic series.

Baartmans and Woeppel [11] followed up these general results by focusing on the automorphisms of $p-$groups of maximal class of exponent $p$ with a maximal subgroup which is abelian. More specifically, the characteristic cyclic series can be taken to be a composition series, in which case $G_i = \gamma_i(G)$ for $i \geq 2$ and $G_1 = C_G(G_2/G_4)$. Baartmans and Woeppel assumed that $G_2$ is abelian.

In this case, they showed by construction that $H \cong C_{p-1} \times C_{p-1}$. Furthermore, $P$ is metabelian of nilpotence class $n-2$ and order $p^{2n-3}$ (Recall that *a metabelian group* is one whose commutator subgroup is abelian). The group $Inn(G)$ has order $p^{n-1}$ and maximal class $n-2$. The commutator subgroup $P^{'}$ is the subgroup of $Inn(G)$ induced by $G_2$. The explicit description of $Aut(G)$ is given in [11].

Other authors who have investigated automorphisms of certain finite $p-$groups of maximal class include: Abbasi [1], Miech [74], who focused on metabelian groups of maximal class; and Wolf [95], who looked at the centralizer $C(G)$ in a certain subgroup of $Aut(G)$. In [59], Juhasz considered more general $p-$groups than $p-$ groups of maximal class. Specifically, he looked at $p-$groups $G$ of nilpotence class $n-1$ in which $\gamma_1(G)/\gamma_2(G_2) \cong C_{p^m} \times C_{p^m}$ and $\gamma_i(G)/\gamma_{i+1}(G_2) \cong C_{p^m}$ for $2 \leq i \leq n-1$. He referred to such groups as being of type $(n, m)$. Groups of type $(n, 1)$ are the $p-$groups of maximal class of order $p^n$.

Assume that $n \geq 4$ and $p > 2$, as with the previous case, groups of the maximal class, $G$, a group of type $(n, 1)$ implies that $Aut(G) \cong P \rtimes H$ where $P$ is a Sylow $p-$subgroup and $H$ its $p^{'}-$complement such that $H \cong C_{p-1} \times C_{p-1}$.

In [91], Webb looked at the automorphism groups of stem covers of elementary abelian $p-$groups. A group $G$ is *a cental extension* of $Q$ by $N$ if $N$ is a normal subgroup of $G$ lying in $Z(G)$ and $G/N \cong Q$. If $N$ lies in $[G, G]$ as well, then $G$ is *a stem extension of* $Q$. The Schur multiplier $M(Q)$ of $Q$ is defined to be the second cohomology group $H^2(Q, \mathbb{C}^*)$, and it turns out that $N$ is isomorphic to a subgroup of $M(Q)$. Alternatively, $M(Q)$ can be defined as the maximal group $N$ so that there exists a stem extension of $Q$ by $N$. Such a stem extension is called *a stem cover.*

The result below was given by Webb:

**Theorem 2.3.10.** *(cf. [91]) Let $G$ be elementary abelian, of order $p^n$ with $p-$odd. As $n \to \infty$, the proportion of stem covers of $G$ with elementary abelian automorphism group of order $p^{n\binom{n}{2}}$ tends to* 1.

Not every finite $p-$group is the automorphism group of a finite $p-$group. Cutolo, Smith and Wiegold have shown in [32] that the only $p-$group of maximal class which is the automorphism group of a finite $p-$group is $D_8$. But, there are several extant results which show that certain quotients of the automorphism group can be arbitrary. For instance Heineken and Liebeck [47] gave the result below:

**Theorem 2.3.11.** *(Heineken and Liebeck [47]) Let $K$ be a finite group and let $p$ be an odd prime. There exists a finite $p-$group $G$ of class 2 and exponent $p^2$ such that $Aut(G)/Aut_c(G) \cong K$*

Lawton [63] modified Heineken and Liebeck's techniques by constructing a smaller group $G$ with $Aut(G)/Aut_c(G) \cong K$. He used undirected graphs which are much smaller, and the $p-$graphs he defined are significantly simpler.

Webb [90] used similar, though more complicated techniques, to obtain further results. She defined a class of graphs called *Z-graphs*(that is, the proportion of graphs on $n$ vertices which are Z-graphs goes to 1 as $n$ goes to $\infty$). To each Z-graph $\wedge$, Webb associated a special $p-$group $G$ for which $Aut(G)/Aut_c(G) \cong Aut(\wedge)$. The set of all special $p-$groups that arise from Z-graphs on $n$ vertices is denoted by $\mathcal{G}(p, n)$.

**Theorem 2.3.12** (Webb)**.** *Let $p$ be any prime. The proportion of groups in $\mathcal{G}_{p,n}$ whose automorphism group is $(C_p)^r$, where $r = n^2(n-1)/2$ goes to 1 as $n \to \infty$.*

The reason the group $(C_p)^r$ arises as the automorphism group is that for $G \in \mathcal{G}(p, n)$, $Aut_c(G)$ is isomorphic to $Hom(G/Z(G), Z(G))$ and hence it is isomorphic to $(C_p)^r$. Webb then showed that $Aut(G)/Aut_c(G)$ is usually trivial.

**Theorem 2.3.13** (Webb)**.** *Let $K$ be a finite group which is not cyclic of order five or less. Then, for any prime $p$, there is a special $p-$group $G \in \mathcal{G}(p, 2 \mid K \mid)$ with $Aut(G)/Aut_c(G) \cong K$.*

In particular, the above theorem extends Heineken and Liebeck's result to the case $p = 2$. The constructed groups are special and $Aut_c(G) = Aut_f(G)$, so that these theorems also prescribe $Aut(G)/Aut_f(G)$. The $p = 2$ analogue of Heineken and Liebeck's result was discussed by Hughes [51].

Bryant and Kovacs [18] looked at prescribing the quotient $Aut(G)/Aut_f(G)$, taking a different approach from Heineken and Liebeck , in that, they assigned $Aut(G)/Aut_f(G)$ as a linear group and did not bound the class of $G$.

**Theorem 2.3.14.** *(cf. [18]) Let $p$ be any prime. Let $K$ be a finite group with dimension $d \geq 2$ as a linear group over $\mathbb{F}_p$. Then, there exists a finite $p-$group $G$ such that $Aut(G)/Aut_f(G) \cong K$ and $d(G) = d$.*

This theorem is non-constructive, in contrast to the results of Heineken and Liebeck. However, the main idea can be understood as follows; Let $F$ be a free group of rank $d$, if $U$ is a normal subgroup of $F$ with $F_{n+1} \leq U \leq F_n$, then $G = F/U$ is a finite $p-$group and $Aut(G)/Aut_f(G)$ is isomorphic to the normalizer of $U$ in $GL(d, \mathbb{F}_p)$. Bryant and Kovacs showed that if $n$ is large enough, then, $F_n/F_{n+1}$ contains a regular $\mathbb{F}_pGL(d, \mathbb{F}_p)-$module, which shows that, any subgroup $K$ of $GL(d, \mathbb{F}_p)$ occurs as the normalizer of some normal subgroup $U$ of $F$ with $F_{n+1} \leq U \leq F_n$.

Ying stated two results in [96] about the occurrence of automorphism groups of $p-$groups, which are $p-$groups, the second being a generalization of a result by Heineken and Liebeck in [46].

**Theorem 2.3.15.** *(cf. [96]) If $G$ is a finite $p-$group and $Aut(G)$ is nilpotent, then, either $G$ is cyclic or $Aut(G)$ is a $p-$group.*

**Theorem 2.3.16.** *(cf. [96]) Let $p$ be an odd prime and let $G$ be a finite $p-$group generated by two elements and with cyclic commutator subgroup. Then, $Aut(G)$ is not a $p-$group if and only if $G$ is the semi-direct product of an abelian subgroup by a cyclic subgroup.*

Heineken and Liebeck [46] also gave a criterion which determines whether or not a $p-$group of class 2 and generated by two elements has an automorphism of order 2 or if the automorphism group is a $p-$group. If $p$ is an odd prime and $G$ is a $p-$group that admits an automorphism which inverts some non-trivial element of $G$, then $G$ is an *s.i group* (a some-inversion group). Clearly, if $G$ is an s.i group, it has an automorphism of order 2. If $G$ is not an s.i group, it is called an *n.i group* (a no-inversion group).

**Theorem 2.3.17.** *(cf. [46]) Let $p$ be an odd prime and let $G$ be a $p-$group of class 2 generated by two elements. Choose generators $x$ and $y$ such that $< x, G' > \cap < y, G' >= G'$, suppose that $< x, G' >=< x^{p^m} >$ and $< y, G' >=< y^{p^n} >$,*

*(i) If either $x^{p^m} = 1$ or $y^{p^n} = 1$ then $G$ is an s.i group.*

*(ii) If $x^{p^m} = [x, y]^{rp^k} \neq 1$ and $y^{p^n} = [x, y]^{sp^l} \neq 1$ with $(r, p) = (s, p) = 1$, and $(n - l + k - n)(k - l)$ is non-negative, then, $G$ is an s.i group.*

*(iii) If $k$ and $l$ are defined as in (ii) and $(n - l + k - n)(k - l)$ is negative, then $G$ is an n.i group and its automorphism group is a $p-$group.*

Now, for any group $G$, let $\pi(G)$ be the set of distinct prime factors of $\mid G \mid$. In [50] Horosevskii gave the following two theorems on the order of the automorphism group of a wreath product;

**Theorem 2.3.18.** *Let $G$ and $H$ be non-trivial finite groups, and let $G_1$ be a maximal abelian subgroup of $G$ which can be distinguished as a direct factor of $G$. Then,*

$$\pi(Aut(G \wr H)) = \pi(G) \cup \pi(H) \cup \pi(Aut(G)) \cup \pi(Aut(H)) \cup \pi(Aut(G_1 \wr H)).$$

**Theorem 2.3.19.** *Let $P_1, P_2, \cdots, P_m$ be non-trivial finite $p-$groups. Then,*

$$\pi(Aut(P_1 \wr P_2 \wr \cdots \wr P_m)) = \bigcup_{i=1}^{m} \pi(Aut(P_i)) \cup \{p\}.$$

Thus, given any finite $p-$groups whose automorphism groups are $p-$groups, one can construct infinitely many more by taking iterated wreath products.

Macdonald [69] calculated the order of the automorphism group of an abelian $p-$group using Hall polynomials as follows;

**Theorem 2.3.20.** *(cf. [69]) Let $G$ be an abelian $p-$group of type $\lambda$. Then,*

$$\mid Aut(G) \mid = p^{|\lambda| + 2n(\lambda)} \prod_{i \geq 1} \phi_{m_i(\lambda)}(p^{-1})),$$

*where* $m_i(\lambda)$ *is the number of parts of* $\lambda$ *equal to* $i$, $n(\lambda) = \sum_{i\geq 1} \left( \begin{array}{c} \lambda_i' \\ 2 \end{array} \right)$ *and* $\phi_m(t) = (1-t)(1-t^2)\cdots(1-t^m)$.

There are a variety of other results in the literature on the automorphism groups of abelian $p-$groups. For instance, Morgado [77, 78] proved the following theorem about the splitting of the sequence $1 \to K(G) \to Aut(G) \to A(G) \to 1$.

**Theorem 2.3.21.** *(cf. [77, 78]) Let* $G$ *be an elementary abelian* $p-$*group. Let* $K(G)$ *be the subgroup of* $Aut(G)$ *that acts trivially on* $G/\Phi(G)$ *and let* $A(G)$ *be the subgroup of* $Aut(G/\Phi(G))$ *induced by the action of* $Aut(G)$ *on* $G/\Phi(G)$*. If* $p \geq 5$, *then, the exact sequence* $1 \to K(G) \to Aut(G) \to A(G) \to 1$ *if and only if* $G$ *has type* $(p^m, p, \cdots, p)$ *for some positive integer* $m$*. If* $p = 2$ *or* $p = 3$, *this condition is sufficient but not necessary.*

A different type of result comes from Abraham [2], who showed that, for any integer $n \geq 0$ and for $p \geq 3$, the automorphism group of any abelian $p-$group $G$ contains a unique subgroup which is maximal with respect to being normal and having exponent at most $p^n$.

The first known example of a finite $p-$group whose automorphism group is a $p-$group was given by Miller [76], who constructed a non-abelian group of order 64 with an abelian automorphism group of order 128. Generalizing Miller's construction, Struik [89] gave the following infinite family of 2 groups whose automorphism groups are abelian 2-groups:

$$G =< a, b, c, d : a^{2^n} = b^2 = c^2 >= d^2 = 1,$$

$$[a, c] = [a, d] = [b, c] = [c, d] = 1, bab = a^{2^{n-1}}, bdb = cd >,$$

where $n \geq 3$ ($G$ can be expressed as a semi-direct product as well ). Struik showed that,

$$Aut(G) \cong (C_2)^6 \times C_{2^{n-2}}.$$

As noted in [89], it turns out that Macdonald [68], showed that $Aut(G)$ is an abelian $2-$group. Also, Jamali [55] constructed, for $m \geq 2$ and $m \geq 3$, a non-abelian $n-$generator group of order $2^{2n+m-2}$ with exponent $2^m$ and abelian automorphism group $(C_2)^{n^2} \times C_{2^{m-2}}$.

More examples of 2-groups whose automorphism groups are 2-groups are given by Newman and O'Brien [79]. As an outgrowth of their computations of 2-groups of order dividing 128, they presented (without proof) three infinite families of 2-groups for which $\mid G \mid = \mid Aut(G) \mid$. They are, for $n \geq 3$,

(1) $C_{2^{n-1}} \times C_2$,

(2) $< a, b : a^{2^{n-1}} = b^2, a^b = a^{1+2^{n-2}} >$ and

(3) $< a, b, c : a^{2^{n-2}} = b^2 = c^2 = [b, a] = 1, a^c = a^{1+2^{n-4}}, b^c = ba^{2^{n-3}} >$

Moving on to finite $p-$groups where $p$ is odd, for each $n \geq 2$, Horosevskii [49] constructed a $p-$group with nilpotence class $n$ whose automorphism group is a $p$-group, and for each $d \geq 3$, he constructed a $p-$group on $d-$generators for each $d \geq 3$ whose automorphism group is a $p-$group. He gave explicit presentations for these groups.

Curran [30] showed that if $(p-1, 3) = 1$, then, there is exactly one group of order $p^5$ whose automorphism group is a $p-$group of order $p^6$. It has the following presentation:

$$G =< a, b : b^p = [a, b]^p = [a, b, b]^p = [a, b, b, b]^p = [a, b, b, b, b]^p = 1,$$
$$a^p = [a, b, b, b] = [b, a, b]^{-1} >$$

When $(p-1, 3) = 3$, there are no groups of order $p^5$ whose automorphism group is a $p-$group. However, in this case, there are three groups of order $p^5$ which have no automorphisms of order 2. Curran also showed that $p^6$ is the smallest order of a $p-$group which can occur as an automorphism group, when $p$ is odd.

In [31], Curran constructed 3-groups $G$ of order $3^n$ with $n \geq 6$ where $\mid Aut(G) \mid = 3^{n+3}$ and $p-$groups $G$ for certain primes $p > 3$ with $\mid Aut(G) \mid = p \mid G \mid$. On the other hand, Menengazzo [72] noted that, for $p-$odd and $n \geq 3$, the automorphism group of

$$G =< a, b : a^{p^n} = 1, b^{p^n} = a^{p^{n-1}}, a^b = a^{1+p} >$$

has order $p \mid G \mid$ .

Ban and Yu [12] proved the existence of a group $G$ of order $p^n$ with $\mid Aut(G) \mid = p^{n+1}$, for $p > 2$ and $n \geq 6$. In [46], Heineken and Liebeck constructed a $p-$group of order $p^6$ and exponent $p^2$ for each odd prime $p$ which has an automorphism group of order $p^{10}$.

Jonah and Konvisser [58] exhibited $p+1$ non-isomorphic groups of order $p^8$ with elementary abelian groups of order $p^{16}$ for each prime $p$. All of these groups have elementary abelian and isomorphic commutator subgroups and commutator quotient groups, and they are nilpotent of class 2. Moreover, all their automorphisms are central.

Malome [70] found more examples of $p-$groups in which all automorphisms are central. For each prime $p$, he constructed a non-abelian finite $p-$group $G$ with a non-abelian automorphism group which comprises only central automorphisms. Moreover, his proof showed that if $F$ is any non-abelian finite $p-$group with $F^{'} = Z(F)$ and $Aut_c(F) = Aut(F)$, then, the direct product of $F$ with a cyclic group of order $p$ has the required property for $G$.

Caranti and Scoppola [19] showed that for every prime $p > 3$, if $n \geq 6$, there is a metabelian $p-$group of maximal class of order $p^n$ which has automorphism group of order $p^{2(n-2)}$, and if $n \geq 7$, there is a metabelian $p-$group of maximal class of order $p^n$ with an automorphism group of order $p^{2(n-2)+1}$. They also showed the existence of non-metabelian $p-$groups ($p > 3$) of maximal class whose automorphism groups have orders $p^7$ and $p^9$.

Fuchs [39], asked for a characterization of abelian groups, which could be groups of units of a ring. This question was noted to be too general for a complete answer by Stewart [88] and the methods that emerged later (cf. [9, 26, 82, 83] e.t.c) and a natural course has been to restrict the classes of groups or rings to be considered. In particular, if $R$ is a completely primary finite ring (not necessary commutative), then, it is well known (cf. ([24, 27])) that the group of units of $R$, contains a cyclic subgroup $< b >$ of order $p^r - 1$ such that $R^*$ is a semi direct product of $1 + J$ and $< b >$. That is,

$$R^* = (1 + J) \times < b > .$$

The automorphisms of $R^*$ are not known, however, the methods used in determining the automorphisms of direct products of finite groups by Hillar and Rheah [48], Menengazzo [72], Fitting [38], Bidwell [14] and Bidwell and McCaughan [16] Han [45] and Shoda [87] can be extended in order to characterize both the structure and order of $Aut(R^*)$.

### 2.3.4 Automorphism Groups of Finite Rings

The determination of the group of automorphisms of finite rings was invigorated by the research of Alkhamees in [6], where he studied finite chain rings of characteristic $p$. In [7], Alkhamees considered the case of finite completely primary rings with the minimal index of nilpotence $J^2 = (0)$ and determined completely the group of automorphisms of such rings. If we consider the other extreme of maximal index of nilpotency, we are led naturally to the case of chain rings [8]. Therefore, in [6] he determined fully the automorphism group, in the commutative case of chain ring of characteristic $p$ and then, showed how this can be used to solve the non-commutative case using ideas introduced in [8]. Since finite principal rings of characteristic $p$ are direct sums of finite chain rings of characteristic $p$, it is possible to determine the group of automorphisms of finite principal rings of characteristic $p$.

Let $R$ be a finite chain ring of characteristic $p$ and $J$ be the set of all zero divisors of $R$, then, $J$ is the unique maximal ideal of $R$, $\mid R \mid= p^{kr}$, $\mid J \mid= p^{(k-1)r}$ and $R$ has a subfield of order $p^r$ where $k$ is the index of nilpotency of $J$ and $p^r$ is the residue order of $R$, namely, $R/J$ is a field of order $p^r$ (cf. [8, 86, 94]). Let $J = R\pi$. Then we have the following facts: We can choose $\pi$ in such a way that there exists an automorphism $\sigma$ of $K$ such that

$$R = \sum_{i=0}^{k-1} \oplus K\pi^i.$$

(as $K-$vector spaces) and for each $r \in K$, $\pi r = r^\sigma \pi$ (cf. [21, 94]). Clearly, $R = K[x, \sigma]/(x^k)$, where $K[x, \sigma]$ is the skew polynomial ring with respect to $\sigma$. It is well known that $\sigma$ is uniquely determined by $R$ and $K$ and it is called the associated automorphism of $R$ with respect to $K$. In [6], $T_R$ denotes the set of all triplets $(K, \pi, \sigma)$ which come from the above descriptions. If $R_1$ is a chain subring of $R$, then $J(R_1) = R_1\pi^{k'}$ so that

$$R_1 = \sum_{i=1}^{k_1-1} \oplus K\pi^{k'_i}$$

where $k_1 = [(k/k') + 1]$. Thus, the chain subring $R_1$ is the only maximal commutative subring of $R$ containing $K$ and it is unique up to inner automorphism of $R$. Considering $J(R)$, $H_i(R) = 1 + J^i(R)$, $G_R-$ the group of units of $R$ and $Aut_K(R)$ as the subgroup of $Aut(R)$ which fixes $K$ elementwise. Alkhamees gave the following facts:

**Lemma 2.3.5.** *(cf.[6]) Let $R$ be a finite chain ring of characteristic $p$. Then $(K, \theta, \sigma) \in T_R$ if and only if $\theta = \lambda\omega\pi$, where $\lambda$ is an element of $K^*$ and $\omega$ an element of $H_1(R_1)$.*

**Proposition 2.3.1.** *Let $R$ be a finite chain ring of characteristic $p$. Then $\phi$ is an automorphism of $R$ if and only if*

$$\phi(\sum r_i\pi^i) = x\sum r_i^\tau(\lambda\omega\pi)^i x^{-1},$$

*where $\lambda$ is an element of $K^*$, $x$ an element of $G_R$, $\tau$ an automorphism of $K$ and $\omega$ an element of $H_1(R_1)$.*

**Remark 2.3.1.** *Let $M = [a_{ij}]$ where $a_{ij} \in K$, define $M^\tau = [a_{ij}^\tau]$. Let $e_{ij}$ denote the matrix with identity of $K$ in $(i, j)$ positions and zeros elsewhere. The group $G_{k-1}$ of all triangular matrices*

$$1 + \sum_{j<1} b_{ij}e_{ij},$$

*where $b_{ij} \in K$ is a Sylow $p-$subgroup of $GL_{k-1}(K)$. Let $E$ be the subgroup of $G_{k-1}$ which contains all the matrices $[a_{ij}]$ where*

$$a_{ij} = \sum_{e+f=i} a_{e.1}a_{f.j-1},$$

*Then, obviously, $E$ is a subgroup of $G$ of order $p^{(k-1)r}$.*

**Theorem 2.3.22.** *(cf. [6]) Let $R$ be a finite commutative chain ring of characteristic $p$*

*and $E$ be the subgroup of $G$ of order $p^{(k-1)r}$. Then,*

$$Aut(R) \cong (Ex_{\theta_1}K^*)x_{\theta_2}Aut(K),$$

*where if $M = [a_{ij}]$ is an element of $E$, $\lambda$ an element of $K^*$ and $\tau$ an element of $Aut(K,)$ then*

$$\theta_1(\lambda)(M) = [\lambda^{i-j}a_{ij}],\ \theta_2(\tau)(M, \lambda) = (M^\tau, \lambda^\tau).$$

**Theorem 2.3.23.** *(cf.[6])Let $R$ be a finite chain ring of characteristic $p$. Then,*

$$Aut(R) \cong (Inn(R)x_\theta Aut(R_1))/Aut_k(R),$$

*where, if $\phi \in Aut(R_1)$, then $\theta(\phi)(\Psi_x) = \Psi_{\phi_{(x)}}$.*

Chikunji [28] described the group of automorphisms of completely primary finite ring $R$ of characteristic $p^2$ and $p^3$ with Jacobson radical $J$ such that $J^3 = (0)$ and $J^2 \neq (0)$. In this case, the annihilator of $J$ coincides with $J^2$ and the maximal Galois (coefficient) subring $R_0$ of $R$ lies in the center of $R$. He determines the automorphisms of $R$ by the images on the generators of the additive group of $R$ and of the invertible element $b$ of order $p^r - 1$ of the Galois subring $R_0$ of $R$. This supplements his earlier work (cf. [27]) on rings of characteristic $p$ and Alkhamees' work (cf. [6]) on automorphisms of chain rings of characteristic $p$.

Let $R$ be a completely primary finite ring, $\mid R/J \mid = p^r$ and $char(R) = p^k$. Then, it can be deduced from [21] that $R$ has a coefficient subring $R_0$ of the form $GR(p^{kr}, p^k)$ which is clearly a maximal Galois subring of $R$. Moreover, if $R_0^{'}$ is another coefficient subring of $R$, then there exists an invertible element $x$ in $R$ such that $R_0^{'} = xR_0x^{-1}$ [86, Theorem 8]. Furthermore, there exist $m_1, \cdots, m_h \in J$ and $\sigma_1, \cdots, \sigma_h \in Aut(R_0)$ such that

$$R = R_0 \oplus \sum_{i=1}^{h} R_0 m_i,$$

$m_i r_0 = r_0^{\sigma_i} m_i\ \forall r_0 \in R_0$ and any $i = 1, \cdot, h$. Moreover, $\sigma_i, ..., \sigma_h$ are uniquely determined by $R$ and $R_0$ [28]. These $\sigma_i$ are called the automorphisms associated with $m_i$ and $\sigma_i, ..., \sigma_h$

called, the associated automorphisms of $R$ with respect to $R_0$.

The rings $R$ whose Jacobson radical satisfies $J^3 = (0)$ and $J^2 \neq (0)$ considered in [28] were studied in [23, 24] where their detailed constructions were given for all the characteristics. Since $R$ is such that $J^3 = (0)$, according to Raghavendran (cf.[86]), the char$(R)$ is either $p, p^2$ or $p^3$ .

**Remark 2.3.2.** *A supplementary construction on the additive group $R = R_0 \oplus U \oplus V$ has been given by Chikunji [28], by defining the multiplication on $R$ as*

$$u_i u_j = a_{ij}^0 p^f + \sum_{l=1}^{d} a_{ij}^l p u_l + \sum_{k=1}^{t} a_{ij}^{d+t};$$

$$u_i \alpha = \alpha u_i, v_k \alpha = \alpha v_k (1 \leq i, j), \alpha \leq s, 1 \leq l \leq d, 1 \leq k \leq t;$$

*where $\alpha, a_{ij}^0, a_{ij}^l, a_{ij}^{d+k} \in R_0/J_0$ and $f = 1$ or $2$ depending on whether char$(R) = p^2$ or $p^3$.*

In that case, $(a_{ij}^l)$ for $l = 0, 1, ..., t$ or $l = 1, 2, ..., d + t$ are $s \times s$ linearly independent matrices with entries in $R_0/pR_0$ if char$(R_0) = p^2$ and $l = 0, 1, ..., d + t$ is $s \times s$ linearly independent matrices with entries in $R_0/pR_0$ if $Char(R) = p^3$. We call $(a_{ij}^l)$ the structural matrices of the ring $R$ and the numbers $p, n, r, s, d, t$, the invariants of the ring $R$. By restricting the findings to cases $p \in J^2$ and $p \in J - J^2$, the following characterizations which can be found in [28] give explicit descriptions of the automorphisms of $R$:

**Theorem 2.3.24.** *(cf. [28]) Let $R$ be a ring of the construction in remark 2.3.2. of characteristic $p^2$ in which $p \in J^2$ and with the invariants $p, n, r, s, t$. Then*

$$Aut(R) \cong [\mathbb{M}_{(1+t)\times s}(R_o/pR_o) \times \mathbb{M}_{(1+t)}(R_o/pR_o) \times (pR_o \oplus U \oplus V)] \times$$

$$\theta_2[Aut(R_o \times \theta_1(GL(s, R_o/pR_o)) \times GL(t, R_o/pR_o)].$$

**Theorem 2.3.25.** *(cf. [28]) Let $R$ be a ring of the construction in remark 2.3.2. of characteristic $p^2$ in which $p \in J - J^2$ and with the invariants $p, n, r, s, t, d$. Then*

$$Aut(R) \cong [\mathbb{M}_{(d+t)\times s}(R_o/pR_o) \times \mathbb{M}_{(d\times t)}(R_o/pR_o) \times (pR_o \oplus U \oplus V)] \times$$

$$\theta_2[Aut(R_o \times \theta_1(GL(s, R_o/pR_o)) \times GL(t, R_o/pR_o) \times GL(d, R_o/pR_o)].$$

**Theorem 2.3.26.** *(cf. [28]) Let $R$ be a ring of the construction in remark 2.3.2. of characteristic $p^3$ in which $J^3 = (0)$ and with the invariants $p, n, r, s, t, d$. Then*

$$Aut(R) \cong [\mathbb{M}_{(1+d+t)\times s}(R_o/pR_o) \times \mathbb{M}_{(1+t)\times d}(R_o/pR_o) \times (pR_o \oplus U \oplus V)] \times$$

$$\theta_2[Aut(R_o \times \theta_1(GL(s, R_o/pR_o)) \times GL(t, R_o/pR_o) \times GL(d, R_o/pR_o)].$$

Raghavendran [86] appears to have made the deepest study into the nature of completely primary finite rings while, Alkhamees [8, 9] has done considerable work on automorphisms of completely primary finite rings. Many expositions on the automorphisms of completely primary finite rings can still be mentioned. For instance, Alkhamees [9] has determined the automorphisms of finite rings in which the product of any two zero divisors is zero, which is a special case of a class of finite rings in which the product of any two zero divisors lies in the coefficient subring. Chikunji's results in [28] precisely describe the group of automorphisms of cube radical zero completely primary finite rings. Oduor [81] has characterized the automorphisms of a certain class of completely primary finite rings. His results (cf.[81]), compare perfectly well with Alkhamees' and Chickunji's results ([6, 7, 8, 9, 28]).

Oduor constructed an additive abelian group $R = R_0 \oplus U$ such that $R_0 = GR(p^{nr}, p^n)$, $n \geq 3$ . This ring $R$ is completely primary of characteristic $p^n$, referred to in [81] as a finite ring with property A and whose Jacobson radical $J(R)$ satisfies;

(i) $J(R) = pR_o \oplus U$,

(ii)$(J(R))^{n-1} = p^{n-1}R_o$,

(iii) $(J(R))^n = (0)$.

The description of the automorphism groups of the class of rings constructed ( which is stated in the next theorem) is an elegant improvement of Alkhamees' description [9, Theorrem 2]. This provides a generalized structure of the automorphisms of certain classes of completely primary finite rings with property A, for all the characteristics of the rings.

**Theorem 2.3.27.** *(cf [81]) Let $R$ be a ring with property A. Then the map*

$$Aut(R) \to U \times_\alpha \left( \prod_{v=1}^{s} GL(l_v, R_o/pR_o) \times_k Aut(R_o/pR_o) \right)$$

*is an isomorphism, and in particular*

$$\mid Aut(R) \mid = (p^r)^h \left( \prod_{v=1}^{s} \prod_{i=0}^{l_v - 1} ((p^r)^{l_v} - (p^r)^i) \right) r.$$

*where $U = U_1 \oplus ... \oplus U_s$ such that each $U_v = \sum_{\sigma_k = \sigma_j} \oplus R_o u_k$, so that $\sigma_k$ is the automorphism associated with $u_k$ and $1 \leq v \leq s$.*

Finite rings have been studied extensively in recent years by various researchers. A few expositions have been demonstrated by among other scholars, Corbas [29], Chickunji [24, 26, 27, 28], Oduor [81], Oduor , Ojiema and Mmasi [82], Oduor and Ojiema [83], Raghavendran [86], Wison [92], Stewart [88], and the tools necessary for describing completely primary finite rings have been available for some time, however, their classification into well known structures that is, units, automorphisms, regular elements, zero divisor graphs excreta, essentially given in Chikunji [24, 26, 27, 28], Oduor [81], Oduor , Ojiema and Mmasi [82], Oduor and Ojiema [83] and Clark [21] is not complete. In particular, from the information in literature, no attempts have been made to characterize the automorphisms of the unit groups of any classes of completely primary finite rings that have already been classified. This motivated our study; thus in this thesis, we provide a partial solution to this elusive problem of classification by considering three classes of commutative completely primary finite rings, whose units are well known, namely, square radical zero, cube radical zero and power four radical zero commutative completely primary finite rings.

## 2.4 Some preliminaries on unit groups and automorphisms

**Proposition 2.4.1.** *[24] Let $R$ be a completely primary finite ring and let $J$ be its unique maximal ideal. Then, there exists an element $b \in R$ of multiplicative order $p^r - 1$ such that if $\psi : R \to R/J$ is the canonical homomorphism, then, $\psi(b)$ is a primitive element of $R/J$ and*

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

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

*Proof.* Obviously, the group of units $G_R$ say, of $R$ is $R - J$ and $\phi : R \to R/J$ induces a surjective multiplicative group homomorphism

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

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

Let $< \beta >= G_{(R/J)}$ and let $b_0 \in \tilde{\phi}^{-1}(\beta)$. Then, the multiplicative order of $b_0$ must be a multiple of $p^r - 1$ and a divisor of

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

hence of the form $p^\lambda(p^r - 1)$. But then $b = b_0^{p^\lambda}$ has multiplicative order $p^r - 1$ and $\tilde{\phi}(b_0^{p^\lambda}) = \beta p^\lambda$ which is still a generator of $G_{(R/J)}$, since $(p^\lambda, p^r - 1) = 1$.

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

**Lemma 2.4.1.** *Let $G = \mathbb{F}_p^n$. The automorphisms of $G$ as an abelian group are just the automorphisms of $G$ as a vector space over $\mathbb{F}_p$. Thus, $Aut(G) = GL_n(\mathbb{F}_p)$. Because $G$ is commutative, all non-trivial automorphisms of $G$ are outer.*

**Example 2.4.1.** *As a particular case to the above lemma, we see that*

$$Aut(C_2 \times C_2) = GL_2(\mathbb{F}_2).$$

*But $GL_2(\mathbb{F}_2) \approx S_3$, that is, $GL_2(\mathbb{F}_2)$ permutes the three non-zero vectors in $\mathbb{F}_2^2$, the 2-dimensional vector spaces over $\mathbb{F}_2$ and so, the non-isomorphic groups $C_2 \times C_2$ and $S_3$ have isomorphic automorphism groups.*

**Lemma 2.4.2.** *Let $G$ be a cyclic group of order $n$, that is, $G =< g >$ . An automorphism $\theta$ of $G$ must send $G$ to another generator of $G$.*

*Proof.* Let $m$ be an integer such that $m \geq 1$. The smallest multiple of $m$ divisible by $n$ is $m.\frac{n}{gcd(m,n)}$. Therefore, $g^m$ has order $\frac{n}{\gcd(m,n)}$, and so, the generators of $G$ are the elements $g^m$ with $\gcd(m, n) = 1$. Thus $\theta(g) = g^m$ for some $m$ relatively prime to $n$, and in fact, the map $\theta \mapsto m$ defines an isomorphism

$$Aut(C_n) \mapsto (\mathbb{Z}/n\mathbb{Z})^*,$$

where $(\mathbb{Z}/n\mathbb{Z})^* = \{m + n\mathbb{Z} \mid \gcd(m, n) = 1\}$ . This isomorphism is independent of the choice of a generator $g$ for $G$. If $\theta(g) = g^m$, then for any other element $g^{'} = g^i$ of $G$,

$$\theta(g^{'}) = \theta(g^i) = \theta(g)^i = g^{mi} = (g^i)^m = (g^{'})^m.$$

□

**Proposition 2.4.2.** *If $C_n = \mathbb{Z}/n\mathbb{Z}$, then $Aut(C_n) \approx (\mathbb{Z}/n\mathbb{Z})^*$.*

*Proof.* If $n = p_1^{r_1}...p_s^{r_s}$ is the factorization of $n$ into powers of distinct primes, then, by Chinese Remainder Theorem, we have an isomorphism

$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p_1^{r_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_s^{r_s}\mathbb{Z},$$

such that $m(mod)n \mapsto m(mod)(p_1^{r_1}), ..., m(mod)(p_s^{r_s})$ which induces an isomorphism

$$(\mathbb{Z}/n\mathbb{Z})^* \cong (\mathbb{Z}/p_1^{r_1}\mathbb{Z})^* \times ... \times (\mathbb{Z}/p_s^{r_s}\mathbb{Z})^*.$$

Hence, we need to only consider the case $n = p^r$, where $p$ is a prime integer.

Suppose first that $p$ is odd, the set $\{0, 1, ..., p^r - 1\}$ is a complete set of representatives for $\mathbb{Z}/p^r\mathbb{Z}$ and $\frac{1}{p}$ of these elements are divisible by $p$. Hence $(\mathbb{Z}/p^r\mathbb{Z})^*$ has order $p^r - \frac{p^r}{p} =$

$p^{r-1}(p-1)$. Because $p-1$ and $p^{r-1}$ are relatively prime, we know that $(\mathbb{Z}/p^r\mathbb{Z})^*$ is isomorphic to the direct product of a group, say $A$ of order $p-1$ and another group $B$ of order $p^{r-1}$. The map

$$(\mathbb{Z}/p^r\mathbb{Z})^* \twoheadrightarrow (\mathbb{Z}/p\mathbb{Z})^* = \mathbb{F}_p^*$$

induces an isomorphism $A \to \mathbb{F}_p^*$, and $\mathbb{F}_p^*$ being a finite subgroup of the multiplicative group of a field, is cyclic. Thus, $(\mathbb{Z}/p^r\mathbb{Z})^* \supset A =< a >$ for some element $a$ of order $p-1$.

Using the binomial theorem, we find that, $1+p$ has order $p^r - 1$ in $(\mathbb{Z}/p^r\mathbb{Z})^*$ and therefore generates $B$. Thus $(\mathbb{Z}/p^r\mathbb{Z})^*$ is cyclic with the generators $a.(1+p)$ and every element can be written uniquely in the form $a^i.(1+p)^j, (0 \leq i \leq p-1, 0 \leq j \leq p^{r-1})$ Thus,

$$(\mathbb{Z}/p^r\mathbb{Z})^* \approx \begin{cases} C_{(p-1)p^{r-1}}, & 2 \nmid p; \\ C_2, & p = 2^2; \\ C_2 \times C_{2^{r-2}}, & p = 2, r > 2. \end{cases}$$

□

**Proposition 2.4.3.** *Let $R$ be a completely primary finite ring. Then, any quotient ring of $R$ (by two sided ideal) and any homomorphic image of $R$ is a completely primary ring.*

*Proof.* Let $\theta : R \to R_1$ be a surjective ring homomorphism. Since $J$ is the unique maximal ideal of $R$, $Ker(\theta) \subset J$. Also, clearly $\{x + Ker(\theta) : x \in J\}$ is the set of all the zero divisors in $R/Ker(\theta)$ and hence it is a subgroup of $(R/Ker(\theta), +)$. So, $R/Ker(\theta)$ is a completely primary finite ring, thus $R_1$ is completely primary too. □

# CHAPTER 3

# THE UNIT GROUPS $R^*$, STRUCTURES AND ORDERS OF THE AUTOMORPHISM GROUPS

## 3.1 Unit Groups of Finite Completely Primary Rings

Completely primary rings with full characteristic $p^n$ have been of interest for some years. Clark mentioned in [21] that Krull worked with these rings as early as 1924 (cf. [62]) and that Januz rediscovered them in [56]. Raghavendran [86] has classified these rings as quotients of polynomial rings. However, Raghavendran's classification of these rings had already been discovered by both Krull and Januz, although their considerations have been less detailed. Indeed, the terminology 'Galois Rings' which Raghavendran used for a coefficient ring of this type, was introduced by Januz.

Several authors have constructed finite rings whose Jacobson radical or group of units yield a particular structure. For instance, in [26], the author has obtained the structure of unit groups of classes of completely primary finite rings in which the product of any three zero divisors is zero, [82] has obtained the structure of units of a class of completely primary finite rings in which the product of any two zero divisors is zero while in [83], the unit groups of some classes of power four radical zero completely primary finite rings have been characterized. Further, it is well known that if $R$ is a finite field, then the group of units is cyclic. In [41], Gilmer characterized all rings whose groups of units are cyclic.

Suppose $R$ is a ring and $R^*$ its multiplicative group of units, then, all such local rings with cyclic groups of units were determined by Ayoub [10] and the same case was also considered by Gilmer [41]. Gilmer showed that it is sufficient to consider finite primary rings. Ayoub [10] restricted attention to finite primary rings and showed some connections between the additive group of $N$, the radical of the ring $R$ and the multiplicative group $1 + N$. Clark [21] investigated $R^*$ where the ideals form a chain and has shown that if $p \geq 3, n \geq 2$ and $r \geq 2$ then the units of the Galois ring $GR(p^{nr}, p^n)$ are a direct sum of cyclic groups of order $p^r - 1$ and $r$ cyclic groups of order $p^n - 1$ (This was also done independently by Raghavandran in [86].

Stewart [88] considered a more general problem by proving that for a given finite group $G$ (not necessarily abelian), there are up to inner isomorphism, only finitely many directly indecomposable finite rings having groups of units isomorphic to $G$. Ganske and McDonald [40] provided a solution for $R^*$ when the local ring $R$ has a Jacobson radical $J$ such that $J^2 = (0)$ by showing that;

$$R^* = (\oplus \sum_{i=1}^{nt} \varepsilon(\pi) \oplus \varepsilon(|K| - 1)),$$

where $n = dim_K(J/J^2)|K| = p^t$ and $\varepsilon(\pi)$ denotes the cyclic group of order $\pi$.

## 3.2 Unit Groups of Square Radical Zero finite commutative Completely Primary Rings

Corbas [29] showed that there are exactly two types of these rings; one being of characteristic $p$ and the other being of characteristic $p^2$. Further study on this class of rings was done by Alkhamees in [7].

Since the index of nilpotency of the Jacobson radical of this class of ring is 2 and every $r \in J$ maps to $r \in ann(J)$, the annihilator of $J$, we call such a ring, square radical zero finite completely primary ring.

Oduor, Ojiema and Mmasi [82] considered a generalized characterization of the units of commutative completely primary finite rings of characteristic $p^n$. The construction given by these authors is a consideration of the values of $n$ such that (a) $n = 1, 2$ and (b) $n \geq 3$, as such is the case, they assumed a general construction. If we restrict our construction to case (a), then, we have a ring of characteristics $p$, $p^2$, whose group of units are of interest in this section.

### 3.2.1 Construction of Square Radical Zero Finite Rings and their Units

We adapt the construction given by Oduor, Ojiema and Mmasi [82] and restrict our attention to case (a) only;

Let $R_0$ be the Galois ring of the form $GR(p^{nr}, p^n)$. For each $i = 1, ..., h$, let $u_i \in J(R)$, such that $U$ is an $h-$ dimensional $R_0-$module generated by $\{u_1, ..., u_h\}$ so that $R = R_0 \oplus U$ is an additive group. On this group, define multiplication by the following relation

(*) If $n = 1, 2$, then $pu_i = u_i u_j = u_j u_i = 0$, $u_i r_0 = (r_0)^{\sigma_i} u_i$,

where $r_0 \in R_0$, $1 \leq i, j \leq h$, $p$ is a prime integer, $n$ and $r$ are positive integers and $\delta_i$ is the automorphism associated with $u_i$. Further, let the generators $\{u_i\}$ for $U$ satisfy the additional condition that, if $u_i \in U$, then, $pu_i = u_i u_j = 0$. From the given multiplication in $R$, we see that if $r_0 + \sum_{i=1}^{h} \lambda_i u_i$ and $s_0 + \sum_{i=1}^{h} \gamma_i u_i$, $r_0, s_0 \in R_0$, $\lambda_i, \gamma_i \in F_0$, are elements of $R$, then,

$$(r_0 + \sum_{i=1}^{h} \lambda_i u_i)(s_0 + \sum_{i=1}^{h} \gamma_i u_i) = r_0 s_0 + \sum_{i=1}^{h} \{(r_0 + pR_o)\gamma_i + \lambda_i (s_0 + pR_0)^{\sigma_i}\} u_i.$$

It is easy to verify that the given multiplication turns the additive abelian group $R$, into a ring with identity $(1, 0, \cdots, 0)$. Moreover, we notice that $p \in J(R)$.

**Remark 3.2.1.** *Since $n = 1, 2$, the construction above yields rings in which multiplication of any two zero divisors is zero, that is , $J^2 = (0)$. Such rings are well known to be completely primary (cf. [9, 27, 29, 81, 83, 86])*

As a consequence of the given construction, the following results (which can be found in [82]) are important;

**Lemma 3.2.1.** *The ring described by the construction above is commutative if and only if $\sigma_i = id_{R_0}$, for each $i = 1, \cdots, h$*

**Proposition 3.2.1.** *Let $R$ be a finite ring from the class of finite rings described by the construction (*). If $U$ is generated by $\{u_1, \cdot, u_h\}$, then, it is also generated by $\{u_1, u_1 + u_2, \cdots, u_1 + u_2 + \cdots + u_h\}$.*

**Proposition 3.2.2.** *Let $R$ be a finite ring from the class of finite rings described by the construction (*). If $h \geq 1$ and $char(R) = p$, then,*

$$1 + J \cong (\mathbb{Z}_p^r)^h.$$

**Proposition 3.2.3.** *Let $R$ be a finite ring from the class of finite rings described by the construction (*). If $h \geq 1$ and char$(R) = p^2$, then,*

$$1 + J \cong \mathbb{Z}_p^r \times (\mathbb{Z}_p^r)^h.$$

**Theorem 3.2.1.** *(cf., [82]) The unit group $R^*$ of the commutative completely primary finite ring of characteristic $p^n$ with maximal ideal $J$ such that $(J(R))^2 = (0)$ when $n = 1, 2$ and $(J(R))^n = (0)$, $(J(R))^{n-1} \neq (0)$, when $n \geq 3$ and with invariants $p$(prime integer), $p \in J(R)$, $r \geq 1$ and $h \geq 1$ is a direct product of cyclic groups as follows:*

*(i) If char $(R) = p$, then,*

$$R^* = \mathbb{Z}_{p^r-1} \times (\mathbb{Z}_p^r)^h.$$

*(ii) If char $(R) = p^2$, then,*

$$R^* = \mathbb{Z}_{p^r-1} \times \mathbb{Z}_p^r \times (\mathbb{Z}_p^r)^h.$$

## 3.3 Automorphism Groups of the Units of Square Radical Zero Finite Completely Primary Rings

The following general structure result for the automorphisms of a finite group follows from a classical result of Gauss in number theory. Let $\mathbb{Z}_n$ denote the additive group of integers mod $n$ and $U(\mathbb{Z}_n)$ the multiplicative group of integers mod $n$. Gauss analyzed the orders of elements in $U(\mathbb{Z}_{p^n})$ for $p$ prime. His results can be summarized as follows:

**Theorem 3.3.1.** *(Gauss) Let $p$ be an odd prime and $n \geq 1$ or $p = 2$ and $n \geq 2$. Then*

$$U(\mathbb{Z}_{p^n}) \cong \mathbb{Z}_{p^{n-1}(p-1)}, U(\mathbb{Z}_{2^n}) \cong \mathbb{Z}_2 \times \mathbb{Z}_{2^{n-2}}.$$

Notice that $U(\mathbb{Z}_n)$ is precisely the set of generators of $\mathbb{Z}_n$. Since any automorphism $\theta \in \mathbb{Z}_n$ sends 1 to a generator, the valuation map $E : Aut(\mathbb{Z}_n) \mapsto U(\mathbb{Z}_{p^n})$ given by $E(\theta) = E(1)$ is an isomorphism of groups. This sets the stage for prime factorization of the integer $n$ and consequently the classification of the automorphisms of an arbitrary finite abelian group. On the other hand, the automorphisms of cyclic groups are precisely known. In fact, given any prime $p$ and any integer $n$, the group $Aut(C_p^n) \cong Aut(\mathbb{Z}_p^n)$, the group of $n$ by $n$ invertible matrices over the field $\mathbb{Z}_p$. These and related matrix groups play important roles in the classification of simple groups.

It has been shown in the previous section that if $R$ is completely primary, the group of units $R^*$ of $R$ is given by $R^* = \mathbb{Z}_{p^r-1} \times (1+J)$, a direct product of abelian groups. We need to find all the elements of $GL_{hr}(\mathbb{Z}_p)$ and $GL_{(h+1)r}(\mathbb{Z}_p)$ for both of the characteristics of $R$ that can be extended to a matrix in $End(1+J)$ and calculate the distinct ways of extending such elements to the endomorphism.

The following Lemma is useful in the sequel:

**Lemma 3.3.1.** *(cf. [48]) Let $H$ and $K$ be finite groups of relatively prime orders. Then,* $Aut(H) \times Aut(K) \cong Aut(H \times K)$.

**Proposition 3.3.1.** *Let* $R^* = \mathbb{Z}_{p^r-1} \times (1+J)$*. Since* $\gcd(p^r-1, \mid 1+J \mid) = 1$, $Aut(R^*) \cong Aut(\mathbb{Z}_{p^r-1} \times 1+J) = Aut(\mathbb{Z}_{p^r-1}) \times Aut(1+J)$.

*Proof.* This is a modification of the proof of Lemma 2.1 in [48].
Let $\theta : Aut(\mathbb{Z}_{p^r-1}) \times Aut(1+J) \to Aut(\mathbb{Z}_{p^r-1} \times (1+J)$ be a homomorphism. Suppose $\phi_1 \in Aut(\mathbb{Z}_{p^r-1})$ and $\phi_2 \in Aut(1+J)$, then, it is easy to see that an automorphism $\theta(\phi_1, \phi_2)$ of $\mathbb{Z}_{p^r-1} \times (1+J)$ is given by $\theta(\phi_1, \phi_2)(x, y) = (\phi_1(x), \phi_2(y))$.

Let $id_1 \in Aut(\mathbb{Z}_{p^r-1})$ and $id_2 \in Aut(1+J)$ be the identity automorphisms of $\mathbb{Z}_{p^r-1}$ and $(1+J)$ respectively. To show that, $\theta$ is indeed a homomorphism, notice that $\theta(id_1, id_2) = id_{(\mathbb{Z}_{p^r-1})\times(1+J)}$ and that, $\theta(\phi_1\phi_1^{'}, \phi_2\phi_2^{'})(x, y) = (\phi_1\phi_1^{'}(x), \phi_2\phi_2^{'}(y))$

$$= \theta(\phi_1, \phi_2)\theta(\phi_1^{'}, \phi_2^{'})(x, y), \forall \phi_1, \phi_1^{'} \in Aut(\mathbb{Z}_{p^r-1}), \phi_2, \phi_2^{'} \in Aut(1+J).$$

Next, we verify that $\theta$ is an isomorphism. Clearly, $\theta$ is injective. Thus, we are left with showing surjectivity.
Let $n = p^r - 1 =\mid \mathbb{Z}_{p^r-1} \mid$ and $m =\mid (1+J) \mid$ such that $\gcd(n, m) = 1$. Write $\phi_{\mathbb{Z}_{p^r-1}}$ and $\phi_{1+J}$ for the standard projection homomorphism $\phi_{\mathbb{Z}_{p^r-1}} : \mathbb{Z}_{p^r-1} \times (1+J) \to \mathbb{Z}_{p^r-1}$ and $\phi_{1+J} : \mathbb{Z}_{p^r-1} \times (1+J) \to 1+J$. Fix $\theta^{'} \in Aut(\mathbb{Z}_{p^r-1} \times (1+J))$ and consider the homomorph-

ism $\alpha : 1+J \to \mathbb{Z}_{p^r-1}$ given by $\alpha(y) = \phi_{\mathbb{Z}_{p^r-1}}(\theta'(id_1, y))$. Notice that $\{y^n : y \in 1+J\} \subseteq Ker(\alpha)$ since $id_1 = \phi_{\mathbb{Z}_{p^r-1}}(\theta'(id_1, y))^n = \phi_{\mathbb{Z}_{p^r-1}}(\theta'(id_1, y)^n) = \phi_{\mathbb{Z}_{p^r-1}}(\theta'(id_1, y^n)) = \alpha(y^n)$.

Also, since $\gcd(m, n) = 1$, the set $\{y^n : y \in 1+J\}$ consists of $m$ elements. Consequently, it follows that $ker\ (\alpha) = (1+J)$ and $\alpha$ is the trivial homomorphism. Similarly, $\delta : \mathbb{Z}_{p^r-1} \to 1+J$ given by $\delta(x) = \phi_{1+J}(\theta'(x, id_2))$ is trivial.

Finally, define endomorphisms of $\mathbb{Z}_{p^r-1}$ and $(1+J)$ by; $\theta'(x) = \phi_{\mathbb{Z}_{p^r-1}}(\theta'(x, id_2))$, $\theta'_{(1+J)}(y) = \phi_{1+J}(\theta'(id_1, y))$. From this construction and the above argument, we have $\theta'(x, y) = \theta'(x, id_2) \cdot \theta'(id_1, y) = (\theta'_{\mathbb{Z}_{p^r-1}}(x), \theta'_{1+J}(y)) = (\theta'_{\mathbb{Z}_{p^r-1}}, \theta'_{1+J}(x, y))$for all $x \in \mathbb{Z}_{p^r-1}$ and $y \in (1+J)$.

It remains to prove that $\theta'_{\mathbb{Z}_{p^r-1}} \in Aut(\mathbb{Z}_{p^r-1})$ and $\theta'_{1+J} \in Aut(1+J)$ and for this, it suffices to show that that $\theta'_{\mathbb{Z}_{p^r-1}}$ and $\theta'_{1+J}$ are injective (since both $n, m < \infty$).

Now, suppose that $\theta'_{\mathbb{Z}_{p^r-1}}(x) = id_1$ for some $x \in \mathbb{Z}_{p^r-1}$. Then, $\theta'(x, id_2) = (\theta'_{\mathbb{Z}_{p^r-1}}(x), \theta'_{1+J}(id_2) = (id_1, id_2)$. So, $x = id_1$ by injectivity of $\theta'$. A similar argument shows that $\theta'_{1+J} \in Aut(1+J)$ and this completes the proof. $\square$

**Remark 3.3.1.** *From the Lemma* 3.3.1 *and the Proposition* 3.3.1 *it is easy to see that since the groups* $\mathbb{Z}_{p^r-1}$ *and* $(1+J)$ *are of relatively prime orders and* $Aut(\mathbb{Z}_{p^r-1}) \cong (\mathbb{Z}_{p^r-1})^*$, *it implies that;*

*(i) when* $char(R) = p$, *then* $Aut(R^*) \cong Aut(\mathbb{Z}_{p^r-1}) \times Aut((\mathbb{Z}_p^r)^h) \cong (\mathbb{Z}_{p^r-1})^* \times Aut((\mathbb{Z}_p^r)^h)$.

*(ii) when* $char(R) = p^2$, *then* $Aut(R^*) \cong (\mathbb{Z}_{p^r-1})^* \times Aut((\mathbb{Z}_p^r)^{h+1})$.

**Lemma 3.3.2.** *Let* $Char\ R = p$, *where* $p$ *is a prime integer and* $B_p = 1+J \cong (\mathbb{Z}_p^r)^h$, *then,* $\mid B_p \mid = p^{rh}$.

**Lemma 3.3.3.** *Let* $Char\ R = p^2$, *where* $p$ *is a prime integer and* $B_p = 1+J \cong (\mathbb{Z}_p^r)^{h+1}$, *then,* $\mid B_p \mid = p^{r(h+1)}$.

In the sequel, we determine $Aut(I+J)$ for both the characteristics of $R$.

### 3.4 The Endomorphism Rings of the group $1 + J$

For a successful characterization of $Aut(R^*)$, it is necessary and sufficient to find a description of $E_p$, the endomorphism ring of $(1 + J)$ and finally specify which endomorphisms are automorphisms. Elements of $E_p$ are group homomorphisms from $1+J$ into itself with ring multiplication given by composition and addition given naturally.

An element of $1 + J$ is a column vector $(x_1, ..., x_n)^T$ in which each $x_i \in \mathbb{Z}/p^{e_i}\mathbb{Z}$ and $x_i \in \mathbb{Z}$ is an integral representative.

#### 3.4.1 Characteristic of $R = p$

**Proposition 3.4.1.** *Let $R$ be a finite ring whose additive group $(R, +)$ is of type $(p^{e_1}, p^{e_2}, \cdots, p^{e_l})$ : $e_i \geq e_2 \geq \cdots \geq e_l$. Then, $R$ can be identified with a subring of the endomorphism ring say, of the additive group. The ring can be considered as the ring of all $l \times l$ matrices $(a_{ij})$ such that $1 \leq i, j \leq l$ of the form,*

$$(a_{ij}) = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1l} \\ p^{e_1-e_2}a_{21} & a_{22} & \cdots & a_{2l} \\ \vdots & \vdots & \vdots & \vdots \\ p^{e_1-e_2}a_{l1} & \cdots & \cdots & a_{ll} \end{pmatrix}$$

*such that*

$$a_{ij} = \begin{cases} a_{ij}, & i \leq j; \\ p^{e_j-e_i}a_{ij}, & i > j. \end{cases}$$

**Definition 3.4.1.** *Let $1 + J = \underbrace{\mathbb{Z}_p^r \times \mathbb{Z}_p^r \times \cdots \times \mathbb{Z}_p^r}_{h}$. We define*

$$R_p = \{(a_{ij}) \in \mathbb{Z}_{n\times n} : p^{e_i-e_j} \mid a_{ij}, \ where\ 1 \leq j \leq i \leq n\}. \quad (3.1)$$

*The set $R_p$ defines a set of all the rings of matrices describing the representations of all the endomorphisms of $1 + J$.*

**Example 3.4.1.** *Suppose $n = 4$. Since $e_1 = 1, e_2 = 2, e_3 = 3, e_4 = 4$, then $G =$*

$\mathbb{Z}_p \times \mathbb{Z}_{p^2} \times \mathbb{Z}_{p^3} \times \mathbb{Z}_{p^4}$ *so that*

$$R_p = \left\{ \begin{pmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ pa_{21} & a_{22} & a_{23} & a_{24} \\ p^2a_{31} & pa_{32} & a_{33} & a_{34} \\ p^3a_{41} & p^2a_{42} & pa_{43} & a_{44} \end{pmatrix} : a_{ij} \in \mathbb{Z} \right\}.$$

*Therefore generally, for* $1 + J = \underbrace{\mathbb{Z}_p \times \cdots \times \mathbb{Z}_p}_{r}$,

$$R_p = \left\{ \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1r} \\ a_{21} & a_{22} & \cdots & a_{2r} \\ \vdots & \vdots & \vdots & \vdots \\ a_{r1} & a_{r2} & \cdots & a_{rr} \end{pmatrix} : a_{ij} \in \mathbb{Z} \right\}.$$

**Lemma 3.4.1.** *[48]* $R_p$ *forms a ring under matrix multiplication.*

*Proof.* Let $A = (a_{ij}) \in R_p$. The condition that $p^{e_i - e_j}$ divides $a_{ij}$ for all $i \geq j$ is equivalent to the existence of a decomposition $A = PA'P^{-1}$, in which $A' \in \mathbb{Z}^{n\times n}$ and $P = diag(p^{e_i}, ..., p^{e_n})$ is diagonal.

Now, if $A, B \in R_p$, then, $AB = (PA'P^{-1})(PB'P^{-1}) = PA'B'P^{-1} \in R_p$ as required. □

**Proposition 3.4.2.** *Let* $\phi_i : \mathbb{Z} \to \mathbb{Z}/p^{e_i}\mathbb{Z}$ *be defined by* $x \mapsto x \mod (p^{e_i})$. *Let* $\phi : \mathbb{Z}^n \to (1 + J)$ *be a homomorphism given by* $\phi(x_1, ..., x_n)^T = (\phi_1(x_1), ..., \phi_n(x_n))^T = (x_1, ..., x_n)^T$. *Then,* $E_p$ *is a multiplication by a matrix* $A \in R_p$ *on a vector of integer representatives followed by an application of* $\phi$.

**Theorem 3.4.1.** *[48] The map* $\psi : R_p \to E_p$ *given by* $\psi(A)(x_1, ..., x_n)^T = \phi(A(x_1, ..., x_n)^T)$ *is a surjective ring homomorphism.*

*Proof.* Follows from the proof of Theorem 3.3 in [48]. □

**Remark 3.4.1.** *Given this description of* $E_p = End(1 + J)$, *we can, characterize, those endomorphisms giving rise to elements in* $Aut(1 + J)$.

**Lemma 3.4.2.** *The kernel of* $\psi$ *is given by the set of matrices* $A = (a_{ij}) \in R_p$ *such that* $p^{e_i - e_j}$ *divides* $a_{ij}$ *for all* $i, j$.

**Remark 3.4.2.** *It is now clear that $E_p$ which is the endomorphism of $(1+J)$ is explicitly characterized as a quotient $R_p/Ker\ (\psi)$.*

**Theorem 3.4.2.** *[48] Let $A \in \mathbb{Z}^{n\times n}$ be such that $det(A) \neq 0$. Then, there exists a unique matrix $B \in \mathbb{Q}^{n\times n}$ called the adjugate of $A$ such that $AB = BA = det(A)I$ and moreover, $B$ has integer entries.*

**Proposition 3.4.3.** *Let $R$ be a square radical zero finite commutative completely primary ring constructed in the previous section. Let the characteristic of $R$ be $p$ so that $1 + J = (\mathbb{Z}_p^r)^h$. Suppose, $B_p = \underbrace{\mathbb{Z}_p \times \cdots \times \mathbb{Z}_p}_{r} \subseteq (1 + J)$ , then we can construct a set of endomorphisms of $B_p$ in a similar manner as in the sequel such that,*

$$R_p = \{(a_{ij}) : p^{e_i-e_j} \mid a_{ij};\ 1 \leq j \leq i \leq r\} = \left\{ \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1r} \\ a_{21} & a_{22} & \cdots & a_{2r} \\ \vdots & \vdots & \vdots & \vdots \\ a_{r1} & a_{r2} & \cdots & a_{rr} \end{pmatrix} : a_{ij} \in \mathbb{Z} \right\} = M_r(\mathbb{Z}_p). \tag{3.2}$$

*As a result, the following conditions hold:*

*(i) $End(B_p) \cong \psi(A)$ such that $A = (a_{ij}) \in M_r(\mathbb{Z}_p)$ and $\psi : M_r(\mathbb{Z}_p) \to End(B_p)$ is a surjective ring homomorphism*

*(ii) $Aut(B_p) = GL_r(\mathbb{Z}_p)$.*

*(iii) $\mid Aut(B_p) \mid = \prod_{i=0}^{r-1}(p^r - p^i)$.*

*Proof.* The proof of (i) and (ii) follow from the previous results.

Now, consider $Aut(\underbrace{\mathbb{Z}_p \times \cdots \times \mathbb{Z}_p}_{r})$. We start with $Aut(\mathbb{Z}_p)$ and $Aut(\mathbb{Z}_p \times \mathbb{Z}_p)$ in order to obtain the size of the automorphism group of $B_p$. In $\mathbb{Z}_p$, each of the $p - 1$ nonidentity elements has order $p$. Suppose $\mathbb{Z}_p =< a >$, then the map $a \mapsto a^i$ is an element of $Aut(\mathbb{Z}_p)$ provided $i \in [1, p-1]$. Thus $\mid Aut(\mathbb{Z}_p) \mid = p-1 = \varphi(p)$, where $\varphi$ is the Euler's phi-function.

Next, let $a$ and $b$ each generate groups of order $p$, so that $\mathbb{Z}_p \times \mathbb{Z}_p =< a >< b >$. A homomorphism $\theta : \mathbb{Z}_p \times \mathbb{Z}_p \mapsto \mathbb{Z}_p \times \mathbb{Z}_p$ is an automorphism if and only if $\mid \theta(a) \mid = \mid \theta(b) \mid = p$ and $< \theta(a) >$ intersects with $< \theta(b) >$ only at identity.

To find $\mid Aut(\mathbb{Z}_p \times \mathbb{Z}_p) \mid$, we must count the pairs $(\beta, \beta^{'})$ of elements in $\mathbb{Z}_p \times \mathbb{Z}_p$ such that $\theta(a) = \beta$ and $\theta(b) = \beta^{'}$ determines an automorphism. Each of the $p^2 - 1$ nonidentity elements of $\mathbb{Z}_p \times \mathbb{Z}_p$ has order $p$ , so, a given element of $Aut(\mathbb{Z}_p \times \mathbb{Z}_p)$ may map $a$ to any of the $p^2 - 1$ different places.

Let $\beta$ be nonidentity element. We must count the elements $\beta^{'}$ of $\mathbb{Z}_p \times \mathbb{Z}_p$ such that $< \beta^{'} >= p$ and $< \beta > \cap < \beta^{'} >= \{e\}$. Since each $\beta$ generates a group of order $p$ and any of the $p^2 - p$ elements of $\mathbb{Z}_p \times \mathbb{Z}_p$ lying outside of $< \beta >$ will generate a group of order $p$ that intersects the group $< \beta >$ only at identity element, it follows that

$$\mid Aut(\mathbb{Z}_p \times \mathbb{Z}_p) \mid = (p^2 - 1)(p^2 - p) \tag{3.3}$$

For $B_p = \underbrace{\mathbb{Z}_p \times \cdots \times \mathbb{Z}_p}_{r}$, let $\{g_1, \cdots, g_r\}$ be a set of generators for $B_p$, so that

$$\underbrace{\mathbb{Z}_p \times \cdots \times \mathbb{Z}_p}_{r} =< g_1 > \times < g_2 > \times \cdots \times < g_r > .$$

Each of the nonidentity elements of $B_p$ has order $p$. We now count the number of injective maps from the above generators to nonidentity elements that generate groups intersecting only at the identity element.

Suppose that an automorphism of $B_p$ sends $g_1$ to some element $\beta$ in $B_p$, then there are $p^r - p$ elements $\beta^{'}$ such that $< \beta > \cap < \beta^{'} >= \{e\}$. Supposing further that this automorphism is given by $g_1 \mapsto \beta$ and $g_2 \mapsto \beta^{'}$ for some $\beta^{'}$ not in $< \beta >$, there remain $p^r - p^2$ elements $\beta^{''} \in B_p$ that are outside of $< \beta > \times < \beta^{'} >$. Sending $g_3$ to any such $\beta^{''}$ gives $(< \beta >< \beta^{'} >) \cap < \beta^{''} >= \{e\}$.

Continuing in this manner, it is easy to specify where an automorphism of $B_p$ sends the first $n$ generators and then find $p^r - p^n$ elements in $B_p$ to which the next generators might be sent. Thus,

$$\mid Aut(\mathbb{Z}_p^r) \mid = \mid Aut(B_p) \mid = \prod_{i=0}^{r-1} (p^r - p^i). \tag{3.4}$$

$\square$

In addition to the result above, we have:

**Theorem 3.4.3.** *Any endomorphism $M = \psi(A)$ where $A \in R_p$ is an automorphism if and only if $A \mod p \in GL_n(\mathbb{F}_p)$ where $n = rank(1+J)$.*

*Proof.* Fix a matrix $A \in R_p$ with $\det(A) \neq 0$. It is well known that an adjugate of $A$ say $B \in \mathbb{Z}^{n\times n}$ exists such that $AB = BA = det(A)I$. We need to show that $B$ is actually an element of $R_p$.

Let $A = PA^{'}P^{-1}$ for some $A^{'} \in \mathbb{Z}^{n\times n}$ and $B^{'} \in \mathbb{Z}^{n\times n}$ be such that $A^{'}B^{'} = B^{'}A^{'} = \det(A^{'})I$. Notice that $det(A) = det(A^{'})$. Let $C = PB^{'}P^{-1}$ and observe that

$$AC = PA^{'}B^{'}P^{-1} = det(A)I = PB^{'}A^{'}P^{-1} = CA.$$

By the uniqueness of $B$, it follows that $B = C = PB^{'}P^{-1}$ and thus, $B$ is in $R_p$ as desired.

Now, suppose that $p \nmid \det(A)$ so that $A \mod p \in GL_n(\mathbb{F}_p)$ and let $\lambda \in \mathbb{Z}$ be such that $\lambda$ is the inverse of $\det(A)$ modulo $p^{e_i}$(such an integer exists since $\gcd(\det(A), p^{e_n}) = 1$). Thus we have, $\det(A) \cdot \lambda \equiv 1 \mod p^{e_j}$ whenever $1 \leq j \leq n$.

Let $B$ be the adjugate of $A$. Define an element of $R_p$ by $A^{(-1)} := \lambda \cdot B$, whose image under $\psi$ is the inverse of the endomorphism represented by $A:$

$$\psi(A^{(-1)}A) = \psi(AA^{(-1)}) = \psi(\lambda \cdot det(A)I) = id_{E_p}.$$

This proves that $\psi(A) \in Aut(1+J)$. Conversely, if $\psi(A) = M$ and $\psi(C) = M^{-1} \in E_p$ exists, then, $\psi(AC - I) = \psi(AC) - id_{E_p} = 0$. Hence, $AC - I \in ker(\psi)$.

From the kernel calculation , it follows that $p \mid (AC - I)$ entry-wise and so, $AC \equiv I \mod p$. Thus, $1 \equiv \det(AC) \equiv \det(A)\det(C) \mod p$. In particular, $p \nmid det(A)$. $\square$

**Lemma 3.4.3.** *Consider $R^*$ such that $char(R) = p$, so that $1 + J = \underbrace{\mathbb{Z}_p^r \times \mathbb{Z}_p^r \times .... \times \mathbb{Z}_p^r}_{h}$. Then,*

$$
(i)\ R_p = \left\{ \begin{pmatrix} a_{11} & \cdots & a_{1r} & a_{1(r+1)} & \cdots & a_{1(2r)} & \cdots & a_{1(hr)} \\ a_{21} & \cdots & a_{2r} & a_{2(r+1)} & \cdots & a_{2(2r)} & \cdots & a_{2(hr)} \\ \vdots & \cdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{r1} & \cdots & a_{rr} & a_{r(r+1)} & \cdots & a_{r(2r)} & \cdots & a_{r(hr)} \\ \vdots & \cdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{(2r)1} & \cdots & a_{(2r)r} & a_{(2r)(r+1)} & \cdots & a_{(2r)(2r)} & \cdots & a_{(2r)(hr)} \\ \vdots & \cdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{(hr)1} & \cdots & a_{(hr)r} & a_{(hr)(r+1)} & \cdots & a_{(hr)(2r)} & \cdots & a_{(hr)(hr)} \end{pmatrix} : a_{ij} \in \mathbb{Z} \right\}
$$

$$
= M_{hr}(\mathbb{Z}_p) \tag{3.5}
$$

*(ii)* $End(1+J) \cong \psi(A)$ *such that* $A = (a_{ij}) \in M_{rh}(\mathbb{Z}_p)$ *and* $\psi : M_{rh}(\mathbb{Z}_p) \to End(1+J)$ *is an onto ring homomorphism.*

*(iii)* $Aut(1+J) = GL_{hr}(\mathbb{Z}_p)$.

**Lemma 3.4.4.** *Consider* $R^*$ *such that* $char(R) = p^2$ *so that* $1 + J = \underbrace{\mathbb{Z}_p^r \times \mathbb{Z}_p^r \times .... \times \mathbb{Z}_p^r}_{h+1}$. *Then*

$$
(i)\ R_p = \left\{ \begin{pmatrix} a_{11} & \cdots & a_{1r} & a_{1(r+1)} & \cdots & a_{1(2r)} & \cdots & a_{1((h+1)r)} \\ a_{21} & \cdots & a_{2r} & a_{2(r+1)} & \cdots & a_{2(2r)} & \cdots & a_{2((h+1)r)} \\ \vdots & \cdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{r1} & \cdots & a_{rr} & a_{r(r+1)} & \cdots & a_{r(2r)} & \cdots & a_{r((h+1)r)} \\ \vdots & \cdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{(2r)1} & \cdots & a_{(2r)r} & a_{(2r)(r+1)} & \cdots & a_{(2r)(2r)} & \cdots & a_{(2r)((h+1)r)} \\ \vdots & \cdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{((h+1)r)1} & \cdots & a_{(hr)r} & a_{(hr)(r+1)} & \cdots & a_{(hr)(2r)} & \cdots & a_{((h+1)r)((h+1)r)} \end{pmatrix} : a_{ij} \in \mathbb{Z} \right\}
$$

$$
= M_{(h+1)r}(\mathbb{Z}_p) \tag{3.6}
$$

*(ii)* $End(1+J) \cong \psi(A)$ *such that* $A = (a_{ij}) \in M_{r(h+1)}(\mathbb{Z}_p)$ *and* $\psi : M_{r(h+1)}(\mathbb{Z}_p) \to End(1+J)$ *is a surjective ring homomorphism.*

*(iii)* $Aut(1+J) = GL_{(h+1)r}(\mathbb{Z}_p)$.

## 3.5 Counting the Automorphisms of $1 + J$ for both characteristics of $R$

### 3.5.1 For the characteristic of $R = p$

From Lemma 3.4.3, $Aut(1 + J) = GL_{hr}(\mathbb{Z}_p)$. Thus, we need to find all the elements of $GL_{hr}(\mathbb{Z}_p)$ that can be extended to a matrix in $End(1 + J)$ and calculate the distinct ways of extending such an element to an endomorphism. So, we need all such matrices $M_{hr}(\mathbb{Z}_p) \in End(1+J)$ that are invertible modulo $p$.

Now, recall that $(1+J) = (\mathbb{Z}_p^r)^h$ and define the following numbers:

$$\alpha_k = max\{m : e_m = e_k\} \; and \; \beta_k = min\{m : e_m = e_k\}. \tag{3.7}$$

Since $e_m = e_k$ for $m = k$, we have the two inequalities $\alpha_k \geq k$ and $\beta_k \leq k$.

Note that $\beta_1 = \beta_2 = \cdots = \beta_{\alpha_1}$ and since $e_1 = e_2 = \cdots = e_n = e_{hr} = 1$, it follows that $n = hr$ and $\alpha_k$ coincides with $\beta_k$ for all the values of $k$.

### 3.5.2 For the characteristic of $R = p^2$

Similarly, since $(1+J) = (\mathbb{Z}_p^r)^{h+1}$ , we define the numbers:

$$\alpha_k = max\{m : e_m = e_k\}, \beta_k = min\{m : e_m = e_k\}$$

Since $e_m = e_k$ for $m = k$, we have the two inequalities $\alpha_k \geq k$ and $\beta_k \leq k$

Note that $\beta_1 = \beta_2 = \cdots = \beta_{\alpha_1}$ and since $e_1 = e_2 = \cdots = e_n = e_{(h+1)r} = 1$, it follows that $n = (h+1)r$ and $\alpha_k$ coincides with $\beta_k$ for all the values of $k$.

Now, for both of the considerations, the number of matrices say $A \in R_p$ that are invertible modulo $p$ are upper block triangular matrices which may be expressed in the following forms:

$$A = \begin{pmatrix} m_{11} & m_{12} & \cdots & m_{1(hr)} \\ \vdots & & & \\ m_{\alpha_1 1} & & & \\ & m_{\alpha_2 2} & & \\ & & \ddots & \\ 0 & & & m_{\alpha_{(hr)} hr} \end{pmatrix} = \begin{pmatrix} m_{1\beta_1} & & & & \\ & m_{2\beta_2} & & & \\ & & \ddots & & \\ 0 & & & m_{(hr)\beta_{(hr)}} & \cdots & m_{(hr)(hr)} \end{pmatrix}$$

for $char(R) = p$ and

$$A = \begin{pmatrix} m_{11} & m_{12} & \cdots & m_{1((h+1)r)} \\ \vdots & & & \\ m_{\alpha_1 1} & & & \\ & m_{\alpha_2 2} & & \\ & & \ddots & \\ 0 & & & m_{\alpha_{((h+1)r))}((h+1)r)} \end{pmatrix}$$

$$= \begin{pmatrix} m_{1\beta_1} & & & & \\ & m_{2\beta_2} & & & \\ & & \ddots & & \\ 0 & & & m_{(h+1)r)\beta_{((h+1)r)}} & \cdots & m_{((h+1)r)((h+1)r)} \end{pmatrix}$$

for $char(R) = p^2$.

The number of such $A$ is $\prod_{k=1}^{hr}(p^{\alpha_k} - p^{k-1})$ for $char(R) = p$ and $\prod_{k=1}^{(h+1)r}(p^{\alpha_k} - p^{k-1})$ for $char(R) = p^2$ since we require linearly independent columns. Thus when char$(R) = p$, the abelian group $(1 + J) = (\mathbb{Z}_p^r)^h$ has $\mid Aut(1 + J) \mid = \prod_{k=1}^{hr}(p^{\alpha_k} - p^{k-1})$ and when char$(R) = p^2$, the abelian group $1 + J = (\mathbb{Z}_p^r)^{h+1}$ has $\mid Aut(1 + J) \mid = \prod_{k=1}^{(h+1)r}(p^{\alpha_k} - p^{k-1})$. The results below follow:

**Theorem 3.5.1.** *The structure of the automorphisms of the unit groups $R^*$ of the commutative completely primary finite ring of characteristics p and $p^2$ with Jacobson radical $J$ such that $J^2 = (0)$ and with invariants p (prime integer), $p \in J, r \geq 1$ and $h \geq 1$ is a direct product of the units of $\mathbb{Z}_{p^r-1}$ and the general linear group whose dimension is the rank of $1 + J$ as follows:*

*(i) When the characteristic of R equals p, then,*

$$Aut(R^*) \cong (\mathbb{Z}_{p^r-1})^* \times GL_{hr}(\mathbb{F}_p).$$

*(ii) When the characteristic of $R = p^2$, then,*

$$Aut(R^*) \cong (\mathbb{Z}_{p^r-1})^* \times GL_{(h+1)r}(\mathbb{F}_p).$$

**Theorem 3.5.2.** *The order of the automorphisms of the unit groups $R^*$ of the commut-*

*ative completely primary finite ring of characteristics $p$ and $p^2$ with Jacobson radical $J$ such that $J^2 = (0)$ and with invariants $p$ (prime integer),$p \in J, r \geq 1$ and $h \geq 1$ is characterized as follows:*

*(i)When the characteristic of $R$ equals $p$, then,*

$$| Aut(R^*) |= \varphi(p^r - 1) \cdot \prod_{k=1}^{hr} (p^{\alpha_k} - p^{k-1}).$$

*(ii) When the characteristic of $R = p^2$, then,*

$$| Aut(R^*) |= \varphi(p^r - 1) \cdot \prod_{k=1}^{(h+1)r} (p^{\alpha_k} - p^{k-1}).$$

### 3.6 Unit Groups of Cube Radical Zero Commutative Completely Primary finite rings

Let $R$ be a commutative completely primary finite ring with maximal ideal $J$ such that $J^3 = (0)$ and $J^2 \neq (0)$. The detailed constructions describing these rings for each characteristic $p$, $p^2$ and $p^3$ are well known (see for example in [23]). Further, $R/J \cong GF(p^r)$ and the characteristic of $R$ is $p^k$ where $1 \leq k \leq 3$. Let $R_0 = GR(p^{nr}, p^n)$ be a Galois subring of $R$, of order $p^{nr}$ and characteristic $p^n$. Then, the ring $R$ can be expressed as an additive abelian group $R = R_0 \oplus \sum_{i=1}^{h} R_0 m_i$ whose maximal ideal $J$ satisfies $J = pR_0 \oplus \sum_{i=1}^{h} R_0 m_i$.

Such a class of a ring expressed as $R = R_0 \oplus U \oplus V \oplus W$ has been constructed by Chickunji in [23], where it has been shown that the Jacobson radical J is of the form $J = pR_0 \oplus U \oplus V \oplus W$ where $U, V$ and $W$ are finitely generated $R_0-$modules . The structure of $R$ was characterized by the invariants $p, n, r, d, s, t$ and $\lambda$, where $p$ is a prime integer, $d$ is the number of generators whose order is different from $p$, and $n$, $r$ are positive integers, $s$, $t$, $\lambda$ are the generators of the sets $U$, $V$, $W$ respectively, and the linearly independent matrices $(\alpha_{ij}^k)$ defined in the multiplication. Moreover, in [28], $d \geq 0$ denotes the number of the sets $\{m_1, ..., m_h\}$ with $pm_h \neq 0$. Similarly, It is considered that $s, t, \lambda$ are the numbers in the generating sets for the $R_0-$modules $U, V, W$ respectively.

In [24], the author determined the unit groups $R^*$ of the ring $R$ when $s = 2$, $t = 1$,

$\lambda = 0$ and the characteristic of $R$ is $p$; and when $t = \frac{s(s+1)}{2}$, $\lambda = 0$ for a fixed integer $s$ for all the characteristics of $R$. In [25], the author obtained the structure of $R^*$ when $s = 2, t = 1, \lambda = 0$ and the characteristic of $R$ is $p^2$ and $p^3$; and the case when $s = 2, t = 2, \lambda = 0$ and the characteristic of $R$ is $p$. In both [24, 25], it was assumed that $\lambda = 0$ so that the annihilator of the maximal ideal $J$ coincides with $J^2$.

It has been shown in [26] that $1+J$ is a direct product of its subgroups $1+pR_0 \oplus U \oplus V$ and $1+W$ and further, the structure of $1+W$ determined in general. The structure of $R^*$ has been determined when $s = 3, t = 1, \lambda \geq 1$ and $\text{char}(R) = p$. A generalization of the structure of $R^*$ in the case when $s = 2, t = 1, t = \frac{s(s+1)}{2}$ for a fixed integer $s$ and for all the characteristics of $R$ has been done, and when $s = 2, t = 2$ and $\text{char}((R) = p)$ determined in [24, 25] to the case when the $ann(J) = J^2 + W$ so that $\lambda \geq 1$. This complements the solution to the problem in the case when $ann(J) = J^2$.

Notice that since $R$ is of order $p^{nr}$ and $R^* = R - J$, it is easy to see that $\mid R^* \mid = p^{(n-1)r}(p^r - 1)$ and $\mid (1+J) \mid = p^{(n-1)r}$ so that $(1+J)$ is an *abelian* $p-$*group*. Thus, since $R$ is commutative,

$$R^* = < b > .(1+J) \cong < b > \times (1+J).$$

a direct product of the $p-$group $(1+J)$ by the cyclic subgroup $< b >$.

### 3.6.1 The Structure of $1+J$

Chikunji [23] has given the structure of $1+W$, a form of $1+J$ of the completely primary finite ring $R = R_0 \oplus U \oplus U \oplus W$ where $R_0 = GR(p^{kr}, p^k)$ $(1 \leq k \leq 3)$, $s, t, \lambda \in \mathbb{Z}^+$ are numbers in the generating sets $\{u_1, ..., u_s\}$, $\{v_1, ..., v_t\}$, and $\{w_1, ..., w_\lambda\}$, for finitely generated $R_0-$ modules $U, V, W$ respectively, where $t \leq \frac{s(s+1)}{2}$ and $\lambda \geq 1$. It was established that,

$$R = R_0 \oplus \sum_{i=1}^{s} R_0 u_i \oplus \sum_{j=1}^{t} R_0 v_j \oplus \sum_{k=1}^{\lambda} R_0 w_k,$$

$$J = pR_0 \oplus \sum_{i=1}^{s} R_0 u_i \oplus \sum_{j=1}^{t} R_0 v_j \oplus \sum_{k=1}^{\lambda} R_0 w_k,$$

$$ann(J) = pR_0 \oplus \sum_{j=1}^{t} R_0 v_j \oplus \sum_{k=1}^{\lambda} R_0 w_k,$$

or

$$ann(J) = p^2 R_0 \oplus \sum_{j=1}^{t} R_0 v_j \oplus \sum_{k=1}^{\lambda} R_0 w_k,$$

$$J^2 = pR_0 \oplus \sum_{j=1}^{t} R_0 v_j,$$

or

$$J^2 = p^2 R_0 \oplus \sum_{j=1}^{t} R_0 v_j,$$

and $J^3 = (0)$. Hence

$$1 + J = 1 + pR_0 \oplus \sum_{i=1}^{s} R_0 u_i \oplus \sum_{j=1}^{t} R_0 v_j \oplus \sum_{k=1}^{\lambda} R_0 w_k.$$

The following results were found to be vital in determining the structure of $1 + J$.

**Proposition 3.6.1.** *[23] If $\lambda \geq 1$, then $1 + \sum_{i=1}^{\lambda} \oplus R_0 w_i$ is a subgroup of $1 + J$.*

**Corollary 3.6.1.** *[23] $1 + ann(J)$ is a subgroup of $1 + J$.*

The following results were given in [23] in order to simplify most of the work in the sequel;

**Proposition 3.6.2.** *The $p-$group $1 + J$ is a direct product of the subgroups $1 + pR_0 \oplus \sum_{i=1}^{s} R_0 u_i \oplus \sum_{j=1}^{t} R_0 v_j$ by $1 + \sum_{k=1}^{\lambda} R_0 w_k$.*

Since the structure of $1+pR_0 \oplus \sum_{i=1}^{s} R_0 u_i \oplus \sum_{j=1}^{t} R_0 v_j$ for $s = 2, t = 1; s = 2, t = 2$ and $\text{char}(R) = p$ and $t = \frac{s(s+1)}{2}$ for a fixed $s$, have been determined in [24, 25], the structure of $1 + W = 1 + \sum_{i=1}^{\lambda} w_i$ is sufficient, it is determined in [26] for every characteristic $p^k$, $(1 \leq k \leq 3)$. It is noted that $pw_i = 0$ for each $w_i \in W (i = 1, \cdots, \lambda)$, since $W \subseteq ann(J) = J^2 + W$. Thus:

**Proposition 3.6.3.** *The group $1 + W = 1 + \sum_{i=1}^{\lambda} w_i \cong \underbrace{\mathbb{Z}_p^r \times \cdots \times \mathbb{Z}_p^r}_{\lambda \geq 1}$ for any prime integer $p$ such that $charR = p^k$ $(1 \leq k \leq 3)$.*

The case when $\text{char}(R) = p$, $s = 3, t = 1$ and $\lambda \geq 1$ has also been considered in [26].

### 3.6.2 The Structure of the Unit Groups

As a result of the previous properties of $(1+J)$ and given that $R^* \cong \mathbb{Z}_{p^r-1} \times (1+J)$, the structure of the unit groups of cube radical zero commutative completely primary finite rings is characterized as follows:

**Theorem 3.6.1.** *(cf. [26])The unit group $R^*$ of a commutative completely primary finite ring $R$ with maximal ideal $J$ such that $J^3 = (0)$ and $J^2 \neq (0)$; and with the invariants $p, k, r, s, t$ and $\lambda \geq 1$ , is a direct product of cyclic groups as follows:*

*(i) If $s = 2, t = 1, \lambda \geq 1$ and char(R)=p, then*

$$R^* = \begin{cases} \mathbb{Z}_{2^r-1} \times \mathbb{Z}_4^r \times \mathbb{Z}_2^r \times (\mathbb{Z}_2^r)^\lambda, & \textit{or;} \\ \mathbb{Z}_{2^r-1} \times \mathbb{Z}_2^r \times \mathbb{Z}_2^r \times \mathbb{Z}_2^r \times (\mathbb{Z}_2^r)^\lambda, & \textit{if } p = 2; \\ \mathbb{Z}_{p^r-1} \times \mathbb{Z}_p^r \times \mathbb{Z}_p^r \times \mathbb{Z}_p^r \times (\mathbb{Z}_p^r)^\lambda, & \textit{if } p \neq 2. \end{cases}$$

*(ii)If $s = 2, t = 1, \lambda \geq 1$ and char(R)=$p^2$, then*

$$R^* = \begin{cases} \mathbb{Z}_{p^r-1} \times \mathbb{Z}_p^r \times \mathbb{Z}_p^r \times \mathbb{Z}_p^r \times \mathbb{Z}_p^r \times (\mathbb{Z}_p^r)^\lambda, & \textit{or;} \\ \mathbb{Z}_{p^r-1} \times \mathbb{Z}_p^r \times \mathbb{Z}_{p^2}^r \times \mathbb{Z}_{p^2}^r \times \mathbb{Z}_p^r \times (\mathbb{Z}_p^r)^\lambda, & \textit{if } p \neq 2. \end{cases}$$

*and if $p = 2$ then,*

$$R^* = \begin{cases} (\mathbb{Z}_2 \times \mathbb{Z}_2) \times (\mathbb{Z}_2 \times \mathbb{Z}_2) \times \mathbb{Z}_2 \times (\mathbb{Z}_2)^\lambda, & \textit{if } r = 1 \textit{ and } p \in J - ann(J); \\ \mathbb{Z}_{2^r-1} \times \mathbb{Z}_4^r \times \mathbb{Z}_4^r \times \mathbb{Z}_2^r \times (\mathbb{Z}_2^r)^\lambda, & \textit{if } r > 1 \textit{ and } p \in J - ann(J); \\ \mathbb{Z}_{2^r-1} \times \mathbb{Z}_4^r \times \mathbb{Z}_4^r \times (\mathbb{Z}_2^r)^\lambda, & \textit{or;} \\ \mathbb{Z}_{2^r-1} \times \mathbb{Z}_4^r \times \mathbb{Z}_2^r \times \mathbb{Z}_2^r \times (\mathbb{Z}_2^r)^\lambda, & \textit{if } p \in J^2; \\ \mathbb{Z}_{2^r-1} \times \mathbb{Z}_4^r \times \mathbb{Z}_2^r \times \mathbb{Z}_2^r \times (\mathbb{Z}_2^r)^\lambda, & \textit{or;} \\ \mathbb{Z}_{2^r-1} \times \mathbb{Z}_2^r \times \mathbb{Z}_2^r \times \mathbb{Z}_2^r \times (\mathbb{Z}_2^r)^\lambda, & \textit{if } p \in ann(J) - J^2. \end{cases}$$

*(iii)If $s = 2, t = 1, \lambda \geq 1$ and char(R)=$p^3$, then*

$$R^* = \begin{cases} \mathbb{Z}_{p^r-1} \times \mathbb{Z}_{p^2}^r \times \mathbb{Z}_p^r \times \mathbb{Z}_p^r \times \mathbb{Z}_p^r \times \mathbb{Z}_p^r \times (\mathbb{Z}_p^r)^\lambda, & \textit{or;} \\ \mathbb{Z}_{p^r-1} \times \mathbb{Z}_{p^2}^r \times \mathbb{Z}_{p^2}^r \times \mathbb{Z}_p^r \times \mathbb{Z}_p^r \times (\mathbb{Z}_p^r)^\lambda, & \textit{if } p \neq 2. \end{cases}$$

*and*

$$R^* = \begin{cases} \mathbb{Z}_{2^r-1} \times \mathbb{Z}_4^r \times \mathbb{Z}_4^r \times \mathbb{Z}_2^r \times (\mathbb{Z}_2^r)^\lambda, & \textit{or;} \\ \mathbb{Z}_{2^r-1} \times \mathbb{Z}_4^r \times \mathbb{Z}_2^r \times \mathbb{Z}_2^r \times \mathbb{Z}_2^r \times (\mathbb{Z}_2^r)^\lambda, & \textit{or;} \\ \mathbb{Z}_{2^r-1} \times \mathbb{Z}_4^r \times \mathbb{Z}_2^r \times \mathbb{Z}_2^r \times \mathbb{Z}_2^r \times \mathbb{Z}_2^r \times (\mathbb{Z}_2^r)^\lambda, & \textit{if } p = 2. \end{cases}$$

*(iv) If $s = 2, t = 2, \lambda \geq 1$ and char(R)=p, then*

$$R^* = \begin{cases} \mathbb{Z}_{p^r-1} \times \mathbb{Z}_p^r \times \mathbb{Z}_p^r \times \mathbb{Z}_p^r \times \mathbb{Z}_p^r \times (\mathbb{Z}_p^r)^\lambda, & \text{if } p \neq 2; \\ \mathbb{Z}_{2^r-1} \times \mathbb{Z}_4^r \times \mathbb{Z}_4^r \times (\mathbb{Z}_2^r)^\lambda, & \text{or;} \\ \mathbb{Z}_{2^r-1} \times \mathbb{Z}_4^r \times \mathbb{Z}_2^r \times \mathbb{Z}_2^r \times (\mathbb{Z}_2^r)^\lambda, & \text{if } p = 2. \end{cases}$$

*(v) If $t = s(s+1)/2, \lambda \geq 1$ for the various characteristics of $R$, then*

$$R^* = \begin{cases} \mathbb{Z}_{2^r-1} \times (\mathbb{Z}_4^r)^s \times (\mathbb{Z}_2^r)^\gamma \times (\mathbb{Z}_2^r)^\lambda, & \text{if } p = 2; \\ \mathbb{Z}_{p^r-1} \times (\mathbb{Z}_p^r)^s \times (\mathbb{Z}_p^r)^s \times (\mathbb{Z}_p^r)^\gamma \times (\mathbb{Z}_p^r)^\lambda, & \text{if } p \neq 2, \end{cases}$$

*for $Char(R) = p$.*

$$R^* = \begin{cases} \mathbb{Z}_{2^r-1} \times \mathbb{Z}_2^r \times (\mathbb{Z}_2^r)^s \times (\mathbb{Z}_2^r)^s \times (\mathbb{Z}_2^r)^\gamma \times (\mathbb{Z}_2^r)^\lambda, & \text{if } p = 2; \\ \mathbb{Z}_{p^r-1} \times \mathbb{Z}_p^r \times (\mathbb{Z}_p^r)^s \times (\mathbb{Z}_{p^2}^r)^s \times (\mathbb{Z}_p^r)^\gamma \times (\mathbb{Z}_p^r)^\lambda, & \text{if } p \neq 2, \end{cases}$$

*for $Char(R) = p^2$.*

$$R^* = \begin{cases} \mathbb{Z}_{2^r-1} \times \mathbb{Z}_2^r \times \mathbb{Z}_2 \times \mathbb{Z}_4^{r-1} \times (\mathbb{Z}_2^r)^s \times (\mathbb{Z}_4^r)^s \times (\mathbb{Z}_2^r)^\gamma \times (\mathbb{Z}_2^r)^\lambda, & \text{if } p = 2; \\ \mathbb{Z}_{p^r-1} \times \mathbb{Z}_{p^2}^r \times (\mathbb{Z}_p^r)^s \times (\mathbb{Z}_{p^2}^r)^s \times (\mathbb{Z}_p^r)^\gamma \times (\mathbb{Z}_p^r)^\lambda, & \text{if } p \neq 2. \end{cases}$$

*for $CharR = p^3$, where $\gamma = (s^2 - s)/2$.*

### 3.7 Automorphism Groups of the Units of Cube Radical Zero Commutative Completely Primary Finite Rings

We now characterize $Aut(R^*)$ by establishing the structure and order of the automorphism groups of the unit groups whose structures are given in the previous theorem. We pay keen attention to the particular cases and describe the set of matrices $R_p$ and endomorphisms $M = \psi(A)$ such that $A \in R_p$ and $\psi : R_p \to End(1+J)$ is a surjective ring homomorphism.

The following results are important in the sequel:

**Proposition 3.7.1.** *Let $1 + J \cong \mathbb{Z}_{p^{e_1}} \times \mathbb{Z}_{p^{e_2}}$ with $e_1 \leq e_2$. Then, the matrix $\begin{pmatrix} i & r \\ j & s \end{pmatrix}$ represents:*

*(i) An Endomorphism of $1 + J$ if and only if $i \in \mathbb{Z}_{p^{e_1}}$, $j \equiv 0 \mod (p^{e_1 - e_2})$, $r \in \mathbb{Z}_{p^{e_2}}$ and $s \in \mathbb{Z}_{p^{e_2}}$.*

*(ii) An Automorphism of $1 + J$ if and only if $i \in (\mathbb{Z}_{p^{e_1}})^*$, $j \equiv 0 \mod (p^{e_1 - e_2})$, $r \in \mathbb{Z}_{p^{e_2}}$ and $s \in (\mathbb{Z}_{p^{e_2}})'$.*

**Lemma 3.7.1.** *Let $R$ be a class of ring considered in this section and $1+J$ be a normal subgroup of its unit group $R^*$. The following conditions hold:*

*(i) The map $\psi : R_p \to End(1+J)$ acting on each column or row of $R_p$ is a surjective ring homomorphism.*

*(ii) Let $K$ be the set of matrices $A = (a_{ij})$ such that $p^{e_i - e_j} \mid a_{ij}$ for all $i, j$. This forms an ideal. The ideal $K$ is the kernel of $\psi$ and the endomorphism $M = \psi(A) \cong R_p/Ker\ \psi$.*

*(iii) The endomorphism $M = \psi(A)$ is an automorphism if and only if $A \mod p \in GL_n(\mathbb{F}_p)$.*

### 3.7.1 Endomorphisms of $1+J$ and their properties for all the characteristics of $R$

**Case 1:** If $s = 2, t = 1, \lambda \geq 1$ and char($R$)=$p$, then

$$1+J = \begin{cases} \mathbb{Z}_4^r \times \mathbb{Z}_2^r \times (\mathbb{Z}_2^r)^\lambda, & \text{or;} \\ \mathbb{Z}_2^r \times \mathbb{Z}_2^r \times \mathbb{Z}_2^r \times (\mathbb{Z}_2^r)^\lambda, & \text{if } p = 2; \\ \mathbb{Z}_p^r \times \mathbb{Z}_p^r \times \mathbb{Z}_p^r \times (\mathbb{Z}_p^r)^\lambda, & \text{if } p \neq 2. \end{cases}$$

**(a)** If $s = 2, t = 1, \lambda \geq 1$ and char($R$) $= 2$ and

$$1+J = \mathbb{Z}_4^r \times \mathbb{Z}_2^r \times (\mathbb{Z}_2^r)^\lambda = (\mathbb{Z}_2)^{r(\lambda+1)} \times \mathbb{Z}_4^r,$$

then, for $a_{ij} \in \mathbb{Z}_2$

$$R_2 = \left\{ \left( \begin{array}{cccccc} a_{11} & \cdots & a_{1(r(\lambda+1))} & a_{1(r(\lambda+1)+1)} & \cdots & a_{1(r(\lambda+2))} \\ a_{21} & \cdots & a_{2(r(\lambda+1))} & a_{2(r(\lambda+1)+1)} & \cdots & a_{2(r(\lambda+2))} \\ \vdots & & & & & \\ a_{(r(\lambda+1))1} & \cdots & a_{(r(\lambda+1))(r(\lambda+1))} & a_{(r(\lambda+1))(r(\lambda+1)+1)} & \cdots & a_{(r(\lambda+1))(r(\lambda+2))} \\ 2\,a_{(r(\lambda+1)+1)1} & \cdots & 2\,a_{(r(\lambda+1)+1)(r(\lambda+1))} & a_{(r(\lambda+1)+1)(r(\lambda+1)+1)} & \cdots & a_{(r(\lambda+1)+1)(r(\lambda+2))} \\ \vdots & & & & & \\ 2\,a_{(r(\lambda+2))1} & \cdots & 2\,a_{(r(\lambda+2))(r(\lambda+1))} & a_{(r(\lambda+2))(r(\lambda+1)+1)} & \cdots & a_{(r(\lambda+2))(r(\lambda+2))} \end{array} \right) \right\}.$$

**Proposition 3.7.2.** *If $s = 2, t = 1, \lambda \geq 1$ and char($R$) $= 2$ and $1+J = (\mathbb{Z}_2)^{r(\lambda+1)} \times \mathbb{Z}_4^r$, then,*

*(i) $R_2 = \{(a_{ij}) : 2^{e_i - e_j} \mid a_{ij} : 1 \leq j \leq i \leq r(\lambda+2)\} = M_{r(\lambda+2)}(\mathbb{Z}_2)$.*

*(ii)* $rank(1+J) = r(\lambda+2)$.

*(iii) For* $A \in R_2$ *and a surjective ring homomorphism* $\psi : R_2 \to ((\mathbb{Z}_2)^{r(\lambda+1)} \times \mathbb{Z}_{2^2}^r)$, $End((\mathbb{Z}_2)^{r(\lambda+1)} \times \mathbb{Z}_{2^2}^r) = \psi(A)$.

*(iv)* $Aut((\mathbb{Z}_2)^{r(\lambda+1)} \times \mathbb{Z}_{2^2}^r) = GL_{(r(\lambda+2))}(\mathbb{F}_2)$.

**(b)** or if $s = 2, t = 1, \lambda \geq 1$, $\text{char}(R) = p = 2$, then

$$1 + J = \mathbb{Z}_2^r \times \mathbb{Z}_2^r \times \mathbb{Z}_2^r \times (\mathbb{Z}_2^r)^\lambda = (\mathbb{Z}_2)^{r(\lambda+3)}.$$

So,

$$R_2 = \left\{ \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1(r+1)} & \cdots & a_{1(r(\lambda+3))} \\ a_{21} & a_{22} & \cdots & a_{2(r+1)} & \cdots & a_{2(r(\lambda+3))} \\ \vdots & & & & & \\ a_{(r)1} & a_{(r)2} & \cdots & a_{(r)(r+1)} & \cdots & a_{(r)(r(\lambda+3))} \\ a_{(r+1)1} & a_{(r+1)2} & \cdots & a_{(r+1)(r+1)} & \cdots & a_{(r+1)(r(\lambda+3))} \\ \vdots & & & & & \\ a_{(r(\lambda+3))1} & a_{(r(\lambda+3))2} & \cdots & a_{(r(\lambda+3)(r+1)} & \cdots & a_{(r(\lambda+3))(r(\lambda+3))} \end{pmatrix} ; a_{ij} \in \mathbb{Z}_2 \right\}.$$

**Proposition 3.7.3.** *If* $s = 2, t = 1, \lambda \geq 1$ *and* $char(R) = 2$ *and* $1 + J = (\mathbb{Z}_2)^{r(\lambda+3)}$, *then,*

*(i)* $R_2 = \{(a_{ij}) : 2^{e_i - e_j} \mid a_{ij} : 1 \leq j \leq i \leq r(\lambda+3)\} = M_{r(\lambda+3)}(\mathbb{Z}_2)$.

*(ii)* $rank(1+J) = r(\lambda+3)$.

*(iii) For* $A \in R_2$ *and a surjective ring homomorphism* $\psi : R_2 \to ((\mathbb{Z}_2)^{r(\lambda+3)})$, $End((\mathbb{Z}_2)^{r(\lambda+3)}) = \psi(A)$.

*(iv)* $Aut((\mathbb{Z}_2)^{r(\lambda+3)}) = GL_{(r(\lambda+3))}(\mathbb{F}_2)$.

**(c)** If $s = 2, t = 1, \lambda \geq 1$ and $\text{char}(R) = p \neq 2$, then,

$$1 + J = \mathbb{Z}_p^r \times \mathbb{Z}_p^r \times \mathbb{Z}_p^r \times (\mathbb{Z}_p^r)^\lambda = (\mathbb{Z}_p)^{r(\lambda+3)}.$$

In this case $a_{ij} \in \mathbb{Z}_p$ and

$$R_p = \left\{ \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1(r+1)} & \cdots & a_{1(r(\lambda+3))} \\ a_{21} & a_{22} & \cdots & a_{2(r+1)} & \cdots & a_{2(r(\lambda+3))} \\ \vdots & & & & & \\ a_{(r)1} & a_{(r)2} & \cdots & a_{(r)(r+1)} & \cdots & a_{(r)(r(\lambda+3))} \\ a_{(r+1)1} & a_{(r+1)2} & \cdots & a_{(r+1)(r+1)} & \cdots & a_{(r+1)(r(\lambda+3))} \\ \vdots & & & & & \\ a_{(r(\lambda+3))1} & a_{(r(\lambda+3))2} & \cdots & a_{(r(\lambda+3)(r+1)} & \cdots & a_{(r(\lambda+3))(r(\lambda+3))} \end{pmatrix} \right\}.$$

**Proposition 3.7.4.** *If $s = 2, t = 1, \lambda \geq 1$ and $char(R) = p \neq 2$ and $1 + J = (\mathbb{Z}_p)^{r(\lambda+3)}$, then,*

*(i) $R_p = \{(a_{ij}) : p^{e_i - e_j} \mid a_{ij} : 1 \leq j \leq i \leq r(\lambda+3)\} = M_{r(\lambda+3)}(\mathbb{Z}_p)$.*

*(ii) $rank(1 + J) = r(\lambda + 3)$.*

*(iii) For $A \in R_p$ and a surjective ring homomorphism $\psi : R_p \to ((\mathbb{Z}_p)^{r(\lambda+3)})$, $End((\mathbb{Z}_p)^{r(\lambda+3)}) = \psi(A)$.*

*(iv) $Aut((\mathbb{Z}_p)^{r(\lambda+3)}) = GL_{(r(\lambda+3))}(\mathbb{F}_p)$.*

**Case 2:** If $s = 2, t = 1, \lambda \geq 1$ and $\text{char}(R) = p^2$, then

$$1 + J = \begin{cases} \mathbb{Z}_p^r \times \mathbb{Z}_p^r \times \mathbb{Z}_p^r \times \mathbb{Z}_p^r \times (\mathbb{Z}_p^r)^\lambda, & \text{or;} \\ \mathbb{Z}_p^r \times \mathbb{Z}_{p^2}^r \times \mathbb{Z}_{p^2}^r \times \mathbb{Z}_p^r \times (\mathbb{Z}_p^r)^\lambda, & \text{if } p \neq 2. \end{cases}$$

If $p = 2$ then,

$$1 + J = \begin{cases} (\mathbb{Z}_2 \times \mathbb{Z}_2) \times (\mathbb{Z}_2 \times \mathbb{Z}_2) \times \mathbb{Z}_2 \times (\mathbb{Z}_2)^\lambda, & \text{if } r = 1 \text{ and } p \in J - ann(J); \\ \mathbb{Z}_4^r \times \mathbb{Z}_4^r \times \mathbb{Z}_2^r \times (\mathbb{Z}_2^r)^\lambda, & \text{if } r > 1 \text{ and } p \in J - ann(J); \\ \mathbb{Z}_4^r \times \mathbb{Z}_4^r \times (\mathbb{Z}_2^r)^\lambda, & \text{or;} \\ \mathbb{Z}_4^r \times \mathbb{Z}_2^r \times \mathbb{Z}_2^r \times (\mathbb{Z}_2^r)^\lambda, & \text{if } p \in J^2; \\ \mathbb{Z}_4^r \times \mathbb{Z}_2^r \times \mathbb{Z}_2^r \times (\mathbb{Z}_2^r)^\lambda, & \text{or;} \\ \mathbb{Z}_2^r \times \mathbb{Z}_2^r \times \mathbb{Z}_2^r \times (\mathbb{Z}_2^r)^\lambda, & \text{if } p \in ann(J) - J^2. \end{cases}$$

**(a)** If $s = 2, t = 1, \lambda \geq 1$ and $\text{char}(R) = p^2$, $p \neq 2$, then,

$$1 + J = \mathbb{Z}_p^r \times \mathbb{Z}_p^r \times \mathbb{Z}_p^r \times \mathbb{Z}_p^r \times (\mathbb{Z}_p^r)^\lambda = (\mathbb{Z}_p)^{r(\lambda+4)}.$$

Thus, for $a_{ij} \in \mathbb{Z}_p$

$$R_p = \left\{ \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1(r+1)} & \cdots & a_{1(r(\lambda+4))} \\ a_{21} & a_{22} & \cdots & a_{2(r+1)} & \cdots & a_{2(r(\lambda+4))} \\ \vdots & & & & & \\ a_{(r)1} & a_{(r)2} & \cdots & a_{(r)(r+1)} & \cdots & a_{(r)(r(\lambda+4))} \\ a_{(r+1)1} & a_{(r+1)2} & \cdots & a_{(r+1)(r+1)} & \cdots & a_{(r+1)(r(\lambda+4))} \\ \vdots & & & & & \\ a_{(r(\lambda+4))1} & a_{(r(\lambda+4))2} & \cdots & a_{(r(\lambda+4)(r+1)} & \cdots & a_{(r(\lambda+4))(r(\lambda+4))} \end{pmatrix} \right\}.$$

**Proposition 3.7.5.** *If $s = 2, t = 1, \lambda \geq 1$ and char$(R)$=$p^2$, $p \neq 2$ and $1 + J = (\mathbb{Z}_p)^{r(\lambda+4)}$,*

*(i) $R_p = \{(a_{ij}) : p^{e_i - e_j} \mid a_{ij} : 1 \leq j \leq i \leq r(\lambda + 4)\} = M_{r(\lambda+4)}(\mathbb{Z}_p)$.*

*(ii) $rank(1 + J) = r(\lambda + 4)$.*

*(iii) For $A \in R_p$ and a surjective ring homomorphism $\psi : R_p \to ((\mathbb{Z}_p)^{r(\lambda+4)})$, $End((\mathbb{Z}_p)^{r(\lambda+4)}) = \psi(A)$.*

*(iv) $Aut((\mathbb{Z}_p)^{r(\lambda+4)}) = GL_{(r(\lambda+4))}(\mathbb{F}_p)$.*

**(b)** If $s = 2, t = 1, \lambda \geq 1$ and char$(R)$=$p^2$, $p \neq 2$, then

$$1 + J = \mathbb{Z}_p^r \times \mathbb{Z}_{p^2}^r \times \mathbb{Z}_{p^2}^r \times \mathbb{Z}_p^r \times (\mathbb{Z}_p^r)^\lambda = (\mathbb{Z}_p)^{r(\lambda+2)} \times \mathbb{Z}_{p^2}^{2r},$$

and for $a_{ij} \in \mathbb{Z}_p$

$$R_p = \left\{ \begin{pmatrix} a_{11} & \cdots & a_{1(r(\lambda+2))} & a_{1(r(\lambda+2)+1)} & \cdots & a_{1(r(\lambda+4))} \\ a_{21} & \cdots & a_{2(r(\lambda+2))} & a_{2(r(\lambda+2)+1)} & \cdots & a_{2(r(\lambda+4))} \\ \vdots & & & & & \\ a_{(r(\lambda+2))1} & \cdots & a_{(r(\lambda+2))(r(\lambda+2))} & a_{(r(\lambda+2))(r(\lambda+2)+1)} & \cdots & a_{(r(\lambda+2))(r(\lambda+4))} \\ p\,a_{(r(\lambda+2)+1)1} & \cdots & p\,a_{(r(\lambda+2)+1)(r(\lambda+2))} & a_{(r(\lambda+2)+1)(r(\lambda+2)+1)} & \cdots & a_{(r(\lambda+2)+1)(r(\lambda+4))} \\ \vdots & & & & & \\ p\,a_{(r(\lambda+4))1} & \cdots & p\,a_{(r(\lambda+4))(r(\lambda+2))} & a_{(r(\lambda+4))(r(\lambda+2)+1)} & \cdots & a_{(r(\lambda+4))(r(\lambda+4))} \end{pmatrix} \right\}.$$

**Proposition 3.7.6.** *If $s = 2, t = 1, \lambda \geq 1$ and char$(R)$=$p^2$, $p \neq 2$, and $1+J = (\mathbb{Z}_p)^{r(\lambda+2)} \times \mathbb{Z}_{p^2}^{2r}$, then*

*(i) $R_p = \{(a_{ij}) : p^{e_i - e_j} \mid a_{ij} : 1 \leq j \leq i \leq r(\lambda + 4)\} = M_{r(\lambda+4)}(\mathbb{Z}_p)$.*

*(ii) $rank(1 + J) = r(\lambda + 4)$.*

*(iii) For $A \in R_p$ and a surjective ring homomorphism $\psi : R_p \to ((\mathbb{Z}_p)^{r(\lambda+2)} \times \mathbb{Z}_{p^2}^{2r})$, $End((\mathbb{Z}_p)^{r(\lambda+2)} \times \mathbb{Z}_{p^2}^{2r}) = \psi(A)$.*

*(iv) $Aut((\mathbb{Z}_p)^{r(\lambda+2)} \times \mathbb{Z}_{p^2}^{2r}) = GL_{(r(\lambda+4))}(\mathbb{F}_p)$.*

**(c)** If $s = 2, t = 1, \lambda \geq 1$ and char($R$)=$p^2$, $p = 2$ , $r = 1$ and $p \in J - ann(J)$, then

$$1 + J = (\mathbb{Z}_2 \times \mathbb{Z}_2) \times (\mathbb{Z}_2 \times \mathbb{Z}_2) \times \mathbb{Z}_2 \times (\mathbb{Z}_2)^{\lambda} = (\mathbb{Z}_2)^{5+\lambda},$$

and for $a_{ij} \in \mathbb{Z}_2$,

$$R_2 = \left\{ \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1(5+1)} & \cdots & a_{1(\lambda+5)} \\ a_{21} & a_{22} & \cdots & a_{2(5+1)} & \cdots & a_{2((\lambda+5))} \\ \vdots & & & & & \\ a_{(5)1} & a_{(5)2} & \cdots & a_{(5)(5+1)} & \cdots & a_{(5)(\lambda+5)} \\ a_{(5+1)1} & a_{(5+1)2} & \cdots & a_{(5+1)(5+1)} & \cdots & a_{(5+1)(\lambda+5)} \\ \vdots & & & & & \\ a_{(\lambda+5)1} & a_{(\lambda+5)2} & \cdots & a_{(\lambda+5)(5+1)} & \cdots & a_{(\lambda+5)(\lambda+5)} \end{pmatrix} \right\}.$$

**Proposition 3.7.7.** *If $s = 2, t = 1, \lambda \geq 1$, $p = 2$, char$(R)$=4, $r = 1$ and $p \in J - ann(J)$ and $1 + J = (\mathbb{Z}_2)^{5+\lambda}$, then*

*(i) $R_2 = \{(a_{ij}) : 2^{e_i - e_j} \mid a_{ij} : 1 \leq j \leq i \leq (\lambda + 5)\} = M_{(\lambda+5)}(\mathbb{Z}_2)$.*

*(ii) $rank(1 + J) = \lambda + 5$.*

*(iii) For $A \in R_2$ and a surjective ring homomorphism $\psi : R_2 \to ((\mathbb{Z}_2)^{5+\lambda})$, $End((\mathbb{Z}_2)^{5+\lambda}) = \psi(A)$.*

*(iv) $Aut((\mathbb{Z}_2)^{5+\lambda}) = GL_{(r(\lambda+5))}(\mathbb{F}_2)$.*

**(d)** If $s = 2, t = 1, \lambda \geq 1$ and char($R$)=4, $r > 1, p \in J - ann(J)$, then,

$$1 + J = \mathbb{Z}_4^r \times \mathbb{Z}_4^r \times \mathbb{Z}_2^r \times (\mathbb{Z}_2^r)^{\lambda} = (\mathbb{Z}_2)^{r(\lambda+1)} \times (\mathbb{Z}_4)^{2r},$$

and for $a_{ij} \in \mathbb{Z}_2$

$$R_2 = \left\{ \begin{pmatrix} a_{11} & \cdots & a_{1(r(\lambda+1))} & a_{1(r(\lambda+1)+1)} & \cdots & a_{1(r(\lambda+3))} \\ a_{21} & \cdots & a_{2(r(\lambda+1))} & a_{2(r(\lambda+1)+1)} & \cdots & a_{2(r(\lambda+3))} \\ \vdots & & & & & \\ a_{(r(\lambda+1))1} & \cdots & a_{(r(\lambda+1))(r(\lambda+1))} & a_{(r(\lambda+1))(r(\lambda+1)+1)} & \cdots & a_{(r(\lambda+1))(r(\lambda+3))} \\ 2\,a_{(r(\lambda+1)+1)1} & \cdots & 2\,a_{(r(\lambda+1)+1)(r(\lambda+1))} & a_{(r(\lambda+1)+1)(r(\lambda+1)+1)} & \cdots & a_{(r(\lambda+1)+1)(r(\lambda+3))} \\ \vdots & & & & & \\ 2\,a_{(r(\lambda+3))1} & \cdots & 2\,a_{(r(\lambda+3))(r(\lambda+1))} & a_{(r(\lambda+3))(r(\lambda+1)+1)} & \cdots & a_{(r(\lambda+3))(r(\lambda+3))} \end{pmatrix} \right\}.$$

**Proposition 3.7.8.** *If $s = 2, t = 1, \lambda \geq 1$ and $char(R) = 4$, $r > 1, p \in J - ann(J)$ and $1 + J = (\mathbb{Z}_2)^{r(\lambda+1)} \times (\mathbb{Z}_{2^2})^{2r}$,*

*(i) $R_2 = \{(a_{ij}) : 2^{e_i - e_j} \mid a_{ij} : 1 \leq j \leq i \leq r(\lambda+3)\} = M_{r(\lambda+3)}(\mathbb{Z}_2)$.*

*(ii) $rank(1 + J) = r(\lambda + 3)$.*

*(iii) For $A \in R_2$ and a surjective ring homomorphism $\psi : R_2 \to ((\mathbb{Z}_2)^{r(\lambda+1)} \times (\mathbb{Z}_{2^2})^{2r})$, $End((\mathbb{Z}_2)^{r(\lambda+1)} \times (\mathbb{Z}_{2^2})^{2r}) = \psi(A)$.*

*(iv) $Aut((\mathbb{Z}_2)^{r(\lambda+1)} \times (\mathbb{Z}_{2^2})^{2r}) = GL_{(r(\lambda+3))}(\mathbb{F}_2)$.*

**(e)** If $s = 2, t = 1, \lambda \geq 1$ and char($R$)=$p^2$, $p = 2, r > 1$, $p \in J - ann(J)$, then

$$1 + J = \mathbb{Z}_4^r \times \mathbb{Z}_4^r \times (\mathbb{Z}_2^r)^\lambda = (\mathbb{Z}_2)^{r\lambda} \times (\mathbb{Z}_4)^{2r},$$

and

$$R_2 = \left\{ \begin{pmatrix} a_{11} & \cdots & a_{1(r\lambda)} & a_{1(r\lambda+1)} & \cdots & a_{1(r(\lambda+2))} \\ a_{21} & \cdots & a_{2(r\lambda)} & a_{2(r\lambda+1)} & \cdots & a_{2(r(\lambda+2))} \\ \vdots & & & & & \\ a_{(r\lambda)1} & \cdots & a_{(r\lambda)(r\lambda)} & a_{(r\lambda)(r\lambda+1)} & \cdots & a_{(r\lambda)(r(\lambda+2))} \\ 2\,a_{(r\lambda)+1)1} & \cdots & 2\,a_{(r\lambda)+1)(r\lambda)} & a_{(r\lambda)+1)(r\lambda+1)} & \cdots & a_{((r\lambda)+1)(r(\lambda+2))} \\ \vdots & & & & & \\ 2\,a_{(r(\lambda+2))1} & \cdots & 2\,a_{(r(\lambda+2))(r\lambda)} & a_{(r(\lambda+2))(r\lambda+1)} & \cdots & a_{(r(\lambda+2))(r(\lambda+2))} \end{pmatrix} : a_{ij} \in \mathbb{Z}_2 \right\}.$$

**Proposition 3.7.9.** *If $s = 2, t = 1, \lambda \geq 1$ and char($R$)=4, $r > 1$, $p \in J - ann(J)$ and $1 + J = (\mathbb{Z}_2)^{r\lambda} \times (\mathbb{Z}_4)^{2r}$, then* *(i)* $R_2 = \{(a_{ij}) : 2^{e_i - e_j} \mid a_{ij} : 1 \leq j \leq i \leq r(\lambda+2)\} = M_{r(\lambda+2)}(\mathbb{Z}_2)$.

*(ii)* $rank(1+J) = r(\lambda+2)$.

*(iii) For* $A \in R_2$ *and a surjective ring homomorphism*

$$\psi : R_2 \to ((\mathbb{Z}_2)^{r\lambda} \times (\mathbb{Z}_4)^{2r}), End((\mathbb{Z}_2)^{r\lambda} \times (\mathbb{Z}_4)^{2r}) = \psi(A).$$

*(iv)* $Aut((\mathbb{Z}_2)^{r\lambda} \times (\mathbb{Z}_{2^2})^{2r}) = GL_{(r(\lambda+2))}(\mathbb{F}_2)$.

**(f)** If $s = 2, t = 1, \lambda \geq 1$ and char$(R)$=$p^2$, $p = 2 \in J^2$ then,

$$1 + J = \mathbb{Z}_4^r \times \mathbb{Z}_2^r \times \mathbb{Z}_2^r \times (\mathbb{Z}_2^r)^\lambda = (\mathbb{Z}_2)^{r(\lambda+2)} \times (\mathbb{Z}_4)^r,$$

and for $a_{ij} \in \mathbb{Z}_2$,

$$R_2 = \left\{ \begin{pmatrix} a_{11} & \cdots & a_{1(r(\lambda+2))} & a_{1(r(\lambda+2)+1)} & \cdots & a_{1(r(\lambda+3))} \\ a_{21} & \cdots & a_{2(r(\lambda+2))} & a_{2(r(\lambda+2)+1)} & \cdots & a_{2(r(\lambda+3))} \\ \vdots & & & & & \\ a_{(r(\lambda+2))1} & \cdots & a_{(r(\lambda+2))(r(\lambda+2))} & a_{(r(\lambda+2))(r(\lambda+2)+1)} & \cdots & a_{(r(\lambda+2))(r(\lambda+3))} \\ 2\,a_{(r(\lambda+2)+1)1} & \cdots & 2\,a_{(r(\lambda+2)+1)(r(\lambda+2))} & a_{(r(\lambda+2)+1)(r(\lambda+2)+1)} & \cdots & a_{(r(\lambda+2)+1)(r(\lambda+3))} \\ \vdots & & & & & \\ 2\,a_{(r(\lambda+3))1} & \cdots & 2\,a_{(r(\lambda+3))(r(\lambda+2))} & a_{(r(\lambda+3))(r(\lambda+2)+1)} & \cdots & a_{(r(\lambda+3))(r(\lambda+3))} \end{pmatrix} \right\}.$$

**Proposition 3.7.10.** *If* $s = 2, t = 1, \lambda \geq 1$ *and char*$(R)$=$p^2$, $p \in J^2$, $p = 2$ *and* $1 + J = (\mathbb{Z}_2)^{r(\lambda+2)} \times (\mathbb{Z}_4)^r$, *then*

*(i)* $R_2 = \{(a_{ij}) : 2^{e_i - e_j} \mid a_{ij},\ \forall i, j :\ 1 \leq j \leq i \leq r(\lambda+3)\} = M_{r(\lambda+3)}(\mathbb{Z}_2)$.

*(ii)* $rank(1+J) = r(\lambda+3)$.

*(iii) For* $A \in R_2$ *and a surjective ring homomorphism*

$$\psi : R_2 \to ((\mathbb{Z}_2)^{r(\lambda+2)} \times (\mathbb{Z}_4)^r), End((\mathbb{Z}_2)^{r(\lambda+2)} \times (\mathbb{Z}_4)^r) = \psi(A).$$

*(iv)* $Aut((\mathbb{Z}_2)^{r(\lambda+2)} \times (\mathbb{Z}_{2^2})^r) = GL_{(r(\lambda+3))}(\mathbb{F}_2)$.

**(g)** Or if $s = 2, t = 1, \lambda \geq 1$ and char($R$)=$p^2$, $p = 2$, $p \in (ann(J) - J^2)$, then

$$1 + J = \mathbb{Z}_4^r \times \mathbb{Z}_2^r \times \mathbb{Z}_2^r \times (\mathbb{Z}_2^r)^\lambda = (\mathbb{Z}_2)^{r(\lambda+2)} \times (\mathbb{Z}_4)^r,$$

and for all $a_{ij} \in \mathbb{Z}_2$,

$$R_2 = \left\{ \left( \begin{array}{cccccc} a_{11} & \cdots & a_{1(r(\lambda+2))} & a_{1(r(\lambda+2)+1)} & \cdots & a_{1(r(\lambda+3))} \\ a_{21} & \cdots & a_{2(r(\lambda+2))} & a_{2(r(\lambda+2)+1)} & \cdots & a_{2(r(\lambda+3))} \\ \vdots & & & & & \\ a_{(r(\lambda+2))1} & \cdots & a_{(r(\lambda+2))(r(\lambda+2))} & a_{(r(\lambda+2))(r(\lambda+2)+1)} & \cdots & a_{(r(\lambda+2))(r(\lambda+3))} \\ 2\,a_{(r(\lambda+2)+1)1} & \cdots & 2\,a_{(r(\lambda+2)+1)(r(\lambda+2))} & a_{(r(\lambda+2)+1)(r(\lambda+2)+1)} & \cdots & a_{(r(\lambda+2)+1)(r(\lambda+3))} \\ \vdots & & & & & \\ 2\,a_{(r(\lambda+3))1} & \cdots & 2\,a_{(r(\lambda+3))(r(\lambda+2))} & a_{(r(\lambda+3))(r(\lambda+2)+1)} & \cdots & a_{(r(\lambda+3))(r(\lambda+3))} \end{array} \right) \right\}.$$

**Proposition 3.7.11.** *If $s = 2, t = 1, \lambda \geq 1$ and char($R$)=$p^2$, $p \in J^2$, $p = 2$ and $1 + J = (\mathbb{Z}_2)^{r(\lambda+2)} \times (\mathbb{Z}_4)^r$, then*

*(i)* $R_2 = \{(a_{ij}) : 2^{e_i - e_j} \mid a_{ij} : 1 \leq j \leq i \leq r(\lambda+3)\} = M_{r(\lambda+3)}(\mathbb{Z}_2)$.

*(ii)* $rank(1 + J) = r(\lambda + 3)$.

*(iii) For $A \in R_2$ and a surjective ring homomorphism*

$$\psi : R_2 \to ((\mathbb{Z}_2)^{r(\lambda+2)} \times (\mathbb{Z}_{2^2})^r), End((\mathbb{Z}_2)^{r(\lambda+2)} \times (\mathbb{Z}_{2^2})^r) = \psi(A).$$

*(iv)* $Aut((\mathbb{Z}_2)^{r(\lambda+2)} \times (\mathbb{Z}_{2^2})^r) = GL_{(r(\lambda+3))}(\mathbb{F}_2)$.

**(h)** If $s = 2, t = 1, \lambda \geq 1$ and char($R$)=$p^2$, $p \in ann(J) - J^2$, then

$$1 + J = \mathbb{Z}_2^r \times \mathbb{Z}_2^r \times \mathbb{Z}_2^r \times (\mathbb{Z}_2^r)^\lambda = \mathbb{Z}_2^{r(\lambda+3)},$$

and for $a_{ij} \in \mathbb{Z}_2$,

$$R_2 = \left\{ \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1(r+1)} & \cdots & a_{1(r(\lambda+3))} \\ a_{21} & a_{22} & \cdots & a_{2(r+1)} & \cdots & a_{2(r(\lambda+3))} \\ \vdots & & & & & \\ a_{(r)1} & a_{(r)2} & \cdots & a_{(r)(r+1)} & \cdots & a_{(r)(r(\lambda+3))} \\ a_{(r+1)1} & a_{(r+1)2} & \cdots & a_{(r+1)(r+1)} & \cdots & a_{(r+1)(r(\lambda+3))} \\ \vdots & & & & & \\ a_{(r(\lambda+3))1} & a_{(r(\lambda+3))2} & \cdots & a_{(r(\lambda+3)(r+1)} & \cdots & a_{(r(\lambda+3))(r(\lambda+3))} \end{pmatrix} \right\}.$$

**Proposition 3.7.12.** *If $s = 2, t = 1, \lambda \geq 1$ and char$(R)$=$p^2$, $p \in ann(J) - J^2$, $p = 2$ and $1 + J = \mathbb{Z}_2^{r(\lambda+3)}$, then*

*(i) $R_2 = \{(a_{ij}) : 2^{e_i - e_j} \mid a_{ij} : \ 1 \leq j \leq i \leq r(\lambda + 3)\} = M_{r(\lambda+3)}(\mathbb{Z}_2)$.*

*(ii) $rank(1 + J) = r(\lambda + 3)$.*

*(iii) For $A \in R_2$ and a surjective ring homomorphism*

$$\psi : R_2 \to (\mathbb{Z}_2^{r(\lambda+3)}), End(\mathbb{Z}_2^{r(\lambda+3)}) = \psi(A).$$

*(iv) $Aut(\mathbb{Z}_2^{r(\lambda+3)}) = GL_{(r(\lambda+3))}(\mathbb{F}_2)$.*

**Case 3:** If $s = 2, t = 1, \lambda \geq 1$ and char$(R)$=$p^3$, then

$$1 + J = \begin{cases} \mathbb{Z}_{p^2}^r \times \mathbb{Z}_p^r \times \mathbb{Z}_p^r \times \mathbb{Z}_p^r \times \mathbb{Z}_p^r \times (\mathbb{Z}_p^r)^\lambda, & \text{or;} \\ \mathbb{Z}_{p^2}^r \times \mathbb{Z}_{p^2}^r \times \mathbb{Z}_p^r \times \mathbb{Z}_p^r \times (\mathbb{Z}_p^r)^\lambda, & \text{if } p \neq 2, \end{cases}$$

and

$$1 + J = \begin{cases} \mathbb{Z}_4^r \times \mathbb{Z}_4^r \times \mathbb{Z}_2^r \times (\mathbb{Z}_2^r)^\lambda, & \text{or;} \\ \mathbb{Z}_4^r \times \mathbb{Z}_2^r \times \mathbb{Z}_2^r \times \mathbb{Z}_2^r \times (\mathbb{Z}_2^r)^\lambda, & \text{or;} \\ \mathbb{Z}_4^r \times \mathbb{Z}_2^r \times \mathbb{Z}_2^r \times \mathbb{Z}_2^r \times \mathbb{Z}_2^r \times (\mathbb{Z}_2^r)^\lambda, & \text{if } p = 2. \end{cases}$$

**(a)** If $s = 2, t = 1, \lambda \geq 1$ and char$(R)$=$p^3$, $p \neq 2$, then

$$1 + J = \mathbb{Z}_{p^2}^r \times \mathbb{Z}_p^r \times \mathbb{Z}_p^r \times \mathbb{Z}_p^r \times \mathbb{Z}_p^r \times (\mathbb{Z}_p^r)^\lambda = (\mathbb{Z}_p)^{r(\lambda+4)} \times \mathbb{Z}_{p^2}^r,$$

and for $a_{ij} \in \mathbb{Z}_p$,

$$R_p = \left\{ \begin{pmatrix} a_{11} & \cdots & a_{1(r(\lambda+4))} & a_{1(r(\lambda+4)+1)} & \cdots & a_{1(r(\lambda+5))} \\ a_{21} & \cdots & a_{2(r(\lambda+4))} & a_{2(r(\lambda+4)+1)} & \cdots & a_{2(r(\lambda+5))} \\ \vdots & & & & & \\ a_{(r(\lambda+4))1} & \cdots & a_{(r(\lambda+4))(r(\lambda+4))} & a_{(r(\lambda+4))(r(\lambda+4)+1)} & \cdots & a_{(r(\lambda+4))(r(\lambda+5))} \\ p\,a_{(r(\lambda+4)+1)1} & \cdots & p\,a_{(r(\lambda+4)+1)(r(\lambda+4))} & a_{(r(\lambda+4)+1)(r(\lambda+4)+1)} & \cdots & a_{(r(\lambda+4)+1)(r(\lambda+5))} \\ \vdots & & & & & \\ p\,a_{(r(\lambda+5))1} & \cdots & p\,a_{(r(\lambda+5))(r(\lambda+4))} & a_{(r(\lambda+5))(r(\lambda+4)+1)} & \cdots & a_{(r(\lambda+5))(r(\lambda+5))} \end{pmatrix} \right\}.$$

**Proposition 3.7.13.** *If $s = 2, t = 1, \lambda \geq 1$ and char$(R)$=$p^3$, $p \neq 2$ and $1 + J = (\mathbb{Z}_p)^{r(\lambda+4)} \times \mathbb{Z}_{p^2}^r$, then*

*(i) $R_p = \{(a_{ij}) : p^{e_i - e_j} \mid a_{ij};\ 1 \leq j \leq i \leq r(\lambda+5)\} = M_{r(\lambda+5)}(\mathbb{Z}_p)$.*

*(ii) rank$(1 + J) = r(\lambda+5)$.*

*(iii) For $A \in R_p$ and a surjective ring homomorphism*

$$\psi : R_p \to ((\mathbb{Z}_p)^{r(\lambda+4)} \times \mathbb{Z}_{p^2}^r), End((\mathbb{Z}_p)^{r(\lambda+4)} \times \mathbb{Z}_{p^2}^r) = \psi(A).$$

*(iv) $Aut((\mathbb{Z}_p)^{r(\lambda+4)} \times \mathbb{Z}_{p^2}^r) = GL_{(r(\lambda+5))}(\mathbb{F}_p)$.*

**(b)** Or if $s = 2, t = 1, \lambda \geq 1$ and char$(R)$=$p^3$, $p \neq 2$, then

$$1 + J = \mathbb{Z}_{p^2}^r \times \mathbb{Z}_{p^2}^r \times \mathbb{Z}_p^r \times \mathbb{Z}_p^r \times (\mathbb{Z}_p^r)^\lambda = (\mathbb{Z}_p)^{r(\lambda+2)} \times (\mathbb{Z}_{p^2})^{2r},$$

and for $a_{ij} \in \mathbb{Z}_p$,

$$R_p = \left\{ \begin{pmatrix} a_{11} & \cdots & a_{1(r(\lambda+2))} & a_{1(r(\lambda+2)+1)} & \cdots & a_{1(r(\lambda+4))} \\ a_{21} & \cdots & a_{2(r(\lambda+2))} & a_{2(r(\lambda+2)+1)} & \cdots & a_{2(r(\lambda+4))} \\ \vdots & & & & & \\ a_{(r(\lambda+2))1} & \cdots & a_{(r(\lambda+2))(r(\lambda+2))} & a_{(r(\lambda+2))(r(\lambda+2)+1)} & \cdots & a_{(r(\lambda+2))(r(\lambda+4))} \\ p\,a_{(r(\lambda+2)+1)1} & \cdots & p\,a_{(r(\lambda+2)+1)(r(\lambda+2))} & a_{(r(\lambda+2)+1)(r(\lambda+2)+1)} & \cdots & a_{(r(\lambda+2)+1)(r(\lambda+4))} \\ \vdots & & & & & \\ p\,a_{(r(\lambda+4))1} & \cdots & pa_{(r(\lambda+4))(r(\lambda+2))} & a_{(r(\lambda+4))(r(\lambda+2)+1)} & \cdots & a_{(r(\lambda+4))(r(\lambda+4))} \end{pmatrix} \right\}.$$

**Proposition 3.7.14.** *If $s = 2, t = 1, \lambda \geq 1$ and char$(R)$=$p^3$, $p \neq 2$ and $1 + J = (\mathbb{Z}_p)^{r(\lambda+2)} \times (\mathbb{Z}_{p^2})^{2r}$,*

*(i) $R_p = \{(a_{ij}) : p^{e_i - e_j} \mid a_{ij};\ 1 \leq j \leq i \leq r(\lambda+4)\} = M_{r(\lambda+4)}(\mathbb{Z}_p)$.*

*(ii)* $rank(1+J) = r(\lambda+4)$.

*(iii) For* $A \in R_p$ *and a surjective ring homomorphism*

$$\psi : R_p \to ((\mathbb{Z}_p)^{r(\lambda+2)} \times (\mathbb{Z}_{p^2})^{2r}), End((\mathbb{Z}_p)^{r(\lambda+2)} \times (\mathbb{Z}_{p^2})^{2r}) = \psi(A).$$

*(iv)* $Aut((\mathbb{Z}_p)^{r(\lambda+2)} \times (\mathbb{Z}_{p^2})^{2r}) = GL_{(r(\lambda+4))}(\mathbb{F}_p)$.

**(c)** If $s = 2, t = 1, \lambda \geq 1$ and char$(R) = 8$, then

$$1 + J = \mathbb{Z}_4^r \times \mathbb{Z}_4^r \times \mathbb{Z}_2^r \times (\mathbb{Z}_2^r)^\lambda = (\mathbb{Z}_2)^{r(\lambda+1)} \times (\mathbb{Z}_4)^{2r},$$

and for $a_{ij} \in \mathbb{Z}_2$,

$$R_2 = \left\{ \begin{pmatrix} a_{11} & \cdots & a_{1(r(\lambda+1))} & a_{1(r(\lambda+1)+1)} & \cdots & a_{1(r(\lambda+3))} \\ a_{21} & \cdots & a_{2(r(\lambda+1))} & a_{2(r(\lambda+1)+1)} & \cdots & a_{2(r(\lambda+3))} \\ \vdots & & & & & \\ a_{(r(\lambda+1))1} & \cdots & a_{(r(\lambda+1))(r(\lambda+1))} & a_{(r(\lambda+1))(r(\lambda+1)+1)} & \cdots & a_{(r(\lambda+1))(r(\lambda+3))} \\ 2\,a_{(r(\lambda+1)+1)1} & \cdots & 2\,a_{(r(\lambda+1)+1)(r(\lambda+1))} & a_{(r(\lambda+1)+1)(r(\lambda+1)+1)} & \cdots & a_{(r(\lambda+1)+1)(r(\lambda+3))} \\ \vdots & & & & & \\ 2\,a_{(r(\lambda+3))1} & \cdots & 2\,a_{(r(\lambda+3))(r(\lambda+1))} & a_{(r(\lambda+3))(r(\lambda+1)+1)} & \cdots & a_{(r(\lambda+3))(r(\lambda+3))} \end{pmatrix} \right\}.$$

**Proposition 3.7.15.** *If* $s = 2, t = 1, \lambda \geq 1$ *and char*$(R)$=$p^3$, $p = 2$ *and* $1 + J = (\mathbb{Z}_2)^{r(\lambda+1)} \times (\mathbb{Z}_4)^{2r}$, *then*

*(i)* $R_2 = \{(a_{ij}) : 2^{e_i - e_j} \mid a_{ij};\ 1 \leq j \leq i \leq r(\lambda+3)\} = M_{r(\lambda+3)}(\mathbb{Z}_2)$.

*(ii)* $rank(1+J) = r(\lambda+3)$..

*(iii) For* $A \in R_2$ *and a surjective ring homomorphism*

$$\psi : R_2 \to ((\mathbb{Z}_2)^{r(\lambda+1)} \times (\mathbb{Z}_{2^2})^{2r}), End((\mathbb{Z}_2)^{r(\lambda+1)} \times (\mathbb{Z}_4)^{2r}) = \psi(A).$$

*(iv)* $Aut((\mathbb{Z}_2)^{r(\lambda+1)} \times (\mathbb{Z}_4)^{2r}) = GL_{(r(\lambda+3))}(\mathbb{F}_2)$.

**(d)** Or if $s = 2, t = 1, \lambda \geq 1$ and char$(R)$=$p^3$, $p = 2$, then

$$1 + J = \mathbb{Z}_4^r \times \mathbb{Z}_2^r \times \mathbb{Z}_2^r \times \mathbb{Z}_2^r \times (\mathbb{Z}_2^r)^\lambda = (\mathbb{Z}_2)^{r(\lambda+3)} \times (\mathbb{Z}_4)^r,$$

and for $a_{ij} \in \mathbb{Z}_2$,

$$R_2 = \left\{ \begin{pmatrix} a_{11} & \cdots & a_{1(r(\lambda+3))} & a_{1(r(\lambda+3)+1)} & \cdots & a_{1(r(\lambda+4))} \\ a_{21} & \cdots & a_{2(r(\lambda+3))} & a_{2(r(\lambda+3)+1)} & \cdots & a_{2(r(\lambda+4))} \\ \vdots & & & & & \\ a_{(r(\lambda+3))1} & \cdots & a_{(r(\lambda+3))(r(\lambda+3))} & a_{(r(\lambda+3))(r(\lambda+3)+1)} & \cdots & a_{(r(\lambda+3))(r(\lambda+4))} \\ 2\,a_{(r(\lambda+3)+1)1} & \cdots & 2\,a_{(r(\lambda+3)+1)(r(\lambda+3))} & a_{(r(\lambda+3)+1)(r(\lambda+3)+1)} & \cdots & a_{(r(\lambda+3)+1)(r(\lambda+4))} \\ \vdots & & & & & \\ 2\,a_{(r(\lambda+4))1} & \cdots & 2\,a_{(r(\lambda+4))(r(\lambda+3))} & a_{(r(\lambda+4))(r(\lambda+3)+1)} & \cdots & a_{(r(\lambda+4))(r(\lambda+4))} \end{pmatrix} \right\}.$$

**Proposition 3.7.16.** *If $s = 2, t = 1, \lambda \geq 1$ and char$(R)$=$p^3$, $p = 2$ and $1 + J = (\mathbb{Z}_2)^{r(\lambda+3)} \times (\mathbb{Z}_4)^r$, then*

*(i)* $R_2 = \{(a_{ij}) : 2^{e_i - e_j} \mid a_{ij};\ 1 \leq j \leq i \leq r(\lambda+4)\} = M_{r(\lambda+4)}(\mathbb{Z}_2)$.

*(ii)* $rank(1+J) = r(\lambda+4)$.

*(iii) For $A \in R_2$ and a surjective ring homomorphism*

$$\psi : R_2 \to ((\mathbb{Z}_2)^{r(\lambda+3)} \times (\mathbb{Z}_{2^2})^r), End((\mathbb{Z}_2)^{r(\lambda+3)} \times (\mathbb{Z}_{2^2})^r) = \psi(A).$$

*(iv)* $Aut((\mathbb{Z}_2)^{r(\lambda+3)} \times (\mathbb{Z}_4)^r) = GL_{(r(\lambda+4))}(\mathbb{F}_2)$.

**(e)** Or if $s = 2, t = 1, \lambda \geq 1$ and char$(R)$=$p^3$, $p = 2$, then,

$$1 + J = \mathbb{Z}_4^r \times \mathbb{Z}_2^r \times \mathbb{Z}_2^r \times \mathbb{Z}_2^r \times \mathbb{Z}_2^r \times (\mathbb{Z}_2^r)^\lambda = (\mathbb{Z}_2)^{r(\lambda+4)} \times (\mathbb{Z}_4)^r,$$

and for $a_{ij} \in \mathbb{Z}_2$,

$$R_2 = \left\{ \begin{pmatrix} a_{11} & \cdots & a_{1(r(\lambda+4))} & a_{1(r(\lambda+4)+1)} & \cdots & a_{1(r(\lambda+5))} \\ a_{21} & \cdots & a_{2(r(\lambda+4))} & a_{2(r(\lambda+4)+1)} & \cdots & a_{2(r(\lambda+5))} \\ \vdots & & & & & \\ a_{(r(\lambda+4))1} & \cdots & a_{(r(\lambda+4))(r(\lambda+4))} & a_{(r(\lambda+4))(r(\lambda+4)+1)} & \cdots & a_{(r(\lambda+4))(r(\lambda+5))} \\ 2\,a_{(r(\lambda+4)+1)1} & \cdots & 2\,a_{(r(\lambda+4)+1)(r(\lambda+4))} & a_{(r(\lambda+4)+1)(r(\lambda+4)+1)} & \cdots & a_{(r(\lambda+4)+1)(r(\lambda+5))} \\ \vdots & & & & & \\ 2\,a_{(r(\lambda+5))1} & \cdots & 2\,a_{(r(\lambda+5))(r(\lambda+4))} & a_{(r(\lambda+5))(r(\lambda+4)+1)} & \cdots & a_{(r(\lambda+5))(r(\lambda+5))} \end{pmatrix} \right\}.$$

**Proposition 3.7.17.** *If $s = 2, t = 1, \lambda \geq 1$ and char$(R) = 8$ and $1+J = (\mathbb{Z}_2)^{r(\lambda+4)} \times (\mathbb{Z}_4)^r$, then*

*(i)* $R_2 = \{(a_{ij}) : 2^{e_i - e_j} \mid a_{ij};\ 1 \leq j \leq i \leq r(\lambda+5)\} = M_{r(\lambda+5)}(\mathbb{Z}_2)$.

*(ii)* $rank(1+J) = r(\lambda+5)$.

*(iii) For $A \in R_2$ and a surjective ring homomorphism*

$$\psi : R_2 \to ((\mathbb{Z}_2)^{r(\lambda+4)} \times (\mathbb{Z}_4)^r), End((\mathbb{Z}_2)^{r(\lambda+4)} \times (\mathbb{Z}_4)^r) = \psi(A).$$

*(iv)* $Aut((\mathbb{Z}_2)^{r(\lambda+4)} \times (\mathbb{Z}_4)^r) = GL_{(r(\lambda+5))}(\mathbb{F}_2)$.

**Case 4:** If $s = 2, t = 2, \lambda \geq 1$ and char$(R)$=$p$,then

$$1 + J = \begin{cases} \mathbb{Z}_p^r \times \mathbb{Z}_p^r \times \mathbb{Z}_p^r \times \mathbb{Z}_p^r \times (\mathbb{Z}_p^r)^\lambda, & \text{if } p \neq 2; \\ \mathbb{Z}_4^r \times \mathbb{Z}_4^r \times (\mathbb{Z}_2^r)^\lambda, & \text{or;} \\ \mathbb{Z}_4^r \times \mathbb{Z}_2^r \times \mathbb{Z}_2^r \times (\mathbb{Z}_2^r)^\lambda, & \text{if } p = 2. \end{cases}$$

**(a)** If $s = 2, t = 2, \lambda \geq 1$ and char$(R)$=$p$, $p \neq 2$, then,

$$1 + J = \mathbb{Z}_p^r \times \mathbb{Z}_p^r \times \mathbb{Z}_p^r \times \mathbb{Z}_p^r \times (\mathbb{Z}_p^r)^\lambda = (\mathbb{Z}_p)^{r(\lambda+4)},$$

and for $a_{ij} \in \mathbb{Z}_p$,

$$R_p = \left\{ \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1(r+1)} & \cdots & a_{1(r(\lambda+4))} \\ a_{21} & a_{22} & \cdots & a_{2(r+1)} & \cdots & a_{2(r(\lambda+4))} \\ \vdots & & & & & \\ a_{(r)1} & a_{(r)2} & \cdots & a_{(r)(r+1)} & \cdots & a_{(r)(r(\lambda+4))} \\ a_{(r+1)1} & a_{(r+1)2} & \cdots & a_{(r+1)(r+1)} & \cdots & a_{(r+1)(r(\lambda+4))} \\ \vdots & & & & & \\ a_{(r(\lambda+4))1} & a_{(r(\lambda+4))2} & \cdots & a_{(r(\lambda+4)(r+1)} & \cdots & a_{(r(\lambda+4))(r(\lambda+4))} \end{pmatrix} \right\}.$$

**Proposition 3.7.18.** *If $s = 2, t = 2, \lambda \geq 1$ and char$(R) = p$, $p \neq 2$ and $1+J = (\mathbb{Z}_p)^{r(\lambda+4)}$, then*

*(i)* $R_p = \{(a_{ij}) : p^{e_i - e_j} \mid a_{ij};\ 1 \leq j \leq i \leq r(\lambda+4)\} = M_{r(\lambda+4)}(\mathbb{Z}_p)$.

*(ii)* $rank(1+J) = r(\lambda+4)$.

*(iii) For* $A \in R_p$ *and a surjective ring homomorphism*

$$\psi : R_p \to ((\mathbb{Z}_p)^{r(\lambda+4)}), End((\mathbb{Z}_p)^{r(\lambda+4)}) = \psi(A).$$

*(iv)* $Aut((\mathbb{Z}_p)^{r(\lambda+4)}) = GL_{(r(\lambda+4))}(\mathbb{F}_p)$.

**(b)** If $s = 2, t = 2, \lambda \geq 1$ and char($R$)=$p$, $p = 2$, then

$$1 + J = \mathbb{Z}_4^r \times \mathbb{Z}_4^r \times (\mathbb{Z}_2^r)^\lambda = (\mathbb{Z}_2)^{r\lambda} \times (\mathbb{Z}_4)^{2r},$$

and for $a_{ij} \in \mathbb{Z}_2$,

$$R_2 = \left\{ \begin{pmatrix} a_{11} & \cdots & a_{1(r\lambda)} & a_{1(r\lambda+1)} & \cdots & a_{1(r(\lambda+2))} \\ a_{21} & \cdots & a_{2(r\lambda)} & a_{2(r\lambda+1)} & \cdots & a_{2(r(\lambda+2))} \\ \vdots & & & & & \\ a_{(r\lambda)1} & \cdots & a_{(r\lambda)(r\lambda)} & a_{(r\lambda)(r\lambda+1)} & \cdots & a_{(r\lambda)(r(\lambda+2))} \\ 2\ a_{(r\lambda)+1)1} & \cdots & 2\ a_{(r\lambda)+1)(r\lambda)} & a_{(r\lambda)+1)(r\lambda+1)} & \cdots & a_{((r\lambda)+1)(r(\lambda+2))} \\ \vdots & & & & & \\ 2\ a_{(r(\lambda+2))1} & \cdots & 2\ a_{(r(\lambda+2))(r\lambda)} & a_{(r(\lambda+2))(r\lambda+1)} & \cdots & a_{(r(\lambda+2))(r(\lambda+2))} \end{pmatrix} \right\}.$$

**Proposition 3.7.19.** *If* $s = 2, t = 2, \lambda \geq 1$ *and char*$(R) = p$*,* $p = 2$ *and* $1 + J = (\mathbb{Z}_2)^{r\lambda} \times (\mathbb{Z}_4)^{2r}$*, then,*

*(i)* $R_2 = \{(a_{ij}) : 2^{e_i - e_j} \mid a_{ij};\ 1 \leq j \leq i \leq r(\lambda+2)\} = M_{r(\lambda+2)}(\mathbb{Z}_2)$.

*(ii)* $rank(1 + J) = r(\lambda + 2)$.

*(iii) For* $A \in R_2$ *and a surjective ring homomorphism*

$$\psi : R_2 \to ((\mathbb{Z}_2)^{r\lambda} \times (\mathbb{Z}_{2^2})^{2r}), End((\mathbb{Z}_2)^{r\lambda} \times (\mathbb{Z}_{2^2})^{2r}) = \psi(A).$$

*(iv)* $Aut((\mathbb{Z}_2)^{r\lambda} \times (\mathbb{Z}_{2^2})^{2r}) = GL_{(r(\lambda+2))}(\mathbb{F}_2)$.

**(c)** Or if $s = 2, t = 2, \lambda \geq 1$ and char($R$)=$p$, $p = 2$, then,

$$1 + J = \mathbb{Z}_4^r \times \mathbb{Z}_2^r \times \mathbb{Z}_2^r \times (\mathbb{Z}_2^r)^\lambda = (\mathbb{Z}_2)^{r(\lambda+2)} \times (\mathbb{Z}_4)^r,$$

and for $a_{ij} \in \mathbb{Z}_2$,

$$R_2 = \left\{ \begin{pmatrix} a_{11} & \cdots & a_{1(r(\lambda+2))} & a_{1(r(\lambda+2)+1)} & \cdots & a_{1(r(\lambda+3))} \\ a_{21} & \cdots & a_{2(r(\lambda+2))} & a_{2(r(\lambda+2)+1)} & \cdots & a_{2(r(\lambda+3))} \\ \vdots & & & & & \\ a_{(r(\lambda+2))1} & \cdots & a_{(r(\lambda+2))(r(\lambda+2))} & a_{(r(\lambda+2))(r(\lambda+2)+1)} & \cdots & a_{(r(\lambda+2))(r(\lambda+3))} \\ 2\,a_{(r(\lambda+2)+1)1} & \cdots & 2\,a_{(r(\lambda+2)+1)(r(\lambda+2))} & a_{(r(\lambda+2)+1)(r(\lambda+2)+1)} & \cdots & a_{(r(\lambda+2)+1)(r(\lambda+3))} \\ \vdots & & & & & \\ 2\,a_{(r(\lambda+3))1} & \cdots & 2\,a_{(r(\lambda+3))(r(\lambda+2))} & a_{(r(\lambda+3))(r(\lambda+2)+1)} & \cdots & a_{(r(\lambda+3))(r(\lambda+3))} \end{pmatrix} \right\}.$$

**Proposition 3.7.20.** *If $s = 2, t = 2, \lambda \geq 1$ and char$(R) = p$, $p = 2$ and $1 + J = (\mathbb{Z}_2)^{r(\lambda+2)} \times (\mathbb{Z}_4)^r$, then,*

*(i) $R_2 = \{(a_{ij}) : 2^{e_i - e_j} \mid a_{ij} : 1 \leq j \leq i \leq r(\lambda+3)\} = M_{r(\lambda+3)}(\mathbb{Z}_2)$.*

*(ii) rank$(1 + J) = r(\lambda + 3)$.*

*(iii) For $A \in R_2$ and a surjective ring homomorphism*

$$\psi : R_2 \to ((\mathbb{Z}_2)^{r(\lambda+2)} \times (\mathbb{Z}_4)^r), End((\mathbb{Z}_2)^{r(\lambda+2)} \times (\mathbb{Z}_{2^2})^r) = \psi(A).$$

*(iv) $Aut((\mathbb{Z}_2)^{r(\lambda+2)} \times (\mathbb{Z}_4)^r) = GL_{(r(\lambda+3))}(\mathbb{F}_2)$.*

**Case 5:** If $t = s(s+1)/2, \lambda \geq 1$ for the various characteristics of $R$, then

$$1 + J = \begin{cases} (\mathbb{Z}_4^r)^s \times (\mathbb{Z}_2^r)^\gamma \times (\mathbb{Z}_2^r)^\lambda, & \text{if } p = 2, \\ (\mathbb{Z}_p^r)^s \times (\mathbb{Z}_p^r)^s \times (\mathbb{Z}_p^r)^\gamma \times (\mathbb{Z}_p^r)^\lambda, & \text{if } p \neq 2, \end{cases}$$

for char$(R) = p$,

$$1 + J = \begin{cases} \mathbb{Z}_2^r \times (\mathbb{Z}_2^r)^s \times (\mathbb{Z}_2^r)^s \times (\mathbb{Z}_2^r)^\gamma \times (\mathbb{Z}_2^r)^\lambda, & \text{if } p = 2, \\ \mathbb{Z}_p^r \times (\mathbb{Z}_p^r)^s \times (\mathbb{Z}_{p^2}^r)^s \times (\mathbb{Z}_p^r)^\gamma \times (\mathbb{Z}_p^r)^\lambda, & \text{if } p \neq 2, \end{cases}$$

for char$(R) = p^2$.

$$1 + J = \begin{cases} \mathbb{Z}_2^r \times \mathbb{Z}_2 \times \mathbb{Z}_4^{r-1} \times (\mathbb{Z}_2^r)^s \times (\mathbb{Z}_4^r)^s \times (\mathbb{Z}_2^r)^\gamma \times (\mathbb{Z}_2^r)^\lambda, & \text{if } p = 2; \\ \mathbb{Z}_{p^2}^r \times (\mathbb{Z}_p^r)^s \times (\mathbb{Z}_{p^2}^r)^s \times (\mathbb{Z}_p^r)^\gamma \times (\mathbb{Z}_p^r)^\lambda, & \text{if } p \neq 2, \end{cases}$$

for char$(R) = p^3$, where $\gamma = (s^2 - s)/2$.

**(a)** If $t = s(s+1)/2, \lambda \geq 1$ for $\text{char}(R) = p$ and $p = 2$, then

$$1 + J = (\mathbb{Z}_4^r)^s \times (\mathbb{Z}_2^r)^\gamma \times (\mathbb{Z}_2^r)^\lambda = (\mathbb{Z}_2)^{r(\lambda+\gamma)} \times (\mathbb{Z}_4)^{rs}$$

where $\gamma = (s^2 - s)/2$, and for $a_{ij} \in \mathbb{Z}_2$,

$$R_2 = \left\{ \begin{pmatrix} a_{11} & \cdots & a_{1(r(\lambda+\gamma))} & a_{1(r(\lambda+\gamma)+1)} & \cdots & a_{1(r(\lambda+\gamma+s))} \\ a_{21} & \cdots & a_{2(r(\lambda+\gamma))} & a_{2(r(\lambda+\gamma)+1)} & \cdots & a_{2(r(\lambda+\gamma+s))} \\ \vdots & & & & & \\ a_{(r(\lambda+\gamma))1} & \cdots & a_{(r(\lambda+\gamma))(r(\lambda+\gamma))} & a_{(r(\lambda+\gamma))(r(\lambda+\gamma)+1)} & \cdots & a_{(r(\lambda+\gamma))(r(\lambda+\gamma+s))} \\ 2\,a_{(r(\lambda+\gamma)+1)1} & \cdots & 2\,a_{(r(\lambda+\gamma)+1)(r(\lambda+\gamma))} & a_{(r(\lambda+\gamma)+1)(r(\lambda+\gamma)+1)} & \cdots & a_{(r(\lambda+\gamma)+1)(r(\lambda+\gamma+s))} \\ \vdots & & & & & \\ 2\,a_{(r(\lambda+\gamma+s))1} & \cdots & 2\,a_{(r(\lambda+\gamma+s))(r(\lambda+\gamma))} & a_{(r(\lambda+\gamma+s))(r(\lambda+\gamma)+1)} & \cdots & a_{(r(\lambda+\gamma+s))(r(\lambda+\gamma+s))} \end{pmatrix} \right\}.$$

**Proposition 3.7.21.** *If $t = s(s+1)/2, \lambda \geq 1$ for $\text{char}(R) = p$ and $p = 2$, $1 + J = (\mathbb{Z}_2)^{r(\lambda+\gamma)} \times (\mathbb{Z}_4)^{rs}$, where $\gamma = (s^2 - s)/2$, then*

*(i) $R_2 = \{(a_{ij}) : 2^{e_i - e_j} \mid a_{ij} : 1 \leq j \leq i \leq r(\lambda + \gamma + s)\} = M_{r(\lambda+\gamma+s)}(\mathbb{Z}_2)$.*

*(ii) $rank(1 + J) = r(\lambda + \gamma + s)$.*

*(iii) For $A \in R_2$ and a surjective ring homomorphism*

$$\psi : R_2 \to ((\mathbb{Z}_2)^{r(\lambda+\gamma)} \times (\mathbb{Z}_4)^{rs}), End((\mathbb{Z}_2)^{r(\lambda+\gamma)} \times (\mathbb{Z}_4)^{rs}) = \psi(A).$$

*(iv) $Aut((\mathbb{Z}_2)^{r(\lambda+\gamma)} \times (\mathbb{Z}_4)^{rs}) = GL_{(r(\lambda+\gamma+s)}(\mathbb{F}_2)$.*

**(b)** If $t = s(s+1)/2, \lambda \geq 1$ for $\text{char}(R) = p$ and $p \neq 2$, then,

$$1 + J = (\mathbb{Z}_p^r)^s \times (\mathbb{Z}_p^r)^s \times (\mathbb{Z}_p^r)^\gamma \times (\mathbb{Z}_p^r)^\lambda = \mathbb{Z}_p^{r(2s+\gamma+\lambda)},$$

where $\gamma = (s^2 - s)/2$ and for $a_{ij} \in \mathbb{Z}_p$,

$$R_p = \left\{ \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1(r+1)} & \cdots & a_{1(r(2s+\lambda+\gamma))} \\ a_{21} & a_{22} & \cdots & a_{2(r+1)} & \cdots & a_{2(r(2s+\lambda+\gamma))} \\ \vdots & & & & & \\ a_{(r)1} & a_{(r)2} & \cdots & a_{(r)(r+1)} & \cdots & a_{(r)(r(2s+\lambda+\gamma))} \\ a_{(r+1)1} & a_{(r+1)2} & \cdots & a_{(r+1)(r+1)} & \cdots & a_{(r+1)(r(2s+\lambda+\gamma))} \\ \vdots & & & & & \\ a_{(r(2s+\lambda+\gamma))1} & a_{(r(2s+\lambda+\gamma))2} & \cdots & a_{(r(2s+\lambda+\gamma)(r+1)} & \cdots & a_{(r(2s+\lambda+\gamma))(r(2s+\lambda+\gamma))} \end{pmatrix} \right\}.$$

**Proposition 3.7.22.** *If $t = s(s+1)/2, \lambda \geq 1$ for char$(R) = p$ and $p \neq 2$ and $1 + J = \mathbb{Z}_p^{r(2s+\gamma+\lambda)}$ where $\gamma = (s^2 - s)/2$, then*

*(i) $R_p = \{(a_{ij}) : p^{e_i - e_j} \mid a_{ij};\ 1 \leq j \leq i \leq r(2s+\lambda+\gamma)\} = M_{r(2s+\lambda+\gamma)}(\mathbb{Z}_p)$.*

*(ii) $rank(1+J) = r(2s+\lambda+\gamma)$.*

*(iii) For $A \in R_p$ and a surjective ring homomorphism*

$$\psi : R_p \to (\mathbb{Z}_p^{r(2s+\gamma+\lambda)}), End(\mathbb{Z}_p^{r(2s+\gamma+\lambda)}) = \psi(A).$$

*(iv) $Aut(\mathbb{Z}_p^{r(2s+\gamma+\lambda)}) = GL_{(r(2s+\lambda+\gamma))}(\mathbb{F}_p)$.*

**(c)** If $t = s(s+1)/2, \lambda \geq 1$ for char$(R) = p^2$ and $p = 2$, then,

$$1 + J = \mathbb{Z}_2^r \times (\mathbb{Z}_2^r)^s \times (\mathbb{Z}_2^r)^s \times (\mathbb{Z}_2^r)^\gamma \times (\mathbb{Z}_2^r)^\lambda = \mathbb{Z}_2^{r(1+2s+\lambda+\gamma)},$$

where $\gamma = (s^2 - s)/2$, and for $a_{ij} \in \mathbb{Z}_2$,

$$R_2 = \left\{ \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1(r+1)} & \cdots & a_{1(r(1+2s+\lambda+\gamma))} \\ a_{21} & a_{22} & \cdots & a_{2(r+1)} & \cdots & a_{2(r(1+2s+\lambda+\gamma))} \\ \vdots & & & & & \\ a_{(r)1} & a_{(r)2} & \cdots & a_{(r)(r+1)} & \cdots & a_{(r)(r(1+2s+\lambda+\gamma))} \\ a_{(r+1)1} & a_{(r+1)2} & \cdots & a_{(r+1)(r+1)} & \cdots & a_{(r+1)(r(1+2s+\lambda+\gamma))} \\ \vdots & & & & & \\ a_{(r(1+2s+\lambda+\gamma))1} & a_{(r(1+2s+\lambda+\gamma))2} & \cdots & \cdots & \cdots & a_{(r(1+2s+\lambda+\gamma))(r(1+2s+\lambda+\gamma))} \end{pmatrix} \right\}.$$

**Proposition 3.7.23.** *If $t = s(s+1)/2, \lambda \geq 1$ for char$R = p^2$ and $p = 2$, $1 + J = \mathbb{Z}_2^{r(1+2s+\lambda+\gamma)}$, where $\gamma = (s^2 - s)/2$, then*

*(i) $R_2 = \{(a_{ij}) : 2^{e_i - e_j} \mid a_{ij} : 1 \leq j \leq i \leq r(1+2s+\lambda+\gamma)\} = M_{r(1+2s+\lambda+\gamma)}(\mathbb{Z}_2)$.*

*(ii) $rank(1+J) = r(1+2s+\lambda+\gamma)$.*

*(iii) For $A \in R_2$ and a surjective ring homomorphism*

$$\psi : R_2 \to (\mathbb{Z}_2^{r(1+2s+\lambda+\gamma)}), End(\mathbb{Z}_2^{r(1+2s+\lambda+\gamma)}) = \psi(A).$$

*(iv)* $Aut(\mathbb{Z}_2^{r(1+2s+\lambda+\gamma)}) = GL_{r(1+2s+\lambda+\gamma)}(\mathbb{F}_2)$.

**(d)** If $t = s(s+1)/2, \lambda \geq 1$ for char$R = p^2$ and $p \neq 2$ and $\gamma = (s^2-s)/2$,

$$1 + J = \mathbb{Z}_p^r \times (\mathbb{Z}_p^r)^s \times (\mathbb{Z}_{p^2}^r)^s \times (\mathbb{Z}_p^r)^\gamma \times (\mathbb{Z}_p^r)^\lambda = \mathbb{Z}_p^{r(1+s+\gamma+\lambda)} \times \mathbb{Z}_{p^2}^{rs}$$

and for all $a_{ij} \in \mathbb{Z}_p$,

$$R_p = \left\{ \begin{pmatrix} a_{11} & \cdots & a_{1(r(1+s+\gamma+\lambda))} & a_{1(r(1+\lambda+\gamma+2s))} \\ a_{21} & \cdots & a_{2(r(1+s+\gamma+\lambda))} & a_{2(r(1+\lambda+\gamma+2s))} \\ \vdots & & & \\ a_{(r(1+s+\lambda+\gamma))1} & \cdots & a_{(r(1+s+\lambda+\gamma))(r(1+s+\gamma+\lambda))} & a_{(r(1+s+\lambda+\gamma))(r(1+\lambda+\gamma+2s))} \\ p\,a_{(r(1+s+\lambda+\gamma)+1)1} & \cdots & p\,a_{(r(1+s+\lambda+\gamma)+1)(r(1+s+\gamma+\lambda))} & a_{(r(1+s+\lambda+\gamma)+1)(r(1+\lambda+\gamma+2s))} \\ \vdots & & & \\ p\,a_{(r(1+\lambda+\gamma+2s))1} & \cdots & p\,a_{(r(1+\lambda+\gamma+2s))(r(1+s+\gamma+\lambda))} & a_{(r(1+\lambda+\gamma+2s))(r(1+\lambda+\gamma+2s))} \end{pmatrix} \right\}.$$

**Proposition 3.7.24.** *If* $t = s(s+1)/2, \lambda \geq 1$ *for char*$(R) = p^2$ *and* $p \neq 2$, $1 + J = \mathbb{Z}_p^{r(1+s+\gamma+\lambda)} \times \mathbb{Z}_{p^2}^{rs}$ *where* $\gamma = (s^2-s)/2$, *then*

*(i)* $R_p = \{(a_{ij}) : p^{e_i - e_j} \mid a_{ij};\ 1 \leq j \leq i \leq r(1+2s+\lambda+\gamma)\} = M_{r(1+2s+\lambda+\gamma)}(\mathbb{Z}_p)$.

*(ii)* $rank(1+J) = r(1+2s+\lambda+\gamma)$.

*(iii) For* $A \in R_p$ *and a surjective ring homomorphism*

$$\psi : R_p \to (\mathbb{Z}_p^{r(1+s+\gamma+\lambda)} \times \mathbb{Z}_{p^2}^{rs}), End(\mathbb{Z}_p^{r(1+s+\gamma+\lambda)} \times \mathbb{Z}_{p^2}^{rs}) = \psi(A).$$

*(iv)* $Aut(\mathbb{Z}_p^{r(1+s+\gamma+\lambda)} \times \mathbb{Z}_{p^2}^{rs}) = GL_{r(1+2s+\lambda+\gamma)}(\mathbb{F}_p)$.

**(e)** If $t = s(s+1)/2, \lambda \geq 1$ for char$(R) = p^3$, $p = 2$ then

$$1 + J = \mathbb{Z}_2^r \times \mathbb{Z}_2 \times \mathbb{Z}_4^{r-1} \times (\mathbb{Z}_2^r)^s \times (\mathbb{Z}_4^r)^s \times (\mathbb{Z}_2^r)^\gamma \times (\mathbb{Z}_2^r)^\lambda = \mathbb{Z}_2^{r(1+s+\lambda+\gamma)+1} \times \mathbb{Z}_{2^2}^{r(1+s)-1},$$

where $\gamma = (s^2-s)/2$, and for $a_{ij} \in \mathbb{Z}_2$, $R_2 =$

$$\left\{\left(\begin{array}{ccc} a_{11} & a_{1(r(1+s+\lambda+\gamma)+1)} & a_{1(r(2+2s+\lambda+\gamma))} \\ a_{21} & a_{2(r(1+s+\lambda+\gamma)+1)} & a_{2(r(2+2s+\lambda+\gamma))} \\ \vdots & & \\ a_{(r(1+s+\lambda+\gamma)+1)1} & a_{(r(1+s+\lambda+\gamma)+1)(r(1+s+\lambda+\gamma)+1)} & a_{(r(1+s+\lambda+\gamma)+1)(r(2+2s+\lambda+\gamma))} \\ 2\,a_{((r(1+s+\lambda+\gamma)+1)+1)1} & 2\,a_{(r(1+s+\lambda+\gamma)+1)+1)(r(1+s+\lambda+\gamma)+1)} & a_{((r(1+s+\lambda+\gamma)+1)+1)(r(2+2s+\lambda+\gamma))} \\ \vdots & & \\ 2\,a_{(r(2+2s+\lambda+\gamma))1} & 2\,a_{(r(2+2s+\lambda+\gamma))(r(1+s+\lambda+\gamma)+1)} & a_{(r(2+2s+\lambda+\gamma))(r(2+2s+\lambda+\gamma))} \end{array}\right)\right\}.$$

**Proposition 3.7.25.** *If $t = s(s+1)/2, \lambda \geq 1$ for char$(R) = p^3$, $p = 2$ and $1 + J = \mathbb{Z}_2^{r(1+s+\lambda+\gamma)+1} \times \mathbb{Z}_{2^2}^{r(1+s)-1}$, where $\gamma = (s^2 - s)/2$, then*

*(i) $R_2 = \{(a_{ij}) : 2^{e_i - e_j} \mid a_{ij};\ 1 \leq j \leq i \leq r(2 + 2s + \lambda + \gamma)\} = M_{r(2+2s+\lambda+\gamma)}(\mathbb{Z}_2)$.*

*(ii) rank$(1 + J) = r(2 + 2s + \lambda + \gamma)$.*

*(iii) For $A \in R_2$ and a surjective ring homomorphism*

$$\psi : R_2 \to (\mathbb{Z}_2^{r(1+s+\lambda+\gamma)+1} \times \mathbb{Z}_{2^2}^{r(1+s)-1}),\ End(\mathbb{Z}_2^{r(1+s+\lambda+\gamma)+1} \times \mathbb{Z}_{2^2}^{r(1+s)-1}) = \psi(A).$$

*(iv) $Aut(\mathbb{Z}_2^{r(1+s+\lambda+\gamma)+1} \times \mathbb{Z}_{2^2}^{r(1+s)-1}) = GL_{r(2+2s+\lambda+\gamma)}(\mathbb{F}_2)$.*

**(f)** If $t = s(s+1)/2, \lambda \geq 1$ for char$(R) = p^3$ and $p \neq 2$, then

$$1 + J = \mathbb{Z}_{p^2}^r \times (\mathbb{Z}_p^r)^s \times (\mathbb{Z}_{p^2}^r)^s \times (\mathbb{Z}_p^r)^\gamma \times (\mathbb{Z}_p^r)^\lambda = \mathbb{Z}_p^{r(s+\lambda+\gamma)} \times \mathbb{Z}_{p^2}^{r(1+s)},$$

where $\gamma = (s^2 - s)/2$, and for $a_{ij} \in \mathbb{Z}_p$,

$$R_p = \left\{\left(\begin{array}{ccccc} a_{11} & \cdots & a_{1(r(s+\lambda+\gamma))} & \cdots & a_{1(r(1+2s+\lambda+\gamma))} \\ a_{21} & \cdots & a_{2r(s+\lambda+\gamma)} & \cdots & a_{2(r(1+2s+\lambda+\gamma))} \\ \vdots & & & & \\ a_{(r(s+\lambda+\gamma)+1)1} & \cdots & a_{(r(s+\lambda+\gamma)+1)(r(s+\lambda+\gamma))} & \cdots & a_{(r(s+\lambda+\gamma)+1)(r(1+2s+\lambda+\gamma))} \\ p\,a_{((r(s+\lambda+\gamma)+1)+1)1} & \cdots & p\,a_{((r(s+\lambda+\gamma)+1)+1)(r(s+\lambda+\gamma))} & \cdots & a_{((r(s+\lambda+\gamma)+1)+1)(r(1+2s+\lambda+\gamma))} \\ \vdots & & & & \\ p\,a_{(r(1+2s+\lambda+\gamma))1} & \cdots & p\,a_{(r(1+2s+\lambda+\gamma))(r(s+\lambda+\gamma))} & \cdots & a_{(r(1+2s+\lambda+\gamma))(r(1+2s+\lambda+\gamma))} \end{array}\right)\right\}.$$

**Proposition 3.7.26.** *If $t = s(s+1)/2, \lambda \geq 1$ for char$(R) = p^3$ and $p \neq 2$ and $1 + J = \mathbb{Z}_p^{r(s+\lambda+\gamma)} \times \mathbb{Z}_{p^2}^{r(1+s)}$, where $\gamma = (s^2 - s)/2$, then,*

*(i) $R_p = \{(a_{ij}) : p^{e_i - e_j} \mid a_{ij}\ ;\ 1 \leq j \leq i \leq r(1 + 2s + \lambda + \gamma)\} = M_{r(1+2s+\lambda+\gamma)}(\mathbb{Z}_p)$.*

*(ii)* $rank(1+J) = r(1+2s+\lambda+\gamma)$.

*(iii) For* $A \in R_p$ *and a surjective ring homomorphism*

$$\psi : R_p \to (\mathbb{Z}_p^{r(s+\lambda+\gamma)} \times \mathbb{Z}_{p^2}^{r(1+s)}), End(\mathbb{Z}_p^{r(s+\lambda+\gamma)} \times \mathbb{Z}_{p^2}^{r(1+s)}) = \psi(A).$$

*(iv)* $Aut(\mathbb{Z}_p^{r(s+\lambda+\gamma)} \times \mathbb{Z}_{p^2}^{r(1+s)}) = GL_{r(1+2s+\lambda+\gamma)}(\mathbb{F}_p)$.

From the Propositions given above, the following Theorem summarizes the structure of $Aut(R^*)$ for all the cases considered:

**Theorem 3.7.1.** *The structure of the automorphisms* $Aut(R^*)$ *of the unit group* $R^*$ *of a commutative completely primary finite ring* $R$ *with maximal ideal* $J$ *such that* $J^3 = (0)$ *and* $J^2 \neq (0)$*; and with the invariants* $p, k, r, s, t$ *and* $\lambda \geq 1$ *, is a direct product as follows:*

*(i) If* $s = 2, t = 1, \lambda \geq 1$ *and char(R)=p, then*

$$Aut(R^*) \cong \begin{cases} (\mathbb{Z}_{2^r-1})^* \times GL_{(r(\lambda+2))}(\mathbb{F}_2), & \textit{or;} \\ (\mathbb{Z}_{2^r-1})^* \times GL_{(r(\lambda+3))}(\mathbb{F}_2), & \textit{if } p = 2; \\ (\mathbb{Z}_{p^r-1})^* \times GL_{(r(\lambda+3))}(\mathbb{F}_p), & \textit{if } p \neq 2. \end{cases}$$

*(ii)If* $s = 2, t = 1, \lambda \geq 1$ *and char(R)=*$p^2$*, then*

$$Aut(R^*) \cong \begin{cases} (\mathbb{Z}_{p^r-1})^* \times GL_{(r(\lambda+4))}(\mathbb{F}_p), & \textit{or;} \\ (\mathbb{Z}_{p^r-1})^* \times GL_{(r(\lambda+4))}(\mathbb{F}_p), & \textit{if } p \neq 2. \end{cases}$$

*and if* $p = 2$ *then,*

$$Aut(R^*) \cong \begin{cases} (\mathbb{Z}_{2^r-1})^* \times GL_{(\lambda+5)}(\mathbb{F}_2), & \textit{if } r = 1 \textit{ and } p \in J - ann(J); \\ (\mathbb{Z}_{2^r-1})^* \times GL_{(r(\lambda+3))}(\mathbb{F}_2), & \textit{if } r > 1 \textit{ and } p \in J - ann(J); \\ (\mathbb{Z}_{2^r-1})^* \times GL_{(r(\lambda+2))}(\mathbb{F}_2), & \textit{or;} \\ (\mathbb{Z}_{2^r-1})^* \times GL_{(r(\lambda+3))}(\mathbb{F}_2), & \textit{if } p \in J^2; \\ (\mathbb{Z}_{2^r-1})^* \times GL_{(r(\lambda+3))}(\mathbb{F}_2), & \textit{or;} \\ (\mathbb{Z}_{2^r-1})^* \times GL_{(r(\lambda+3))}(\mathbb{F}_2), & \textit{if } p \in ann(J) - J^2. \end{cases}$$

*(iii)If* $s = 2, t = 1, \lambda \geq 1$ *and char(R)=*$p^3$*, then*

$$Aut(R^*) \cong \begin{cases} (\mathbb{Z}_{p^r-1})^* \times GL_{(r(\lambda+5))}(\mathbb{F}_p), & \textit{or;} \\ (\mathbb{Z}_{p^r-1})^* \times GL_{(r(\lambda+4))}(\mathbb{F}_p), & \textit{if } p \neq 2. \end{cases}$$

*and*

$$Aut(R^*) \cong \begin{cases} (\mathbb{Z}_{2^r-1})^* \times GL_{(r(\lambda+3))}(\mathbb{F}_2), & \textit{or;} \\ (\mathbb{Z}_{2^r-1})^* \times GL_{(r(\lambda+4))}(\mathbb{F}_2), & \textit{or;} \\ (\mathbb{Z}_{2^r-1})^* \times GL_{(r(\lambda+5))}(\mathbb{F}_2), & \textit{if } p = 2. \end{cases}$$

*(iv) If $s = 2, t = 2, \lambda \geq 1$ and char(R)=p, then*

$$Au(R^*) \cong \begin{cases} (\mathbb{Z}_{p^r-1})^* \times GL_{(r(\lambda+4))}(\mathbb{F}_p), & \textit{if } p \neq 2; \\ (\mathbb{Z}_{2^r-1})^* \times GL_{(r(\lambda+2))}(\mathbb{F}_2), & \textit{or;} \\ (\mathbb{Z}_{2^r-1})^* \times GL_{(r(\lambda+3))}(\mathbb{F}_2), & \textit{if } p = 2. \end{cases}$$

*(v) If $t = s(s+1)/2, \lambda \geq 1$ for the various characteristics of R, then*

$$Aut(R^*) \cong \begin{cases} (\mathbb{Z}_{2^r-1})^* \times GL_{(r(\lambda+\gamma+s)}(\mathbb{F}_2), & \textit{if } p = 2; \\ (\mathbb{Z}_{p^r-1})^* \times GL_{(r(2s+\lambda+\gamma))}(\mathbb{F}_p), & \textit{if } p \neq 2, \end{cases}$$

*for char $(R) = p$,*

$$Aut(R^*) \cong \begin{cases} (\mathbb{Z}_{2^r-1})^* \times GL_{r(1+2s+\lambda+\gamma)}(\mathbb{F}_2), & \textit{if } p = 2; \\ (\mathbb{Z}_{p^r-1})^* \times GL_{r(1+2s+\lambda+\gamma)}(\mathbb{F}_p), & \textit{if } p \neq 2, \end{cases}$$

*for char$(R) = p^2$, and,*

$$Aut(R^*) \cong \begin{cases} (\mathbb{Z}_{2^r-1})^* \times GL_{r(2+2s+\lambda+\gamma)}(\mathbb{F}_2), & \textit{if } p = 2; \\ (\mathbb{Z}_{p^r-1})^* \times GL_{r(1+2s+\lambda+\gamma)}(\mathbb{F}_p), & \textit{if } p \neq 2. \end{cases}$$

*for char$(R) = p^3$, where $\gamma = (s^2 - s)/2$.*

### 3.7.2 Counting the Automorphisms of (1+J)

Since the structure of $Aut(1+J)$ is a general linear group $GL_{rk(1+J)}(\mathbb{F}_p)$, we need to count them:

**Definition 3.7.1.** *Let $\mathbb{F}$ be a field. Denote by $rk(1+J)$ the rank of $1+J$, then, a general linear group $GL_{rk(1+J)}(\mathbb{F})$ is the group of invertible $rk(1+J) \times rk(1+J)$ matrices with entries in $\mathbb{F}$ under matrix multiplication.*

Clearly, $GL_{rk(1+J)}(\mathbb{F})$ is a group because: matrix multiplication is associative, the identity element is $I_{rk(1+J)}$; the $rk(1+J) \times rk(1+J)$ matrix with $1'$s along the main diagonal and zeros elsewhere. If $a \in \mathbb{F}$, $a \neq 0$, then $a \cdot I_{rk(1+J)}$ is an invertible $rk(1+J) \times rk(1+J)$ matrix with inverse $a^{-1}I_{rk(1+J)\times rk(1+J)}$. In fact, the set of all such matrices forms a subgroup of $GL_{rk(1+J)}(\mathbb{F})$ that is isomorphic to $\mathbb{F}^{\times} = \mathbb{F} \setminus \{0\}$

For a prime $p$, $\mathbb{F}_p$ is a finite field in all the cases, thus, it is immediate that $GL_{rk(1+J)}(\mathbb{F}_p)$ has only finitely many elements. Now, suppose $rk(1+J) = 1$, then $GL_{rk(1+J)}(\mathbb{F}_p) \cong \mathbb{F}_p^{\times}$ has $p-1$ elements.

Let $rk(1+J) = 2$, and let $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Then for $M$ to be invertible, it is necessary and sufficient that $ad \neq bc$. If $a, b, c$ and $d$ are all nonzero, then, we can fix $a, b, c$ arbitrarily and $d$ can be anything but not $a^{-1}bc$. This gives us $(p-1)^3(p-2)$ matrices. If exactly one of the entries is 0, then the other three can be anything nonzero for a total of $4(p-1)^3$ matrices. Finally, if exactly two entries are 0, then, these entries must be opposite each other for the matrix to be invertible and the other two entries can be anything nonzero for a total of $2(p-1)^2$ matrices. So altogether we have:

$$(p-1)^3(p-2) + 4(p-1)^3 + 2(p-1)^2$$

$$= (p-1)^2((p-1)(p-2) + 4(p-1) + 2)$$

$$= (p-1)^2(p^2+p) = (p^2-1)(p^2-p).$$

**Claim 3.7.1.** *Evidently, calculating the size of $GL_{rk(1+J)}(\mathbb{F})$ by directly calculating the determinant, then, determining what values of the entries make the determinant nonzero is quite a tedious exercise and hence error prone. But one of the basic properties of determinants is that the determinant of a matrix is nonzero if and only if the rows of the matrix are linearly independent. Thus we have*

**Proposition 3.7.27.** *Let $rk(1+J) = n$ and $1+J = \underbrace{\mathbb{Z}_p \times \cdots \times \mathbb{Z}_p}_{n}$. The number of elements in $GL_n(\mathbb{F}_p)$ is $\prod_{k=0}^{n-1}(p^n - p^k)$.*

*Proof.* Notice that $e_1 = e_2 = \cdots e_{rk(1+J)} = 1$. We count the number of $n \times n$ matrices $A \in R_p$ whose rows are linearly independent. This is done by building the matrix $A$ from scratch. The first row can be anything other than the zero row, so, there are $p^n - 1$ possibilities. The second row must be linearly independent from the first row. Since there are $p$ multiples of the first row, there are $p^n - p$ possibilities for the second row. Generally, the $i^{th}$ row must be linearly independent from the first $i-1$ rows. There are $p^{i-1}$ linear combinations of the first $i-1$ rows, so, there are $p^n - p^{i-1}$ possibilities for the $i^{th}$ row. Once we build the entire matrix this way, we know that the rows are all linearly independent by choice. Also, we can build any $n \times n$ matrix whose rows are linearly independent in this fashion. Thus there have

$$(p^n - 1)(p^n - p)\cdots(p^n - p^{n-1}) = \prod_{k=0}^{n-1}(p^n - p^k)$$

matrices. $\square$

In order to be exhaustive for all the structures of $1+J$, we need to find all the elements of $GL_{rk(1+J)}(\mathbb{F}_p)$ that can be extended to matrices in $End(1+J)$ and calculate the distinct ways of extending such elements to endomorphisms.

We define the following numbers:

$$\alpha_k = max\{m : e_m = e_k\}, \beta_k = min\{m : e_m = e_k\}.$$

Since $e_m = e_k$ for $m = k$, we have the two inequalities $\alpha_k \geq k$ and $\beta_k \leq k$.

Note that $\beta_1 = \beta_2 = \cdots = \beta_{\alpha_1}$ , so we have $\beta_1 = \cdots = \beta_{\alpha_1} \leq \beta_{\alpha_1+1}$.

When $e_i = e_j = \cdots = e_{rk(1+J)}$, for all $i, j$ then it follows that $\alpha_k = \beta_k$.

Suppose the $e_i$ are different, we can introduce the numbers $e_i^{'}, c_i, d_i$ as follows: Define the set of distinct numbers $\{e_i^{'}\}$ such that $\{e_i^{'}\} = \{e_j\}$ and $e_1^{'} < e_2^{'} < \cdots$,

Let $l \in \mathbb{N}$ be the size of $\{e_i^{'}\}$. So, $e_1^{'} = e_1$, $e_2^{'} = e_{\alpha_1+1}, \cdots, e_l^{'} = e_n$. Now define

$$d_i = max\{m : e_m = e_i^{'}\}, c_i = min\{m : e_m = e_i^{'}\}.$$

Note that $c_1 = 1$, and $d_l = rk(1+J)$. Also, for convenience define $c_{l+1} = (rk(1+J)) + 1$.

Now, for both of the considerations, the number of matrices say $A \in R_p$ that are invertible modulo $p$ are upper block triangular matrices which may be expressed in any of the following three forms:

$$
A = \begin{pmatrix}
m_{11} & & & & & & & & * \\
\vdots & & & & & & & & \\
m_{d_1 1} & \cdots & m_{d_1 d_1} & & & & & & \\
 & & & m_{c_2 c_2} & & & & & \\
 & & & \vdots & & & & & \\
 & & & m_{d_2 c_2} & \cdots & m_{d_2 d_2} & & & \\
 & & & & & & \ddots & & \\
 & & & & & & & m_{c_l c_l} & \\
 & & & & & & & \vdots & \\
0 & & & & & & & m_{d_l c_l} \; \cdots & m_{d_l c_l}
\end{pmatrix}
$$

or

$$
A = \begin{pmatrix}
m_{11} & m_{12} & \cdots & m_{1(rk(1+J))} \\
\vdots & & & \\
m_{\alpha_1 1} & & & \\
 & m_{\alpha_2 2} & & \\
 & & \ddots & \\
0 & & & m_{\alpha_{(rk(1+J))}(rk(1+J))}
\end{pmatrix}
$$

$$
= \begin{pmatrix}
m_{1\beta_1} & & & & \\
 & m_{2\beta_2} & & & \\
 & & \ddots & & \\
0 & & & m_{(rk(1+J))\beta_{(rk(1+J))}} \; \cdots & m_{(rk(1+J))(rk(1+J))}
\end{pmatrix}
$$

The number of such $A$ is $\prod_{k=1}^{rk(1+J)}(p^{\alpha_k} - p^{k-1})$, since we require linearly independent columns. So, the first step of calculating $\mid Aut(1+J) \mid$ is done.

The second half of the computation is to count the number of extensions of $A$ to $Aut(1+J)$. To extend each entry $m_{ij}$ from $m_{ij} \in \mathbb{Z}/p\mathbb{Z}$ to $a_{ij} \in p^{e_i - e_j}\mathbb{Z}/p^{e_i}\mathbb{Z}$ if $e_i > e_j$, or $a_{ij} \in \mathbb{Z}/p^{e_i}\mathbb{Z}$ if $e_i \leq e_j$, such that $a_{ij} \equiv m_{ij} \mod p$, we have $p^{e_j}$ ways to do so for the necessary zeros (that is , when $e_i > e_j$) as any element of $p^{e_i - e_j}\mathbb{Z}/p^{e_i}\mathbb{Z}$ works.

Similarly, there are $p^{e_i - 1}$ ways for the not necessarily zero entries (that is , when $e_i \leq e_j$) as any element of $p\mathbb{Z}/p^{e_i}\mathbb{Z}$ will do.

Finally, the result below summarizes the order structures of the automorphism groups of the units $R^*$ of the cube radical zero commutative completely primary finite rings for all the characteristics of $R$.

**Theorem 3.7.2.** *The order of the automorphisms $Aut(R^*)$ of the unit group $R^*$ of a* *commutative completely primary finite ring $R$ with maximal ideal $J$ such that $J^3 = (0)$ and $J^2 \neq (0)$; and with the invariants $p, k, r, s, t$ and $\lambda \geq 1$ for all the characteristics of $R$ are as follows:*

*(i) If $s = 2, t = 1, \lambda \geq 1$ and char$(R)$=$p$, then* $\mid Aut(R^*) \mid =$

$$\begin{cases} \varphi(2^r-1)\cdot\prod_{k=1}^{r(\lambda+2)}(2^{\alpha_k}-2^{k-1})\prod_{j=1}^{r(\lambda+2)}(2^{e_j})^{r(\lambda+2)-\alpha_j}\prod_{i=1}^{r(\lambda+2)}(2^{e_i-1})^{r(\lambda+2)-\beta_i+1}, & \text{or;} \\ \varphi(2^r-1)\cdot\prod_{k=1}^{r(\lambda+3)}(2^{\alpha_k}-2^{k-1}), & \text{if } p=2; \\ \varphi(p^r-1)\cdot\prod_{k=1}^{r(\lambda+3)}(p^{\alpha_k}-p^{k-1}), & \text{if } p\neq 2. \end{cases}$$

*(ii)If $s = 2, t = 1, \lambda \geq 1$ and char$(R)$=$p^2$, then*

$$\begin{cases} \varphi(p^r-1)\cdot\prod_{k=1}^{r(\lambda+4)}(p^{\alpha_k}-p^{k-1}), & \text{or;} \\ \varphi(p^r-1)\cdot\prod_{k=1}^{r(\lambda+4)}(p^{\alpha_k}-p^{k-1})\prod_{j=1}^{r(\lambda+4)}(p^{e_j})^{r(\lambda+4)-\alpha_j}\prod_{i=1}^{r(\lambda+4)}(p^{e_i-1})^{r(\lambda+4)-\beta_i+1}, & \text{if } p\neq 2. \end{cases}$$

*and if $p = 2$ then,* $\mid Aut(R^*) \mid =$

$$\begin{cases} \varphi(2^r-1)\cdot\prod_{k=1}^{(\lambda+5)}(2^{\alpha_k}-2^{k-1}), & : r=1\ ; \\ \varphi(2^r-1)\cdot\prod_{k=1}^{r(\lambda+3)}(2^{\alpha_k}-2^{k-1})\prod_{j=1}^{r(\lambda+3)}(2^{e_j})^{r(\lambda+3)-\alpha_j}\prod_{i=1}^{r(\lambda+3)}(2^{e_i-1})^{r(\lambda+3)-\beta_i+1}, & : r>1\ ; \\ \varphi(2^r-1)\cdot\prod_{k=1}^{r(\lambda+2)}(2^{\alpha_k}-2^{k-1})\prod_{j=1}^{r(\lambda+2)}(2^{e_j})^{r(\lambda+2)-\alpha_j}\prod_{i=1}^{r(\lambda+2)}(2^{e_i-1})^{r(\lambda+2)-\beta_i+1}, & \text{or;} \\ \varphi(2^r-1)\cdot\prod_{k=1}^{r(\lambda+3)}(2^{\alpha_k}-2^{k-1})\prod_{j=1}^{r(\lambda+3)}(2^{e_j})^{r(\lambda+3)-\alpha_j}\prod_{i=1}^{r(\lambda+3)}(2^{e_i-1})^{r(\lambda+3)-\beta_i+1}, & : p\in J^2; \\ \varphi(2^r-1)\cdot\prod_{k=1}^{r(\lambda+3)}(2^{\alpha_k}-2^{k-1})\prod_{j=1}^{r(\lambda+3)}(2^{e_j})^{r(\lambda+3)-\alpha_j}\prod_{i=1}^{r(\lambda+3)}(2^{e_i-1})^{r(\lambda+3)-\beta_i+1}, & \text{or;} \\ \varphi(2^r-1)\cdot\prod_{k=1}^{r(\lambda+3)}(2^{\alpha_k}-2^{k-1}), & : p\in\tau. \end{cases}$$

*where, when $r = 1$, then $p \in J - ann(J)$ and when $r > 1$, $p \in J - ann(J)$ and $\tau = ann(J) - J^2$.*

*(iii)If $s = 2, t = 1, \lambda \geq 1$ and char$(R)$=$p^3$, then* $\mid Aut(R^*) \mid =$

$$\begin{cases} \varphi(p^r-1)\cdot\prod_{k=1}^{r(\lambda+5)}(p^{\alpha_k}-p^{k-1})\prod_{j=1}^{r(\lambda+5)}(p^{e_j})^{r(\lambda+5)-\alpha_j}\prod_{i=1}^{r(\lambda+5)}(p^{e_i-1})^{r(\lambda+5)-\beta_i+1}, & \text{or;} \\ \varphi(p^r-1)\cdot\prod_{k=1}^{r(\lambda+4)}(p^{\alpha_k}-p^{k-1})\prod_{j=1}^{r(\lambda+4)}(p^{e_j})^{r(\lambda+4)-\alpha_j}\prod_{i=1}^{r(\lambda+4)}(p^{e_i-1})^{r(\lambda+4)-\beta_i+1}, & \text{if } p\neq 2. \end{cases}$$

*and* $\mid Aut(R^*) \mid =$

$$\begin{cases} \varphi(2^r-1)\cdot\prod_{k=1}^{r(\lambda+3)}(2^{\alpha_k}-2^{k-1})\prod_{j=1}^{r(\lambda+3)}(2^{e_j})^{r(\lambda+3)-\alpha_j}\prod_{i=1}^{r(\lambda+3)}(2^{e_i-1})^{r(\lambda+3)-\beta_i+1}, & \text{or;} \\ \varphi(2^r-1)\cdot\prod_{k=1}^{r(\lambda+4)}(2^{\alpha_k}-2^{k-1})\prod_{j=1}^{r(\lambda+4)}(2^{e_j})^{r(\lambda+4)-\alpha_j}\prod_{i=1}^{r(\lambda+4)}(2^{e_i-1})^{r(\lambda+4)-\beta_i+1}, & \text{or;} \\ \varphi(2^r-1)\cdot\prod_{k=1}^{r(\lambda+5)}(2^{\alpha_k}-2^{k-1})\prod_{j=1}^{r(\lambda+5)}(2^{e_j})^{r(\lambda+5)-\alpha_j}\prod_{i=1}^{r(\lambda+5)}(2^{e_i-1})^{r(\lambda+5)-\beta_i+1}, & \text{if } p=2. \end{cases}$$

*(iv) If $s = 2, t = 2, \lambda \geq 1$ and char$(R)$=$p$, then* $\mid Aut(R^*) \mid =$

$$\begin{cases} \varphi(p^r-1)\cdot\prod_{k=1}^{r(\lambda+4)}(p^{\alpha_k}-p^{k-1}), & \text{if } p\neq 2; \\ \varphi(2^r-1)\cdot\prod_{k=1}^{r(\lambda+2)}(2^{\alpha_k}-2^{k-1})\prod_{j=1}^{r(\lambda+2)}(2^{e_j})^{r(\lambda+2)-\alpha_j}\prod_{i=1}^{r(\lambda+2)}(2^{e_i-1})^{r(\lambda+2)-\beta_i+1}, & \text{or;} \\ \varphi(2^r-1)\cdot\prod_{k=1}^{r(\lambda+3)}(2^{\alpha_k}-2^{k-1})\prod_{j=1}^{r(\lambda+3)}(2^{e_j})^{r(\lambda+3)-\alpha_j}\prod_{i=1}^{r(\lambda+3)}(2^{e_i-1})^{r(\lambda+3)-\beta_i+1}, & \text{if } p=2. \end{cases}$$

*(v) If $t = s(s + 1)/2, \lambda \geq 1$ for the various characteristics of $R$, then* $\mid Aut(R^*) \mid =$

$$\begin{cases} \varphi(2^r-1)\cdot\prod_{k=1}^{\omega_1}(2^{\alpha_k}-2^{k-1})\prod_{j=1}^{\omega_1}(2^{e_j})^{\omega_1-\alpha_j}\prod_{i=1}^{\omega_1}(2^{e_i-1})^{\omega_1-\beta_i+1}, & \text{if } p=2; \\ \varphi(p^r-1)\cdot\prod_{k=1}^{r(\lambda+\gamma+2s)}(p^{\alpha_k}-p^{k-1}), & \text{if } p\neq 2, \end{cases}$$

*for char* $(R) = p$, *where* $\omega_1 = r(\lambda+\gamma+s)$.

$$\begin{cases} \varphi(2^r-1)\cdot\prod_{k=1}^{r(\lambda+\gamma+2s+1)}(2^{\alpha_k}-2^{k-1}), & \textit{if } p=2; \\ \varphi(p^r-1)\cdot\prod_{k=1}^{r(\lambda+\gamma+2s+1)}(p^{\alpha_k}-p^{k-1})\prod_{j=1}^{\nu_1}(p^{e_j})^{\nu_1-\alpha_j}\prod_{i=1}^{\nu_1}(p^{e_i-1})^{\nu_1-\beta_i+1}, & \textit{if } p\neq 2, \end{cases}$$

*for char*$(R) = p^2$ *where* $\nu_1 = r(\lambda+\gamma+2s+1)$. *And,*

$$\begin{cases} \varphi(2^r-1)\cdot\prod_{k=1}^{\nu_2}(2^{\alpha_k}-2^{k-1})\prod_{j=1}^{\nu_2}(2^{e_j})^{\nu_2-\alpha_j}\prod_{i=1}^{\nu_2}(2^{e_i-1})^{\nu_2-\beta_i+1}, & \textit{if } p=2; \\ \varphi(p^r-1)\cdot\prod_{k=1}^{\nu_3}(p^{\alpha_k}-p^{k-1})\prod_{j=1}^{\nu_3}(p^{e_j})^{\nu_3-\alpha_j}\prod_{i=1}^{\nu_3}(p^{e_i-1})^{\nu_3-\beta_i+1}, & \textit{if } p\neq 2. \end{cases}$$

*for char*$(R) = p^3$, *where* $\gamma = (s^2-s)/2$, $\nu_2 = r(\lambda+\gamma+2s+2)$, $\nu_3 = r(\lambda+\gamma+2s+1)$.

## 3.8 Units of Power Four Radical Zero Commutative finite Completely Primary Rings

In [83], we constructed some classes of power four radical zero commutative completely primary finite rings and determined their unit groups. In this section, we give detailed recap of the same constructions, demonstrate the structures of the unit groups whose automorphisms are determined in the next section.

### 3.8.1 Rings of Characteristic $p$

For any prime integer $p$ and a positive integer $r$, let $R_0 = GR(p^r, p)$ be a Galois ring of order $p^r$ and characteristic $p$. Suppose $U, V$ and $W$ are finitely generated $R_0$-modules such that $dim_{R_o} U = s$, $dim_{R_o} V = t$ and $dim_{R_o} W = \lambda$ and $s + t + \lambda = h$. Let $\{u_1, u_2, ...u_s\}$,$\{v_1, v_2, ...v_t\}$ and $\{w_1, w_2, ...w_\lambda\}$ be the generators of $U, V$ and $W$ respectively so that $R = R_0 \oplus U \oplus V \oplus W$ is an additive abelian group. Further, assume that $s = 1, t = 1, \lambda = h - 2$, so that $R = R_0 \oplus R_0 u \oplus R_0 v \oplus \sum_{j=1}^{h-2} R_0 w_j$ and $pu = pv = pw_j = 0, 1 \leq j \leq h - 2$. On $R$, define multiplication as follows:

$(r_0, r_1, r_2, ..., r_h)(s_0, s_1, s_2, ..., s_h) = (r_0 s_0, r_0 s_1 + r_1 s_0, r_0 s_2 + r_2 s_0 + r_1 s_1, r_0 s_3 + r_3 s_0 + r_1 s_2 + r_2 s_1, ..., r_0 s_h + r_h s_0 + r_1 s_2 + r_2 s_1)$. It is easy to verify that the given multiplication turns $R$ into a commutative ring with identity $(1, 0, .., 0)$.

**Proposition 3.8.1.** *[83] The ring $R$ of the above construction is completely primary, of characteristic $p$ and*

$$\begin{aligned} J &= R_0 u \oplus R_0 v \oplus \sum_{j=1}^{\lambda} R_0 w_j, \\ J^2 &= R_0 v \oplus \sum_{j=1}^{\lambda} R_0 w_j, \\ J^3 &= \sum_{j=1}^{\lambda} R_0 w_j, \\ J^4 &= (0). \end{aligned}$$

**Lemma 3.8.1.** *[83, Proposition 3] Let $R$ be the ring constructed above and $J$ be its*

*Jacobson radical. Then if* $p \neq 2$,

$$R^* \cong \mathbb{Z}_{p^r-1} \times \mathbb{Z}_{p^2}^r \times (\mathbb{Z}_p^r)^\lambda.$$

### 3.8.2 Rings of characteristic $p^2$

For any prime integer $p$ and positive integer $r$, let $R_0 = GR(p^{2r}, p^2)$ be a Galois ring of order $p^{2r}$ and characteristic $p^2$. Suppose $U, V$ and $W$ are finitely generated $R_0$-modules such that $dim_{R_o}U = s$, $dim_{R_o}V = t$ and $dim_{R_o}W = \lambda$ and $s+t+\lambda = h$ . Let $\{u_1, ..., u_s\}$, $\{v_1, ..., v_t\}$ and $\{w_1, ..., w_\lambda\}$ be the generators of $U, V$ and $W$ respectively so that $R = R_0 \oplus U \oplus V \oplus W$ is an additive abelian group. Further, assume that $s = h-1, t = 1, \lambda = 0$, so that $R$ can be expressed as $R = R_0 \oplus \sum_{j=1}^{h-1} R_0 u_j \oplus R_0 v$, where $pu_j \neq 0, p^2 u_j = 0, 1 \leq j \leq s$ and $pv = 0$. On $R$, define multiplication as follows:

$(r_0, r_1, r_2, ..., r_{h-1}, \overline{r_h})(s_0, s_1, s_2, ..., s_{h-1}, \overline{s_h}) = (r_0 s_0 + p \sum_{i,j=1}^{h-1} r_i s_j, r_0 s_1 + r_1 s_0, ..., r_0 s_{h-1} + r_{h-1} s_o, r_o \overline{s_h} + \overline{r_h} s_o)$ where $\overline{r_h}, \overline{s_h} \in R_o/pR_o$. It is easy to verify that the given multiplication turns $R$ into a commutative ring with identity $(1, 0, ...0, \overline{0})$.

**Proposition 3.8.2.** *[83] The ring R constructed is completely primary of characteristic* $p^2$ *and*

$$J = pR_0 \oplus \sum_{j=1}^{s} R_0 u_j \oplus R_0 v,$$
$$J^2 = pR_0 \oplus p \sum_{j=1}^{s} R_0 u_j \oplus R_0 v,$$
$$J^3 = p \sum_{j=1}^{s} R_0 u_j,$$
$$J^4 = (0).$$

**Lemma 3.8.2.** *[83, Proposition 5] Let R be the ring constructed and J be its Jacobson radical. Then*

$$R^* \cong \mathbb{Z}_{p^r-1} \times (\mathbb{Z}_{p^2}^r)^s \times (\mathbb{Z}_p^r)^2,$$

*for every prime integer* $p$ *and positive integer* $r$.

### 3.8.3 Rings of characteristic $p^3$

For any prime integer $p$ and positive integer $r$, let $R_0 = GR(p^{3r}, p^3)$ be a Galois ring of order $p^{3r}$ and characteristic $p^3$. Suppose $U, V$ and $W$ are finitely generated $R_0$-modules such that $dim_{R_o}U = s$, $dim_{R_o}V = t$ and $dim_{R_o}W = \lambda$ and $s + t + \lambda = h$. Let $\{u_1, ..., u_s\}$, $\{v_1, ..., v_t\}$ and $\{w_1, ..., w_\lambda\}$ be the generators of $U, V$ and $W$ respectively so that $R = R_0 \oplus U \oplus V \oplus W$ is an additive abelian group. Further, assume that $s = h-1, t = 1, \lambda = 0$, so that $R$ can be expressed as $R = R_0 \oplus \sum_{j=1}^{h-1} R_0u_j \oplus R_0v$, where , $p^2u_j \neq 0, p^3u_j = 0; 1 \leq j \leq s$ and $pv = 0$. On $R$, define multiplication as follows:

$(r_0, \overline{r_1}, \overline{r_2}, ..., \overline{r_{h-1}}, \widehat{r_h})(s_0, \overline{s_1}, \overline{s_2}, ..., \overline{s_{h-1}}, \widehat{s_h}) = (r_0s_0, r_0\overline{s_1} + \overline{r_1}s_0, ..., r_0\overline{s_{h-1}} + \overline{r_{h-1}}s_0, r_0\widehat{s_h} + \widehat{r_h}s_0 + \sum_{i,j=1}^{h-1} \overline{r_i}\overline{s_j})$ where $\overline{r_i}, \overline{s_j} \in R_o/p^2R_o$ and $\widehat{r_h}, \widehat{s_h} \in R_o/pR_o$. It is readily verified that the given multiplication turns $R$ into a commutative ring with identity $(1, \bar{0}, ..., \bar{0}, \widehat{0})$.

**Proposition 3.8.3.** *[83] The ring constructed is completely Primary of characteristic $p^3$ and*

$$\begin{aligned} J &= pR_0 \oplus \sum_{j=1}^{s} R_0u_j \oplus R_0v, \\ J^2 &= p^2R_0 \oplus p\sum_{j=1}^{s} R_0u_j \oplus R_0v, \\ J^3 &= pR_0v, \\ J^4 &= (0). \end{aligned}$$

**Lemma 3.8.3.** *[83, Proposition 7] Let $R$ be a ring constructed and $J$ be its Jacobson radical, then its group of units is characterized as follows*

$$R^* \cong \begin{cases} \mathbb{Z}_{2^r-1} \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_4^{r-1} \times \mathbb{Z}_8^r \times \mathbb{Z}_4^r \times (\mathbb{Z}_2^r)^{s-1}, & \text{if } p = 2; \\ \mathbb{Z}_{p^r-1} \times \mathbb{Z}_{p^2}^r \times \mathbb{Z}_{p^2}^r \times \mathbb{Z}_{p^2}^r \times (\mathbb{Z}_{p^2}^r)^s, & \text{if } p \neq 2. \end{cases}$$

### 3.8.4 Rings of Characteristics $p^4$

For a prime integer $p$ and a positive integer $r$, let $R_0 = GR(p^{4r}, p^4)$ be a Galois ring of order $p^{4r}$ and characteristic $p^4$. Suppose $U, V$ and $W$ are finitely generated $R_0$-modules such that $dim_{R_o}U = s$, $dim_{R_o}V = t$ and $dim_{R_o}W = \lambda$ and $s + t + \lambda = h$. Let $\{u_1, ..., u_s\}$,

$\{v_1, ..., v_t\}$ and $\{w_1, ..., w_\lambda\}$ be the generators of $U, V$ and $W$ respectively so that $R = R_0 \oplus U \oplus V \oplus W$ is an additive abelian group. Further, assume that $s = h$, $t = 0$, $\lambda = 0$ so that $R = R_o \sum_{j=1}^{s} R_o u_j$ where $pu_j = 0$, $1 \leq j \leq s$. On $R$, define multiplication as follows:

$(r_0, \overline{r_1}, \overline{r_2}, ..., \overline{r_h})(s_0, \overline{s_1}, \overline{s_2}, ..., \overline{s_h}) = (r_0 s_0, r_0 \overline{s_1} + \overline{r_1} s_0, ..., r_0 \overline{s_h} + \overline{r_h} s_0)$ where, $\overline{r_i}, \overline{s_j} \in R_0/pR_0; 1 \leq i, j \leq h$. This multiplication turns $R$ into a commutative ring with identity $(1, \bar{0}, ..., \bar{0})$.

**Proposition 3.8.4.** *[83] The ring constructed is completely primary, of characteristic $p^4$ with Jacobson radical such that*

$$\begin{aligned} J = pR_0 \oplus \sum_{j=1}^{s} R_o u_j, \\ J^2 = p^2 R_0, \\ J^3 = p^3 R_0, \\ J^4 = (0). \end{aligned}$$

**Lemma 3.8.4.** *[83, Proposition 9] Let $R$ be the ring described by the construction above. Then*

$$R^* \cong \begin{cases} \mathbb{Z}_{2^r-1} \times \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_8^{r-1} \times (\mathbb{Z}_2^r)^s & \text{if } p = 2; \\ \mathbb{Z}_{p^r-1} \times \mathbb{Z}_{p^3}^r \times (\mathbb{Z}_p^r)^s & \text{if } p \neq 2. \end{cases}$$

**Theorem 3.8.1.** *The structure of the units $R^*$ of the commutative completely primary finite ring $R$ of characteristic $p, p^2, p^3, p^4$ with maximal ideal $J$ such that $J^4 = (0)$ and $J^3 \neq (0)$, with the invariants $p, r, s, t, h$ and $\lambda$ where $p \in J$, is a direct product of cyclic groups as follows:*

*(i) If the char$(R) = p$, then,*

$$R^* \cong \mathbb{Z}_{p^r-1} \times \mathbb{Z}_{p^2}^r \times (\mathbb{Z}_p^r)^\lambda : p \neq 2.$$

*(ii) If the char$(R) = p^2$, then,*

$$R^* \cong \mathbb{Z}_{p^r-1} \times (\mathbb{Z}_p^r)^2 \times (\mathbb{Z}_{p^2}^r)^s$$

*(iii) If the char*$(R) = p^3$*, then,*

$$R^* \cong \begin{cases} \mathbb{Z}_{2^r-1} \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_4^{r-1} \times \mathbb{Z}_8^r \times \mathbb{Z}_4^r \times (\mathbb{Z}_2^r)^{s-1}, & \text{if } p = 2; \\ \mathbb{Z}_{p^r-1} \times \mathbb{Z}_{p^2}^r \times \mathbb{Z}_{p^2}^r \times (\mathbb{Z}_{p^2}^r)^s, & \text{if } p \neq 2. \end{cases}$$

*(iv) If the char*$(R) = p^4$*, then,*

$$R^* \cong \begin{cases} \mathbb{Z}_{2^r-1} \times \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_8^{r-1} \times (\mathbb{Z}_2^r)^s & \text{if } p = 2; \\ \mathbb{Z}_{p^r-1} \times \mathbb{Z}_{p^3}^r \times (\mathbb{Z}_p^r)^s & \text{if } p \neq 2. \end{cases}$$

## 3.9 Automorphism Groups of the Units of Power Four Radical Zero Completely Primary Finite Rings

We explicitly describe $Aut(R^*)$ by completely characterizing the structure and order of the automorphism groups of the units whose structures are given by Theorem 3.8.1.

### 3.9.1 Endomorphisms of $1 + J$ and their properties

We form $R_p$ which is a set of matrices given by $R_p = \{(a_{ij}) : p^{e_i - e_j} \mid a_{ij};\ 1 \leq j \leq i \leq rk(1+J)\}$, where $a_{ij} \in \mathbb{Z}_p$, for all the cases considered and determine the endomorphisms say $E_p = \psi(A)$ from that description.

**Case 1:** If the characteristic of $R = p \neq 2$, $s = 1, t = 1$ and $\lambda = h - 2$, then, $1 + J = \mathbb{Z}_p^{r\lambda} \times \mathbb{Z}_{p^2}^r$. Clearly, $e_1 = \cdots = e_{r\lambda} = 1$ and $e_{(r\lambda)+1} = \cdots = e_{r(\lambda+1)} = 2$ so that for $a_{ij} \in \mathbb{Z}_p$, $R_p$ is given by

$$R_p = \left\{ \begin{pmatrix} a_{11} & \cdots & a_{1(r\lambda)} & a_{1((r\lambda)+1)} & \cdots & a_{1(r(\lambda+1))} \\ a_{21} & \cdots & a_{2(r\lambda)} & a_{2((r\lambda)+1)} & \cdots & a_{2(r(\lambda+1))} \\ \vdots & & & & & \\ a_{(r\lambda)1} & \cdots & a_{(r\lambda)(r\lambda)} & a_{(r\lambda)((r\lambda)+1)} & \cdots & a_{(r\lambda)r(\lambda+1)} \\ pa_{((r\lambda)+1)1} & \cdots & pa_{((r\lambda)+1)(r\lambda)} & a_{((r\lambda)+1)((r\lambda)+1)} & \cdots & a_{((r\lambda)+1)(r(\lambda+1))} \\ \vdots & & & & & \\ pa_{(r(\lambda+1))1} & \cdots & pa_{(r(\lambda+1))(r\lambda)} & a_{(r(\lambda+1))((r\lambda)+1)} & \cdots & a_{(r(\lambda+1))(r(\lambda+1))} \end{pmatrix} \right\}.$$

**Proposition 3.9.1.** *If the characteristic of* $R = p$, $s = 1, t = 1$ *and* $p \neq 2$, $1 + J = \mathbb{Z}_p^{r\lambda} \times \mathbb{Z}_{p^2}^r$*, then* *(i)* $R_p = \{(a_{ij}) : p^{e_i - e_j} \mid a_{ij};\ 1 \leq j \leq i \leq r(\lambda+1)\} = M_{r(\lambda+1)}(\mathbb{Z}_p)$.

*(ii)* $rank(1+J) = r(\lambda+1)$.

*(iii) For* $A \in R_p$ *and a surjective ring homomorphism*

$$\psi : R_p \to (\mathbb{Z}_p^{r\lambda} \times \mathbb{Z}_{p^2}^{r}), End(\mathbb{Z}_p^{r\lambda} \times \mathbb{Z}_{p^2}^{r}) = \psi(A).$$

*(iv)* $Aut(\mathbb{Z}_p^{r\lambda} \times \mathbb{Z}_{p^2}^{r}) = GL_{(r(\lambda+1))}(\mathbb{F}_p)$.

**Case 2:** If the characteristic of $R = p^2$, $s = h-1$, $t = 1$ and $\lambda = 0$, then $1 + J = \mathbb{Z}_p^{2r} \times \mathbb{Z}_{p^2}^{rs}$. Clearly $e_1 = \cdots = e_{2r} = 1$ and $e_{2r+1} = \cdots = e_{r(s+2)} = 2$ so that for all $a_{ij} \in \mathbb{Z}_p$,

$$R_p = \left\{ \begin{pmatrix} a_{11} & \cdots & a_{1(2r)} & a_{1(2r+1)} & \cdots & a_{1(r(s+2))} \\ a_{21} & \cdots & a_{2(2r)} & a_{2(2r+1)} & \cdots & a_{2(r(s+2))} \\ \vdots & & & & & \\ a_{(2r)1} & \cdots & a_{(2r)(2r)} & a_{(2r)((2r)+1)} & \cdots & a_{(2r)r(s+2)} \\ pa_{((2r)+1)1} & \cdots & pa_{((2r)+1)(2r)} & a_{((2r)+1)((2r)+1)} & \cdots & a_{((2r)+1)(r(s+2))} \\ \vdots & & & & & \\ pa_{(r(s+2))1} & \cdots & pa_{(r(s+2))(2r)} & a_{(r(s+2))((2r)+1)} & \cdots & a_{(r(s+2))(r(s+2))} \end{pmatrix} \right\}.$$

**Proposition 3.9.2.** *If the characteristic of* $R = p^2$, $s = h-1$, $t = 1$ *and* $\lambda = 0$, $1 + J = \mathbb{Z}_p^{2r} \times \mathbb{Z}_{p^2}^{rs}$, *then*

*(i)* $R_p = \{(a_{ij}) : p^{e_i - e_j} \mid a_{ij};\ 1 \leq j \leq i \leq r(s+2)\} = M_{r(s+2)}(\mathbb{Z}_p)$.

*(ii)* $rank(1+J) = r(s+2)$.

*(iii) For* $A \in R_p$ *and a surjective ring homomorphism*

$$\psi : R_p \to (\mathbb{Z}_p^{2r} \times \mathbb{Z}_{p^2}^{rs}), End(\mathbb{Z}_p^{2r} \times \mathbb{Z}_{p^2}^{rs}) = \psi(A).$$

*(iv)* $Aut(\mathbb{Z}_p^{2r} \times \mathbb{Z}_{p^2}^{rs}) = GL_{r(s+2)}(\mathbb{F}_p)$.

**Case 3.** If the characteristic of $R = p^3, s = h-1, t = 1$ and $\lambda = 0$,

**(a).** When $p = 2$, $1+J = \mathbb{Z}_2^{2+rs-r} \times \mathbb{Z}_4^{2r-1} \times \mathbb{Z}_8^r$. In this case $e_1 = e_2 = \cdots = e_{2+rs-r} = 1$, $e_{3+rs-r} = \cdots = e_{1+rs+r} = 2$ and $e_{2+rs+r} = \cdots = e_{1+rs+2r} = 3$. So for all $a_{ij} \in \mathbb{Z}_2$, $R_2 =$

$$\left\{ \begin{pmatrix} a_{11} & \cdots & a_{1(\mu)} & \cdots & a_{1(v)} & \cdots & a_{1(w)} \\ \vdots & & & & & & \\ a_{(2+rs-r)1} & \cdots & a_{(2+rs-r)(\mu)} & \cdots & a_{(2+rs-r)(v)} & \cdots & a_{(2+rs-r)(w)} \\ 2a_{((2+rs-r)+1)1} & \cdots & 2a_{((2+rs-r)+1)(\mu)} & \cdots & 2a_{((2+rs-r)+1)(v)} & \cdots & a_{((2+rs-r)+1)(w)} \\ \vdots & & & & & & \\ 2a_{(1+rs+r)1} & \cdots & 2a_{(1+rs+r)(\mu)} & \cdots & 2a_{(1+rs+r)(v)} & \cdots & a_{(1+rs+r)(w)} \\ 4a_{((1+rs+r)+1)1} & \cdots & 4a_{((1+rs+r)+1)(\mu)} & \cdots & 2a_{((1+rs+r)+1)(v)} & \cdots & a_{((1+rs+r)+1)(w)} \\ \vdots & & & & & & \\ 4a_{(1+rs+2r)1} & \cdots & 4a_{(1+rs+2r)(\mu)} & \cdots & 2a_{(1+rs+2r)(v)} & \cdots & a_{(1+rs+2r)(w)} \end{pmatrix} \right\},$$

where $\mu = 2 + rs - r$, $v = 1 + rs + r$ and $w = 1 + rs + 2r = rank(1 + J)$.

**Proposition 3.9.3.** *If the characteristic of $R = p^3, s = h - 1, t = 1$ and $\lambda = 0$, $p = 2$, $1 + J = \mathbb{Z}_2^{2+rs-r} \times \mathbb{Z}_4^{2r-1} \times \mathbb{Z}_8^r$, then,*

*(i)* $R_2 = \{(a_{ij}) : p^{e_i - e_j} \mid a_{ij};\ 1 \leq j \leq i \leq 1 + rs + 2r\} = \{M_{(1+rs+2r)}(\mathbb{Z}_2)\}$.

*(ii)* $rank(1 + J) = 1 + rs + 2r$.

*(iii) For $A \in R_2$ and a surjective ring homomorphism*

$$\psi : R_2 \to (\mathbb{Z}_2^{2+rs-r} \times \mathbb{Z}_4^{2r-1} \times \mathbb{Z}_8^r), End(\mathbb{Z}_2^{2+rs-r} \times \mathbb{Z}_4^{2r-1} \times \mathbb{Z}_8^r) = \psi(A).$$

*(iv)* $Aut(\mathbb{Z}_2^{2+rs-r} \times \mathbb{Z}_4^{2r-1} \times \mathbb{Z}_8^r) = GL_{1+rs+2r}(\mathbb{F}_2)$.

**(b).** When $p \neq 2$, $1 + J = \mathbb{Z}_{p^2}^{r(s+2)}$, then $e_1 = e_2 = \cdots = e_{r(s+2)} = 2$. Therefore, for all $a_{ij} \in \mathbb{Z}_p$,

$$R_p = \left\{ \begin{pmatrix} a_{11} & \cdots & a_{1r} & a_{1(r+1)} & \cdots & a_{1(r(s+2))} \\ a_{21} & \cdots & a_{2r} & a_{2(r+1)} & \cdots & a_{2(r(s+2))} \\ \vdots & & & & & \\ a_{r1} & \cdots & a_{rr} & a_{r(r+1)} & \cdots & a_{r(r(s+2))} \\ a_{(r+1)1} & \cdots & a_{(r+1)r} & a_{(r+1)(r+1)} & \cdots & a_{(r+1)(r(s+2))} \\ \vdots & & & & & \\ a_{(r(s+2))1} & \cdots & a_{(r(s+2))r} & a_{(r(s+2))(r+1)} & \cdots & a_{(r(s+2))(r(s+2))} \end{pmatrix} \right\}.$$

**Proposition 3.9.4.** *If the characteristic of $R = p^3, s = h-1, t = 1$ and $\lambda = 0$, $p \neq 2$, $1 + J = \mathbb{Z}_{p^2}^{r(s+2)}$, then,*

*(i)* $R_p = \{(a_{ij}) : p^{e_i - e_j} \mid a_{ij} : 1 \leq j \leq i \leq r(s+2)\} = M_{(r(s+2))}(\mathbb{Z}_p)$.

*(ii)* $rank(1 + J) = r(s+2)$.

*(iii) For* $A \in R_p$ *and a surjective ring homomorphism*

$$\psi : R_p \to (\mathbb{Z}_{p^2}^{r(s+2)}), End(\mathbb{Z}_{p^2}^{r(s+2)}) = \psi(A).$$

*(iv)* $Aut(\mathbb{Z}_{p^2}^{r(s+2)}) = GL_{r(s+2)}(\mathbb{F}_p)$.

**Case 4:** If the characteristic of $R = p^4$, $s = h$, $t = 0$, $\lambda = 0$

**(a).** when $p = 2$ and $1 + J = \mathbb{Z}_2^{rs+1} \times \mathbb{Z}_{2^2} \times \mathbb{Z}_{2^3}^{r-1}$, then $e_1 = \cdots = e_{rs+1} = 1$, $e_{rs+2} = 2$ and finally $e_{rs+3} = \cdots = e_{rs+r+1} = 3$, and it follows by definition that for $a_{ij} \in \mathbb{Z}_2$,

$$R_2 = \left\{ \begin{pmatrix} a_{11} & \cdots & a_{1(1+rs)} & \cdots & a_{1(2+rs)} & \cdots & a_{1(1+rs+r)} \\ \vdots & & & & & & \\ a_{(1+rs)1} & \cdots & a_{(1+rs)(1+rs)} & \cdots & a_{(1+rs)(2+rs)} & \cdots & a_{(1+rs)(1+rs+r)} \\ 2a_{(2+rs)1} & \cdots & 2a_{(2+rs)(1+rs)} & \cdots & 2a_{(2+rs)(2+rs)} & \cdots & a_{(2+rs)(1+rs+r)} \\ \vdots & & & & & & \\ 4a_{(3+rs)1} & \cdots & 4a_{(3+rs)(1+rs)} & \cdots & 2a_{(3+rs)(2+rs)} & \cdots & a_{(3+rs)(1+rs+r)} \\ \vdots & & & & & & \\ 4a_{(1+rs+r)1} & \cdots & 4a_{(1+rs+r)(1+rs)} & \cdots & 2a_{((1+rs+r)(2+rs)} & \cdots & a_{(1+rs+r)(1+rs+r)} \end{pmatrix} \right\}.$$

**Proposition 3.9.5.** *If the characteristic of $R = p^4$, $s = h$, $t = 0$, $\lambda = 0$ $p = 2$ and $1 + J = \mathbb{Z}_2^{rs+1} \times \mathbb{Z}_{2^2}^1 \times \mathbb{Z}_{2^3}^{r-1}$, then*

*(i)* $R_2 = \{(a_{ij}) : p^{e_i - e_j} \mid a_{ij};\ 1 \leq j \leq i \leq 1 + rs + r\} = M_{(1+rs+r)}(\mathbb{Z}_2)$.

*(ii)* $rank(1 + J) = 1 + rs + r$.

*(iii) For* $A \in R_2$ *and a surjective ring homomorphism*

$$\psi : R_2 \to (\mathbb{Z}_2^{rs+1} \times \mathbb{Z}_{2^2}^1 \times \mathbb{Z}_{2^3}^{r-1}), End(\mathbb{Z}_2^{rs+1} \times \mathbb{Z}_{2^2}^1 \times \mathbb{Z}_{2^3}^{r-1}) = \psi(A).$$

*(iv)* $Aut(\mathbb{Z}_2^{rs+1} \times \mathbb{Z}_{2^2} \times \mathbb{Z}_{2^3}^{r-1}) = GL_{1+rs+r}(\mathbb{F}_2)$.

**(b):** When $p \neq 2$ and $1+J = \mathbb{Z}_p^{rs} \times \mathbb{Z}_{p^3}^r$ then $e_1 = \cdots = e_{rs} = 1$ and $e_{rs+1} = \cdots = e_{r(s+1)} = 3$. Thus for all $a_{ij} \in \mathbb{Z}_p$,

$$R_p = \left\{ \begin{pmatrix} a_{11} & \cdots & a_{1(rs)} & a_{1(rs+1)} & \cdots & a_{1(r(s+1))} \\ a_{21} & \cdots & a_{2(rs)} & a_{2(rs+1)} & \cdots & a_{2(r(s+1))} \\ \vdots & & & & & \\ a_{(rs)1} & \cdots & a_{(rs)(rs)} & a_{(rs)(rs+1)} & \cdots & a_{(rs)(r(s+1))} \\ p^2 a_{(rs+1)1} & \cdots & p^2 a_{(rs+1)(rs)} & a_{(rs+1)(rs+1)} & \cdots & a_{(rs+1)(r(s+1))} \\ \vdots & & & & & \\ p^2 a_{(r(s+1))1} & \cdots & p^2 a_{(r(s+1))(rs)} & a_{(r(s+1))(rs+1)} & \cdots & a_{(r(s+1))(r(s+1))} \end{pmatrix} \right\}.$$

**Proposition 3.9.6.** *If the characteristic of $R = p^4$, $s = h$, $t = 0$, $\lambda = 0$ $p \neq 2$ and $1+J = \mathbb{Z}_p^{rs} \times \mathbb{Z}_{p^3}^r$, then*

*(i)* $R_p = \{(a_{ij}) : p^{e_i - e_j} \mid a_{ij} : 1 \leq j \leq i \leq r(s+1)\} = M_{(r(s+1))}(\mathbb{Z}_p)$.

*(ii)* $rank(1+J) = r(s+1)$.

*(iii) For $A \in R_p$ and a surjective ring homomorphism*

$$\psi : R_p \to (\mathbb{Z}_p^{rs} \times \mathbb{Z}_{p^3}^r), End(\mathbb{Z}_p^{rs} \times \mathbb{Z}_{p^3}^r) = \psi(A).$$

*(iv)* $Aut(\mathbb{Z}_p^{rs} \times \mathbb{Z}_{p^3}^r) = GL_{r(s+1)}(\mathbb{F}_p)$.

Consequently, we give the structure of $Aut(R^*)$:

**Theorem 3.9.1.** *The structures of the automorphisms $Aut(R^*)$ of the unit groups $R^*$ of the commutative completely primary finite ring $R$ of characteristic $p, p^2, p^3$ and $p^4$ with maximal ideal $J$ such that $J^4 = (0)$ and $J^3 \neq (0)$, with the invariants $p, r, s, t, h$ and $\lambda$ where $p \in J$, are characterized as follows:*

*(i) If the $char(R) = p$, $s = 1, t = 1$ and $\lambda = h - 2$, then, for all $p$,*

$$Aut(R^*) \cong (\mathbb{Z}_{p^r - 1})^* \times GL_{(r(\lambda+1))}(\mathbb{F}_p).$$

*(ii) If the char*$(R) = p^2$, $s = h - 1$, $t = 1$ *and* $\lambda = 0$ *then, for all* $p$

$$Aut(R^*) \cong (\mathbb{Z}_{p^r-1})^* \times GL_{(r(s+2))}(\mathbb{F}_p).$$

*(iii) If the char*$(R) = p^3$, $s = h - 1, t = 1$ *and* $\lambda = 0$ *then,*

$$Aut(R^*) \cong \begin{cases} (\mathbb{Z}_{2^r-1})^* \times GL_{(r(1+rs+2r))}(\mathbb{F}_2), & \textit{if } p = 2; \\ (\mathbb{Z}_{p^r-1})^* \times GL_{(r(s+2))}(\mathbb{F}_p), & \textit{if } p \neq 2. \end{cases}$$

*(iv) If the char*$(R) = p^4$, $s = h$, $t = 0$, $\lambda = 0$ *then,*

$$Aut(R^*) \cong \begin{cases} (\mathbb{Z}_{2^r-1})^* \times GL_{(1+rs+r)}(\mathbb{F}_2), & \textit{if } p = 2; \\ (\mathbb{Z}_{p^r-1})^* \times GL_{(r(s+1))}(\mathbb{F}_p), & \textit{if } p \neq 2. \end{cases}$$

### 3.9.2 Counting the Automorphisms

It is worth noting that the method of counting the automorphisms of $1+J$ as general linear groups is similar to the one employed for the cube radical zero commutative completely primary rings. However, we discuss the properties of some special subgroups of $Aut(1+J) = GL_{rk(1+J)}(\mathbb{F}_p)$. These are:

(1). **The special Linear group** $SL_{rk(1+J)}(\mathbb{F}_p)$: The determinant function given by

$$\det : GL_{rk(1+J)}(\mathbb{F}_p) \to \mathbb{F}_p^{\times},$$

is a homomorphism. It maps the identity matrix to 1 and it is multiplicative as desired. Now, $SL_{rk(1+J)}(\mathbb{F}_p)$ is the kernel of this homomorphism. Thus,

$$SL_{rk(1+J)}(\mathbb{F}_p) = \Big\{M \in GL_{rk(1+J)}(\mathbb{F}_p) \mid \det(M) = 1\Big\}$$

**Proposition 3.9.7.** *Denote by* $rk(1 + J)$ *the rank of* $(1 + J)$. *Then, the number of elements in* $SL_{rk(1+J)}(\mathbb{F}_p)$ *is given by:*

$$\mid SL_{rk(1+J)}(\mathbb{F}_p) \mid = \left( \left( \prod_{i=0}^{(rk(1+J))-1} (p^{rk(1+J)} - p^i) \right) /(p-1) \right)$$

*Proof.* Consider the homomorphism $\det : GL_{rk(1+J)}(\mathbb{F}_p) \to \mathbb{F}_p^{\times}$. This map is surjective, that is, the image of $GL_{rk(1+J)}(\mathbb{F}_p)$ under det is the whole space $\mathbb{F}_p^{\times}$. This is true because, for instance, suppose $rk(1+J) = 4$, the matrix

$$\begin{pmatrix} a & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}$$

is an invertible $rk(1+J) \times rk(1+J)$ matrix of determinant $a$. Since $SL_{rk(1+J)}(\mathbb{F}_p)$ is the kernel of the homomorphism, it follows from the First Isomorphism Theorem that

$$GL_{rk(1+J)}(\mathbb{F}_p)/SL_{rk(1+J)}(\mathbb{F}_p) \cong \mathbb{F}_p^{\times}.$$

Thus,

$$\mid SL_{rk(1+J)}(\mathbb{F}_p) \mid = \frac{\mid GL_{rk(1+J)}(\mathbb{F}_p) \mid}{\mid \mathbb{F}_p^{\times} \mid} = \frac{\prod_{i=0}^{(rk(1+J))-1}(p^{rk(1+J)} - p^i)}{p-1}.$$

□

(2). **The Centers of $Aut(1+J)$ and $SL_{rk(1+J)}(\mathbb{F}_p)$:**

**Proposition 3.9.8.** *$Z(GL_{rk(1+J)}(\mathbb{F}_p)) = \{a \cdot I_{rk(1+J)} \mid a \in \mathbb{F}_p^{\times}\}$ and $Z(SL_{rk(1+J)}(\mathbb{F}_p)) = \left\{a \cdot I_{rk(1+J)} \mid a \in \mathbb{F}_p^{\times}, a^{rk(1+J)}\right\}$.*

*Proof.* For $M$ to be in $Z(GL_{rk(1+J)}(\mathbb{F}_p))$, it must commute with every $N \in GL_{rk(1+J)}(\mathbb{F}_p)$. In particular, $M$ commutes with every elementary matrices. Multiplying $M$ on the left by an elementary matrix corresponds to performing an elementary row operation; multiplying $M$ on the right by an elementary matrix corresponds to performing an elementary column operation. Thus for instance, multiplying the $i^{th}$ row of $M$ by $a$ gives the same matrix as multiplying the $i^{th}$ column of $M$ by $a$. This implies that the matrix $M$ is diagonal. Then, since swapping the $i^{th}$ and $j^{th}$ rows of $M$ gives the same matrix as swapping the $i^{th}$ and $j^{th}$ columns of $M$, it implies that the $i^{th}$ and $j^{th}$ entries along the diagonals are equal for all $i$ and $j$. Therefore, $M$ must be a multiple of $I_{rk(1+J)}$. Finally, it is easy to see that all nonzero multiples of $I_{rk(1+J)}$ do commute with all $N \in GL_{rk(1+J)}(\mathbb{F}_p)$. So, the proposition is proved for $Z(GL_{rk(1+J)}(\mathbb{F}_p))$. The proof for $Z(SL_{rk(1+J)}(\mathbb{F}_p))$ is similar. $\square$

**Remark 3.9.1.** *As a result of the process of counting and the fact that* $\mid Aut(\mathbb{Z}_{p^r-1}) \mid = \varphi(p^r-1)$*, we give the following result:*

**Theorem 3.9.2.** *The orders of the automorphisms* $Aut(R^*)$ *of the unit groups* $R^*$ *of the commutative completely primary finite ring* $R$ *of characteristic* $p, p^2, p^3, p^4$ *with maximal ideal* $J$ *such that* $J^4 = (0)$ *and* $J^3 \neq (0)$*, with the invariants* $p, r, s, t, h$ *and* $\lambda$ *where* $p \in J$*, are characterized as follows:*

*(i) If the char*$(R) = p$, $s = 1, t = 1$ *and* $\lambda = h - 2$*, then, for all* $p$,

$$\mid Aut(R^*) \mid = \varphi(p^r-1) \cdot \prod_{k=1}^{r(\lambda+1)} (p^{\alpha_k} - p^{k-1}) \prod_{j=1}^{r(\lambda+1)} (p^{e_j})^{r(\lambda+1)-\alpha_j} \prod_{i=1}^{r(\lambda+1)} (p^{e_i-1})^{r(\lambda+1)-\beta_i+1}.$$

*(ii) If the char*$(R) = p^2$, $s = h - 1$, $t = 1$ *and* $\lambda = 0$ *then, for all* $p$

$$\mid Aut(R^*) \mid = \varphi(p^r-1) \cdot \prod_{k=1}^{r(s+2)} (p^{\alpha_k} - p^{k-1}) \prod_{j=1}^{r(s+2)} (p^{e_j})^{r(s+2)-\alpha_j} \prod_{i=1}^{r(s+2)} (p^{e_i-1})^{r(s+2)-\beta_i+1}.$$

*(iii) If the char*$(R) = p^3$, $s = h - 1, t = 1$ *and* $\lambda = 0$ *then,* $\mid Aut(R^*) \mid =$

$$\begin{cases} \varphi(2^r-1)\cdot\prod_{k=1}^{1+rs+2r}(2^{\alpha_k}-2^{k-1})\prod_{j=1}^{1+rs+2r}(2^{e_j})^{(1+rs+2r)-\alpha_j}\prod_{i=1}^{w}(2^{e_i-1})^{w-\beta_i+1}, & \text{if } p = 2;\\ \varphi(p^r-1)\cdot\prod_{k=1}^{r(s+2)}(p^{\alpha_k}-p^{k-1}), & \text{if } p \neq 2,\end{cases}$$

*where* $w = (1 + rs + 2r)$.

*(iv) If the char*$(R) = p^4$, $s = h$, $t = 0$, $\lambda = 0$ *then,* $\mid Aut(R^*) \mid =$

$$\begin{cases} \varphi(2^r-1)\cdot\prod_{k=1}^{1+rs+r}(2^{\alpha_k}-2^{k-1})\prod_{j=1}^{1+rs+r}(2^{e_j})^{(1+rs+r)-\alpha_j}\prod_{i=1}^{1+rs+r}(2^{e_i-1})^{w-\beta_i+1}, & \text{if } p = 2;\\ \varphi(p^r-1)\cdot\prod_{k=1}^{r(s+1)}(p^{\alpha_k}-p^{k-1})\prod_{j=1}^{r(s+1)}(p^{e_j})^{r(s+1)-\alpha_j}\prod_{i=1}^{r(s+1)}(p^{e_i-1})^{r(s+1)-\beta_i+1}, & \text{if } p \neq 2,\end{cases}$$

*where* $w = (1 + rs + r)$.

# CHAPTER 4

# SUMMARY OF FINDINGS, CONCLUSION AND RECOMMENDATIONS

## 4.1 Summary of findings

This study was set up with an objective of characterizing the automorphisms of the unit groups of square radical zero, cube radical zero and power four radical zero finite commutative completely primary rings. This has been done in a number of steps by considering the classes of the rings separately. We began by describing the structures of the unit groups $R^*$ whose automorphisms were desired. Owing to the structure of $1+J$ which is a subgroup of $R^*$, we developed a set of square matrices $R_p$ whose order is the rank of $1+J$ in all the cases considered. From $R_p$, we identified all the endomorphisms of $1+J$ and specified which endomorphisms are the automorphisms of $1+J$. Since elementary abelian $p-$groups are also $\mathbb{F}_p$ vector spaces, the groups of automorphisms of such $p-$groups are groups of invertible linear transformations. Thus, we found that $Aut(1+J) = GL_{rk(1+J)}(\mathbb{F}_p)$ for the $p-$group $1+J$ whose rank is $rk(1+J)$. But the unit groups of the classes of the finite completely primary rings considered is given by $R^* \cong (\mathbb{Z}_{p^r-1}) \times (1+J)$ where $\gcd(p^r-1, \mid 1+J \mid) = 1$ . Since $Aut(\mathbb{Z}_{p^r-1}) \cong (\mathbb{Z}_{p^r-1})^*$, we established that the structure of $Aut(R^*) \cong (\mathbb{Z}_{p^r-1})^* \times GL_{rk(1+J)}(\mathbb{F}_p)$ for each $1+J$. Moreover, we discussed some properties of three subgroups of $Aut(1+J)$, that is $SL_{rk(1+J)}(\mathbb{F}_p)$, $Z(GL_{rk(1+J)}(\mathbb{F}_p))$ and $Z(SL_{rk(1+J)}(\mathbb{F}_p))$. In particular, by the First Isomorphism Theorem, we proved the relationship between $\mid GL_{rk(1+J)}(\mathbb{F}_p) \mid$ and $\mid SL_{rk(1+J)}(\mathbb{F}_p) \mid$. We noticed that since each $R^*$ of the classes of the rings studied had different ranks, the automorphisms $Aut(R^*)$ obtained yielded unique structures for every particular case.

Finally, we counted the number of automorphisms of $R^*$, that is $\mid Aut(R^*) \mid$ . Since $Aut(\mathbb{Z}_{p^r-1}) \cong (\mathbb{Z}_{p^r-1})^*$, $\mid Aut(\mathbb{Z}_{p^r-1}) \mid = \varphi(p^r-1)$ where $\varphi$ is the Euler$'$s phi- function. A natural problem in group theory is to determine all the possible ways of representing a given group as matrices, so we then counted the number of automorphisms of $(1+J)$ for the various cases exhaustively by using the the invertible matrix approach and considered all the possible extensions.

### 4.2 Conclusion

After a number of considerations from our results, for instance, the ranks of $1 + J$, the values of $p$ and $e_i$ for all $i$, we developed both the structure and order theorems for the automorphisms of the units groups $R^*$ of the classes of finite rings in question. These considerations contributed to the different structures and orders of $Aut(R^*)$ for each particular case. This indeed generalizes the classification and the properties of these finite rings up to isomorphism. The main results of this study have been captured in Theorems 3.5.1, 3.5.2, 3.7.1, 3.7.2, 3.9.1 and 3.9.2.

### 4.3 Recommendations

The classification of finite rings still remains an open problem. Several tools, ideas and geometrical properties of finite rings can still be explored in order to contribute towards this endeavour. In particular, a block triangular matrix approach can be used to characterize automorphisms of $p-$groups. Thus our research leaves some gaps worth a study. Therefore, for future research, we recommend that the following studies can be attempted:

(1) Automorphisms of unit groups of local rings whose index of nilpotence of the Jacobson radical is greater than four.

(2) Effect of Automorphisms of the unit groups of finite rings to the rate of convergence of random processes.

**REFERENCES**


[1] Abbasi G. Q. (1985), *Automorphism Groups of Certain metabelian $p-$groups of maximal class*, Punjab Univ. J. Math. (Lahore), 18, 55-62.

[2] Abraham R. P. (1998), *Normal $p-$subgroups of the automorphism group of an abelian $p-$group* , J. Algebra, 199(1), 116-123.

[3] Agrawal M. (2006), *Morphisms of Rings and Applications to Complexity*, PhD Thesis, Indian Institute of Technology, Kanpur.

[4] Agrawal M., Kayal N. and Saxena N. (2004), *Primes in $p$*, Annals of Mathematics, Vol. 160, 2, 781-793.

[5] Alexander H. (1996), *Konstruction transitiver Permutations gruppe*, PhD thesis, RWTH Aachen.

[6] Alkhamees Y. (1991), *The Determination of the Group of Automorphisms of a finite Chain Ring of characteristic $p$,* Quart. J. Math. Oxford (2), 42, 387-391.

[7] Alkhamees Y. (1981), *Finite Rings in which the Multiplication of Any two zero Divisors is Zero,* Arch. Math. 37. 144-149.

[8] Alkhamees Y. (1981), *The Enumeration of Finite Principal Completely Primary Rings,* Abhandlungen Math. Sem. Uni. Hamburg, 51, 226-231.

[9] Alkhamees Y. (1994), *Finite Completly primary rings in which the product of any two zero divisors of a ring is in its coefficient subring,* Internat. J. Math. and Math. Sci. 17. No.3, 463-468.

[10] Ayoub C. W. (1969), *On finite primary rings and their groups of units,* Compositio Math. 50, 247-252.

[11] Baartmans A. H. and Woeppel J. J. (1976), *The Automorphism group of a $p-$group of maximal class with an abelian maximal subgroup,* Fund. Math. 93(1), 41-46.

[12] Ban G. A. and Yu S. X. (1994), *A counterexample to Curran's Third Conjecture,* Adv. in Math. (China), 23(3): 272-274.

[13] Beider K. I. (1977), *A ring of Invariants under the Action of a Finite Group of Automorphisms of a ring,* Uspekhi Math. Nauk., 32, 193, 159-160.

[14] Bidwell J. N. S. (2008), *Automorphisms of Direct Products of Finite Groups II,* Arch. Math. 91, 481-489.

[15] Bidwell J. N. S. and Curran M. J. (2006), *Automorphisms of A Split Metacyclic $p-$group,* Arch. Math.

[16] Bidwell J. N. S. Curran M. J. and Mccaughan D. J. (2006), *Automorphisms of Direct Products of Finite Groups,* Arch. Math. 86, 111-121.

[17] Bondarchuk Y. V. (1984), *Structure of Automorphism Groups of the Sylow $p-$subgroups of the Symmetrical group $S_{p^n}(p = 2)$,* Ukr. Math. Zh, 36(6), 688-694.

[18] Bryant R. M. and Kovacs L. G. (1978), *Lie Representations and Groups of prime power order,* J. London Math. Soc., (2) 17, 415-421.

[19] Caranti A. and Scoppola C. M. (1990), *A remark on the orders of $p-$groups that are automorphism groups,* Boll. Un. Mat. Ital. A(7), 4(2): 201-207.

[20] Caranti A. and Scoppola C. M. (1991), *Endomorphisms of two-generated metabelian groups that induce the identity modulo the derived group,* Arch. Math. 17 . 218-227.

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

[22] Cheng Y. (1982), *On Finite $p-$groups with cyclic commutator subgroups,* Arch. Math., 39. 295-298.

[23] Chikunji C. J. (1999), *On a Class of Finite Rings,* Comm. Algebra, 27, 5049-5081.

[24] Chikunji C. J. (2005), *Unit groups of cube radical zero commutative completely primary finite rings,* Int. Journal of Math. and Math. Sci., 4, 579-592.

[25] Chikunji C. J. (2005), *Unit groups of a certain class of completely primary finite rings,* Mathematical Journal of Okayama University, 47, 39-53.

[26] Chikunji C. J. (2008), *On unit groups of completely primary finite rings,* Mathematical Journal of Okayama University, 50, 149-160.

[27] Chikunji C. J. (2008), *Automorphisms of completely primary finite rings of characteristic p,* Colloq. Math. 111 91-113.

[28] Chikunji C. J. (2008), *Automorphism Groups of Finite Rings of Characteristics $p^2$ and $p^3$,* Glasnik Matematicki, 43, No. 63, 25-40 .

[29] Corbas B. (1969), *Rings with finite zero divisor,* Math. Ann. 181, 1-7.

[30] Curran M. J. (1988), *Automorphisms of a certain $p-$group, $p-$odd,* Bull. Austral. Math. Soc., 38(2): 299-305.

[31] Curran M. J. (1990), *A note on $p-$groups that are Automorphism groups,* Rend. Circ. Math. Palermo, 23(2): 57-61.

[32] Cutolo G., Smith H. and Wiegold J. (2003), *$p-$groups with maximal class as automorphism groups,* Illinois J. Math. 47(1-2).

[33] Davitt R. M and Otto A. D. (1971), *On the Automorphism group of a finite $p-$group with central quotient metacyclic,* Proc. Amer. Math. Soc., 30, 467-472.

[34] Dolzan D. (2002), *Group of units in a finite ring,* J. Pure APP. Algebra, 170, No 2-3, 175-183.

[35] Durbin J. R. and McDonald M. (1971), *Groups with a characteristic cyclic series,* J. Algebra, 18, 453-460.

[36] Felsch V. and Neubuser J. (1968), *Uber ein programm zur Berechnung der Automorphismeng ruppe einer endlichen Gruppe,* Numer. Math. 11; 277-292.

[37] Felsch V. and Neubuser J. (1970), *On a programme for the determination of the automorphism group of a finite group,* Computational Problems in Abstract Algebra, Oxford, Pergamon Press; Oxford london, Edinburg, 59-60.

[38] Fitting H. (1934), *Uber die direkten produktzerlegungen einer Gruppe in direkt unzerlegbare Faktoren*, Math. Z. 39, 16-34.

[39] Fuchs L. (1960), *Abelian Groups,* 3rd ed., International Series of Monographs on Pure and Applied Mathematics, Pergamon Press, New York.

[40] Ganske G. and McDonald B. R. (1973), *Finite Local rings,* Rocky Mountain J. Math. 3, No. 4.

[41] Gilmer R. W. Jr. (1963), *Finite rings having a cyclic multiplicative group of units,* American Journal of Mathematics, 85,447-452.

[42] Glasby S. P. and Howlett R. B. (1992), *Extraspecial towers and Weil representaions,* J. Algebra, 151(1), 236-260.

[43] Gorenstein D. (1968), *Finite Groups,* Harper and Row Publishers, New york.

[44] Griess R. L. Jr. (1973), *Automorphisms of extra special groups and nonvanishing degree 2 cohomology,* Pacific J. Math., 48, 403-422.

[45] Han J. (2006), *The General Liner Groups over a finite Ring,* Bull. Korean Math. Soc., 43, 619-626.

[46] Heineken H. and Liebeck H. (1973), *On $p-$groups with odd order automorphism groups,* Arch. Math. (Basel) 24, 464-471.

[47] Heineken H. and Liebeck H. (1974), *The Occurance of finite groups in the automorphism group of nilpotent groups of class 2,* Arch. Math. 25, 8-16.

[48] Hillar C. and Rheah D. (2007), *Automorphisms of an abelian $p-$group,* Amer. Math. Monthly, 114, 917-922.

[49] Horosevskii M. V. (1971), *The Automorphism Groups of finite $p-$groups,* Algebra and Logic, 10, 54-57.

[50] Horosevskii M. V. (1973), *The Automorphism Groups of wreath products of finite groups,* Siberian Math. J, 14: 453-458.

[51] Hughes A. (1980), *Automorphisms of nilpotent groups and supersolvable orders,* Proc. Sympos. Pure Math, 37, 205-207.

[52] Huppert B. (1967), *Endriche Gruppen. I,* Die Grundlehren der Mathematischen Wissenschaften, Band 134. Springer- Vergal, Berlin.

[53] Isaacs I. M. (1971), *Symplectic Action and the Schur Index In Representation Theory of Finite Groups and Related topics,* Amer. Math. Soc., Providence, R.I, Vol. XXI, 73-75

[54] Isaacs I. M. (2006), *The Automorphism Groups of the extraspecial $p-$ groups,* group-pub-forum mailing list at group pub-forum@list.math.bath.ac.uk.

[55] Jamali A. R. (2002), *Some new non-abelian 2-groups with abelian automorphism groups,* J. Group Theory, 5(1): 53-57.

[56] Janusz G. J. (1966), *Separable Algebras over commutative rings,* Trans. Amer. Math. Soc. 122, 461-497.

[57] John C. and Deker H. F. (2001), *Automorphism group computation and Isomorphism testing in finite groups,* Preprint.

[58] Jonah D. and Konvisser M. (1975), *Some non-abelian $p-$groups with abelian automorphism groups,* Arch. Math. (Basel), 26: 131-133.

[59] Juhasz A. (1982), *The group of Automorphisms of a class of finite $p-$groups,* Trans. Amer. Math. Soc., 270(2), 469-481.

[60] Kado J. (1984), *The fixed subrings of a finite group of Automorphisms $X_0-$Continuous Regular Rings,* Osaka J. Math. 21, 683-686.

[61] Kharchenko V. K. (1991), *Automorphiosms and Derivations of Associative Rings,* Institute for Mathematics Novosibirsk U.S.S.R, Vo. 69, Kluwer Academic Publishers, London.

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

[63] Lawton R. (1978/79), *A note on a theorem of Heineken and Liebeck,* Arch. Math. (Basel), 31(5); 520-523.

[64] Leedham-Green C. R. and McKay S. (2002), *The Structure of Groups of prime power order,* Vol.27 of *London Mathematical Society Monographs.* New Series, Oxford University Press, Oxford Science Publications.

[65] Lentoudis P. (1985), *Determination du groupe des automorphismes du p-grupe de Sylow du groupe symetrique de degre $p^m$ l'idee de la methode,* CR. Math. Rep. Acad. Sci. Canada, 7(1), 67-71.

[66] Lentoudis P. (1985), *Determining the Automorphism Groups of Sylow p-group of the symmetric group of degree $p^m$: the ideas of the methods,* CR. Math. Rep. Acad. Sci. Canada, 7(5), 325.

[67] Lentoudis P. (1985), *Determination du groupe des automorphismes du p-grupe de Sylow du groupe symetrique de degre $p^m$ :resultats*, CR. Math. Rep. Acad. Sci. Canada, 7(2), 133-136.

[68] Macdonald I.D. (1968), *The Theory of Groups,* Clarendon Press, Oxford.

[69] Macdonald I. G. (1995), *Symmetric functions and Hall polynomials,* Oxford Mathematical Monographs. The Clarendon Press, Oxford University Press, New York, Second Edition.

[70] Malome J. J. (1984), *$p-$groups with non-abelian Automorphism groups with all automorphisms central,* Bull. Austral. Math. Soc., 29(1): 35-37.

[71] Martin W. (1993), *Isomorphisms of modular group algebras: An algorithm and its application to groups of order* $2^6$*,* J. Symbolic Comput. 15, 211-227.

[72] Menengazzo F. (1993), *Automorphisms of $p-$groups with cyclic Commutator Subgroup,* Rend. Sem. Math. Padova, Vol.90, 81-101.

[73] Miech R. J. (1975), *On $p-$groups with a cyclic commutator subgroup,* J. Austral. Math. Soc., 20, 178-198.

[74] Miech R. J. (1978), *The metabelian $p-$groups of maximal class,* Trans. Amer. Math. Soc., 236: 93-119.

[75] Michael S. J. (1994), *Computing Automorphisms of finite soluble groups,* PhD. Thesis, Australian National University.

[76] Miller G. A. (1913), *A non-abelian group whose group of isomorphisms is abelian*, Messenger Math. 43; 124-125.

[77] Morgado E. R. (1980), *On the Group of Automorphisms of a finite abelian $p-$group,* Ukranian Math. J. 32(5), 403-407.

[78] Morgado E. R. (1981), *On the Group of automorphisms of abelian $p-$groups,* Cienc. Math. (Havana), 2(2): 105-119.

[79] Newman M. F. and O'Brien E. A. (1987), *A CAYLEY library for the groups of order dividing 128.* In Group Theory, Singapore, 437-442.

[80] Newman M. F. (1977), *Determination of groups of prime-power order,* Springer-Vergal, Berlin, Heidelberg, New York, 73-84.

[81] Oduor M. O. (2012), *Automorhisms of a certain class of Completely Primary Finite Rings,* IJPAM, 74, No. 4, 465-482.

[82] Oduor M. O., Ojiema M. O. and Mmasi E. (2013), *Units of commutative completely primary finite rings of characteristic $p^n$,* International Journ. of Algebra, 7, No.6, 259-266.

[83] Oduor O. M. and Ojiema O. M. (2014), *Unit Groups of Some Classes of Power Four Radical Zero Commutative Completely Primary Finite Rings,* IJA, 8, No.8, 357-363.

[84] O'Brien E. A. (1990), *The $p-$group generation algorithm,* J. Symbolic Comput. 9; 677-698.

[85] O'Brien E. A (1992), *Computing Automorphism groups of $p-$group,* Computational Algebra and Number Theory, Sydney, Kluwer Academic publishers, Dordrecht, 85-92.

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

[87] Shoda K. (1928), *Uber die Automorphismen einer endlichen Abelschen Gruppe,* Math. Ann. 100, 674-686.

[88] Stewart I. (1972), *Finite rings with a specified groups of units,* Math. Z, 126, 51-58.

[89] Struik R. R. (1982), *Some non-abelian 2-groups with abelian automorphism groups,* Arch. Math. (Basel) 39(4): 299-302.

[90] Webb U. M. (1981), *The Occurance of groups of Automorphisms of nilpotent $p-$groups,* Arch. Math. (Basel), 37(6), 481-498.

[91] Webb U. M. (1983), *The Number of Stem Covers of an elementary abelian $p-$group,* Math. Z, 182(3),327-337.

[92] Wilson R. S. (1973), *On the structure of finite rings,* Compositio. Math. 26.

[93] Winter D. L (1972), *The Automorphism Group of an extraspecial $p-$group,* Rocky Mountain. Math. Monthly, **2(2)**, 159-168.

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

[95] Wolf B. (1997), *A note on $p^{'}-$Automorphisms of $p-$groups $P$ of maximal class centralizing the center of $P$,* J. Algebra, 190(1), 163-171.

[96] Ying J. H. (1977), *On finite groups whose automorphism groups are nilpotent,* Arch. Math. (Basel) 29(1) 41-44.