ON THE CHARACTERIZATION OF THE UNIT GROUPS OF A CLASS OF TOTAL QUOTIENT RINGS

Wanambisi Aldrin Wekesa

A Thesis submitted in partial fulfillment of the requirements for the degree of Doctor of Philosophy in Pure Mathematics of Masinde Muliro University of Science and Technology

October 2017

DECLARATION

This research thesis is my original work prepared with no other than the indicated sources and support and has not been presented elsewhere for a degree or any other award.

Signature..... Date .....

Name: Wanambisi Aldrin Wekesa

SEP/H/04/10

APPROVAL

We the undersigned certify that we have read and hereby recommend for acceptance of Masinde Muliro University of Science and Technology a research thesis entitled, ´´On the Characterization of the Unit Groups of a Class of Total Quotient Rings. ``

1. Signature..... Date.....

Prof. Maurice Owino Oduor

Department of Mathematics and Computer Science

University of Kabianga.

2. Signature..... Date.....

Prof. Shem Aywa

Department of Mathematics

Kibabii University.

ABSTRACT

Let R be a completely primary finite ring of characteristic p^k, where p is a prime and k is a positive integer. Such finite rings have been studied extensively in recent years and the tools necessary for describing completely primary finite rings have been available for some time. However, their characterization is not exhaustive. Several attempts have been made in the recent past in the characterization of the unit groups of this class of rings though not in general. The characterization of a finite abelian group is precisely known and from the fundamental theorem of finitely generated abelian groups, it has been represented as a direct product of cyclic groups. If R is a finite field then $U(R)$ the unit group of R is cyclic. Suppose S is a saturated multiplicative subset of R so that R_S is a total quotient ring of R obtained by the localization of R at the maximal ideal $J(R)$. Since R is local, then $R \cong R_S$. We have characterized the unit groups of R_S, denoted $U(R_S)$ as $U(R_S) = \mathbb{Z}_{p^r-1} \times \left(\frac{1}{1} + J(R_S)\right)$ by determining the generators of the group $\frac{1}{1} + J(R_S)$. The methods used include construction of R_S using the method of idealization, proofs and verification of the proposed statements and claims. The results obtained, provide an alternative understanding of the structures of unit groups of these classes of finite rings and provides a partial solution to the problem of isomorphic rings with similar groups of units. This results also find practical applications in various fields including Computer Algebra and forms and structure of elements in chemistry.

TABLE OF CONTENTS

INDEX OF NOTATIONS

R: A commutative ring

R_S: A Total quotient or Localized ring

$U(R_S)$: A group of units in R_S

$J(R_S)$: Jacobson radical of R_S

$M_2(\mathbb{R})$: A 2×2 matrix consisting of real entries

$ann(I)$: Annihilator of I

$\mathbb{Z}_n$: Ring of integers modulo n

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

$CharR_S$: Characteristic of R_S

$ker\phi$: Kernel of ϕ

$|X|$: Order of X

$< (r, s) >$: Cyclic group generated by (r, s)

$[(r, s)] = \left[\frac{r}{s}\right]$: The equivalence class of the element (r, s)

$| x, y |$: The greatest common divisor of x and y.

$R - S$: The complement of S relative to R.

$Spec(R)$: The spectrum of R.

(x): The ideal generated by x

CHAPTER ONE

INTRODUCTION

1.1 Background information

Finite commutative ring theory is a fast-developing subject and has recently been seen to have important applications in theoretical areas like Combinatorics, Finite Geometries and the Analysis of Algorithms. Moreover, in the last twenty years, there has been a growing interest in application of finite commutative rings and ideals over finite Non-Commutative rings to Algebraic Cryptography and Coding Theory [17, 20]. In fact, several codes over finite fields, which are widely used in Information and Communication Theory, have been investigated as images of codes over Galois rings (especially over the ring of integers modulo 4).

Although finite rings have been studied extensively in recent years by Corbas [12, 13], Edmund [16], Janusz [22], Ganesan [18], Raghavendran [35] and Wilson [39], and the tools necessary for describing completely primary finite rings have been available for some time, their classification into well known structures (which is essentially given in Chikunji [6], [7], [8], Ayoub [5], Dolzan [15], Owino [29, 30, 31, 32], Clark [10] and [27]) is not exhaustive. As such is the case, since completely primary finite rings have not been characterized in general. Furthermore, given a completely primary ring R and a subset S of invertible elements of R, the ring of quotients $S^{-1}R$ is representative of local rings. In this context, the process of obtaining quotient rings from R is called *Localization*

Several attempts have been made in the recent past in the characterization of the unit groups of some commutative rings though not in general [27]. Moreover, other previous studies for instance in [6, 7, 8, 12, 13, 29, 35] have restricted the classes of rings under consideration. On the other hand, the characterization of a finite abelian group is precisely known and from the fundamental theorem of finitely generated abelian groups, it has been represented as a direct product of cyclic groups. If R is a finite field then $U(R)$ the unit group of R is cyclic.

Moreover, if R is a finite commutative ring, then, $U(R)$ is isomorphic to a direct product of cyclic groups [35]. It is known that all completely primary finite rings are local.

Much of the recent work on these rings has demonstrated the fundamental importance in the structure theory of finite rings with identity. These rings play an important role in the classification of finite rings with identity [35]. Generally, in ring theory, localization is a useful technique. Problems dealing with properties of objects that may be preserved under localization may be best dealt with by viewing the localization in a specific category of those objects with the property under consideration and morphisms preserving that property. This study therefore seeks to determine and classify in general the structures of the unit groups of some classes of localized completely primary finite rings which have been constructed in terms of quotient rings.

1.2 Basic Concepts

In this section we recall some known definitions and results required in the sequel.

Definition 1.2.1 ([36]). *A commutative ring R with identity 1 is a non-empty set endowed with two binary operations of addition and multiplication such that;*

(i) R is an abelian group under addition

(ii) R is a multiplicative semigroup

(iii) Multiplication is commutative, that is $ab = ba\ \forall a, b \in R$

(iv) Multiplication distributes over addition $a(b + c) = ab + ac$ and $(a + b)c = ac + bc$

(v) $\exists x \in R$ such that for each $x \in R$, $x1 = 1x = x$.

Definition 1.2.2 ([36]). *Let R be a commutative ring and S be the set of elements which are not zero divisors in R, the localization of the ring R with respect to the set S yields a total quotient ring $S^{-1}R = R_S$.*

Definition 1.2.3. *[36] A group G is called soluble if it has a subnormal series whose factor groups are all abelian.*

Definition 1.2.4 ([23]). *An ideal I of a ring R is called a nil ideal if all its elements are nil potent; if for some positive integer n, $I^n = (0)$,then I is called a nil potent ideal of R.*

Definition 1.2.5 ([36]). *Let $R[x]$ be the ring of polynomials over a commutative ring R. A polynomial $f(x) \in R[x]$ is called monic if the coefficient of highest power of x in $f(x)$ is equal to 1, the identity in R.*

Definition 1.2.6 ([36]). *Let R be a ring and T be a sub-ring of R. The Centralizer of T in R is the set $\{r \in R : rt = tr \forall t \in T\}$ and is denoted by $Z_R(T)$.*

Definition 1.2.7 ([36]). *The Jacobson radical of a ring $R, J(R)$ is the intersection of all maximal left[right] ideals of R. Indeed it contains all left,right nil ideals of R and if $r \in J(R)$, then $1 + r$ is a unit in R*

Definition 1.2.8 ([37]). *An* Ideal *in a commutative ring R is a subset I of R such that;*

(i) $0 \in I$

(ii) $a, b \in I$ *implies that* $a + b \in I$

(iii) $a \in I$ *and* $r \in R$ *then* $ra = ar \in I$.

Definition 1.2.9 ([36]). *An element x of a ring R is quasi-regular if $1 + x$ is a unit or equivalently there exists $y \in R$ such that $x + y + yx = 0$ and $x + y + xy = 0$. Thus, a one-sided ideal I is quasi- regular provided that it consists of quasi-regular elements.*

Definition 1.2.10 ([36]). *Let R be a ring , $m \geq 1$. Then m is called the index of nilpotency of $J(R)$ if $(J(R))^m = \{0\}$ and $(J(R))^{m-1} \neq \{0\}$.*

Theorem 1 ([36]). *Let R be a local ring, then $J(R)$ is nilpotent.*

Theorem 2 ([36]). *Let R be a ring and I a quasi-regular ideal of R. Then $a \in R$ is a unit if and only if $a + I$ is a unit in R/I.*

Definition 1.2.11 ([36]). *A ring R is called a duo ring if every right or left ideal of R is a two-sided ideal of R.*

Definition 1.2.12 ([23]). *Let R be a ring U be an $R-$module which has a composition series of $R-$submodules*

$$U = U_0 \supset U_1 \supset ... \supset U_n = \{0\}$$

Then n is called the length of U as an $R-$module.

Theorem 3 ([23]). *Let R be a ring and U an $R-$module. If*

$$U = U_0 \oplus U_1 \oplus ... \oplus U_n, U_i \neq \{0\} \quad \forall i, 0 \leq i \leq n$$

and

$$V = V_0 \oplus V_1 \oplus ... \oplus V_m, V_j \neq \{0\} \quad \forall j, 0 \leq j \leq m$$

such that $n \leq m$ *and* $U_i \subseteq V_j$ *for each* i, $0 \leq i \leq n$ *and* $0 \leq j \leq m$, *then* $U_i = V_j$ *and* $n = m$

Remark 1 ([27]). *Let* R *be a ring,* U *an* $R-$*module and* I *an ideal of* R *such that* $IU = \{0\}$. *Then* U *is an* $R/I-$*module such that for any* $a + I \in R/I$ *and* $u \in U$,

$$(a + I)u = au + I$$

Theorem 4 ([27]). *(Primary decomposition)*

(i)Every finite abelian group G *is a direct sum of its p-primary components, that is* $G = G_{p_1} \oplus G_{p_2} \oplus ... \oplus G_{p_n}$.

(ii) Two finite abelian groups G *and* G' *are isomorphic iff* $G_p \cong G'_p$ *for every prime integer* p.

Definition 1.2.13 ([23]). *A subset* S *of a ring* R *is a subring if;*

(i) $1 \in S$

(ii) $a, b \in S$ *implies that* $a - b \in S$

(iii) $a, b \in S$ *implies that* $ab \in S$

Definition 1.2.14 ([23]). *A field* $\mathbb{F}$ *is a commutative division ring, that is, a commutative ring in which every non zero element is invertible. So,* $\forall a \in \mathbb{F}$, *there is an element* $a^{-1} \in \mathbb{F}$ *with* $aa^{-1} = a^{-1}a = 1$. *In other words, a commutative ring* R *is a field if and only if the non zero elements of* R *forms a multiplicative group.*

The ring R itself and the subset consisting of zero alone denoted $\{0\}$ are always the trivial ideals in R. An ideal $I \neq R$ is called a proper ideal.

Definition 1.2.15 ([23]). *An ideal* I *is called* prime *if* $ab \in I$ *implies that either* $a \in I$ *or* $b \in I$.

Definition 1.2.16 ([36]). *An ideal* I *of a ring* R *is said to be maximal if;*

(i) $I \neq R$

(ii) Given an ideal $J \supseteq I$ *then* $I = J$ *or* $J = R$

A ring R *is said to be* local *if it has a unique maximal ideal.*

Definition 1.2.17 ([36]). *The Nilradical* $N(R)$ *of a ring* R *is the set* $\{x \in R | x^n = 0\}$ *of nilpotent elements of* R *for some positive integer* n

Definition 1.2.18 ([9]). *The Jacobson radical* $J(R)$ *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.*
The Nilradical of R *is the intersection of all the prime ideals of the ring.*

Definition 1.2.19 ([3]). *Let* R *be a ring with unity. Suppose* I *is an ideal of* R, *then an annihilator of* I *is the set* $ann(I) = \{x \in R | Ix = xI = (0)\}$

Definition 1.2.20 ([5]). *Two non-zero elements* a *and* b *of a ring are respectively called a left zero divisor and right zero divisor if* $ab = 0$. *An element that is both a left and a right zero divisor is called a two-sided zero divisor. If the ring is commutative then the left and right zero divisors are the same.A non zero element of a ring that is not a zero divisor is called regular.*

We have the following characterization of local rings;

Proposition 1 ([35]). *For a ring* R *the following statements are equivalent:*

(i) R *is a local ring;*

(ii) R *has a unique maximal left ideal;*

(iii) $J(R)$ *is a maximal left ideal;*

(iv) The set of elements of R *without left inverses is closed under addition;*

(v) $R/J(R)$ *is a division ring;*

(vi) $J(R) = \{x \in R : x \notin U(R)\}$;

(vii) If $x \in R$, then either x or $1+x$ is a unit.

Definition 1.2.21 ([11]). *Let R be a ring and S a multiplicatively closed subset of R which does not contain zero element. The set $R_S = \{[(r,s)] : r \in R, s \in S\}$ is called the ring of quotients of R with respect to S. The process of passing from R to R_S is called localization at S.*

Definition 1.2.22 ([11]). *Let R be a ring. Then the smallest sub-ring $\mathcal{P}$ of R containing the identity $1 \neq 0$ is called a prime subring of R if for any integer n, $n-1$ is a unit in R, and $(n-1)^{-1} \in \mathcal{P}$. If $\mathcal{P}$ is a field, then it is called the prime subfield of R.*

But the prime sub field of $R/J(R)$ is isomorphic to $\mathbb{Z}/p\mathbb{Z} = \mathbb{Z}_p$. Hence $\mathcal{P} + J(R)/J(R)$ is the prime subfield of $R/J(R)$

Proposition 2 (see [35]). *Let R be a Galois ring of the form $GR(p^n, r)$. Then $R = \mathbb{Z}_{p^n}[b]$, where $b \in R$ is a root of monic polynomial $g(x)$ over $\mathbb{Z}_{p^n}$ which is irreducible modulo p and of degree r.*

Proposition 3 ([11]). *Let R be a finite local ring. Then R is a Galois ring if and only if $J(R) = pR$ for some prime number p.*

Proposition 4 ([35]). *Let R be a Galois ring of the form $GR(p^n, r)$. Then R has a unique Galois sub-ring of the form $GR(p^n, t)$ if and only if $t|r$.*

Proposition 5 ([3]). *A sub-ring of a Galois ring is not necessarily Galois and a ring is Galois if and only if it is the principal ideal ring.*

Proposition 6 ([**?**]). *Let R, R' be two Galois rings of the same characteristic. Then $R \cong R'$ if and only if $R/J(R) \cong R'/J(R')$.*

All symbols introduced in this section will retain their meaning throughout this thesis unless otherwise stated.

1.3 Localization

Let R be a commutative completely primary finite ring with identity 1. A subset $S \subset R$ is multiplicative if $1 \in S, 0 \in S$ and $xy \in S$ if $x, y \in S$. Moreover, S is saturated if $y \notin S$ implies $x \notin S$ and y does not divide x. The set of equivalence classes $R \times S$ under the equivalence relation $(r, s) \sim (r', s')$ if and only if there exists $v \in S$ such that $v(rs' - r's) = 0$ shall be denoted by R_S or $S^{-1}R$. The equivalence class of (r, s) is denoted by $\left[\frac{r}{s}\right]$. Using addition and multiplication of quotients, it is easily verified that $S^{-1}R = \left\{\left[\frac{r}{s}\right] \mid r \in R, s \in S\right\}$ is a commutative ring with identity $\left[\frac{1}{1}\right]$. We may also regard $S^{-1}R$ as an $R-$algebra with the structure morphism $f : R \to S^{-1}R$ defined by $r \mapsto \left[\frac{r}{s}\right]$ verifiable as a ring homomorphism. The $R-$algebra structure on $S^{-1}R$ is defined by $r \cdot \left[\frac{r'}{s}\right] = \left[\frac{rr'}{s}\right]$ [11].

Let $f : R_1 \to R_2$ be a ring homomorphism then R_2 is an R_1-algebra (via f). Suppose $I \subseteq R_1$ is an ideal, then I can be expanded to R_2 via $I'_e = (f(I)) = f(I)R_2 = \sum_i a_i r_i, a_i \in f(I), r_i \in R_2$.
If $J \subseteq R_2$ is an ideal, then $J_C = f^{-1}(J) = f^{-1}(J) \cap R_1$ is the contraction of J to R_1. The following result is easily proved using Zorn's Lemma.

Theorem 5 ([36]). *Let R be a commutative ring with identity 1. Suppose $S \subseteq R$ is a multiplicative, then there exists a prime and maximal ideal P with respect to inclusion among all the ideals in the complement of S in R.*

Theorem 6 ([36]). *Let R be a commutative ring with identity 1. Then the following are equivalent:*

i. S is saturated

ii. $R - S = \cup_{i \in \Lambda} P_i$ where $\{P_i\} = Spec(R)$ such that $P_i \cap S = \phi$

Proof. Let S be a subset of R consisting of units and $x \in S$. Then $(x) \cap S = \phi$. By Zorn's Lemma, there exists an ideal P with $(x) \subseteq P$ such that $P \cap S = \phi$ and P is a prime ideal. This implies $x \in \cup_{i \in \Lambda} P_i$. On the other hand, let $x \in \cup_{i \in \Lambda} P_i$, then, there exists a prime ideal

P such that $x \in P$. But $P \cap S = \phi$ so $x \in R - S$.

Now, suppose (ii) holds. If $x \in S$ and $y \mid x$, then $x = yr$ for some $r \in R$. Since $x \in S$, then $x \in R - P_i, \forall i$. Suppose $y \notin S$. Then $y \in P_i$ for some i implying that $x = ry \in P_i$ to mean $x \notin S$, a contradiction. Thus $y \in S$, so S is saturated, which completes the proof. □

The following are examples of saturated sets

- Let R be a commutative ring with identity 1. The set of all units in R, denoted $U(R)$ is a saturated multiplicative set and the complement of $U(R)$, that is $R - U(R) = \cup_{i \in M} M_i$ where M_i are maximal ideals in R.
- The set of all non-zero divisors is a saturated multiplicative set.
- $R - P$ is a saturated multiplicative set if P is a prime ideal.

Theorem 7 ([36]). *(Universal property of the Quotient Ring) The canonical homomorphism $f : R \to S^{-1}R$ defined by $f(r) = \left[\frac{r}{s}\right] \forall s \in S$ is an $R-$algebra homomorphism, so that f satisfies the following axioms*

i. f is a ring homomorphism and $f(s) \subseteq U(S^{-1}R) \forall s \in S$.

ii. If $\theta : R \to R'$ is a ring homomorphism with $\theta(S) \subseteq U(R')$, then there exists a unique homomorphism $\psi : S^{-1}R \to R'$ such that $\psi \cdot f = \theta$.

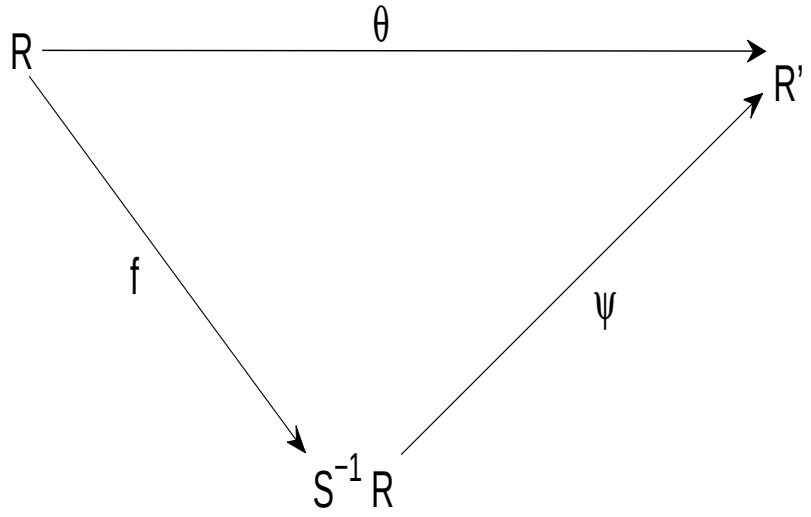
Property (ii) is called the universal property of the ring of quotients.

Proof. To prove $(i), f(s) = \left[\frac{s}{1}\right]$ and $\left[\frac{s}{1}\right]\left[\frac{1}{s}\right] = \left[\frac{1}{1}\right]$ implies that $f(s)$ is invertible.
Now suppose f and θ are described as in (ii). If $\psi\left(\left[\frac{r}{s}\right]\right) = \theta(r)(\theta(s))^{-1}$, then $\psi \circ f = \theta$ easily follows from the diagram: □

Theorem 8 ([11]). *Let S be a multiplicative set of a unital commutative ring R. Then*

(i) Proper ideals of the ring $S^{-1}R$ are of the form $IS^{-1}R = S^{-1}I = \left\{\left[\frac{i}{s}\right] \mid i \in I, s \in S\right\}$ with $I \subseteq R$ an ideal and $I \cap S = \phi$.

(ii) Prime ideals in $S^{-1}R$ are of the form $S^{-1}P$ where P is prime in R and $P \cap S = \phi$.



Universal property of the Quotient Ring

Proof. (i) Let J be a proper ideal of $S^{-1}R$, and $I = J \cap R$. Since $J \cap R$ is an ideal, I is an ideal. Next, suppose $I \cap S \neq \phi$. Take $s \in S \cap I \Rightarrow \left[\frac{s}{1}\right] \in J \Rightarrow J = R$, a contradiction , therefore $I \cap S = \phi$.

Now, we prove that $J = S^{-1}I$. Let $\left[\frac{i}{s}\right] = \left[\frac{i}{s}\right] \cdot \left[\frac{1}{s}\right] \in J$, so that $S^{-1}I \subseteq J$. On the other hand, let $j \in J$. Then $j \in \left[\frac{k}{s}\right]$ so that $\left[\frac{k}{s}\right] \cdot \left[\frac{s}{1}\right] \in J \Rightarrow \left[\frac{k}{1}\right] \in J$ and $k \in I$. Thus $J \subseteq S^{-1}I$.

(ii) Consider $I = S^{-1}P$ where $P \cap S = \phi$. Note that $P = I \cap R$. Suppose I is prime, $p_1p_2 \in P$ so that $\left[\frac{p_1p_2}{1}\right] \in I \Rightarrow \left[\frac{p_1}{1}\right] \in I$ or $\left[\frac{p_2}{1}\right] \in I \Rightarrow p_1 \in P$ or $p_2 \in P$. Then P is prime and $P \cap S = \phi$ implies $S^{-1}P$ is prime. Let $\frac{p_1}{s_1} \cdot \frac{p_2}{s_2} = \frac{p_1p_2}{s_1s_2} \in S^{-1}P$, then we can prove that $\left[\frac{p_1}{s_1}\right] \in S^{-1}P$ or $\left[\frac{p_2}{s_2}\right] \in S^{-1}P$.

□

Proposition 7 ([11])**.** *Let $S \subseteq R$ be multiplicative. Let I and J be ideals in R. Then $S^{-1}(I + J) = S^{-1}I + S^{-1}J$.*

Proof. Consider $\frac{i+j}{s} \in S^{-1}(I + J)$ where $i \in I$ and $j \in J$. Then $\frac{i+j}{s} = \frac{i}{s} + \frac{j}{s} \in S^{-1}I + S^{-1}J$ so that $S^{-1}(I + J) \subseteq S^{-1}I + S^{-1}J$. The other containment can be shown easily. □

The following theorem shows that localization commutes with taking quotients.

Theorem 9 ([11])**.** *Let R be a commutative ring with identity and $S \subseteq R$ a multiplicative subset, I is an ideal of R and $S = Im(S)$, the natural image of S in R/I, then $S^{-1}R/S^{-1}I \cong S^{-1}(R/I)$ as an $R-$algebra.*

Proof. The canonical map $R \to R/I \to S^{-1}(R/I)$ induces an $R-$algebra homomorphism $R \to S^{-1}(R/I)$ by $r \to \left[\frac{r}{1}\right]$. This map sends S to $U(S^{-1}(R/I))$.

By the universal property of quotient rings, this map induces an $R-$algebra homomorphism $S^{-1}R \to S^{-1}(R/I)$ by $\left[\frac{r}{s}\right] \to \left[\frac{r}{s}\right]$. This map also sends $S^{-1}I$ to 0, which induces an $R-$algebra homomorphism $\sigma : S^{-1}R/S^{-1}I \to S^{-1}(R/I)$. To establish isomorphism, it is possible to define by a similar sequence of steps, an $R-$algebra homomorphism $\theta : S^{-1}(R/I) \to S^{-1}R/S^{-1}I$ by $\theta\left(\left[\frac{r}{s}\right]\right) = \left[\frac{r}{s}\right]$. Consequently $\sigma\theta = \theta\sigma = id_{Hom}$. □

1.4 Statement of the problem

The problem of classification of finite rings has been overarching for decades. Several researchers have classified some classes of finite associative, commutative and non-commutative rings in to well known structures. For instance, Alkhamees [3] and Corbas [13] have classified finite rings in which the product of any two zero divisors is zero. On the other hand, Raghavendran [35], Chikunji [6],[7],[8], Owino [31] and Owino and Chikunji [30] among other scholars have characterized the groups of units of some classes of completely primary finite rings of characteristic p^k. However, the process of classification has not been done in a general setting for all unit groups. In particular, if R a finite ring and $S \subseteq R$ is the saturated multiplicative subset of R, the structure of the total quotient ring R_S is still scanty in the literature. In this thesis, we have characterized the unit groups of these rings of characteristic p^k, where p is a prime integer and k is a positive integer. We have determined the generators of the groups of units and represented them in terms of direct product of cyclic groups of prime power order.

1.5 Objective of the study

1.5.1 Main Objective

The primary objective of this study was to characterize unit groups of total quotient rings of characteristic p^k with $k = 1, 2, 3, \ldots, n$.

1.5.2 Specific Objectives

(i) To construct a total quotient ring of completely primary finite rings of characteristic p^k with $k = 1, 2, 3, \ldots, n$.

(ii) To determine the generators of the unit groups of the rings constructed in (i).

(iii) To characterize the unit groups determined in (ii).

1.6 Significance of the study

The study of the structure of unit groups of total quotient rings of characteristic p^k is an important contribution to knowledge towards the classification of finite rings. Our results

mark a useful step in the classification of total quotient finite rings.

CHAPTER TWO

LITERATURE REVIEW

In this chapter, we give a review of the literature related to our work.

2.1 Finite Rings

Determination and characterization of the structure of finite rings has been a subject of discussion in the past few decades. For instance, Alkhamees [3] has classified finite rings in which the product of any two zero divisors is zero. On the other hand, Raghavendran [35], Chikunji [6],[7],[8], Owino [31], Owino and Chikunji [30] among other scholars have characterized the groups of units of some classes of completely primary finite rings of characteristic p^k.

If we consider $f(x) \in \mathbb{Z}_{p^k}[x]$ as a monic polynomial of degree r irreducible modulo p, then, it is well known that $\mathbb{Z}_{p^k}[x]/(f(x))$ is the Galois ring of order p^{kr} and characteristic p^k and denoted as $GR(p^{kr}, p^k)$. Basically then, a Galois ring is an irreducible algebraic extension of degree r of the cyclic ring $\mathbb{Z}_{p^k}$, and, any two irreducible algebraic extensions of $\mathbb{Z}_{p^k}$ of degree r are isomorphic. This class of rings was first studied by Krull in 1924 and later rediscovered by Janusz [22], Raghavendran [35] among others in subsequent studies . In deed, Raghavendran described the structure of the multiplicative group of every Galois ring. The importance of Galois rings at least in our case is that if R is a completely primary finite ring of characteristic p^k, with Jacobson radical J such that $R/J \cong GF(p^r)$, then, R contains a unique copy (up to inner isomorphism) of $GR(p^{kr}, p^k) = R$ (see Janusz, [22]); hence a completely primary finite ring is a $GR(p^{kr}, p^k)$-bimodule whose structural theory was developed by Robert Wilson in [39]. Any finite ring contains a cyclic subring and it is quite possible that the cyclic subring is the largest Galois ring. So in essence, Wilson's work does not represent much of a step forward in the study of general finite rings. However in the study of completely primary finite rings, one can obtain a tractable complete characterization if one studies the Szele's representation over the largest Galois subring [39]. This can in particular include the complete characterization of their groups of units which is our main objective.

In [35], Raghavedran proved that any finite ring with identity will contain at least one Galois ring. The structures of the prime power rings were determined. This result gave an idea on how to prove the well known Wedderburn Theorem on finite division rings and a generalization of this Theorem to the case of completely primary finite rings (not necessarily commutative) which is exhibited as a ring of matrices over a field. Similarly, Raghavendran considered a problem posed by Ganesan, [18] and generalized by Eldridge in two private communications to Ganesan .

On the other hand, the paper illustrates the structures of all rings not necessarily possessing identity with p^2 elements and the structures of all rings possessing identity with p^3 elements where p is any prime integer. In particular it establishes that there is essentially only one non-commutative ring of order p^2 and to within isomorphism, there is only one ring of order p^3 with identity which is not commutative e.g the ring of all 2×2 upper triangular matrices over the field, $GF(p)$. This was noted by Edmund [16] in a series of papers.

Snapper [37] discussed extensively the properties of completely primary rings, primary rings and associated topics for the commutative case. His work extended some of these theories to the non-commutative case; most of them extend intact for the duo rings in which the left zero divisors are the right zero divisors and every left ideal is a right ideal. He considers a ring R to be completely N primary provided R/N is a field; in this definition if we substitute for N the symbols J and P, we have the definitions for completely J-primary and P-primary rings where P is a two sided ideal whose structures were exhausted in Edmund [16]. The work however did not give detailed structures of the ideals, zero divisors and even the units of that ring and therefore does not give complete structures of completely primary finite rings with which Edmund's rings share properties.

In Ganesan, [18], a ring with a finite number of zero divisors have been characterized. The main result which is contained in Theorem 1 of this paper is that, such a ring is finite and contains not more than $(n+1)^2$ elements, where $n \geq 1$ is the number of non-zero zero divisors. In such a case , 0 is also included as a zero divisor. Consequently, suppose the ring R possesses only the following $n \geq 1$ of non-zero zero divisors $z_1, z_2 ... z_n$ and $A_i = xz_i = 0$ is the annihilator ideal

consisting of all annihilators of z_i for $i = 1, 2, 3...n$ and $x \in R$, then clearly, since $z_i \neq 0, A_i$ is a finite ideal of R. Also, any finite commutative integral domain is a Galois field of p^k elements where p is a prime integer and k any positive integer.

In order to examine further the extent to which the claims by Ganesan in [18] hold, Janusz [22] restricts the findings to commutative separable algebras over commutative rings. The main ideas here are based on the classical Galois theory of fields. An arbitrary commutative ring with no idempotents except $0, 1$ and R-algebras separable and projective as R-modules are structured. The study dropped the assumptions that the algebras are projective and placed a restriction on R to be a local ring. This gives an external characterization of separable algebras. This is a very important result because it automatically characterizes local ring upon that restriction. However, not all local rings are completely primary thus there is need to deeply study the latter rings which is our main focus.

2.2 Completely primary finite rings

Suppose R is a ring and $U(R)$ its multiplicative group of units, then all such local rings with cyclic groups of units were determined by Ayoub [5] and the same case was also considered by Gilmer [21]. Gilmer showed that it is sufficient to consider (finite) primary rings. In this note, after proving a preliminary result (Theorem 1 in [22]), Ayoub 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 [10] has investigated $U(R)$ where the ideals form a chain and has shown that if $p \geq 3, k \geq 2$ and $r \geq 2$ then the units of the Galois ring $GR(p^{kr}, p^k)$ are a direct sum of a cyclic group of order $p^r - 1$ and r cyclic groups of order $p^k - 1$ (This was also done independently by Raghavendran in [35])

Stewart [38] considered a more general problem by proving that for a given finite group G(not necessarily abelian), there are upto isomorphism, only finitely many directly indecomposable finite rings having groups of units isomorphic to G. Ganske and McDonald [19] provided a solution for $U(R)$ when the local ring R has a Jacobson radical J such that $J^2 = (0)$ by

showing that

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

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

2.3 Total quotient rings

Little has been done with regard to the structure theory of quotient rings. Kainrath[25] has studied the quotients formed by unit groups of a semilocal ring R. He set two subrings R_1, R_2 of R such that $R_1 \subset R_2$ is an extension of rings such that R_1 is noetherian and semilocal and R_2 is a finitely generated R_1-module. The study established the properties of the quotients of R_1 and R_2 and their units. This study is limited to semilocal rings and therefore does not give an exact picture on the structures of local rings and their units.

Owino, Ojiema and Mmasi[33] have characterized the quotient groups of subgroups of the unit groups of a class of completely primary finite rings. They adopted the same constructions used in [32] and varied the invariants throughout before giving the general structures of the unit groups and consequently the quotients of the subgroups in question. Ongati and Owino in [28] determined the structures of the quotient groups $1 + J^i/1 + J^{i+1}$ for every characteristic of R such that $1 \leq i \leq k - 1$. The results in [33], are not exhaustive since the authors restricted their findings to subgroups of the unit groups characterized. As such is the case, quotient rings have not been characterized in general in terms of the structures of their unit groups.

2.4 Unit groups

The works of Chikunji [6, 8] focused on the structure of the groups of units of the ring $R = R_0 \oplus U \oplus V$ where $R_0 = GR(p^{kr}, p^k)$ is the Galois sub-ring of the ring R while V and U are finitely generated R_0-modules such that $J^3 = (0), J^2 \neq (0)$. Owino [29] however extended this result and determined the generators of $U(R)$ the group of units of R where R is completely primary finite ring. Upon consideration of s, t, λ to be the number of elements in the generating sets for U, V, W respectively where U, V, W are R_0-modules, Chikunji [8]

determined the general structure of $1+W$ of the unit groups of $R = R_0 \oplus U \oplus V \oplus W$ and the structure of $U(R)$ of R when $s = 3, t = 1, \lambda \geq 1$ and char $R = p$. Furthermore, Owino, [29, 30] generalized the solutions of the cases when $s = 2, t = 1, t = s(s+1)/2$ for a fixed s and $p \leq charR \leq p^3$ and when $s = 2, t = 2, charR = p$ to the case when the annihilator $ann(J) = J^2 + W$ so that $\lambda \geq 1$. Indeed both [8] and [31] have a point of shift from the works of Corbas, Koh, Wilson, Janusz and many other scholars who never studied unit groups of completely primary finite rings in particular but just mentioned them while studying associative and general finite rings. However, they have restricted the classes of rings under consideration. As such is the case, the characterization of the groups of units of the ring R has not been exhausted.

A more general study on the unit groups done by Owino , et al [32] characterized the units of Commutative completely primary finite rings of Characteristic p^k for a prime p and a positive integer k. This paper has very important properties of such unit groups with regards to their structures upto $k = 3$ and to some extent, the Jacobson radical of the rings constructed in the paper coincide with the ideals considered in this thesis especially for a generalized case when $k \geq 3$. Kainrath[25] has studied the quotients formed by unit groups of a semilocal ring R. He set two subrings R_1, R_2 of R such that $R_1 \subset R_2$ is an extension of rings such that R_1 is noetherian and semilocal and R_2 is a finitely generated R_1-module. The study established the properties of the quotients of R_1 and R_2 and their units. This study is limited to semilocal rings and therefore does not give an exact picture on the structures of local rings and their units.

Owino, et al [33] have characterized the quotient groups of subgroups of the unit groups of a class of completely primary finite rings. They adopted the same constructions used in [32] and varied the invariants throughout before giving the general structures of the unit groups and consequently the quotients of the subgroups in question. The procedure used in [33] is more of a routine check based on the same procedures used by Ongati and Owino in [28] where they determined the structures of the quotient groups $1 + J^i/1 + J^{i+1}$ for every characteristic of R such that $1 \leq i \leq k-1$. From the results in [33], these quotient groups are not exhaustive

since they restricted their findings to subgroups of the unit groups characterized.

Its apparent that so much has been done on unit groups of certain classes of completely primary finite rings for instance some of the results recently obtained by researchers include the following;

Theorem 10. *(See, [7]). The unit group $U(R)$ of a commutative completely primary finite ring R with maximal ideal $J(R)$ such that $J(R)^3 = (0)$ and $J(R)^2 \neq (0)$; 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 charR=p,then

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

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

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

and if $p = 2$ then,

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

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

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

and

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

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

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

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

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

for Char $R = p$,

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

for Char. $R = p^2$ and,

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

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

Theorem 11. *(See, [29]) The unit group $U(R)$ of the commutative completely primary finite ring R of characteristic p^k with maximal ideal $J(R)$ such that $J(R)^{k+1} = (0)$ and $J(R)^k \neq (0)$, with the invariants p, k, r and h where $p \in J(R)$, is a direct product of cyclic groups as follows:*

(i) If $h \geq 1$, $r \geq 1$ and Char $R = p$, then

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

.

(ii) If $h \geq 1$,$r \geq 1$ and Char $R = p^2$,then

$$U(R) = \mathbb{Z}_{p^r-1} \times \mathbb{Z}_p^r \times (\mathbb{Z}_{p^2}^r)^h$$

.

(iii) If $h \geq 1$,$r \geq 1$ and Char $R = p^k; k \geq 3$,then

$$U(R) = \begin{cases} \mathbb{Z}_{2^r-1} \times \mathbb{Z}_2 \times \mathbb{Z}_{2^{k-2}} \times \mathbb{Z}_{2^{k-2}}^{r-1} \times (\mathbb{Z}_{2^k}^r)^h, & \text{if } p = 2; \\ \mathbb{Z}_{p^r-1} \times \mathbb{Z}_{p^{k-1}}^r \times (\mathbb{Z}_{p^k}^r)^h, & \text{if } p \text{ is odd.} \end{cases}$$

Proof. Follows from the proofs of propositions 3,4 and 5 of [29] □

Theorem 12. *(See, [32]) The unit group $U(R)$ of the commutative completely primary finite ring of characteristic p^k with maximal ideal $J(R)$ such that $(J(R))^2 = (0)$ when $n = 1, 2$;*

$(J(R))^k = (0)$,$(J(R))^{k-1} \neq (0)$, *when* $k \geq 3$ *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*

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

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

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

.

(iii) If Char $R = p^k, k \geq 3$*, then*

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

but little has been done on the determination and characterization of unit groups of localized finite rings. In this study we have determined the generators of the unit groups of total quotient rings of characteristic p^k. A characterization of the unit groups has also been achieved.

2.5 Preliminary results

Proposition 8 ([11])**.** *Let* R *be a local ring with* $J(R)$ *a nil ideal and* $\mathcal{P}$ *the prime sub-ring of* R*, then*

(i) *If* $charR = 0$*, then* $\mathcal{P} \cong \mathbb{Q}$.

(ii) *If* $charR = p^n$*, then* $\mathcal{P} \cong \mathbb{Z}_{p^n}$.

Proof. Let $\mathcal{P} = \{(n+1)(m+1)^{-1} : n, m \in \mathbb{Z}, (m+1)^{-1} \text{ exists in } R \ \}$.

(i) $CharR = 0$. Then $CharR/J(R) = 0$. For $m \in \mathbb{Z}$,$m \neq 0$, $m+1 \in \mathcal{P}$, $m+1 \notin J(R)$, gives $(m+1)^{-1}$ exists. Also $\mathbb{Z}+1 = \{n+1 : n \in \mathbb{Z}\} \cong \mathbb{Z}$. So $\mathcal{P} = \{(n+1)(m+1)^{-1} : n, m \in \mathbb{Z}$ with $m \neq 0\} \cong \mathbb{Q}$.

(ii) $CharR = p^n$. Then $\mathbb{Z} + 1 = \{m + 1 : m \in \mathbb{Z}\} \cong \mathbb{Z}_{p^n}$. Here $m + 1$ has an inverse in R if and only if $gcd(m, p^n) = 1$; that is $gcd(m, p) = 1$. But any $m + (p^n) \in \mathbb{Z}_{p^n}$ has an inverse in $\mathbb{Z}_{p^n}$, whenever $gcd(m, p) = 1$. So

$$\mathcal{P} = \{m + 1 : m \in \mathbb{Z}\} \cong \mathbb{Z}_{p^n}.$$

□

Proposition 9 ([11])**.** *Let R be a local ring with $J(R)$ a nil ideal and $\mathcal{P}$ the prime sub-ring of R. Then $\mathcal{P} + J(R)/J(R)$ is the prime subfield of $R/J(R)$.*

Proof. Case 1: $charR = 0$. Then $\mathcal{P} \cong \mathbb{Q}$, $\mathcal{P} \cap J(R) = 0$. So $\mathcal{P} \cong \mathcal{P}/\mathcal{P} \cap J(R) \cong \mathcal{P} + J(R)/J(R)$ and hence $\mathcal{P} + J(R)/J(R) \cong \mathbb{Q}$. Thus $\mathcal{P} + J(R)/J(R)$ is the prime subfield of $R/J(R)$.
Case 2: $charR = p^n$. Then $\mathcal{P} \cong \mathbb{Z}_{p^n}$, $J(\mathcal{P}) = p\mathcal{P} = \mathcal{P} \cap J(R)$. So

$$\mathbb{Z}/p\mathbb{Z} \cong \mathcal{P}/p\mathcal{P} \cong \mathcal{P} + J(R)/J(R).$$

□

The following results due to Raghavendran [35] shall be useful in the sequel;

Lemma 1 ([35])**.** *Let R be a completely primary finite ring with maximal ideal $J(R)$, then*

(i) $|R| = p^{kr}$ where p is a prime integer , k, r are positive integers

(ii) $J(R)$ is the Jacobson radical.

(iii) $(J(R))^m = (0)$, where $m \leq k$ and the residue field $R/J(R)$ is a finite field $GF(p^r)$ for some prime integer p and positive integer r

(iv) Char $R = p^n$ where n is a positive integer such that $1 \leq n \leq k$

Theorem 13. *Let R be a completely primary finite ring and let $J(R)$ be its unique maximal ideal then, $J(R)^n = (0)$, $|R| = p^{nr}$ and $|J(R)| = p^{(n-1)r}$ for some prime integer p and positive integers n, r.*

Proof. (See, [8]). Let $x \in J(R)$. Since R is finite, $x^i = x^j$ for $i < j$. Hence, $x^i(x^{j-i} - 1) = 0$ and $x^{j-i} - 1$ is invertible since $x^{j-i} - 1$ is not contained in $J(R)$. Hence $x^i = 0$; ie $J(R)$ is a nil ideal. But again, finiteness of R implies that $J(R)$ is nilpotent, say $J(R)^n = (0)$ for some positive integer n. On the other hand, we can consider $J(R)^i/J(R)^{i+1}$ as a vector space over R/J with respect to

$$(r + J(R))(x + J^{i+1}) = rx + J^{i+1}$$

Therefore $|J(R)^i/J(R)^{i+1}| = p^{c_i r}$ for some positive integer c_i

Taking into account that $J^n = (0)$, we have

$$|R| = |R/J(R)| \cdot |J(R)/J(R)^2| \cdot \cdots |J(R)^{h-2}/J(R)^{h-1}| = p^{nr}$$

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

Notice that since $c_i \geq 1$, we have $h \leq n$. But $R/J(R) \cong GF(p^r)$ and hence , $|J(R)| = |R|/|\mathbb{F}_{p^r}| = p^{nr}/p^r = p^{r(n-1)}$ □

The above stated theorems show the characterization of the unit groups of certain classes of completely primary finite rings . In the next chapter, we shall focus on the construction of the total quotient ring of a completely primary finite ring R of characteristic p^k; $k = 1, 2, 3, \ldots, n$. and finally in chapter five we shall determine the structure of their unit groups.

CHAPTER THREE

LOCALIZATION OF COMPLETELY PRIMARY RINGS OF CHARACTERISTIC p^k

3.1 Introduction

The construction of completely primary finite rings of characteristic p^k has been done in [32].

3.2 Localization of the Completely Primary Finite Ring

The following results are useful in our construction

Definition 3.2.1. *Two elements (a, b) and (c, d) in $S^{-1}R$ are equivalent denoted by $(a, b) \equiv (c, d)$ if and only if $ad = bc$.*

Proposition 10. *The relation $\equiv$ on $S^{-1}R$ as described in the above definition is an equivalence relation.*

Proof. (i) Reflexive: $(a, b) \equiv (a, b)$ since $ab = ba$, for multiplication in R is commutative.

(ii) Symmetric: If $(a, b) \equiv (c, d)$, then $ad = bc$.

Since multiplication in R is commutative (see [32]) we deduce that $cb = da$ and consequently $(c, d) \equiv (a, b)$.

(iii) Transitive: If $(a, b) \equiv (c, d)$ and $(c, d) \equiv (e, f)$, then $ad = bc$ and $cf = de$.

Using these relations and the fact that multiplication in R is commutative, we have: $afd = fad = fbc = bcf = bde = bed$. Now $d \neq 0$, and R is completely primary, cancellation is valid.

Hence from $afd = bed$ we obtain $af = be$, so that $(a, b) \equiv (e, f)$.

□

Now, the $\equiv$ gives a partition of $S^{-1}R$ into equivalence classes.

Definition 3.2.2. *Let* $[(a,b)]$ *be the equivalence class of* (a,b) *in* $S^{-1}R$ *under the relation* $\equiv$*.Define* R_S *to be the set of all equivalence classes* $[(a,b)]$ *for* $(a,b) \in S^{-1}R$*.* R_S *is called the localization of* R *at* S*.*

Let $S^{-1}R = \{\left[\frac{r}{s}\right] | r \in R, s \in S\}$ and define addition and multiplication on $S^{-1}R$ by

$$\left[\frac{a}{s}\right] + \left[\frac{b}{t}\right] = \left[\frac{at+bs}{st}\right] \qquad 1$$

$$\left[\frac{a}{s}\right]\left[\frac{b}{t}\right] = \left[\frac{ab}{st}\right] \qquad 2$$

We check that addition and multiplication are well defined:
Suppose $\left[\frac{a}{s}\right] = \left[\frac{a'}{s'}\right]$ and $\left[\frac{b}{t}\right] = \left[\frac{b'}{t'}\right]$ then $\left[\frac{a}{s}\right] + \left[\frac{b}{t}\right] = \left[\frac{a'}{s'}\right] + \left[\frac{b'}{t'}\right]$ which is equivalent to showing that

$$\left[\frac{at+bs}{st}\right] = \left[\frac{a't'+b's'}{s't'}\right] \text{ or } (at+bs)(s't') = (a't'+b's')(st) \qquad 3$$

Beginning with $\left[\frac{a}{s}\right] = \left[\frac{a'}{s'}\right]$ and $\left[\frac{b}{t}\right] = \left[\frac{b'}{t'}\right]$. This implies that

$$as' = a's \qquad 4$$

$$bt' = b't \qquad 5$$

We multiply both equations and get

$$(as')(tt') = (a's)(tt') \qquad 6$$

$$(bt')(ss') = (b't)(ss') \qquad 5$$

We now add both equations and get

$$(as')(tt') + (bt')(ss') = (a's)(tt') + (b't)(ss')$$

We rearrange terms on the right side and the left side of the equation and get:

$$(at)(s't') + (bs)(s't') = (st)(a't') + (st)(s'b')$$

We pull out common terms on each side and get

$$(at + bs)(s't') = (a't' + b's')(st)$$

This is equivalent to equation 3 which we wanted to show it is true.

Now we check that multiplication is well defined:

Suppose $\left[\frac{a}{s}\right] = \left[\frac{a'}{s'}\right]$ and $\left[\frac{b}{t}\right] = \left[\frac{b'}{t'}\right]$

Then for some $u, v \in S, (as' - a's)u = 0$ and $(bt' - b't)v = 0$

We want to show that

$$\left[\frac{ab}{st}\right] = \left[\frac{a'b'}{s't'}\right]$$

We have

$$[(ab)(s't') - (a'b')(st)]\, uv = (ab)(s't')(uv) - (a'b')(st)(uv) - (a's)(bt')(uv) + (a's)(bt')(uv)$$

$$= (as' - a's)u(bt'v) + (bt' - b't)v(a'su) = 0 + 0 = 0$$

Thus

$$\left[\frac{ab}{st}\right] = \left[\frac{a'b'}{s't'}\right]$$

which verifies that multiplication is well defined.

We now construct a total quotient ring R_S from the completely primary finite ring R. Every element $[\frac{r}{s}] \in R_S$ where $r = r' + \sum_{i=1}^{h} \lambda_i u_i$ and $s = \alpha + pr' + \sum_{i=1}^{h} \lambda_i u_i$ where $\lambda_i \in \mathbb{F}_p, pr' + \sum_{i=1}^{h} \lambda_i u_i \in J(R)$ and $\alpha \in S$.

Proposition 11. *Let the addition in equation 1 be defined on R_S. Then, the multiplication given by* (2) *turns R_S into a finite local ring with identity.*

Proof. We start by showing that the abelian group R_S is closed under addition. Let

$$\left[\frac{r' + \sum_{i=1}^{h} \lambda_i u_i}{\alpha + pr' + \sum_{i=1}^{h} \lambda_i u_i}\right], \left[\frac{s' + \sum_{i=1}^{h} \tau_i u_i}{\alpha + ps' + \sum_{i=1}^{h} \tau_i u_i}\right] \in R_S$$

for each $1 \leq i \leq h$, by the addition we have

$$\left[\frac{r' + \sum_{i=1}^{h} \lambda_i u_i}{\alpha + pr' + \sum_{i=1}^{h} \lambda_i u_i}\right] + \left[\frac{s' + \sum_{i=1}^{h} \tau_i u_i}{\alpha + ps' + \sum_{i=1}^{h} \tau_i u_i}\right]$$

$$= \left[\frac{(r^{'} + \sum_{i=1}^{h} \lambda_i u_i)(\alpha + ps^{'} + \sum_{i=1}^{h} \tau_i u_i) + (s^{'} + \sum_{i=1}^{h} \tau_i u_i)(\alpha + pr^{'} + \sum_{i=1}^{h} \lambda_i u_i)}{(\alpha + pr^{'} + ps^{'} + p^2 r^{'} s^{'} + \sum_{i=1}^{h} \{(r' + pR')\tau_i + \lambda_i (s' + pR')^{\alpha_i}\} u_i)} \right],$$

Since $\alpha^2 = \alpha \in S$.

but

$$(r^{'} + \sum_{i=1}^{h} \lambda_i u_i)(\alpha + ps^{'} + \sum_{i=1}^{h} \tau_i u_i) + (s^{'} + \sum_{i=1}^{h} \tau_i u_i)(\alpha + pr^{'} + \sum_{i=1}^{h} \lambda_i u_i) \in R$$

and

$$(\alpha + pr^{'} + ps^{'} + p^2 r^{'} s^{'} + \sum_{i=1}^{h} \{(r' + pR')\tau_i + \lambda_i (s' + pR')^{\alpha_i}\} u_i) \in S$$

.

Thus

$$\left[\frac{(r^{'} + \sum_{i=1}^{h} \lambda_i u_i)(\alpha + ps^{'} + \sum_{i=1}^{h} \tau_i u_i) + (s^{'} + \sum_{i=1}^{h} \tau_i u_i)(\alpha + pr^{'} + \sum_{i=1}^{h} \lambda_i u_i)}{(\alpha + pr^{'} + ps^{'} + p^2 r^{'} s^{'} + \sum_{i=1}^{h} \{(r' + pR')\tau_i + \lambda_i (s' + pR')^{\alpha_i}\} u_i)} \right] \in R_S.$$

We now show that commutativity holds in R_S, by our multiplication we have

$$\left[\frac{r^{'} + \sum_{i=1}^{h} \lambda_i u_i}{\alpha + pr^{'} + \sum_{i=1}^{h} \lambda_i u_i} \right] \cdot \left[\frac{s^{'} + \sum_{i=1}^{h} \tau_i u_i}{\alpha + ps^{'} + \sum_{i=1}^{h} \tau_i u_i} \right]$$

$$= \left[\frac{(r^{'} + \sum_{i=1}^{h} \lambda_i u_i)(s^{'} + \sum_{i=1}^{h} \tau_i u_i)}{(\alpha + pr^{'} + \sum_{i=1}^{h} \lambda_i u_i)(\alpha + ps^{'} + \sum_{i=1}^{h} \tau_i u_i)} \right]$$

$$= \left[\frac{r^{'} s^{'} + \sum_{i=1}^{h} \{(r' + pR')\tau_i + \lambda_i (s' + pR')^{\alpha_i}\} u_i}{\alpha + p(r^{'} + s^{'} + pr^{'} s^{'}) + \sum_{i=1}^{h} \{(r' + pR')\tau_i + \lambda_i (s' + pR')^{\alpha_i}\} u_i} \right]$$

Since $\alpha^2 = \alpha \in S$

but R is commutative thus

$$\left[\frac{s^{'} r' + \sum_{i=1}^{h} \{(s' + pR')\lambda_i + \tau_i (r' + pR')^{\alpha_i}\} u_i}{\alpha + p(s^{'} + r^{'} + ps^{'} r^{'}) + \sum_{i=1}^{h} \{(s' + pR')\lambda_i + \tau_i (r' + pR')^{\alpha_i}\} u_i} \right]$$

$$= \left[\frac{s^{'} + \sum_{i=1}^{h} \lambda_i u_i}{\alpha + ps^{'} + \sum_{i=1}^{h} \tau_i u_i} \right] \cdot \left[\frac{r^{'} + \sum_{i=1}^{h} \lambda_i u_i}{\alpha + pr^{'} + \sum_{i=1}^{h} \tau_i u_i} \right]$$

which establishes commutativity.

Next we show that given multiplication turns R_S into a commutative ring with identity $\frac{(1,0,\ldots,0)}{(1,0,\ldots,0)}$.

Let

$$\left[\frac{r^{'}+\sum_{i=1}^{h}\lambda_i u_i}{\alpha+pr^{'}+\sum_{i=1}^{h}\lambda_i u_i}\right]$$

be an element of R_S then there exists

$$\left[\frac{s^{'}+\sum_{i=1}^{h}\tau_i u_i}{\alpha+ps^{'}+\sum_{i=1}^{h}\tau_i u_i}\right]\in R_S$$

such that

$$\left(\left[\frac{r^{'}+\sum_{i=1}^{h}\lambda_i u_i}{\alpha+pr^{'}+\sum_{i=1}^{h}\lambda_i u_i}\right]\right)\cdot\left(\left[\frac{s^{'}+\sum_{i=1}^{h}\tau_i u_i}{\alpha+ps^{'}+\sum_{i=1}^{h}\tau_i u_i}\right]\right)=\left[\frac{r^{'}+\sum_{i=1}^{h}\lambda_i u_i}{\alpha+pr^{'}+\sum_{i=1}^{h}\lambda_i u_i}\right].$$

Now if

$$\left(\left[\frac{r^{'}+\sum_{i=1}^{h}\lambda_i u_i}{\alpha+pr^{'}+\sum_{i=1}^{h}\lambda_i u_i}\right]\right)\cdot\left(\left[\frac{s^{'}+\sum_{i=1}^{h}\tau_i u_i}{\alpha+ps^{'}+\sum_{i=1}^{h}\tau_i u_i}\right]\right)=\left[\frac{r^{'}+\sum_{i=1}^{h}\lambda_i u_i}{\alpha+pr^{'}+\sum_{i=1}^{h}\lambda_i u_i}\right]$$

then

$$\left[\frac{s^{'}r^{\prime}+\sum_{i=1}^{h}\{(s^{\prime}+pR^{\prime})\lambda_i+\tau_i(r^{\prime}+pR^{\prime})^{\alpha_i}\}u_i)}{\alpha+p(s^{'}+r^{'}+ps^{'}r^{'})+\sum_{i=1}^{h}\{(s^{\prime}+pR^{\prime})\lambda_i+\tau_i(r^{\prime}+pR^{\prime})^{\alpha_i}\}u_i}\right]=\left[\frac{r^{'}+\sum_{i=1}^{h}\lambda_i u_i}{\alpha+pr^{'}+\sum_{i=1}^{h}\lambda_i u_i}\right].$$

So

$$r^{\prime}s^{\prime}=r^{\prime}\implies s^{\prime}=\frac{r^{\prime}}{r^{\prime}}=1$$

and

$$\alpha+p(s^{'}+r^{'}+ps^{'}r^{'})=\alpha+pr^{\prime}\implies\alpha+ps^{\prime}=1.$$

On the other hand,

$$\sum_{i=1}^{h}\{(s^{\prime}+pR^{\prime})\lambda_i+\tau_i(r^{\prime}+pR^{\prime})^{\alpha_i}\}u_i=\sum_{i=1}^{h}\lambda_i u_i$$

Which implies that

$$[1-(s'+pR')]\lambda_i+\tau_i(r'+pR')^{\alpha_i}=0$$

for each $i=1,\ldots,h$

Thus

$$\left[\frac{s^{'}+\sum_{i=1}^{h}\tau_i u_i}{\alpha+ps^{'}+\sum_{i=1}^{h}\tau_i u_i}\right]=\left[\frac{(1,0,\ldots,0)}{(1,0,\ldots,0)}\right].$$

In a similar manner we can show that,

$$\left[\frac{s^{'}+\sum_{i=1}^{h}\tau_i u_i}{\alpha+ps^{'}+\sum_{i=1}^{h}\tau_i u_i}\right]\cdot\left[\frac{r^{'}+\sum_{i=1}^{h}\lambda_i u_i}{\alpha+pr^{'}+\sum_{i=1}^{h}\lambda_i u_i}\right]=\left[\frac{s^{'}+\sum_{i=1}^{h}\tau_i u_i}{\alpha+ps^{'}+\sum_{i=1}^{h}\tau_i u_i}\right],$$

then

$$\left[\frac{r^{'}+\sum_{i=1}^{h}\lambda_i u_i}{\alpha+pr^{'}+\sum_{i=1}^{h}\lambda_i u_i}\right]=\left[\frac{(1,0,\ldots,0)}{(1,0,\ldots,0)}\right]$$

the identity element of R_S.

We now show that the given multiplication is associative.

Suppose that

$$\left[\frac{r^{'}+\sum_{i=1}^{h}\lambda_i u_i}{\alpha+pr^{'}+\sum_{i=1}^{h}\lambda_i u_i}\right],\left[\frac{s^{'}+\sum_{i=1}^{h}\tau_i u_i}{\alpha+ps^{'}+\sum_{i=1}^{h}\tau_i u_i}\right],\left[\frac{t^{'}+\sum_{i=1}^{h}\upsilon_i u_i}{\alpha+pt^{'}+\sum_{i=1}^{h}\upsilon_i u_i}\right]\in R_S,$$

then

$$\left[\frac{r^{'}+\sum_{i=1}^{h}\lambda_i u_i}{\alpha+pr^{'}+\sum_{i=1}^{h}\lambda_i u_i}\right]\cdot\left(\left[\frac{s^{'}+\sum_{i=1}^{h}\tau_i u_i}{\alpha+ps^{'}+\sum_{i=1}^{h}\tau_i u_i}\right]\cdot\left[\frac{t^{'}+\sum_{i=1}^{h}\upsilon_i u_i}{\alpha+pt^{'}+\sum_{i=1}^{h}\upsilon_i u_i}\right]\right)$$

$$=\left[\frac{r^{'}+\sum_{i=1}^{h}\lambda_i u_i}{\alpha+pr^{'}+\sum_{i=1}^{h}\lambda_i u_i}\right]\cdot\left[\frac{s^{'}t'+\sum_{i=1}^{h}\{(s'+pR')\tau_i+\upsilon_i(r'+pR')^{\alpha_i}\}u_i}{\alpha+p(s^{'}+t^{'}+ps^{'}t')+\sum_{i=1}^{h}\{(s'+pR')\upsilon_i+\tau_i(t'+pR')^{\alpha_i}\}u_i}\right]$$

$$=\left[\frac{(r^{'}+\sum_{i=1}^{h}\lambda_i u_i)(s^{'}t'+\sum_{i=1}^{h}\{(s'+pR')\tau_i+\upsilon_i(t'+pR')^{\alpha_i)}\}u_i}{(\alpha+pr^{'}+\sum_{i=1}^{h}\lambda_i u_i)(\alpha+p(s^{'}+t^{'}+ps^{'}t')+\sum_{i=1}^{h}\{(s'+pR')\upsilon_i+\tau_i(t'+pR')^{\alpha_i}\}u_i)}\right].$$

Since $\alpha^2=\alpha\in S$

By the associativity of R, we have,

$$= \left[\frac{(r's' + \sum_{i=1}^{h}\{(r'+pR')\lambda_i + \tau_i(s'+pR')^{\alpha_i}\}u_i)(t' + \sum_{i=1}^{h}\upsilon_i u_i)}{(\alpha + p(r'+s'+pr's') + \sum_{i=1}^{h}\{(r'+pR')\tau_i + \lambda_i(s'+pR')^{\alpha_i}\}u_i)(\alpha + pt' + \sum_{i=1}^{h}\upsilon_i u_i)}\right]$$

$$= \left(\left[\frac{r' + \sum_{i=1}^{h}\lambda_i u_i}{\alpha + pr' + \sum_{i=1}^{h}\lambda_i u_i}\right] \cdot \left[\frac{s' + \sum_{i=1}^{h}\tau_i u_i}{\alpha + ps' + \sum_{i=1}^{h}\tau_i u_i}\right]\right) \cdot \left[\frac{t' + \sum_{i=1}^{h}\upsilon_i u_i}{\alpha + pt' + \sum_{i=1}^{h}\upsilon_i u_i}\right],$$

therefore the given multiplication is associative.

Lastly, consider

$$\left[\frac{r' + \sum_{i=1}^{h}\lambda_i u_i}{\alpha + pr' + \sum_{i=1}^{h}\lambda_i u_i}\right] \cdot \left(\left[\frac{s' + \sum_{i=1}^{h}\tau_i u_i}{\alpha + ps' + \sum_{i=1}^{h}\tau_i u_i}\right] + \left[\frac{t' + \sum_{i=1}^{h}\upsilon_i u_i}{\alpha + pt' + \sum_{i=1}^{h}\upsilon_i u_i}\right]\right) =$$

$$\left[\frac{r' + \sum_{i=1}^{h}\lambda_i u_i}{\alpha + pr' + \sum_{i=1}^{h}\lambda_i u_i}\right] \left(\left[\frac{(s' + \sum_{i=1}^{h}\tau_i u_i)(\alpha + pt' + \sum_{i=1}^{h}\upsilon_i u_i) + (t' + \sum_{i=1}^{h}\upsilon_i u_i)(\alpha + ps' + \sum_{i=1}^{h}\tau_i u_i)}{(\alpha + ps' + \sum_{i=1}^{h}\tau_i u_i)(\alpha + pt' + \sum_{i=1}^{h}\upsilon_i u_i)}\right]\right.$$

$$= \left[\frac{r' + \sum_{i=1}^{h}\lambda_i u_i \left((s' + \sum_{i=1}^{h}\tau_i u_i)(\alpha + pt' + \sum_{i=1}^{h}\upsilon_i u_i) + (t' + \sum_{i=1}^{h}\upsilon_i u_i)(\alpha + ps' + \sum_{i=1}^{h}\tau_i u_i)\right)}{(\alpha + pr' + \sum_{i=1}^{h}\lambda_i u_i)(\alpha + ps' + \sum_{i=1}^{h}\tau_i u_i)(\alpha + pt' + \sum_{i=1}^{h}\upsilon_i u_i)}\right]$$

$$= \left[\frac{r' + \sum_{i=1}^{h}\lambda_i u_i}{\alpha + pr' + \sum_{i=1}^{h}\lambda_i u_i}\right] \cdot \left[\frac{s' + \sum_{i=1}^{h}\tau_i u_i}{\alpha + ps' + \sum_{i=1}^{h}\tau_i u_i}\right] + \left[\frac{r' + \sum_{i=1}^{h}\lambda_i u_i}{\alpha + pr' + \sum_{i=1}^{h}\lambda_i u_i}\right] \cdot \left[\frac{t' + \sum_{i=1}^{h}\upsilon_i u_i}{\alpha + pt' + \sum_{i=1}^{h}\upsilon_i u_i}\right].$$

Similarly we can show that,

$$\left(\left[\frac{r' + \sum_{i=1}^{h}\lambda_i u_i}{\alpha + pr' + \sum_{i=1}^{h}\lambda_i u_i}\right] + \left[\frac{s' + \sum_{i=1}^{h}\tau_i u_i}{\alpha + ps' + \sum_{i=1}^{h}\tau_i u_i}\right]\right) \cdot \left[\frac{t' + \sum_{i=1}^{h}\upsilon_i u_i}{\alpha + pt' + \sum_{i=1}^{h}\upsilon_i u_i}\right]$$

$$= \left[\frac{r' + \sum_{i=1}^{h}\lambda_i u_i}{\alpha + pr' + \sum_{i=1}^{h}\lambda_i u_i}\right] \cdot \left[\frac{t' + \sum_{i=1}^{h}\upsilon_i u_i}{\alpha + pt' + \sum_{i=1}^{h}\upsilon_i u_i}\right] + \left[\frac{s' + \sum_{i=1}^{h}\tau_i u_i}{\alpha + ps' + \sum_{i=1}^{h}\tau_i u_i}\right] \cdot \left[\frac{t' + \sum_{i=1}^{h}\upsilon_i u_i}{\alpha + pt' + \sum_{i=1}^{h}\upsilon_i u_i}\right].$$

□

It remains for us to show that $S^{-1}R$ can be regarded as containing R. To do this, we show that there is an isomorphism f of R with a sub-domain of $S^{-1}R$.

Lemma 2. *The map $f : R \to S^{-1}R$ given by $f(x) = [(x, 1)]$ is an isomorphism of R with a sub-domain of $S^{-1}R$*

Proof. Consider $x, y \in R$. We have

$$f(x+y) = [(x+y,1)] = [(x,1)] + [(y,1)] = f(x) + f(y).$$

Furthermore

$$f(xy) = [(xy,1)] = [(x,1)][(y,1)] = f(x)f(y)$$

It remains for us to show only that f is one-to-one. If $f(x) = f(y)$ then,

$$[(x,1)] = [(y,1)].$$

Let $Kerf = \{x \in R | f(x) = \frac{0}{1}\}$ by definition of f. So f is $1-1$. □

For instance $R = \mathbb{Z}_4, J(R) = 2\mathbb{Z}_4, S = 1+J(R) = 1+2\mathbb{Z}_4$. So that $R_S = \left\{ \left[\frac{0}{1}\right], \left[\frac{1}{1}\right], \left[\frac{2}{1}\right], \left[\frac{3}{1}\right] \right\} \cong R$.

Proposition 12. *Any unital commutative finite ring R can be enlarged to the ring of quotients $S^{-1}R$ such that every element of $S^{-1}R$ can be expressed as a quotient of an element of R and S.*

Uniqueness:
$S^{-1}R$ could be regarded in some sense as a minimal ring containing R. Since every ring containing R must contain all elements $\left[\frac{r}{s}\right]$ for every $r \in R$ and $s \in S$.
The next proposition will show that every ring containing R contains a subring of quotients of R, and that any two localized rings at S of R are isomorphic.

Proposition 13. *Let R_S be a localized ring of R at S and let T be any ring containing R. Then there exists a map $\varphi : S^{-1}R \to T$ that gives an isomorphism of $S^{-1}R$ with a subring of T such that $\varphi(x) = x$ for $x \in R$.*

Proof. Let $[(r,s)] \in S^{-1}R$ we want to map $[(r,s)]$ onto $[(r',s')] \in T$. W e define $\psi : S^{-1}R \to T$ such that

$$\psi([(r,s)]) = [(r,s)] \text{ for } [(r,s)] \in S^{-1}R$$

Now every $x \in S^{-1}R$ is a quotient (r, s) of some two elements $r \in R$ and $s \in S$. Let us define ψ by $\psi(r, s) = (\psi(r), \psi(s))$. We first show that this map is well-defined. Since ψ is the identity on R, so our definition makes sense.

If $[(r, s)] = [(r', s')] \in S^{-1}R$, then $rs' = r's \in R$, so $\psi(rs') = \psi(r's)$. But since ψ is the identity on R,

$$\psi(rs') = \psi(r)\psi(s') \text{ and } \psi(r's) = \psi(r')\psi(s)$$

Thus $(\psi(r), \psi(s)) = (\psi(r'), \psi(s'))$ in T, so ψ is well-defined.

The equations

$$\psi(xy) = \psi(x)\psi(y) \text{ and } \psi(x + y) = \psi(x) + \psi(y)$$

follow from the definition of ψ on $S^{-1}R$ and from the fact that ψ is the identity on R.

If $\psi((r, s)) = \psi((r', s'))$ in $S^{-1}R$, we have $(\psi(r), \psi(s)) = (\psi(r'), \psi(s'))$ in T so $\psi(r)\psi(s') = \psi(s)\psi(r')$. Since ψ is the identity on R we deduce that $rs' = sr'$, so $(r, s) = (r', s')$ in R. Thus ψ is $1 - 1$. By definition, $\psi(r) = r$ for $r \in R$. □

Corollary 1. *Every field T containing a ring R contains a total quotient ring R_S*

Proof. In the proof of Proposition 12, every element of the subring $\psi(S^{-1}R)$ of T is a total quotient ring in T of elements of R and S. □

Corollary 2. *Any two localized rings of a commutative ring R are isomorphic.*

Proof. Suppose in Proposition 13 that T is a localized ring of R, so that every element x of T can be expressed in the form $(r, s) \in S^{-1}R$ for $r \in R$ and $s \in S$. Then T as a ring is thus isomorphic to $S^{-1}R$. □

3.3 Properties of the Total Quotient Ring

We now investigate some properties of R_S which are useful in the sequel.

Proposition 14. *(cf. [9]) Let R_S be a total quotient ring with identity $\left[\frac{1}{1}\right]$, then there is no distinction between left and right zero-divisors in R_S. Moreover every element of R_S is either a zero divisor or a unit.*

Corollary 3. *Let R_S be a localized ring with identity $\left[\frac{1}{1}\right]$, then every non-trivial ideal of R_S consists entirely of zero divisors.*

The following result demonstrates the importance of zero divisors in a finite ring:

Proposition 15. *(cf. [9]) Let R_S be a total quotient ring containing a finite number $n \geq 2$ of left zero divisors, then R_S is finite and $|R_S| \leq n^2$.*

We see also that if the set of all equivalence classes of $J(R_S)$ of its zero divisors form an additive group, in other words if R_S is completely primary and with the fact that $J(R_S)$ is a unique maximal ideal of R_S see [9] , then R_S is a *Local ring.*

Proposition 16. *(cf. [9]) Let R_S be the total quotient ring constructed in Section 3.2 and S be a multiplicative subset of R consisting of units, then R_S is a local ring with unique maximal ideal*

$$J(R_S) = \left\{ [(pr^{'} + \sum_{i=1}^{h} \lambda_i u_i, \alpha + pr^{'} + \sum_{i=1}^{h} \lambda_i u_i)] \mid r^{'} + \sum_{i=1}^{h} \lambda_i u_i \in R, \alpha + pr^{'} + \sum_{i=1}^{h} \lambda_i u_i \in S \right\}$$

Proof. (For this proof we shall denote the elements of R_S as $\left[\frac{r}{s}\right]$)
Now, $\left[\frac{r}{s}\right] \in R_S$ is a unit if and only if there exists $t \in R, u, v \in S$ such that

$$u(rt - sv) = 0$$

that is,

$$\left[\frac{rt}{sv}\right] = \left[\frac{1}{1}\right]$$

For some $x \in R$, if $x \notin S$, then it would be in $R - S$. So xy would be in $R - S$ which is a contradiction. Hence $x \in S$.
Thus every unit in R_S is of the form (x, y) with $x, y \in S$; Conversely it is trivial that every such element is a unit. Hence, the non units in R_S consist precisely elements of the form (r, s) where $r \in R - S$ and $s \in S$. From the argument we see that the $J(R_S)$ forms a unique maximal ideal and so R_S is a local ring. □

Corollary 4. *(cf. [9]) Let R_S be a localized ring and $J(R_S)$ its unique maximal ideal, then*

$$R_S/J(R_S) \cong GF(p^r)$$

for some prime p and positive integer r.

Proof. $R_S/J(R_S)$ is a finite division ring and hence $R_S/J(R_S) \cong GF(p^r)$. □

Proposition 17. *(cf. [9]) Let R_S be a total quotient ring of characteristic p^k and order p^{kr}, with unique maximal ideal $J(R_S)$ of index nilpotency i, then $1 \leq k \leq i \leq n$.*

Proof. We have only to prove that $k \leq i$. We know that $J(R_S) \neq 0$, So that $i \geq 2$. Since $p^k = 0$, it follows that $p \in J(R_S)$ and $i \geq k$. □

R_S has the following property:

Proposition 18. *(cf. [9]) Let R_S be a total quotient ring with maximal ideal $J(R_S)$, then R_S contains an element $\xi = [(r, s)]$ such that:*

i. $\xi + J(R_S)$ is a primitive element of $R_S/J(R_S)$

ii. ξ has a multiplicative order $p^r - 1$ and

iii. if $u, v \in K_S$ with $u - v \in J(R_S)$ then $v = u$ where $K_S =< \xi > \cup\{(0, 1)\}$.

Proposition 19. *(cf. [9]) Let R_S be a total quotient ring, then any subring $R'_{S'}$ of R_S is a local ring with maximal ideal $J(R'_{S'}) = J(R_S) \cap R'_{S'}$. Furthermore there are integers k' and r' such that $|R'_{S'}| = p^{k'r'}$, $|J(R'_{S'})| = p^{k'-1}r'$, where $r'|r$.*

Proof. We have $J(R_S) \cap R'_{S'}$ is the set of all zero divisors of R'_S and $J(R_S) \cap R'_{S'}$ is a subgroup of R_S^+ (by Proposition 13), hence $R'_{S'}$ is a local ring with maximal ideal $J(R_S) \cap R'_{S'}$. □

Proposition 20. *(cf. [9]) Let R_S be a total quotient ring, then any quotient of R_S by a two sided ideal and any homomorphic image of R_S is a local ring.*

Proof. Let $f : R_S \to R'_{S'}$ be a surjective ring homomorphism. Since $J(R_S)$ is the unique maximal ideal of $R_S, Kerf \subset J(R_S)$. Also, $\{[(a, b)] + Kerf \mid [(a, b)] \in J(R_S)\}$ is the set $R_S/Kerf$, and hence it is a subgroup of $(R_S/Kerf)^+$. So $R_S/Kerf$ is a local ring and hence $R'_{S'}$ is also local. □

Proposition 21. *(cf. [9]) Let R_S be a localized ring, then the set $K_S = R_S/J(R_S)$ forms a subfield of R_S if and only if char $R_S = p$.*

Proof. Since $K_S \subset R_S$ and addition is associative in R_S, it follows that K_S is a group under addition. We see that $\alpha + \beta = \beta + \alpha$ for all $\alpha, \beta \in K_S$. The distributive laws follows trivially since $K_S \subset R_S$. But the non zero elements of K_S form a multiplicative group, hence, K_S is a subfield of R_S.

Conversely, if K_S is a subfield of R_S, then the characteristic of K_S = characteristic of $R_S = p$, since the identity element in R_S is that in K_S. □

Proposition 22. *(cf. [9]) Let R_S be a localized ring of order p^{kr}, characteristic p^k and maximal ideal $J(R_S)$ such that $R_S/J(R_S) \cong GF(p^r)$. Let $R'_{S'} = \mathbb{Z}_{p^k}[\xi]$, then $R'_{S'}$ is a subring of R_S with $R'_{S'}/R_S \cap J(R_S) \cong R_S/J(R_S)$ and minimal with respect to $R'_{S'}/(R'_{S'} \cap J(R_S)) \cong R_S/J(R_S)$.*

Proof. Let $R'_{S'}$ be a commutative subring of R_S. by Proposition 19, $R'_{S'}$ is a local ring with maximal ideal $R'_{S'} \cap J(R_S)$ and residue order $p^{r'}$, where $r' \mid r$. But R'_S contains $< \xi >$, and its residue field therefore contains at least p^r elements. Hence, $R'_{S'}$ is a commutative local ring with residue field isomorphic to $R_S/J(R_S) \equiv GF(p^r)$.

Let T' be a subring of R_S minimal with respect to $T'/(T' \cap J(R_S)) \equiv R_S/J(R_S)$ and let $\psi : R_S \to R_S/J(R_S)$ be the canonical ring homomorphism. Since $T' \cap J(R_S)$ is the unique maximal ideal of T' the restriction of ψ to T' is surjective. Hence T' contains an element $< \xi' >$ of multiplicative order $p^r - 1$ and hence $\mathbb{Z}_{p^k}[\xi'] \subset T'$.

However, ψ has also a surjective restriction to $\mathbb{Z}_{p^k}[\xi']$ and so

$$\mathbb{Z}_{p^k}[\xi']/\mathbb{Z}_{p^k}[\xi'] \cap J(R_S) \equiv R_S/J(R_S).$$

But then, by the minimality of T', we have that $T' = \mathbb{Z}_{p^k}[\xi']$. By proposition 21, $< \xi >= [(a,b)] < \xi' > [(a,b)]^{-1}$ for some element $[(a,b)] \in U(R_S)$, and hence $\mathbb{Z}_{p^k}[\xi']$ is conjugate to $\mathbb{Z}_{p^k}[\xi]$. That R'_S is minimal with respect to $R'_{S'}/(R'_{S'} \cap J(R_S)) \equiv R_S/J(R_S)$ is essentially contained in the above argument. □

Lemma 3. *(cf. [9]) Let R_S be a localized ring, then the group of units $U(R_S)$ of R_S is $R_S - J(R_S)$.*

Proof. Follows from the fact that in a finite ring with identity $\left[\frac{1}{1}\right]$, an element is either a unit or a zero divisor. □

Proposition 23. *(cf. [9]) Let R_S be a localized ring and let $U(R_S)$ be its group of units, then $|U(R_S)| = (p^r - 1)p^{(k-1)r}$.*

Proof. Since $\mid R_S \mid = p^{kr}, \mid J(R_S) \mid = p^{(k-1)r}$ and $U(R_S) = R_S - J(R_S)$ (by Lemma 4 above), we see that

$$\mid U(R_S) \mid = \mid R_S - J(R_S) \mid = \mid R_S \mid - \mid J(R_S) \mid = p^{kr} - p^{(k-1)r} = p^{(k-1)r}(p^r - 1).$$

□

Proposition 24. *(cf. [9]) The group $U(R_S)$ contains a maximal subgroup of order $p^{(k-1)r}$ and a subgroup of order $p^r - 1$.*

Proof. Notice that $R_S/J(R_S) \cong GF(p^r)$. So $U(R_S)/\frac{1}{1} + J(R_S) \cong \mathbb{Z}_{p^r-1}$. Now, $\frac{1}{1} + J(R_S) \cong J(R_S)$, and $|J(R_S)| = \frac{p^{kr}}{p^r} = p^{(k-1)r}$. The result easily follows by Langrange's Theorem. □

Proposition 25. *(cf. [9]) The group $\frac{1}{1} + J(R_S)$ is a normal subgroup of $U(R_S)$.*

Proof. This subgroup $\frac{1}{1} + J(R_s)$ is normal in $U(R_S)$, $\left[\frac{r}{s}\right](\frac{1}{1} + J(R_S)) = (\frac{1}{1} + J(R_S))\left[\frac{r}{s}\right]$. Since $J(R_S)$ is the set of all the zero divisors in R_S. □

Proposition 26. *(cf. [9]) Let R_S be a localized ring, then if G is a subgroup $U(R_S)$ of order $p^r - 1$, then G is conjugate to $< \xi >$ in $U(R_S)$.*

Proof. This follows from $p-$solvable groups contained in the variation of Sylow's theorem, since the order of G is prime to it's index in $U(R_S)$. □

Proposition 27. *(cf. [9]) Let R_S be a total quotient ring. If $U(R_S)$ contains a normal subgroup of order $p^r - 1$, then the set K_S is contained in the center of R_S.*

Proof. By Proposition 28 above, $< \xi > \lhd U(R_S)$ and since $\left(\frac{1}{1} + J(R_S)\right) \lhd U(R_S)$ with $|< \xi > \cap \left(\frac{1}{1} + J(R_S)\right)| = \frac{1}{1}$ it follows that $< \xi >$ and $\left(\frac{1}{1} + J(R_S)\right)$ commute element-wise. Hence, by Corollary 4, ξ is in the center of R_S. □

Remark 2. *cf. [9] Let R_S be a localized ring, then the following conditions hold:*

(i) $U(R_S) = \left(\frac{1}{1} + J(R_S)\right) \ltimes < \xi >$ *a semi-direct product;*

(ii) $\left(\frac{1}{1} + J(R_S)^k\right) / \left(\frac{1}{1} + J(R_S)^{k+1}\right) \cong J(R_S)^k / J(R_S)^{k+1}$.

Lemma 4. *cf. [9] If R_S is commutative, then $\frac{1}{1} + J(R_S)$ is isomorphic to a direct product of cyclic p-groups.*

Proof. Follows from the fundamental theorem of finitely generated abelian groups. □

CHAPTER FOUR

UNIT GROUPS OF THE TOTAL QUOTIENT RING

4.1 Introduction

Let R_S be the total quotient ring obtained by the construction in Chapter 3. We recall that R_S is a ring of fractions consisting of equivalence classes of the form $[(r,s)] = [\frac{r}{s}]$, which we shall represent as $\left(\frac{r}{s}\right)$ or simply $s^{-1}r$ in the sequel, where $r = (r_0, r_1, \ldots, r_h \in R)$, $s = (s_0, s_1, \ldots, s_h)$. We see that R_S is a finite ring with identity $\left[\frac{(1,0,\ldots,0)}{(1,0,\ldots,0)}\right]$, which shall be denoted as $\left[\frac{1}{1}\right]$ and $J(R_S)$ its set of zero divisors. Clearly $(J(R_S))^{k-1} \neq \left[\frac{0}{1}\right]$. It is easy to see that $J(R_S)$ together with the usual fraction addition forms an additive group. As an immediate consequence we have the result that R_S will, then, be a local ring with $J(R_S)$ as its radical. For, as R_S does not contain one-sided zero divisors, we see that $J(R_S)$ will be the unique maximal ideal in R_S; so that $J(R_S)$ will be the Jacobson radical of the ring. As every element of $U(R_S) = R_S - J(R_S)$ is an invertible element, and that the quotient ring $R_S/J(R_S)$ is a division ring. In fact we have the following result

Proposition 28. *If R is local, then R_S is also local.*

Proof. The proof follows from the above discussion. □

And thus the following property:

Theorem 14. *([11]) The only prime ideals of $S^{-1}R$ are $S^{-1}P$ where P is a prime ideal of R such that $P \cap S = \phi$. That is there exists a one-to-one and onto function say, $h : S^{-1}P \to P$ with P a prime ideal of R and $P \cap S = \phi$.*

As a consequence we have the following corollary

Corollary 5. *The only maximal ideals of $S^{-1}R$ are $S^{-1}J(R)$ where $J(R)$ is a maximal ideal of R such that $J(R) \cap S = \phi$*

We now proceed to obtain some properties of R_S in the following proposition which is essential for the object of this thesis.

Proposition 29. *cf. [35] Let R_S be a localized ring with multiplicative identity $\left[\frac{1}{1}\right]$, whose zero-divisors form an additive group $J(R_S)$. Then*

(i) *$J(R_S)$ is the Jacobson radical of R_S.*

(ii) *$|R_S| = p^k$, and $|J(R_S)| = p^{k-1}$ for some prime p and some positive integer k.*

(iii) *$(J(R_S))^k = [(0,1)]$*

(iv) *the characteristic of the ring R_S is p^k for some positive integer k with $1 \leq k \leq n$and*

(v) *If the characteristic is p^k with $k = n$, then R_S is commutative.*

The following propositions describe the structure of the group of units $U(R_S)$ for the local ring R_S

Proposition 30. *Let R_S be a total quotient ring. Then the group of units $U(R_S)$ contains a cyclic subgroup ξ of order $p-1$ and $U(R_S)$ is a semi direct product of $\frac{1}{1} + J(R_S)$ by $< \xi >$.*

Proof. The cardinality of $U(R_S) = R_S - J(R_S)$ is $|U(R_S)| = p^{k-1}(p-1)$, and so $\phi : R_S \to R_S/J(R_S)$ induces an onto multiplicative group homomorphism $\varphi : U(R_S) \to U(R_S/J(R_S))$. Since the kernel of ϕ is $J(R_S)$, we have kernel of φ is $\frac{1}{1} + J(R_S)$. In particular, $\frac{1}{1} + J(R_S)$ is a normal subgroup of $U(R_S)$. Let $\langle\beta\rangle = (R_S/J(R_S))$ and let $\xi \in \varphi^{-1}(\beta)$. Then the multiplicative order of β_0 is a multiple of $p-1$ and a divisor of $\mid R_S \mid - \mid J(R_S \mid = p^k - p^{k-1} = p^{k-1}(p-1)$; hence of the form $p^k(p-1)$. But $\xi = (\beta_0)^{p^k}$ has a multiplicative order $p-1$ and $\varphi(\xi)^{p^k} = \beta p^k$, which is still a generator of $U(R_S/J(R_S))$, since $(p^k, p-1) = 1$. Finally since $|U(R_S)| = |\frac{1}{1} + J(R_S)|.| < \xi > |$, and $\frac{1}{1} + J(R_S) \cap < \xi >= \left[\frac{1}{1}\right]$, we have $U(R_S) = (\frac{1}{1} + J(R_S)) \times \langle\xi\rangle$ hence $U(R_S) = \frac{1}{1} + J(R_S) \ltimes \langle\xi\rangle$, a semi direct product. □

For complete classification of $U(R_S)$, we need to determine the generators of $\frac{1}{1} + J(R_S)$. Since $U(R_S)$ is abelian, $\frac{1}{1} + J(R_S)$ is a normal subgroup of $U(R_S)$. If R_S is a ring with the property in Proposition 37, then $\frac{1}{1} + J(R_S)$ is an abelian $p-$ subgroup of the unit group $U(R_S)$. The group has the filtration

$$\tfrac{1}{1} + J(R_S) \supset \tfrac{1}{1} + (J(R_S))^2 \supset \tfrac{1}{1} + (J(R_S))^3 \supset ... \supset \tfrac{1}{1} + (J(R_S))^k = \left\{ \left[\tfrac{1}{1}\right] \right\}$$

with filtration quotients

$$\tfrac{1}{1} + J(R_S)/\tfrac{1}{1} + (J(R_S))^2, \tfrac{1}{1} + (J(R_S))^2/\tfrac{1}{1} + (J(R_S))^3, ..., \tfrac{1}{1} + (J(R_S))^k/\tfrac{1}{1} = \tfrac{1}{1} + (J(R_S))^k$$

Isomorphic to the additive groups

$$J(R_S)/(J(R_S))^2, (J(R_S))^2/(J(R_S))^3, ..., (J(R_S))^k$$

respectively cf. [32].

We now state proposition used in the determination of the structure of $\frac{1}{1} + J(R_S)$:

Proposition 31. *Let $annJ(R_S)$ be the two sided annihilator of $J(R_S)$. Then $\frac{1}{1} + ann(J(R_S))$ is a subgroup of $\frac{1}{1} + J(R_S)$.*

Proof. Clearly, $\frac{1}{1} + ann(J(R_S)) = \left[\frac{1}{1}\right]$ when char $R_S = p$, which follows from the above proposition. When characteristic p^k for $k \geq 2$, $\frac{1}{1} + ann(J(R_S)) = \frac{1}{1} + p^{k-1}J(R_S)$, Now let $\frac{1}{1} + p^{k-1}(\left[\frac{r}{s}\right]) \in \frac{1}{1} + ann(J(R_S))$. Then $\frac{1}{1} + p^{k-1}(\left[\frac{r}{s}\right])$ is an element of $\frac{1}{1} + ann(J(R_S))$. □

In the sequel, $R' = GR(p^{kr}, p^k) = \mathbb{Z}_{p^k}[x]/ < f >$ where $f \in \mathbb{Z}_{p^k}[x]$ is a monic polynomial of degree r whose image in $\mathbb{Z}_p[x]$ is irreducible discussed in Section 3.4.1. Moreover, R' is considered to be a Galois subring of R which is maximal.

4.2 Total quotient rings of characteristic p^k

4.2.1 The construction of the ring

Let R_S be the ring constructed in Section 3.2 and $S = U(R)$ be its multiplicative subset. Then $R_S = \{[(r, s)] \mid r \in R, s \in S\}$ an additive abelian group with the neutral element $\left[\frac{(0,0,...,0)}{(1,0,...,0)}\right]$ which shall denoted as $\left[\frac{0}{1}\right]$.

4.2.2 Zero Divisors when the characteristic of R_S is p^k with $k = 1, 2, 3, \ldots, n$

The construction yields a total quotient ring in which $(J(R_S))^{k-1} \neq [(0, 1)]$ and $(J(R_S))^k = [(0, 1)]$.

Proposition 32. *(cf. [30]) Let R_S be the total quotient ring constructed above and $J(R_S)$ be its Jacobson radical, then*

(i) $J(R_S) = \left\{ \left[(pr^{'} + \sum_{i=1}^{h} \lambda_i u_i, \alpha + pr^{'} + \sum_{i=1}^{h} \lambda_i u_i) \right] \mid r^{'} \in R', \lambda_i \in \mathbb{Z}_p, u_i \in R, \alpha \in U(R) \right\}$

(ii) $(J(R_S))^{k-1} = \left\{ \left[(p^{k-1} r^{'}, \alpha + p^{k-1} r^{'}) \right] \mid r^{'} \in R', \alpha \in U(R) \right\}$ *and*

(iii) $(J(R_S))^{k} = [(0,1)]$

Proof. We claim that the elements not in $J(R_S)$ are invertible.

Let r_0 be non zero, for some

$$\left[\frac{(r_0, r_1, \ldots, r_h)}{(s_0, s_1, \ldots, s_h)} \right]$$

in R_S, we find that the inverse of

$$\left[\frac{(r_0, r_1, \ldots, r_h)}{(s_0, s_1, \ldots, s_h)} \right]$$

is say,

$$\left[\frac{(t_0, t_1, \ldots, t_h)}{(b_0, b_1, \ldots, b_h)} \right].$$

By multiplication (*), we require that

$$r_0 t_0 = 1, r_0 t_1 + r_1 t_0 = 0, \ldots, r_0 t_h + r_h t_0 = 0, s_0 b_0 = 1, s_0 b_1 + s_1 b_0 = 0$$

and

$$s_0 b_h + s_h b_0 = 0;$$

which implies that

$$r_0^{-1} = t_0, r_0 t_1 = -r_1 t_0 = -r_1 r_0^{-1} \Rightarrow t_1 = -r_1 r_0^{-2}, r_0 t_h = -r_h t_0 = -r_h r_0^{-1} \Rightarrow t_h = -r_h r_0^{-2};$$

$$s_0^{-1} = b_0, s_0 b_1 = -s_1 b_0 = -s_1 s_0^{-1} \Rightarrow b_1 = -s_1 s_0^{-2}, s_0 b_h = -s_h b_0 = -s_h s_0^{-1} \Rightarrow b_h = -s_h s_0^{-2}$$

Therefore

$$\left(\left[\frac{(r_0, r_1, \ldots, r_h)}{(s_0, s_1, \ldots, s_h)} \right] \right)^{-1} = \left[\frac{(r_0^{-1}, -r_1 r_0^{-2}, \ldots, -r_h r_0^{-2})}{(s_0^{-1}, -s_1 s_0^{-2}, \ldots, -s_h s_0^{-2})} \right].$$

We notice that there is no distinction between a right and a left zero divisor.

(ii) easily follows from (i).

To prove (iii), we have

$$J(R_S)\left[(pr^{'}+\sum_{i=1}^{h}\lambda_i u_i, \alpha+pr^{'}+\sum_{i=1}^{h}\lambda_i u_i)\right]=\left[(pr^{'}+\sum_{i=1}^{h}\lambda_i u_i, \alpha+pr^{'}+\sum_{i=1}^{h}\lambda_i u_i)\right]J(R_S)=[(0,1)]\,.$$

Hence $(J(R_S))^k=[(0,1)]\,.$ □

We begin with the case when $k=1$:

The construction in section 3.2 yields a total quotient ring in which $(J(R_S))^2=[(0,1)]$. These rings are completely primary and therefore we can employ well known procedures below to study their unit groups.

4.2.3 The Unit groups when the characteristic of R_S is p

Let R_S be the total quotient ring of the construction above with maximal ideal $J(R_S)$ such that $(J(R_S))^2=[(0,1)]$. Then R_S is of order p^{hr}. Since R_S is of the given order and $U(R_S)=R_S-J(R_S)$, then $|U(R_S)|=p^{hr}(p^r-1)$ and $|\frac{1}{1}+J(R_S)|=p^{hr}$. So $\frac{1}{1}+J(R_S)$ is an abelian p-group.

Proposition 33. *Let R_S be a local ring of characteristic p. Then the group of units $U(R_S)$ of R_S contains a cyclic subgroup $<\xi>$ of order p^r-1 and $U(R_S)$ is a semi direct product of $\frac{1}{1}+J(R_S)$ by $<\xi>$.*

Proof. See Proposition 30. □

We now determine the structure of $\frac{1}{1}+J(R_S)$ for this case since $U(R_S)\cong\mathbb{Z}_{p^r-1}\times\left(\frac{1}{1}+J(R_S)\right)$.

Proposition 34. *Let R_S be the ring constructed in section 3.2. If $r=1, k=1$ and $h\geq 1$, then*

$$U(R_S)\cong\begin{cases}\mathbb{Z}_2^h & \text{if } p=2;\\ \mathbb{Z}_{p-1}\times\mathbb{Z}_p^h & \text{if } p\neq 2.\end{cases}$$

Proof. Given that $k=1$, then it is easily shown that

$$J(R_S)=\left\{\left[\frac{\lambda_1u_1+\cdots+\lambda_hu_h}{s}\right]\mid\lambda_i\in\mathbb{Z}_p, u_i\in R, 1\leq i\leq h, s\in U(R)\right\}$$

and $(J(R_S))^2 = \left[\frac{0}{1}\right]$. Since $\left[\frac{p}{s}\right] \in J(R_S), \left[\frac{p}{s}\right] \cdot \left[\frac{m}{s}\right] = \left[\frac{pm}{s^2}\right] = \left[\frac{0}{1}\right]$ for any $\left[\frac{m}{s}\right] \in J(R_S)$.

Also $\mid J(R_S) \mid = p^h$ for some positive integer h such that $\mid U(R_S) \mid = p^h(p-1)$. But

$$U(R_S) = \left\{ \left[\frac{\alpha + \lambda_1 u_1 + \cdots + \lambda_h u_h}{s} \right] \mid \alpha, s \in U(R), \lambda_i \in \mathbb{Z}_p, u_i \in R, 1 \leq i \leq h \right\}$$

Let $p = 2$.

Suppose $\lambda_1 \in \mathbb{Z}_2$ and consider the element

$$\left[\frac{1}{1} + \frac{\lambda_1 u_1}{s}\right] \in U(R_S).$$

Then

$$\left(\left[\frac{1}{1} + \frac{\lambda_1 u_1}{s}\right]\right)^2 = \left[\frac{1}{1} + 2\frac{\lambda_1 u_1}{s}\right]$$

(since $u_1^2 = 0$)

$$= \left[\frac{1}{1}\right]$$

(since char $R = 2$ and $2\frac{\lambda_1 u_1}{s} = \frac{0}{s}$).

So $\left[\frac{1}{1} + \frac{\lambda_1 u_1}{s}\right]$ generates a cyclic subgroup of $U(R_S)$ of order 2.

Next, consider the element

$$\left[\frac{1}{1} + \frac{\lambda_2 u_2}{s}\right] \in U(R_S).$$

Then

$$\left(\left[\frac{1}{1} + \frac{\lambda_2 u_2}{s}\right]\right)^2 = \left[\frac{1}{1} + 2\frac{\lambda_2 u_2}{s}\right]$$

(since $u_2^2 = 0$)

$$= \left[\frac{1}{1}\right]$$

(since char $R = 2$ and $2\frac{\lambda_2 u_2}{s} = \frac{0}{s}$).

So

$$\left[\frac{1}{1} + \frac{\lambda_2 u_2}{s}\right]$$

generates a cyclic subgroup of $U(R_S)$ of order 2.

Continuing inductively up to the element

$$\left[\frac{1}{1} + \frac{\lambda_h u_h}{s}\right],$$

we notice that the element also generates a cyclic subgroup of $U(R_S)$ of order 2. Since $U(R_S)$ is abelian, each cyclic subgroup is normal, the intersection of any pair of the cyclic subgroups is the identity group $\left[\frac{1}{1}\right]$ and the order of the group generated by the direct product of the h cyclic subgroups coincides with $\mid U(R_S) \mid$. Hence, the direct product exhausts $U(R_S)$.

Let p be odd.

It is well known that $U(R_S) = \left(U(R_S)/\frac{1}{1} + J(R_S)\right) \times \left(\frac{1}{1} + J(R_S)\right) =< \xi > \times \left(\frac{1}{1} + J(R_S)\right)$, where ξ is of order $p-1$.

Next, we show that $\frac{1}{1} + J(R_S)$ is isomorphic to a direct product of h cyclic subgroups each of order p.

Consider, the elements

$$\left[\frac{1}{1} + \frac{\lambda_1 u_1}{s}\right], \left[\frac{1}{1} + \frac{\lambda_2 u_2}{s}\right], \ldots \left[\frac{1}{1} + \frac{\lambda_h u_h}{s}\right]$$

where $\lambda_1, \ldots, \lambda_h \in U(\mathbb{Z}_p), u_1, \ldots, u_h \in R, s \in U(R)$. Clearly, each of the elements generates a cyclic subgroup of $\frac{1}{1} + J(R_S)$ of order p. Since $\frac{1}{1} + J(R_S)$ is abelian, each cyclic subgroup is normal.

Moreover, the order of the group generated by the direct product of the h subgroups coincides with $\mid \frac{1}{1} + J(R_S) \mid$. So the direct product of the subgroups exhausts $\frac{1}{1} + J(R_S)$. Therefore, $\mid U(R_S) \mid = \mid < \xi > \mid \cdot \mid \frac{1}{1} + J(R_S) \mid$implying that $U(R_S) \cong \mathbb{Z}_{p-1} \times \left(\frac{1}{1} + J(R_S)\right)$, which completes the proof. □

Proposition 35. *The unit group $U(R_S)$ of a total quotient ring constructed in section 3.2 with characteristic p and $r > 1$ is isomorphic to $\mathbb{Z}_{p^r-1} \times (\mathbb{Z}_p^r)^h$*

Proof. Let $\lambda_1, \ldots, \lambda_r \in R'$ with $\lambda_1 = 1$ such that $\overline{\lambda_1}, \ldots, \overline{\lambda_r} \in R'/pR'$ form a basis for R'/pR' regarded as a vector space over its prime subfield $\mathbb{F}_p$. Further, let $s_1, \ldots, s_h \in S = U(R_S)$. Since $J(R_S)$ is a maximal ideal of R_S, $(R_S/J(R_S))$ is a field, so that $U\left(R_S/J(R_S)\right)$ is a cyclic group of order $p^r - 1$ with respect to the equivalence relation on fractions in R_S. But $U\left(R_S/J(R_S)\right) = U(R_S)/\frac{1}{1} + J(R_S)$. So

$$U(R_S) = U\left(R_S/J(R_S)\right) \cdot \left(\frac{1}{1} + J(R_S)\right) \cong \mathbb{Z}_{p^r-1} \times \left(\frac{1}{1} + J(R_S)\right).$$

Next, we determine the structure of $\frac{1}{1}+J(R_S)$.

For every $l=1,\ldots,r$ and $1\leq i\leq h$, $\left[\frac{1}{1}+\frac{\lambda_l u_i}{s_i}\right]\in\frac{1}{1}+J(R_S)$, $\left[\frac{1}{1}+\frac{\lambda_l u_i}{s_i}\right]^2=\frac{1}{1}$. For positive integers $a_{2l},a_{1l},\ldots,a_{hl}$ with $a_{1l}\leq p, a_{2l}\leq p.\ldots,a_{hl}\leq p$, we assert that

$$\prod_{l=1}^{r}\left\{\left(\left[\frac{1}{1}+\frac{\lambda_l u_1}{s_1}\right]\right)^{a_{1l}}\right\}\cdot\prod_{l=1}^{r}\left\{\left(\left[\frac{1}{1}+\frac{\lambda_l u_2}{s_2}\right]\right)^{a_{2l}}\right\}\cdot\ldots\cdot\prod_{l=1}^{r}\left\{\left(\left[\frac{1}{1}+\frac{\lambda_l u_h}{s_h}\right]\right)^{a_{hl}}\right\}=\left[\frac{1}{1}\right]$$

will imply $a_{il}=p$ for every $l=1,\ldots,r$ and $1\leq i\leq h$.

If we set

$$S_{1l}=\left\{\left(\left[\frac{1}{1}+\frac{\lambda_l u_1}{s_1}\right]\right)^{a_1}\mid a_1=1,\ldots,p\right\}$$
$$S_{2l}=\left\{\left(\left[\frac{1}{1}+\frac{\lambda_l u_2}{s_2}\right]\right)^{a_2}\mid a_2=1,\ldots,p\right\}$$
$$\vdots$$
$$S_{hl}=\left\{\left(\left[\frac{1}{1}+\frac{\lambda_l u_h}{s_h}\right]\right)^{a_h}\mid a_h=1,\ldots,p\right\};$$

it is easily noticed that $S_{1l},S_{2l},\ldots,S_{hl}$ are cyclic subgroups of the group $\frac{1}{1}+J(R_S)$ and each is of order p. Since

$$\prod_{l=1}^{r}|<\left[\frac{1}{1}+\frac{\lambda_l u_1}{s_1}\right]>|\cdot\prod_{l=1}^{r}|<\left[\frac{1}{1}+\frac{\lambda_l u_2}{s_2}\right]>|\cdot\cdots\cdot\prod_{l=1}^{r}|<\left[\frac{1}{1}+\frac{\lambda_l u_h}{s_h}\right]>|=p^{hr},$$

the intersection of any pair of the cyclic subgroups yields the identity group $<\frac{1}{1}>$, then the product of the hr subgroups $S_{1l},S_{2l},\ldots,S_{hl}$ is direct, exhausting the group $\frac{1}{1}+J(R_S)$.

□

Example 1. *From the above proposition, let $r=1$, $p=2$ and $h=1$ so that $R=\mathbb{Z}_2\oplus\mathbb{Z}_2, J(R)=2\mathbb{Z}_2=\{0\}, S=\{1\}$ and*

$$S^{-1}R=\left\{\frac{(0,0)}{(1,0)},\frac{(0,1)}{(1,0)},\frac{(1,0)}{(1,0)},\frac{(1,1)}{(1,0)},\frac{(0,0)}{(1,1)},\frac{(0,1)}{(1,1)},\frac{(1,0)}{(1,1)},\frac{(1,1)}{(1,1)}\right\}$$

By definition 3.2.2 we see that R_S consists of the following equivalence classes

$$\left\{\left[\frac{(0,0)}{(1,0)}\right],\left[\frac{(0,1)}{(1,0)}\right],\left[\frac{(1,0)}{(1,0)}\right],\left[\frac{(1,1)}{(1,0)}\right]\right\}$$
$$J(R_S)=\left\{\left[\frac{(0,0)}{(1,0)}\right],\left[\frac{(0,1)}{(1,0)}\right]\right\}$$

and

$$\frac{(1,0)}{(1,0)} + J(R_S) = \left\{ \left[\frac{(1,0)}{(1,0)}\right], \left[\frac{(1,1)}{(1,0)}\right] \right\} = U(R_S).$$

In this case we see that $\frac{(1,0)}{(1,0)} + J(R_S)$ *and* $U(R_S)$ *coincide. Here we see that* $\left[\frac{(1,1)}{(1,0)}\right]$ *generates the abelian group* $\frac{(1,0)}{(1,0)} + J(R_S)$ *since*

$$\left(\left[\frac{(1,1)}{(1,0)}\right]\right)^2 = \frac{(1,0)}{(1,0)};$$

we notice that the element $\left[\frac{(1,1)}{(1,0)}\right]$ *is of order* 2*, thus*

$$< \left[\frac{(1,1)}{(1,0)}\right] > \cong \mathbb{Z}_2$$

Example 2. *When* $p = 3$*,* $r = 1$ *and* $h = 1$ *then*

$$S^{-1}R = \left\{ \frac{(0,0)}{(1,0)}, \frac{(0,1)}{(1,0)}, \frac{(0,2)}{(1,0)}, \frac{(1,0)}{(1,0)}, \frac{(1,1)}{(1,0)}, \frac{(1,2)}{(1,0)}, \frac{(2,0)}{(1,0)}, \frac{(2,1)}{(1,0)}, \frac{(2,2)}{(1,0)}, \frac{(0,0)}{(1,1)}, \frac{(0,1)}{(1,1)}, \frac{(0,2)}{(1,1)}, \frac{(1,0)}{(1,1)}, \right.$$

$$\frac{(1,1)}{(1,1)}, \frac{(1,2)}{(1,1)}, \frac{(2,0)}{(1,1)}, \frac{(2,1)}{(1,1)}, \frac{(2,2)}{(1,1)}, \frac{(0,0)}{(1,2)}, \frac{(0,1)}{(1,2)}, \frac{(0,2)}{(1,2)}, \frac{(1,0)}{(1,2)}, \frac{(1,1)}{(1,2)}, \frac{(1,2)}{(1,2)}, \frac{(2,0)}{(1,2)}, \frac{(2,1)}{(1,2)}, \frac{(2,2)}{(1,2)},$$

$$\frac{(0,0)}{(2,0)}, \frac{(0,1)}{(2,0)}, \frac{(0,2)}{(2,0)}, \frac{(1,0)}{(2,0)}, \frac{(1,1)}{(2,0)}, \frac{(1,2)}{(2,0)}, \frac{(2,0)}{(2,0)}, \frac{(2,1)}{(2,0)}, \frac{(2,2)}{(2,0)}, \frac{(0,0)}{(2,1)}, \frac{(0,1)}{(2,1)}, \frac{(0,2)}{(2,1)}, \frac{(1,0)}{(2,1)}, \frac{(1,1)}{(2,1)},$$

$$\left. \frac{(1,2)}{(2,1)}, \frac{(2,0)}{(2,1)}, \frac{(2,1)}{(2,1)}, \frac{(2,2)}{(2,1)}, \frac{(0,0)}{(2,2)}, \frac{(0,1)}{(2,2)}, \frac{(0,2)}{(2,2)}, \frac{(1,0)}{(2,2)}, \frac{(1,1)}{(2,2)}, \frac{(1,2)}{(2,2)}, \frac{(2,0)}{(2,2)}, \frac{(2,1)}{(2,2)}, \frac{(2,2)}{(2,2)} \right\}.$$

By definition 3.2.2, we have the following equivalence classes

$$R_S = \left\{ \left[\frac{(0,0)}{(1,0)}\right], \left[\frac{(0,1)}{(1,0)}\right], \left[\frac{(0,2)}{(1,0)}\right], \left[\frac{(1,0)}{(1,0)}\right], \left[\frac{(1,1)}{(1,0)}\right], \left[\frac{(1,2)}{(1,0)}\right], \left[\frac{(2,0)}{(1,0)}\right], \left[\frac{(2,1)}{(1,0)}\right], \left[\frac{(2,2)}{(1,0)}\right] \right\}.$$

Now we have

$$J(R_S) = \left\{ \left[\frac{(0,0)}{(1,0)}\right], \left[\frac{(0,1)}{(1,0)}\right], \left[\frac{(0,2)}{(1,0)}\right] \right\}.$$

$$U(R_S) = R_S - J(R_S) = \left\{ \left[\frac{(1,0)}{(1,0)}\right], \left[\frac{(1,1)}{(1,0)}\right], \left[\frac{(1,2)}{(1,0)}\right], \left[\frac{(2,0)}{(1,0)}\right], \left[\frac{(2,1)}{(1,0)}\right], \left[\frac{(2,2)}{(1,0)}\right] \right\}$$

and

$$\frac{(1,0)}{(1,0)} + J(R_S) = \left\{ \left[\frac{(1,0)}{(1,0)}\right], \left[\frac{(1,1)}{(1,0)}\right], \left[\frac{(1,2)}{(1,0)}\right] \right\}.$$

Through inspection we see that the only generator is $\left[\frac{(1,1)}{(1,0)}\right]$. *This can be verified as follows*

$$\left(\left[\frac{(1,1)}{(1,0)}\right]\right)^2 = \left[\frac{(1,2)}{(1,0)}\right]$$

$$\left(\left[\frac{(1,1)}{(1,0)}\right]\right)^3 = \left[\frac{(1,2)}{(1,0)}\right] \cdot \left[\frac{(1,1)}{(1,0)}\right] = \frac{(1,0)}{(1,0)}$$

We see that the element $\left[\frac{(1,1)}{(1,0)}\right]$ *generates the group* $\frac{(1,0)}{(1,0)} + J(R_S)$ *and is of order* 3.

Thus

$$< \left[\frac{(1,1)}{(1,0)}\right] > \cong \mathbb{Z}_3$$

Next, we consider the case when $k = 2$:

The construction in section 3.2 yields a total quotient ring R_S in which $(J(R_S))^2 = [(0,1)]$.

4.2.4 The Unit groups when the characteristic of R_S is p^2

Let R_S be the total quotient ring with maximal ideal $J(R_S)$ such that $(J(R_S))^2 = [(0,1)]$. Then R_S is of order $p^{(h+2)r}$. Since R_S is of the given order and $U(R_S) = R_S - J(R_S)$, then $|U(R_S)| = p^{(h+1)r}(p^r - 1)$ and $|\frac{1}{1} + J(R_S)| = p^{(h+1)r}$. So $\frac{1}{1} + J(R_S)$ is an abelian p-group.

Proposition 36. *Let* R_S *be the ring constructed in Section 3.2. If* $r = 1, k = 2$ *and* $h \geq 1$, *then*

$$U(R_S) \cong \begin{cases} \mathbb{Z}_2 \times \mathbb{Z}_2^h & \text{if } p = 2; \\ \mathbb{Z}_{p-1} \times \mathbb{Z}_p \times \mathbb{Z}_p^h & \text{if } p \neq 2. \end{cases}$$

Proof. Now

$$U(R_S) = U\left(R_S/J(R_S)\right) \cdot \left(\frac{1}{1} + J(R_S)\right) \cong \mathbb{Z}_{p-1} \times \left(\frac{1}{1} + J(R_S)\right).$$

The structure of $\frac{1}{1} + J(R_S)$. is obtained as follows:

$$J(R_S) = \left\{ \left[\frac{p\lambda_1 + \lambda_1 u_1 + \cdots + \lambda_h u_h}{s}\right] \mid \lambda_i \in \mathbb{Z}_p, u_i \in R, 1 \leq i \leq h, s \in U(R) \right\}$$

and $(J(R_S))^2 = [(0,1)]$. Also $\mid J(R_S) \mid = p^{h+1}$ for some positive integer h such that $\mid U(R_S) \mid =$

$p^{h+1}(p-1)$. But

$$U(R_S) = \left\{ \left[\frac{\alpha + p\lambda_1 + \lambda_1 u_1 + \cdots + \lambda_h u_h}{s} \right] \mid \alpha \in U(R), \lambda_i \in \mathbb{Z}_p, u_i \in R, 1 \leq i \leq h, s \in U(R) \right\}$$

Let $p = 2$.

Suppose $\lambda_1 \in \mathbb{Z}_{p^2}/p\mathbb{Z}_{p^2}$ and

$$\left[\frac{1}{1} + \frac{p\lambda_1}{s}\right], \left[\frac{1}{1} + \frac{\lambda_i u_i}{s}\right] \in U(R_S).$$

Now, consider the element

$$\left[\frac{1}{1} + \frac{p\lambda_1}{s}\right].$$

Then

$$\left(\left[\frac{1}{1} + \frac{p\lambda_1}{s}\right]\right)^p = \left[\frac{1}{1} + 2\frac{p\lambda_1}{s}\right]$$

(since $p^2 = 0$)

$$= \left[\frac{1}{1}\right]$$

(since char $R = p^2$ and $2\frac{p\lambda_1}{s} = \frac{4\lambda_1}{s} = \frac{0}{s}$).

So $\left[\frac{1}{1} + \frac{p\lambda_1}{s}\right]$ generates a cyclic subgroup of $U(R_S)$ of order p.

Next, consider the element

$$\left[\frac{1}{1} + \frac{\lambda_1 u_1}{s}\right] \in U(R_S).$$

Then

$$\left(\left[\frac{1}{1} + \frac{\lambda_1 u_1}{s}\right]\right)^p = \left[\frac{1}{1} + p\frac{\lambda_1 u_1}{s}\right]$$

(since $u_1^2 = 0$)

$$= \left[\frac{1}{1}\right]$$

(since char $R = p^2$ and $p\frac{\lambda_1 u_1}{s} = \frac{0}{s}$).

So,

$$\left[\frac{1}{1} + \frac{\lambda_1 u_1}{s}\right]$$

generates a cyclic subgroup of $U(R_S)$ of order p.

Next, consider the element

$$\left[\frac{1}{1}+\frac{\lambda_2 u_2}{s}\right] \in U(R_S).$$

Then

$$\left(\left[\frac{1}{1}+\frac{\lambda_2 u_2}{s}\right]\right)^p = \left[\frac{1}{1}+p\frac{\lambda_2 u_2}{s}\right]$$

(since $u_2^2 = 0$)

$$= \left[\frac{1}{1}\right]$$

(since char $R = p^2$ and $p\frac{\lambda_2 u_2}{s} = \frac{0}{s}$).

So,

$$\left[\frac{1}{1}+\frac{\lambda_2 u_2}{s}\right]$$

generates a cyclic subgroup of $U(R_S)$ of order p.

Continuing in a similar manner up to the element $\left[\frac{1}{1}+\frac{\lambda_h u_h}{s}\right]$, we notice that it also generates a cyclic subgroup of $U(R_S)$ of order p. Since $U(R_S)$ is abelian, each cyclic subgroup is normal, the intersection of any pair of the cyclic subgroups is the identity group $\left[\frac{1}{1}\right]$ and the order of the group generated by the direct product of the $h+1$ cyclic subgroups coincides with $\mid U(R_S) \mid$. Hence, the direct product exhausts $U(R_S)$.

□

Proposition 37. *The unit group $U(R_S)$ of the total quotient ring constructed in section 3.2 with characteristic p^2 is isomorphic to $\mathbb{Z}_{p^r-1} \times \mathbb{Z}_p^r \times (\mathbb{Z}_p^r)^h$*

Proof. Let $\lambda_1, \ldots, \lambda_r \in R'$ with $\lambda_1 = 1$ such that $\overline{\lambda_1}, \ldots, \overline{\lambda_r} \in R'/pR'$ form a basis for R'/pR' regarded as a vector space over its prime subfield $\mathbb{F}_p$. Let $s_1, \ldots, s_h \in S = U(R_S)$. Now

$$U(R_S) = U\left(R_S/J(R_S)\right) \cdot \left(\frac{1}{1}+J(R_S)\right) \cong \mathbb{Z}_{p^r-1} \times \left(\frac{1}{1}+J(R_S)\right).$$

The structure of $\frac{1}{1}+J(R_S)$. is obtained as follows;

For each $l = 1, \ldots, r$ and $1 \leq i \leq h$, $\left[\frac{1}{1}+\frac{p\lambda_l}{s}\right], \left[\frac{1}{1}+\frac{\lambda_l u_i}{s_i}\right] \in \frac{1}{1}+J(R_S)$ and $\left(\left[\frac{1}{1}+\frac{p\lambda_l}{s}\right]\right)^p = \frac{1}{1}, \left(\left[\frac{1}{1}+\frac{\lambda_l u_1}{s_1}\right]\right)^p = \frac{1}{1}, \left(\left[\frac{1}{1}+\frac{\lambda_l u_2}{s_2}\right]\right)^p = \frac{1}{1}, \ldots, \left(\left[\frac{1}{1}+\frac{\lambda_l u_h}{s_h}\right]\right)^p = \frac{1}{1}$. For positive integers $\alpha_l, \beta_{1l}, \ldots, \beta_{hl}$

with $\alpha_l \leq p, \beta_{il} \leq p (1 \leq i \leq h, 1 \leq l \leq r)$, we notice that

$$\prod_{l=1}^{r} \left\{ \left(\left[\frac{1}{1} + \frac{p\lambda_l}{s} \right] \right)^{\alpha_l} \right\} \cdot \prod_{l=1}^{r} \left\{ \left(\left[\frac{1}{1} + \frac{\lambda_l u_1}{s_1} \right] \right)^{\beta_{1l}} \right\} \cdot \prod_{l=1}^{r} \left\{ \left(\left[\frac{1}{1} + \frac{\lambda_l u_2}{s_2} \right] \right)^{\beta_{2l}} \right\} \cdot$$

$$\cdots \prod_{l=1}^{r} \left\{ \left(\left[\frac{1}{1} + \frac{\lambda_l u_h}{s_h} \right] \right)^{\beta_{hl}} \right\} = \left\{ \left[\frac{1}{1} \right] \right\}$$

will imply $\alpha_l = \beta_{il} = p$ for every $l = 1, \ldots, r$ and $1 \leq i \leq h$.

If we set

$$T_l = \left\{ \left(\left[\frac{1}{1} + \frac{p\lambda_l}{s} \right] \right)^{\alpha} \mid \alpha = 1, \ldots, p \right\}$$

$$S_{1l} = \left\{ \left(\left[\frac{1}{1} + \frac{\lambda_l u_1}{s_1} \right] \right)^{\beta_1} \mid \beta_1 = 1, \ldots, p \right\}$$

$$S_{2l} = \left\{ \left(\left[\frac{1}{1} + \frac{\lambda_l u_2}{s_2} \right] \right)^{\beta_2} \mid \beta_2 = 1, \ldots, p \right\}$$

$$\vdots$$

$$S_{hl} = \left\{ \left(\left[\frac{1}{1} + \frac{\lambda_l u_h}{s_h} \right] \right)^{\beta_h} \mid \beta_h = 1, \ldots, p \right\};$$

it is easily noticed that $T_l, S_{1l}, S_{2l}, \ldots, S_{hl}$ are cyclic subgroups of the group $\frac{1}{1} + J(R_S)$ and each is of order p. Since

$$\prod_{l=1}^{r} |< \left[\frac{1}{1} + \frac{p\lambda_l}{s} \right] >| \cdot \prod_{l=1}^{r} |< \left[\frac{1}{1} + \frac{\lambda_l u_1}{s_1} \right] >| \cdot \prod_{l=1}^{r} |< \left[\frac{1}{1} + \frac{\lambda_l u_2}{s_2} \right] >| \cdot \ldots$$

$$\cdot \prod_{l=1}^{r} |< \left[\frac{1}{1} + \frac{\lambda_l u_h}{s_h} \right] >| = p^{(h+1)r},$$

the intersection of any pair of the cyclic subgroups yields the identity group $< \left[\frac{1}{1} \right] >$, then the product of the $(h+1)r$ subgroups $T_l, S_{1l}, S_{2l}, \ldots, S_{hl}$ is direct and exhausts the group $\frac{1}{1} + J(R_S)$. □

Example 3. *From the proposition above, let* $p = 2, k = 2, r = 1$ *and* $h = 1$

$R = \mathbb{Z}_4 \oplus \mathbb{F}_2, J(R_S) = 2\mathbb{Z}_4, S = 1 + 2\mathbb{Z}_4$ *and* $S^{-1}R = (1 + 2\mathbb{Z}_4)^{-1}(\mathbb{Z}_4 \oplus \mathbb{F}_2)$.

$$S^{-1}R = \left\{ \frac{(0,0)}{(1,0)}, \frac{(0,1)}{(1,0)}, \frac{(0,2)}{(1,0)}, \frac{(0,3)}{(1,0)} \frac{(1,0)}{(1,0)}, \frac{(1,1)}{(1,0)}, \frac{(1,2)}{(1,0)}, \frac{(1,3)}{(1,0)}, \right.$$

$$\frac{(2,0)}{(1,0)}, \frac{(2,1)}{(1,0)}, \frac{(2,2)}{(1,0)}, \frac{(2,3)}{(1,0)}, \frac{(3,0)}{(1,0)}, \frac{(3,1)}{(1,0)}, \frac{(3,2)}{(1,0)}, \frac{(3,3)}{(1,0)}$$

$$\frac{(0,0)}{(1,2)}, \frac{(0,1)}{(1,2)}, \frac{(0,2)}{(1,2)}, \frac{(0,3)}{(1,2)} \frac{(1,0)}{(1,2)}, \frac{(1,1)}{(1,2)}, \frac{(1,2)}{(1,2)}, \frac{(1,3)}{(1,2)},$$

$$\frac{(2,0)}{(1,2)}, \frac{(2,1)}{(1,2)}, \frac{(2,2)}{(1,2)}, \frac{(2,3)}{(1,2)}, \frac{(3,0)}{(1,2)}, \frac{(3,1)}{(1,2)}, \frac{(3,2)}{(1,2)}, \frac{(3,3)}{(1,2)},$$

$$\frac{(0,0)}{(1,3)}, \frac{(0,1)}{(1,3)}, \frac{(0,2)}{(1,3)}, \frac{(0,3)}{(1,3)} \frac{(1,0)}{(1,3)}, \frac{(1,1)}{(1,3)}, \frac{(1,2)}{(1,3)}, \frac{(1,3)}{(1,3)},$$

$$\frac{(2,0)}{(1,3)}, \frac{(2,1)}{(1,3)}, \frac{(2,2)}{(1,3)}, \frac{(2,3)}{(1,3)}, \frac{(3,0)}{(1,3)}, \frac{(3,1)}{(1,3)}, \frac{(3,2)}{(1,3)}, \frac{(3,3)}{(1,3)},$$

$$\frac{(0,0)}{(3,1)}, \frac{(0,1)}{(3,1)}, \frac{(0,2)}{(3,1)}, \frac{(0,3)}{(3,1)} \frac{(1,0)}{(3,1)}, \frac{(1,1)}{(3,1)}, \frac{(1,2)}{(3,1)}, \frac{(1,3)}{(3,1)},$$

$$\frac{(2,0)}{(3,1)}, \frac{(2,1)}{(3,1)}, \frac{(2,2)}{(3,1)}, \frac{(2,3)}{(3,1)}, \frac{(3,0)}{(3,1)}, \frac{(3,1)}{(3,1)}, \frac{(3,2)}{(3,1)}, \frac{(3,3)}{(3,1)},$$

$$\frac{(0,0)}{(3,2)}, \frac{(0,1)}{(3,2)}, \frac{(0,2)}{(3,2)}, \frac{(0,3)}{(3,2)} \frac{(1,0)}{(3,2)}, \frac{(1,1)}{(3,2)}, \frac{(1,2)}{(3,2)}, \frac{(1,3)}{(3,2)},$$

$$\frac{(2,0)}{(3,2)}, \frac{(2,1)}{(3,2)}, \frac{(2,2)}{(3,2)}, \frac{(2,3)}{(3,2)}, \frac{(3,0)}{(3,2)}, \frac{(3,1)}{(3,2)}, \frac{(3,2)}{(3,2)}, \frac{(3,3)}{(3,2)},$$

$$\frac{(0,0)}{(3,3)}, \frac{(0,1)}{(3,3)}, \frac{(0,2)}{(3,3)}, \frac{(0,3)}{(3,3)} \frac{(1,0)}{(3,3)}, \frac{(1,1)}{(3,3)}, \frac{(1,2)}{(3,3)}, \frac{(1,3)}{(3,3)},$$

$$\frac{(2,0)}{(3,3)}, \frac{(2,1)}{(3,3)}, \frac{(2,2)}{(3,3)}, \frac{(2,3)}{(3,3)}, \frac{(3,0)}{(3,3)}, \frac{(3,1)}{(3,3)}, \frac{(3,2)}{(3,3)}, \frac{(3,3)}{(3,3)} \Bigg\}$$

By definition 3.2.2 we see that R_S consists of the following equivalence classes

$$R_S = \Bigg\{ \left[\frac{(0,0)}{(1,0)}\right], \left[\frac{(0,1)}{(1,0)}\right], \left[\frac{(0,2)}{(1,0)}\right], \left[\frac{(0,3)}{(1,0)}\right], \left[\frac{(1,0)}{(1,0)}\right], \left[\frac{(1,1)}{(1,0)}\right], \left[\frac{(1,2)}{(1,0)}\right], \left[\frac{(1,3)}{(1,0)}\right],$$

$$\left[\frac{(2,0)}{(1,0)}\right], \left[\frac{(2,1)}{(1,0)}\right], \left[\frac{(2,2)}{(1,0)}\right], \left[\frac{(2,3)}{(1,0)}\right], \left[\frac{(3,0)}{(1,0)}\right], \left[\frac{(3,1)}{(1,0)}\right], \left[\frac{(3,2)}{(1,0)}\right], \left[\frac{(3,3)}{(1,0)}\right] \Bigg\}$$

$$J(R_S) = \left\{ \left[\frac{(0,0)}{(1,0)}\right], \left[\frac{(0,1)}{(1,0)}\right], \left[\frac{(0,2)}{(1,0)}\right], \left[\frac{(0,3)}{(1,0)}\right], \left[\frac{(2,0)}{(1,0)}\right], \left[\frac{(2,1)}{(1,0)}\right], \left[\frac{(2,2)}{(1,0)}\right], \left[\frac{(2,3)}{(1,0)}\right] \right\}$$

and

$$\frac{(1,0)}{(1,0)} + J(R_S) = \left\{ \left[\frac{(1,0)}{(1,0)}\right], \left[\frac{(1,1)}{(1,0)}\right], \left[\frac{(1,2)}{(1,0)}\right], \left[\frac{(1,3)}{(1,0)}\right], \left[\frac{(3,0)}{(1,0)}\right], \left[\frac{(3,1)}{(1,0)}\right], \left[\frac{(3,2)}{(1,0)}\right], \left[\frac{(3,3)}{(1,0)}\right] \right\}.$$

We now determine the generators of $\frac{(1,0)}{(1,0)} + J(R_S)$. Here we see through inspection that the generators are

$$\left(\left[\frac{(1,1)}{(1,0)}\right]\right)^2 = \frac{(1,0)}{(1,0)}$$

and

$$\left(\left[\frac{(3,0)}{(1,0)}\right]\right)^2 = \frac{(1,0)}{(1,0)}$$

Both $\left[\frac{(1,1)}{(1,0)}\right]$ *and* $\left[\frac{(3,0)}{(1,0)}\right]$ *are of order* 2, *thus*

$$< \left(\left[\frac{(1,1)}{(1,0)}\right]\right) > \cong \mathbb{Z}_2$$

$$< \left(\left[\frac{(3,0)}{(1,0)}\right]\right) > \cong \mathbb{Z}_2.$$

Therefore the product is given by

$$< \left(\left[\frac{(1,1)}{(1,0)}\right]\right) > \cdot < \left(\left[\frac{(3,0)}{(1,0)}\right]\right) > \cong \mathbb{Z}_2 \times \mathbb{Z}_2$$

Example 4. *Let* $p = 3$ *then set of equivalence classes is given as*

$$R_S = \left\{ \left[\frac{(0,0)}{(1,0)}\right], \left[\frac{(0,1)}{(1,0)}\right], \left[\frac{(0,2)}{(1,0)}\right], \left[\frac{(1,0)}{(1,0)}\right], \left[\frac{(1,1)}{(1,0)}\right], \left[\frac{(1,2)}{(1,0)}\right], \left[\frac{(2,0)}{(1,0)}\right], \left[\frac{(2,1)}{(1,0)}\right], \left[\frac{(2,2)}{(1,0)}\right], \right.$$
$$\left[\frac{(3,0)}{(1,0)}\right], \left[\frac{(3,1)}{(1,0)}\right], \left[\frac{(3,1)}{(1,0)}\right], \left[\frac{(4,0)}{(1,0)}\right], \left[\frac{(4,1)}{(1,0)}\right], \left[\frac{(4,2)}{(1,0)}\right], \left[\frac{(5,0)}{(1,0)}\right], \left[\frac{(5,1)}{(1,0)}\right], \left[\frac{(5,2)}{(1,0)}\right],$$
$$\left.\left[\frac{(6,0)}{(1,0)}\right], \left[\frac{(6,1)}{(1,0)}\right], \left[\frac{(6,1)}{(1,0)}\right], \left[\frac{(7,0)}{(1,0)}\right], \left[\frac{(7,1)}{(1,0)}\right], \left[\frac{(7,2)}{(1,0)}\right], \left[\frac{(8,0)}{(1,0)}\right], \left[\frac{(8,1)}{(1,0)}\right], \left[\frac{(8,2)}{(1,0)}\right] \right\}.$$

We now have

$$J(R_S) = \left\{ \left[\frac{(0,0)}{(1,0)}\right], \left[\frac{(0,1)}{(1,0)}\right], \left[\frac{(0,2)}{(1,0)}\right], \left[\frac{(3,0)}{(1,0)}\right], \left[\frac{(3,1)}{(1,0)}\right], \left[\frac{(3,2)}{(1,0)}\right], \left[\frac{(6,0)}{(1,0)}\right], \left[\frac{(6,1)}{(1,0)}\right], \left[\frac{(6,2)}{(1,0)}\right] \right\}$$

and

$$\frac{(1,0)}{(1,0)} + J(R_S) = \left\{ \left[\frac{(1,0)}{(1,0)}\right], \left[\frac{(1,1)}{(1,0)}\right], \left[\frac{(1,2)}{(1,0)}\right], \left[\frac{(4,0)}{(1,0)}\right], \left[\frac{(4,1)}{(1,0)}\right], \left[\frac{(4,2)}{(1,0)}\right], \right.$$
$$\left.\left[\frac{(7,0)}{(1,0)}\right], \left[\frac{(7,1)}{(1,0)}\right], \left[\frac{(7,2)}{(1,0)}\right] \right\}.$$

Through inspection we see that the elements

$$\left[\frac{(1,1)}{(1,0)}\right]$$

and

$$\left[\frac{(4,0)}{(1,0)}\right]$$

generate the group $\frac{(1,0)}{(1,0)} + J(R_S)$. *This can be verified as follows*

$$\left(\left[\frac{(1,1)}{(1,0)}\right]\right)^2 = \left[\frac{(1,2)}{(1,0)}\right]$$

$$\left(\left[\frac{(1,1)}{(1,0)}\right]\right)^3 = \left[\frac{(1,2)}{(1,0)}\right] \cdot \left[\frac{(1,1)}{(1,0)}\right] = \left[\frac{(1,0)}{(1,0)}\right]$$

and

$$\left(\left[\frac{(4,0)}{(1,0)}\right]\right)^2 = \left[\frac{(7,0)}{(1,0)}\right]$$

$$\left(\left[\frac{(4,0)}{(1,0)}\right]\right)^3 = \left[\frac{(7,0)}{(1,0)}\right] \cdot \left[\frac{(4,0)}{(1,0)}\right] = \left[\frac{(1,0)}{(1,0)}\right].$$

We see that the elements

$$\left[\frac{(1,1)}{(1,0)}\right]$$

and

$$\left[\frac{(4,0)}{(1,0)}\right]$$

generate the group $\frac{(1,0)}{(1,0)} + J(R_S)$ *and each is of order* 3.

Thus

$$< \left(\left[\frac{(1,1)}{(1,0)}\right]\right) > \cong \mathbb{Z}_3$$

and

$$< \left(\left[\frac{(4,0)}{(1,0)}\right]\right) > \cong \mathbb{Z}_3.$$

Taking the product we have

$$< \left(\left[\frac{(4,0)}{(1,0)}\right]\right) > \cdot < \left(\left[\frac{(1,1)}{(1,0)}\right]\right) > \cong \mathbb{Z}_3 \times \mathbb{Z}_3$$

Finally, let us consider the case when $k \geq 3$

The construction in Section 3.2 yields a total quotient ring in which $(J(R_S))^k = [(0,1)]$. We now determine the structure of their unit groups.

4.2.5 The Unit groups when the characteristic of R_S is p^k with $k \geq 3$

Proposition 38. *Let R_S be a local ring of characteristic p^k with $k \geq 3$. Then the group of units $U(R_S)$ of R_S contains a cyclic subgroup $< \xi >$ of order $p^r - 1$, and $U(R_S)$ is a semi direct product of $\frac{1}{1} + J(R_S)$ by $< \xi >$.*

Proof. See proposition 30. □

In order to completely classify the groups of units of the total quotient ring, we determine the structure of $\frac{1}{1} + J(R_S)$.

Proposition 39. *Let R_S be the total quotient ring construction of Section 3.2. If $k = 3, r = 1$ and $h \geq 1$, then*

$$\frac{1}{1} + J(R_S) \cong \begin{cases} \mathbb{Z}_2 \times \mathbb{Z}_2 \times (\mathbb{Z}_2)^h & \text{if } p = 2; \\ \mathbb{Z}_{p^2} \times (\mathbb{Z}_p)^h & \text{if } p \neq 2. \end{cases}$$

Proof. Now let

$$U(R_S) = U\left(R_S/J(R_S)\right) \cdot \left(\frac{1}{1} + J(R_S)\right) \cong \mathbb{Z}_{p-1} \times \left(\frac{1}{1} + J(R_S)\right).$$

The structure of $\frac{1}{1} + J(R_S)$. is obtained as follows:

$$J(R_S) = \left\{ \left[\frac{p\lambda + \lambda_1 u_1 + \cdots + \lambda_h u_h}{s} \right] \mid \lambda \in R', \lambda_i \in \mathbb{Z}_p, u_i \in R, 1 \leq i \leq h, s \in U(R) \right\}$$

and $(J(R_S))^3 = \left[\frac{0}{1}\right]$. Also $\mid J(R_S) \mid = p^{h+2}$ for some positive integer h such that $\mid U(R_S) \mid = p^{h+2}(p-1)$. But

$$\frac{1}{1} + J(R_S) = \left\{ \left[\frac{\alpha + p\lambda + \lambda_1 u_1 + \cdots + \lambda_h u_h}{s} \right] \mid s, \alpha \in U(R), \lambda \in R', \lambda_i \in \mathbb{Z}_p, u_i \in R, 1 \leq i \leq h \right\}$$

When $p = 2$.

We let $\psi \in R'$ such that $x^2 + x + \overline{\psi} = \overline{0}$ over R'/pR' has no solution in the field R'/pR' and $\overline{\psi} \in R'/pR'$, we obtain the following:

$$\left[\frac{1}{1} + \frac{4\lambda}{s}\right] \in \frac{1}{1} + ann(J(R_S)),$$

and

$$\left[\frac{1}{1} + \frac{4\psi}{s}\right], \left[\frac{1}{1} + \frac{\lambda_i u_i}{s}\right] \in \frac{1}{1} + J(R_S).$$

Now consider the element

$$\left[\frac{1}{1} + \frac{4\lambda}{s}\right],$$

then

$$\left(\left[\frac{1}{1} + \frac{4\lambda}{s}\right]\right)^2 = \left[\frac{1}{1} + 2\frac{4\lambda_1}{s}\right]$$

(since $16(mod 8) = 0$)

$$= \left[\frac{1}{1}\right]$$

(since char $R = 8$ and $\frac{8\lambda_1}{s} = \frac{0}{s}$).

So

$$\left[\frac{1}{1} + \frac{4\lambda_1}{s}\right]$$

generates a cyclic subgroup of $\frac{1}{1} + J(R_S)$ of order 2.

Next, consider the element

$$\left[\frac{1}{1} + \frac{4\psi}{s}\right] \in \frac{1}{1} + J(R_S),$$

then

$$\left(\left[\frac{1}{1} + \frac{4\psi}{s}\right]\right)^2 = \left[\frac{1}{1} + 2\frac{4\psi}{s}\right]$$

(since $16(mod 8) = 0$)

$$= \left[\frac{1}{1}\right]$$

(since char $R = 8$ and $\frac{8\psi}{s} = \frac{0}{s}$).

So

$$\left[\frac{1}{1} + \frac{4\psi}{s}\right]$$

generates a cyclic subgroup of $\frac{1}{1} + J(R_S)$ of order 2.

Next, consider the element

$$\left[\frac{1}{1} + \frac{\lambda_1 u_1}{s}\right] \in U(R_S).$$

Then

$$\left(\left[\frac{1}{1} + \frac{\lambda_1 u_1}{s}\right]\right)^2 = \left[\frac{1}{1} + 2\frac{\lambda_1 u_1}{s}\right]$$

(since $u_1^2 = 0$)

$$= \left[\frac{1}{1}\right]$$

(since char $R = 8$ and $2\frac{\lambda_1 u_1}{s} = \frac{0}{s}$).

So

$$\left[\frac{1}{1} + \frac{\lambda_1 u_1}{s}\right]$$

generates a cyclic subgroup of $U(R_S)$ of order 2.

Similarly, the element

$$\left[\frac{1}{1} + \frac{\lambda_2 u_2}{s}\right] \in U(R_S).$$

Then

$$\left(\left[\frac{1}{1} + \frac{\lambda_2 u_2}{s}\right]\right)^2 = \left[\frac{1}{1} + 2\frac{\lambda_2 u_2}{s}\right]$$

(since $u_2^2 = 0$)

$$= \left[\frac{1}{1}\right]$$

(since char $R = 8$ and $2\frac{\lambda_2 u_2}{s} = \frac{0}{s}$).

So

$$\left[\frac{1}{1} + \frac{\lambda_2 u_2}{s}\right]$$

generates a cyclic subgroup of $U(R_S)$ of order p.

Continuing inductively up to

$$\left[\frac{1}{1} + \frac{\lambda_h u_h}{s}\right],$$

we notice that the element also generates a cyclic subgroup of

$$\frac{1}{1} + J(R_S)$$

of order 2. Since

$$\frac{1}{1} + J(R_S)$$

is abelian, each cyclic subgroup is normal, the intersection of any pair of the cyclic subgroups is the identity group

$$\left[\frac{1}{1}\right]$$

and the order of the group generated by the direct product of the $h+2$ cyclic subgroups coincides with $\mid U(R_S) \mid$. Hence, the direct product exhausts $\frac{1}{1} + J(R_S)$.

Let $p \neq 2$

We show that $\frac{1}{1} + J(R_S)$ is isomorphic to a direct product of $h+1$ cyclic subgroups.

Consider, the element

$$\left[\frac{1}{1} + p\lambda\right],$$

then

$$\left(\left[\frac{1}{1} + p\lambda\right]\right)^{p^2} = \left[\frac{1}{1}\right].$$

Next, consider the elements

$$\left[\frac{1}{1} + \frac{\lambda_1 u_1}{s}\right], \left[\frac{1}{1} + \frac{\lambda_2 u_2}{s}\right], \ldots, \left[\frac{1}{1} + \frac{\lambda_h u_h}{s}\right]$$

where

$$\lambda_1, \ldots, \lambda_h \in U(\mathbb{Z}_p), u_1, \ldots, u_h \in R, s \in U(R).$$

We notice that each of the elements generates a cyclic subgroup of $\frac{1}{1} + J(R_S)$ of order p. Since $\frac{1}{1} + J(R_S)$ is abelian, each cyclic subgroup is normal.

Moreover, the order of the group generated by the direct product of the $h+1$ subgroups coincides with $\mid \frac{1}{1} + J(R_S) \mid$. So the direct product of the subgroups exhausts $\frac{1}{1} + J(R_S)$. $\square$

Proposition 40. *The structure of the unit group $U(R_S)$ of the total quotient ring constructed in Section 3.2 with characteristic $p^3, r \geq 1$ and $h \geq 1$ is as follows:*

$$\frac{1}{1}+J(R_S)\cong\begin{cases}\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_4^{r-1}\times(\mathbb{Z}_2^r)^h & \text{if } p=2;\\ \mathbb{Z}_{p^2}^r\times(\mathbb{Z}_p^r)^h & \text{if } p\neq 2.\end{cases}$$

and

$$U(R_S)\cong\begin{cases}\mathbb{Z}_{2^r-1}\times\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_4^{r-1}\times(\mathbb{Z}_2^r)^h & \text{if } p=2;\\ \mathbb{Z}_{p^r-1}\times\mathbb{Z}_{p^2}^r\times(\mathbb{Z}_p^r)^h & \text{if } p\neq 2.\end{cases}$$

Proof. Let $\lambda_1,\ldots,\lambda_r\in R'$ with $\lambda_1=1$ such that $\overline{\lambda_1},\ldots,\overline{\lambda_r}\in R'/pR'$ form a basis for R'/pR' regarded as a vector space over its prime subfield $\mathbb{F}_p$. Let $s_1,\ldots,s_h\in S=U(R_S)$. Now

$$U(R_S)=U\left(R_S/J(R_S)\right)\cdot\left(\frac{1}{1}+J(R_S)\right)\cong\mathbb{Z}_{p^r-1}\times\left(\frac{1}{1}+J(R_S)\right).$$

Since the two cases do not overlap, we consider them separately:

Let $p=2$

The structures of $\frac{1}{1}+J(R_S)$. are obtained as follows;

Suppose $l=1,\ldots,r,1\leq i\leq h$ and let $\psi\in R'$ such that

$$x^2+x+\overline{\psi}=\overline{0}$$

over R'/pR' has no solution in the field R'/pR' and $\overline{\psi}\in R'/pR'$, we obtain the following results:

$$\left(\left[\frac{1}{1}+\frac{4\lambda_1}{s}\right]\right)^2=\left[\frac{1}{1}\right],\left(\left[\frac{1}{1}+\frac{4\psi}{s}\right]\right)^2=\left[\frac{1}{1}\right].$$

Also

$$\left(\left[\frac{1}{1}+\frac{2\lambda_l}{s}\right]\right)^4=\left[\frac{1}{1}\right]$$

for $l=2,\ldots,r,\left(\left[\frac{1}{1}+\frac{\lambda_1u_1}{s}\right]\right)^2=\left[\frac{1}{1}\right],\left(\left[\frac{1}{1}+\frac{\lambda_2u_2}{s}\right]\right)^2=\left[\frac{1}{1}\right],\ldots,\left(\left[\frac{1}{1}+\frac{\lambda_hu_h}{s}\right]\right)^2=\left[\frac{1}{1}\right]$ for every $l=1,\ldots,r$. Now, consider positive integers $\alpha,\beta,\kappa_l,\tau_{1l},\ldots,\tau_{hl}$ with $\alpha\leq 2,\beta\leq 2,\kappa_l\leq 4,\tau_{il}\leq 2(1\leq i\leq h,1\leq l\leq r)$, we notice that the equation

$$\left(\left[\frac{1}{1}+\frac{4\lambda_1}{s}\right]\right)^{\alpha}\cdot\left(\left[\frac{1}{1}+\frac{4\psi}{s}\right]\right)^{\beta}\cdot\prod_{l=2}^{r}\left\{\left(\left[\frac{1}{1}+\frac{2\lambda_l}{s}\right]\right)^{\kappa_l}\right\}\cdot$$

$$\prod_{l=1}^{r}\left\{\left(\left[\frac{1}{1}+\frac{\lambda_lu_1}{s_1}\right]\right)^{\tau_{1l}}\right\}\cdot\prod_{l=1}^{r}\left\{\left(\left[\frac{1}{1}+\frac{\lambda_lu_2}{s_2}\right]\right)^{\tau_{2l}}\right\}\cdot$$

$$\cdots \prod_{l=1}^{r} \left\{ \left(\left[\frac{1}{1} + \frac{\lambda_l u_h}{s_h} \right] \right)^{\tau_{hl}} \right\} = \left\{ \frac{1}{1} \right\}$$

will imply $\alpha = \beta = 2, \kappa_l \leq 4$ for $l = 2, \ldots, r$ and $\tau_{il} = 2$ for every $l = 1, \ldots, r$ and $1 \leq i \leq h$.

If we set

$$H = \left\{ \left(\left[\frac{1}{1} + \frac{4\lambda_1}{s} \right] \right)^{\alpha} \mid \alpha = 1, 2 \right\}$$

$$G = \left\{ \left(\left[\frac{1}{1} + \frac{4\psi}{s} \right] \right)^{\alpha} \mid \beta = 1, 2 \right\}$$

$$T_l = \left\{ \left(\left[\frac{1}{1} + \frac{2\lambda_l}{s} \right] \right)^{\kappa} \mid \kappa = 1, \ldots, 4 \right\}; l = 2, \ldots, r$$

$$S_{1l} = \left\{ \left(\left[\frac{1}{1} + \frac{\lambda_l u_1}{s_1} \right] \right)^{\tau_1} \mid \tau_1 = 1, 2 \right\}$$

$$S_{2l} = \left\{ \left(\left[\frac{1}{1} + \frac{\lambda_l u_2}{s_2} \right] \right)^{\tau_2} \mid \tau_2 = 1, 2 \right\}$$

$$\vdots$$

$$S_{hl} = \left\{ \left(\left[\frac{1}{1} + \frac{\lambda_l u_h}{s_h} \right] \right)^{\tau_h} \mid \tau_h = 1, 2 \right\};$$

it is easily noticed that $H, G, T_l, S_{1l}, S_{2l}, \ldots, S_{hl}$ are cyclic subgroups of the group $\frac{1}{1} + J(R_S)$ and they are of the orders indicated in their definition. Since,

$$|< \left[\frac{1}{1} + \frac{4\lambda_1}{s} \right] >| \cdot |< \left[\frac{1}{1} + \frac{4\psi}{s} \right] >| \cdot \prod_{l=2}^{r} | \cdot < \left[\frac{1}{1} + \frac{2\lambda_l}{s} \right] >|$$

$$\cdot \prod_{l=1}^{r} | \cdot < \left[\frac{1}{1} + \frac{\lambda_l u_1}{s_1} \right] >| \cdot \prod_{l=1}^{r} |< \left[\frac{1}{1} + \frac{\lambda_l u_2}{s_2} \right] >| \cdot \cdots \cdot \prod_{l=1}^{r} |< \left[\frac{1}{1} + \frac{\lambda_l u_h}{s_h} \right] >| = p^{(h+k-1)r},$$

the intersection of any pair of the cyclic subgroups yields the identity group

$$\left\{ \left[\frac{1}{1} \right] \right\},$$

and the product of the $(h + k - 1)r$ subgroups $H, G, T_l, S_{1l}, S_{2l}, \ldots, S_{hl}$ is direct and exhausts the group $\frac{1}{1} + J(R_S)$.

Let $p \neq 2$

For $l = 1, \ldots, r$,

$$\left(\left[\frac{1}{1} + p\lambda_l\right]\right)^{p^2} = \left[\frac{1}{1}\right],$$
$$\left(\left[\frac{1}{1} + \frac{\lambda_l u_1}{s}\right]\right)^{p} = \left[\frac{1}{1}\right],$$
$$\vdots$$
$$\left(\left[\frac{1}{1} + \frac{\lambda_l u_h}{s}\right]\right)^{p} = \left[\frac{1}{1}\right].$$

For positive integers $\alpha_l, \beta_{1l}, \ldots, \beta_{hl}$ with $\alpha_l \leq p^2, \beta_{il} \leq p (1 \leq i \leq h)$, we notice that the equation

$$\prod_{l=1}^{r} \left\{ \left(\left[\frac{1}{1} + p\lambda_l\right] \right)^{\alpha_l} \right\} \cdot \prod_{l=1}^{r} \left\{ \left(\left[\frac{1}{1} + \frac{\lambda_l u_1}{s}\right] \right)^{\beta_{1l}} \right\} \cdot \ldots$$
$$\cdot \prod_{l=1}^{r} \left\{ \left(\left[\frac{1}{1} + \frac{\lambda_l u_h}{s}\right] \right)^{\beta_{hl}} \right\} = \left\{ \left[\frac{1}{1}\right] \right\}$$

will imply $\alpha_l = p^2, \beta_{il} = p (1 \leq i \leq h, l = 1, \ldots, r)$. If we set

$$T_l = \left\{ \left(\left[\frac{1}{1} + p\lambda_l\right] \right)^{\alpha} \mid \alpha = 1, \ldots, p^2 \right\}$$
$$S_{1l} = \left\{ \left(\left[\frac{1}{1} + \frac{\lambda_l u_1}{s}\right] \right)^{\alpha} \mid \alpha = 1, \ldots, p \right\}$$
$$\vdots$$
$$S_{hl} = \left\{ \left(\left[\frac{1}{1} + \frac{\lambda_l u_h}{s}\right] \right)^{\alpha} \mid \alpha = 1, \ldots, p \right\}$$

We see that $T_l, S_{1l}, \ldots, S_{hl}$ are all cyclic subgroups of $\frac{1}{1} + J(R_S)$ and they are of the orders indicated by their definitions. Since

$$\prod_{l=1}^{r} |< \left[\frac{1}{1} + p\lambda_l\right] >| \cdot \prod_{l=1}^{r} |< \left[\frac{1}{1} + \frac{\lambda_l u_1}{s}\right] >| \cdot \cdots \cdot \prod_{l=1}^{r} |< \left[\frac{1}{1} + \frac{\lambda_l u_h}{s}\right] >| = p^{(h+k-1)r}$$

and the intersection of any pair of the cyclic subgroups gives the identity group, the product of the $h + 1$ subgroups $T_l, S_{1l}, \ldots, S_{hl}$ is direct and the product exhausts the group $\frac{1}{1} + J(R_S)$. □

We now give the generalization as follows;

Proposition 41. *The structure of the unit group $U(R_S)$ of the total quotient ring constructed in section 3.2 with characteristic $p^k, k \geq 3, r = 1$ and $h \geq 1$ is as follows:*

$$\frac{1}{1} + J(R_S) \cong \begin{cases} \mathbb{Z}_2 \times \mathbb{Z}_{2^{k-2}} \times \mathbb{Z}_2^h & \text{if } p = 2; \\ \mathbb{Z}_{p^{k-1}} \times \mathbb{Z}_p^h & \text{if } p \neq 2. \end{cases}$$

and

$$U(R_S) \cong \begin{cases} \mathbb{Z}_2 \times \mathbb{Z}_{2^{k-2}} \times \mathbb{Z}_2^h & \text{if } p = 2; \\ \mathbb{Z}_{p-1} \times \mathbb{Z}_{p^{k-1}} \times \mathbb{Z}_p^h & \text{if } p \neq 2. \end{cases}$$

Proof. Now let

$$U(R_S) = U\left(R_S/J(R_S)\right) \cdot \left(\frac{1}{1} + J(R_S)\right) \cong \mathbb{Z}_{p-1} \times \left(\frac{1}{1} + J(R_S)\right).$$

The structure of $\frac{1}{1} + J(R_S)$. is obtained as follows; It can be shown that

$$J(R_S) = \left\{ \left[\frac{p\lambda + \lambda_1 u_1 + \cdots + \lambda_h u_h}{s} \right] \mid \lambda \in R', \lambda_i \in \mathbb{Z}_p, u_i \in R, 1 \leq i \leq h, s \in U(R) \right\}$$

and $(J(R_S))^k = \left[\frac{0}{1}\right]$. Also $\mid J(R_S) \mid = p^{h+k-1}$ for some positive integer h such that $\mid U(R_S) \mid = p^{h+k-1}(p-1)$. But

$$\frac{1}{1} + J(R_S) = \left\{ \left[\frac{\alpha + p\lambda + \lambda_1 u_1 + \cdots + \lambda_h u_h}{s} \right] \mid \lambda \in R', \alpha \in U(R), \lambda_i \in \mathbb{Z}_p, u_i \in R, 1 \leq i \leq h, s \in U(R) \right\}$$

When $p = 2$.

We let $\psi \in R'$ such that $x^2 + x + \overline{\psi} = \overline{0}$ over R'/pR' has no solution in the field R'/pR' and $\overline{\psi} \in R'/pR'$, we obtain the following:

$$\left[\frac{1}{1} + \frac{2^{k-1}\lambda}{s}\right] \in \frac{1}{1} + ann(J(R_S)),$$

$$\left[\frac{1}{1} + \frac{4\psi}{s}\right], \left[\frac{1}{1} + \frac{\lambda_i u_i}{s}\right] \in \frac{1}{1} + J(R_S).$$

Now consider the element

$$\left[\frac{1}{1} + \frac{2^{k-1}\lambda}{s}\right],$$

then

$$\left(\left[\frac{1}{1}+\frac{2^{k-1}\lambda}{s}\right]\right)^2=\left[\frac{1}{1}+2\frac{2^{k-1}\lambda}{s}\right]$$

(since $2^{2k-2}=0$)

$$=\left[\frac{1}{1}\right]$$

(since char $R=2^k$ and $\frac{2^k\lambda}{s}=\frac{0}{s}$).

So

$$\left[\frac{1}{1}+\frac{2^{k-1}\lambda}{s}\right]$$

generates a cyclic subgroup of $\frac{1}{1}+J(R_S)$ of order 2.

Next, consider the element

$$\left[\frac{1}{1}+\frac{4\psi}{s}\right]\in\frac{1}{1}+J(R_S),$$

then

$$\left(\left[\frac{1}{1}+\frac{4\psi}{s}\right]\right)^{2^{k-2}}=\left[\frac{1}{1}+2^{k-2}\frac{4\psi}{s}\right]$$

(since $2^k=0$)

$$=\left[\frac{1}{1}\right]$$

(since char $R=2^k$ and $2^{k-2}\frac{4\psi}{s}=\frac{0}{s}$).

So

$$\left[\frac{1}{1}+\frac{4\psi}{s}\right]$$

generates a cyclic subgroup of $\frac{1}{1}+J(R_S)$ of order 2^{k-2}.

Next, consider the element

$$\left[\frac{1}{1}+\frac{\lambda_1 u_1}{s}\right]\in U(R_S).$$

Then

$$\left(\left[\frac{1}{1}+\frac{\lambda_1 u_1}{s}\right]\right)^2=\left[\frac{1}{1}+2\frac{\lambda_1 u_1}{s}\right]$$

(since $u_1^2=0$)

$$=\left[\frac{1}{1}\right]$$

(since char $R=2^k$ and $2\frac{\lambda_1 u_1}{s}=\frac{0}{s}$).

So

$$\left[\frac{1}{1}+\frac{\lambda_1 u_1}{s}\right]$$

generates a cyclic subgroup of $U(R_S)$ of order 2.

Similarly, the element

$$\left[\frac{1}{1}+\frac{\lambda_2 u_2}{s}\right] \in U(R_S).$$

Then

$$\left(\left[\frac{1}{1}+\frac{\lambda_2 u_2}{s}\right]\right)^2 = \left[\frac{1}{1}+2\frac{\lambda_2 u_2}{s}\right]$$

(since $u_2^2 = 0$)

$$= \left[\frac{1}{1}\right]$$

(since char $R = 2^k$ and $2\frac{\lambda_2 u_2}{s} = \frac{0}{s}$).

So

$$\left[\frac{1}{1}+\frac{\lambda_2 u_2}{s}\right]$$

generates a cyclic subgroup of $U(R_S)$ of order 2.

Continuing inductively up to

$$\left[\frac{1}{1}+\frac{\lambda_h u_h}{s}\right],$$

we notice that the element also generates a cyclic subgroup of

$$\frac{1}{1}+J(R_S)$$

of order 2. Since

$$\frac{1}{1}+J(R_S)$$

is abelian, each cyclic subgroup is normal, the intersection of any pair of the cyclic subgroups is the identity group

$$\left[\frac{1}{1}\right]$$

and the order of the group generated by the direct product of the $h+2$ cyclic subgroups coincides with $\mid U(R_S) \mid$. Hence, the direct product exhausts $\frac{1}{1}+J(R_S)$.

Let $p \neq 2$

We show that $\frac{1}{1} + J(R_S)$ is isomorphic to a direct product of $h+1$ cyclic subgroups.

Consider, the element

$$\left[\frac{1}{1} + p\lambda\right],$$

then

$$\left(\left[\frac{1}{1} + p\lambda\right]\right)^{p^{k-1}} = \left[\frac{1}{1}\right].$$

Next, consider the elements

$$\left[\frac{1}{1} + \frac{\lambda_1 u_1}{s}\right], \left[\frac{1}{1} + \frac{\lambda_2 u_2}{s}\right], \ldots \left[\frac{1}{1} + \frac{\lambda_h u_h}{s}\right]$$

where

$$\lambda_1, \ldots, \lambda_h \in U(\mathbb{Z}_p), u_1, \ldots, u_h \in R, s \in U(R).$$

We notice that each of the elements generates a cyclic subgroup of $\frac{1}{1} + J(R_S)$ of order p. Since $\frac{1}{1} + J(R_S)$ is abelian, each cyclic subgroup is normal.

Moreover, the order of the group generated by the direct product of the $h+1$ subgroups coincides with $|\ \frac{1}{1} + J(R_S)\ |$. So the direct product of the subgroups exhausts $\frac{1}{1} + J(R_S)$.

□

Proposition 42. *The structure of the unit group $U(R_S)$ of the total quotient ring constructed in section 3.2 with characteristic $p^k, k \geq 3, r \geq 1$ and $h \geq 1$ is as follows:*

$$\frac{1}{1} + J(R_S) \cong \begin{cases} \mathbb{Z}_2 \times \mathbb{Z}_{2^{k-2}} \times \mathbb{Z}_{2^{k-1}}^{r-1} \times (\mathbb{Z}_2^r)^h & \text{if } p = 2; \\ \mathbb{Z}_{p^{k-1}}^r \times (\mathbb{Z}_p^r)^h & \text{if } p \neq 2. \end{cases}$$

and

$$U(R_S) \cong \begin{cases} \mathbb{Z}_{2^r-1} \times \mathbb{Z}_2 \times \mathbb{Z}_{2^{k-2}} \times \mathbb{Z}_{2^{k-1}}^{r-1} \times (\mathbb{Z}_2^r)^h & \text{if } p = 2; \\ \mathbb{Z}_{p^r-1} \times \mathbb{Z}_{p^{k-1}}^r \times (\mathbb{Z}_p^r)^h & \text{if } p \neq 2. \end{cases}$$

Proof. Let $\lambda_1, \ldots, \lambda_r \in R'$ with $\lambda_1 = 1$ such that $\overline{\lambda_1}, \ldots, \overline{\lambda_r} \in R'/pR'$ form a basis for R'/pR'

regarded as a vector space over its prime subfield $\mathbb{F}_p$. Let $s_1, \ldots, s_h \in S = U(R)$. Now

$$U(R_S) = U\left(R_S/J(R_S)\right) \cdot \left(\frac{1}{1} + J(R_S)\right) \cong \mathbb{Z}_{p^r-1} \times \left(\frac{1}{1} + J(R_S)\right).$$

Since the two cases do not overlap, we consider them separately:

Let $p = 2$

The structures of $\frac{1}{1} + J(R_S)$. are obtained as follows;

Suppose $l = 1, \ldots, r, 1 \leq i \leq h$ and let $\psi \in R'$ such that $x^2 + x + \overline{\psi} = \overline{0}$ over R'/pR' has no solution in the field R'/pR' and $\overline{\psi} \in R'/pR'$, we obtain the following results:

$$\left(\left[\frac{1}{1} + \frac{2^{k-1}\lambda_1}{s}\right]\right)^2 = \left[\frac{1}{1}\right],$$

$$\left(\left[\frac{1}{1} + \frac{4\psi}{s}\right]\right)^{2^{k-2}} = \left[\frac{1}{1}\right].$$

Also

$$\left(\left[\frac{1}{1} + \frac{2\lambda_l}{s}\right]\right)^{2^{k-1}} = \left[\frac{1}{1}\right]$$

for $l = 2, \ldots, r$,

$$\left(\left[\frac{1}{1} + \frac{\lambda_l u_1}{s}\right]\right)^2 = \left[\frac{1}{1}\right],$$

$$\left(\left[\frac{1}{1} + \frac{\lambda_l u_2}{s}\right]\right)^2 = \left[\frac{1}{1}\right],$$

$$\vdots$$

$$\left(\left[\frac{1}{1} + \frac{\lambda_l u_h}{s}\right]\right)^2 = \left[\frac{1}{1}\right]$$

for every $l = 1, \ldots, r$. Now, consider positive integers $\alpha, \beta, \kappa_l, \tau_{1l}, \ldots, \tau_{hl}$ with $\alpha \leq 2, \beta \leq 2^{k-2}, \kappa_l \leq 2^{k-1}, \tau_{il} \leq p (1 \leq i \leq h, 1 \leq l \leq r)$, we notice that the equation

$$\left(\left[\frac{1}{1} + \frac{2^{k-1}\lambda_1}{s}\right]\right)^{\alpha} \cdot \left(\left[\frac{1}{1} + \frac{4\psi}{s}\right]\right)^{\beta} \cdot \prod_{l=2}^{r} \left\{\left(\left[\frac{1}{1} + \frac{2\lambda_l}{s}\right]\right)^{\kappa_l}\right\} \cdot$$

$$\prod_{l=1}^{r} \left\{\left(\left[\frac{1}{1} + \frac{\lambda_l u_1}{s}\right]\right)^{\tau_{1l}}\right\} \cdot \prod_{l=1}^{r} \left\{\left(\left[\frac{1}{1} + \frac{\lambda_l u_2}{s}\right]\right)^{\tau_{2l}}\right\} \cdot$$

$$\cdots \prod_{l=1}^{r} \left\{\left(\left[\frac{1}{1} + \frac{\lambda_l u_h}{s}\right]\right)^{\tau_{hl}}\right\} = \left\{\left[\frac{1}{1}\right]\right\}$$

will imply $\alpha = 2, \beta = 2^{k-2}, \kappa_l \leq 2^{k-1}$ for $l = 2, \ldots, r$ and $\tau_{il} = 2$ for every $l = 1, \ldots, r$ and $1 \leq i \leq h$.

If we set

$$H = \left\{ \left(\left[\frac{1}{1} + \frac{2^{k-1}\lambda_1}{s} \right] \right)^{\alpha} \mid \alpha = 1, 2 \right\}$$

$$G = \left\{ \left(\left[\frac{1}{1} + \frac{4\psi}{s} \right] \right)^{\alpha} \mid \beta = 1, \ldots, 2^{k-2} \right\}$$

$$T_l = \left\{ \left(\left[\frac{1}{1} + \frac{2\lambda_l}{s} \right] \right)^{\kappa} \mid \kappa = 1, \ldots, 2^{k-1} \right\}; l = 2, \ldots, r$$

$$S_{1l} = \left\{ \left(\left[\frac{1}{1} + \frac{\lambda_l u_1}{s} \right] \right)^{\tau_1} \mid \tau_1 = 1, 2 \right\}$$

$$S_{2l} = \left\{ \left(\left[\frac{1}{1} + \frac{\lambda_l u_2}{s} \right] \right)^{\tau_2} \mid \tau_2 = 1, 2 \right\}$$

$$\vdots$$

$$S_{hl} = \left\{ \left(\left[\frac{1}{1} + \frac{\lambda_l u_h}{s} \right] \right)^{\tau_h} \mid \tau_h = 1, 2 \right\};$$

it is noticed that $H, G, T_l, S_{1l}, S_{2l}, \ldots, S_{hl}$ are cyclic subgroups of the group $\frac{1}{1} + J(R_S)$ and they are of the orders indicated in their definition. Since,

$$|< \left[\frac{1}{1} + \frac{2^{k-1}\lambda_1}{s} \right] >| \cdot |< \left[\frac{1}{1} + \frac{4\psi}{s} \right] >| \cdot \prod_{l=2}^{r} | \cdot < \left[\frac{1}{1} + \frac{2\lambda_l}{s} \right] >|$$

$$\cdot \prod_{l=1}^{r} | \cdot < \left[\frac{1}{1} + \frac{\lambda_l u_1}{s} \right] >| \cdot \prod_{l=1}^{r} |< \left[\frac{1}{1} + \frac{\lambda_l u_2}{s} \right] >| \cdot \ldots$$

$$\cdot \prod_{l=1}^{r} |< \left[\frac{1}{1} + \frac{\lambda_l u_h}{s} \right] >| = p^{(h+k-1)r},$$

the intersection of any pair of the cyclic subgroups yields the identity group $\left[\frac{1}{1}\right]$, and the product of the $h+3$ subgroups $H, G, T_l, S_{1l}, S_{2l}, \ldots, S_{hl}$ is direct and exhausts the group $\frac{1}{1} + J(R_S)$.

Let $p \neq 2$

For $l = 1, \ldots, r$,

$$\left(\left[\frac{1}{1} + p\lambda_l \right] \right)^{p^{k-1}} = \left[\frac{1}{1} \right],$$

$$\left(\left[\frac{1}{1} + \frac{\lambda_1 u_1}{s} \right] \right)^{p} = \left[\frac{1}{1} \right],$$

$$\vdots$$

$$\left(\left[\frac{1}{1}+\frac{\lambda_h u_h}{s}\right]\right)^p=\left[\frac{1}{1}\right].$$

For positive integers $\alpha_l,\beta_{1l},\ldots,\beta_{hl}$ with $\alpha_l\leq p^{k-1},\beta_{il}\leq p(1\leq i\leq h)$, we notice that the equation

$$\prod_{l=1}^{r}\left\{\left(\left[\frac{1}{1}+p\lambda_l\right]\right)^{\alpha_l}\right\}\cdot\prod_{l=1}^{r}\left\{\left(\left[\frac{1}{1}+\frac{\lambda_1 u_1}{s}\right]\right)^{\beta_{1l}}\right\}\cdot$$

$$\cdots\cdot\prod_{l=1}^{r}\left\{\left(\left[\frac{1}{1}+\frac{\lambda_h u_h}{s}\right]\right)^{\beta_{hl}}\right\}=\left\{\left[\frac{1}{1}\right]\right\}$$

will imply $\alpha_l=p^{k-1},\beta_{il}=p(1\leq i\leq h,l=1,\ldots,r)$. If we set

$$T_l=\left\{\left(\left[\frac{1}{1}+p\lambda_l\right]\right)^{\alpha}\mid\alpha=1,\ldots,p^{k-1}\right\}$$

$$S_{1l}=\left\{\left(\left[\frac{1}{1}+\frac{\lambda_1 u_1}{s}\right]\right)^{\alpha}\mid\alpha=1,\ldots,p^{k-1}\right\}$$

$$\vdots$$

$$S_{hl}=\left\{\left(\left[\frac{1}{1}+\frac{\lambda_h u_h}{s}\right]\right)^{\alpha}\mid\alpha=1,\ldots,p^{k-1}\right\}$$

We see that $T_l,S_{1l},\ldots,S_{hl}$ are all cyclic subgroups of $\frac{1}{1}+J(R_S)$ and they are of the orders indicated by their definitions. Since

$$\prod_{l=1}^{r}|<\left[\frac{1}{1}+p\lambda_l\right]>|\cdot\prod_{l=1}^{r}|<\left[\frac{1}{1}+\frac{\lambda_1 u_1}{s}\right]>|\cdot\cdots\cdot\prod_{l=1}^{r}|<\left[\frac{1}{1}+\frac{\lambda_h u_h}{s}\right]>|=p^{(h+k-1)r}$$

and the intersection of any pair of the cyclic subgroups gives the identity group, the product of the $(h+1)r$ subgroups $T_l,S_{1l},\ldots,S_{hl}$ is direct and the product exhausts the group $\frac{1}{1}+J(R_S)$.

□

Example 5. $R=\mathbb{Z}_8\oplus\underbrace{GF(2)\oplus\cdots\oplus GF(2)}_{h},J(R_S)=2\mathbb{Z}_8\oplus\underbrace{GF(2)\oplus\cdots\oplus GF(2)}_{h},S=1+2\mathbb{Z}_8\oplus\underbrace{GF(2)\oplus\cdots\oplus GF(2)}_{h}$ *and* $S^{-1}R=(1+2\mathbb{Z}_8\oplus\underbrace{GF(2)\oplus\cdots\oplus GF(2)}_{h})^{-1}(\mathbb{Z}_8\oplus\underbrace{GF(2)\oplus\cdots\oplus GF(2)}_{h})$.

The above construction gives the following equivalence classes

$$R_S = \left\{ \left[\frac{(0,0,0,\ldots,0)}{(1,0,\ldots,0)}\right], \left[\frac{(0,1,0,\ldots,0)}{(1,0,\ldots,0)}\right], \ldots, \left[\frac{(0,0,\ldots,0,1)}{(1,0,\ldots,0)}\right], \right.$$
$$\left[\frac{(1,0,0,\ldots,0)}{(1,0,\ldots,0)}\right], \left[\frac{(1,1,0,\ldots,0)}{(1,0,\ldots,0)}\right], \ldots, \left[\frac{(1,0,\ldots,0,1)}{(1,0,\ldots,0)}\right],$$
$$\left[\frac{(2,0,0,\ldots,0)}{(1,0,\ldots,0)}\right], \left[\frac{(2,1,0,\ldots,0)}{(1,0,\ldots,0)}\right], \ldots, \left[\frac{(2,0,\ldots,0,1)}{(1,0,\ldots,0)}\right],$$
$$\left[\frac{(3,0,0,\ldots,0)}{(1,0,\ldots,0)}\right], \left[\frac{(3,1,0,\ldots,0)}{(1,0,\ldots,0)}\right], \ldots, \left[\frac{(3,0,\ldots,0,1)}{(1,0,\ldots,0)}\right],$$
$$\left[\frac{(4,0,0,\ldots,0)}{(1,0,\ldots,0)}\right], \left[\frac{(4,1,0,\ldots,0)}{(1,0,\ldots,0)}\right], \ldots, \left[\frac{(4,0,\ldots,0,1)}{(1,0,\ldots,0)}\right],$$
$$\left[\frac{(5,0,0,\ldots,0)}{(1,0,\ldots,0)}\right], \left[\frac{(5,1,0,\ldots,0)}{(1,0,\ldots,0)}\right], \ldots, \left[\frac{(5,0,\ldots,0,1)}{(1,0,\ldots,0)}\right],$$
$$\left[\frac{(6,0,0,\ldots,0)}{(1,0,\ldots,0)}\right], \left[\frac{(6,1,0,\ldots,0)}{(1,0,\ldots,0)}\right], \ldots, \left[\frac{(6,0,\ldots,0,1)}{(1,0,\ldots,0)}\right],$$
$$\left.\left[\frac{(7,0,0,\ldots,0)}{(1,0,\ldots,0)}\right], \left[\frac{(7,1,0,\ldots,0)}{(1,0,\ldots,0)}\right], \ldots, \left[\frac{(7,0,\ldots,0,1)}{(1,0,\ldots,0)}\right] \right\}.$$

Now, we have

$$J(R_S) = \left\{ \left[\frac{(0,0,0,\ldots,0)}{(1,0,\ldots,0)}\right], \left[\frac{(0,1,0,\ldots,0)}{(1,0,\ldots,0)}\right], \ldots, \left[\frac{(0,0,\ldots,0,1)}{(1,0,\ldots,0)}\right], \right.$$
$$\left[\frac{(2,0,0,\ldots,0)}{(1,0,\ldots,0)}\right], \left[\frac{(2,1,0,\ldots,0)}{(1,0,\ldots,0)}\right], \ldots, \left[\frac{(2,0,\ldots,0,1)}{(1,0,\ldots,0)}\right],$$
$$\left[\frac{(4,0,0,\ldots,0)}{(1,0,\ldots,0)}\right], \left[\frac{(4,1,0,\ldots,0)}{(1,0,\ldots,0)}\right], \ldots, \left[\frac{(4,0,\ldots,0,1)}{(1,0,\ldots,0)}\right],$$
$$\left.\left[\frac{(6,0,0,\ldots,0)}{(1,0,\ldots,0)}\right], \left[\frac{(6,1,0,\ldots,0)}{(1,0,\ldots,0)}\right], \ldots, \left[\frac{(6,0,\ldots,0,1)}{(1,0,\ldots,0)}\right] \right\}$$

and

$$\frac{(1,0,\ldots,0)}{(1,0,\ldots,0)} + J(R_S) = \left\{ \left[\frac{(1,0,0,\ldots,0)}{(1,0,\ldots,0)}\right], \left[\frac{(1,1,0,\ldots,0)}{(1,0,\ldots,0)}\right], \ldots, \left[\frac{(1,0,\ldots,0,1)}{(1,0,\ldots,0)}\right], \right.$$
$$\left[\frac{(3,0,0,\ldots,0)}{(1,0,\ldots,0)}\right], \left[\frac{(3,1,0,\ldots,0)}{(1,0,\ldots,0)}\right], \ldots, \left[\frac{(3,0,\ldots,0,1)}{(1,0,\ldots,0)}\right],$$
$$\left[\frac{(5,0,0,\ldots,0)}{(1,0,\ldots,0)}\right], \left[\frac{(5,1,0,\ldots,0)}{(1,0,\ldots,0)}\right], \ldots, \left[\frac{(5,0,\ldots,0,1)}{(1,0,\ldots,0)}\right],$$
$$\left.\left[\frac{(7,0,0,\ldots,0)}{(1,0,\ldots,0)}\right], \left[\frac{(7,1,0,\ldots,0)}{(1,0,\ldots,0)}\right], \ldots, \left[\frac{(7,0,\ldots,0,1)}{(1,0,\ldots,0)}\right] \right\}$$

The generators of the group $\frac{(1,0,\ldots,0)}{(1,0,\ldots,0)} + J(R_S)$ *are*

$$\left[\frac{(3,0,0,\ldots,0)}{(1,0,0,\ldots,0)}\right],$$

$$\left[\frac{(5,0,0,\ldots,0)}{(1,0,0,\ldots,0)}\right],$$

$$\left[\frac{(1,1,0,\ldots,0)}{(1,0,0,\ldots,0)}\right],$$

$$\vdots$$

$$\left[\frac{(1,0,\ldots,0,1)}{(1,0,\ldots,0,0)}\right],$$

we verify this as follows:

$$\left(\left[\frac{(3,0,0,\ldots,0)}{(1,0,0,\ldots,0)}\right]\right)^2 = \left[\frac{(1,0,0,\ldots,0)}{(1,0,0,\ldots,0)}\right]$$

$$\left(\left[\frac{(5,0,0,\ldots,0)}{(1,0,0,\ldots,0)}\right]\right)^2 = \left[\frac{(1,0,0,\ldots,0)}{(1,0,0,\ldots,0)}\right]$$

$$\left(\left[\frac{(1,1,0,\ldots,0)}{(1,0,0,\ldots,0)}\right]\right)^2 = \left[\frac{(1,0,0,\ldots,0)}{(1,0,0,\ldots,0)}\right]$$

$$\vdots$$

$$\left(\left[\frac{(1,0,\ldots,0,1)}{(1,0,\ldots,0,0)}\right]\right)^2 = \left[\frac{(1,0,\ldots,0,0)}{(1,0,\ldots,0,0)}\right]$$

We see that each of the $h+2$ *elements*

$$\left[\frac{(3,0,0,\ldots,0)}{(1,0,0,\ldots,0)}\right],$$

$$\left[\frac{(5,0,0,\ldots,0)}{(1,0,0,\ldots,0)}\right],$$

$$\left[\frac{(1,1,0,\ldots,0)}{(1,0,0,\ldots,0)}\right],$$

$$\vdots$$

$$\left[\frac{(1,0,\ldots,0,1)}{(1,0,\ldots,0,0)}\right]$$

is of order 2, *thus*

$$< \left(\left[\frac{(3,0,\ldots,0)}{(1,0,\ldots,0)} \right] \right) > \cong \mathbb{Z}_2,$$
$$< \left(\left[\frac{(5,0,\ldots,0)}{(1,0,\ldots,0)} \right] \right) > \cong \mathbb{Z}_2,$$

$$< \left(\left[\frac{(1,1,0,\ldots,0)}{(1,0,0,\ldots,0)} \right] \right) > \cong \mathbb{Z}_2$$

$$\vdots$$

$$< \left(\left[\frac{(1,0,\ldots,0,1)}{(1,0,\ldots,0,0)} \right] \right) > \cong \mathbb{Z}_2$$

Therefore taking the product of all the generators we have

$$< \left(\left[\frac{(3,0,\ldots,0)}{(1,0,\ldots,0)} \right] \right) > \cdot < \left(\left[\frac{(5,0,\ldots,0)}{(1,0,\ldots,0)} \right] \right) > \cdot < \left(\left[\frac{(1,1,0,\ldots,0)}{(1,0,0,\ldots,0)} \right] \right) >$$

$$\cdots\cdots < \left(\left[\frac{(1,0,\ldots,0,1)}{(1,0,\ldots,0,0)} \right] \right) > \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \underbrace{\mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2}_{h} = \mathbb{Z}_2 \times \mathbb{Z}_2 \times (\mathbb{Z}_2)^h$$

Case (ii) When $p \neq 2$

For $p = 3$, *we have the following equivalence classes*

$$R_S = \left\{ \left[\frac{(0,0,0,\ldots,0)}{(1,0,\ldots,0)} \right], \left[\frac{(0,1,0,\ldots,0)}{(1,0,\ldots,0)} \right], \ldots, \left[\frac{(0,0,\ldots,0,1)}{(1,0,\ldots,0)} \right], \left[\frac{(0,2,0,\ldots,0)}{(1,0,\ldots,0)} \right], \ldots, \left[\frac{(0,0,\ldots,0,2)}{(1,0,\ldots,0)} \right] \right.$$

$$\left[\frac{(1,0,0,\ldots,0)}{(1,0,\ldots,0)} \right], \left[\frac{(1,1,0,\ldots,0)}{(1,0,\ldots,0)} \right], \ldots, \left[\frac{(1,0,\ldots,0,1)}{(1,0,\ldots,0)} \right], \left[\frac{(1,2,0,\ldots,0)}{(1,0,\ldots,0)} \right], \ldots, \left[\frac{(1,0,\ldots,0,2)}{(1,0,\ldots,0)} \right],$$

$$\left[\frac{(2,0,0,\ldots,0)}{(1,0,\ldots,0)} \right], \left[\frac{(2,1,0,\ldots,0)}{(1,0,\ldots,0)} \right], \ldots, \left[\frac{(2,0,\ldots,0,1)}{(1,0,\ldots,0)} \right], \left[\frac{(2,2,0,\ldots,0)}{(1,0,\ldots,0)} \right], \ldots, \left[\frac{(2,0,\ldots,0,2)}{(1,0,\ldots,0)} \right],$$

$$\left[\frac{(3,0,0,\ldots,0)}{(1,0,\ldots,0)} \right], \left[\frac{(3,1,0,\ldots,0)}{(1,0,\ldots,0)} \right], \ldots, \left[\frac{(3,0,\ldots,0,1)}{(1,0,\ldots,0)} \right], \left[\frac{(3,2,0,\ldots,0)}{(1,0,\ldots,0)} \right], \ldots, \left[\frac{(3,0,\ldots,0,2)}{(1,0,\ldots,0)} \right],$$

$$\left[\frac{(4,0,0,\ldots,0)}{(1,0,\ldots,0)} \right], \left[\frac{(4,1,0,\ldots,0)}{(1,0,\ldots,0)} \right], \ldots, \left[\frac{(4,0,\ldots,0,1)}{(1,0,\ldots,0)} \right], \left[\frac{(4,2,0,\ldots,0)}{(1,0,\ldots,0)} \right], \ldots, \left[\frac{(4,0,\ldots,0,2)}{(1,0,\ldots,0)} \right],$$

$$\left[\frac{(5,0,0,\ldots,0)}{(1,0,\ldots,0)} \right], \left[\frac{(5,1,0,\ldots,0)}{(1,0,\ldots,0)} \right], \ldots, \left[\frac{(5,0,\ldots,0,1)}{(1,0,\ldots,0)} \right], \left[\frac{(5,2,0,\ldots,0)}{(1,0,\ldots,0)} \right], \ldots, \left[\frac{(5,0,\ldots,0,2)}{(1,0,\ldots,0)} \right],$$

$$\left[\frac{(6,0,0,\ldots,0)}{(1,0,\ldots,0)} \right], \left[\frac{(6,1,0,\ldots,0)}{(1,0,\ldots,0)} \right], \ldots, \left[\frac{(6,0,\ldots,0,1)}{(1,0,\ldots,0)} \right], \left[\frac{(6,2,0,\ldots,0)}{(1,0,\ldots,0)} \right], \ldots, \left[\frac{(6,0,\ldots,0,2)}{(1,0,\ldots,0)} \right],$$

$$\left[\frac{(7,0,0,\ldots,0)}{(1,0,\ldots,0)} \right], \left[\frac{(7,1,0,\ldots,0)}{(1,0,\ldots,0)} \right], \ldots, \left[\frac{(7,0,\ldots,0,1)}{(1,0,\ldots,0)} \right], \left[\frac{(7,2,0,\ldots,0)}{(1,0,\ldots,0)} \right], \ldots, \left[\frac{(7,0,\ldots,0,2)}{(1,0,\ldots,0)} \right],$$

$$\left[\frac{(8,0,0,\ldots,0)}{(1,0,\ldots,0)}\right],\left[\frac{(8,1,0,\ldots,0)}{(1,0,\ldots,0)}\right],\ldots,\left[\frac{(8,0,\ldots,0,1)}{(1,0,\ldots,0)}\right],\left[\frac{(8,2,0,\ldots,0)}{(1,0,\ldots,0)}\right],\ldots,\left[\frac{(8,0,\ldots,0,2)}{(1,0,\ldots,0)}\right],$$

$$\vdots$$

$$\left[\frac{(26,0,0,\ldots,0)}{(1,0,\ldots,0)}\right],\left[\frac{(26,1,0,\ldots,0)}{(1,0,\ldots,0)}\right],\ldots,\left[\frac{(26,0,\ldots,0,1)}{(1,0,\ldots,0)}\right],$$
$$\left[\frac{(26,2,0,\ldots,0)}{(1,0,\ldots,0)}\right],\ldots,\left[\frac{(26,0,\ldots,0,2)}{(1,0,\ldots,0)}\right]\Bigg\}.$$

We now have

$$J(R_S)=\Bigg\{\left[\frac{(0,0,0,\ldots,0)}{(1,0,\ldots,0)}\right],\left[\frac{(0,1,0,\ldots,0)}{(1,0,\ldots,0)}\right],\ldots,\left[\frac{(0,0,\ldots,0,1)}{(1,0,\ldots,0)}\right],\left[\frac{(0,2,0,\ldots,0)}{(1,0,\ldots,0)}\right],\ldots,$$

$$\left[\frac{(0,0,\ldots,0,2)}{(1,0,\ldots,0)}\right],\left[\frac{(3,0,0,\ldots,0)}{(1,0,\ldots,0)}\right],\left[\frac{(3,1,0,\ldots,0)}{(1,0,\ldots,0)}\right],\ldots,\left[\frac{(3,0,\ldots,0,1)}{(1,0,\ldots,0)}\right],\left[\frac{(3,2,0,\ldots,0)}{(1,0,\ldots,0)}\right],\ldots,$$
$$\left[\frac{(3,0,\ldots,0,2)}{(1,0,\ldots,0)}\right],\left[\frac{(6,0,0,\ldots,0)}{(1,0,\ldots,0)}\right],\left[\frac{(6,1,0,\ldots,0)}{(1,0,\ldots,0)}\right],\ldots,$$
$$\left[\frac{(6,0,\ldots,0,1)}{(1,0,\ldots,0)}\right],\left[\frac{(6,2,0,\ldots,0)}{(1,0,\ldots,0)}\right],\ldots,\left[\frac{(6,0,\ldots,0,2)}{(1,0,\ldots,0)}\right],$$

$$\vdots$$

$$\left[\frac{(24,0,0,\ldots,0)}{(1,0,\ldots,0)}\right],\left[\frac{(24,1,0,\ldots,0)}{(1,0,\ldots,0)}\right],\ldots,\left[\frac{(24,0,\ldots,0,1)}{(1,0,\ldots,0)}\right],\left[\frac{(24,2,0,\ldots,0)}{(1,0,\ldots,0)}\right],\ldots,$$
$$\left[\frac{(24,0,\ldots,0,2)}{(1,0,\ldots,0)}\right]\Bigg\}$$

and

$$\frac{(1,0,\ldots,0)}{(1,0,\ldots,0)}+J(R_S)=\Bigg\{\left[\frac{(1,0,0,\ldots,0)}{(1,0,\ldots,0)}\right],\left[\frac{(1,1,0,\ldots,0)}{(1,0,\ldots,0)}\right],\ldots,\left[\frac{(1,0,\ldots,0,1)}{(1,0,\ldots,0,0)}\right],$$

$$\left[\frac{(1,2,0,\ldots,0)}{(1,0,\ldots,0)}\right],\ldots\left[\frac{(1,0,\ldots,0,2)}{(1,0,\ldots,0)}\right],$$
$$\left[\frac{(4,0,0,\ldots,0)}{(1,0,\ldots,0)}\right],\left[\frac{(4,1,0,\ldots,0)}{(1,0,\ldots,0)}\right],\ldots,\left[\frac{(4,0,\ldots,0,1)}{(1,0,\ldots,0)}\right],\left[\frac{(4,2,0,\ldots,0)}{(1,0,\ldots,0)}\right],\ldots,\left[\frac{(4,0,\ldots,0,2)}{(1,0,\ldots,0)}\right],$$
$$\left[\frac{(7,0,0,\ldots,0)}{(1,0,\ldots,0)}\right],\left[\frac{(7,1,0,\ldots,0)}{(1,0,\ldots,0)}\right],\ldots,\left[\frac{(7,0,\ldots,0,1)}{(1,0,\ldots,0)}\right],\left[\frac{(7,2,0,\ldots,0)}{(1,0,\ldots,0)}\right],\ldots,\left[\frac{(7,0,\ldots,0,2)}{(1,0,\ldots,0)}\right],$$

$$\vdots$$

$$\left[\frac{(25,0,0,\ldots,0)}{(1,0,\ldots,0)}\right],\left[\frac{(25,1,0,\ldots,0)}{(1,0,\ldots,0)}\right],\ldots,\left[\frac{(25,0,\ldots,0,1)}{(1,0,\ldots,0)}\right],$$

$$\left[\frac{(25,2,0,\ldots,0)}{(1,0,\ldots,0)}\right],\ldots,\left[\frac{(25,0,\ldots,0,2)}{(1,0,\ldots,0)}\right]\Bigg\}.$$

Through inspection we have the generators as

$$\left[\frac{(16,0,0,\ldots,0)}{(1,0,\ldots,0)}\right],\left[\frac{(1,1,0,\ldots,0)}{(1,0,\ldots,0)}\right],\ldots,\left[\frac{(1,0,\ldots,0,1)}{(1,0,\ldots,0)}\right].$$

This can be verified as follows:

$$\left(\left[\frac{(16,0,0,\ldots,0)}{(1,0,\ldots,0)}\right]\right)^2=\left(\left[\frac{(13,0,0,\ldots,0)}{(1,0,\ldots,0)}\right]\right)$$

$$\left(\left[\frac{(16,0,0,\ldots,0)}{(1,0,\ldots,0)}\right]\right)^3=\left(\left[\frac{(13,0,0,\ldots,0)}{(1,0,\ldots,0)}\right]\right)\cdot\left(\left[\frac{(16,0,0,\ldots,0)}{(1,0,\ldots,0)}\right]\right)=\left(\left[\frac{(19,0,0,\ldots,0)}{(1,0,\ldots,0)}\right]\right),$$

$$\left(\left[\frac{(16,0,0,\ldots,0)}{(1,0,\ldots,0)}\right]\right)^4=\left(\left[\frac{(19,0,0,\ldots,0)}{(1,0,\ldots,0)}\right]\right)\cdot\left(\left[\frac{(16,0,0,\ldots,0)}{(1,0,\ldots,0)}\right]\right)=\left(\left[\frac{(7,0,0,\ldots,0)}{(1,0,\ldots,0)}\right]\right),$$

$$\left(\left[\frac{(16,0,0,\ldots,0)}{(1,0,\ldots,0)}\right]\right)^5=\left(\left[\frac{(7,0,0,\ldots,0)}{(1,0,\ldots,0)}\right]\right)\cdot\left(\left[\frac{(16,0,0,\ldots,0)}{(1,0,\ldots,0)}\right]\right)=\left(\left[\frac{(4,0,0,\ldots,0)}{(1,0,\ldots,0)}\right]\right),$$

$$\left(\left[\frac{(16,0,0,\ldots,0)}{(1,0,\ldots,0)}\right]\right)^6=\left(\left[\frac{(4,0,0,\ldots,0)}{(1,0,\ldots,0)}\right]\right)\cdot\left(\left[\frac{(16,0,0,\ldots,0)}{(1,0,\ldots,0)}\right]\right)=\left(\left[\frac{(10,0,0,\ldots,0)}{(1,0,\ldots,0)}\right]\right),$$

$$\left(\left[\frac{(16,0,0,\ldots,0)}{(1,0,\ldots,0)}\right]\right)^7=\left(\left[\frac{(10,0,0,\ldots,0)}{(1,0,\ldots,0)}\right]\right)\cdot\left(\left[\frac{(16,0,0,\ldots,0)}{(1,0,\ldots,0)}\right]\right)=\left(\left[\frac{(25,0,0,\ldots,0)}{(1,0,\ldots,0)}\right]\right),$$

$$\left(\left[\frac{(16,0,0,\ldots,0)}{(1,0,\ldots,0)}\right]\right)^8=\left(\left[\frac{(25,0,0,\ldots,0)}{(1,0,\ldots,0)}\right]\right)\cdot\left(\left[\frac{(16,0,0,\ldots,0)}{(1,0,\ldots,0)}\right]\right)=\left(\left[\frac{(22,0,0,\ldots,0)}{(1,0,\ldots,0)}\right]\right),$$

$$\left(\left[\frac{(16,0,0,\ldots,0)}{(1,0,\ldots,0)}\right]\right)^9=\left(\left[\frac{(22,0,0,\ldots,0)}{(1,0,\ldots,0)}\right]\right)\cdot\left(\left[\frac{(16,0,0,\ldots,0)}{(1,0,\ldots,0)}\right]\right)=\left(\left[\frac{(1,0,0,\ldots,0)}{(1,0,\ldots,0)}\right]\right),$$

$$\left(\left[\frac{(1,1,0,\ldots,0)}{(1,0,\ldots,0)}\right]\right)^2=\left[\frac{(1,2,0,\ldots,0)}{(1,0,\ldots,0)}\right]$$

$$\left(\left[\frac{(1,1,0,\ldots,0)}{(1,0,\ldots,0)}\right]\right)^3=\left[\frac{(1,2,0,\ldots,0)}{(1,0,\ldots,0)}\right]\cdot\left[\frac{(1,1,0,\ldots,0)}{(1,0,\ldots,0)}\right]=\left[\frac{(1,0,0,\ldots,0)}{(1,0,\ldots,0)}\right]$$

$$\vdots$$

$$\left(\left[\frac{(1,0,\ldots,0,1)}{(1,0,\ldots,0,0)}\right]\right)^2=\left[\frac{(1,0,\ldots,0,2)}{(1,0,\ldots,0,0)}\right]$$

$$\left(\left[\frac{(1,0,\ldots,0,1)}{(1,0,\ldots,0,0)}\right]\right)^3=\left[\frac{(1,0,\ldots,0,2)}{(1,0,\ldots,0,0)}\right]\cdot\left[\frac{(1,0,\ldots,0,1)}{(1,0,\ldots,0,0)}\right]=\left[\frac{(1,0,\ldots,0,0)}{(1,0,\ldots,0,0)}\right].$$

We see that the $h+1$ *elements*

$$\left[\frac{(16,0,0,\ldots,0)}{(1,0,\ldots,0)}\right]$$

of order 9 *and*

$$\left[\frac{(1,1,0,\ldots,0)}{(1,0,\ldots,0)}\right],$$

$$\vdots$$

$$\left[\frac{(1,0,\ldots,0,1)}{(1,0,\ldots,0,0)}\right]$$

each of order 3 *generate the group* $\frac{(1,0,\ldots,0)}{(1,0,\ldots,0)} + J(R_S)$.

Thus

$$< \left(\left[\frac{(16,0,0,\ldots,0)}{(1,0,\ldots,0)}\right]\right) > \cong \mathbb{Z}_9$$

$$< \left(\left[\frac{(1,1,0,\ldots,0)}{(1,0,\ldots,0)}\right]\right) > \cong \mathbb{Z}_3$$

$$\vdots$$

$$< \left(\left[\frac{(1,0,\ldots,0,1)}{(1,0,\ldots,0,0)}\right]\right) > \cong \mathbb{Z}_3.$$

Taking the product of all the cyclic groups we obtain the following

$$< \left(\left[\frac{(16,0,0,\ldots,0)}{(1,0,\ldots,0)}\right]\right) > \cdot < \left(\left[\frac{(1,1,0,\ldots,0)}{(1,0,\ldots,0)}\right]\right) > \cdot \ldots$$

$$\cdot < \left(\left[\frac{(1,0,\ldots,0,1)}{(1,0,\ldots,0,0)}\right]\right) > \cong \mathbb{Z}_9 \times \underbrace{\mathbb{Z}_3 \times \cdots \times \mathbb{Z}_3}_{h} = \mathbb{Z}_9 \times \mathbb{Z}_3^h.$$

CHAPTER FIVE

SUMMARY OF FINDINGS, CONCLUSION AND RECOMMENDATIONS

5.1 Summary of Findings

In this research, we sought to achieve the characterization of the unit groups of the total quotient ring of a completely primary finite ring of characteristic p^k. This was done in three steps; using the usual multiplication of fractions we constructed the total quotient ring. We showed that our local ring has a unique maximal ideal $J(R_S)$ and the groups of units $U(R_S)$ have a unique characterization of $\mathbb{Z}_{p^r-1} \times \left(\frac{1}{1} + J(R_S)\right)$ such that $(\mid \mathbb{Z}_{p^r-1} \mid, \mid \left(\frac{1}{1} + J(R_S)\right) \mid) = 1$ for some prime integer p and positive integers k and r. To completely characterize the structure of $U(R_S)$, we determined the generators of $\frac{1}{1} + J(R_S)$. We found that the generators formed cyclic groups of prime power order $G_i \mid i = 1, \ldots, h$ such that $G_i \cap G_j = \frac{1}{1}$, $G_i \trianglelefteq \frac{1}{1} + J(R_S)$ and $\prod_{i=1}^{h} G_i = \frac{1}{1} + J(R_S)$.

Our findings can be summarized by the following theorem.

Theorem 15. *Let R be a completely primary finite ring given in section 3.1. Suppose S is a saturated multiplicative subset of R consisting of all the units in R and R_S is the localized ring constructed in Proposition 11. Then the structure of the unit group $U(R_S)$ is summarized as follows:*

$$U(R_S) \cong \begin{cases} \mathbb{Z}_{p^r-1} \times (\mathbb{Z}_p^r)^h & \text{if char } R = p; \\ \mathbb{Z}_{p^r-1} \times \mathbb{Z}_p^r \times (\mathbb{Z}_p^r)^h & \text{if char } R = p^2; \\ \mathbb{Z}_{2^r-1} \times \mathbb{Z}_2 \times \mathbb{Z}_{2^{k-2}} \times \mathbb{Z}_{2^{k-2}}^{r-1} \times (\mathbb{Z}_2^r)^h & \text{if char } R = p^k, k \geq 3, p = 2 \ ; \\ \mathbb{Z}_{p^r-1} \times \mathbb{Z}_{p^{k-1}}^r \times (\mathbb{Z}_p^r)^h & \text{if char } R = p^k, k \geq 3, p \neq 2. \end{cases}$$

5.2 Conclusion

This study has revealed that if $R_1 \cong R_2$, then $U(R_1) \cong U(R_2)$. Our results can be compared to those obtained in [32], but provide an alternative way by constructing isomorphic rings to R. We provided a partial solution to the question of possible constructions of rings isomorphic to R by the process of localization so that their unit groups are isomorphic to $U(R)$.

5.3 Recommendations

We recommend that future research should extend this study by exploring possible constructions of all the rings isomorphic to R_S so that their groups of units are the same as $U(R_S)$.

REFERENCES

[1] Alkhamees, Y.(1982), The intersection of distinct Galois sub-rings is not necessarily Galois, *Compositio Math.*, **40**, 283 - 286.

[2] Alkhamees, Y. (1981), Finite rings in which the multiplication of any two zero divisors is zero, *Arch. Math.* **37**, 144-149.

[3] 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(**3**), 463-468.

[4] Anderson, F.W. and Fuller, K.R. (1974), *Rings and Categories of Modules*, Graduate texts in Mathematics, 13, Springer-Verlag.

[5] Ayoub, C. W. (1969), On finite primary rings and their groups of units, *Compositio Math.* **50**, 247-252.

[6] Chikunji C. J. (2005), Unit groups of a certain class of completely primary finite rings, *Mathematical Journal of Okayama University*, **47**, 39 - 53.

[7] Chikunji, C. J. (2005), Unit groups of cube radical zero commutative completely primary finite rings, *International Journal of Mathematics and Mathematical Science*, **4**, 579-592.

[8] Chikunji, C. J. (2008), On unit groups of completely primary finite rings, *Mathematical Journal of Okayama University*, **50**, 34-49.

[9] Chikunji, C. J. (2013), A review of the theory of completely primary finite rings, *Conference Proceedings of the 2nd Strathmore International Mathematics Conference (SIMC 2013)*, 12 -16, Strathmore University, Kenya.

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

[11] Clark, W.E. and Drake, D. A. (1973), Finite chain rings, *Abhandlungen Math. Seminar der Univ. Hamburg*, 39(**1**), 147 - 153.

[12] Corbas, B. (1969), Rings with finite zero divisor, *Math. Ann.* **181**, 1-7.

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

[14] Cohn, P. M. (1991), *Algebra*, Chichester, John Wiley and Sons Ltd, (2nd ed.), 474.

[15] Dolzan, D. (2002), Group of units in a finite ring, *J. Pure APP. Algebra*, **170**, 175-183.

[16] Edmund, H. F. (1758), Properties of Primary non-commutative rings, *Amer. Math. Soc.*, **52**, 79-91.

[17] Gabidulin, E.M.,Paramonov A.V. and Tretjakov O. V. (1991), *Ideals over Non-Commutative ring and their Application to Cryptology*, Lecture notes in Computer Science, **547**, 482-489.

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

[19] Ganske, G. and McDonald, B.R. (1973), Finite Local ring, *Rocky Mountain J. Math.*, **4**.

[20] Gilberto, B. and Flaminio, F. (2015), *Finite Commutative rings and their Applications*, Klumer Academic Publishers, Springer.

[21] Gilmer, R.W. Jr. (1963), Finite rings having a cyclic multiplicative group of units, *American Journal of Mathematics*, **85**, 447-452.

[22] Janusz, G. J. (1966), Separable Algebras over commutative rings, *Trans. Amer. Math. Soc.*, **122**, 461-497.

[23] Hall, P. (1958), *Some sufficient conditions for a group to be nilpotent*, Illinois J. Math., **2**, 787-801.

[24] Hungerford, T. W. (1974), *Algebra*, Holt, Rinehart and Winston Inc.

[25] Kainrath, F. (1998), A note on quotients formed by units groups of semi local rings, *Houston Journal of Mathematics*, 21(**4**), 613-618.

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

[27] Ojiema, M. O. (2013), *On the Structure of unit groups of completely primary finite rings*, Masters Thesis, MMUST.

[28] Omolo, N. O., Owino, M.O. (2009), On the structures of quotient groups, *IJPAM*, 54(**4**), 497-502.

[29] Owino, M. O. , Chikunji, C.J and Ongati, O.N. (2009), Unit Groups of k+1 Index Radical Zero Commutative Finite Rings, *International Journal of Pure and Applied Mathematics*, **57**, 57-67.

[30] Owino, M. O. and Chikunji, C.J. (2009) ,Unit Groups of a Certain class of Commutative Finite Rings, *Jour. Math. Scie.*, **20**(**3**), , 275-280.

[31] Owino, M. O. (2010), Units of commutative finite rings with zero divisors satisfying the idempotent property, *Jour. Math. Sci.*, **21**, 301-307.

[32] Owino, M. O., Ojiema, M. O. and Mmasi E. (2013), Units of commutative completely primary finite rings of characteristic p^n, *Journ. of Algebra*, 7 (**6**), 259-266

[33] Owino, M. O., Mmasi, E. and Ojiema, M. (2015), On the quotient groups of subgroups of the units of a class of completely primary finite rings, *Pure Mathematical Sciences*, 4(**3**), 121-126.

[34] Pearson, K.R. and Schneider, J.E. (1970), Rings with a cyclic groups of units, *J. Algebra*, **16**, 243-251.

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

[36] Rotman, J. J. (2003), *Advanced modern algebra*, prentice Hall. (2nd Ed.).

[37] Snapper, E. (1950), Completely primary rings, *I. Annals of Math.*, **52**, 666-693.

[38] Stewart, I. (1972), Finite rings with a specified groups of units, *Math. Z*, **126**, 51-58.

[39] Wilson, R. S. (1973), On the structure of finite rings, *Compositio. Math.*, **26**, 234-238.

[40] Wilson, R. S. (1974), Representation of finite rings, *Pacific Journal of Mathematics*, 53(**2**).