"UNIT GROUPS OF CERTAIN CLASSES OF COMMUTATIVE FINITE RINGS"

BY

OWINO MAURICE ODUOR

A thesis submitted in fulfillment of the requirements for the award of the degree of

DOCTOR OF PHILOSOPHY IN PURE MATHEMATICS

Department of Mathematics and Applied Statistics
Maseno University

Abstract

The characterization of abelian groups which could be groups of units of a ring still remains a general problem. Previous studies have restricted the classes of groups or rings to be considered. The determination of the structures of the unit groups of both Galois and completely primary finite rings has been of significant interest in the recent past. However much of the restriction has been on classes of finite rings of characteristic p, p^2 or p^3, with Jacobson radical J such that $J^2 = (0)$; and $J^3 = (0)$, $J^2 \neq (0)$. In this thesis, we have determined the structures of the unit groups of commutative finite rings of characteristic p^k with Jacobson radical J such that $J^k \neq (0)$, $J^{k+1} = (0)$ where k is a positive integer. We have also constructed a ring R with Jacobson radical J which satisfies the property $J^{k+1} \neq (0)$, $J^{k+2} = (0)$ and determined the structure of its group of units. Moreover, we have determined the structures of some quotient groups of the subgroups of the unit groups of the rings constructed.

Chapter 1

Introduction

1.1 Structure of the thesis

Chapter 1 is introductory, and basically explains the concepts of units and zero divisors. We also give some essential results that are fundamental to the results in the following chapters in the thesis.

Chapter 2 provides a review of some studies previously conducted by researchers, in relation to our area of study.

Chapter 3 deals with the structure of the group of units of the ring of integers modulo n, where $n \geq 2$.

In Chapter 4, we construct a class of finite rings. The structure of the group of units of the constructed rings is also obtained.

Chapter 5 deals with another construction of a class of finite rings and the structure of its group of units is determined.

In Chapter 6, we obtain the structures of the quotient groups of the subgroups of the groups of units of the finite rings constructed in Chapters 4 and 5.

Finally, we indicate our contributions to knowledge in Chapter 7.

1.2 Units and zero divisors

Let R be a commutative finite ring with identity $1 \neq 0$. An element $u \in R$ is a unit if there exists $v \in R$ such that

$$uv = vu = 1 \neq 0.$$

An element $x \in R$ is a zero divisor if there exists a nonzero element $y \in R$ such that $xy = yx = 0$.

A field is a ring in which the identity $1 \neq 0$ and every non zero element has a multiplicative inverse. Let R be a commutative finite ring and R^* denotes the multiplicative group of units of R. Then R is local if it has a unique maximal ideal K and $1 + K \subseteq R^*$. Also R is local if all the non units of R form an ideal. A completely primary finite ring is a ring R with identity $1 \neq 0$ whose subset of all its zero divisors forms the unique maximal ideal. A Galois ring is a finite ring with identity $1 \neq 0$ such that the set of all its zero divisors with 0 included forms a principal ideal. For instance, $\mathbf{Z}_{p^k}$, for some positive integer k, is a Galois ring with (p) as its unique maximal ideal. When $k = 1$, $\mathbf{Z}_{p^k} = \mathbf{F}_p$ is the field of order p and $(p) = (0)$ is the zero ideal which is of course maximal in $\mathbf{F}_p$.

The leading role in the classification of all the finite rings with identity possibly makes completely primary finite rings attractive to most researchers. Similar to completely primary finite rings so far studied, our attention has been restricted to the commutative finite rings in which the set of all the zero divisors forms an additive group.

Let R be an arbitrary ring (not necessarily rings considered in the thesis), then the set of all the zero divisors of the ring is not necessarily an ideal of the ring. For instance, the elements $(2, 3)$ and $(1, 4)$ of the ring $\mathbf{Z}_4 \oplus \mathbf{Z}_6$ endowed with componentwise addition and multiplication are zero divisors, but if the set of the zero divisors were to be an ideal, then $(3, 1)$ would be a zero divisor, an obvious contradiction.

Let p be a prime integer. We have constructed commutative finite rings with unique maximal ideal J such that $J^{k+1} = (0)$ and $J^k \neq (0)$ for the cases when char$R = p$, char$R = p^2$ and char$R = p^k$ where $k \geq 3$. We have determined the structures of the unit groups of the rings constructed for different cases. Moreover, we have determined the structure of the unit group of a commutative finite ring with unique maximal ideal J such that $J^{k+2} = (0)$ and $J^{k+1} \neq (0)$. The following results have been fundamental in the determination of the structure of the unit groups of the rings studied in this thesis.

Theorem 1.2.1. *(see section* 1 *in [7]). If a ring R is finite, then every left unit is a right unit and every left zero divisor is a right zero divisor. Furthermore, every element of R is either a zero divisor or a unit.*

Proof. Let $x \in R$ and assume that x is not a left zero divisor. Let $\theta : R^+ \to R^+$ be an additive group automorphism defined by $\theta(r) = xr$. Then

$$ker\theta = \{r \in R^+ : xr = 0\} = \{0\}.$$

Therefore, θ is injective. Since R is finite, θ is also surjective. So, there exists $y \in R$ such that $xy = 1$ which shows that x is a left unit. Suppose now that there exists $s \in R$ such that $sx = 0$. Then

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

and therefore, x is not a right zero divisor.

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

The contrapositive of the above argument completes the proof. □

Theorem 1.2.2. *(see section 1 in [8]). If a ring R has $n \geq 2$ left zero divisors (including zero), then R is a finite ring, and $| R | \leq n^2$.*

Proof. Suppose $0 \neq a$ is a left zero divisor in R and consider the right ideal Ra of R. Since a is a left zero divisor in R, there exists $0 \neq x \in R$ such that $ax = 0$, so that, for all $r \in R$,

$$r(ax) = (ra)x = 0.$$

So Ra consists entirely of left zero divisors. Thus $| Ra | \leq n$. Now, since Ra is finite, consider the surjective additive group homomorphism

$$\varphi : R \to Ra$$

defined by $r \to ra$ with

$$ker\varphi = \{y \in R : ya = 0\}.$$

We have $R/ker\varphi \cong Ra$, and every element of the kernel is a left zero divisor of R (since $a \neq 0$), so that $| ker\varphi | \leq n$. Thus $ker\varphi$ and

Ra are finite, so that R is finite and moreover,

$$| R |=| ker\varphi || Ra |\leq n^2$$

□

Corollary 1.2.3. *Let R be a finite ring with identity $1 \neq 0$. Then, every non- trivial ideal of R consists entirely of zero divisors.*

From now onwards, an element of a ring R which is a right or a left zero divisor will be called a zero divisor . Similarly, a right or a left unit will be be called a unit.

Theorem 1.2.4. *If G is a cyclic group of order n, then $G \cong \mathbf{Z}_n$(see [2])*

Proof. Let $< a >$ be a cyclic group generated by a and of finite order n. If we define a map $< a >\longrightarrow \mathbf{Z}_n$ by $a^k \rightarrow k+ < n >$ where $k = 0, 1, ..., n - 1$, then the map is clearly an isomorphism. □

1.3 Statement of the problem

The characterization of abelian groups which could be groups of units of a ring still remains a general problem. Previous studies have restricted the classes of groups or rings to be considered. In this thesis, we have determined the structures of the unit groups of $k+1$ index radical zero commutative completely primary finite rings. A specific case of the structure of the unit group of $k+2$ index radical zero commutative completely primary finite ring has also been studied. Moreover, structures of some quotient groups of the subgroups of the unit groups of the constructed rings have also been determined.

1.4 Objective of the study

Our goal was to determine the structures of the unit groups of certain classes of commutative finite rings with identity.

the units of the Galois ring $GR(p^{nr}, p^n)$ are a direct sum of a cyclic group of order $p^r - 1$ and r cyclic groups of order $p^n - 1$. Raghavendran [15] independently considered this case and further described the structure of the multiplicative group of every Galois ring.

In [16], Stewart considered a problem related to that asked by Fuchs [10] by proving that for a given finite group G (not necessarily abelian), there are up to isomorphism only finitely many directly indecomposable finite rings having group of units isomorphic to G.

A study by Ganske and McDonald [11] revealed that when the local ring R has a Jacobson radical J such that $J^2 = (0)$, then

$$R^* =<| K | -1 > \times \prod_{i=1}^{nt} \varepsilon(\pi),$$

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

Dolzan in [9] found all non isomorphic rings with group of units isomorphic to a group G with n elements, where n is a power of a prime or any product of prime powers, not divisible by 4; and also found all groups with n elements which can be groups of units of a finite ring, a contribution to Stewart's problem [16]. In [3] and [4], Chikunji determined the structure of the group of units of the ring

$R = R_0 \oplus U \oplus V$, where $R_0 = GR(p^{kr}, p^k)$ is the Galois subring of R, while U and V are finitely generated R_0- modules. The author further determined the generators of R^*. Upon consideration of s, t and λ to be the number of elements in the generating sets for U, V and W respectively, Chikunji in [5] determined in general the structure of the subgroup $1+W$ of the unit group of $R = R_0 \oplus U \oplus V \oplus W$ and the structure of the group of units R^* of the ring R when $s = 3$, $t = 1$, $\lambda \geq 1$ and char$R = p$. Furthermore the author generalized the structures of R^* in the cases when $s = 2$, $t = 1$; $t = s(s+1)/2$ for a fixed s, and $p \leq$ char$R \leq p^3$; $s = 2$, $t = 2$ and char$R = p$ to the case when the annihilator, ann$(J) = J^2 + W$, so that $\lambda \geq 1$.

In this thesis we have determined in general, the structures of the unit groups of $k+1$ index radical zero commutative finite rings together with a specific case when $J^{k+2} = (0)$. Moreover, some structures of the resultant quotient groups have also been determined.

Chapter 3

Preliminary Results

We discuss some results for $(\mathbf{Z}_n)^*$, $n \geq 2$. It is also useful to note that addition and multiplication of the elements in $R_1 \times ... \times R_s$ are done componentwise in this chapter.

3.1 The Chinese Remainder Theorem

The Chinese Remainder Theorem from elementary number theory asserts that if $m_1, m_2, ..., m_s$ are integers that are coprime in pairs, and $a_1, a_2, ..., a_s$ are integers, then there exists an integer a such that $a \equiv a_i (\text{mod } m_i)$ for each $i = 1, 2, ..., s$.

Definition 3.1.1. *The ideals I_n and I_m of a ring R are said to be comaximal if $I_n + I_m = R$.*

In terms of rings, the Chinese Remainder Theorem is stated by the following theorem.

Theorem 3.1.1. *(see [13] or [17]) Let $I_1, ..., I_k$ be ideals in a ring R. The map $R \longrightarrow R/I_1 \times R/I_2 \times ...R/I_k$ defined by*

$$r \longrightarrow (r + I_1, r + I_2, ..., r + I_k)$$

is a ring homomorphism with kernel $I_1 \cap I_2 \cap ... \cap I_k$.

If for each $i, j \in \{1, 2, ..., k\}$ with $i \neq j$, the ideals I_i and I_j are comaximal, then this map is surjective and

$$I_1 \cap I_2 \cap ... \cap I_k = I_1.I_2...I_k,$$

so

$$R/(I_1.I_2...I_k) = R/(I_1 \cap I_2 \cap ... \cap I_k) \cong R/I_1 \times R/I_2 \times ... \times R/I_k.$$

The following result is due to Chikunji [3].

Lemma 3.1.2. *(see [3]) Let R_1 and R_2 be finite rings. Then every (ring) isomorphism between R_1 and R_2 restricts to an isomorphism between R_1^* and R_2^*.*

However, it is not always true that if R_1^* and R_2^* are isomorphic, then the rings R_1 and R_2 are isomorphic as may be illustrated by the following:

$(\mathbf{Z}_3)^* = \{1, 2\} \cong (\mathbf{Z}_4)^* = \{1, 3\}$, while $\mathbf{Z}_3$ and $\mathbf{Z}_4$ are non-isomorphic rings.

Proposition 3.1.3. *(see [2]) Suppose R_1 and R_2 are finite rings each with identity $1 \neq 0$. Then*

$$(R_1 \times R_2)^* = R_1^* \times R_2^*.$$

Proof. Let $(r_1, r_2) \in (R_1 \times R_2)^*$. Then, there exists $(s_1, s_2) \in (R_1 \times R_2)^*$ such that $(r_1, r_2).(s_1, s_2) = (r_1 s_1, r_2 s_2) = (1, 1)$. In other words

$$(R_1 \times R_2)^* = \{(r_1, r_2) \mid r_1 \in R_1^* \text{ and } r_2 \in R_2^*\}$$

$$= R_1^* \times R_2^*.$$

□

The mentioned result can be extended inductively to prove that if R is the finite direct product of a family of rings R_i, $i = 1, 2, ..., n$, then the group of units R^* of the ring R consists of the elements of the form $(r_1, r_2, ..., r_n)$, where each r_i is invertible in R_i, that is

$$R^* = R_1^* \times R_2^* \times ... \times R_n^*$$

The following result is a consequence of Theorem 3.1.1, Lemma 3.1.2 and Proposition 3.1.3.

Corollary 3.1.4. *(Chinese Remainder Theorem for Multiplicative Groups). Let n be a positive integer and let $p_1^{\alpha 1} p_2^{\alpha 2} ... p_k^{\alpha_k}$, be its factorization into powers of distinct primes. Then*

$$\mathbf{Z}_n \cong \mathbf{Z}_{p_1^{\alpha 1}} \times \mathbf{Z}_{p_2^{\alpha 2}} \times ... \times \mathbf{Z}_{p_k^{\alpha_k}}$$

as rings, so in particular we have the following isomorphism of multiplicative groups,

$$(\mathbf{Z}_n)^* \cong (\mathbf{Z}_{p_1^{\alpha 1}})^* \times (\mathbf{Z}_{p_2^{\alpha 2}})^* \times ... \times (\mathbf{Z}_{p_k^{\alpha_k}})^*$$

Proposition 3.1.5. *Let $n \in Z^+$. Then the number of elements of $(\mathbf{Z}_n)^*$ is $\varphi(n)$ where φ denotes the Euler φ function.*

Proof. If we compare orders of the two sides of the isomorphism in Corollary 3.1.4, we obtain the formula

$$\varphi(n) = \varphi(p_1^{\alpha 1})\varphi(p_2^{\alpha 2}) ... \varphi(p_k^{\alpha_k})$$

for the Euler φ- function. This in turn implies that φ is a multiplicative function , namely $\varphi(ab) = \varphi(a)\varphi(b)$, whenever a and b are relatively prime positive integers.

The value of φ on prime powers p^{α} is easily seen to be $\varphi(p^{\alpha}) = p^{\alpha-1}(p-1)$. From this and the multiplicativity of φ we obtain its value on all positive integers. □

Remark: Corollary 3.1.4 is also a step towards a determination of the decomposition of the abelian group $(\mathbf{Z}_n)^*$ into a direct product of cyclic groups.

Corollary 3.1.6. *Let p be a prime. Then $(Z_p)^*$ is cyclic.*

Proof. This is the multiplicative group of the finite field $\mathbf{Z}_p$ and its structure is well known. □

Corollary 3.1.7. *Let $n \geq 2$ be an integer with factorization $n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}$ in Z^+ where p_1, p_2,...,p_k are distinct primes. We have the following isomorphisms of (multiplicative) groups:*

(i) $(Z_n)^* \cong (Z_{p_1^{\alpha_1}})^* \times (Z_{p_2^{\alpha_2}})^* \times ... \times (Z_{p_k^{\alpha_k}})^*$

(ii) $(Z_{2^{\alpha}})^*$ is the direct product of a cyclic group of order 2 and a cyclic group of order $2^{\alpha-2}$, for all $\alpha \geq 2$.

(iii) $(Z_{p^{\alpha}})^*$ is a cyclic group of order $p^{\alpha-1}(p-1)$, for all odd primes p.

Proof. The isomorphism in (i) follows from the Corollary to the Chinese Remainder Theorem (Corollary 3.1.4).

The isomorphism in (ii) is well known (see [15]).

If p is an odd prime, then $(\mathbf{Z}_{p^\alpha})^*$ is an abelian group of order $p^{\alpha-1}(p-1)$. The Sylow $p-$ subgroup of this group is cyclic. The map $\mathbf{Z}_{p^\alpha} \longrightarrow \mathbf{Z}_p$ defined by $a + (p^\alpha) \longrightarrow a + (p)$ is a ring homomorphism (reduction mod p) which gives a surjective group homomorphism from $(\mathbf{Z}_{p^\alpha})^*$ onto $(\mathbf{Z}_p)^*$. This latter group is cyclic of order $p-1$ (see Corollary 3.1.6). The kernel of this map is of order $p^{\alpha-1}$, hence for all primes $q \neq p$, the Sylow q- subgroup of $(\mathbf{Z}_{p^\alpha})^*$ maps isomorphically into the cyclic group $(\mathbf{Z}_p)^*$. All Sylow subgroups of $(\mathbf{Z}_{p^\alpha})^*$ are therefore cyclic, so (iii) holds, completing the proof. □

Remark: The above isomorphisms describe the group theoretic structure of the automorphism group of the cyclic group, $\mathbf{Z}_n$, of order n since $\mathrm{Aut}(\mathbf{Z}_n) \cong (\mathbf{Z}_n)^*$. In particular, for a prime p, the automorphism of the cyclic group of order p is cyclic of order $p-1$. The following result is an interesting arithmetic consequence of Corollary 3.1.6

Corollary 3.1.8. *Let $n \in Z^+$. The prime number p divides an* *integer of the form $n^2 + 1$ if and only if p is either 2 or an odd prime congruent to 1 modulo 4.*

Proof. The statement for $p = 2$ is trivial since 2 divides $1^2 + 1$. If p is an odd prime, we note that $p \mid n^2 + 1$ is equivalent to $n^2 = -1$ in $\mathbf{Z}_p$. This in turn is equivalent to saying that the residue class of n is of order 4 in $(\mathbf{Z}_p)^*$. Thus p divides an integer of the form $n^2 + 1$ if and only if $(\mathbf{Z}_p)^*$ contains an element of order 4. By Corollary 3.1.6, this group is cyclic, hence it contains an element of order 4 if and only if 4 divides its order, $p - 1$; that is $p \equiv 1 (\text{mod } 4)$. □

Chapter 4

A class of finite rings I

In this chapter, we study the unit groups R^* of a commutative finite ring R of characteristic p^k, with unique maximal ideal J such that $R/J \cong GF(p^r)$, $J^{k+1} = (0)$ and $J^k \neq (0)$, for some prime integer p and positive integers k and r.

4.1 Construction A

Let R_0 be the Galois ring of the form $GR(p^{kr}, p^k)$ and let $u_i \in R$, where $1 \leq i \leq h$ so that $R = R_0 \oplus R_0u_1 \oplus ... \oplus R_0u_h$ is an additive abelian group. On the additive abelian group, define multiplication by the following relations:

$$u_iu_j = 0 \ (1 \leq i, j \leq h); r_0u_i = u_ir_0, \ r_0 \in R_0; p^{k-1}u_i \neq 0.$$

Theorem 4.1.1. *The additive abelian group R defined above is a commutative finite ring with identity* $(1, 0, 0, ..., 0)$

Proof. From the given definition of multiplication in R, we see clearly that if $(r_0, r_1, ..., r_h)$ and $(s_0, s_1, ..., s_h)$ are any two elements in R, then

$$(r_0, r_1, ..., r_h)(s_0, s_1, ..., s_h) = (r_0s_0, r_0s_1 + r_1s_0, ..., r_0s_h + r_hs_0).$$

We verify that the given multiplication turns the additive abelian group into a commutative ring with identity $(1, 0, 0, ..., 0)$.

Let

$$(r_0, r_1, ..., r_h) \in R,$$

then

$$(r_0, r_1, ..., r_h)(1, 0, ..., 0) = (r_0, r_1, ..., r_h).$$

So $(1, 0, 0, ..., 0)$ is the multiplicative identity of R.

We now show that the multiplication is associative.

Let

$$(r_0, r_1, ..., r_h), (s_0, s_1, ..., s_h), (t_0, t_1, ..., t_h) \in R.$$

Then

$$
\begin{aligned}
&(r_0, r_1, ..., r_h)((s_0, s_1, ..., s_h)(t_0, t_1, ..., t_h))\\
&\quad = (r_0, r_1, ..., r_h)(s_0t_0, s_0t_1 + s_1t_0, ..., s_0t_h + s_ht_0)\\
&\quad = (r_0s_0t_0, r_0s_0t_1 + r_0s_1t_0 + r_1s_0t_0, ..., r_0s_0t_h + r_0s_ht_0 + r_hs_0t_0)\\
&\quad = (r_0s_0t_0, r_0s_0t_1 + (r_0s_1 + r_1s_0)t_0, ..., r_0s_0t_h + (r_0s_h + r_hs_0)t_0)\\
&\quad = (r_0s_0, r_0s_1 + r_1s_0, ..., r_0s_h + r_hs_0)(t_0, t_1, ..., t_h)\\
&\quad = ((r_0, r_1, ..., r_h)(s_0, s_1, ..., s_h))(t_0, t_1, ..., t_h)
\end{aligned}
$$

showing that multiplication is associative.

Moreover,

$$
\begin{aligned}
&((r_0, r_1, ..., r_h) + (s_0, s_1, ..., s_h))(t_0, t_1, ..., t_h)\\
&\quad = (r_0 + s_0, r_1 + s_1, ..., r_h + s_h)(t_0, t_1, ..., t_h)\\
&\quad = (r_0t_0 + s_0t_0, r_0t_1 + s_0t_1 + r_1t_0 + s_1t_0, ..., r_0t_h + s_0t_h + r_ht_0 + s_ht_0)\\
&\quad = (r_0t_0, r_0t_1 + r_1t_0, ..., r_0t_h + r_ht_0) + (s_0t_0, s_0t_1 + s_1t_0, ..., s_0t_h + s_ht_0)\\
&\quad = (r_0, r_1, ..., r_h)(t_0, t_1, ..., t_h) + (s_0, s_1, ..., s_h)(t_0, t_1, ..., t_h).
\end{aligned}
$$

and

$$\begin{aligned}
&(r_0, r_1, ..., r_h)((s_0, s_1, ..., s_h) + (t_0, t_1, ..., t_h)) \\
&\quad = (r_0, r_1, ..., r_h)(s_0 + t_0, s_1 + t_1, ..., s_h + t_h) \\
&\quad = (r_0s_0 + r_0t_0, r_0s_1 + r_0t_1 + r_1s_0 + r_1t_0, ..., r_0s_h + r_0t_h + r_hs_0 + r_ht_0) \\
&\quad = (r_0s_0, r_0s_1 + r_1s_0, ..., r_0s_h + r_hs_0) + (r_0t_0, r_0t_1 + r_1t_0, ..., r_0t_h + r_ht_0) \\
&\quad = (r_0, r_1, ..., r_h)(s_0, s_1, ..., s_h) + (r_0, r_1, ..., r_h)(t_0, t_1, ..., t_h).
\end{aligned}$$

So, the multiplication is both right and left distributive over addition. Hence the multiplication turns the additive group into a ring. The ring is commutative because

$$\begin{aligned}
&(r_0, r_1, ..., r_h)(s_0, s_1, ..., s_h) \\
&\quad = (r_0s_0, r_0s_1 + r_1s_0, ..., r_0s_h + r_hs_0) \\
&\quad = (s_0r_0, s_0r_1 + s_1r_0, ..., s_0r_h + s_hr_0) \\
&\quad = (s_0, s_1, ..., s_h)(r_0, r_1, ..., r_h).
\end{aligned}$$

This completes the proof. □

Remark: In order to simplify our work, we shall write

$$\begin{aligned}
R &= R_0 \oplus R_0u_1 \oplus ... \oplus R_0u_h \\
&= \{a_0 + a_1u_1 + ... + a_hu_h \mid a_0, a_i \in R_0,\ u_iu_j = 0, (1 \leq i, j \leq h)\}
\end{aligned}$$

Proposition 4.1.2. *The ring R is completely primary of characteristic p^k, and*

(i) $J = pR_0 \oplus R_0u_1 \oplus ... \oplus R_0u_h$

(ii) $J^2 = p^2R_0 \oplus pR_0u_1 \oplus ... \oplus pR_0u_h$

(iii) $J^{k-1} = p^{k-1}R_0 \oplus p^{k-2}R_0u_1 \oplus ... \oplus p^{k-2}R_0u_h$

(iv) $J^k = p^kR_0 \oplus p^{k-1}R_0u_1 \oplus ... \oplus p^{k-1}R_0u_h$

(v) $J^{k+1} = (0)$

Proof. First, we show that char $R = p^k$, for some prime p and positive integer k.

Since char $R_0 = p^k$, then for every $y \in R_0$, $p^ky = 0$. But

$$R = \{y_0 + y_1u_1 + ... + y_hu_h \mid y_0, y_i \in R_0,\ u_iu_j = 0, (1 \leq i, j \leq h)\}.$$

Now, suppose $p^s \in R$ where $s < k$ and y_0 is not a member of pR_0. Then, by the distributive property in R,

$$p^s(y_0 + y_1u_1 + ... + y_hu_h) = p^sy_0 + p^sy_1u_1 + ... + p^sy_hu_h \neq 0.$$

The same argument holds for any other positive integer less than p^k. So char $R = p^k$.

With the obvious identifications, we can think of R_0 as a subset of R. Now, it follows immediately from the way multiplication has been defined that if

$$J = pR_0 \oplus R_0u_1 \oplus ... \oplus R_0u_h,$$

then

$$J^2 = p^2R_0 \oplus pR_0u_1 \oplus ... \oplus pR_0u_h,$$

$$J^{k-1} = p^{k-1}R_0 \oplus p^{k-2}R_0u_1 \oplus ... \oplus p^{k-2}R_0u_h,$$

$$J^k = p^kR_0 \oplus p^{k-1}R_0u_1 \oplus ... \oplus p^{k-1}R_0u_h,$$

and that

$$J(p^kR_0 \oplus p^{k-1}R_0u_1 \oplus ... \oplus p^{k-1}R_0u_h) = (p^kR_0 \oplus p^{k-1}R_0u_1 \oplus ... \oplus p^{k-1}R_0u_h)J$$

$$= (0).$$

Hence

$$J^{k+1} = (0).$$

Also from the definition of multiplication, it follows that $RJ = JR \subseteq J$ so that J is an ideal. Suppose there is an ideal $K \supseteq J$, then by Theorem 1.2.1, K contains a unit $z \in R$ such that $zz^{-1} = z^{-1}z = 1$. So $K = R$. Therefore J is the unique maximal ideal in R since any maximal ideal distinct from J contains a unit. We now show that J is indeed $pR_0 \oplus R_0u_1 \oplus ... \oplus R_0u_h$.

Let $\alpha \in R_0$ with α not a member of pR_0 and $s \in J$. We have

$$(\alpha + s)^{p^r} = \alpha^{p^r} + t \text{ (with } t \in J)$$
$$= \alpha + v \text{ (with } v \in J).$$

But then $(\alpha + v)^{p-1} = 1 + q$ (with $q \in J$) and $(1+q)^{p^{k-1}} = 1$. Hence $\alpha + s$ is invertible. Since $\mid J \mid = p^{(k(h+1)-1)r}$ and

$$\mid (R_0/pR_0)^* + J \mid = (p^r - 1)p^{(k(h+1)-1)r},$$

it follows that $(R_0/pR_0)^* + J = R - J$ and hence all the elements outside J are invertible. Therefore R is completely primary and satisfies the given properties. □

Let R be a completely primary finite ring of Construction A, with maximal ideal J such that $J^{k+1} = (0)$, $J^k \neq (0)$. Then R is of order $p^{k(h+1)r}$ and the residue field R/J is the finite field $GF(p^r)$, for some prime integer p and positive integers k, h and r. A concrete model of R_0 is the quotient $\mathbf{Z}_{p^k}[x]/(f)$ where $f \in \mathbf{Z}_{p^k}[x]$ is a monic polynomial of degree r irreducible modulo p. Then it can be deduced from the main theorem in [6] that R has a coefficient subring R_0 of the form $GR(p^{kr}, p^k)$ which is clearly a maximal Galois subring of R. A trivial case is $GR(p^k, p^k) = \mathbf{Z}_{p^k}$. Notice that since R is of order $p^{k(h+1)r}$ and $R^* = R - J$, then $\mid R^* \mid = p^{(k(h+1)-1)r}(p^r - 1)$ and $\mid 1 + J \mid = p^{(k(h+1)-1)r}$. So $1 + J$ is an abelian $p-$ group. Thus $R^* \cong$(abelian $p-$ group)$\times$(cyclic group of order $\mid R/J \mid -1$)

In the sequel, the following result due to Chikunji [4] will be useful.

Proposition 4.1.3. *Let R be a completely primary finite ring (not necessarily commutative). Then the group of units R^* of the ring R contains a cyclic subgroup $< b >$ of order $p^r - 1$ and R^* is a semi direct product of $1 + J$ and $< b >$.*

Since the rings of Construction A are commutative, we deduce from the above Proposition that if A is a cyclic group of order $\mid R/J \mid -1$, then

$$R^* = A.(1 + J) \cong A \times (1 + J)$$

a direct product.

Remark: In order to clarify our work we shall begin each section by determining the structure of the group of units of the ring $R = R_0 \oplus R_0u_1 \oplus ... \oplus R_0u_h$ where $R_0 = GR(p^k, p^k)$ is the Galois ring of characteristic p^k and order p^k. In other words, we determine the structure of the groups of units of the ring when $r = 1$. We then proceed to determine the structure of the group of units of R

for any positive integer r.

4.2 Units of rings of characteristic p

Let $k = 1$ so that $R_0 = \mathbf{Z}_p$ is a Galois ring. Then

$$R = \mathbf{Z}_p \oplus \mathbf{Z}_p u_1 \oplus \ldots \oplus \mathbf{Z}_p u_h$$

Proposition 4.2.1. *If $h = 1$, then the unit group of the ring defined in this section is cyclic of order $p(p-1)$ for any prime integer p.*

Proof. Given that $k = 1$ and $h = 1$, we notice that $\mid \mathbf{Z}_p \oplus \mathbf{Z}_p u \mid = p^2$ and $\mid J \mid = p$. So

$$\mid R^* \mid = p^2 - p = p(p-1).$$

Suppose $a_1 + a_2 u \in (\mathbf{Z}_p \oplus \mathbf{Z}_p u)^*$ we seek to show that if $a_1 + a_2 u$ generates $(\mathbf{Z}_p \oplus \mathbf{Z}_p u)^*$, then $(a_1 + a_2 u)^{p(p-1)} = 1$. But

$$(\mathbf{Z}_p \oplus \mathbf{Z}_p u)^* = \{a_1 + a_2 u \mid a_1 \in (\mathbf{Z}_p)^*,\ a_2 \in \mathbf{Z}_p\}$$

So, let $a_1 + a_2 u \in (\mathbf{Z}_p \oplus \mathbf{Z}_p u)^*$ with maximum possible order. We claim that the order of $a_1 + a_2 u$, is

$$o(a_1 + a_2 u) = \begin{cases} p \text{ if } p = 2 \\ p(p-1) \text{ if } p \text{ is odd} \end{cases}$$

This is true because, if $p = 2$, then

$$\begin{aligned}(a_1 + a_2u)^2 &= (a_1 + a_2u)(a_1 + a_2u)\\ &= a_1^2 + a_1a_2u + a_2ua_1 \text{ (since } u^2 = 0)\\ &= a_1^2 + 2a_1a_2u \text{ (since } (\mathbf{Z}_2 \oplus \mathbf{Z}_2u)^* \text{ is abelian)}\\ &= a_1^2 \text{ (since char } (\mathbf{Z}_2 \oplus \mathbf{Z}_2u) = 2, \text{ and } 2u = 0)\\ &= 1 \text{ (since } a_1 \in (\mathbf{Z}_2)^*)\end{aligned}$$

Now, suppose p is odd. Then, since $u^2 = 0$,

$$\begin{aligned}(a_1 + a_2u)^p &= a_1^p + (a_1^{p-1}a_2 + a_1^{p-2}a_2a_1 + ... + a_2a_1^{p-1})u\\ &= a_1^p + p(a_1^{p-1}a_2)u \text{ (since } (\mathbf{Z}_p \oplus \mathbf{Z}_pu)^* \text{ is abelian)}\\ &= a_1^p \text{ (since char} (\mathbf{Z}_p \oplus \mathbf{Z}_pu) = p, \text{ and } pu = 0).\end{aligned}$$

Now

$$\begin{aligned}a_1^p &= a_1^{p-1}a_1\\ &= a_1 \text{ (since } a_1 \in (\mathbf{Z}_p)^*)\end{aligned}$$

Therefore,

$$\begin{aligned}(a_1 + a_2u)^{p(p-1)} &= a_1^{p-1}\\ &= 1 \text{ (since } a_1 \in (\mathbf{Z}_p)^*).\end{aligned}$$

Hence $(a_1+a_2u)^{p(p-1)} = 1$, for any prime p, proving that $(\mathbf{Z}_p \oplus \mathbf{Z}_p u)^*$ is cyclic. □

Remark: Let R be a ring defined in this section. If $r = 1$, then R has Jacobson radical J, and $J^2 = (0)$ so that $p \in J$, where p is a prime integer. The structure of R^* has been determined completely by Ganske and McDonald [11]. For the sake of completion, we state and prove it here in a different way. We begin with the case when $r = 1$.

Proposition 4.2.2. *Let R be the ring defined in this section. If $r = 1$, then*

$$R^* \cong \begin{cases} Z_2^h \text{ if } p = 2 \\ \\ Z_{p-1} \times Z_p^h \text{ if } p \text{ is odd} \end{cases}$$

Proof. If $k = 1$, then it can easily be shown that

$$J = \{s_1u_1 + ... + s_hu_h \mid s_i \in \mathbf{Z}_p,\ u_i \in R,\ 1 \leq i \leq h\}$$

and $J^2 = (0)$. Since $p \in J$, $pm = 0$, for any $m \in J$. Also $\mid J \mid = p^h$ for some positive integer h, such that $\mid R^* \mid = p^h(p-1)$. But

$$R^* = \{s_0 + s_1u_1 + ... + s_hu_h \mid s_0 \in (\mathbf{Z}_p)^*, s_i \in \mathbf{Z}_p,\ u_i \in R,\ 1 \leq i \leq h\}.$$

Suppose $p = 2$.

Let $y \in (\mathbf{Z}_2)^*$ and consider the element $1 + yu_1 \in R^*$. Then

$$(1 + yu_1)^2 = 1 + 2yu_1 \text{ (since } u_1^2 = 0)$$

$$= 1 \text{ (since char}R\text{=2 and } 2u_1 = 0).$$

So $1 + yu_1$ generates a cyclic subgroup of R^* of order 2.

Next, consider the element $1 + yu_1 + yu_2 \in R^*$. Then

$$(1 + yu_1 + yu_2)^2 = 1 + 2yu_1 + 2yu_2 \text{(since } u_iu_j = 0)$$

$$= 1 \text{ (since char}R\text{=2 and } 2u_i = 0).$$

So $1 + yu_1 + yu_2$ generates a cyclic subgroup of R^* of order 2. Continuing in a similar manner up to the element $1+yu_1+...+yu_h$, we see that $1 + yu_1 + ... + yu_h$ also generates a cyclic subgroup of R^* of order 2. Since R^* is abelian, each cyclic subgroup is normal, the intersection of any pair of the cyclic subgroups is the identity group and the order of the group generated by the direct product of the h cyclic subgroups coincides with $\mid R^* \mid$. Hence, the direct product of the cyclic subgroups exhausts R^*.

Suppose p is odd.

Then it is well known that $R^* =< b > \times (1 + J)$ (see [4]). We note that $< b >= R^*/(1 + J)$. It now remains to show that $1 + J$ is isomorphic to a direct product of h cyclic subgroups, each of order

p.

Consider the following h elements of $1+J$.

$1+yu_1$,

$1+yu_1+yu_2$,

$\vdots$

$1+yu_1+...+yu_h$, where $y \in (\mathbf{Z}_p)^*$

Clearly each of the elements generates a cyclic subgroup of $1+J$ of order p. Since $1+J$ is abelian, each of the cyclic subgroups is normal. Moreover the order of the group generated by the direct product of the h cyclic subgroups coincides with $\mid 1+J \mid$. So the direct product of the subgroups exhausts $1+J$. Therefore $\mid R^* \mid = \mid < b > \mid \times \mid 1+J \mid$ and this completes the proof. □

We now generalize the structure of the unit groups of the rings defined in this section for any positive integer r.

Let $R_0 = \mathbf{F}_q = GF(p^r)$, the Galois field of $q = p^r$ elements. Let $u_i \in R$, $(1 \leq i \leq h)$ such that

$$R = \mathbf{F}_q \oplus \mathbf{F}_q u_1 \oplus ... \oplus \mathbf{F}_q u_h,$$

the Jacobson radical

$$J = \mathbf{F}_q u_1 \oplus ... \oplus \mathbf{F}_q u_h$$

and

$$J^2 = (0)$$

The multiplication in R is given by the relations $u_i u_j = 0$; $r_0 u_i = u_i r_0$, where $r_0 \in R_0$ and $1 \leq i, j \leq h$.

Since R^* is a direct product of the cyclic group, say A of order $p^r - 1$ by the group $1 + J$ of order p^{hr}, it suffices to determine the structure of $1 + J$. In this case

$$1 + J = 1 + \mathbf{F}_q u_1 \oplus \ldots \oplus \mathbf{F}_q u_h.$$

We shall compare our result to the following result due to Ganske and McDonald.

Proposition 4.2.3. *(see [11]) If $r \geq 1$ and $h \geq 1$, then*

$$R^* =<\mid K \mid -1 > \times \prod_{i=1}^{rh} \epsilon(p),$$

where $h = dim_K(J/J^2)$, $\mid K \mid = p^r$, $\epsilon(p)$ denotes the cyclic group of order p.

Proposition 4.2.4. *If $charR = p$ and $h \geq 1$, then*

$$1 + J \cong \underbrace{\boldsymbol{Z}_p^r \times \ldots \times \boldsymbol{Z}_p^r}_{h \text{ copies}}$$

Proof. Let $\alpha_1, ..., \alpha_r \in \mathbf{F}_q$ with $\alpha_1 = 1$ such that $\overline{\alpha_1}, ..., \overline{\alpha_r} \in \mathbf{F}_q$ form a basis for $\mathbf{F}_q$ regarded as a vector space over its prime subfield $\mathbf{F}_p$, where $q = p^r$ for any prime integer p and positive integer r. We note that, for every $l = 1, ..., r$ and $1 \leq i \leq h$, $1 + \alpha_l u_i \in 1 + J$, $(1 + \alpha_l u_1)^p = 1$, $(1 + \alpha_l u_1 + \alpha_l u_2)^p = 1$,...,$(1 + \alpha_l u_1 + \alpha_l u_2 + ... + \alpha_l u_h)^p = 1$, $y^p = 1$, $\forall y \in 1 + J$.

For positive integers a_{1l} , a_{2l} ,...,a_{hl} with $a_{1l} \leq p$, $a_{2l} \leq p$,..., $a_{hl} \leq p$, we notice that the equation

$$\prod_{l=1}^{r}\{(1 + \alpha_l u_1)^{a_{1l}}\}.\prod_{l=1}^{r}\{(1 + \alpha_l u_1 + \alpha_l u_2)^{a_{2l}}\}$$

$$...\prod_{l=1}^{r}\{(1 + \alpha_l u_1 + \alpha_l u_2 + ... + \alpha_l u_h)^{a_{hl}}\} = 1$$

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

If we set

$$S_{1l} = \{(1 + \alpha_l u_1)^{a_1} \mid a_1 = 1, ..., p\},$$

$$S_{2l} = \{(1 + \alpha_l u_1 + \alpha_l u_2)^{a_2} \mid a_2 = 1, ..., p\}$$

$$\vdots$$

$$S_{hl} = \{(1 + \alpha_l u_1 + \alpha_l u_2 + ... + \alpha_l u_h)^{a_h} \mid a_h = 1, ..., p\}$$

we see that S_{1l}, S_{2l},...,S_{hl} are all cyclic subgroups of the group $1 + J$ and they are each of order p.

We also notice that as each element in $1+J$ raised to the power p equals 1, then $1+J$ is an elementary abelian group.

Now, since

$$\prod_{l=1}^{r} |< 1+\alpha_l u_1 >| \cdot \prod_{l=1}^{r} |< 1+\alpha_l u_1 + \alpha_l u_2 >|$$
$$\ldots \prod_{l=1}^{r} |< 1+\alpha_l u_1 + \alpha_l u_2 + \ldots + \alpha_l u_h >| = p^{hr}$$

and the intersection of any pair of the cyclic subgroups gives the identity group, the product of the hr subgroups S_{1l}, S_{2l},...,S_{hl} is direct. So their product exhausts the group $1+J$. □

4.3 Units of rings of characteristic p^2

Let $r = 1$ and $k = 2$. By the definition of multiplication in construction A and the properties of the Jacobson radical J, $p^2m = 0$, $m \in J$. Therefore $p^2 \in J^2$.

We investigate subgroups of $1 + J$ in this construction.

Remark: Since R^* is abelian, $1 + J$ is a normal subgroup of R^*.

Lemma 4.3.1. *For each prime integer p,* $1+p\mathbf{Z}_{p^2}$ *is a subgroup of* $1 + J$.

Proof. Let $1 + py_1, 1 + py_2 \in 1 + p\mathbf{Z}_{p^2}$ where $y_1, y_2 \in \mathbf{Z}_{p^2}$. Since $p^2y_2 = 0$, we see that $(1 + py_2)^{-1} = 1 - py_2$. So

$$\begin{aligned}&(1 + py_1)(1 + py_2)^{-1}\\ &= (1 + py_1)(1 - py_2)\\ &= 1 + p(y_1 - y_2)\end{aligned}$$

an element of $1 + p\mathbf{Z}_{p^2}$. □

Lemma 4.3.2. *For each prime integer p,* $1 + \sum_{i=1}^{h} \oplus \mathbf{Z}_{p^2}u_i$ *is a subgroup of* $1 + J$.

Proof. Let $1+\sum_{i=1}^{h} a_iu_i$ and $1+\sum_{i=1}^{h} b_iu_i$ belong to $1+\sum_{i=1}^{h} \oplus\mathbf{Z}_{p^2}u_i$, where $a_i, b_i \in \mathbf{Z}_{p^2}$ $(i = 1, ..., h)$. Since $u_iu_j = 0$, then $(1+\sum_{i=1}^{h} b_iu_i)^{-1} =$

$1 - \sum_{i=1}^{h} b_i u_i$. So

$$\begin{aligned}(1 + \sum_{i=1}^{h} a_i u_i)(1 + \sum_{i=1}^{h} b_i u_i)^{-1} \\ &= (1 + a_1 u_1 + a_2 u_2 + ... + a_h u_h)(1 - (b_1 u_1 + b_2 u_2 + ... + b_h u_h)) \\ &= 1 + (a_1 - b_1)u_1 + (a_2 - b_2)u_2 + ... + (a_h - b_h)u_h \\ &= 1 + \sum_{i=1}^{h}(a_i - b_i)u_i\end{aligned}$$

an element of $1 + \sum_{i=1}^{h} \oplus \mathbf{Z}_{p^2} u_i$. □

We now determine the structure of R^* of the ring given by construction A ,when $r = 1$ and char$R = p^2$.

Proposition 4.3.3. *Let R be a ring defined by construction A. If $r = 1$, $k = 2$ and J is the radical of the ring, then the group of units of the ring is a direct product of a cyclic group of order $p - 1$ by $1 + J$, where $1 + J \cong \mathbf{Z}_p \times \mathbf{Z}_{p^2}^h$ for any prime integer p.*

Proof. Let $k = 2$ and R be a ring of Construction A. Then we know that

$$J = p\mathbf{Z}_{p^2} \oplus \mathbf{Z}_{p^2} u_1 \oplus ... \oplus \mathbf{Z}_{p^2} u_h$$

$$J^2 = p^2\mathbf{Z}_{p^2} \oplus p\mathbf{Z}_{p^2} u_1 \oplus ... \oplus p\mathbf{Z}_{p^2} u_h,$$

and

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

Moreover, $R^* = R - J$ and $\mid R^* \mid = p^{2h+1}(p-1)$, $\mid 1 + J \mid = p^{2h+1}$.

Since $R^* \cong \mathbf{Z}_{p-1} \times (1+J)$. We need only show that $1+J \cong \mathbf{Z}_p \times \mathbf{Z}_{p^2}^h$.

Let $y \in (\mathbf{Z}_{p^2})^*$. Consider the element $1 + py \in 1 + J$, then

$$(1+py)^p = 1 + p^2y + \frac{(p-1)p^3y^2}{2} + ... + p^py^p$$

$$= 1 \text{ (since char } R = p^2).$$

Therefore, $1 + py$ generates a cyclic subgroup of $1 + J$ of order p.

Now, let $y \in (\mathbf{Z}_{p^2})^*$.

Since char $R = p^2$ and $u_iu_j = 0$,

$$(1 + yu_1)^p = 1 + pyu_1$$

and

$$(1 + pyu_1)^p = 1 + p^2yu_1$$

$$= 1 \text{ (since } p^2u_1 = 0).$$

Also

$$(1 + yu_1 + yu_2)^p = 1 + pyu_1 + pyu_2$$

and

$$(1 + pyu_1 + pyu_2)^p = 1 + p^2yu_1 + p^2yu_2$$

$$= 1 \text{ (since char } R = p^2 \text{ and } p^2u_i = 0).$$

Continuing in a similar manner up to the element $1+yu_1+...+yu_h$, we obtain $(1+yu_1+...+yu_h)^p = 1+pyu_1+...+pyu_h$ and

$$\begin{aligned}&(1+pyu_1+...+pyu_h)^p\\ &\quad = 1+p^2yu_1+...+p^2yu_h\\ &\quad = 1 \text{ (since char } R = p^2 \text{ and } p^2u_i = 0).\end{aligned}$$

Therefore, the h elements $1+yu_1$, $1+yu_1+yu_2$,...,$1+yu_1+...+yu_h$ generate cyclic subgroups of $1+J$ each of order p^2. Since the groups generated are normal, the order of the group generated by the direct product of the cyclic subgroups $< 1+py >, < 1+yu_1 >, < 1+yu_1+yu_2 >, ..., < 1+yu_1+...+yu_h >$ coincides with $\mid 1+J \mid$ and the intersection of any pair of the cyclic subgroups is the identity group, it follows that $1+J =< 1+py > \times < 1+yu_1 > \times$
$< 1+yu_1+yu_2 > \times ... \times < 1+yu_1+...+yu_h >$. □

We now generalize the structure of the unit groups of the rings defined in this section for any positive integer r.

Consider $R_0 = GR(p^{2r}, p^2)$, the Galois ring of characteristic p^2 and order p^{2r} and $u_i \in R$ $(1 \leq i \leq h)$ so that

$$R = R_0 \oplus R_0u_1 \oplus ... \oplus R_0u_h.$$

Then

$$J = pR_0 \oplus R_0u_1 \oplus ... \oplus R_0u_h$$

$$J^2 = p^2R_0 \oplus pR_0u_1 \oplus ... \oplus pR_0u_h$$

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

We know that

$$1 + J = 1 + pR_0 \oplus R_0u_1 \oplus ... \oplus R_0u_h$$

Lemma 4.3.4. *For each prime integer p, $1 + pR_0$ is a subgroup of $1 + J$.*

Proof. Similar to the proof of Lemma 4.3.1 with some modifications

□

Lemma 4.3.5. *If $1 \leq i \leq h$ and $k = 2$, then $1 + \sum_{i=1}^{h} \oplus R_0u_i$ is a subgroup of $1 + J$.*

Proof. Similar to the proof of Lemma 4.3.2 with some modifications

□

Proposition 4.3.6. *If* $\mathrm{char} R = p^2$ *and* $h \geq 1$, *then*

$$1 + J \cong \boldsymbol{Z}_p^r \times \underbrace{\boldsymbol{Z}_{p^2}^r \times ... \times \boldsymbol{Z}_{p^2}^r}_{h \text{ copies}}$$

Proof. Let $\alpha_1, ..., \alpha_r \in R_0$ with $\alpha_1 = 1$ such that $\overline{\alpha_1}, ..., \overline{\alpha_r} \in R_0/pR_0$ form a basis for R_0/pR_0 regarded as a vector space over its prime subfield $\mathbf{F}_p$. We note that for every $l = 1, ..., r$, $(1+p\alpha_l)^p = 1$, $(1 + \alpha_l u_1)^{p^2} = 1$, $(1 + \alpha_l u_1 + \alpha_l u_2)^{p^2} = 1$,...,
$(1 + \alpha_l u_1 + \alpha_l u_2 + ... + \alpha_l u_h)^{p^2} = 1$.

For positive integers $a_l, b_{1l}, b_{2l}, ..., b_{hl}$ with $a_l \leq p$, $b_{1l} \leq p^2$, ..., $b_{hl} \leq p^2$, we notice that the equation

$$\prod_{l=1}^{r}\{(1+p\alpha_l)^{a_l}\}.\prod_{l=1}^{r}\{(1+\alpha_l u_1)^{b_{1l}}\}.\prod_{l=1}^{r}\{(1+\alpha_l u_1+\alpha_l u_2)^{b_{2l}}\}$$
$$...\prod_{l=1}^{r}\{(1+\alpha_l u_1+\alpha_l u_2+...+\alpha_l u_h)^{b_{hl}}\} = 1$$

will imply $a_l = p$, $b_{il} = p^2$ for every $l = 1, ..., r$ and $1 \leq i \leq h$.

If we set

$$T_l = \{(1+p\alpha_l)^a \mid a = 1, ..., p\},$$

$$S_{1l} = \{(1+\alpha_l u_1)^{b_1} \mid b_1 = 1, ..., p^2\},$$

$$S_{2l} = \{(1+\alpha_l u_1+\alpha_l u_2)^{b_2} \mid b_2 = 1, ..., p^2\}$$

$$\vdots$$

$$S_{hl} = \{(1+\alpha_l u_1+\alpha_l u_2+...+\alpha_l u_h)^{b_h} \mid b_h = 1, ..., p^2\}$$

we see that T_l, S_{1l}, S_{2l},...,S_{hl} are all cyclic subgroups of the group

$1+J$ and they are of the orders indicated by their definition. Since

$$\prod_{l=1}^{r} |< 1 + p\alpha_l >| . \prod_{l=1}^{r} |< 1 + \alpha_l u_1 >| . \prod_{l=1}^{r} |< 1 + \alpha_l u_1 + \alpha_l u_2 >|$$

$$... \prod_{l=1}^{r} |< 1 + \alpha_l u_1 + \alpha_l u_2 + ... + \alpha_l u_h >|= p^{(2h+1)r}$$

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}, S_{2l},...,S_{hl} is direct. So their product exhausts the group $1 + J$. □

4.4 Units of rings of characteristic p^k, where $k \geq 3$

We begin by investigating subgroups of $1 + J$ in this construction when $r = 1$.

Lemma 4.4.1. *For each prime integer p, $1 + p\mathbf{Z}_{p^k}$ is a subgroup of $1 + J$.*

Proof. Let $1 + ps_1$, $1 + ps_2 \in 1 + p\mathbf{Z}_{p^k}$ where $s_1, s_2 \in \mathbf{Z}_{p^k}$. Since $p^k s_2 = 0$, $(1 + ps_2)^{-1} = 1 - ps_2 + p^2 s_2^2 - p^3 s_2^3 + ... + (-1)^{k+1} p^{k-1} s_2^{k-1}$.

So

$$(1 + ps_1)(1 + ps_2)^{-1}$$

$$= (1 + ps_1)(1 - ps_2 + p^2 s_2^2 - p^3 s_2^3 + ... + (-1)^{k+1} p^{k-1} s_2^{k-1})$$

$$= 1 + p((s_1 - s_2) + p(s_2^2 - s_1 s_2) + p^2(s_1 s_2^2 - s_2^3) + p^3(s_2^4 - s_1 s_2^3) + ... +$$

$$(-1)^{k+1} p^{k-2}(s_2^{k-1} - s_1 s_2^{k-2}))$$

an element of $1 + p\mathbf{Z}_{p^k}$. □

Lemma 4.4.2. *For each prime integer p, and $k \geq 3$, $1 + \sum_{i=1}^{h} \oplus \mathbf{Z}_{p^k} u_i$ is a subgroup of $1 + J$.*

Proof. Let $1 + \sum_{i=1}^{h} a_i u_i$ and $1 + \sum_{i=1}^{h} b_i u_i$ belong to $1 + \sum_{i=1}^{h} \oplus \mathbf{Z}_{p^k} u_i$, where $a_i, b_i \in \mathbf{Z}_{p^k}$ $(i = 1, ..., h)$. Then since $u_i u_j = 0$, $(1 + \sum_{i}^{h} b_i u_i)^{-1} =$

$1 - (\sum_i^h b_i u_i)$. So

$$\begin{aligned}
&(1 + \sum_{i=1}^{h} a_i u_i)(1 + \sum_{i=1}^{h} b_i u_i)^{-1} \\
&\quad = (1 + a_1 u_1 + a_2 u_2 + \ldots + a_h u_h)(1 - (b_1 u_1 + b_2 u_2 + \ldots + b_h u_h)) \\
&\quad = 1 + (a_1 - b_1)u_1 + (a_2 - b_2)u_2 + \ldots + (a_h - b_h)u_h \\
&\quad = 1 + \sum_{i=1}^{h} (a_i - b_i)u_i
\end{aligned}$$

an element of $1 + \sum_{i=1}^{h} \oplus \mathbf{Z}_{p^k} u_i$. □

We now determine the structure of R^*.

Proposition 4.4.3. *Let R be a ring defined by Construction A. If $k \geq 3$ and $r = 1$, then the group of units of the ring is a direct product of a cyclic group of order $p - 1$ by $1 + J$ where*

$$1 + J \cong \begin{cases} \mathbf{Z}_2 \times \mathbf{Z}_{2^{k-2}} \times \mathbf{Z}_{2^k}^h \text{ if } p = 2 \\ \\ \mathbf{Z}_{p^{k-1}} \times \mathbf{Z}_{p^k}^h \text{ if } p \text{ is odd} \end{cases}$$

Proof. Given that $k \geq 3$ and R is the defined ring, then $J = p\mathbf{Z}_{p^k} \oplus \mathbf{Z}_{p^k} \oplus \ldots \oplus \mathbf{Z}_{p^k}$. Moreover $R^* = R - J$ then $\mid R^* \mid = p^{k(h+1)-1}(p-1)$, $\mid 1 + J \mid = p^{k(h+1)-1}$. We know that

$$R^* \cong \mathbf{Z}_{p-1} \times (1 + J)$$

and therefore need only to determine the structure of $1 + J$.

We begin with the case when $p = 2$.

Suppose $w \in \mathbf{Z}_{2^k}$ such that w is not a member of $2^{k-1}\mathbf{Z}_{2^k}$. Let $w(w+1) \equiv 0(\text{mod } 2^{k-2})$. Then

$$(1+2w)^2$$

$$= 1 + 2^2(w + w^2)$$

$$= 1 + 2^k t, \ t \in \mathbf{Z}_{2^k}$$

$$= 1 \text{ (since char } R = 2^k).$$

Therefore, $1 + 2w$ generates a cyclic subgroup of $1 + J$ of order 2.

If $k = 3$, choose $y \in \mathbf{Z}_{2^k}$ such that y is not a member of $2^2\mathbf{Z}_{2^3}$ and $y \neq w$, then $(1+2y)^2 = 1$.

Suppose $k > 3$.

Let $y \in \mathbf{Z}_{2^k}$ such that y is not a member of $2^{k-1}\mathbf{Z}_{2^k}$ and $y(y+1)$ is not congruent to $0(\text{mod } 2^{k-2})$, then

$$(1+2y)^{2^{k-2}}$$

$$= 1 + 2^{k-2}(2y) + \frac{2^{k-2}(2^{k-2}-1)(2y)^2}{2} + \frac{2^{k-2}(2^{k-2}-1)(2^{k-2}-2)(2y)^3}{6}$$

$$+ ... + (2y)^{2^{k-2}}$$

$$= 1 + 2^{k-1}(y + ((2^{k-2}-1) + \frac{(2^{k-2}-1)(2^{k-2}-2)2y}{3}$$

$$+ ... + 2^{2^{k-2}-k+1}y^{2^{k-2}-2})y^2)$$

$$= 1 + 2^{k-1}(y + \beta y^2) \qquad (*)$$

where $\beta = (2^{k-2} - 1) + \frac{(2^{k-2}-1)(2^{k-2}-2)2y}{3} + ... + 2^{2^{k-2}-k+1}y^{2^{k-2}-2})$.

Now, since $\beta \in \mathbf{Z}_{2^k}$ is odd, the equation (*) becomes $1 + 2^k\delta$ where $\delta \in \mathbf{Z}_{2^k}$. But, since char$R = 2^k$, $1 + 2^k\delta = 1$. Thus $1 + 2y$ generates a cyclic subgroup of $1 + J$ of order 2^{k-2}.

Now, let $z \in (\mathbf{Z}_{2^k})^*$. Then, since $u_1^2 = 0$,

$$(1 + zu_1)^2 = 1 + 2zu_1$$

$$(1 + 2zu_1)^2 = 1 + 2^2zu_1$$

$$(1 + 2^2zu_1)^2 = 1 + 2^3zu_1.$$

Applying the procedure 2^k times, we obtain

$$\begin{aligned}(1 + 2^{k-1}zu_1)^2 &= 1 + 2^kzu_1 \\ &= 1 \text{ (since char } R = 2^k \text{ and } 2^ku_1 = 0)\end{aligned}$$

Therefore, $1 + zu_1$ generates a cyclic subgroup of $1 + J$ of order 2^k. Similarly $1 + zu_1 + zu_2$ generates a cyclic subgroup of $1 + J$ of order 2^k. Continuing in a similar manner up to the element $1 + zu_1 + ... + zu_h$, then the element also generates a cyclic subgroup of $1 + J$ of order 2^k. Since $1 + J$ is abelian, all the cyclic subgroups are normal. Moreover the order of the group generated by

$$< 1 + 2w >, < 1 + 2y >, < 1 + zu_1 >, ..., < 1 + zu_1 + ... + zu_h >$$

coincides with $\mid 1+J \mid$ and the intersection of any pair of the cyclic subgroups is the identity group. So the direct product of the cyclic subgroups exhausts $1+J$.

Now, consider the case when p is odd.

Let $z \in (\mathbf{Z}_{p^k})^*$. Then

$$(1+pz)^{p^{k-1}} = 1 + p^k\beta$$

where

$$\beta = z + \frac{(p^{k-1}-1)(pz^2)}{2} + \frac{(p^{k-1}-1)(p^{k-1}-2)p^2z^3}{6} + ... + p^{p^{k-1}-k}z^{p^{k-1}}$$

Now, since char $R = p^k$ and $\beta \in (\mathbf{Z}_{p^k})^*$ we obtain that

$(1+pz)^{p^{k-1}} = 1$. Thus $1+pz$ generates a cyclic subgroup of $1+J$ of order p^{k-1}. Again, let $z \in (\mathbf{Z}_{p^k})^*$. Then, since $u_1^2 = 0$,

$$(1+zu_1)^p = 1 + pzu_1$$

$$(1+pzu_1)^p = 1 + p^2zu_1$$

$$(1+p^2zu_1)^p = 1 + p^3zu_1$$

Applying the procedure 2^k times, we obtain

$$(1+p^{k-1}zu_1)^p = 1 + p^kzu_1$$

$$= 1 \text{ (since char } R = p^k \text{ and } p^ku_1 = 0)$$

Therefore, $1 + zu_1$ generates a cyclic subgroup of $1 + J$ of order p^k. Similarly $1 + zu_1 + zu_2$ generates a cyclic subgroup of $1 + J$ of order p^k. Continuing in a similar manner up to the element $1 + zu_1 + ... + zu_h$, then the element also generates a cyclic subgroup of $1 + J$ of order p^k. Since $1 + J$ is abelian, all the cyclic subgroups are normal. Moreover the order of the group generated by

$$< 1+pz >, < 1+zu_1 >, < 1+zu_1+zu_2 >, ..., < 1+zu_1+...+zu_h >$$

coincides with $\mid 1 + J \mid$ and the intersection of any pair of the cyclic subgroups is the identity group. So, the direct product of the cyclic subgroups exhausts $1 + J$. □

We now generalize the structure of the unit groups of the rings defined in this section for any positive integer r.

Let $R_0 = GR(p^{kr}, p^k)$, the Galois ring of characteristic p^k and order p^{kr} and $u_i \in R$ $(1 \leq i \leq h)$ so that

$$R = R_0 \oplus R_0 u_1 \oplus ... \oplus R_0 u_h.$$

We know that

$$J = pR_0 \oplus R_0 u_1 \oplus ... \oplus R_0 u_h$$

$$J^2 = p^2 R_0 \oplus pR_0 u_1 \oplus ... \oplus pR_0 u_h$$

$$\vdots$$

$$J^k = p^k R_0 \oplus p^{k-1} R_0 u_1 \oplus ... \oplus p^{k-1} R_0 u_h$$

and

$$J^{k+1} = (0).$$

Lemma 4.4.4. *For each prime integer p, $1 + pR_0$ is a subgroup of $1 + J$.*

Proof. Similar to the proof of Lemma 4.4.1 with some modifications

□

Lemma 4.4.5. *If $1 \leq i \leq h$ and $k \geq 3$, then $1 + \sum_{i=1}^{h} \oplus R_0 u_i$ is a subgroup of $1 + J$.*

Proof. Similar to the proof of Lemma 4.4.2 with some modifications

□

Proposition 4.4.6. *If $charR = p^k$ where $k \geq 3$ and $h \geq 1$, then*

$$1 + J \cong \begin{cases} \mathbb{Z}_2 \times \mathbb{Z}_{2^{k-2}} \times \mathbb{Z}_{2^{k-1}}^{r-1} \times \underbrace{\mathbb{Z}_{2^k}^r \times ... \times \mathbb{Z}_{2^k}^r}_{h \text{ copies}} & \text{if } p = 2 \\ \\ \mathbb{Z}_{p^{k-1}}^r \times \underbrace{\mathbb{Z}_{p^k}^r \times ... \times \mathbb{Z}_{p^k}^r}_{h \text{ copies}} & \text{if } p \text{ is odd} \end{cases}$$

Proof. Let $\alpha_1, \alpha_2, ..., \alpha_r \in R_0$ with $\alpha_1 = 1$ such that $\overline{\alpha_1}, \overline{\alpha_2}, ..., \overline{\alpha_r} \in R_0/pR_0$ form a basis for R_0/pR_0 regarded as a vector space over its prime subfield $\mathbf{F}_p$. We consider the two cases separately.

Suppose $p = 2$.

If $l = 1, ..., r$ and y is an element of R_0 such that $x^2 + x + \overline{y} = \overline{0}$ over R_0/pR_0, has no solution in the field R_0/pR_0, we obtain the following results: $(-1 + 2^{k-1}\alpha_1) \in 1 + pR_0$, $(-1 + 2^{k-1}\alpha_1)^2 = 1$, $(1 + 4y)^{2^{k-2}} = 1$ and $w^{2^{k-1}} = 1$ for every $w \in 1 + pR_0$. We also notice that $(1 + 2\alpha_l)^{2^{k-1}} = 1$ for $l = 2, ..., r$, $(1 + \alpha_l u_1)^{2^k} = 1$, $(1 + \alpha_l u_1 + \alpha_l u_2)^{2^k} = 1$,..., $(1 + \alpha_l u_1 + \alpha_l u_2 + ... + \alpha_l u_h)^{2^k} = 1$, for every $l = 1, ..., r$.

Now, for positive integers $a, b, c_l, d_{1l}..., d_{hl}$ with $a \leq 2$, $b \leq 2^{k-2}$, $c_l \leq 2^{k-1}$ for $l = 2, ..., r$ and $d_{il} \leq 2^k$ for every $l = 1, ..., r$ and $1 \leq i \leq h$, we notice that

$$(-1 + 2^{k-1}\alpha_1)^a.(1 + 4y)^b.\prod_{l=2}^{r}\{(1 + 2\alpha_l)^{c_l}\}.\prod_{l=1}^{r}\{(1 + \alpha_l u_1)^{d_{1l}}\}.$$
$$\prod_{l=1}^{r}\{(1 + \alpha_l u_1 + \alpha_l u_2)^{d_{2l}}\}...\prod_{l=1}^{r}\{(1 + \alpha_l u_1 + \alpha_l u_2 + ... + \alpha_l u_h)^{d_{hl}}\} = 1$$

will imply $a = 2$, $b = 2^{k-2}$, $c_l = 2^{k-1}$ for $l = 2, ..., r$ and $d_{il} = 2^k$ for every $l = 1, ..., r$ and $1 \leq i \leq h$.

If we set

$$H = \{(-1 + 2^{k-1}\alpha_1)^a \mid a = 1, 2\},$$

$$Q = \{(1 + 4y)^b \mid b = 1, ..., 2^{k-2}\},$$

$$T_l = \{(1+2\alpha_l)^c \mid c = 1, ..., 2^{k-1}\}$$

for $l = 2, ..., r$

$$S_{1l} = \{(1+\alpha_l u_1)^{d_1} \mid d_1 = 1, ..., 2^k\},$$

$$S_{2l} = \{(1+\alpha_l u_1 + \alpha_l u_2)^{d_2} \mid d_2 = 1, ..., 2^k\}$$

$$\vdots$$

$$S_{hl} = \{(1+\alpha_l u_1 + \alpha_l u_2 + ... + \alpha_l u_h)^{d_h} \mid d_h = 1, ..., 2^k\}$$

we see that H, Q, T_l, S_{1l}, S_{2l},...,S_{hl} are all cyclic subgroups of the group $1+J$ and they are of the orders indicated by their definition.

Since

$$|< -1+2^{k-1}\alpha_l >| \,.\, |< 1+4y >| \,.\prod_{l=2}^{r} |< 1+2\alpha_l >| \,.\prod_{l=1}^{r} |< 1+\alpha_l u_1 >| \,.$$
$$\prod_{l=1}^{r} |< 1+\alpha_l u_1+\alpha_l u_2 >| \ldots \prod_{l=1}^{r} |< 1+\alpha_l u_1+\alpha_l u_2+\ldots+\alpha_l u_h >|$$
$$= 2^{(k(h+1)-1)r}$$

and the intersection of any pair of the cyclic subgroups gives the identity group, the product of the $(h+1)r+1$ subgroups H, Q, T_l, S_{1l}, S_{2l},...,S_{hl} is direct. So their product exhausts the group $1+J$.

Suppose p is odd.

We notice that for every $l = 1, ..., r$, $(1+p\alpha_l)^{p^{k-1}} = 1$, $(1+\alpha_l u_1)^{p^k} =$

1, $(1+\alpha_l u_1+\alpha_l u_2)^{p^k}=1$,...,$(1+\alpha_l u_1+\alpha_l u_2+...+\alpha_l u_h)^{p^k}=1$.

Now, for positive integers $a_l, b_{1l}, b_{2l}, ..., b_{hl}$ with $a_l \leq p^{k-1}$, $b_{il} \leq p^k$ for $1 \leq i \leq h$, we notice that

$$\prod_{l=1}^{r}\{(1+p\alpha_l)^{a_l}\}.\prod_{l=1}^{r}\{(1+\alpha_l u_1)^{b_{1l}}\}.$$
$$\prod_{l=1}^{r}\{(1+\alpha_l u_1+\alpha_l u_2)^{b_{2l}}\}...\prod_{l=1}^{r}\{(1+\alpha_l u_1+\alpha_l u_2+...+\alpha_l u_h)^{b_{hl}}\}=1$$

will imply $a_l = p^{k-1}$, $b_{il} = p^k$, for every $l = 1, ..., r$ and $1 \leq i \leq h$.

If we set

$$T_l = \{(1+p\alpha_l)^a \mid a = 1, ..., p^{k-1}\},$$

$$S_{1l} = \{(1+\alpha_l u_1)^{b_1} \mid b_1 = 1, ..., p^k\},$$

$$S_{2l} = \{(1+\alpha_l u_1+\alpha_l u_2)^{b_2} \mid b_2 = 1, ..., p^k\}$$

$$\vdots$$

$$S_{hl} = \{(1+\alpha_l u_1+\alpha_l u_2+...+\alpha_l u_h)^{b_h} \mid b_h = 1, ..., p^k\}$$

we see that T_l, S_{1l}, S_{2l},...,S_{hl} are all cyclic subgroups of the group $1+J$ and they are of the orders indicated by their definition. Since

$$\prod_{l=1}^{r}|<1+p\alpha_l>|.\prod_{l=1}^{r}|<1+\alpha_l u_1>|.$$
$$\prod_{l=1}^{r}|<1+\alpha_l u_1+\alpha_l u_2>|...\prod_{l=1}^{r}|<1+\alpha_l u_1+\alpha_l u_2+...+\alpha_l u_h>|$$
$$=p^{(k(h+1)-1)r}$$

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}, S_{2l},...,S_{hl} is direct. So their product exhausts the group $1+J$. □

We have thus proved the following:

Theorem 4.4.7. *The unit group R^* of the commutative completely primary finite ring R of characteristic p^k in Construction A with maximal ideal J such that $J^{k+1}=(0)$ and $J^k \neq (0)$, with invariants p, k, r and h where $p \in J$, is a direct product of cyclic groups as follows:*

i) If $h \geq 1$, $r \geq 1$ and $\operatorname{char} R = p$, *then*

$$R^* \cong \boldsymbol{Z}_{p^r-1} \times \underbrace{\boldsymbol{Z}_p^r \times \ldots \times \boldsymbol{Z}_p^r}_{h \text{ copies}}$$

ii)If $h \geq 1$, $r \geq 1$ and $\operatorname{char} R = p^2$, *then*

$$R^* \cong \boldsymbol{Z}_{p^r-1} \times \boldsymbol{Z}_p^r \times \underbrace{\boldsymbol{Z}_{p^2}^r \times \ldots \times \boldsymbol{Z}_{p^2}^r}_{h \text{ copies}}$$

iii) If $h \geq 1$, $r \geq 1$ and $\operatorname{char} R = p^k; k \geq 3$, *then*

$$R^* \cong \begin{cases} \boldsymbol{Z}_{2^r-1} \times \boldsymbol{Z}_2 \times \boldsymbol{Z}_{2^{k-2}} \times \boldsymbol{Z}_{2^{k-1}}^{r-1} \times \underbrace{\boldsymbol{Z}_{2^k}^r \times \ldots \times \boldsymbol{Z}_{2^k}^r}_{h \text{ copies}} & \text{if } p = 2 \\ \\ \boldsymbol{Z}_{p^r-1} \times \boldsymbol{Z}_{p^{k-1}}^r \times \underbrace{\boldsymbol{Z}_{p^k}^r \times \ldots \times \boldsymbol{Z}_{p^k}^r}_{h \text{ copies}} & \text{if } p \text{ is odd} \end{cases}$$

Proof. Follows from Propositions 4.2.4, 4.3.6, and 4.4.6 □

Let

$$(r_0, r_1), (s_0, s_1), (t_0, t_1) \in R.$$

Then

$$
\begin{aligned}
&(r_0, r_1)((s_0, s_1)(t_0, t_1))\\
&\quad = (r_0, r_1)(s_0t_0 + p^{k-1}s_1t_1, s_0t_1 + s_1t_0)\\
&\quad = (r_0s_0t_0 + p^{k-1}r_0s_1t_1 + p^{k-1}r_1s_0t_1 + p^{k-1}r_1s_1t_0, r_0s_0t_1 + r_0s_1t_0 + r_1s_0t_0 + p^{k-1}r_1s_1t_1)\\
&\quad = (r_0s_0 + p^{k-1}r_1s_1, r_0s_1 + r_1s_0)(t_0, t_1)\\
&\quad = ((r_0, r_1)(s_0, s_1))(t_0, t_1).
\end{aligned}
$$

showing that multiplication is associative.

Moreover,

$$
\begin{aligned}
&((r_0, r_1) + (s_0, s_1))(t_0, t_1)\\
&\quad = (r_0 + s_0, r_1 + s_1)(t_0, t_1)\\
&\quad = (r_0t_0 + s_0t_0 + p^{k-1}r_1t_1 + p^{k-1}s_1t_1, r_0t_1 + s_0t_1 + r_1t_0 + s_1t_0)\\
&\quad = (r_0t_0 + p^{k-1}r_1t_1, r_0t_1 + r_1t_0) + (s_0t_0 + p^{k-1}s_1t_1, s_0t_1 + s_1t_0)\\
&\quad = (r_0, r_1)(t_0, t_1) + (s_0, s_1)(t_0, t_1)
\end{aligned}
$$

and

$$
\begin{aligned}
&(r_0, r_1)((s_0, s_1) + (t_0, t_1)) \\
&\qquad = (r_0, r_1)(s_0 + t_0, s_1 + t_1) \\
&\qquad = (r_0s_0 + r_0t_0 + p^{k-1}r_1s_1 + p^{k-1}r_1t_1, r_0s_1 + r_0t_1 + r_1s_0 + r_1t_0) \\
&\qquad = (r_0s_0 + p^{k-1}r_1s_1, r_0s_1 + r_1s_0) + (r_0t_0 + p^{k-1}r_1t_1, r_0t_1 + r_1t_0) \\
&\qquad = (r_0, r_1)(s_0, s_1) + (r_0, r_1)(t_0, t_1).
\end{aligned}
$$

Therefore, multiplication is both left and right distributive over addition . Hence the multiplication turns the additive abelian group into a ring with identity $(1, 0)$.

The ring is commutative because

$$
\begin{aligned}
&(r_0, r_1)(s_0, s_1) \\
&\qquad = (r_0s_0 + p^{k-1}r_1s_1, r_0s_1 + r_1s_0) \\
&\qquad = (s_0r_0 + p^{k-1}s_1r_1, s_0r_1 + s_1r_0) \\
&\qquad = (s_0, s_1)(r_0, r_1).
\end{aligned}
$$

□

Remark: In order to simplify our work, we shall write

$$
\begin{aligned}
R &= R_0 \oplus R_0u \\
&\quad = \{a + bu \mid a, b \in R_0,\ u^2 = 0\}
\end{aligned}
$$

Proposition 5.1.2. *Let $k \geq 3$. Then the ring R is of characteristic p^k, and satisfies the following conditions:*

(i) $J = pR_0 \oplus R_0u$

(ii) $J^k = p^kR_0 \oplus p^{k-1}R_0u$

(iii) $J^{k+1} = (0)$

Proof. First, we show that char $R = p^k$, for some prime p and $k \geq 3$.

Since char $R_0 = p^k$, then for every $y \in R_0$, $p^ky = 0$. But

$$R = \{y_0 + y_1u \mid y_0, y_1 \in R_0,\ u^2 = 0\}.$$

Now, suppose $p^s \in R$ where $s < k$ and y_0 is not a member of pR_0. Then, by the distributive property in R,

$$p^s(y_0 + y_1u) = p^sy_0 + p^sy_1u \neq 0.$$

The same argument holds for any positive integer less than p^k. So char $R = p^k$.

With the obvious identifications, we can think of R_0 as a subset of R. It follows immediately from the way multiplication has been defined that if

$$J = pR_0 \oplus R_0u,$$

then

$$J^k = p^k R_0 \oplus p^{k-1} R_0 u$$

and that

$$J(p^k R_0 \oplus p^{k-1} R_0 u) = (p^k R_0 \oplus p^{k-1} R_0 u)J = (0).$$

Hence

$$J^{k+1} = (0).$$

We now show that J is indeed $pR_0 \oplus R_0 u$.

Let $\alpha \in R_0$, with α not a member of pR_0 and $s \in J$. We have

$$(\alpha + s)^{p^r} = \alpha^{p^r} + t \text{ (with } t \in J)$$

$$= \alpha + v \text{ (with } v \in J).$$

But then $(\alpha + v)^{p-1} = 1 + q$ (with $q \in J$) and $(1+q)^{p^{k-1}} = 1$. Hence $\alpha + s$ is invertible. Since $\mid J \mid= p^{(2k-1)r}$ and $\mid (R_0/pR_0)^* + J \mid= (p^r - 1)p^{(2k-1)r}$. It follows that $(R_0/pR_0)^* + J = R - J$ and hence all the elements outside J are invertible.

□

Remarks: From the definition of multiplication, it follows that $RJ = JR \subseteq J$ so that J is an ideal. Suppose there is an ideal $K \supseteq J$, then by Theorem 1.2.1, K contains a unit $z \in R$ such that

$zz^{-1} = z^{-1}z = 1$. So $K = R$. Therefore J is the unique maximal ideal in R since any maximal ideal distinct from J contains a unit.

5.2 Units of rings of characteristic p^k where $k \geq 3$.

We begin with the case when $r = 1$.

Let $R = \mathbf{Z}_{p^k} \oplus \mathbf{Z}_{p^k}u$, then $J = p\mathbf{Z}_{p^k} \oplus \mathbf{Z}_{p^k}u$. Also $\mid R^* \mid = (p-1)p^{2k-1}$.

Now $1 + J$ is a normal subgroup of R^* and $\mid 1 + J \mid = p^{2k-1}$. So R^* is a direct product of a subgroup of R^* say A, of order $p - 1$ by $1 + J$. Then $R^* = A \times (1 + J) \cong \mathbf{Z}_{p-1} \times (1 + J)$ a direct product.

We proceed to determine the structure of $1 + J$.

The following Lemmata are useful in the determination of the structure of $1 + J$.

Lemma 5.2.1. *For every prime p, $1 + p\mathbf{Z}_{p^k}$ is a subgroup of $1 + J$.*

Proof. Let $1 + pr_1, 1 + pr_2 \in 1 + p\mathbf{Z}_{p^k}$ where $r_1, r_2 \in \mathbf{Z}_{p^k}$.

Since $p^k r_2 = 0$,

then $(1 + pr_2)^{-1} = 1 - pr_2 + p^2r_2^2 - p^3r_2^3 + ... + (-1)^{k+1}p^{k-1}r_2^{k-1}$.

So

$$\begin{aligned}
&(1+pr_1)(1+pr_2)^{-1} \\
&= (1+pr_1)(1-pr_2+p^2r_2^2-p^3r_2^3+...+(-1)^{k+1}p^{k-1}r_2^{k-1}) \\
&= 1-pr_2+p^2r_2^2-p^3r_2^3+...+(-1)^{k+1}p^{k-1}r_2^{k-1}+pr_1 \\
&\quad -p^2r_1r_2+p^3r_1r_2^2-p^4r_1r_2^3+...+(-1)^kp^{k-1}r_2^{k-2}r_1 \\
&= 1+p((r_1-r_2)+p(r_2^2-r_1r_2)+p^2(r_1r_2^2-r_2^3)+p^3 \\
&\quad (r_2^4-r_1r_2^3)+...+p^{k-2}((-1)^{k+1}r_2^{k-1}+(-1)^kr_1r_2^{k-2}))
\end{aligned}$$

an element of $1+p\mathbf{Z}_{p^k}$ □

Lemma 5.2.2. *For each prime p, $1+p^{k-1}\mathbf{Z}_{p^k}\oplus\mathbf{Z}_{p^k}u$ is a subgroup of $1+J$.*

Proof. Let $1+p^{k-1}r_1+r_2u$, $1+p^{k-1}s_1+s_2u$ belong to $1+p^{k-1}\mathbf{Z}_{p^k}\oplus\mathbf{Z}_{p^k}u$ where $r_1,r_2,s_1,s_2\in\mathbf{Z}_{p^k}$.

Case I: Let $s_2 \in (\mathbf{Z}_{p^k})^*$. Then

$$\begin{aligned}
&(1+p^{k-1}r_1+r_2u)(1+p^{k-1}s_1+s_2u)^{-1} = (1+p^{k-1}r_1+r_2u)(-(1+p^{k-1}s_1)^{-1}\\
&\quad(p^{k-1}s_2(1+p^{k-1}s_1)^{-1}-s_2^{-1}(1+p^{k-1}s_1))^{-1}s_2^{-1}(1+p^{k-1}s_1)+\\
&\quad((1+p^{k-1}s_1)^{-1} \quad (p^{k-1}s_2(1+p^{k-1}s_1)^{-1}-s_2^{-1}(1+p^{k-1}s_1))^{-1})u)\\
&\quad= \quad (1+p^{k-1}r_1+r_2u)(-(p^{k-1}s_2^2-(1+p^{k-1}s_1))^{-1}+((p^{k-1}s_2-s_2^{-1}(1+p^{k-1}s_1)^2)^{-1})u)\\
&\quad= \quad (1+p^{k-1}r_1+r_2u)((1-p^{k-1}s_1+p^{k-2}s_2^2)+(s_2(-1+2p^{k-1}s_1-p^{k-1}s_2^2))u)\\
&\quad= \quad 1-p^{k-1}s_1+p^{k-1}s_2^2+p^{k-1}r_1+p^{k-1}r_2s_2(-1+2p^{k-1}s_1-p^{k-1}s_2^2)+\\
&\qquad((1+p^{k-1}r_1)s_2(-1+2p^{k-1}s_1-p^{k-1}s_2^2)+r_2(1-p^{k-1}s_1+p^{k-1}s_2^2))u\\
&\quad= \quad 1+p^{k-1}(r_1+s_2^2-s_1-r_2s_2)+(r_2-s_2+p^{k-1}(2s_1s_2+r_2s_2^2-s_1r_2-r_1s_2-s_2^3))u
\end{aligned}$$

which is an element of $1+p^{k-1}\mathbf{Z}_{p^k}\oplus\mathbf{Z}_{p^k}u$

Case II: Let $s_2 \in p\mathbf{Z}_{p^k}$ then

$$\begin{aligned}
&(1+p^{k-1}r_1+r_2u)(1+p^{k-1}s_1+s_2u)^{-1}\\
&\quad=(1+p^{k-1}r_1+r_2u)((1+p^{k-1}s_1)^{-1}+(-s_2(1+p^{k-1}s_1)^{-2})u)\\
&\quad=(1+p^{k-1}r_1)(1+p^{k-1}s_1)^{-1}+(-s_2(1+p^{k-1}r_1)(1+p^{k-1}s_1)^{-2}+r_2(1+p^{k-1}s_1)^{-1})u\\
&\quad=(1+p^{k-1}r_1)(1-p^{k-1}s_1)+(-s_2(1+p^{k-1}r_1)(1-2p^{k-1}s_1)+r_2(1-p^{k-1}s_1))u\\
&\quad=1+p^{k-1}(r_1-s_1)+(r_2-s_2+p^{k-1}(2s_1s_2-r_1s_2-s_1r_2))u
\end{aligned}$$

an element of $1+p^{k-1}\mathbf{Z}_{p^k}\oplus\mathbf{Z}_{p^k}u$.

Therefore, $1+p^{k-1}\mathbf{Z}_{p^k}\oplus\mathbf{Z}_{p^k}u$ is a subgroup of $1+J$. □

Proposition 5.2.3. *Let*

$$R = Z_{p^k} \oplus Z_{p^k}u$$

be a ring with multiplication defined by

$$(r_1, r_2)(s_1, s_2) = (r_1s_1 + p^{k-1}r_2s_2, r_1s_2 + r_2s_1)$$

Then $R^* \cong Z_{p-1} \times (1 + J)$, *where*

$$1 + J \cong \begin{cases} Z_2 \times Z_{2^{k-2}} \times Z_{2^k}, \text{ if } p = 2 \\ \\ Z_{p^{k-1}} \times Z_{p^k}, \text{ if } p \text{ is odd} \end{cases}$$

Proof. First, we consider the case when $p = 2$.

Let $y \in \mathbf{Z}_{2^k}$ such that y is not a member of $2^{k-1}\mathbf{Z}_{2^k}$. Suppose $y(y + 1) \equiv 0(\text{mod}2^{k-2})$. Then

$$(1 + 2y)^2 = 1 + 2^2y + 2^2y^2$$

$$= 1 + 2^2(y + y^2)$$

$$= 1 + 2^2.2^{k-2}.\alpha \text{ since } y + y^2 = 2^{^{k-2}}\alpha \text{ for some } \alpha \in \mathbf{Z}_{2^k}$$

$$= 1 + 2^k\alpha$$

$$= 1 \text{ since char } R = 2^k$$

Therefore $1 + 2y$ generates a cyclic subgroup of $1 + J$ of order 2.

If $k = 3$, choose $z \in \mathbf{Z}_{2^k}$ such that z is not a member of $2^2\mathbf{Z}_{2^3}$ and $z \neq y$, then $(1 + 2z)^2 = 1$.

Suppose $k > 3$.

Now, let $z \in \mathbf{Z}_{2^k}$, so that z is not a member of $2^{k-1}\mathbf{Z}_{2^k}$ and $z(z+1)$ is not congruent to 0 $(\mathrm{mod} 2^{k-2})$. Then

$$(1+2z)^{2^{k-2}} = \underbrace{(1+2z)(1+2z)...(1+2z)}_{2^{k-2} \text{ factors}}$$

$$= 1 + 2^{k-2}(2z) + \frac{2^{k-2}(2^{k-2}-1)(2z)^2}{2} + \frac{2^{k-2}(2^{k-2}-1)(2^{k-2}-3)(2z)^3}{6} +$$

$$... + (2z)^{2^{k-2}}$$

$$= 1 + 2^{k-1}(z + ((2^{k-2}-1) + \frac{(2^{k-2}-1)(2^{k-2}-2)2z}{3} +$$

$$... + 2^{2^{k-2}-k+1}z^{2^{k-2}-2})z^2)$$

$$= 1 + 2^{k-1}(z + \beta z^2)$$

where $\beta = (2^{k-2}-1) + \frac{(2^{k-2}-1)(2^{k-2}-2)2z}{3} + ... + 2^{2^{k-2}-k+1}z^{2^{k-2}-2}$.

Since $\beta \in \mathbf{Z}_{p^k}$ is odd, and $z(z+1) = 2\alpha$, $\alpha \in \mathbf{Z}_{2^k}$, the element $1 + 2^{k-1}(z + \beta z^2)$ becomes $1 + 2^k\tau = 1$, for some $\tau \in \mathbf{Z}_{2^k}$. Thus $1 + 2z$ generates a cyclic subgroup of $1 + J$ of order 2^{k-2}.

Now, let $w \in \mathbf{Z}_{2^k}$, $s \in (\mathbf{Z}_{2^k})^*$. Then

$$(1 + 2^{k-1}w + su)^2 = (1 + 2^{k-1}w + su)(1 + 2^{k-1}w + su)$$

$$= 1 + 2^{k-1}s^2 + 2su \text{ (since char } R = 2^k \text{ and } u^2 = 0)$$

$$(1+2^{k-1}s^2+2su)^2 = (1+2^{k-1}s^2+2su)(1+2^{k-1}s^2+2su)$$

$$= (1+2^{k-1}.2^2.s^2+2^2su) \text{ (since char } R = 2^k \text{ and } u^2=0)$$

$$= 1+2^{k+1}s^2+2^2su$$

$$= 1+2^2su \text{ (since char } R = 2^k)$$

and

$$(1+2^2su)^2 = (1+2^2su)(1+2^2su)$$

$$= 1+2^3su \text{ (since char } R = 2^k \text{ and } u^2=0).$$

Continuing inductively

$$(1+2^{k-1}w+su)^{2^k} = (1+2^{k-1}su)^2$$

$$= (1+2^{k-1}su)(1+2^{k-1}su)$$

$$= 1+2^ksu \text{ (since char } R = 2^k \text{ and } u^2=0)$$

$$= 1 \text{ (since char } R = 2^k \text{ and } 2^ku=0)$$

Therefore, $1+2^{k-1}w+su$ generates a cyclic subgroup of $1+J$ of order 2^k. Since $1+J$ is abelian, all the cyclic subgroups are normal. Moreover, the order of the group generated by the direct product of $< 1+2y >$, $< 1+2z >$ and $< 1+2^{k-1}w+su >$ coincides with $\mid 1+J \mid$ and the intersection of any pair of the subgroups is the identity group. So the direct product of the cyclic subgroups exhausts $1+J$. This proves part (i).

We now consider the case when p is odd.

Let $s \in (\mathbf{Z}_{p^k})^*$. Then

$$(1+ps)^{p^{k-1}} = \underbrace{(1+ps)...(1+ps)}_{p^{k-1} \text{ factors}}$$

$$= (1+p^{k-1}(ps) + \frac{(p^{k-1})(p^{k-1}-1)(ps)^2}{2} + \frac{p^{k-1}(p^{k-1}-1)(p^{k-1}-2)(ps)^3}{6}$$

$$+ ... + (ps)^{p^{k-1}})$$

$$= (1+p^k(s + \frac{p(p^{k-1}-1)s^2}{2} + \frac{p^2(p^{k-1}-1)(p^{k-1}-2)s^3}{6} + ... + p^{p^{k-1}-k}s^{p^{k-1}}))$$

$$= 1+p^k t$$

where $t = s + \frac{p(p^{k-1}-1)s^2}{2} + \frac{p^2(p^{k-1}-1)(p^{k-1}-2)s^3}{6} + ... + p^{p^{k-1}-k}s^{p^{k-1}} \in \mathbf{Z}_{p^k}$. So

$$1+p^k t = 1$$

Therefore, $1+ps$ generates a cyclic subgroup of $1+J$ of order p^{k-1}.

Now, let $w \in \mathbf{Z}_{p^k}$ and $s \in (\mathbf{Z}_{p^k})^*$. Then

$$(1+p^{k-1}w+su)^p = \underbrace{(1+p^{k-1}w+su)...(1+p^{k-1}w+su)}_{p \text{ factors}}$$

$$= 1+(ps+\kappa p^{k-1}s^{k-1})u, \text{ with } \kappa \in \{0,1\}$$

and

$$(1+(ps+\kappa p^{k-1}s^{k-1})u)^p = 1+p^2 su$$

$$(1 + p^2 su)^p = 1 + p^3 su$$

since char $R = p^k$ and $u^2 = 0$.

Continuing inductively,

$$(1 + p^{k-1} w + su)^{p^k} = (1 + p^{k-1} su)^p = 1 + p^k su = 1$$

since char$R = p^k$ and $u^2 = 0$. Thus $1 + p^{k-1}w + su$ generates a cyclic subgroup of $1+J$ of order p^k. Moreover, the order of the group generated by the direct product of $< 1+ps >$ and $< 1+p^{k-1}w+su >$ coincides with $\mid 1 + J \mid$ and their intersection is the identity group. So the direct product of the cyclic subgroups exhausts $1 + J$. This proves part (ii) and completes the proof. □

We now obtain the generalized result by considering the case when r is any positive integer. Let R be a commutative completely primary finite ring with maximal ideal J such that $J^{k+1} = (0)$ and $J^k \neq (0)$. Then R is of order p^{2kr} and the residue field R/J is the finite field $GF(p^r)$ for some prime integer p and positive integer r. The characteristic of R is p^k, where $k \geq 3$. We notice that since R is of order p^{2kr} and $R^* = R - J$, then $\mid R^* \mid = p^{(2k-1)r}(p^r - 1)$ and $\mid 1 + J \mid = p^{(2k-1)r}$ is an abelian $p-$ group. Thus

$R^* \cong$(abelian $p-$ group)×(cyclic group of order $\mid R/J \mid -1$).

We now proceed to determine the structure of $1+J$.

We notice that $1+J = 1+pR_0 \oplus R_0u$.

Lemma 5.2.4. *For every prime integer p, $1+pR_0$ is a subgroup of $1+J$.*

Proof. Similar to the proof of Proposition 5.2.1 with some modifications. □

Lemma 5.2.5. *For every prime integer p, $1+p^{k-1}R_0 \oplus R_0u$ is a subgroup of $1+J$.*

Proof. Similar to the proof of Proposition 5.2.2 with some modifications. □

Proposition 5.2.6. *Let $R = R_0 \oplus R_0u$ be a commutative finite ring with multiplication defined by $(r_0, r_1)(s_0, s_1) = (r_0s_0 + p^{k-1}r_1s_1, r_0s_1 + r_1s_0)$. If* $\text{char}R = p^k$; $k \geq 3$ *and J is the radical of R, then $R^* \cong \boldsymbol{Z}_{p^r-1} \times (1+J)$, where*

$$1+J \cong \begin{cases} \boldsymbol{Z}_2 \times \boldsymbol{Z}_{2^{k-2}} \times \boldsymbol{Z}_{2^{k-1}}^{r-1} \times \boldsymbol{Z}_{2^k}^{r}, & \text{if } p = 2 \\ \boldsymbol{Z}_{p^{k-1}}^{r} \times \boldsymbol{Z}_{p^k}^{r}, & \text{if } p \text{ is odd} \end{cases}$$

Proof. Given $\mid R \mid = p^{2kr}$ and $R^* = R - J$, then

$$\mid R^* \mid = p^{(2k-1)r}(p^r - 1),$$

and$|\ 1+J\ |= p^{(2k-1)r}$. Now the quotient group $R^*/(1+J) \cong (\mathbf{F}_{p^r})^*$, and since,

$$|\ R^*\ |=|\ R^*/1+J\ ||\ 1+J\ |,$$

it follows that $R^* \cong \mathbf{Z}_{p^r-1} \times (1+J)$.

We now determine the structure of $1+J$.

Let $\alpha_1, ..., \alpha_r \in R_0$ with $\alpha_1 = 1$ such that $\overline{\alpha_1}, ..., \overline{\alpha_r} \in R_0/pR_0$ form a basis for R_0/pR_0 regarded as a vector space over its prime subfield $\mathbf{F}_p$. We consider the two cases separately.

Suppose $p = 2$.

If $l = 1, ..., r$ and y is an element of R_0 such that $x^2 + x + \overline{y} = \overline{0}$ over R_0/pR_0, has no solution in the field R_0/pR_0, we obtain the following results: $(-1 + 2^{k-1}\alpha_1) \in 1 + pR_0$, $(-1 + 2^{k-1}\alpha_1)^2 = 1$, $(1+4y)^{2^{k-2}} = 1$ and $w^{2^{k-1}} = 1$ for every $w \in 1 + pR_0$. We also notice that $(1+2\alpha_l)^{2^{k-1}} = 1$ for $l = 2, ..., r$, $(1+2^{k-1}z+\alpha_l u)^{2^k} = 1$, for every $l = 1, ..., r$ and $z \in R_0$.

Now, for positive integers a, b, c_l, d_l with $a \leq 2$, $b \leq 2^{k-2}$, $c_l \leq 2^{k-1}$ for $l = 2, ..., r$ and $d_l \leq 2^k$ for every $l = 1, ..., r$, we notice that the equation

$$(-1+2^{k-1}\alpha_1)^a.(1+4y)^b.\prod_{l=2}^{r}\{(1+2\alpha_l)^{c_l}\}.\prod_{l=1}^{r}\{(1+2^{k-1}z+\alpha_l u)^{d_l}\} = 1.$$

will imply $a = 2$, $b = 2^{k-2}$, $c_l = 2^{k-1}$ for $l = 2, ..., r$ and $d_l = 2^k$ for every $l = 1, ..., r$.

If we set

$$H = \{(-1 + 2^{k-1}\alpha_1)^a \mid a = 1, 2\},$$

$$Q = \{(1 + 4y)^b \mid b = 1, ..., 2^{k-2}\},$$

$$T_l = \{(1 + 2\alpha_l)^c \mid c = 1, ..., 2^{k-1}\}$$

for $l = 2, ..., r$ and

$$S_l = \{(1 + 2^{k-1}z + \alpha_l u)^d \mid d = 1, ..., 2^k\},$$

we see that H, Q, T_l, S_l, are all cyclic subgroups of the group $1 + J$ and they are of the orders indicated by their definition. Since

$$|< -1+2^{k-1}\alpha_l >| \,.\, |< 1+4y >| \,.\, \prod_{l=2}^{r} |< 1+2\alpha_l >| \,.\, \prod_{l=1}^{r} |< 1+2^{k-1}z+\alpha_l u >|= 2^{(2k-1)r}.$$

and the intersection of any pair of the cyclic subgroups gives the identity group, the product of the $2r + 1$ subgroups H, Q, T_l, S_l, is direct. So their product exhausts the group $1 + J$.

Suppose p is odd.

We notice that, for every $l = 1, ..., r$ and $z \in R_0$, $(1 + p\alpha_l)^{p^{k-1}} = 1$ and $(1 + p^{k-1}z + \alpha_l u)^{p^k} = 1$.

Now, for positive integers a_l and b_l with $a_l \leq p^{k-1}$ and $b_l \leq p^k$, we notice that the equation

$$\prod_{l=1}^{r}\{(1+p\alpha_l)^{a_l}\}.\prod_{l=1}^{r}\{(1+p^{k-1}z+\alpha_l u)^{b_l}\}=1$$

will imply $a_l = p^{k-1}$ and $b_l = p^k$, for every $l = 1, ..., r$.

If we set

$$Q_l = \{(1+p\alpha_l)^a \mid a = 1, ..., p^{k-1}\}$$

and

$$T_l = \{(1+p^{k-1}z+\alpha_l u)^b \mid b = 1, ..., p^k\}$$

we see that Q_l and T_l are cyclic subgroups of the group $1+J$ and they are of the orders indicated by their definition.

Since

$$\prod_{l=1}^{r} |< 1+p\alpha_l >| \,.\prod_{l=1}^{r} |< 1+p^{k-1}z+\alpha_l u >|= p^{(2k-1)r}$$

and the intersection of any pair of the cyclic subgroups gives the identity group, the product of the $2r$ subgroups Q_l and T_l is direct. So their product exhausts the group $1+J$. □

5.3 Units of a finite ring R such that $J^{k+2} = (0)$ and $J^{k+1} \neq (0)$

We now study the structure of the group of units of a class of rings given by construction B but satisfies the following properties:

(i) J is a unique maximal ideal

(ii) $J^{k+1} \neq (0)$

(iii) $J^{k+2} = (0)$.

Let $R_0 = GR(p^{2r}, p^2)$. Consider the additive group $R_0 \oplus R_0 u$ where $u \in R$ with multiplication defined by $(r_0, r_1)(s_0, s_1) = (r_0 s_0 + p r_1 s_1, r_0 s_1 + r_1 s_0)$. It can be shown that this multiplication turns the additive group into a ring.

We now prove some properties satisfied by R.

Proposition 5.3.1. *Let $k = 2$. Then the ring $R = R_0 \oplus R_0 u$ is of characteristic p^2 and*

i) $J = pR_0 \oplus R_0 u$

ii) $J^2 = pR_0 \oplus pR_0 u$

iii) $J^3 = p^2 R_0 \oplus pR_0 u$

iv) $J^4 = (0)$

Proof. First, we show that char $R = p^2$, for some prime p.

Since char $R_0 = p^2$, then for every $y \in R_0$, $p^2 y = 0$. But

$$R = \{y_0 + y_1 u \mid y_0, y_1 \in R_0,\ u^2 = 0\}.$$

Now, suppose $p^s \in R$ where $s = 1$ and y_0 is not a member of pR_0. Then, by the distributive property in R,

$$p(y_0 + y_1 u) = py_0 + py_1 u \neq 0.$$

A similar argument holds for any positive integer less than p^2. So char $R = p^2$.

With the obvious identifications, we can think of R_0 as a subset of R. It follows immediately from the way multiplication has been defined that if

$$J = pR_0 \oplus R_0 u,$$

then

$$J^2 = pR_0 \oplus pR_0 u.$$

Also

$$J^3 = p^2 R_0 \oplus pR_0 u,$$

and that

$$J(p^2 R_0 \oplus pR_0 u) = (p^2 R_0 \oplus pR_0 u)J = (0).$$

Hence

$$J^4 = (0).$$

The proof that J is indeed $pR_0 \oplus R_0u$ is similar to Proposition 5.1.2 □

Now, we determine the structure of the group of units of the ring defined in this section.

We begin with the case when $r = 1$.

Given $R = \mathbf{Z}_{p^2} \oplus \mathbf{Z}_{p^2}u$, then by the multiplication given in Construction B, $J = p\mathbf{Z}_{p^2} \oplus \mathbf{Z}_{p^2}u$. Also

$$\mid R^* \mid = p^3(p-1)$$

and $\mid 1 + J \mid = p^3$. So R^* is a direct product of a subgroup, say A of order $p-1$ by $1+J$, that is

$$R^* = A \times (1+J) \cong \mathbf{Z}_{p-1} \times (1+J),$$

a direct product. The following Lemmata are useful in the determination of the structure of $1+J$.

Lemma 5.3.2. *For each prime p, $1 + p\mathbf{Z}_{p^2}$ is a subgroup of $1 + J$.*

Proof. Let $1 + py_1, 1 + py_2 \in 1 + p\mathbf{Z}_{p^2}$, $y_1, y_2 \in \mathbf{Z}_{p^2}$. We note that

$(1+py_2)^{-1} = 1 - py_2$ because $p^2y_2 = 0$ for every $y_2 \in \mathbf{Z}_{p^2}$. So

$$\begin{aligned}
&(1+py_1)(1+py_2)^{-1}\\
&\quad = (1+py_1)(1-py_2)\\
&\quad = 1 + p(y_1 - y_2)
\end{aligned}$$

an element of $1 + p\mathbf{Z}_{p^2}$. □

Lemma 5.3.3. *For each prime p, $1+p\mathbf{Z}_{p^2} \oplus \mathbf{Z}_{p^2}u$ is a subgroup of $1+J$.*

Proof. It follows from the fact that $J = p\mathbf{Z}_{p^2} \oplus \mathbf{Z}_{p^2}u$. □

Proposition 5.3.4. *Let $R = \mathbf{Z}_{p^2} \oplus \mathbf{Z}_{p^2}u$ be a ring with multiplication defined by $(r_1, r_2)(s_1, s_2) = (r_1s_1 + pr_2s_2, r_1s_2 + r_2s_1)$. Then $R^* \cong \mathbf{Z}_{p-1} \times (1+J)$ where $1+J \cong \mathbf{Z}_p \times \mathbf{Z}_{p^2}$ for any prime p.*

Proof. Since R is commutative,

$$R^* \cong \mathbf{Z}_{p-1} \times (1+J).$$

It suffices to show that $1+J \cong \mathbf{Z}_p \times \mathbf{Z}_{p^2}$ for any prime p.

For each $z \in (\mathbf{Z}_{p^2})^*$, let $1+pz \in 1+p\mathbf{Z}_{p^2}$. Then $(1+pz)^p = 1$ since char $R = p^2$. Therefore, $1+pz$ generates a cyclic subgroup of $1+J$ of order p.

Next, consider the element $1 + zu \in 1 + p\mathbf{Z}_{p^2} + \mathbf{Z}_{p^2}u$, then since char $R = p^2$ and $u^2 = 0$, $(1 + zu)^p = 1 + spz^2 + (pz + tpz^3)u$ where $s = 1$ when $p = 2$, $s \equiv 0(\text{mod } p)$ when p is odd and $t = 1$ when $p = 3$, $t \equiv 0(\text{mod } p)$ when $p \neq 3$.

Also

$$\begin{aligned} &(1 + spz^2 + (pz + tpz^3)u)^p \\ &\quad = 1 + sp^2z^2(p^2z + tp^2z^3)u \\ &\quad = 1 \end{aligned}$$

where again, $s = 1$ when $p = 2$, $s \equiv 0(\text{mod } p)$ when p is odd and $t = 1$ when $p = 3$, $t \equiv 0(\text{mod } p)$ when $p \neq 3$. Therefore $1 + zu$ generates a cyclic subgroup of $1 + J$ of order p^2.

Since $1 + J$ is abelian, the groups generated by $1 + pz$ and $1 + zu$ are normal, the order of the group generated by the direct product of the cyclic subgroups $< 1 + pz >$ and $< 1 + zu >$ coincides with $\mid 1 + J \mid$ and their intersection is the identity group, it follows that

$$1 + J =< 1 + pz > \times < 1 + zu >$$

□

We extend the study of the units of the above ring to the case when r is any positive integer. So, we determine the unit group

R^* of a commutative completely primary finite ring R with unique maximal ideal J such that $R/J \cong GF(p^r)$, $J^4 = (0)$, $J^3 \neq (0)$, so that the characteristic of R is p^2 for every prime integer p and positive integer r.

Let R_0 be the Galois ring of the form $GR(p^{2r}, p^2)$ and let $u \in R$ so that $R = R_0 \oplus R_0u$ is an additive group. On this additive group, define multiplication by $(r_0, r_1)(s_0, s_1) = (r_0s_0 + pr_1s_1, r_0s_1 + r_1s_0)$. It can be verified that R is a commutative finite ring with identity $(1, 0)$

Lemma 5.3.5. *For each prime integer p, $1 + pR_0$ is a subgroup of $1 + J$.*

Lemma 5.3.6. *For each prime integer p, $1 + pR_0 \oplus R_0u$ is a subgroup of $1 + J$.*

Proposition 5.3.7. *Let $R = R_0 \oplus R_0u$ be the ring defined in this section. Then $R^* \cong \boldsymbol{Z}_{p^r-1} \times (1 + J)$ where $1 + J \cong \boldsymbol{Z}_p^r \times \boldsymbol{Z}_{p^2}^r$ for any prime integer p.*

Proof. Since $\mid R \mid= p^{4r}$ and $R^* = R - J$, then $\mid R^* \mid= p^{3r}(p^r - 1)$, $\mid 1 + J \mid= p^{3r}$. Now the quotient group $R^*/(1 + J) \cong (\mathbf{F}_{p^r})^*$ and since $\mid R^* \mid=\mid R^*/1+J \mid\mid 1+J \mid$, it follows that $R^* \cong \mathbf{Z}_{p^r-1} \times (1+J)$.

We now determine the structure of $1 + J$.

Let $\alpha_1, ..., \alpha_r \in R_0$ with $\alpha_1 = 1$ such that $\overline{\alpha_1}, ..., \overline{\alpha_r} \in R_0/pR_0$ form a basis for R_0/pR_0 regarded as a vector space over its prime subfield $\mathbf{F}_p$. We note that if $l = 1, ..., r$ then $(1 + p\alpha_l)^p = 1$ and $(1 + \alpha_l u)^{p^2} = 1$.

Now, for positive integers a_l and b_l with $a_l \leq p$ and $b_l \leq p^2$, we notice that the equation

$$\prod_{l=1}^{r}\{(1 + p\alpha_l)^{a_l}\}.\prod_{l=1}^{r}\{(1 + \alpha_l u)^{b_l}\} = 1$$

will imply $a_l = p$ and $b_l = p^2$ for every $l = 1, ..., r$.

If we set

$$Q_l = \{(1 + p\alpha_l)^a \mid a = 1, ..., p\}$$

and

$$T_l = \{(1 + \alpha_l u)^b \mid b = 1, ..., p^2\}$$

we see that Q_l and T_l are all cyclic subgroups of the group $1 + J$ and they are of the orders indicated by their definition. Since

$$\prod_{l=1}^{r} |< 1 + p\alpha_l >| . \prod_{l=1}^{r} |< 1 + \alpha_l u >| = p^{3r}$$

and the intersection of any pair of the cyclic subgroups gives the identity group, the product of the $2r$ subgroups Q_l and T_l is direct. So their product exhausts the group $1 + J$. □

Chapter 6

Structures of Quotient Groups

6.1 Quotient Groups of Rings in Construction A

Let R be a commutative finite ring given by Construction A with maximal ideal J such that $J^{k+1} = (0)$ and $J^k \neq (0)$. Let $1 + J$ be the abelian $p-$ subgroup of the unit group R^*. The group $1+J$ has a filtration

$$1 + J \supset 1 + J^2 \supset 1 + J^3 \supset ... \supset 1 + J^k \supset 1 + J^{k+1} = \{1\},$$

with filtration quotients

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

isomorphic to the additive groups

$$J/J^2, J^2/J^3, ..., J^k$$

respectively.

Remark: Notice that for each $j = 1, 2, ..., k-1$, $1 + J^{j+1}$ is a normal subgroup of $1 + J^j$. But, in general $1 + J^j$ does not have a subgroup which is isomorphic to the quotient $(1 + J^j)/(1 + J^{j+1})$ as may be illustrated by the following example in [4].

Example

Let $R = \mathbf{Z}_{p^3}$, where p is an odd prime. Then $J = p\mathbf{Z}_{p^3}$, $\text{ann}(J) = J^2$ and $1 + J \cong \mathbf{Z}_{p^2}$, $1 + J^2 \cong \mathbf{Z}_p$, $(1 + J)/(1 + J^2) \cong \mathbf{Z}_p$.

Remark: In view of the above remark and example, we investigate the structure of quotient groups of subgroups of $1+J$, where $1+J$ is the subgroup of R^*. We begin by showing that for $j = 1, 2, ..., k-1$, the quotient J^j/J^{j+1} is a vector space over the prime subfield of the quotient ring R/J.

Lemma 6.1.1. *Let J be the Jacobson radical of a ring R defined in Construction A. Then the quotient J^j/J^{j+1}, $j = 1, 2, ..., k-1$ is a vector space over $GF(p) \subseteq R/J$.*

Proof. Given that J is a maximal ideal in R, the quotient ring R/J is a field. For every prime integer p, let $\mathbf{F}_p$ be a prime subfield of R/J. Since J^j is an additive abelian group, the additive subgroup

J^{j+1} is also abelian. Hence J^{j+1} is a normal subgroup of J^j. So the quotient J^j/J^{j+1} is an additive abelian group since J^j is an additive abelian group. To prove the other axioms, let $y_1, y_2 \in J^j$ such that $y_1 + J^{j+1}$ and $y_2 + J^{j+1}$ belong to J^j/J^{j+1}, $a, a_1, a_2 \in \mathbf{F}_p$, then

$$\begin{aligned}
&(a_1 + a_2)(y_1 + J^{j+1}) \\
&\quad = (a_1 + a_2)y_1 + J^{j+1} \\
&\quad = a_1y_1 + a_2y_1 + J^{j+1} \\
&\quad = a_1y_1 + J^{j+1} + a_2y_1 + J^{j+1} \\
&\quad = a_1(y_1 + J^{j+1}) + a_2(y_1 + J^{j+1}).
\end{aligned}$$

Also,

$$\begin{aligned}
&(a_1.a_2)(y_1 + J^{j+1}) \\
&\quad = (a_1.a_2)y_1 + J^{j+1} \\
&\quad = a_1.(a_2y_1 + J^{j+1}) \\
&\quad = a_1(a_2(y_1 + J^{j+1}))
\end{aligned}$$

and

$$\begin{aligned} & a((y_1 + J^{j+1}) + (y_2 + J^{j+1})) \\ & \quad = a((y_1 + y_2) + J^{j+1}) \\ & \quad = (a(y_1 + y_2)) + J^{j+1} \\ & \quad = ay_1 + ay_2 + J^{j+1} \\ & \quad = ay_1 + J^{j+1} + ay_2 + J^{j+1} \\ & \quad = a(y_1 + J^{j+1}) + a(y_2 + J^{j+1}) \end{aligned}$$

Finally

$$1(y_1 + J^{j+1}) = y_1 + J^{j+1}.$$

This completes the proof □

Now,

$$\begin{aligned} \mid R \mid =\mid R/J \mid . \mid J/J^2 \mid ... \mid J^{k-1}/J^k \mid . \mid J^k \mid \\ = p^{(1+\overbrace{(h+1)+...+(h+1)}^{k-1 \text{ times}}+h)r}, h \geq 1 \\ = p^{k(h+1)r} \end{aligned}$$

Thus R is indeed finite.

Remark: Finiteness of R implies that J is nilpotent, say $J^{k+1} = (0)$.

Notice that $1+J^{j+1}$ is a normal subgroup of $1+J^j$ and by Lagrange's theorem $\mid 1+J^j/1+J^{j+1} \mid= p^{(h+1)r}$ where $j=1,...,k-1$. We now determine the structure of $1+J^j/1+J^{j+1}$ for $j=1,2,...,k-1$. We begin with the case when char $R=p^2$.

Proposition 6.1.2. *Let R be a ring defined in Construction A. Suppose J is the Jacobson radical of R, then for $k=2$, the quotient group $1+J/1+J^2 \cong \underbrace{Z_p^r \times ... \times Z_p^r}_{h+1 \text{ copies}}$ for every prime integer p.*

Proof. Let $\alpha_1,...,\alpha_r \in R_0$ such that $\overline{\alpha_1},...,\overline{\alpha_r} \in R_0/pR_0$ form a basis for R_0/pR_0 regarded as a vector space over its prime subfield $\mathbf{F}_p$. Consider the element $(1+p\alpha_l)1+J^2 \in 1+J/1+J^2$. Then

$$((1+p\alpha_l)1+J^2)^p = (1+p\alpha_l)^p 1+J^2$$

$$= (1+p^2\alpha_l+...+p^p{\alpha_l}^p)1+J^2$$

$$= 1+J^2 \text{ since char} R = p^2$$

Next, consider the element $(1+\alpha_l u_1)1+J^2 \in 1+J/1+J^2$. Then

$$((1+\alpha_l u_1)1+J^2)^p = (1+\alpha_l u_1)^p 1+J^2$$

$$= (1+p\alpha_l u_1)1+J^2$$

$$= 1+J^2 \text{ since } 1+p\alpha_l u_1 \in 1+J^2$$

Similarly, $((1+\alpha_l u_1+\alpha_l u_2)1+J^2)^p = 1+J^2$. Continuing in a similar manner up to the element $(1+\alpha_l u_1+\alpha_l u_2+...+\alpha_l u_h)1+J^2$,we obtain $((1+\alpha_l u_1+\alpha_l u_2+...+\alpha_l u_h)1+J^2)^p = 1+J^2$.

For positive integers a_l, b_{1l}, b_{2l},...,b_{hl} with $a_l \leq p$, $b_{il} \leq p$ where $1 \leq i \leq h$, we notice that the equation

$$\prod_{l=1}^{r}\{((1+p\alpha_l)1+J^2)^{a_l}\}.\prod_{l=1}^{r}\{(1+\alpha_l u_1)1+J^2)^{b_{1l}}\}.\prod_{l=1}^{r}\{(1+\alpha_l u_1+\alpha_l u_2)$$

$$1+J^2)^{b_{2l}}\}...\prod_{l=1}^{r}\{((1+\alpha_l u_1+\alpha_l u_2+...+\alpha_l u_h)1+J^2)^{b_{hl}}\} = 1+J^2$$

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

If we set

$$T_l = \{((1+p\alpha_l)1+J^2)^a \mid a = 1,...,p\},$$

$$S_{1l} = \{((1+\alpha_l u_1)1+J^2)^{b_1} \mid b_1 = 1,...,p\},$$

$$S_{2l} = \{((1+\alpha_l u_1+\alpha_l u_2)1+J^2)^{b_2} \mid b_2 = 1,...,p\}$$

$$\vdots$$

$$S_{hl} = \{((1+\alpha_l u_1+\alpha_l u_2+...+\alpha_l u_h)1+J^2)^{b_h} \mid b_h = 1,...,p\}$$

we see that T_l, S_{1l}, S_{2l},...,S_h are all cyclic subgroups of the group $1+J/1+J^2$ and they are of the orders indicated by their definition.

Since

$$\prod_{l=1}^{r} |< (1+p\alpha_l)1 + J^2 >| . \prod_{l=1}^{r} |< (1+\alpha_l u_1)1 + J^2 >| .$$
$$\prod_{l=1}^{r} |< (1+\alpha_l u_1 + \alpha_l u_2)1 + J^2 >|$$
$$\ldots \prod_{l=1}^{r} |< (1+\alpha_l u_1 + \alpha_l u_2 + \ldots + \alpha_l u_h)1 + J^2 >|$$
$$= p^{(h+1)r}$$

and the intersection of any pair of the cyclic subgroups gives the identity group $1+J^2$, the product of the $(h+1)r$ subgroups T_l, S_{1l}, S_{2l},...,S_{hl} is direct. So their product exhausts the group $1+J/1+J^2$. □

Proposition 6.1.3. *Let R be a ring defined in Construction A. Suppose J is the Jacobson radical of R, then for $k \geq 3$, the quotient group $1+J^j/1+J^{j+1} \cong \underbrace{\boldsymbol{Z}_p^r \times \ldots \times \boldsymbol{Z}_p^r}_{h+1 \text{ copies}}$ for every prime integer p.*

Proof. Let $\alpha_1, \ldots, \alpha_r \in R_0$ such that $\overline{\alpha_1}, \ldots, \overline{\alpha_r} \in R_0/pR_0$ form a basis for R_0/pR_0 regarded as a vector space over its prime subfield $\mathbf{F}_p$.

Suppose $j=1$.

Then the proof is essentially of Proposition 6.1.2.

Suppose $j \geq 2$.

Consider the element $(1+p^j\alpha_l)1+J^{j+1} \in 1+J^j/1+J^{j+1}$. Then

$$
\begin{aligned}
((1+p^j\alpha_l)1+J^{j+1})^p &= (1+p^j\alpha_l)^p 1+J^{j+1} \\
&= 1(1+J^{j+1}) \\
&= 1+J^{j+1}
\end{aligned}
$$

Next, consider the element $(1+p^{j-1}\alpha_l u_1)1+J^{j+1} \in 1+J^j/1+J^{j+1}$.

Then

$$
\begin{aligned}
((1+p^{j-1}\alpha_l u_1)1+J^{j+1})^p &= (1+p^{j-1}\alpha_l u_1)^p 1+J^{j+1} \\
&= (1+p^j\alpha_l u_1)1+J^{j+1} \\
&= 1+J^{j+1} \text{ since } 1+p^j\alpha_l u_1 \in 1+J^{j+1}.
\end{aligned}
$$

Similarly, $((1+p^{j-1}\alpha_l u_1+p^{j-1}\alpha_l u_2)1+J^{j+1})^p = 1+J^{j+1}$. Continuing in a similar manner up to the element $(1+p^{j-1}\alpha_l u_1+p^{j-1}\alpha_l u_2+ \ldots +p^{j-1}\alpha_l u_h)1+J^{j+1}$ we obtain $((1+p^{j-1}\alpha_l u_1+p^{j-1}\alpha_l u_2+\ldots+ p^{j-1}\alpha_l u_h)1+J^{j+1})^p = 1+J^{j+1}$.

Now, for positive integers a_l, b_{1l},...,b_{hl} with $a_l \leq p$, $b_{il} \leq p$ for every

$l = 1, ..., r$ and $1 \leq i \leq h$, we notice that the equation

$$\begin{aligned}&\prod_{l=1}^{r}\{((1+p^{j}\alpha_l)1+J^{j+1})^{a_l}\}.\prod_{l=1}^{r}\{((1+p^{j-1}\alpha_l u_1)1+J^{j+1})^{b_1}\}.\\ &\quad\prod_{l=1}^{r}\{((1+p^{j-1}\alpha_l u_1+p^{j-1}\alpha_l u_2)1+J^{j+1})^{b_2}\}...\\ &\quad\prod_{l=1}^{r}\{((1+p^{j-1}\alpha_l u_1+p^{j-1}\alpha_l u_2+...+p^{j-1}\alpha_l u_h)1+J^{j+1})^{b_h}\}\\ &\quad=1+J^{j+1}\end{aligned}$$

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

If we set

$$T_l = \{((1+p^{j}\alpha_l)1+J^{j+1})^{a} \mid a = 1, ..., p\},$$

$$S_{1l} = \{((1+p^{j-1}\alpha_l u_1)1+J^{j+1})^{b_1} \mid b_1 = 1, ..., p\},$$

$$S_{2l} = \{((1+p^{j-1}\alpha_l u_1+p^{j-1}\alpha_l u_2)1+J^{j+1})^{b_2} \mid b_2 = 1, ..., p\}$$

$$\vdots$$

$$S_{hl} = \{((1+p^{j-1}\alpha_l u_1+p^{j-1}\alpha_l u_2+...+p^{j-1}\alpha_l u_h)1+J^{j+1})^{b_h} \mid b_h = 1, ..., p\}$$

we see that T_l, S_{1l}, S_{2l},...,S_{hl} are all cyclic subgroups of the group $1+J^j/1+J^{j+1}$ and they are of the orders indicated by their definition.

Since

$$\prod_{l=1}^{r} |< (1+p^{j}\alpha_l)1 + J^{j+1} >| . \prod_{l=1}^{r} |< (1+p^{j-1}\alpha_l u$$

$$\prod_{l=1}^{r} |< (1+p^{j-1}\alpha_l u_1 + p^{j-1}\alpha_l u_2)1 + J^{j+1} >|$$

$$...\prod_{l=1}^{r} |< (1+p^{j-1}\alpha_l u_1 + p^{j-1}\alpha_l u_2 + ... + p^{j-1}$$

$$= p^{(h+1)r}$$

and the intersection of any pair of the cyclic subg

$1 + J^{i+1}$, the product of the $(h+1)r$ subgroups T_l is

direct. So their product exhausts the group $1 + J$ □

6.2 Quotient Groups of Rings in Construction B

In the sequel, we study the structures of the quotient groups of the rings defined in Construction B for the case when $r = 1$. We determine the structure of $1 + J^j/1 + J^{j+1}$ for $j = 1, 2, ..., k - 1$

Proposition 6.2.1. *Let R be a ring defined in Construction B. Suppose J is the Jacobson radical of R, then for $k = 2$, $j = 1, 2$, the quotient group $1 + J^j/1 + J^{j+1} \cong \mathbf{Z}_p$ for every prime integer p.*

Proof. Case I: $j = 1$

Suppose $y \in \mathbf{Z}_{p^2}$ and $z \in (\mathbf{Z}_{p^2})^*$. Let $(1 + py + zu)1 + J^2 \in 1 + J/1 + J^2$. Then $o((1 + py + zu)1 + J^2) = p$, that is

$$\begin{aligned}
((1 + py + zu)1 + J^2)^p &= (1 + py + zu)^p 1 + J^2 \\
&= (1 + p^2 y + spz^2 + (pz + kpyz + tpz^3)u)1 + J^2 \\
&= (1 + spz^2 + (pz + kpyz + tpz^3)u)1 + J^2 \\
&= 1 + J^2 \text{ since } 1 + spz^2 + (pz + kpyz + tpz^3)u \in 1 + J^2
\end{aligned}$$

where $s = 1$ when $p = 2$ and $s \equiv 0(\text{mod } p)$ when p is odd ; $k \equiv 0(\text{mod } p)$; $t = 1$ when $p = 3$, $t \equiv 0(\text{mod } p)$ when $p \neq 3$. By

Lagrange's theorem,

$$| 1+J/1+J^2 |=\frac{p^3}{p^2}=p.$$

Therefore the order of the group generated by $(1+py+zu)1+J^2$ coincides with the order of the group $1+J/1+J^2$. So $1+J/1+J^2$ is a cyclic group of order p.

Case II: $j=2$

Suppose $y \in \mathbf{Z}_{p^2}$ and $z \in (\mathbf{Z}_{p^2})^*$. Let $(1+pz+pyu)1+J^3 \in 1+J^2/1+J^3$. Then $o((1+pz+pyu)1+J^3)=p$, that is

$$((1+pz+pyu)1+J^3)^p = (1+pz+pyu)^p 1+J^3$$

$$= (1+p^2z+p^2yu)1+J^3$$

$$= 1+J^3 \text{ since } 1+p^2z+p^2yu \in 1+J^3$$

Therefore the order of the group generated by $(1+pz+pyu)1+J^3$ coincides with the order of the group $1+J^2/1+J^3$. So $1+J^2/1+J^3$ is a cyclic group of order p. This completes the proof. □

Proposition 6.2.2. *Let R be a ring defined in Construction B. Suppose J is the Jacobson radical of R, then for $k \geq 3$ and $j=1,2,...,k-1$, the quotient group $1+J^j/1+J^{j+1} \cong \mathbf{Z}_p \times \mathbf{Z}_p$ for every prime integer p.*

Proof. Suppose $j = 1$.

Let $y \in \mathbf{Z}_{p^k}$ and $z \in (\mathbf{Z}_{p^k})^*$. Let $(1+pz+yu)1+J^2 \in 1+J/1+J^2$.

Then $o((1+pz+yu)1+J^2) = p$. This is true because

$$((1+pz+yu)1+J^2)^p = (1+pz+yu)^p 1+J^2$$

$$= (1+p^2z+s_1p^2z^2+s_2p^3z^3+...+s_{p-1}p^pz^p+mp^{k-1}y^2+$$

$$(py+k_1pyz+k_2p^2yz^2+...+k_{p-1}p^{p-1}yz^{p-1}+np^{k-1}y^3)u)1+J^2$$

$$= 1+J^2 \text{ since } (1+p^2z+s_1p^2z^2+s_2p^3z^3+...+s_{p-1}p^pz^p+mp^{k-1}y^2+$$

$$(py+k_1pyz+k_2p^2yz^2+...+k_{p-1}p^{p-1}yz^{p-1}+np^{k-1}y^3)u) \in 1+J^2$$

where $s_\tau \equiv 0(\text{mod}p)$, $1 \leq \tau \leq p-2$. If $k-1$ is prime, $s_{p-1} = 1$ or $s_{p-1} \equiv 0(\text{mod}p)$. If $k-1$ is composite, then $s_{p-1} \equiv 0(\text{mod}p)$.

We also notice that $m = 1$ when $p = 2$ and $m \equiv 0(\text{mod } p)$ when p is odd. Also $k_\nu \equiv 0(\text{mod } p)$, $1 \leq \nu \leq p-1$; $n = 1$ when $p = 3$, $n \equiv 0(\text{mod } p)$ when $p \neq 3$.

So the element $(1+pz+yu)1+J^2$ generates a cyclic subgroup of $1+J/1+J^2$ of order p.

Now, consider the element $(1+p^2y+zu)1+J^2 \in 1+J/1+J^2$.

Then

$$((1+p^2y+zu)1+J^2)^p = (1+p^2y+zu)^p1+J^2$$
$$= (1+p^3y+s_1p^4y^2+s_2p^6y^3+\ldots+s_{p-1}p^{2p}y^p+mp^{k-1}z^2+$$
$$(pz+k_1p^2zy+k_2p^4zy^2+\ldots+k_{p-1}p^{2(p-1)}zy^{p-1}+np^{k-1}z^3)u)1+J^2$$
$$= 1+J^2$$

since

$$1+p^3y+s_1p^4y^2+s_2p^6y^3+\ldots+s_{p-1}p^{2p}y^p+mp^{k-1}z^2+$$
$$(pz+k_1p^2zy+k_2p^4zy^2+\ldots+k_{p-1}p^{2(p-1)}zy^{p-1}+np^{k-1}z^3)u \in 1+J^2$$

where $s_\tau \equiv 0(\text{mod}p)$, $1 \leq \tau \leq p-2$, $m = 1$ when $p = 2$ and $m = 0$, when p is odd ;$s_{p-1} = 1$, $k_\nu \equiv 0(\text{mod } p)$, $1 \leq \nu \leq p-1$; $n = 1$ when $p = 3$, $n \equiv 0(\text{mod } p)$ when $p \neq 3$. . So the element $(1+p^2y+zu)1+J^2$ generates a cyclic subgroup of $1+J/1+J^2$ of order p.

Since $1+J$ is abelian, the quotient group $1+J/1+J^2$ is abelian. So the cyclic subgroups $<(1+pz+yu)1+J^2>$ and $<(1+p^2y+zu)1+J^2>$ are normal. Also

$$\mid 1+J/1+J^2 \mid = \frac{p^{2k-1}}{p^{2k-3}} = p^2.$$

The order of the group generated by the direct product of the cyclic subgroups $< (1 + pz + yu)1 + J^2 >$ and $< (1 + p^2y + zu)1 + J^2 >$ coincides with the order of $1 + J/1 + J^2$ and the intersection of the cyclic subgroups is the identity group. So the direct product of the cyclic subgroups exhausts $1 + J/1 + J^2$.

Case II: $j \geq 2$

Consider $(1 + p^{j+1}y + p^{j-1}zu)1 + J^{j+1} \in 1 + J^j/1 + J^{j+1}$.

If $p = 2$, then

$$((1 + 2^{j+1}y + 2^{j-1}zu)1 + J^{j+1})^2 = (1 + 2^{j+1}y + 2^{j-1}zu)^2 1 + J^{j+1}$$

$$= (1 + 2^{j+2}y + 2^{2j+2}y^2 + (2^j z + 2^{2j+2}yz)u)1 + J^{j+1}$$

$$= 1 + J^{j+1} \text{ since } (1 + 2^{j+2}y + 2^{2j+2}y^2 + (2^j z + 2^{2j+2}yz)u) \in 1 + J^{j+1}.$$

If p is odd, then

$$((1 + p^{j+1}y + p^{j-1}zu)1 + J^{j+1})^p = (1 + p^{j+1}y + p^{j-1}zu)^p 1 + J^{j+1}$$

$$= (1 + p^{j+2}y + k_1 p^{2j+2}y^2 + k_2 p^{3j+3}y^3 + ... +$$

$$k_{p-3}p^{(p-2)j+(p-2)}y^{p-2} + p^{(p-1)j+p}y^{p-1} + p^{pj+p}y^p +$$

$$(p^j z + s_1 p^{2j}yz + s_2 p^{3j+1}y^2 z + ... +$$

$$s_{p-2}p^{(p-1)j+(p-3)}y^{p-2}z + p^{pj+(p-1)}y^{p-1}z)u)1 + J^{j+1}$$

$$= 1 + J^{j+1}$$

since

$$1 + p^{j+2}y + k_1p^{2j+2}y^2 + k_2p^{3j+3}y^3 + ... + k_{p-3}p^{(p-2)j+(p-2)}y^{p-2} +$$
$$p^{(p-1)j+p}y^{p-1} + p^{pj+p}y^p + (p^jz + s_1p^{2j}yz + s_2p^{3j+1}y^2z + ... +$$
$$s_{p-2}p^{(p-1)j+(p-3)}y^{p-2}z + p^{pj+(p-1)}y^{p-1}z)u \in 1 + J^{j+1}$$

where $k_\tau \equiv 0(\mathrm{mod} p)$, $1 \leq \tau \leq p-3$ and $s_\nu \equiv 0(\mathrm{mod} p)$, $1 \leq \nu \leq p-2$. Therefore, for every prime integer p, $(1 + p^{j+1}y + p^{j-1}zu)1 + J^{j+1}$ generates a cyclic subgroup of $1 + J^j/1 + J^{j+1}$ of order p.

Now, consider the element $(1+p^jz+(p^{j-1}z)u)1+J^{j+1} \in 1+J^j/1+J^{j+1}$.

If $p = 2$, then

$$((1 + 2^jz + 2^{j-1}zu)1 + J^{j+1})^2 = (1 + 2^jz + 2^{j-1}zu)^21 + J^{j+1}$$
$$= (1 + 2^{j+1}z + 2^{2j}z^2 + (2^jz + 2^{2j}z^2)u)1 + J^{j+1}$$
$$= 1 + J^{j+1} \text{ since } (1 + 2^{j+1}z + 2^{2j}z^2 + (2^jz + 2^{2j}z^2)u \in 1 + J^{j+1}.$$

If p is odd, then

$$\begin{aligned}((1+p^{j}z+p^{j-1}zu)1+J^{j+1})^{p} &= (1+p^{j}z+p^{j-1}zu)^{p}1+J^{j+1}\\ &= (1+p^{j+1}z+k_{1}p^{2j}z^{2}+k_{2}p^{3j}z^{3}+\ldots+\\ &\quad k_{p-3}p^{(p-2)j}z^{p-2}+p^{(p-1)j+1}z^{p-1}+p^{pj}z^{p}+\\ &\quad (p^{j}z+s_{1}p^{2j-1}z^{2}+s_{2}p^{3j-1}z^{3}+\ldots+\\ &\quad s_{p-2}p^{(p-1)j-1}z^{p-1}+p^{pj}z^{p})u)1+J^{j+1}\\ &= 1+J^{j+1}\end{aligned}$$

since

$$\begin{aligned}&1+p^{j+1}z+k_{1}p^{2j}z^{2}+k_{2}p^{3j}z^{3}+\ldots+\\ &\quad k_{p-3}p^{(p-2)j}z^{p-2}+p^{(p-1)j+1}z^{p-1}+p^{pj}z^{p}+\\ &\quad (p^{j}z+s_{1}p^{2j-1}z^{2}+s_{2}p^{3j-1}z^{3}+\ldots+\\ &\quad s_{p-2}p^{(p-1)j-1}z^{p-1}+p^{pj}z^{p})u\in 1+J^{j+1}\end{aligned}$$

where $k_{\tau}\equiv 0(\mathrm{mod}p)$, $1\leq\tau\leq p-3$ and $s_{\nu}\equiv 0(\mathrm{mod}p)$, $1\leq\nu\leq p-2$. Therefore, for every prime integer p, $(1+p^{j}z+p^{j-1}zu)1+J^{j+1}$ generates a cyclic subgroup of $1+J^{j}/1+J^{j+1}$ of order p.

Since $1+J^{j}$ is abelian, the quotient group $1+J^{j}/1+J^{j+1}$ is abelian. So the cyclic subgroups $<(1+p^{j+1}y+p^{j-1}zu)1+J^{j+1}>$ and

$< (1+p^j z+p^{j-1}zu)1+J^{j+1} >$ are normal. By Lagrange's theorem

$$| 1+J^j/1+J^{j+1} |= \frac{p^{2k-2j+1}}{p^{2k-2j-1}} = p^2.$$

The order of the group generated by the direct product of the cyclic subgroups coincides with the order of $1+J^j/1+J^{j+1}$ and the intersection of the cyclic subgroups is the identity group. So the direct product of the cyclic subgroups exhausts $1+J^j/1+J^{j+1}$. This completes the proof. □

Chapter 7

Conclusion

In this thesis, we have endeavoured to determine the structures of the unit groups of certain classes of finite rings. We have established two constructions of finite rings and shown that they are indeed finite rings satisfying the given conditions. Although the multiplication used in our construction A is similar to the multiplication defined on rings in which the product of any two zero divisors is zero, it appears to have been of little use in the previous studies of the unit groups of completely primary finite rings. This study has made significant contributions to knowledge because of the following:

(i) It seems that the previous studies dealt mainly with completely primary finite rings in which the unique maximal ideal J satisfies the properties $J^2 = (0)$; and of $J^2 \neq (0)$, $J^3 = (0)$. In our rings, we have eliminated the restriction on the index of nilpotence of the unique maximal ideal J.

(ii) We have not only determined the structures of the unit groups of finite rings in which the unique maximal ideal J satisfies the properties $J^k \neq (0)$ and $J^{k+1} = (0)$ but also in a specific case determined the structure of the unit groups of finite rings in which $J^{k+1} \neq (0)$ and $J^{k+2} = (0)$. We have also determined the structures of some quotient groups of subgroups of the unit groups of the rings constructed here.

Finally, we recommend that further studies on this work may be done when R_0 is defined to be the quotient of a polynomial ring in a finite number of variables by an ideal generated by a monic irreducible polynomial in the given ring.

References

[1] Ayoub C.W., On finite primary rings and their groups of units, *Compositio Math.* **21** (1969), 247-252.

[2] Bhattacharya P.B , Jain S.K, Nagpaul S.R., *Basic abstract algebra,* Cambridge University Press (2008).

[3] Chikunji C.J., Unit groups of a certain class of completely primary finite rings, *Mathematical Journal of Okayama University* **47** (2005), 39-53.

[4] Chikunji C.J., Unit groups of cube radical zero commutative completely primary finite rings, *International Journal of Mathematics and Mathematical sciences* **4** (2005), 579-592.

[5] Chikunji C.J., On unit groups of completely primary finite rings,

Mathematical Journal of Okayama University **50** (2008), 149-160.

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

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

[8] Corbas B., Finite rings in which the product of any two zero divisors is zero, *Math. Ann.* **21**(1970), 466-469.

[9] Dolzan D., Group of units in a finite ring, *J. Pure Appl. Algebra* **170(2)** (2002), 175-183.

[10] Fuchs L., Abelian groups, 3rd ed., *International series of monographs on pure and applied mathematics*, Pergamon Press, New York, (1960).

[11] Ganske G and Mc Donald B.R., Finite local rings, *Rocky Mountain J. Math.* **3 (4)** (1973),521-540.

[12] Gilmer R.W., Finite rings having a cyclic multiplicative group of units, *American Journal of Mathematics* **85** (1963), 447-452.

[13] Ireland K and Rosen M., *The Chinese Remainder Theorem "A classical introduction to modern number theory"*, New York, Verlag (1990).

[14] Pearson K.R and Schneider J.E., Rings with a cyclic group of units, *J. Algebra* **16** (1970), 243-251.

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

[16] Stewart I., Finite rings with a specified group of units, *Math. Z.* **126** (1972), 51-58.

[17] Weisstein E.W., *Chinese Remainder Theorem,* (http:// mathworld.wolfram.com/ Chinese Remainder Theorem. html) at Mathworld (11:10:2008).