Math. J. Okayama Univ. **50** (2008), 149–160

ON UNIT GROUPS OF COMPLETELY PRIMARY FINITE RINGS

Chiteng'a John CHIKUNJI

Abstract. Let R be a commutative completely primary finite ring with the unique maximal ideal $\mathcal{J}$ such that $\mathcal{J}^3 = (0)$ and $\mathcal{J}^2 \neq (0)$. Then $R/\mathcal{J} \cong GF(p^r)$ and the characteristic of R is p^k, where $1 \leq k \leq 3$, for some prime p and positive integers $k,\ r$. Let $R_o = GR(p^{kr},\ p^k)$ be a galois subring of R so that $R = R_o \oplus U \oplus V \oplus W$, where $U,\ V$ and W are finitely generated R_o-modules. Let non-negative integers $s,\ t$ and λ be numbers of elements in the generating sets for $U,\ V$ and W, respectively. In this work, we determine the structure of the subgroup $1 + W$ of the unit group R^* in general, and the structure of the unit group R^* of R when $s = 3,\ t = 1,\ \lambda \geq 1$ and characteristic of R is p. We then generalize the solution of the cases when $s = 2,\ t = 1$; $t = s(s+1)/2$ for a fixed s; for all the characteristics of R ; and when $s = 2,\ t = 2$, and characteristic of R is p to the case when the annihilator $ann(\mathcal{J}) = \mathcal{J}^2 + W$, so that $\lambda \geq 1$. This complements the author's earlier solution of the problem in the case when the annihilator of the radical coincides with the square of the radical.

1. Introduction

Throughout this paper we will assume that all rings are commutative rings with identity, that ring homomorphisms preserve identities, and that a ring and its subrings have the same identity. Moreover, we adopt the notation used in [2] and [3], that is, R will denote a finite ring, unless otherwise stated, $\mathcal{J}$ will denote the Jacobson radical of R, and we will denote the Galois ring $GR(p^{nr},\ p^n)$ of characteristic p^n and order p^{nr} by R_o, for some prime integer p, and positive integers $n,\ r$. We denote the unit group of R by R^*; if g is an element of R^*, then $o(g)$ denotes its order, and $< g >$ denotes the cyclic group generated by g. Further, for a subset A of R or R^*, $|A|$ will denote the number of elements in A. The ring of integers modulo the number n will be denoted by $\mathbb{Z}_n$, and the characteristic of R will be denoted by char$R$.

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

Let R be a completely primary finite ring with maximal ideal $\mathcal{J}$. Then R is of order p^{nr}; $\mathcal{J}$ is the Jacobson radical of R; $\mathcal{J}^m = (0)$, where $m \leq n$, and the residue field $R/\mathcal{J}$ is a finite field $GF(p^r)$, for some prime p and

Mathematics Subject Classification. Primary 13M05, 16P10, 16U60; Secondary 20K01, 20K25.

Key words and phrases. unit groups, completely primary finite rings, galois rings.

positive integers n, r. The char$R = p^k$, where k is an integer such that $1 \leq k \leq m$. If $k = n$, then $R = \mathbb{Z}_{p^k}[b]$, where b is an element of R of multiplicative order $p^r - 1$; $\mathcal{J} = pR$ and $Aut(R) \cong Aut(R/pR)$. Such a ring is called a *Galois ring,* denoted by $GR(p^{kr}, p^k)$. Let $GR(p^{kr}, p^k)$ be the Galois ring of characteristic p^k and order p^{kr}, i.e., $GR(p^{kr}, p^k) = \mathbb{Z}_{p^k}[x]/(f)$, where $f \in \mathbb{Z}_{p^k}[x]$ is a monic polynomial of degree r whose image in $\mathbb{Z}_p[x]$ is irreducible. If char$R = p^k$, then R has a coefficient subring R_o of the form $GR(p^{kr}, p^k)$ which is clearly a maximal Galois subring of R. Moreover, there exist elements $m_1,\ m_2,\ ...,\ m_h \in \mathcal{J}$ and automorphisms $\sigma_1, ...,\ \sigma_h \in Aut(R_o)$ such that

$$R = R_o \oplus \sum_{i=1}^{h} R_o m_i \text{ (as } R_o\text{−modules)}, \ m_i r = r^{\sigma_i} m_i,$$

for every $r \in R_o$ and any $i = 1, ..., h$. Further, $\sigma_1, ...,\ \sigma_h$ are uniquely determined by R and R_o. The maximal ideal of R is

$$\mathcal{J} = pR_o \oplus \sum_{i=1}^{h} R_o m_i.$$

Let R be a completely primary finite ring (not necessarily commutative). The following facts are useful (e.g. see [2, §2]): The group of units R^* of R contains a cyclic subgroup $< b >$ of order $p^r - 1$, and R^* is a semi-direct product of $1 + \mathcal{J}$ by $< b >$; the group of units R^* is solvable; if G is a subgroup of R^* of order $p^r - 1$, then G is conjugate to $< b >$ in R^*; if R^* contains a normal subgroup of order $p^r - 1$, then the set $K_o =< b > \cup \{0\}$ is contained in the center of the ring R; and $(1 + \mathcal{J}^i)/(1 + \mathcal{J}^{i+1}) \cong \mathcal{J}^i/\mathcal{J}^{i+1}$ (the left hand side as a multiplicative group and the right hand side as an additive group).

Now let R be a commutative completely primary finite ring with maximal ideal $\mathcal{J}$ such that $\mathcal{J}^3 = (0)$ and $\mathcal{J}^2 \neq (0)$. The author gave constructions describing these rings for each characteristic and for details, we refer the reader to sections 4 and 6 of [1]. Then $R/\mathcal{J} \cong GF(p^r)$ and the characteristic of R is p^k, where $1 \leq k \leq 3$. Let $R_o = GR(p^{kr},\ p^k)$ be a galois subring of R. Then $R = R_o \oplus \sum_{i=1}^{h} R_o m_i$ and the maximal ideal of R is $\mathcal{J} = pR_o \oplus \sum_{i=1}^{h} R_o m_i$. Moreover, from Constructions A and B in [1],

$$R = R_o \oplus U \oplus V \oplus W$$

and

$$\mathcal{J} = pR_o \oplus U \oplus V \oplus W,$$

where the R_o−modules U, V and W are finitely generated. The structure of R is characterized by the invariants $p,\ n,\ r,\ d,\ s,\ t$ and λ; and the linearly independent matrices (α_{ij}^k) defined in the multiplication. In [1], $d \geq 0$ denotes the number of the $m_i \in \{m_1, \ ..., \ m_h\}$ with $pm_i \neq 0$.

Let $s, \ t, \ \lambda$ be numbers in the generating sets for the R_o-modules $U, \ V, \ W$, respectively. In [2] we have determined the unit group R^* of the ring R when $s = 2, \ t = 1, \ \lambda = 0$ and characteristic of R is p; and when $t = s(s+1)/2, \ \lambda = 0$, for a fixed integer s, for all the characteristics of R. In [3] we obtained the structure of R^* when $s = 2, \ t = 1, \ \lambda = 0$ and characteristic of R is p^2 and p^3; and the case when $s = 2, \ t = 2, \ \lambda = 0$ and characteristic of R is p. In both papers [2] and [3], we assumed that $\lambda = 0$ so that the annihilator of the maximal ideal $\mathcal{J}$ coincides with $\mathcal{J}^2$.

In Section 2, we show that $1 + \mathcal{J}$ is a direct product of its subgroups $1 + pR_o \oplus U \oplus V$ and $1 + W$ and further determine the structure of $1 + W$, in general; and in Section 3, we determine the structure of R^* when $s = 3, \ t = 1, \ \lambda \geq 1$ and char$R = p$. In the final Section, we generalize the structure of R^* in the cases when $s = 2, \ t = 1$; $t = s(s+1)/2$, for a fixed integer s, and for all characteristics of R; and when $s = 2, \ t = 2$ and char$R = p$; determined in [2] and [3], to the case when $ann(\mathcal{J}) = \mathcal{J}^2 + W$ so that $\lambda \geq 1$. This complements our earlier solution to the problem in the case when $ann(\mathcal{J}) = \mathcal{J}^2$.

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

$$R^* = < b > \cdot (1 + \mathcal{J}) \cong < b > \times (1 + \mathcal{J});$$

a direct product of the $p-$group $1 + \mathcal{J}$ by the cyclic subgroup $< b >$.

2. The structure of $1 + W$

Let R be a commutative completely primary finite ring with maximal ideal $\mathcal{J}$ such that $\mathcal{J}^3 = (0)$ and $\mathcal{J}^2 \neq (0)$. Let $R_o = GR(p^{kr}, p^k)$ $(1 \leq k \leq 3)$ and let non-negative integers $s, \ t$ and λ be numbers in the generating sets $\{u_1, \ ..., \ u_s\}, \ \{v_1, \ ..., \ v_t\}$ and $\{w_1, \ ..., \ w_\lambda\}$ for finitely generated R_o-modules $U, \ V$ and W, respectively, where $t \leq s(s+1)/2$ and $\lambda \geq 1$. Then $R = R_o \oplus U \oplus V \oplus W$ and hence,

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

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

$$ann(\mathcal{J}) = pR_o \oplus \sum_{j=1}^{t} R_o v_j \oplus \sum_{k=1}^{\lambda} R_o w_k \text{ or } p^2 R_o \oplus \sum_{j=1}^{t} R_o v_j \oplus \sum_{k=1}^{\lambda} R_o w_k,$$

$$\mathcal{J}^2 = pR_o \oplus \sum_{j=1}^{t} R_o v_j \text{ or } p^2 R_o \oplus \sum_{j=1}^{t} R_o v_j;$$

and $\mathcal{J}^3 = (0)$. Hence,

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

The following proposition and its corollary play an important role in determining the structure of $1 + \mathcal{J}$.

Proposition 2.1. *If $\lambda \geq 1$, then $1 + \sum_{i=1}^{\lambda} \oplus R_o w_i$ is a subgroup of $1 + \mathcal{J}$.*

Proof. This follows easily since for any two elements $1 + \sum \alpha_i w_i$ and $1 + \sum \beta_i w_i$ in $1 + \sum_{i=1}^{\lambda} \oplus R_o w_i$, we have

$$(1 + \sum \alpha_i w_i)(1 + \sum \beta_i w_i) = 1 + \sum (\alpha_i + \beta_i) w_i,$$

an element in $1 + \sum_{i=1}^{\lambda} \oplus R_o w_i$. □

Corollary 2.2. *$1 + ann(\mathcal{J})$ is a subgroup of $1 + \mathcal{J}$.*

The following result simplifies most of the work in the sequel.

Proposition 2.3. *The $p-$group $1 + \mathcal{J}$ is a direct product of the subgroups $1 + pR_o \oplus \sum_{i=1}^{s} R_o u_i \oplus \sum_{j=1}^{t} R_o v_j$ by $1 + \sum_{i=1}^{\lambda} \oplus R_o w_i$.*

Proof. Follows easily because $\sum_{i=1}^{\lambda} \oplus R_o w_i \subseteq ann(\mathcal{J})$ and a routine check shows that

$$\begin{aligned} & (1 + pR_o \oplus \sum_{i=1}^{s} R_o u_i \oplus \sum_{j=1}^{t} R_o v_j) \times (1 + \sum_{i=1}^{\lambda} \oplus R_o w_i) \\ = \;& 1 + pR_o \oplus \sum_{i=1}^{s} R_o u_i \oplus \sum_{j=1}^{t} R_o v_j \oplus \sum_{k=1}^{\lambda} R_o w_k \\ = \;& 1 + \mathcal{J}. \end{aligned}$$

□

Since the structure of $1 + pR_o \oplus \sum_{i=1}^{s} R_o u_i \oplus \sum_{j=1}^{t} R_o v_j$, for $s = 2,\ t = 1$; $s = 2,\ t = 2$ and char$R = p$, and $t = s(s+1)/2$ for a fixed s, have been determined in [2] and [3], and following Proposition 2.2, it suffices to determine the structure of $1+W = 1+\sum_{i=1}^{\lambda} \oplus R_o w_i$. We do this for every characteristic p^k $(1 \leq k \leq 3)$ of R.

We first note that $pw_i = 0$ for each $w_i \in W$ $(i = 1, \ ..., \ \lambda)$, since $W \subseteq ann(\mathcal{J}) = \mathcal{J}^2 + W$.

Proposition 2.4. *The group* $1+\sum_{i=1}^{\lambda} \oplus R_o w_i \cong \underbrace{\mathbb{Z}_p^r \times \ ... \ \times \mathbb{Z}_p^r}_{\lambda \geq 1 \text{ times}}$ *, for any prime integer* p *such that* p^k *=char*R $(1 \leq k \leq 3)$.

Proof. Let $\varepsilon_1, \ \varepsilon_2, \ ..., \ \varepsilon_r$ be elements of R_o with $\varepsilon_1 = 1$ so that $\overline{\varepsilon_1}, \ \overline{\varepsilon_2}, \ ..., \ \overline{\varepsilon_r} \in R_o/pR_o \cong GF(p^r)$ form a basis of $GF(p^r)$ over its prime subfield $GF(p)$. First notice that, for $1+\varepsilon_j w_i \in 1+\sum_{i=1}^{\lambda} \oplus R_o w_i$, and for each $j = 1, \ ..., \ r$; $(1+\varepsilon_j w_i)^p = 1$ and $g^p = 1$ for all $g \in 1+\sum_{i=1}^{\lambda} \oplus R_o w_i$, where p is a prime integer such that p^k =char$R$ $(1 \leq k \leq 3)$.

For integers $l_j, \ m_j, \ ..., \ n_j \leq p$, we assert that

$$\prod_{j=1}^{r} \left\{ (1+\varepsilon_j w_1)^{l_j} \right\} \times \prod_{j=1}^{r} \{(1+\varepsilon_j w_2)^{m_j}\} \times \ ... \ \times \prod_{j=1}^{r} \{(1+\varepsilon_j w_\lambda)^{n_j}\} = 1,$$

will imply that $l_j = m_j = \ ... = n_j = p$, for all $j = 1, \ldots r$.

If we set

$$\begin{aligned} F_j &= \left\{ (1+\varepsilon_j w_1)^l : l = 1, \ ..., \ p \right\}, \\ G_j &= \{(1+\varepsilon_j w_2)^m : m = 1, \ ..., \ p\}, \ ..., \\ H_j &= \{(1+\varepsilon_j w_\lambda)^n : n = 1, \ ..., \ p\}, \end{aligned}$$

for all $j = 1, \ ..., \ r$; we see that $F_j, \ G_j, \ ..., \ H_j$ are all cyclic subgroups of $1+\sum_{i=1}^{\lambda} \oplus R_o w_i$ and these are all of order p as indicated in their definition. The argument above will show that the product of the λr subgroups $F_j, \ G_j, \ ...,$ and H_j is direct. So, their product will exhaust $1+\sum_{i=1}^{\lambda} \oplus R_o w_i$. □

3. The case when char$R = p, \ s = 3, \ t = 1$ and $\lambda \geq 1$

Let the characteristic of the ring R be p and let $s = 3, \ t = 1$ and $\lambda \geq 1$. Then

$$R = \mathbb{F}_q \oplus \mathbb{F}_q u_1 \oplus \mathbb{F}_q u_2 \oplus \mathbb{F}_q u_3 \oplus \mathbb{F}_q v \oplus \sum_{i=1}^{\lambda} \oplus \mathbb{F}_q w_i,$$

and

$$\mathcal{J} = \mathbb{F}_q u_1 \oplus \mathbb{F}_q u_2 \oplus \mathbb{F}_q u_3 \oplus \mathbb{F}_q v \oplus \sum_{i=1}^{\lambda} \oplus \mathbb{F}_q w_i,$$

where $\mathbb{F}_q = GF(p^r)$, the Galois field of p^r elements, for any positive integer r, and prime integer p, and we have

$$u_i u_j = a_{ij} v, \text{where } a_{ij} \in \mathbb{F}_q.$$

The symmetric matrix $A = (a_{ij})$ is non-zero and one verifies that any such matrix gives rise to a ring of the present type. If we change to new generators $u_i^{'}, v^{'}, w_i^{'}$ with corresponding matrix $A^{'}$, then $u_1^{'}, u_2^{'}, u_3^{'}$ are linear combinations of u_i, v, w_i. Since $\mathcal{J}^3 = (0)$, we may assume that the coefficients of v and w_i are zero and write $u_i^{'} = p_{1i}u_1 + p_{2i}u_2 + p_{3i}u_3$, so that $P = (p_{ij})$ is the transition matrix from the basis $\{u_1, u_2, u_3\}$ of $\mathcal{J}/ann(\mathcal{J})$ to the basis $\{u_1^{'}, u_2^{'}, u_3^{'}\}$. If also $v^{'} = kv$ $(k \in \mathbb{F}_q^*)$ and we now calculate $u_i^{'}u_j^{'}$ and compare coefficients of v, we obtain an equation which, in matrix form is

$$P^t AP = kA^{'},$$

where P^t is the transpose of the matrix P. The problem of classifying the present class of rings up to isomorphism is now readily seen to amount to that of classifying symmetric matrices A under the above equivalence relation, in which $P \in GL_3(\mathbb{F}_q)$, $k \in \mathbb{F}_q^*$ are arbitrary. Observe that k is the transition element from the basis $\{v\}$ of $\mathcal{J}^2$ to $\{v^{'}\}$. This is similar to the situation of [4, 5], wherein $k \in \mathbb{F}_q^*$. We deduce from Theorem 3 in [5] that if $p = 2$, there are up to isomorphism, four commutative rings with structural matrices

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix};$$

and from Theorem 4 in [4] that if p is odd, there are up to isomorphism, five commutative rings with structural matrices

$$\begin{pmatrix} \alpha & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & \alpha & 0 \\ 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \alpha \end{pmatrix}, \ (\alpha = 1, \ \epsilon),$$

where ϵ is a fixed non-square in $\mathbb{F}_q$. Note that the first matrix in the case when p is odd may be multiplied by $1/\alpha$ to obtain the five non-isomorphic classes of rings under consideration.

We now determine the structure of the $p-$group $1 + \mathcal{J}$. Notice that

$$1 + \mathcal{J} = 1 + \mathbb{F}_q u_1 \oplus \mathbb{F}_q u_2 \oplus \mathbb{F}_q u_3 \oplus \mathbb{F}_q v \oplus \sum_{i=1}^{\lambda} \oplus \mathbb{F}_q w_i.$$

The following result is fundamental in the study of the unit groups of the rings in this paper.

Lemma 3.1. *Let R and S be rings (not necessarily rings considered in this paper). Then every ring isomorphism between R and S restricts to an isomorphism between R^* and S^*.*

However, it is not always true that if $R^* \cong S^*$, then the rings R and S are isomorphic, as may be illustrated by the following: $\mathbb{Z}^* = \{1, \ -1\} \cong \mathbb{Z}_3^*$, while $\mathbb{Z}$ (infinite) and $\mathbb{Z}_3$ (finite) are non-isomorphic rings.

To simplify our notation, we shall call a ring of characteristic $p = 2$, a *ring of Type I* if it is isomorphic to a ring with structural matrix

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \text{ or } \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix};$$

and a *ring of Type II* if it is isomorphic to a ring with structural matrix

$$\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}.$$

Proposition 3.2. *If $charR = p$, $s = 3$, $t = 1$ and $\lambda \geq 1$, then*

$$1 + \mathcal{J} \cong \mathbb{Z}_p^r \times \mathbb{Z}_p^r \times \mathbb{Z}_p^r \times \mathbb{Z}_p^r \times (\mathbb{Z}_p^r)^\lambda \text{ if } p \text{ is odd},$$

and when $p = 2$,

$$1 + \mathcal{J} \cong \begin{cases} \mathbb{Z}_4^r \times \mathbb{Z}_2^r \times \mathbb{Z}_2^r \times (\mathbb{Z}_2^r)^\lambda & \text{if } R \text{ is of Type I;} \\ \mathbb{Z}_2^r \times \mathbb{Z}_2^r \times \mathbb{Z}_2^r \times \mathbb{Z}_2^r \times (\mathbb{Z}_2^r)^\lambda & \text{if } R \text{ is of Type II.} \end{cases}$$

Proof. Let $\varepsilon_1, \ ..., \ \varepsilon_r \in \mathbb{F}_q$ with $\varepsilon_1 = 1$ such that $\bar{\varepsilon}_1, \ ..., \ \bar{\varepsilon}_r \in \mathbb{F}_q$ form a basis for $\mathbb{F}_q$ over its prime subfield $\mathbb{F}_p$, where $q = p^r$ for any prime p and positive integer r.

We consider the two cases separately. So, suppose that p is odd. We first note the following results: For each $i = 1, \ ..., r$, $(1 + \varepsilon_i u_1)^p = 1$, $(1+\varepsilon_i u_2)^p = 1$, $(1+\varepsilon_i u_3)^p = 1$, $(1+\varepsilon_i v)^p = 1$, $(1+\varepsilon_i w_j)^p = 1$, $(j = 1, \ ..., \ \lambda)$, and $g^p = 1$ for all $g \in 1 + \mathcal{J}$. For integers $k_i, \ l_i, \ m_i, \ n_i, \ t_i \leq p$, we assert that

$$\prod_{i=1}^{r}\{(1 + \varepsilon_i u_1)^{k_i}\} \cdot \prod_{i=1}^{r}\{(1 + \varepsilon_i u_2)^{l_i}\} \cdot \prod_{i=1}^{r}\{(1 + \varepsilon_i u_3)^{m_i}\} \cdot \prod_{i=1}^{r}\{(1 + \varepsilon_i v)^{n_i}\}$$
$$\cdot \prod_{j=1}^{\lambda}\prod_{i=1}^{r}\{(1 + \varepsilon_i w_j)^{t_i}\} = 1,$$

will imply $k_i, \ l_i, \ m_i, \ n_i, \ t_i = p$ for all $i = 1, \ ..., r$.

If we set $D_i = \{(1+\varepsilon_i u_1)^k : k = 1, \ ..., \ p\}$, $E_i = \{(1+\varepsilon_i u_2)^l : l = 1, \ ..., \ p\}$, $F_i = \{(1 + \varepsilon_i u_3)^m : m = 1, \ ..., \ p\}$, $G_i = \{(1 + \varepsilon_i v)^n : n = 1, \ ..., \ p\}$ and $H_{i,j} = \{(1 + \varepsilon_i w_j)^t : t = 1, \ ..., \ p\}$ $(j = 1, \ ..., \ \lambda)$, for all $i = 1, \ ..., r$; we see that $D_i,\ E_i,\ F_i,\ G_i,\ H_{i,j}$ are all subgroups of the group $1+\mathcal{J}$ and these are all of order p as indicated in their definition. The argument above will show that the product of the $(4+\lambda)r$ subgroups $D_i,\ E_i,\ F_i,\ G_i,\ H_{i,j}$ is direct. So, their product will exhaust $1+\mathcal{J}$. This proves the case when p is odd.

To prove the second part, suppose $p=2$. We first observe that $(1+\varepsilon_i u_1)^4=1$ if the ring R is of Type I, and if the ring R is of Type II, the elements $1+\varepsilon_i u_1$, $1+\varepsilon_i u_2$, $1+\varepsilon_i u_3$, $1+\varepsilon_i v$ and $1+\varepsilon_i w_j$ $(j=1,\ ...,\lambda)$, are all of order 2.

If the ring R is of Type I, the elements $1+\varepsilon_i u_2$, and $1+\varepsilon_i u_3$, are each of order 4, for all $i=1,\ ...,\ r$, according as the structural matrix A of R is of the form $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}$ or $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$. In particular, if $A=\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$, then $o(1+\varepsilon_i u_2)=o(1+\varepsilon_i u_3)=o(1+\varepsilon_i w_j)=2$; if $A=\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}$, then $o(1+\varepsilon_i u_3)=o(1+\varepsilon_i w_j)=2$; and if $A=\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, then $o(1+\varepsilon_i w_j)=2$; $(j=1,\ ...,\ \lambda)$. Observe further that in this type of rings, $(1+\varepsilon_i u_1)^2=1+\varepsilon_i^2 v$.

Now, if R is a ring of Type II, then for each $i=1,\ ...,\ r$ and for integers $k_i,\ l_i,\ m_i,\ n_i,\ t_i\le 2$, we assert that the equation

$$\prod_{i=1}^{r}\{(1+\varepsilon_i u_1)^{k_i}\}\cdot\prod_{i=1}^{r}\{(1+\varepsilon_i u_2)^{l_i}\}\cdot\prod_{i=1}^{r}\{(1+\varepsilon_i u_3)^{m_i}\}\cdot\prod_{i=1}^{r}\{(1+\varepsilon_i v)^{n_i}\}$$
$$\cdot\prod_{j=1}^{\lambda}\prod_{i=1}^{r}\{(1+\varepsilon_i w_j)^{t_i}\}=1,$$

will imply $k_i,\ l_i,\ m_i,\ n_i,\ t_i=2$, for all $i=1,\ ...,r$.

If we set $D_i=\{(1+\varepsilon_i u_1)^k : k=1,\ 2\}$, $E_i=\{(1+\varepsilon_i u_2)^l : l=1,\ 2\}$, $F_i=\{(1+\varepsilon_i u_3)^m : m=1,\ 2\}$, $G_i=\{(1+\varepsilon_i v)^n : n=1,\ 2\}$ and $H_{i,j}=\{(1+\varepsilon_i w_j)^t : t=1,\ 2\}$ $(j=1,\ ...,\ \lambda)$, for all $i=1,\ ...,r$; we see that $D_i,\ E_i,\ F_i,\ G_i,\ H_{i,j}$ are all subgroups of the group $1+\mathcal{J}$, each of order 2. The argument above will show that the product of the $(4+\lambda)r$ subgroups $D_i,\ E_i,\ F_i,\ G_i,\ H_{i,j}$ is direct. So, their product will exhaust $1+\mathcal{J}$.

If R is a ring of Type I and $A=\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$, the equation

$$\prod_{i=1}^{r}\{(1+\varepsilon_i u_1)^{k_i}\}\cdot\prod_{i=1}^{r}\{(1+\varepsilon_i u_2)^{l_i}\}\cdot\prod_{i=1}^{r}\{(1+\varepsilon_i u_3)^{m_i}\}\cdot$$

$$\prod_{j=1}^{\lambda}\prod_{i=1}^{r}\{(1+\varepsilon_i w_j)^{n_i}\}=1,$$

will imply $k_i = 4$, and $l_i = m_i = n_i = 2$, for all $i = 1, \ldots, r$, and $j = 1, \ldots, \lambda$.

If we set $D_i = \{(1+\varepsilon_i u_1)^k : k = 1, \ldots, 4\}$, $E_i = \{(1+\varepsilon_i u_2)^l : l = 1, 2\}$, $F_i = \{(1+\varepsilon_i u_3)^m : m = 1, 2\}$, and $G_{i,j} = \{(1+\varepsilon_i w_j)^t : t = 1, 2\}$ $(j = 1, \ldots, \lambda)$, for all $i = 1, \ldots, r$; we see that $D_i, E_i, F_i, G_{i,j}$ are all subgroups of the group $1+\mathcal{J}$, and these are of the precise order as indicated in their definition. The argument above will show that the product of the $(3+\lambda)r$ subgroups $D_i, E_i, F_i, G_{i,j}$ is direct. So, their product will exhaust $1+\mathcal{J}$.

If R is of Type I and $A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}$, the equation

$$\prod_{i=1}^{r}\{(1+\varepsilon_i u_1)^{k_i}\}\cdot\prod_{i=1}^{r}\{(1+\varepsilon_i u_1+\varepsilon_i u_2+\varepsilon_i v+)^{l_i}\}\cdot\prod_{i=1}^{r}\{(1+\varepsilon_i u_3)^{m_i}\}\cdot$$
$$\prod_{j=1}^{\lambda}\prod_{i=1}^{r}\{(1+\varepsilon_i w_j)^{n_i}\}=1,$$

will imply $k_i = 4$, and $l_i = m_i = n_i = 2$, for all $i = 1, \ldots, r$, and $j = 1, \ldots, \lambda$. A similar argument with slight modifications as in the previous case leads to the result.

If R is of Type I and $A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, then $1+\mathcal{J}$ contains subgroups $< 1+\varepsilon_i u_1+\varepsilon_i u_2+\varepsilon_i v >$, $< 1+\varepsilon_i u_1+\varepsilon_i u_3+\varepsilon_i v >$ each of order 2, for every $i = 1, \ldots, r$, and since any intersection of the cyclic subgroups $< 1+\varepsilon_i u_1 >$, $< 1+\varepsilon_i u_1+\varepsilon_i u_2+\varepsilon_i v >$, $< 1+\varepsilon_i u_1+\varepsilon_i u_3+\varepsilon_i v >$ and $< 1+\varepsilon_i w_j >$ $(j = 1, \ldots, \lambda)$, is trivial, and that the order of the group generated by the direct product of these cyclic subgroups coincides with $|1+\mathcal{J}|$, it follows that

$$\begin{aligned} 1+\mathcal{J} &= \prod_{i=1}^{r} < 1+\varepsilon_i u_1 > \times \prod_{i=1}^{r} < 1+\varepsilon_i u_1+\varepsilon_i u_2+\varepsilon_i v > \times \\ & \prod_{i=1}^{r} < 1+\varepsilon_i u_1+\varepsilon_i u_3+\varepsilon_i v > \times \prod_{j=1}^{\lambda}\prod_{i=1}^{r} < 1+\varepsilon_i w_j >, \end{aligned}$$

a direct product. This proves the first part.

To prove the second part; since for each $i = 1, \ldots, r$, $(1+\varepsilon_i u_1)^2 = 1$, $(1+\varepsilon_i u_2)^2 = 1$, $(1+\varepsilon_i u_3)^2 = 1$, $(1+\varepsilon_i v)^2 = 1$, $(1+\varepsilon_i w_j)^2 = 1$ $(j =$

1, ..., λ), and the order of the group generated by the product of the cyclic subgroups $< 1+\varepsilon_i u_1 >$, $< 1+\varepsilon_i u_2 >$, $< 1+\varepsilon_i u_3 >$ $< 1+\varepsilon_i v >$, and $< 1+\varepsilon_i w_j >$ $(j = 1, \ldots, \lambda)$ coincides with $|1+\mathcal{J}|$, and any intersection of these subgroups gives the identity group, it follows that

$$\begin{aligned} 1+\mathcal{J} &= \prod_{i=1}^{r} < 1+\varepsilon_i u_1 > \times \prod_{i=1}^{r} < 1+\varepsilon_i u_2 > \times \prod_{i=1}^{r} < 1+\varepsilon_i u_3 > \times \\ & \prod_{i=1}^{r} < 1+\varepsilon_i v > \times \prod_{j=1}^{\lambda}\prod_{i=1}^{r} < 1+\varepsilon_i w_j >, \end{aligned}$$

a direct product. This completes the proof. □

4. A generalized result

In view of Proposition 2.3, we now state the following result which summarizes the structure of the unit group R^* of the ring R of the introduction, in the cases when $s = 2,\ t = 1$; $t = s(s+1)/2$, for a fixed integer s, and for all characteristics of R; and when $s = 2,\ t = 2$ and char$R = p$; determined in [2] and [3], to the general case when $ann(\mathcal{J}) = \mathcal{J}^2 + W$ so that $\lambda \geq 1$. This complements our earlier solution to the problem in the case when $ann(\mathcal{J}) = \mathcal{J}^2$.

Theorem 4.1. *The unit group R^* of a commutative completely primary finite ring R with maximal ideal $\mathcal{J}$ such that $\mathcal{J}^3 = (0)$ and $\mathcal{J}^2 \neq (0)$, and with the invariants $p,\ k,\ r,\ s,\ t$, and $\lambda \geq 1$, is a direct product of cyclic groups as follows:*

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

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

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

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

and if $p = 2$

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

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

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

and

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

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

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

v) If $t = s(s+1)/2,\ \lambda \geq 1$, and
(a) $charR = p$, then

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

(b) $charR = p^2$, then

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

(c) $charR = p^3$, then

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

where $\gamma = (s^2 - s)/2$.

Proof. Follows from Section 3.1 in [2], Propositions 2.2, 2.3, 2.4 and 2.5 in [3], Theorem 4.1 in [2] and Proposition 2.3. □

References

[1] C. J. Chikunji, *On a class of finite rings*, Comm. Algebra, **27**(**10**) (1999), 5049-5081.

[2] C. J. Chikunji, *Unit groups of cube radical zero commutative completely primary finite rings*, Inter. J. Maths. & Math. Sciences, **2005:4** (2005), 579-592.

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

[4] B. Corbas and G. D. Williams, *Congruence classes in $M_3(_q)$ (q odd)*, Discrete Mathematics, **219** (2000), 37-47.

[5] B. Corbas and G. D. Williams, *Congruence classes in $M_3(_q)$ (q even)*, Discrete Mathematics, **257** (2002), 15-27.

Chiteng'a John Chikunji
Department of Basics Sciences
Botswana College of Agriculture
Private Bag 0027
Gaborone, Botswana
e-mail address: jchikunj@bca.bw

(*Received February 01, 2007*)