UNIT GROUPS OF CUBE RADICAL ZERO COMMUTATIVE COMPLETELY PRIMARY FINITE RINGS

CHITENG’A JOHN CHIKUNJI

Received 1 July 2004

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 $J$. Let $R$ be a commutative completely primary finite ring with the unique maximal ideal $J$ such that $J^3 = (0)$ and $J^2 \neq (0)$. Then $R/J \cong GF(p^k)$, where $1 \leq k \leq 3$, for some prime $p$ and positive integer $r$. Let $R_o = GR(p^{kr}, p^k)$ be a Galois subring of $R$ and let the annihilator of $J$ be $J^2$ so that $R = R_o \oplus U \oplus V$, where $U$ and $V$ are finitely generated $R_o$-modules. Let nonnegative integers $s$ and $t$ be numbers of elements in the generating sets for $U$ and $V$, respectively. When $s = 2$, $t = 1$, and the characteristic of $R$ is $p$; and when $t = s(s + 1)/2$, for any fixed $s$, the structure of the group of units $R^*$ of the ring $R$ and its generators are determined; these depend on the structural matrices $(a_{ij})$ and on the parameters $p$, $k$, $r$, and $s$.

Notations

Throughout this paper, $R$ will denote a finite ring, unless otherwise stated, $J$ will denote the Jacobson radical of $R$, and we will denote the Galois ring $GR(p^n, p^n)$ of characteristic $p^n$ and order $p^{nr}$ by $R_o$, for some prime $p$, and positive integers $n$, $r$.

We denote the group of units of $R$ by $R^*$ and a cyclic group of order $\pi$ by $\epsilon(\pi)$. If $g$ is an element of $R^*$, then $o(g)$ denotes its order, and $\langle g \rangle$ denotes the cyclic group generated by $g$. Furthermore, 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 $\text{char} R$.

1. Introduction

In [6], Fuchs asked for a characterization of abelian groups which could be groups of units of a ring. This question was noted to be too general for a complete answer [12], and a natural course is to restrict the classes of groups or rings to be considered.

Let $R$ be a ring and let $R^*$ denote its multiplicative group of unit elements. All local rings $R$ with $R^*$ cyclic were determined by Gilmer [8] and this case was also considered by Ayoub [1] (also proofs are given in [10, 11]). Pearson and Schneider have found all
finite ring with maximal ideal $J$
sdirectly indecomposable finite rings having group of units isomorphic to $G$

In [5], Dolzan found all nonisomorphic rings with a group of units isomorphic to a

finite group $G$ (not necessarily abelian), there are, up to isomorphism, only finitely many
directly indecomposable finite rings having group of units isomorphic to $G$.

Ganske and McDonald [7] provided a solution for $R^*$ when the local ring $R$ has Jacob-
son radical $J$ such that $J^2 = (0)$ by showing that

$$R^* = \bigoplus_{i=1}^{nt} \epsilon(p)i \oplus \epsilon(|K| - 1),$$

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

In [5], Dolzan found all nonisomorphic rings with a 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 [12]. More recently, X.-D. Hou et al.
gave an algorithmic method for computing the structure of the group of units of a finite

commutative chain ring and further strengthening the known result by listing a set of

linearly independent generators for the group of units.

The present paper focuses on the group of units $R^*$ of a commutative completely pri-
mary finite ring $R$ with unique maximal ideal $J$ such that $R/J \cong GF(p^r)$, $J^3 = (0)$, and

$f^2 \neq (0)$ so that the characteristic of $R$ is $p^k$, where $1 \leq k \leq 3$; and further identifies sets of

generators for $R^*$.

In particular, let $R_o = GR(p^{kr}, p^k)$ be a Galois subring of $R$ and let the annihilator of
$J$ be $f^2$ so that $R = R_o \oplus U \oplus V$, where $U$ and $V$ are finitely generated $R_o$-modules. Let nonnegative integers $s$ and $t$ be numbers of elements in the generating sets for $U$ and $V$, respectively. When $s = 2$, $t = 1$, and $\text{char} R = p$, and when $t = s(s + 1)/2$, for any fixed $s$, the structure of the group of units $R^*$ of the ring $R$ and its generators have been determined; these depend on the structural matrices $(a_{ij})$ and on the parameters $p$, $k$, $r$, and $s$.

2. Preliminaries

We refer the reader to [2] for the general background of completely primary finite rings
$R$ with maximal ideals $J$ such that $J^3 = \{0\}$ and $J^2 \neq \{0\}$. Let $R$ be a completely primary finite ring with maximal ideal $J$ such that $J^3 = (0)$ and $J^2 \neq (0)$. Then $R$ is of order $p^{nr}$ and the residue field $R/J$ is a finite field $GF(p^r)$, for some prime $p$ and positive integers $n$, $r$. The characteristic of $R$ is $p^k$, where $k$ is an integer such that $1 \leq k \leq 3$. Let $GR(p^{kr}, p^k)$ be the Galois ring of characteristic $p^k$ and order $p^{kr}$, that is, $GR(p^{kr}, p^k) = \mathbb{Z}_{p^r}[x]/(f)$, where $f \in \mathbb{Z}_{p^r}[x]$ is a monic polynomial of degree $r$ whose image in $\mathbb{Z}_{p}[x]$ is irreducible.

Then, it can be deduced from the main theorem in [4] that $R$ 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 $m_1, m_2, \ldots, m_h \in J$ and automorphisms $\sigma_1, \ldots, \sigma_h \in \text{Aut}(R_0)$ such that

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

(as $R_0$-modules), $m_i r = r^{\sigma_i} m_i$, for every $r \in R_0$ and any $i = 1, \ldots, h$. Further, $\sigma_1, \ldots, \sigma_h$ are uniquely determined by $R$ and $R_0$. The maximal ideal of $R$ is

$$J = pR_0 \oplus \sum_{i=1}^{h} R_{o} m_i.$$ 

It is worth noting that $R$ contains an element $b$ of multiplicative order $p^r - 1$ and that $R_o = \mathbb{Z}_{p^r}[b]$ (see, e.g., [2, Result 1.3]).

The following results will be useful.

**Proposition 2.1.** Let $R$ be a completely primary finite ring (not necessarily commutative). Then the group of units $R^*$ of $R$ contains a cyclic subgroup $\langle b \rangle$ of order $p^r - 1$, and $R^*$ is a semidirect product of $1 + J$ and $\langle b \rangle$.

**Proof.** Obviously, the group of units $R^*$ of $R$ is $R - J$, $|R^*| = p^{(n-1)r}(p^r - 1)$, and $\phi : R \rightarrow R/J$ induces a surjective multiplicative group homomorphism $\phi : R^* \rightarrow (R/J)^*$. Since $\ker \phi = J$, we have $\ker \phi = 1 + J$. In particular, $1 + J$ is a normal subgroup of $R^*$.

Let $\langle \beta \rangle = (R/J)^*$, and let $b_o \in \phi^{-1}(\beta)$. Then, the multiplicative order of $b_o$ is a multiple of $p^r - 1$ and a divisor of $|R - J| = p^{nr} - p^{(n-1)r} = p^{(n-1)r}(p^r - 1)$; hence, of the form $p^{s}(p^r - 1)$. But then $b = b_o^{p^s}$ has multiplicative order $p^r - 1$ and $\phi(b_o^{p^s}) = \beta^{p^s}$, which is still a generator of $(R/J)^*$, since $(p^s, p^r - 1) = 1$.

Finally, since $|R^*| = |1 + J| \cdot |\langle b \rangle|$, and $(1 + J) \cap \langle b \rangle = 1$, we have $R^* = (1 + J) \cdot \langle b \rangle$, hence, $R^* = (1 + J) \times_\theta \langle b \rangle$, a semidirect product.

**Proposition 2.2.** Let $R$ be a completely primary finite ring (not necessarily commutative). Then the group of units $R^*$ is solvable.

**Proof.** That $R^*$ is a solvable group follows from the fact that $1 + J$ is a normal $p$-subgroup of $R^*$, and $R^*/(1 + J)$ is cyclic.

**Lemma 2.3.** Let $R$ be a completely primary finite ring (not necessarily commutative). If $G$ is a subgroup of $R^*$ of order $p^r - 1$, then $G$ is conjugate to $\langle b \rangle$ in $R^*$.

**Proof.** This follows from key properties of $p$-solvable groups contained in the variation of Sylow’s theorem, due to Philip Hall, since the order of $G$ is prime to its index in $R^*$ (see, e.g., [9, Theorem 8.2 page 25]).

**Proposition 2.4.** Let $R$ be a completely primary finite ring (not necessarily commutative). If $R^*$ contains a normal subgroup of order $p^r - 1$, then the set $K_o = \langle b \rangle \cup \{0\}$ is contained in the center of the ring $R$.

**Proof.** By Lemma 2.3, $\langle b \rangle$ is normal in $R^*$ and since $1 + J$ is a normal subgroup of $R^*$ with $|\langle b \rangle \cap (1 + J)| = 1$, it follows that $\langle b \rangle$ and $1 + J$ commute elementwise. Hence, $b$ lies in the center of $R$. 


Proposition 2.5. Let $R$ be a completely primary finite ring. Then, $(1 + J^i)/(1 + J^{i+1}) \cong J^i/J^{i+1}$ (the left-hand side as a multiplicative group and the right-hand side as an additive group).

Proof. Consider the map

$$\eta : (1 + J^i)/(1 + J^{i+1}) \longrightarrow J^i/J^{i+1}$$

defined by

$$(1 + x)(1 + J^{i+1}) \longrightarrow x + J^{i+1}.$$  (2.4)

Then it is easy to see that $\eta$ is an isomorphism. $\square$

Remark 2.6 (see [3, Result 2.7]). Let $R$ be a completely primary finite ring of characteristic $p^k$ and with Jacobson radical $J$. Let $R_o$ be a Galois subring of $R$. If $m \in J$ and $p^t$ is the additive order of $m$, for some positive integer $t$, then $|R_o m| = p^{tr}$.

Proof. Apply the fact that $R_o m \cong R_o/p^t R_o$. (2.5)

Now let $R$ be a commutative completely primary finite ring with maximal ideal $J$ such that $J^3 = (0)$ and $J^2 \neq (0)$. In [2], the author gave constructions describing these rings for each characteristic and for details, we refer the reader to [2, Sections 4 and 6].

If $R$ is a commutative completely primary finite ring with maximal ideal $J$ such that $J^3 = (0)$ and $J^2 \neq (0)$, then from Constructions A and B [2],

$$R = R_o \oplus U \oplus V \oplus W,$$  (2.6)

$$J = pR_o \oplus U \oplus V \oplus W,$$  (2.7)

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 $\lambda$; and the linearly independent matrices $(a_{ij}^k)$ defined in the multiplication. Let $\text{ann}(J)$ denote the two-sided annihilator of $J$ in $R$. Notice that since $J^2 \subseteq \text{ann}(J)$, we can write $R = R_o \oplus U \oplus M$, and hence, $J = pR_o \oplus U \oplus M$, where $M = V \oplus W$, and the multiplication in $R$ may be written accordingly. It is therefore easy to see that the description of rings of this type reduces to the case where $\text{ann}(J)$ coincides with $J^2$. Therefore, when investigating the structure of the group of units of this type of rings for a given order, say $p^{nr}$, where $\text{ann}(J)$ does not coincide with $J^2$, we will first write all the rings of this type of order $\leq p^{nr}$, where $\text{ann}(J)$ coincides with $J^2$.

In what follows, we assume that $\text{ann}(J) = J^2$.

Let $R_o = GR(p^{kr}, p^k)(1 \leq k \leq 3)$ and let nonnegative integers $s$ and $t$ be numbers of elements in the generating sets $\{u_1, \ldots, u_s\}$ and $\{v_1, \ldots, v_t\}$ for finitely generated $R_o$-modules $U$ and $V$, respectively, where $t \leq s(s + 1)/2$. Assume that $u_1, u_2, \ldots, u_s$ and $v_1, \ldots, v_t$ are commuting indeterminates. Then $R = R_o \oplus U \oplus V$.

By Proposition 2.1, and since $R$ is commutative,

$$R^* = \langle b \rangle \cdot (1 + J) \cong \langle b \rangle \times (1 + J),$$  (2.8)

a direct product.
Again, notice that since $R$ is of order $p^{nr}$ and $R^* = R - J$, it is easy to see that $|R^*| = p^{(n-1)r}(p' - 1)$ and $|1 + J| = p^{(n-1)r}$, so that $1 + J$ is an abelian $p$-group. Thus, $R^* \cong (\text{abelian } p\text{-group}) \times (\text{cyclic group of order } |R/J| - 1)$.

Our goal is to determine the structure and identify a set of generators of the multiplicative abelian $p$-group $1 + J$.

3. The group $1 + J$

Now let $R$ be a commutative completely primary finite ring with maximal ideal $J$ such that $J^3 = (0)$ and $J^2 \neq (0)$. Let $1 + J$ be the abelian $p$-subgroup of the unit group $R^*$.

The group $1 + J$ has a filtration $1 + J \supset 1 + J^2 \supset 1 + J^3 = \{1\}$ with filtration quotients $(1 + J)/(1 + J^2)$ and $(1 + J^2)/\{1\} = 1 + J^2$ isomorphic to the additive groups $J/J^2$ and $J^2$, respectively.

Remark 3.1. Notice that $1 + J^2$ is a normal subgroup of $1 + J$. But, in general, $1 + J$ does not have a subgroup which is isomorphic to the quotient $(1 + J)/(1 + J^2)$ as may be illustrated by the following example.

Example 3.2. Let $R = \mathbb{Z}_{p^3}$, where $p$ is an odd prime. Then $J = p\mathbb{Z}_{p^3}$, $\text{ann}(J) = J^2$, and $1 + J \cong \mathbb{Z}_{p^2}$, $1 + J^2 \cong \mathbb{Z}_p$, $(1 + J)/(1 + J^2) \cong \mathbb{Z}_p$.

Remark 3.3. In view of the above remark and example, we investigate the structure of $1 + J$ by considering various subgroups of $1 + J$.

3.1. The case when $s = 2$, $t = 1$, and char $R = p$. Suppose $s = 2$, $t = 1$, and char $R = p$. Let $R_0 = \mathbb{F}_q = GF(p^r)$, the Galois field of $q = p^r$ elements. Then

$$R = \mathbb{F}_q \oplus \mathbb{F}_q u_1 \oplus \mathbb{F}_q u_2 \oplus \mathbb{F}_q v,$$

the Jacobson radical

$$J = \mathbb{F}_q u_1 \oplus \mathbb{F}_q u_2 \oplus \mathbb{F}_q v,$$

$$J^2 = \mathbb{F}_q v. \quad (3.3)$$

The multiplication in $R$ is given by

$$u_1^2 = a_{11}v, \quad u_1 u_2 = u_2 u_1 = a_{12}v, \quad u_2^2 = a_{22}v, \quad (3.4)$$

where $a_{ij} \in \mathbb{F}_q$. The elements $a_{ij}$ form a nonzero symmetric matrix

$$\begin{pmatrix}
a_{11} & a_{12} \\
a_{21} & a_{22}
\end{pmatrix} \quad (3.5)$$

since $J^2 \neq (0)$.

Since $R^*$ is a direct product of the cyclic group $\langle b \rangle$ of order $p^r - 1$ and the group $1 + J$ of order $p^{3r}$, it suffices to determine the structure of $1 + J$. 

In this case,
\[
1 + J = 1 + \mathbb{F}_q u_1 \oplus \mathbb{F}_q u_2 \oplus \mathbb{F}_q v,
\]
and since \( s \) and \( t \) are fixed, the structure of \( 1 + J \) now depends on the prime \( p \), the integer \( r \), and the structural matrix \( \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \). We investigate this by considering cases depending on the type of the structural matrix.

Let \( \varepsilon_1, \varepsilon_2, \ldots, \varepsilon_r \) be elements of \( \mathbb{F}_q \) with \( \varepsilon_1 = 1 \) so that \( \bar{\varepsilon}_1, \bar{\varepsilon}_2, \ldots, \bar{\varepsilon}_r \) form a basis for \( \mathbb{F}_q \) regarded as a vector space over its prime subfield \( \mathbb{F}_p \).

**Case (i).** Suppose that \( \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \), with \( a \neq 0 \). Then
\[
1 + J \cong \begin{cases} \mathbb{Z}_4^r \times \mathbb{Z}_2^r, & \text{if char } R = 2, \\ \mathbb{Z}_p^r \times \mathbb{Z}_p^r \times \mathbb{Z}_p^r, & \text{if char } R = p \neq 2. \end{cases}
\]

To see this, we consider the two cases separately. So, suppose that \( p = 2 \). We first note the following results:
\[
1 + \varepsilon_i u_1 \in 1 + J, \quad (1 + \varepsilon_i u_1)^4 = 1, \quad (1 + \varepsilon_i u_2)^2 = 1, \quad g^4 = 1, \quad \forall g \in 1 + J.
\]

For positive integers \( k_i, l_i \), with \( k_i \leq 4, l_i \leq 2 \), we assert that
\[
\prod_{i=1}^{r} \left\{ (1 + \varepsilon_i u_1)^{k_i} \right\} \cdot \prod_{i=1}^{r} \left\{ (1 + \varepsilon_i u_2)^{l_i} \right\} = 1
\]
will imply \( k_i = 4 \) for all \( i = 1, \ldots, r \); and \( l_i = 2 \) for all \( i = 1, \ldots, r \).

If we set \( F_i = \{ (1 + \varepsilon_i u_1)^k \mid k = 1, \ldots, 4 \} \) for all \( i = 1, \ldots, r \); and \( G_i = \{ (1 + \varepsilon_i u_2)^l \mid l = 1, 2 \} \) for all \( i = 1, \ldots, r \), we see that \( F_i, G_i \) are all cyclic subgroups of the group \( 1 + J \) and that these are of the precise orders indicated by their definition. The argument above will show that the product of \( 2r \) subgroups \( F_i \) and \( G_i \) is direct. So, their product will exhaust the group \( 1 + J \).

When \( p \) is an odd prime, we have to consider the equation
\[
\prod_{i=1}^{r} \left\{ (1 + \varepsilon_i u_1)^{k_i} \right\} \cdot \prod_{i=1}^{r} \left\{ (1 + \varepsilon_i u_2)^{l_i} \right\} \cdot \prod_{i=1}^{r} \left\{ (1 + \varepsilon_i v)^{m_i} \right\} = 1
\]
and as each element in \( 1 + J \) raised to the power \( p \) equals 1, we see that \( 1 + J \) will be an elementary abelian group.

**Case (ii).** Suppose that \( \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} = \begin{pmatrix} 0 & a \\ a & 0 \end{pmatrix} \), with \( a \neq 0 \). Then
\[
1 + J \cong \mathbb{Z}_p^r \times \mathbb{Z}_p^r \times \mathbb{Z}_p^r,
\]
for every \( p = \text{char}R \). In this case, we consider the equation

\[
\prod_{i=1}^{r} \left\{ (1 + \varepsilon_i u_1)^{k_i} \right\} \cdot \prod_{i=1}^{r} \left\{ (1 + \varepsilon_i u_2)^{k_i} \right\} \cdot \prod_{i=1}^{r} \left\{ (1 + \varepsilon_i v)^{m_i} \right\} = 1 \tag{3.12}
\]

and the integers \( k_i, l_i, m_i \) will imply \( k_i = l_i = m_i = p \) for all \( i = 1, \ldots, r \).

If we set \( F_i = \{(1 + \varepsilon_i u_1)^k | k = 1, \ldots, p \} \) for all \( i = 1, \ldots, r \); \( G_i = \{(1 + \varepsilon_i u_2)^l | l = 1, \ldots, p \} \) for all \( i = 1, \ldots, r \); and \( H_i = \{(1 + \varepsilon_i v)^m | m = 1, \ldots, p \} \) for all \( i = 1, \ldots, r \), we see that \( F_i, G_i, \) and \( H_i \) are all cyclic subgroups of the group \( 1 + J \) and that these are all of order \( p \). The product of the \( 3r \) subgroups \( F_i, G_i, \) and \( H_i \) is direct. So, their product will exhaust the group \( 1 + J \).

**Case (iii).** Suppose now that \( \left( \begin{array}{c} a_{11} \\ a_{21} \\ a_{22} \end{array} \right) = \left( \begin{array}{c} a \\ b \\ 0 \end{array} \right) \), with \( a \) and \( b \) being nonzero. Then

\[
1 + J \cong \begin{cases} \mathbb{Z}_4^r \times \mathbb{Z}_2^r, & \text{if char } R = 2, \\ \mathbb{Z}_p^r \times \mathbb{Z}_p^r \times \mathbb{Z}_p^r, & \text{if char } R = p \neq 2. \end{cases} \tag{3.13}
\]

The argument is similar to that in Case (i).

**Case (iv).** Suppose \( \left( \begin{array}{c} a_{11} \\ a_{21} \\ a_{22} \end{array} \right) = \left( \begin{array}{c} a \\ 0 \\ b \end{array} \right) \), with \( a \) and \( b \) being nonzero. Then \( u_1^2 = av, u_2^2 = bv, \) and \( u_1 u_2 = u_2 u_1 = 0 \).

If char \( R = p \neq 2, \) then \( o(1 + \varepsilon_i u_1) = o(1 + \varepsilon_i u_2) = p(i = 1, \ldots, r) \). Moreover, for every \( i = 1, \ldots, r, \) \( \{1 + \varepsilon_i u_1\} \cap \{1 + \varepsilon_i u_2\} = \{1\} \). Also, \( o(1 + \varepsilon_i v) = p, \) and the element \( 1 + \varepsilon_i v (i = 1, \ldots, r) \) generates a cyclic subgroup of order \( p \).

If char \( R = 2, \) then in \( 1 + J, \) we see that \( o(1 + \varepsilon_i u_1) = 4 \) and for each \( \varepsilon_i, \) by considering the element \( 1 + \varepsilon_i u_1 + \varepsilon_i u_2 + \varepsilon_i v \) of order 2, one obtains the direct product

\[
1 + J = \prod_{i=1}^{r} \langle 1 + \varepsilon_i u_1 \rangle \times \prod_{i=1}^{r} \langle 1 + \varepsilon_i u_1 + \varepsilon_i u_2 + \varepsilon_i v \rangle. \tag{3.14}
\]

Hence,

\[
1 + J \cong \begin{cases} \mathbb{Z}_4^r \times \mathbb{Z}_2^r, & \text{if char } R = 2, \\ \mathbb{Z}_p^r \times \mathbb{Z}_p^r \times \mathbb{Z}_p^r, & \text{if char } R = p \neq 2. \end{cases} \tag{3.15}
\]

**Case (v).** Finally, suppose that \( \left( \begin{array}{c} a_{11} \\ a_{21} \\ a_{22} \end{array} \right) = \left( \begin{array}{c} a \\ b \\ c \end{array} \right) \), with \( a, b, \) and \( c \) being nonzero. Then \( u_1^2 = av, u_2^2 = cv, \) and \( u_1 u_2 = u_2 u_1 = bv \). In this case, it is easy to verify that

\[
1 + J \cong \begin{cases} \mathbb{Z}_4^r \times \mathbb{Z}_2^r, & \text{if char } R = 2, \\ \mathbb{Z}_p^r \times \mathbb{Z}_p^r \times \mathbb{Z}_p^r, & \text{if char } R = p \neq 2. \end{cases} \tag{3.16}
\]

The number of cases involved in determining the structure of \( 1 + J \) for larger values of \( s \) and for \( t < s(s+1)/2 \) compels us to investigate the problem by considering the extreme case when the invariant \( t = s(s+1)/2, \) and to leave the other cases for subsequent work.
3.2. The case when \( t = \frac{s(s+1)}{2} \), for \( s \) fixed. Suppose that \( t = \frac{s(s+1)}{2} \) for a fixed non-negative integer \( s \). Let \( u_1, u_2, \ldots, u_s \) be commuting indeterminates over the Galois ring \( R_0 = GR(p^k, p^k) \), where \( 1 \leq k \leq 3 \). Then it is easy to verify that

\[
R = R_0 \oplus \sum_{i=1}^s R_0 u_i \oplus \sum_{i,j=1}^s R_0 u_i u_j,
\]

(3.17)

where

\[
u_i u_j = u_j u_i,
\]

\[
u_i^2 = u_i^2 u_j = u_i u_j^2 = 0,
\]

for every \( i, j = 1, \ldots, s \),

(3.18)
is a commutative completely primary finite ring with Jacobson radical

\[
J = pR_0 \oplus \sum_{i=1}^s R_0 u_i \oplus \sum_{i,j=1}^s R_0 u_i u_j;
\]

(3.19)

\[
J^2 = pR_0 \oplus \sum_{i,j=1}^s R_0 u_i u_j \quad \text{or} \quad J^2 = p^2 R_0 \oplus \sum_{i,j=1}^s R_0 u_i u_j; \quad J^3 = (0).
\]

(3.20)

In this case, the linearly independent matrices \((a_{ij}^k)\) defined in the multiplication of \( R \) are the \( t = \frac{s(s+1)}{2}, s \times s \) symmetric matrices with 1’s in the \((i, j)\)th and \((j, i)\)th positions, and zeros elsewhere.

It follows clearly that

\[
1 + J = 1 + pR_0 \oplus \sum_{i=1}^s R_0 u_i \oplus \sum_{i,j=1}^s R_0 u_i u_j,
\]

(3.21)

and it can easily be deduced that every element \( x \) of \( 1 + J \) has a unique expression of the form

\[
x = 1 + p a_o + \sum_{i=1}^s a_i u_i + \sum_{i,j=1}^s a_{ij} u_i u_j,
\]

(3.22)

where \( a_o, a_i, a_{ij} = a_{ji} \) are in \( K = R_0/pR_0 \).

Let \( s \) be a fixed nonnegative integer and suppose that \( t = \frac{s(s+1)}{2} \). If \( \text{char} R = p \), then

\[
|R| = p^{((s^2+3s+2)/2)r}, \quad |J| = p^{((s^2+3s)/2)r}
\]

(3.23)
because \( |R_0 u_i| = p^r \) (for each \( i = 1, \ldots, s \)) and \( |R_0 u_i u_j| = p^r \) (for \( i, j = 1, \ldots, s \); thus

\[
|1 + J| = p^{(s^2+3s)/2r}.
\]

(3.24)

If \( \text{char} R = p^2 \), then

\[
|R| = p^{((s^2+5s+4)/2)r}, \quad |J| = p^{((s^2+5s+2)/2)r}
\]

(3.25)
because $|R_o| = p^{2^r}$, $|pR_o| = p^r$, $|R_o u_i| = p^{2^r}$, if $p u_i \neq 0$ (for each $i = 1, \ldots, s$) and $|R_o u_i u_j| = p^r$ (for $i$, $j = 1, \ldots, s$) (see Remark 2.6), and thus

$$|1 + J| = p^{((s^2 + 5s + 2)/2)r}.$$  (3.26)

Finally, if char $R = p^3$, then

$$|R| = p^{((s^2 + 5s + 6)/2)r}, \quad |J| = p^{((s^2 + 5s + 4)/2)r}$$  (3.27)

because $|R_o| = p^{3^r}$, $|pR_o| = p^{2^r}$ and if $p u_i \neq 0$, $|R_o u_i| = p^{2^r}$ (because $p^2 u_i = 0$) (for each $i = 1, \ldots, s$) and $|R_o u_i u_j| = p^r$ (for $i$, $j = 1, \ldots, s$) (see Remark 2.6 and also because $p u_i u_j = 0$), and hence,

$$|1 + J| = p^{((s^2 + 5s + 4)/2)r}.$$  (3.28)

**Proposition 3.4.** If char $R = p^k$, where $k = 2$ or 3, then $1 + J$ contains $1 + pR_o$ as its subgroup.

**Proof.** We only show the case for char $R = p^2$, the other case follows easily from this. Now, each element of $1 + pR_o$ is of the form $1 + pr$, for every $r \in R_o$, and for any two elements $1 + pr_1$ and $1 + pr_2$, we have

$$(1 + pr_1)(1 + pr_2) = 1 + (r_1 + r_2)$$  (3.29)

which is clearly an element of $1 + pR_o$. □

**Proposition 3.5.** For each pair $u_i$, $u_j$ with $i \neq j$ and $u_i u_j = u_j u_i$, $1 + R_o u_i u_j$ is a subgroup of $1 + J$.

**Proof.** It is easy to see that $1 + R_o u_i u_j$ is a subgroup of $1 + J$ because for any two elements $1 + r_1 u_i u_j$ and $1 + r_2 u_i u_j$ in $1 + R_o u_i u_j$, we have

$$(1 + r_1 u_i u_j)(1 + r_2 u_i u_j) = 1 + (r_1 + r_2)u_i u_j \in 1 + R_o u_i u_j$$  (3.30)

since $(u_i u_j)^2 = 0$. □

**Proposition 3.6.** For every $i = 1, \ldots, s$, $1 + R_o u_i + R_o u_i^2$ is a subgroup of $1 + J$.

**Proof.** Obviously,

$$(1 + r_1 u_i + r_2 u_i^2)(1 + s_2 u_i + s_2 u_i^2) = 1 + (r_1 + s_1) u_i + (r_1 s_1 + r_2 + s_2) u_i^2$$  (3.31)

lies in $1 + R_o u_i + R_o u_i^2$, for any pair $1 + r_1 u_i + r_2 u_i^2$ and $1 + s_2 u_i + s_2 u_i^2$ of elements in $1 + R_o u_i + R_o u_i^2$. □

In view of Remark 2.6 and Propositions 3.4, 3.5, and 3.6, we may now state the following.
Proposition 3.7. Let \( 1 + pR_o, 1 + R_o u_i + R_o u_i^2, \) and \( 1 + R_o u_i u_j \) be the subgroups of \( 1 + J \) defined above. Then

\[
\begin{align*}
|1 + pR_o| &= \begin{cases} p^r, & \text{if char } R = p^2, \\ p^{2r}, & \text{if char } R = p^3, \end{cases} \\
|1 + R_o u_i + R_o u_i^2| &= \begin{cases} p^{2r}, & \text{if char } R = p, \\ p^{3r}, & \text{if char } R = p^2, \\ p^{3r}, & \text{if char } R = p^3, \end{cases} \\
|1 + R_o u_i u_j| &= p^r,
\end{align*}
\]

(3.32) (3.33) (3.34)

for every characteristic of \( R. \)

Proposition 3.8. The group \( 1 + J \) is a direct product of the subgroup \( 1 + pR_o, s \) subgroups \( 1 + R_o u_i + R_o u_i^2, \) and \( s(s - 1)/2 \) subgroups \( 1 + R_o u_i u_j, \) where \( i \neq j \) and \( u_i u_j = u_j u_i. \)

Proof. This follows from the fact that \( 1 + pR_o, 1 + R_o u_i + R_o u_i^2, \) and \( 1 + R_o u_i u_j \) are subgroups of \( 1 + J, \) intersection of any pair of these subgroups is trivial (for every \( i, j = 1, \ldots, s \)), and by Proposition 3.7,

\[
|1 + J| = |1 + pR_o| \times \prod_{i=1}^{s} |1 + R_o u_i + R_o u_i^2| \times \prod_{i \neq j = 1}^{s} |1 + R_o u_i u_j|.
\]

(3.35)

\[\Box\]

3.2.1. The structure of \( 1 + pR_o. \) The structure of \( 1 + pR_o \) is completely determined by Raghavendran in [11]. For convenience of the reader, we state here the results useful for our purpose. For detailed proofs, refer to [11, Theorem 9].

We take \( r \) elements \( \epsilon_1, \ldots, \epsilon_r \) in \( R_o \) with \( \epsilon_1 = 1 \) such that the set \( \{\overline{\epsilon_1}, \ldots, \overline{\epsilon_r}\} \) is a basis of the quotient ring \( R_o/pR_o \) regarded as a vector space over its prime subfield \( GF(p). \) Then we have the following.

Proposition 3.9 [11, Theorem 9]. If \( \text{char } R_o = p^2, \) then \( 1 + pR_o \) is a direct product of \( r \) cyclic groups \( \langle 1 + p\epsilon_j \rangle, \) each of order \( p, \) for any prime \( p. \)

Proposition 3.10 [11, Theorem 9]. Let \( \text{char } R_o = p^3. \) If \( p = 2, \) then \( 1 + pR_o \) is a direct product of \( 2 \) cyclic groups \( \langle -1 + 4\epsilon_1 \rangle \) and \( \langle 1 + 4\epsilon_1 \rangle, \) each of order \( 2, \) and \( (r - 1) \) cyclic groups \( \langle 1 + 2\epsilon_j \rangle (j = 2, \ldots, r), \) each of order \( 4. \) If \( p \neq 2, \) then \( 1 + pR_o \) is a direct product of \( r \) cyclic groups \( \langle 1 + p\epsilon_j \rangle (j = 1, \ldots, r), \) each of order \( p^2. \)

3.2.2. The structure of \( 1 + R_o u_i + R_o u_i^2. \) We now consider the structure of the subgroup \( 1 + R_o u_i + R_o u_i^2 \) of the \( p \)-group \( 1 + J. \) We first note that if \( \text{char } R_o = p, \) then \( R_o = GF(p^r) \) the field of \( p^r \) elements, if \( \text{char } R_o = p^2, \) then \( R_o \) is the Galois ring \( GR(p^{2r}, p^2) \) of order \( p^{2r}, \) and if \( \text{char } R_o = p^3, \) \( R_o = GR(p^{3r}, p^3) \) the Galois ring of order \( p^{3r}. \)

We choose \( r \) elements \( \epsilon_1, \ldots, \epsilon_r \) in \( R_o \) with \( \epsilon_1 = 1 \) such that the set \( \{\overline{\epsilon_1}, \ldots, \overline{\epsilon_r}\} \) is a basis of the quotient ring \( R_o/pR_o \) regarded as a vector space over its prime subfield \( GF(p). \) Then we have the following.
Proposition 3.11. Let \( \text{char} R_o = p \). If \( p = 2 \), then \( 1 + R_o u_i + R_o u_i^2 \) is a direct product of \( r \) cyclic groups \( \langle 1 + \epsilon_j u_i \rangle (j = 1, \ldots, r) \), each of order 4. If \( p \neq 2 \), then \( 1 + R_o u_i + R_o u_i^2 \) is a direct product of \( 2r \) cyclic groups \( \langle 1 + \epsilon_j u_i \rangle \) and \( \langle 1 + 2\epsilon_j u_i \rangle (j = 1, \ldots, r) \), each of order \( p \).

Proof. If \( \text{char} R_o = 2 \), then \( \langle 1 + \epsilon_j u_i \rangle \) is of order 4, for every \( j = 1, \ldots, r \) and for any \( i = 1, \ldots, s \), and hence

\[
\prod_{j=1}^{r} \left| \langle 1 + \epsilon_j u_i \rangle \right| = 4^r = \left| 1 + R_o u_i + R_o u_i^2 \right|.
\]  

(3.36)

Therefore, the product \( \prod_{j=1}^{r} \langle 1 + \epsilon_j u_i \rangle \) is direct.

Similarly, if \( \text{char} R_o = p \neq 2 \), the elements \( 1 + \epsilon_j u_i \) and \( 1 + 2\epsilon_j u_i \) are each of order \( p \),

\[
\langle 1 + \epsilon_j u_i \rangle \cap \langle 1 + 2\epsilon_j u_i \rangle = \{1\},
\]  

(3.37)

for every \( j = 1, \ldots, r \), and

\[
\prod_{j=1}^{r} \left| \langle 1 + \epsilon_j u_i \rangle \right| \cdot \prod_{j=1}^{r} \left| \langle 1 + 2\epsilon_j u_i \rangle \right| = p^r \cdot p^r = \left| 1 + R_o u_i + R_o u_i^2 \right|,
\]  

(3.38)

hence

\[
1 + R_o u_i + R_o u_i^2 = \prod_{j=1}^{r} \langle 1 + \epsilon_j u_i \rangle \times \prod_{j=1}^{r} \langle 1 + 2\epsilon_j u_i \rangle,
\]  

(3.39)

a direct product.

\( \square \)

Proposition 3.12. Let \( \text{char} R_o = p^2 \). If \( p = 2 \), then \( 1 + R_o u_i + R_o u_i^2 \) is a direct product of \( r \) cyclic groups \( \langle 1 + 2\epsilon_j u_i \rangle \), each of order 2, and \( r \) cyclic groups \( \langle 1 + 3\epsilon_j u_i \rangle (j = 1, \ldots, r) \), each of order 4. If \( p \neq 2 \), then \( 1 + R_o u_i + R_o u_i^2 \) is a direct product of \( r \) cyclic groups \( \langle 1 + p\epsilon_j u_i \rangle \), each of order \( p \), and \( r \) cyclic groups \( \langle 1 + \epsilon_j u_i \rangle (j = 1, \ldots, r) \), each of order \( p^2 \).

Proof. Suppose \( \text{char} R_o = p^2 \). If \( p = 2 \), \( \langle 1 + 2\epsilon_j u_i \rangle \) is of order 2 and \( \langle 1 + 3\epsilon_j u_i \rangle \) is of order 4,

\[
\langle 1 + 2\epsilon_j u_i \rangle \cap \langle 1 + 3\epsilon_j u_i \rangle = \{1\},
\]  

(3.40)

for every \( j = 1, \ldots, r \) and any \( i = 1, \ldots, s \). Since

\[
\prod_{j=1}^{r} \left| \langle 1 + 2\epsilon_j u_i \rangle \right| \cdot \prod_{j=1}^{r} \left| \langle 1 + 3\epsilon_j u_i \rangle \right| = 2^r \cdot 4^r = \left| 1 + R_o u_i + R_o u_i^2 \right|,
\]  

(3.41)

it follows that

\[
1 + R_o u_i + R_o u_i^2 = \prod_{j=1}^{r} \langle 1 + 2\epsilon_j u_i \rangle \times \prod_{j=1}^{r} \langle 1 + 3\epsilon_j u_i \rangle
\]  

(3.42)

is a direct product.
If $p \neq 2$, it is easy to check that $|\langle 1 + p\varepsilon_j u_i \rangle| = p$, $|\langle 1 + \varepsilon_j u_i \rangle| = p^2$ and
\[
\langle 1 + p\varepsilon_j u_i \rangle \cap \langle 1 + \varepsilon_j u_i \rangle = \{1\}, \tag{3.43}
\]
for every $j = 1, \ldots, r$ and any $i = 1, \ldots, s$. Since
\[
\prod_{j=1}^r |\langle 1 + p\varepsilon_j u_i \rangle| \cdot \prod_{j=1}^r |\langle 1 + \varepsilon_j u_i \rangle| = p^r \cdot (p^2)^r = p^{3r} = |1 + R_o u_i + R_o u_i^2|, \tag{3.44}
\]
it follows that the product
\[
1 + R_o u_i + R_o u_i^2 = \prod_{j=1}^r \langle 1 + 2\varepsilon_j u_i \rangle \times \prod_{j=1}^r \langle 1 + 3\varepsilon_j u_i \rangle \tag{3.45}
\]
is direct.

**Proposition 3.13.** Let $\text{char } R_o = p^3$. If $p = 2$, then $1 + R_o u_i + R_o u_i^2$ is a direct product of $r$ cyclic groups $\langle 1 + \varepsilon_j u_i \rangle$, each of order 2, and $r$ cyclic groups $\langle 1 + \varepsilon_j u_i \rangle$ ($j = 1, \ldots, r$), each of order 4. If $p \neq 2$, then $1 + R_o u_i + R_o u_i^2$ is a direct product of $r$ cyclic groups $\langle 1 + \varepsilon_j u_i \rangle$, each of order $p$, and $r$ cyclic groups $\langle 1 + \varepsilon_j u_i \rangle$ ($j = 1, \ldots, r$), each of order $p^2$.

**Proof.** Similar to the proofs of Propositions 3.11 and 3.12. □

3.2.3. The structure of $1 + R_o u_i u_j$. Choose $r$ elements $\varepsilon_1, \ldots, \varepsilon_r$ in $R_o$ with $\varepsilon_1 = 1$ such that the elements $\overline{\varepsilon_1}, \ldots, \overline{\varepsilon_r}$ form a basis of the quotient ring $R_o/pR_o$ regarded as a vector space over its prime subfield $GF(p)$. Then we have the following.

**Proposition 3.14.** The group $1 + R_o u_i u_j$ is a direct product of $r$ cyclic groups $\langle 1 + \varepsilon_l u_i u_j \rangle$ ($l = 1, \ldots, r$), each of order $p$, for any characteristic $p^k$ ($1 \leq k \leq 3$) of $R$.

**Proof.** We first note that if the characteristic of $R$ is $p^k$, where $1 \leq k \leq 3$, then $p u_i u_j = 0$. Hence, $|1 + R_o u_i u_j| = p^r$. Also, for any $x \in 1 + R_o u_i u_j$, $x^{p^3} = 1$.

Now, for $r$ elements $\varepsilon_1, \ldots, \varepsilon_r \in R_o$ defined above, since for any $\nu \neq \mu$,
\[
\langle 1 + \varepsilon_\mu u_i u_j \rangle \cap \langle 1 + \varepsilon_\nu u_i u_j \rangle = 1, \tag{3.46}
\]
the result follows. □

We now state the main results of this section.

**Theorem 3.15.** Let $\text{char } R = p$. If $p = 2$, then $1 + J$ is a direct product of $(s(s - 1)/2)r$ cyclic groups, each of order 2, and $sr$ cyclic groups, each of order 4. If $p \neq 2$, then $1 + J$ is a direct product of $((s^2 + 3s)/2)r$ cyclic groups, each of order $p$.

**Proof.** This follows from Propositions 3.11 and 3.14 and by the fact that the order of $1 + J$ is $p^r((s^2 + 3s)/2)r$. □

**Theorem 3.16.** Let $\text{char } R = p^2$. Then $1 + J$ is a direct product of $((s^2 + s + 2)/2)r$ cyclic groups, each of order $p$, and $sr$ cyclic groups, each of order $p^2$, for any prime $p$. □
Proof. This follows from Propositions 3.9, 3.12, and 3.14 and from the fact that the order of $1 + J$ is $p^{((s^2 + 5s + 2)/2)r}$. □

**Theorem 3.17.** Let $\text{char } R = p^3$. If $p = 2$, then $1 + J$ is a direct product of $2 + ((s^2 + s)/2)r$ cyclic groups, each of order 2, and $r - 1 + sr$ cyclic groups, each of order 4. If $p \neq 2$, then $1 + J$ is a direct product of $((s^2 + s)/2)r$ cyclic groups, each of order $p$, and $(s + 1)r$ cyclic groups, each of order $p^2$.

Proof. First observe that the order of $1 + J$ is $p^{((s^2 + 5s + 4)/2)r}$. By Propositions 3.10, 3.13, and 3.14, the result follows. □

### 4. The Main theorem

By Proposition 2.1, the group of units $R^*$ of $R$ contains a cyclic subgroup $\langle b \rangle$ of order $p^r - 1$, and $R^*$ is a direct product of $1 + J$ and $\langle b \rangle$. Moreover, the structure of $1 + J$ has been determined in Section 3 (Theorems 3.15, 3.16, and 3.17). We thus have the following result.

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

(i) if $\text{char } R = p$, then

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

(ii) if $\text{char } R = p^2$, then

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

(iii) if $\text{char } R = p^3$, then

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

where $y = (s^2 - s)/2$.

Proof. Follows from Propositions 2.1 and 3.9 through 3.14 and Theorems 3.15, 3.16, and 3.17. □

**Remark 4.2.** The structure of the multiplicative groups of commutative completely primary finite rings $R$ with maximal ideals $J$ such that $J^3 = (0)$ and $J^2 \neq (0)$, for which $t < s(s + 1)/2$ for a fixed nonnegative integer $s$, will be considered in subsequent work.
References


Chiteng’a John Chikunji: Department of Mathematics, University of Transkei, Private Bag X1, Umtata 5117, South Africa
E-mail address: chikunji@getafix.utr.ac.za
Special Issue on
Singular Boundary Value Problems for Ordinary Differential Equations

Call for Papers

The purpose of this special issue is to study singular boundary value problems arising in differential equations and dynamical systems. Survey articles dealing with interactions between different fields, applications, and approaches of boundary value problems and singular problems are welcome.

This Special Issue will focus on any type of singularities that appear in the study of boundary value problems. It includes:

- Theory and methods
- Mathematical Models
- Engineering applications
- Biological applications
- Medical Applications
- Finance applications
- Numerical and simulation applications

Before submission authors should carefully read over the journal’s Author Guidelines, which are located at http://www.hindawi.com/journals/bvp/guidelines.html. Authors should follow the Boundary Value Problems manuscript format described at the journal site http://www.hindawi.com/journals/bvp/. Articles published in this Special Issue shall be subject to a reduced Article Processing Charge of €200 per article. Prospective authors should submit an electronic copy of their complete manuscript through the journal Manuscript Tracking System at http://mts.hindawi.com/ according to the following timetable:

<table>
<thead>
<tr>
<th>Event</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manuscript Due</td>
<td>May 1, 2009</td>
</tr>
<tr>
<td>First Round of Reviews</td>
<td>August 1, 2009</td>
</tr>
<tr>
<td>Publication Date</td>
<td>November 1, 2009</td>
</tr>
</tbody>
</table>

Lead Guest Editor

Juan J. Nieto, Departamento de Análisis Matemático, Facultad de Matemáticas, Universidad de Santiago de Compostela, Santiago de Compostela 15782, Spain; juanjose.nieto.roig@usc.es

Guest Editor

Donal O’Regan, Department of Mathematics, National University of Ireland, Galway, Ireland; donal.oregan@nuigalway.ie

Hindawi Publishing Corporation
http://www.hindawi.com