UNIT GROUPS OF A CERTAIN CLASS OF COMPLETELY PRIMARY FINITE RINGS

Chiteng’a John CHIKUNJI

Abstract. 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 $R/J \cong GF(p^r)$ and the characteristic of $R$ is $p^k$, 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 non-negative 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 $p^2$ and $p^3$; and when $s = 2, t = 2$ and the characteristic of $R$ is $p$, 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 $p, k, r, s$ and $t$.

1. INTRODUCTION

This is a sequel to [3] and 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. To recall, the problem is to determine the group of units $R^*$ of a commutative completely primary finite ring $R$ with unique maximal ideal $J$ such that $R/J \cong GF(p^r)$, $J^3 = (0)$ and $J^2 \neq (0)$ so that the characteristic of $R$ is $p^k$, for some prime $p$ and positive integers $r$ and $k$, where $1 \leq k \leq 3$; and further identify sets of linearly independent generators for $R^*$. In particular, let $R_o = GR(p^{kr}, p^k)$ be a Galois ring 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 non-negative integers $s$ and $t$ be numbers of elements in the generating sets for $U$ and $V$, respectively.

In the companion paper to the present we have determined $R^*$ when $s = 2, t = 1$ and $\text{char} R = p$; and when $t = \frac{s(s+1)}{2}$, for any fixed positive integer $s$, and we turn our attention here to the case where $s = 2, t = 1$ and characteristic of $R$ is $p^2$ and $p^3$; and the case where $s = 2, t = 2$ and $\text{char} R = p$. Our earlier strategy (that of considering different types of symmetric matrices) is thus not viable anymore and we have to follow a different
approach; that is, that of considering structural matrices of isomorphism classes of these types of rings with the same invariants $p$, $r$, $k$, $s$, and $t$.

We refer the reader to [1] 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 $\mathbb{G}(p^{k^r}, p^k)$ be the Galois ring of characteristic $p^k$ and order $p^{k^r}$, i.e., $\mathbb{G}(p^{k^r}, p^k) = \mathbb{Z}_{p^k}[x]/(f)$, where $f \in \mathbb{Z}_{p^k}[x]$ is a monic polynomial of degree $r$ whose image in $\mathbb{Z}_p[x]$ is irreducible. Then, it can be deduced from the main theorem in [6] that $R$ has a coefficient subring $R_0$ of the form $\mathbb{G}(p^{k^r}, p^k)$ which is clearly a maximal Galois subring of $R$. Moreover, there exist elements $m_1, m_2, \ldots, m_h \in J$ and automorphisms $\sigma_1, \ldots, \sigma_h \in Aut(R_0)$ such that

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

(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

$$J = pR_0 \oplus \sum_{i=1}^{h} R_0 m_i.$$

It is worth noting that $R$ contains an element $b$ of multiplicative order $p^r - 1$ and that $R_0 = \mathbb{Z}_{p^k}[b]$ (see, e.g. 1.3 in [1]).

The following results will be assumed (see [7] and [2]):

**Proposition 1.1.** Let $R$ be a completely primary finite ring (not necessarily commutative). Then,

(i) 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 $1 + J$ and $< b >$;

(ii) the group of units $R^*$ is solvable;

(iii) if $G$ is a subgroup of $R^*$ of order $p^r - 1$, the group $G$ is conjugate to $< b >$ in $R^*$;

(iv) if $R^*$ contains a normal subgroup of order $p^r - 1$, the set $K_0 = < b > \cup\{0\}$ is contained in the center of the ring $R$;

(v) $(1 + J^i)/(1 + J^{i+1}) \cong J^i/J^{i+1}$ (the left hand side as a multiplicative group and the right hand side as an additive group).

**Lemma 1.2.** [2, 2.7.] Let $R$ be a completely primary finite ring of characteristic $p^k$ and with Jacobson radical $J$. Let $R_0$ 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 $|R_om| = p^{tr}$.

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 [1], the author gave constructions describing these rings for each characteristic and for details, we refer the reader to sections 4 and 6 of [1].

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 in [1],

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

and

$$J = pR_o \oplus U \oplus V \oplus W,$$

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 $\lambda$; and the linearly independent matrices $(a_{ij}^k)$ defined in the multiplication. Let $ann(J)$ denote the two sided annihilator of $J$ in $R$. Notice that since $J^2 \subseteq ann(J)$, 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 $ann(J)$ 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 $ann(J)$ does not coincide with $J^2$, we shall first write all the rings of this type of order $\leq p^{nr}$, where $ann(J)$ coincides with $J^2$.

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

Let $R_o = GR(p^{kr_0}, p^k)$ $(1 \leq k \leq 3)$ and let non-negative integers $s$ and $t$ be numbers of elements in the generating sets $\{u_1, ..., u_s\}$ and $\{v_1, ..., v_t\}$ for finitely generated $R_o$—modules $U$ and $V$, respectively, where $t \leq \frac{s(s+1)}{2}$. Assume that $u_1$, $u_2$, ..., $u_s$ and $v_1$, ..., $v_t$ are commuting indeterminates. Then $R = R_o \oplus U \oplus V$.

As before, and since $R$ is commutative,

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

a direct product.

Again, notice that since $R$ is of order $p^{nr}$ and $R^* = R - J$, it is easy to see that $|R^*| = p^{(n-1)r}(p^r - 1)$ 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 $1 + J$. 
2. THE GROUP $1 + J$

In this section we determine the structure of the abelian $p$–group $1 + J$. We do this case by case based on the characteristic of the ring $R$ and the invariants $s$ and $t$.

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

The following result is fundamental in the study of the group of units of the rings in this paper.

**Lemma 2.1.** 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: $\mathbb{Z}^* = \{1, -1\} \cong \mathbb{Z}_3^* = \{1, 2\}$, while $\mathbb{Z}$ (infinite) and $\mathbb{Z}_3$ (finite) are non-isomorphic rings.

2.1. **The case when char$R = p^2$, $s = 2$ and $t = 1$.** Let the characteristic of the ring $R$ be $p^2$, and let $s = 2$ and $t = 1$. Then

$$R = R_o \oplus R_o u_1 \oplus R_o u_2 \oplus R_o v_1,$$

and the Jacobson radical

$$J = pR_o \oplus R_o u_1 \oplus R_o u_2 \oplus R_o v_1,$$

where $R_o = GR(p^{2r}$, $p^2$), the Galois ring of characteristic $p^2$ and order $p^{2r}$, for any positive integer $r$, and prime integer $p$, and we have

$$u_i u_j = a_{ij}^1 p + a_{ij}^2 pu_1 + a_{ij}^3 pu_2 + a_{ij}^4 v_1,$$

where $a_{ij}^1$, $a_{ij}^2$, $a_{ij}^3$, $a_{ij}^4 \in R_o/pR_o$. 
From the definition of the multiplication in the ring $R$, we deduce two cases; namely, (i) the case when $p \in J^2$, and (ii) the case when $p \in J - J^2$. These cases do not overlap and we treat them in turn.

2.1.1. Case (i). Suppose that $p \in J^2$. Then the multiplication in $R$ is as defined

$$u_i u_j = a^1_{ij} p + a^2_{ij} v_1.$$ 

Since these four products span $J^2$, the symmetric matrices $A = (a^1_{ij})$, $B = (a^2_{ij})$ are linearly independent, and one verifies that any such pair of matrices gives rise to a ring of the present type. If we change to new generators $u_1', u_2', v_1'$ with corresponding matrices $A', B'$, then $u_1', u_2'$ are linear combinations of $u_1, u_2, v_1, p$. Since $J^3 = (0)$, we may assume that the coefficients of $v_1, p$ are zero and write

$$u_i = p_1 u_1 + p_2 u_2,$$

and compare coefficients of $v_1, p$ we obtain equations which, in matrix form are:

$$\begin{align*}
P^t A P &= k A', \\
P^t B P &= m A' + B',
\end{align*}$$

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 pairs of symmetric matrices $(A, B)$ under the above equivalence relation, in which $P \in GL_2(R_o/pR_o)$, $k \in (R_o/pR_o)^*$, $m \in R_o/pR_o$ are arbitrary. Observe that $Q = \begin{pmatrix} k & 0 \\ m & 1 \end{pmatrix}$ is the transition matrix from the basis $\{v_1, p\}$ of $J^2$ to the basis $\{v_1', p\}$. This is similar to the situation of [4, 5], wherein $Q$ is an element of $GL_2$. We deduce from Theorem 3 in [5] that if $p = 2$, there are up to isomorphism, three commutative rings with pairs of structural matrices

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

and from Theorem 3 in [4] that if $p$ is odd, there are up to isomorphism, three commutative rings with pairs of structural matrices

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

where $g$ is a fixed non-square in $(R_o/pR_o)^*$.

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

$$1 + J = 1 + pR_o \oplus R_o u_1 \oplus R_o u_2 \oplus R_o v_1.$$
To simplify our notation, we shall call a ring with characteristic $2^2$, a ring of Type I, if it is isomorphic to a ring with structural matrices

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

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

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

**Proposition 2.2.** If $\text{char } R = p^2$, $s = 2$, $t = 1$, and suppose that $p \in J^2$. Then

(i) $1 + J \cong \mathbb{Z}_p^r \times \mathbb{Z}_p^r \times \mathbb{Z}_p^r \times \mathbb{Z}_p^r$, if $p$ is odd; and when $p = 2$,

(ii) $1 + J \cong \left\{ \begin{array}{ll}
\mathbb{Z}_2^r \times \mathbb{Z}_2^r, & \text{if } R \text{ is of Type I;} \\
\mathbb{Z}_2^r \times \mathbb{Z}_2^r \times \mathbb{Z}_2^r, & \text{if } R \text{ is of Type II.}
\end{array} \right.$

**Proof.** If $p \in J^2$, let $a = 1 + x$ be an element of $1 + J$ with the highest possible order and assume that $x \in J - J^2$. Then

$$o(a) = \begin{cases} p, & \text{if } p \text{ is odd;} \\
p^2, & \text{if } p = 2.\end{cases}$$

This is true because

$$(1 + x)^p = 1 + px + \frac{p(p-1)}{2}x^2 \quad (\text{since } x^3 = 0)$$

$$= 1 + \frac{p(p-1)}{2}x^2 \quad (\text{since } p \in J^2 \text{ and } px = 0).$$

It is easy to see that if $p$ is odd, then $(1 + x)^p = 1$; and if $p = 2$, then $(1 + x)^p = 1 + x^2$. But then

$$(1 + x^2)^2 = 1 + 2x^2 + x^4$$

$$= 1, \quad \text{since } x^3 = 0 \text{ and } 2x^2 = 0.$$

Now, let $\varepsilon_1, \ldots, \varepsilon_r \in R_o$ with $\varepsilon_1 = 1$ such that $\overline{\varepsilon}_1, \ldots, \overline{\varepsilon}_r \in R_o/pR_o \cong GF(p')$ form a basis for $GF(p')$ over $GF(p)$.

We consider the two cases separately. So, suppose that $p$ is odd. We first note the following results: For each $i = 1, \ldots, r$, $\varepsilon_{i}p, (1 + \varepsilon_{i}p)^p = 1$, $(1 + \varepsilon_{i}u_1)^p = 1, (1 + \varepsilon_{i}u_2)^p = 1, (1 + \varepsilon_{i}v_1)^p = 1$, and $g^p = 1$ for all $g \in 1 + J$.

For integers $k_i, l_i, m_i, n_i \leq p$, we assert that

$$\prod_{i=1}^{r}(1 + \varepsilon_{i}p)^{k_i} \cdot \prod_{i=1}^{r}(1 + \varepsilon_{i}u_1)^{l_i} \cdot \prod_{i=1}^{r}(1 + \varepsilon_{i}u_2)^{m_i} \cdot \prod_{i=1}^{r}(1 + \varepsilon_{i}v_1)^{n_i} = 1,$$

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

If we set $E_i = \{ (1 + \varepsilon_{i}p)^k | k = 1, \ldots, p \}, F_i = \{ (1 + \varepsilon_{i}u_1)^l | l = 1, \ldots, p \}$, $G_i = \{ (1 + \varepsilon_{i}u_2)^m | m = 1, \ldots, p \}$ and $H_i = \{ (1 + \varepsilon_{i}v_1)^n | n = 1, \ldots, p \}$, for all
$i = 1, \ldots, r$; we see that $E_i$, $F_i$, $G_i$, $H_i$ are all subgroups of the group $1 + J$ and these are all of order $p$ as indicated in their definition. The argument above will show that the product of the $4r$ subgroups $E_i$, $F_i$, $G_i$ and $H_i$ is direct. So, their product will exhaust $1 + J$. This proves (i).

To prove part (ii), suppose $p = 2$. We first observe that $(1 + \varepsilon_i u_1)^4 = 1$, in both cases, and if the ring $R$ is of Type II, the element $1 + \varepsilon_i u_2$ will be of order 2, while if it is of Type I, it will be of order 4.

If $R$ is of Type II, then for each $i = 1, \ldots, r$, and for integers $k_i \leq 4$, and $l_i, m_i \leq p$, we assert that the equation

\[
\prod_{i=1}^{r} \{(1 + \varepsilon_i u_1)^{k_i}\} \cdot \prod_{i=1}^{r} \{(1 + \varepsilon_i u_2)^{l_i}\} \cdot \prod_{i=1}^{r} \{(1 + \varepsilon_i v_1)^{m_i}\} = 1,
\]

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

If we set $E_i = \{(1 + \varepsilon_i u_1)^k|k = 1, \ldots, 4\}$, $F_i = \{(1 + \varepsilon_i u_2)^l|l = 1, 2\}$, and $G_i = \{(1 + \varepsilon_i v_1)^m|m = 1, 2\}$, for all $i = 1, \ldots, r$; we see that $E_i$, $F_i$, $G_i$ are all subgroups of the group $1 + J$ and these are of the precise order as indicated in their definition; and if $R$ is of Type I, the equation

\[
\prod_{i=1}^{r} \{(1 + \varepsilon_i u_1)^{k_i}\} \cdot \prod_{i=1}^{r} \{(1 + \varepsilon_i u_2)^{l_i}\} = 1,
\]

will imply $k_i = 4$, and $l_i = 4$, for all $i = 1, \ldots, r$. If we set $H_i = \{(1 + \varepsilon_i u_1)^k|k = 1, \ldots, 4\}$, and $K_i = \{(1 + \varepsilon_i u_2)^l|l = 1, \ldots, 4\}$, we see that $E_i$ and $F_i$ are subgroups of $1 + J$, each of order 4. The argument above will show that the product of the $3r$ subgroups $E_i$, $F_i$, and $G_i$ is direct; and the product of the $2r$ subgroups $H_i$ and $K_i$ is direct; and in both cases, these products will exhaust $1 + J$. \hfill \Box

2.1.2. Case (ii). Suppose that $p \in J - J^2$. Then the multiplication in $R$ is now defined by

\[u_i u_j = a_{ij}^1 p u_1 + a_{ij}^2 p u_2 + a_{ij}^3 v_1.\]

Let us assume that $pu_1 \neq 0$ and $pu_2 \neq 0$. Since these four products span $J^2$, the symmetric matrices $A = (a_{ij}^1)$, $B = (a_{ij}^2)$ and $C = (a_{ij}^3)$ are linearly independent over $R_o/pR_o$, and one verifies that any such triple of linearly independent symmetric matrices $A$, $B$, $C$ gives rise to a ring of the present type. All rings of this type are isomorphic to the ring with structural matrices of the form

\[
\begin{pmatrix}
1 & 0 \\
0 & 0
\end{pmatrix}, \quad \begin{pmatrix}
0 & 0 \\
0 & 1
\end{pmatrix}, \quad \begin{pmatrix}
0 & 1 \\
1 & 0
\end{pmatrix};
\]

since all vector spaces of symmetric $2 \times 2$ matrices of equal dimension 3 over the same field $\mathbb{F}_{q}$, are isomorphic.
Proposition 2.3. If $\text{char} R = p^2$, $s = 2$, $t = 1$, and suppose that $p \in J - J^2$. Suppose further that $pu_1 \neq 0$ and $pu_2 \neq 0$. Then

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

Proof. If $p \in J - J^2$, let $a = 1 + x$ be an element of $1 + J$ with the highest possible order and assume that $x \in J - J^2$. Then

$$o(a) = \begin{cases} 
p^2, & \text{if } p \text{ is odd; or } p = 2 \text{ and } r > 1; 
p, & \text{if } p = 2 \text{ and } r = 1.
\end{cases}$$

This is true because, for any $\varepsilon_i$ ($i = 1, \ldots, r$),

$$(1 + \varepsilon_i x)^p = 1 + p\varepsilon_i x + \frac{p(p-1)}{2}(\varepsilon_i x)^2 \quad \text{(since } x^3 = 0).$$

If $p$ is odd, then $(1 + \varepsilon_i x)^p = 1 + p\varepsilon_i x$, since $px^2 = 0$. Now,

$$\begin{align*}
(1 + p\varepsilon_i x)^p &= 1 + p^2\varepsilon_i x + \frac{p(p-1)}{2}(p\varepsilon_i x)^2 \\
&= 1, \quad \text{since } \text{char} R = p^2.
\end{align*}$$

Hence, $(1 + \varepsilon_i x)^{p^2} = 1$. However, if $p$ is even, and $\varepsilon_i \neq 1$, for $i = 2, \ldots, r$, then

$$(1 + \varepsilon_i x)^2 = 1 + 2\varepsilon_i x + 2\varepsilon_i^2 x \text{ and } (1 + \varepsilon_i x)^4 = 1;$$

and if $r = 1$,

$$\begin{align*}
(1 + x)^2 &= 1 + 2x + x^2 \\
&= 1 + 2x + 2x \quad \text{(since in this case, } x^2 = px) \\
&= 1 + 2^2 x \\
&= 1,
\end{align*}$$

so that $o(1 + x) = 2$ and $o(1 + \varepsilon_i x) = 4$, $\varepsilon_i \neq 1$, for $i = 2, \ldots, r$.

Notice also that $1 + J = (1 + pR_o) \times (1 + R_0u_1 \oplus R_0u_2 \oplus R_0v_1)$. Choose $\varepsilon_1, \ldots, \varepsilon_r \in R_o$ with $\varepsilon_1 = 1$ such that $\varepsilon_1, \ldots, \varepsilon_r \in R_o/pR_o \cong GF(p^r)$ form a basis for $GF(p^r)$ over $GF(p)$.

If $p$ is odd, since for each $i = 1, \ldots, r$, $(1 + \varepsilon_i u_1)^p = 1$, $(1 + \varepsilon_i u_2)^p = 1$, $(1 + \varepsilon_i v_1)^p = 1$, the direct product of the cyclic subgroups $< 1 + \varepsilon_i u_1 >$, $< 1 + \varepsilon_i u_2 >$ and $< 1 + \varepsilon_i v_1 >$ exhaust $1 + R_0u_1 \oplus R_0u_2 \oplus R_0v_1$.

If $p = 2$, and $r = 1$, $(1 + u_1)^2 = 1$, $(1 + 2u_1)^2 = 1$, $(1 + u_2)^2 = 1$, $(1 + 2u_2)^2 = 1$, and $(1 + v_1)^2 = 1$, and these elements generate subgroups of $1 + J$ of the given orders; and
if \( p = 2 \), \( r > 1 \), we have \((1 + \varepsilon_i u_1)^4 = 1\), \((1 + \varepsilon_i u_2)^4 = 1\), and \((1 + \varepsilon_i v)^2 = 1\), and also these elements generate subgroups of \(1 + J\) of the given orders. Moreover, their direct product gives rise to the subgroup \(1 + R_o u_1 \oplus R_o u_2 \oplus R_o v_1\).

The structure of \(1 + pR_o\) is given in [7], Theorem 9 (1), and it is a direct product of \(r\) cyclic groups, each of order \(p\). Thus, \(1 + J\) is of the required form, and this completes the proof.

We remark here that the case for which only one of \(pu_1\), \(pu_2\) is zero has a similar argument to that given in 2.1.1, and one may deduce the structure of \(1 + J\) from Proposition 2.2.

2.2. The case when \(\text{char} R = p^3\), \(s = 2\) and \(t = 1\). Let the characteristic of the ring \(R\) be \(p^3\), and let \(s = 2\) and \(t = 1\). Then

\[ R = R_o \oplus R_o u_1 \oplus R_o u_2 \oplus R_o v_1, \]

and the Jacobson radical

\[ J = pR_o \oplus R_o u_1 \oplus R_o u_2 \oplus R_o v_1, \]

where \(R_o = GR(p^{3r}, p^3)\), the Galois ring of characteristic \(p^3\) and order \(p^{3r}\), for any positive integer \(r\), and prime integer \(p\), and we have

\[ u_i u_j = a_{ij}^1 p^2 + a_{ij}^2 pu_1 + a_{ij}^3 pu_2 + a_{ij}^4 v_1, \]

where \(a_{ij}^1, a_{ij}^2, a_{ij}^3, a_{ij}^4 \in R_o/pR_o\).

From the definition of the multiplication in the ring \(R\), we deduce two cases; namely, (i) the case when \(pu_1 = 0\), \(pu_2 = 0\), and (ii) the case when one of \(pu_1\), \(pu_2\) is zero, and the other product is non-zero. These two cases do not overlap and we treat them in turn. Notice that \(pu_1\), \(pu_2\) can not both be non-zero, since this will lead to 4 symmetric \(2 \times 2\) matrices which are clearly dependent over \(R_o/pR_o\).

2.2.1. Case(i). Suppose that \(pu_1 = 0\), \(pu_2 = 0\). Then the multiplication in \(R\) is as defined by

\[ u_i u_j = a_{ij}^1 p^2 + a_{ij}^2 v_1, \]

and we have two linearly independent symmetric matrices \(A = (a_{ij}^1)\), \(B = (a_{ij}^2)\) over \(R_o/pR_o\). The argument is the same as that in 2.1.1, and we may deduce from Theorem 3 in [5] that if \(p = 2\), there are up to isomorphism, three commutative rings with pairs of structural matrices

\[
\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}; \quad \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}; \quad \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix};
\]
and from Theorem 3 in [4] that if $p$ is odd, there are up to isomorphism, three commutative rings with pairs of structural matrices
\[
\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}; \begin{pmatrix} 1 & 0 \\ 0 & g \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}; \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix};
\]
where $g$ is a fixed non-square in $(R_o/pR_o)^*$. We again simplify our notation by calling a ring of characteristic 2 a ring of Type III, if it is isomorphic to the ring with structural matrices
\[
\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \text{ or } \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix};
\]
and of Type IV, if it is isomorphic to a ring with structural matrices
\[
\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.
\]

**Proposition 2.4.** If $char R = p^3$, $s = 2$, $t = 1$, and suppose that $pu_1 = 0$, $pu_2 = 0$. Then

(i) $1 + J \cong \mathbb{Z}_p^3 \times \mathbb{Z}_p^3 \times \mathbb{Z}_p^3 \times \mathbb{Z}_p^3$, if $p$ is odd; and when $p = 2$,

(ii) $1 + J \cong \begin{cases} \mathbb{Z}_4^3 \times \mathbb{Z}_4^3 \times \mathbb{Z}_2, & \text{if } R \text{ is of Type III;} \\
\mathbb{Z}_4^3 \times \mathbb{Z}_4^3 \times \mathbb{Z}_2^2 \times \mathbb{Z}_2^2, & \text{if } R \text{ is of Type IV.}
\end{cases}

**Proof.** If $pu_1 = 0$, $pu_2 = 0$, let $a = 1 + x$ be an element of $1 + J$ with the highest possible order and assume that $x \in J - J^2$. Then $o(a) = p^2$, for every prime $p$. This is true because

\[
(1 + x)^p = 1 + px + \frac{p(p-1)}{2} x^2 \quad \text{(since } x^3 = 0)\]

It is easy to see that if $p$ is odd, then $(1 + x)^p = 1 + px$, since $px^2 = 0$. So,

\[
(1 + px)^p = 1 + p(px) + \frac{p(p-1)}{2} (px)^2 = 1 + p^2 x = 1, \quad \text{since } p^2 x = 0.
\]

If $p = 2$, then $(1 + x)^2 = 1 + 2x + x^2$, and

\[
(1 + 2x + x^2)^2 = 1 + 4x + 6x^2 + 4x^3 + x^4 = 1 + 4x + 6x^2 = 1, \quad \text{since } char R = 2^3 \text{ and } 2x^2 = 0.
\]

Now, let $\varepsilon_1, \ldots, \varepsilon_r \in R_o$ with $\varepsilon_1 = 1$ such that $\overline{\varepsilon_1}, \ldots, \overline{\varepsilon_r} \in R_o/pR_o \cong GF(p^r)$ form a basis for $GF(p^r)$ over $GF(p)$. Then the proof is essentially the proof of Proposition 2.2 with slight changes that

(i) if $p$ is odd, then $1 + J$ contains subgroups $<1 + \varepsilon_i p + \varepsilon_i u_1>$ each of order $p^2$, for every $i = 1, \ldots, r$; and
(ii) if $p$ is even, then $1 + J$ contains an extra $r$ subgroups, each of order $p$.

The small changes preserve each of the previous results up to the inclusion of the direct products of these extra subgroups. Therefore, with a few modifications, everything goes through as before. Hence, if $p$ is odd, then

$$1 + J = \prod_{i=1}^{r} < 1 + \varepsilon_{i} > \times \prod_{i=1}^{r} < 1 + \varepsilon_{i} > \times \prod_{i=1}^{r} < 1 + \varepsilon_{i} >$$

a direct product (proving part (i)); and if $p$ is even and $R$ is of type III, then

$$1 + J = \prod_{i=1}^{r} < 1 + 4\varepsilon_{i} > \times \prod_{i=1}^{r} < 1 + \varepsilon_{i} > \times \prod_{i=1}^{r} < 1 + \varepsilon_{i} >$$

a direct product, and if $R$ is of type IV, then

$$1 + J = \prod_{i=1}^{r} < 1 + 4\varepsilon_{i} > \times \prod_{i=1}^{r} < 1 + \varepsilon_{i} > \times \prod_{i=1}^{r} < 1 + \varepsilon_{i} >$$

a direct product. This completes the proof. \[\square\]

2.2.2. Case (ii). Suppose that $pu_1 = 0$, $pu_2 \neq 0$. Then the multiplication in $R$ is now defined by

$$u_iu_j = a_{ij}^{1}p^2 + a_{ij}^{2}pu_2 + a_{ij}^{3}v_1.$$  

Since these four products span $J^2$, the symmetric matrices $A = (a_{ij}^{1})$, $B = (a_{ij}^{2})$ and $C = (a_{ij}^{3})$ are linearly independent over $R_0/pR_0$, and one verifies that any such triple of linealy independent symmetric matrices $A$, $B$, $C$ gives rise to a ring of the present type. All rings of this type are isomorphic to the ring with structural matrices of the form

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

(see 2.1.2 case (ii)).

**Proposition 2.5.** If $\text{char} R = p^3$, $s = 2$, $t = 1$, and suppose that $pu_1 = 0$, $pu_2 \neq 0$. Then

$$1 + J \cong \begin{cases} \mathbb{Z}_2^r \times \mathbb{Z}_2^r \times \mathbb{Z}_2^r \times \mathbb{Z}_2^r, & \text{if } p = 2; \\
\mathbb{Z}_p^r \times \mathbb{Z}_p^r \times \mathbb{Z}_p^r \times \mathbb{Z}_p^r, & \text{if } p \neq 2. \end{cases}$$
Proof. If \( pu_1 = 0, pu_2 \neq 0 \), let \( a = 1 + x \) be an element of \( 1 + J \) with the highest possible order and assume that \( x \in J - J^2 \). Then \( o(a) = p^2 \), for every prime \( p \). This is true because

\[
(1 + x)^p = 1 + px + \frac{p(p - 1)}{2} x^2 \quad \text{(since } x^3 = 0).\]

It is easy to see that if \( p \) is odd, then \( (1 + x)^p = 1 + px \), since \( px^2 = 0 \). So,

\[
(1 + px)^p = 1 + p(px) + \frac{p(p - 1)}{2} (px)^2 \\
= 1 + p^2 x \\
= 1, \text{ since } p^2 x = 0.
\]

If \( p = 2 \), then \( (1 + x)^2 = 1 + 2x + x^2 \), and

\[
(1 + 2x + x^2)^2 = 1 + 4x + 6x^2 + 4x^3 + x^4 \\
= 1 + 4x + 6x^2 \\
= 1, \text{ since } char R = 2^3 \text{ and } 2x^2 = 0.
\]

Now, let \( \varepsilon_1, \ldots, \varepsilon_r \in R_o \) with \( \varepsilon_1 = 1 \) such that \( \varepsilon_1, \ldots, \varepsilon_r \in R_o/pR_o \cong GF(p^r) \) form a basis for \( GF(p^r) \) over \( GF(p) \). Then since for each \( i = 1, \ldots, r, \) and \( p \) odd, \( (1 + \varepsilon_i p + \varepsilon_i u_1)^2 = 1, (1 + \varepsilon_i u_1)^p = 1, (1 + \varepsilon_i u_2)^2 = 1, \) \( (1 + \varepsilon_i u_1) \) is trivial, and the order of the group generated by the direct product of these cyclic subgroups coincides with \( |1 + J| \), it follows that

\[
1 + J = \prod_{i=1}^{r} < 1 + \varepsilon_i p + \varepsilon_i u_1 > \times \prod_{i=1}^{r} < 1 + \varepsilon_i u_1 > \times \prod_{i=1}^{r} < 1 + \varepsilon_i u_2 > \\
= \prod_{i=1}^{r} < 1 + \varepsilon_i v_1 >,
\]

a direct product. This proves the second result. To prove the first part, we first observe that \( (1 + \varepsilon_i u_1)^4 = 1 \), and the elements \( 1 + \varepsilon_i u_2 \) and \( 1 + \varepsilon_i u_2 \) are all of order 2. Now, since for each \( i = 1, \ldots, r, (1 + 4\varepsilon_i)^2 = 1, (1 + \varepsilon_i u_1)^4 = 1, \) \( (1 + \varepsilon_i u_2)^2 = 1, (1 + 2\varepsilon_i u_2)^2 = 1, \) \( (1 + \varepsilon_i v_1)^2 = 1 \), and the order of the group generated by the direct product of the cyclic subgroups \( < 1 + 4\varepsilon_i >, \) \( < 1 + \varepsilon_i u_1 >, < 1 + \varepsilon_i u_2 >, < 1 + 2\varepsilon_i u_2 > \) and \( < 1 + \varepsilon_i v_1 > \) coincides with \( |1 + J| \), and their intersection is the identity group, it follows that

\[
1 + J = \prod_{i=1}^{r} < 1 + 4\varepsilon_i > \times \prod_{i=1}^{r} < 1 + \varepsilon_i u_1 > \times \prod_{i=1}^{r} < 1 + \varepsilon_i u_2 >
\]
\[
\times \prod_{i=1}^{r} < 1 + 2\varepsilon_i u_2 > \times \prod_{i=1}^{r} < 1 + \varepsilon_i v_1 >,
\]
a direct product. This completes the proof. \( \square \)

2.3. **The case when** \( \text{char} R = p, s = 2 \) **and** \( t = 2 \). **In this case,**

\[
R = \mathbb{F}_q \oplus \mathbb{F}_q u_1 \oplus \mathbb{F}_q u_2 \oplus \mathbb{F}_q v_1 \oplus \mathbb{F}_q v_2,
\]

and the Jacobson radical

\[
J = \mathbb{F}_q u_1 \oplus \mathbb{F}_q u_2 \oplus \mathbb{F}_q v_1 \oplus \mathbb{F}_q v_2,
\]

where \( \mathbb{F}_q = GF(p^r) \), for some positive integer \( r \) and any prime integer \( p \).

The multiplication in \( R \) is defined by

\[
u_i u_j = a_{ij}^1 v_1 + a_{ij}^2 v_2,
\]

where \( a_{ij}^1, a_{ij}^2 \in \mathbb{F}_q \), and the two symmetric matrices \( A = (a_{ij}^1), B = (a_{ij}^2) \) are linearly independent over \( \mathbb{F}_q \), since the four products \( u_i u_j \) span \( J^2 \). The ring structure is determined by the pair of \( 2 \times 2 \) symmetric matrices \( A = (a_{ij}^1), B = (a_{ij}^2) \), which are linearly independent over \( \mathbb{F}_q \), and any pair of independent symmetric matrices defines such a ring. The problem of determining the number of isomorphism classes of such rings and of finding normal forms for the pair of matrices \( A, B \) defining them, was treated in [4] and [5]. There are exactly three commutative types of these rings for any prime characteristic \( p \). These are represented by the following structural matrices:

\[
\begin{pmatrix}
1 & 0 \\
0 & 0
\end{pmatrix}, \quad
\begin{pmatrix}
0 & 0 \\
0 & 1
\end{pmatrix}; \quad
\begin{pmatrix}
1 & 0 \\
0 & 1
\end{pmatrix}, \quad
\begin{pmatrix}
0 & 1 \\
1 & 1
\end{pmatrix}; \quad
\begin{pmatrix}
1 & 0 \\
0 & 0
\end{pmatrix}, \quad
\begin{pmatrix}
0 & 1 \\
1 & 0
\end{pmatrix};
\]

if \( p = 2 \); and

\[
\begin{pmatrix}
1 & 0 \\
0 & 0
\end{pmatrix}, \quad
\begin{pmatrix}
0 & 0 \\
0 & 1
\end{pmatrix}; \quad
\begin{pmatrix}
1 & 0 \\
0 & g
\end{pmatrix}, \quad
\begin{pmatrix}
0 & 1 \\
1 & 0
\end{pmatrix}; \quad
\begin{pmatrix}
1 & 0 \\
0 & 0
\end{pmatrix}, \quad
\begin{pmatrix}
0 & 1 \\
1 & 0
\end{pmatrix};
\]

if \( p \) is odd, where \( g \) is a fixed non-square in \( \mathbb{F}_q \) (see e.g. Theorem 3 [5], and Theorem 3 [4], respectively).

We now proceed to determine the structure of \( 1 + J \). Notice that

\[
1 + J = 1 + \mathbb{F}_q u_1 \oplus \mathbb{F}_q u_2 \oplus \mathbb{F}_q v_1 \oplus \mathbb{F}_q v_2.
\]

To simplify our notation again, we shall call a ring of characteristic 2, a **ring of Type V**, if it is isomorphic to a ring with structural matrices

\[
\begin{pmatrix}
1 & 0 \\
0 & 0
\end{pmatrix}, \quad
\begin{pmatrix}
0 & 0 \\
0 & 1
\end{pmatrix} \quad \text{or} \quad
\begin{pmatrix}
1 & 0 \\
0 & 1
\end{pmatrix}, \quad
\begin{pmatrix}
0 & 1 \\
1 & 1
\end{pmatrix};
\]

and a **ring of Type VI** if it is isomorphic to a ring with structural matrices

\[
\begin{pmatrix}
1 & 0 \\
0 & 0
\end{pmatrix}, \quad
\begin{pmatrix}
0 & 1 \\
1 & 0
\end{pmatrix}.
\]
Proposition 2.6. If $\text{char}R = p$, $s = 2$, $t = 2$, then

(i) $1 + J \cong \mathbb{Z}_p^r \times \mathbb{Z}_p^r \times \mathbb{Z}_p^r \times \mathbb{Z}_p^r$, if $p$ is odd; and when $p = 2$,

(ii) $1 + J \cong \begin{cases} \mathbb{Z}_2^r \times \mathbb{Z}_4^r, & \text{if } R \text{ is of Type V;} \\ \mathbb{Z}_4^r \times \mathbb{Z}_2^r \times \mathbb{Z}_2^r, & \text{if } R \text{ is of Type VI.} \end{cases}$

Proof. Let $a = 1 + x$ be an element of $1 + J$ with the highest possible order and assume that $x \in J - J^2$. Then

$$o(a) = \begin{cases} p, & \text{if } p \text{ is odd;} \\ p^2, & \text{if } p = 2. \end{cases}$$

This is true because

$$(1 + x)^p = 1 + px + \frac{p(p-1)}{2}x^2 \quad \text{(since } x^3 = 0)$$

$$= 1 + \frac{p(p-1)}{2}x^2 \quad \text{(since } p \in J^2 \text{ and } px = 0).$$

It is easy to see that if $p$ is odd, then $(1 + x)^p = 1$; and if $p = 2$, then $(1 + x)^p = 1 + x^2$. But then

$$(1 + x^2)^2 = 1 + 2x^2 + x^4$$

$$= 1, \quad \text{since } x^3 = 0 \text{ and } 2x^2 = 0.$$ 

Now, let elements $\varepsilon_1, ..., \varepsilon_r \in \mathbb{F}_q$ with $\varepsilon_1 = 1$ be a basis for $GF(p^r)$ over $GF(p)$. Then the proof is essentially the proof of Proposition 2.2, with a few modifications; and if $p$ is odd, then

$$1 + J = \prod_{i=1}^{r} < 1 + \varepsilon_i u_1 > \times \prod_{i=1}^{r} < 1 + \varepsilon_i u_2 > \times \prod_{i=1}^{r} < 1 + \varepsilon_i v_1 >$$

$$\times \prod_{i=1}^{r} < 1 + \varepsilon_i v_2 >,$$

a direct product, proving (i); and if $p$ is even and $R$ is of type V, then

$$1 + J = \prod_{i=1}^{r} < 1 + \varepsilon_i u_1 > \times \prod_{i=1}^{r} < 1 + \varepsilon_i u_2 >,$$

a direct product, while if $R$ is of type VI,

$$1 + J = \prod_{i=1}^{r} < 1 + \varepsilon_i u_1 > \times \prod_{i=1}^{r} < 1 + \varepsilon_i u_2 + \varepsilon_i v_1 > \times \prod_{i=1}^{r} < 1 + \varepsilon_i v_2 >,$$

a direct product; proving part (ii). This completes the proof. \hfill \Box

In summary, we have proved:
Theorem 2.7. Let $R$ be a commutative completely primary finite ring of the introduction with unique maximal ideal $J$. If $\text{char} R = p^2$ or $p^3$, $s = 2$, $t = 1$; and $\text{char} R = p$, $s = 2$, $t = 2$; then, the group of units $R^\ast$ of $R$ is the direct product of a cyclic group $\mathbb{Z}_{p^r - 1}$ and the $p$–group $(1 + J)$, whose structure is given in Propositions 2.2 – 2.6.

ACKNOWLEDGEMENT

The author is very grateful to the Managing Editor, Professor Naoki Tanaka for the valuable advice on the use of jokayama.cls package.

REFERENCES