Units of a class of finite rings of characteristic p^3

Chitengá John Chikunji
Department of Biometry and Mathematics
Botswana University of Agriculture and Natural Resources
Private Bag 0027, Gaborone
Botswana
jchikunj@buan.ac.bw

Abstract. Let R be a commutative completely primary finite ring with Jacobson radical $\mathcal{J}$ such that $\mathcal{J}^3 = (0)$, $\mathcal{J}^2 \neq (0)$ and $R/\mathcal{J} \cong GF(p^r)$, the finite field with p^r elements, for any prime p and any positive integer r. Then, characteristic of R is either p, p^2 or p^3. In this paper, we determine the structure and generators of the group of units of the ring R in the special case when the characteristic of R is p^3. We treat the problem by considering fixed dimensions and bases for the vector spaces $\mathcal{J}^i/\mathcal{J}^{i+1}$ $(i = 1,\ 2)$ over the residue field $R/\mathcal{J}$ and by fixing the order of the ideal $\mathcal{J}^2$. This complements the author's earlier solution to the problem in the case when the characteristic of R is p or p^2 and $\mathcal{J}^2 \subseteq ann(\mathcal{J})$, the annihilator of $\mathcal{J}$.

Keywords: finite commutative rings, unit groups.

1. Introduction

Throughout this paper, all rings are finite and commutative (unless otherwise stated) with identity element $1 \neq 0$, subrings have the same identity, ring homomorphisms preserve 1 and modules are unital. A finite ring R is called *completely primary* if all its zero divisors including the zero element form the unique maximal ideal $\mathcal{J}$. Completely primary finite rings are precisely local rings with unique maximal ideals. For a given completely primary finite ring R, 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 a prime integer p and positive integers $n,\ r$. We denote the group of units of R by $U(R)$; if g is an element of $U(R)$, then $o(g)$ denotes its order, and $< g >$ denotes the cyclic group generated by g. Similarly, if $f(x) \in R[x]$, we shall denote by $< f(x) >$ the ideal generated by $f(x)$. Further, for a subset A of R or $U(R)$, $|A|$ 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$R$. The symbol K will denote the residue field $R/\mathcal{J}$ and K_o will denote the set of coset representatives of the maximal ideal $\mathcal{J}$ in the ring R. We denote a direct product of r cyclic groups of $\mathbb{Z}_m$ by $\mathbb{Z}_m^r$ or by $\underbrace{\mathbb{Z}_m \times \ \cdots \ \times \mathbb{Z}_m}_{r}$.

If I is an ideal of R generated by the elements $a,\ b$, we shall denote this by $I = (a,\ b)$.

Let R be a completely primary finite ring with maximal ideal $\mathcal{J}$. Then, $|R| = p^{nr}$, $\mathcal{J}$ is the Jacobson radical of R, $\mathcal{J}^m = (0)$, where $m \leqslant n$, $|\mathcal{J}| = p^{(n-1)r}$, and the residue field $R/\mathcal{J} \cong GF(p^r)$, the finite field of p^r elements, for some prime p and positive integers $n,\ r$. The characteristic char$R$ of R is equal to $R = p^k$, where $1 \leqslant k \leqslant m$. If $k = n$, then $R = \mathbb{Z}_{p^k}[b]$, where b is an element of R of order $p^r - 1$; $\mathcal{J} = pR$ and $Aut(R) \cong Aut(R/pR)$ (see Proposition 2 in [5]). Such a ring is called a *Galois ring*, denoted by $GR(p^{kr},\ p^k)$, and a concrete model is the quotient $\mathbb{Z}_{p^k}[x]/ < f(x) >$, where $f(x)$ is a monic polynomial of degree r, irreducible modulo p. Any such polynomial will do: the rings are all isomorphic. Trivial cases are $GR(p^n,\ p^n) = \mathbb{Z}_{p^n}$ and $GR(p^n,\ p) = \mathbb{F}_{p^n}$. Furthermore, if $k < n$ and char$R = p^k$, it can be deduced from [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, if $R_o^{'}$ is another coefficient subring of R then there exists an invertible element x in R such that $R_o^{'} = xR_ox^{-1}$ (see Theorem 8 in [5]). The maximal ideal of R_o is

$$\mathcal{J}_o = pR_o = \mathcal{J} \cap R_o, \quad \text{and} \quad R_o/\mathcal{J}_o \cong GF(p^r).$$

Let $\psi : R_o \longrightarrow R_o/\mathcal{J}_o$ be the canonical map. Since the element b has order $p^r - 1$ and $\mathcal{J}_o \subset \mathcal{J}$, we have that $\psi(b)$ is a primitive element of $R_o/\mathcal{J}_o$. Let $K_o =< b > \cup\{0\}$ and let $R_o = \mathbb{Z}_{p^k}[b]$ be a coefficient subring of R of order p^{kr}. Then, it is easy to show that every element of R_o can be written uniquely as $\sum_{i=0}^{k-1} \lambda_i p^i$, where $\lambda_i \in K_o$. Also, there exist elements $m_1,\ m_2, \ldots, m_h \in \mathcal{J}$ and automorphisms $\sigma_1, \ldots, \sigma_h \in Aut(R_o)$ such that

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

for every $r \in R_o$ and any $i = 1, \ldots, h$. Further, $\sigma_1, \ldots, \sigma_h$ 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 ring (not necessarily commutative) of order p^{nr} with unique maximal ideal $\mathcal{J}$. Then, the set $R - \mathcal{J}$ consisting of invertible elements in R forms a group with respect to the multiplication defined on R, called the group of units of R. The following facts are useful for our purpose (e.g. see [5, §2]): The group of units $U(R)$ of R contains a cyclic subgroup $< b >$ of order $p^r - 1$, and it is a semi-direct product of $1 + \mathcal{J}$ by $< b >$; the group $U(R)$ is solvable; if G is a subgroup of $U(R)$ of order $p^r - 1$, then G is conjugate to $< b >$ in $U(R)$; if $U(R)$ 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). It is easy to check that $|U(R)| = p^{(n-1)r}(p^r - 1)$ and that $|1 + \mathcal{J}| = p^{(n-1)r}$, so that $1 + \mathcal{J}$ is a p-group.

In [1], the author studied completely primary finite rings with unique maximal ideals $\mathcal{J}$ such that $\mathcal{J}^3 = (0)$, $\mathcal{J}^2 \neq (0)$ for all the characteristics. For more details on the structure and construction of these rings, the interested reader may refer to [1].

Let R be a commutative completely primary finite ring with Jacobson radical $\mathcal{J}$ such that $\mathcal{J}^3 = (0)$ and $\mathcal{J}^2 \neq (0)$ (see, for example, [1]). Then, in view of the above results, char$R$ is either $p,\ p^2$ or p^3. The ring R contains a coefficient subring R_o with charR_o =char$R$, and with R_o/pR_o equal to $R/\mathcal{J}$. Moreover, R_o is a Galois ring of the form $GR(p^{kr},\ p^k)$, $k = 1,\ 2$ or 3. Let $ann(\mathcal{J})$ denote the two-sided annihilator of $\mathcal{J}$ in R. Of course $ann(\mathcal{J})$ is an ideal of R. Because $\mathcal{J}^3 = (0)$, it follows easily that $\mathcal{J}^2 \subseteq ann(\mathcal{J})$.

From now on, we assume that the characteristic of the ring R is p^3. Because $\mathcal{J}^3 = (0)$, we have that $p^2 m_i = 0$, for all $m_i \in \mathcal{J}$. Further, $pm_i = 0$ for all $m_i \in ann(\mathcal{J})$. In particular, $pm_i = 0$ for all $m_i \in \mathcal{J}^2$. It is now obvious to see that p lies in $\mathcal{J} - \mathcal{J}^2$, and $p^2 \in \mathcal{J}^2$. Let $B_1 = \{p,\ u_1,\ ...,\ u_s\}$ denote the set of elements of $\mathcal{J}$ whose images modulo $\mathcal{J}^2$ form a $K-$basis for $\mathcal{J}/\mathcal{J}^2$ so that $dim_K(\mathcal{J}/\mathcal{J}^2)$ is $d_1 = 1 + s$, and let $B_2 = \{p^2,\ pu_1,\ ..., pu_d,\ u_1^2,\ u_1u_2, \ldots, u_s^2\}$ denote the set of elements of $\mathcal{J}$ whose images modulo $\mathcal{J}^3(\cong (0))$ form a $K-$basis for $\mathcal{J}^2$, so that $dim_K(\mathcal{J}^2)$ is $d_2 = 1 + d + t$, where $t \leqslant s(s+1)/2$, i.e. $d_2 \leqslant (1+s)(2+s)/2$. Then, an arbitrary element in R is of the form

$$a_o + a_1 p + a_2 p^2 + \sum_{i}^{s} b_i u_i + \sum_{l=1}^{d} c_l p u_l + \sum_{i,j=1}^{s} d_{ij} u_i u_j, \quad (a_o,\ a_1,\ b_i,\ c_l,\ d_{ij} \in K_o).$$

Clearly, the products $u_i u_j \in \mathcal{J}^2$. Hence, we conclude that p^2, pu_i and $u_i u_j$ $(i,\ j = 1, \ldots, s)$ generate $\mathcal{J}^2$. In fact, we can write any $v \in \mathcal{J}^2$ as a linear combination of p^2, pu_i and $u_i u_j$ as follows:

$$v = \alpha_0 p^2 + \sum_{i=1}^{d} \alpha_i p u_i + \sum_{i,\ j=1}^{s} \alpha_{ij} u_i u_j,$$

where $\alpha_0,\ \alpha_i,\ \alpha_{ij} \in R_o/pR_o$. Clearly, $|R| = p^{3r} \cdot p^{2dr} \cdot p^{(s-d)r} \cdot p^{tr} = p^{(3+s+d+t)r}$ and $|\mathcal{J}| = p^{(2+s+d+t)r}$. (Notice that $|R_o u_i| = p^{2r}$ if $pu_i \neq 0$, and $|R_o u_i| = p^r$, if otherwise.)

In this paper, we determine explicitly the group of units of all commutative completely primary finite rings R with Jacobson radical $\mathcal{J}$ such that $\mathcal{J}^3 = (0)$, $\mathcal{J}^2 \neq (0)$, and of characteristic p^3. We treat the problem by considering fixed dimensions and bases for the vector spaces $\mathcal{J}^i/\mathcal{J}^{i+1}$ $(i = 1,\ 2)$ over the residue field $K = R/\mathcal{J}$ and by fixing the order of the ideal $\mathcal{J}^2$. First, if a ring R has $\mathcal{J}$ such that d_i =dim$_K\mathcal{J}^i/\mathcal{J}^{i+1}$ $(i = 1,\ 2)$, then as we shall see later, we may further classify R according to the behaviour of a generating set for $\mathcal{J}$. In particular, we determine the group of units of the ring R with $dim_K(\mathcal{J}/\mathcal{J}^2) = 1 + s$ and $dim_K(\mathcal{J}^2) \leqslant (1+s)(2+s)/2$ under the given conditions (see Section

2) on the basis elements of $\mathcal{J}^2$ over K. This complements the author's earlier solution of the problem [2] in the case when the characteristic of R is p or p^2 and $\mathcal{J}^2 \subseteq ann(\mathcal{J})$, the annihilator of $\mathcal{J}$.

2. The group of units

Let R be a commutative completely primary finite ring with Jacobson radical $\mathcal{J}$ such that $\mathcal{J}^3 = (0)$, $\mathcal{J}^2 \neq (0)$, and of characteristic p^3. Suppose that $\mathcal{J} = (p,\ u_1,\ ...,\ u_s)$ so that $dim_K(\mathcal{J}/\mathcal{J}^2) = 1 + s$, for any integer $s \geqslant 0$. As noted above, the non-zero elements p^2, $pu_i\ (i = 1, \ldots, s)$, $u_iu_j\ (i,\ j = 1, \ldots, s)$ span $\mathcal{J}^2$ over K. If $pu_i = 0$, then $u_i \in ann(\mathcal{J}) \supseteq \mathcal{J}^2$ and as such for every element $x \in \mathcal{J}$, we have $u_ix = xu_i = 0$. In particular, $u_iu_j = 0\ (\forall i,\ j = 1, \ldots, s)$. We also note that $p\mathcal{J} \subseteq \mathcal{J}^2$ is spanned by the non-zero elements p^2 and $pu_i\ (i = 1, \ldots, s)$, since $pu_iu_j = 0\ (\forall i,\ j = 1, \ldots, s)$.

Following the above observations, we determine the structure of the group of units $U(R)$ of the ring R under the conditions listed below:
(i) $\mathcal{J} = (p,\ u_1, \ldots, u_s)$, $pu_i = u_iu_j = 0$, so that $\mathcal{J}^2 = (p^2)$, $dim_K(\mathcal{J}^2) = 1$ and $|\mathcal{J}^2| = p^r$;
(ii) $\mathcal{J} = (p,\ u_1, \ldots, u_s)$, $\mathcal{J}^2 = p\mathcal{J}$, so that $u_iu_j = 0$, $dim_K(\mathcal{J}^2) \leqslant 1 + s$ and $|\mathcal{J}^2| \leqslant p^{(1+s)r}$; and
(iii) $\mathcal{J} = (p,\ u_1, \ldots, u_s)$, $\mathcal{J}^2 = (p^2,\ pu_i, \ldots, pu_s,\ u_iu_j)\ (i,\ j = 1, \ldots, s)$, $dim_K(\mathcal{J}^2) \leqslant (s + 1)(s + 2)/2$ and $|\mathcal{J}^2| \leqslant p^{[(s+1)(s+2)/2]r}$.

One easily verifies that the above cases are all commutative completely primary finite rings of characteristic p^3 with unique maximal ideal $\mathcal{J}$ such that $\mathcal{J}^3 = (0)$ and $\mathcal{J}^2 \neq (0)$. Also, to distinguish (iii) from the other two cases, we assume that $pu_i \neq 0$ for at least one u_i, and $u_iu_j \neq 0$ for at least one product.

We know that for a commutative completely primary finite ring R,

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

a direct product of the $p-$group $1 + \mathcal{J}$ by the cyclic subgroup $< b >$. Thus, since the structure of $< b >$ is basic, it suffices to determine the structure of the subgroup $1 + \mathcal{J}$ in order to obtain the complete structure of $U(R)$.

There are many important results on the group of units of certain finite rings. For example, it is well known that the multiplicative group of the finite field $GF(p^r)$ is a cyclic group of order $p^r - 1$, and the multiplicative group of the finite ring $\mathbb{Z}/p^k\mathbb{Z}$, the ring of integers modulo p^k, for p a prime number, and k a positive integer, is a cyclic group of order $p^{k-1}(p - 1)$ if p is odd, and is a direct product of a cyclic group of order 2 and a cyclic group of order 2^{k-2}, if $p = 2$.

Let $U(R_o)$ denote the group of units of the Galois ring $R_o = GR(p^{nr},\ p^n)$. Then, $U(R_o)$ has the following structure [5]:

Theorem 2.1. *$U(R_o) = < b > \times (1 + pR_o)$, where $< b >$ is the cyclic group of order $p^r - 1$ and $1 + pR_o$ is of order $p^{(n-1)r}$ whose structure is described below.*

(i) If (a) p is odd, or (b) $p = 2$ and $n \leqslant 2$, then $1 + pR_o$ is the direct product of r cyclic groups each of order $p^{(n-1)}$.

(ii) When $p = 2$ and $n \geqslant 3$, the group $1 + pR_o$ is the direct product of a cyclic group of order 2, a cyclic group of order $2^{(n-2)}$ and $r - 1$ cyclic groups each of order $2^{(n-1)}$.

In Propositions 2.2 and 2.3, we will provide detailed proofs for the two types of rings of this paper, while in Proposition 2.1, we merely state $U(R)$ and their generators for the other type of rings, as the proofs are very similar and may be proved by slight modifications of these.

For the rest of this paper, we shall take r elements $\varepsilon_1, \ldots, \varepsilon_r$ in R_o with $\varepsilon_1 = 1$ such that $\{\overline{\varepsilon_1}, \ldots, \overline{\varepsilon_r}\}$ is a basis for the quotient ring R_o/pR_o regarded as a vector space over its prime subfield $GF(p)$.

2.1 The case when $\mathcal{J}^2 = (p^2)$ and $pu_i = u_iu_j = 0$

Let $dim_K(\mathcal{J}/\mathcal{J}^2) = 1 + s$ and suppose that $\mathcal{J} = (p,\ u_1, \ldots, u_s)$, for any integer $s \geqslant 0$. Suppose further that $pu_i = u_iu_j = 0$, for every $i,\ j = 1, \ldots, s$. Then, $\mathcal{J}^2 = (p^2)$, $dim_K(\mathcal{J}^2) = 1$ and $|\mathcal{J}^2| = p^r$. The following result determines the structure of the group of units of R and its generators.

Proposition 2.1. *Let R be a ring of characteristic p^3 with maximal ideal $\mathcal{J}$ such that $\mathcal{J}^3 = \{0\}$, $\mathcal{J}^2 \neq \{0\}$. Suppose further that there exist elements $u_1, \ldots, u_s$ in $\mathcal{J}$ such that the multiplication in R is defined by $pu_i = 0$, $u_iu_j = 0$, for every $i,\ j = 1,\ \ldots,\ s$. Then,*

$$U(R) \cong \begin{cases} \mathbb{Z}_{2^r-1} \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_4^{r-1} \times \underbrace{\mathbb{Z}_2^r \times \ \cdots \ \times \mathbb{Z}_2^r}_{s}, & if\ p = 2; \\ \mathbb{Z}_{p^r-1} \times \mathbb{Z}_{p^2}^r \times \underbrace{\mathbb{Z}_p^r \times \ \cdots \ \times \mathbb{Z}_p^r}_{s}, & if\ p\ is\ odd. \end{cases}$$

Moreover, if $p = 2$, then $1 + \mathcal{J}$ is generated by $(-1 + 4\varepsilon_1)$, $(1 + 4\varepsilon_1)$, each of order 2, $(r-1)$ cyclic groups $< 1 + 2\varepsilon_j >$ $(j = 2, \ldots, r)$, each of order 4, and sr cyclic groups $< 1 + \varepsilon_j u_i >$, each of order 2, for $i = 1, \ldots, s$. If p is odd, then $1 + \mathcal{J}$ is generated by $1 + p\varepsilon_j$ $(j = 1, \ldots, r)$, each of order p^2, and sr cyclic groups $1 + \varepsilon_j u_i$ $(j = 1, \ldots, r)$, each of order p, for $i = 1, \ldots, s$.

2.2 The case when $\mathcal{J}^2 = p\mathcal{J}$

Let $dim_K(\mathcal{J}/\mathcal{J}^2) = 1 + s$ and suppose that $\mathcal{J} = (p,\ u_1, \ldots, u_s)$, for any integer $s \geqslant 0$. Suppose further that $pu_i \neq 0$ for $i = 1, \ldots, d \leqslant s$ and $pu_j = 0$ for $j = d+1, \ldots, s$. Then, $u_iu_j = 0$, for every $i,\ j = 1, \ldots, s$ and $dim_K(\mathcal{J}^2) \leqslant 1+s$. The following determines the structure and generators of the group of units of the ring R.

Proposition 2.2. *Let R be a ring of characteristic p^3 with maximal ideal $\mathcal{J}$ such that $\mathcal{J}^3 = \{0\}$, $\mathcal{J}^2 \neq \{0\}$. Suppose further that there exist elements $u_1, \ldots, u_s$*

in $\mathcal{J}$ such that the multiplication in R is defined by $pu_i \neq 0$, for $i = 1, \dots, d \leqslant s$, $pu_j = 0$, for $j = d+1, \dots, s$, and $u_iu_j = 0$, for every $i,\ j = 1,\ \dots,\ s$. Then,

$$U(R) \cong \begin{cases} \mathbb{Z}_{2^r-1} \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_4^{r-1} \times \underbrace{\mathbb{Z}_4^r \times \ \cdots \ \times \mathbb{Z}_4^r}_{d} \\ \times \underbrace{\mathbb{Z}_2^r \times \ \cdots \ \times \mathbb{Z}_2^r}_{s-d}, \quad if\ p = 2 \\ \mathbb{Z}_{p^r-1} \times \mathbb{Z}_{p^2}^r \times \underbrace{\mathbb{Z}_{p^2}^r \times \ \cdots \ \times \mathbb{Z}_{p^2}^r}_{d} \\ \times \underbrace{\mathbb{Z}_p^r \times \ \cdots \ \times \mathbb{Z}_p^r}_{s-d}, \quad if\ p \neq 2 \end{cases}$$

Moreover, if p is odd, then $1+\mathcal{J}$ is generated by r elements $1+p\varepsilon_k$ $(k = 1, \dots, r)$, each of order p^2, dr elements $1+\varepsilon_k u_i$ $(k = 1, \dots, r)$, each of order p^2, for $i = 1, \dots, d \leqslant s$ and by $(s-d)r$ elements $1+\varepsilon_k u_j$ $(k = 1, \dots, r)$, each of order p, for $j = d+1, \dots, s$.

If $p = 2$, then $1+\mathcal{J}$ is a direct product of 2 cyclic groups $< -1+4\varepsilon_1 >$ and $< 1+4\varepsilon_1 >$, each of order 2, $(r-1)$ cyclic groups $< 1+2\varepsilon_k >$ $(k = 2, \dots, r)$, each of order 4, dr cyclic groups $< 1+\varepsilon_k u_i >$, each of order 4, for $i = 1, \dots, d \leqslant s$ and by $(s-d)r$ cyclic groups $< 1+\varepsilon_k u_j >$, each of order 2, for $j = d+1, \dots, s$.

Proof. Suppose $pu_i \neq 0$ for $i = 1,\ \dots,\ d \leqslant s$, $pu_j = 0$ for $j = d+1, \dots, s$ and $u_iu_j = 0$ for $1 \leqslant i,\ j \leqslant d \leqslant s$. Let $a = 1+x$ be an element of $1+\mathcal{J}$ with the highest possible order and assume that $x \in \mathcal{J} - \mathcal{J}^2$. Then, $o(a) = p^2$. This is true because, for any ε_k $(k = 1, \dots, r)$,

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

For every odd prime p, $(1+\varepsilon_k x)^p = 1+p\varepsilon_k x$, since $px^2 = 0$. Now,

$$\begin{aligned} (1+p\varepsilon_k x)^p &= 1 + p^2\varepsilon_k x + \frac{p(p-1)}{2}(p\varepsilon_k x)^2 \\ &= 1, \quad \text{since } p^2x = 0 \text{ and } p^3x^2 = 0. \end{aligned}$$

Hence, $(1+\varepsilon_k x)^{p^2} = 1$.

For $p = 2$, $(1+\varepsilon_k x)^2 = 1 + 2\varepsilon_k x + (\varepsilon_k x)^2$, and $(1+\varepsilon_k x)^4 = 1$, since $4x = 0,\ 6x^2 = 0,\ 4x^3 = 0$ and $x^4 = 0$.

For any prime number p and for each $k = 1,\ \dots,\ r$, we see that $(1+\varepsilon_k p)^{p^2} = 1$, $(1+\varepsilon_k u_i)^{p^2} = 1$, for $i = 1, \dots, d \leqslant s$, while $(1+\varepsilon_k u_j)^p = 1$, for $j = d+1, \dots, s$.

For integers $h_{ki} \leqslant p^2$, $l_{kj} \leqslant p$, we asset that

$$\prod_{k=1}^{r}\prod_{i=1}^{d}(1+\varepsilon_k u_i)^{h_{ki}} \cdot \prod_{k=1}^{r}\prod_{j=d+1}^{s}(1+\varepsilon_k u_j)^{l_{kj}} = 1,$$

will imply $h_{ki} = p^2$, for all $k = 1, \dots, r$ and $i = 1, \dots, d \leqslant s$; $l_{kj} = p$, for all $k = 1, \dots, r$ and $j = d+1, \ \dots, \ s$.

If we set $D_{ki} = \{(1+\varepsilon_k u_i)^{h_{ki}} : h_{ki} = 1, \dots, p^2\}, E_{kj} = \{(1+\varepsilon_k u_j)^{l_{kj}} : l_{kj} = 1, \dots, p\}$, for all $k = 1, \dots, r$, we see that D_{ki}, E_{kj} are all subgroups of $1 + \sum R_0 u_i \oplus \sum pR_0 u_i$ and that D_{ki} are all of order p^2 and that E_{kj} are all of order p as indicated in their definition. Also, pairwise intersection of these subgroups is trivial.

The argument above will show that the product of the dr subgroups D_{kj}, and $(s-d)r$ subgroups E_{ki} is direct. Thus, their product will exhaust $1 + \sum R_0 u_i \oplus \sum pR_0 u_i$.

It is straightforward to check that if $p = 2$, then $1 + \mathcal{J}$ is a direct product of 2 cyclic groups $< -1 + 4\varepsilon_1 >$ and $< 1 + 4\varepsilon_1 >$, each of order 2, $(r-1)$ cyclic groups $< 1+2\varepsilon_k > \ (k = 2, \dots, r)$, each of order 4, dr cyclic groups $< 1+\varepsilon_k u_i >$, each of order 4, for $i = 1, \dots, d \leqslant s$ and by $(s-d)r$ cyclic groups $< 1 + \varepsilon_k u_j >$, each of order 2, for $j = d+1, \dots, s$.

Also, if p is odd, then $1+\mathcal{J}$ is generated by r elements $1+p\varepsilon_k \ (k = 1, \dots, r)$, each of order p^2, dr elements $1 + \varepsilon_k u_i \ (k = 1, \dots, r)$, each of order p^2, for $i = 1, \dots, d \leqslant s$ and by $(s-d)r$ elements $1 + \varepsilon_k u_j \ (k = 1, \dots, r)$, each of order p, for $j = d+1, \dots, s$.

This completes the proof. □

2.3 The case when $\mathcal{J}^2 = (p^2, \ pu_i, \ u_i u_j)$

Let $dim_K(\mathcal{J}/\mathcal{J}^2) = 1+s$ and suppose that $dim_K(\mathcal{J}^2) \leqslant (s+1)(s+2)/2$. Then, $\mathcal{J}^2 = (p^2, \ pu_i, \ u_i u_j)$. Suppose further that $pu_i \neq 0$, for $i = 1, \dots, d \leqslant s$ and that $pu_j = 0$, for $j = d+1, \dots, s$. Then, $u_i u_j \neq 0$ for all $i, \ j = 1, \dots, d \leqslant s$ (since in this case u_i, u_j are not in $ann(\mathcal{J})$); and $u_i u_j = 0$ for all $i = 1, \dots, s$ and $j = d+1, \dots, s$. Recall that if $pu_j = 0$, then $u_j \in ann(\mathcal{J})$ and as such $u_j x = 0$ for every $x \in \mathcal{J}$. The following describes the structure of $U(R)$ and its possible generators.

Proposition 2.3. *Let R be a ring of characteristic p^3 with maximal ideal $\mathcal{J}$ such that $\mathcal{J}^3 = \{0\}$, $\mathcal{J}^2 \neq \{0\}$. Suppose further that there exist elements $u_1, \dots, u_s$ in $\mathcal{J}$ such that the multiplication in R is defined by $pu_i \neq 0$, for $i = 1, \dots, d \leqslant s$, and that $pu_j = 0$, for $j = d+1, \dots, s$ so that $u_i u_j \neq 0$ for all $i, \ j = 1, \dots, d \leqslant s$; and $u_i u_j = 0$ for all $i = 1, \dots, s$ and $j = d+1, \dots, s$. Then,*

$$U(R) \cong \begin{cases} \mathbb{Z}_{2^r-1} \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_4^{r-1} \times \underbrace{\mathbb{Z}_4^r \times \ \cdots \ \mathbb{Z}_4^r}_{d} \times \underbrace{\mathbb{Z}_2^r \times \ \cdots \ \times \mathbb{Z}_2^r}_{s-d} \times \\ \underbrace{\mathbb{Z}_2^r \times \ \cdots \ \times \mathbb{Z}_2^r}_{d(d+1)/2}, \quad if \ p = 2 \\ \mathbb{Z}_{p^r-1} \times \mathbb{Z}_{p^2}^r \times \underbrace{\mathbb{Z}_{p^2}^r \times \ \cdots \ \mathbb{Z}_{p^2}^r}_{d} \times \underbrace{\mathbb{Z}_p^r \times \ \cdots \ \times \mathbb{Z}_p^r}_{s-d} \times \\ \underbrace{\mathbb{Z}_p^r \times \ \cdots \ \times \mathbb{Z}_p^r}_{d(d+1)/2}, \quad if \ p \neq 2 \end{cases}$$

Proof. Suppose $pu_i \neq 0$ for all $i = 1, \ \ldots, \ d \leqslant s$ and $u_iu_j \neq 0$ for $1 \leqslant i, \ j \leqslant d \leqslant s$. Let $a = 1 + x$ be an element of $1 + \mathcal{J}$ with the highest possible order and assume that $x \in \mathcal{J} - \mathcal{J}^2$. Then, $o(a) = p^2$. This is true because, for any ε_k $(k = 1, \ldots, r)$,

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

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

$$\begin{aligned}(1 + p\varepsilon_k x)^p &= 1 + p^2\varepsilon_k x + \frac{p(p-1)}{2}(p\varepsilon_k x)^2 \\ &= 1, \quad \text{since } p^2 x = 0 \ \text{ and } p^3 x^2 = 0.\end{aligned}$$

Hence, $(1 + \varepsilon_k x)^{p^2} = 1$.

For any odd prime number p and for each $k = 1, \ \ldots, \ r$, we see that $(1 + \varepsilon_k p)^{p^2} = 1$, $(1 + \varepsilon_k u_i)^{p^2} = 1$, for $i = 1, \ldots, d \leqslant s$, while $(1 + \varepsilon_k u_j)^p = 1$, for $j = d + 1, \ldots, s$, and for non-zero elements u_i^2, u_iu_j $(i \neq j)$, we have $(1 + \varepsilon_k u_i^2)^p = 1$, $(1 + \varepsilon_k u_i u_j)^p = 1$.

For integers $h_{ki} \leqslant p^2$, $l_{kj} \leqslant p$, m_{ki} and $n_{kij} \leqslant p$, we asset that

$$\prod_{k=1}^{r}\prod_{i=1}^{d}(1 + \varepsilon_k u_i)^{h_{ki}} \cdot \prod_{k=1}^{r}\prod_{j=d+1}^{s}(1 + \varepsilon_k u_j)^{l_{kj}} \cdot \prod_{k=1}^{r}\prod_{i=1}^{d}(1 + \varepsilon_k u_i^2)^{m_{ki}} \cdot \prod_{k=1}^{r}\prod_{i,\ j=1}^{d}(1 + \varepsilon_k u_i u_j)^{n_{kij}} = 1,$$

will imply $h_{ki} = p^2$, for all $k = 1, \ldots, r$ and $i = 1, \ldots, d$; $l_{kj} = p$, for all $k = 1, \ldots, r$ and $j = d+1, \ \ldots, \ s$; $m_{ki} = p$ for all $k = 1, \ldots, r$ and $i = 1, \ \ldots, \ d$; and $n_{kij} = p$, for all $k = 1, \ldots, r$ and $i, \ j = 1, \ \ldots \ d$.

If we set

$$\begin{aligned} D_{ki} &= \{(1 + \varepsilon_k u_i)^{h_{ki}} : h_{ki} = 1, \ldots, p^2\} \\ E_{kj} &= \{(1 + \varepsilon_k u_j)^{l_{kj}} : l_{kj} = 1, \ldots, p\}, \\ F_{ki} &= \{(1 + \varepsilon_k u_i^2)^{m_{ki}} : m_{ki} = 1, \ldots, p\}, \\ G_{kij} &= \{(1 + \varepsilon_k u_i u_j)^{n_{kij}} : n_{kij} = 1, \ldots, p\}, \end{aligned}$$

for all $k = 1, \ldots, r$, we see that D_{ki}, E_{kj}, F_{ki} and G_{kij} are all subgroups of $1 + \sum R_0 u_i \oplus \sum R_0 u_i u_j$ and that D_{ki} are all of order p^2 and the others are all of order p as indicated in their definition. Also, pairwise intersection of these subgroups is trivial.

The argument above will show that the product of the dr subgroups D_{ki}, $(s - d)r$ subgroups E_{kj}, dr subgroups F_{ki} and the $r[d(d + 1)/2]$ subgroups G_{kij} is direct. Thus, their product will exhaust $1 + \sum R_0 u_i \oplus \sum R_0 u_i u_j$, and we see that the proof for the case when p is odd is complete.

Now, assume that $p = 2$. Then, for each $k = 1, \ldots, r$, we see that $(1 + \varepsilon_k u_i)^2 = 1 + 2\varepsilon_k u_i + \varepsilon_k^2 u_i^2$, $(1 + \varepsilon_k u_i)^4 = 1$, for $i = 1, \ldots, d \leqslant s$; $(1 + \varepsilon_k u_j)^2 = 1$, for $j = d + 1, \ldots, s$; and $(1 + \varepsilon_k u_i u_j)^2 = 1$, for every $i \neq j = 1, \ldots, d$.

For integers $h_{ki} \leqslant 4$, $l_{kj} \leqslant 2$, m_{ki} and $n_{kij} \leqslant 2$, we asset that

$$\prod_{k=1}^{r}\prod_{i=1}^{d}(1 + \varepsilon_k u_i)^{h_{ki}} \cdot \prod_{k=1}^{r}\prod_{j=d+1}^{s}(1 + \varepsilon_k u_j)^{l_{kj}} \cdot \prod_{k=1}^{r}\prod_{i=1}^{d}(1 + \varepsilon_k u_i^2)^{m_{ki}} \cdot$$
$$\prod_{k=1}^{r}\prod_{i,\ j=1}^{d}(1 + \varepsilon_k u_i u_j)^{n_{kij}} = 1,$$

will imply $h_{ki} = 4$, for all $k = 1, \ldots, r$; and $i = 1, \ldots, d$; $l_{kj} = 2$, for all $k = 1, \ldots, r$; and $j = d+1, \ \ldots, \ s$; $m_{ki} = 2$ for all $k = 1, \ldots, r$; and $i = 1, \ \ldots, \ d$; and $n_{kij} = 2$, for all $k = 1, \ldots, r$; and $i, \ j = 1, \ \ldots \ d$.

If we set

$$\begin{aligned} D_{ki} &= \{(1 + \varepsilon_k u_i)^{h_{ki}} : h_{ki} = 1, \ldots, 4\} \\ E_{kj} &= \{(1 + \varepsilon_k u_j)^{l_{kj}} : l_{kj} = 1,\ 2\}, \\ F_{ki} &= \{(1 + \varepsilon_k u_i^2)^{m_{ki}} : m_{ki} = 1,\ 2\}, \\ G_{kij} &= \{(1 + \varepsilon_k u_i u_j)^{n_{kij}} : n_{kij} = 1,\ 2\}, \end{aligned}$$

for all $k = 1, \ldots, r$, we see that D_{ki}, E_{kj}, F_{ki} and G_{kij} are all subgroups of $1 + \sum R_0 u_i \oplus \sum R_0 u_i u_j$ and that D_{ki} are all of order 4 and the others are all of order 2 as indicated in their definition. Also, pairwise intersection of these subgroups is trivial.

The argument above will show that the product of the dr subgroups D_{ki}, $(s - d)r$ subgroups E_{kj}, dr subgroups F_{ki} and the $r[d(d + 1)/2]$ subgroups G_{kij} is direct. Thus, their product will exhaust $1 + \sum R_0 u_i \oplus \sum R_0 u_i u_j$, and we see that the proof for the case when $p = 2$ is complete. □

This completes our investigation of the structure of the group of units of commutative completely primary finite rings of characteristic p^3 with unique maximal ideals $\mathcal{J}$ such that $\mathcal{J}^3 = (0)$, $\mathcal{J}^2 \neq (0)$ with given constraints on the generators for the ideals $\mathcal{J}$ and $\mathcal{J}^2$.

Acknowledgement

The author would like to thank the anonymous referee(s) whose comments and suggestions improved the final version of this paper.

References

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

[2] C. J. Chikunji, *On unit groups of commutative completely primary finite rings,* Math. J. Okayama Univ., 50 (2008), 149-160.

[3] C. J. Chikunji, *Unit groups of finite rings with products of zero divisors in their coefficient subrings,* Publ. Inst. Math. (Beograd) (N.S.), 95 (2014), 215-220.

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

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

[6] R. S. Wilson, *On the structure of finite rings,* Compositio Math., 26 (1973), 79-93.

Accepted: February 21, 2022