IMHOTEP

AFRICAN JOURNAL OF PURE AND APPLIED MATHEMATICS

Imhotep Mathematical Proceedings
Volume 1, Numéro 1, (2014),
pp. 40 – 48.

Groups of units of commutative completely primary finite rings

Chiteng'a J. Chikunji
Department of Basic Sciences,
Botswana College of Agriculture,
Private Bag 0027, Gaborone,
BOTSWANA.
jchikunj@bca.bw

Abstract

It is well known that the group of units of a completely primary finite ring R of order p^{nr} is a semi-direct product of a cyclic group of order $p^r - 1$ by a p-group of order $p^{(n-1)r}$. The structure of the p-subgroup is not completely determined. In this presentation, we investigate and determine the structure of the $p-$subgroup of the group of units of a commutative completely primary finite ring R of order p^{nr} with unique maximal ideal $\mathcal{J}$ such that $\mathcal{J}^3 = (0)$, $\mathcal{J}^2 \neq (0)$, and with characteristic p^2, for any prime number p and positive integers n and r.

Proceedings of the 2nd Strathmore International Mathematics Conference (SIMC 2013), 12 - 16 August 2013, Strathmore University, Nairobi, Kenya.

IMHOTEP - Math. Proc. **1** (2014), 40–48
1608-9324/010040–39, DOI 13.1007/s00009-003-0000

IMHOTEP Mathematical Proceedings

Groups of units of commutative completely primary finite rings

Chiteng'a J. Chikunji

Abstract. It is well known that the group of units of a completely primary finite ring R of order p^{nr} is a semi-direct product of a cyclic group of order $p^r - 1$ by a p-group of order $p^{(n-1)r}$. The structure of the p-subgroup is not completely determined. In this presentation, we investigate and determine the structure of the $p-$subgroup of the group of units of a commutative completely primary finite ring R of order p^{nr} with unique maximal ideal $\mathcal{J}$ such that $\mathcal{J}^3 = (0)$, $\mathcal{J}^2 \neq (0)$, and with characteristic p^2, for any prime number p and positive integers n and r.

Mathematics Subject Classification (2000). Primary 16P10, 13M05; Secondary 20K01, 20K25.

Keywords. Finite commutative rings, Galois rings, group of units, direct products, abelian p-groups.

I. Introduction

A finite ring R is called *completely primary* if all its zero divisors including the zero element form the unique maximal ideal $\mathcal{J}$. Finite completely primary rings are precisely local rings with unique maximal ideals.

All rings considered in this work are commutative with identity $1 \neq 0$ unless specified otherwise, that ring homomorphisms preserve identities, and that a ring and its subrings have the same identity. Moreover, we adopt the notation used in [1], [2] and [3], that is, R will denote a finite ring, unless otherwise stated, $\mathcal{J}$ will denote the Jacobson radical of R, and we will denote the Galois ring $GR(p^k,\ p^{kr})$ of characteristic p^k and order p^{kr} by R_o, for some prime integer p, and positive integers $k,\ r$. We denote the unit group of R by $U(R)$; if g is an element of $U(R)$, then $o(g)$ denotes its order, and $\langle g\rangle$ denotes the cyclic group generated by g. Similarly, if $f(x) \in R[x]$, we shall denote by $\langle f(x)\rangle$ 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$R$. We denote a direct product of r cyclic groups $\mathbb{Z}_m$ by $\mathbb{Z}_m^r$ or by $\underbrace{\mathbb{Z}_m \times \ \ldots \ \times \mathbb{Z}_m}_{r}$.

The rest of the paper is organized as follows. In Section 2, we state without proofs some general results on groups of units of completely primary finite rings which are relevant to our work. In section 3, we give an explicit description of the known structures of groups of units of certain completely primary finite rings R of order p^{nr} with maximal ideals $\mathcal{J}$ such

Paper presented at the 2nd Strathmore International Mathematics Conference (SIMC 2013), 12 - 16 August 2013, Strathmore University, Nairobi, Kenya.

that $\mathcal{J}^3 = (0)$, $\mathcal{J}^2 \neq (0)$. Finally, in section 4, we determine the structure of the unit group $U(R)$ of R and in some cases, its generators, when the characteristic of R is p^2, $s \geq 3$ and $1 \leq dim_{R_o/pR_o}(\mathcal{J}^2) < s(s+1)/2$, without considering structural matrices of isomorphic classes of these types of rings. This complements the author's earlier solution of the problem in the case when the characteristic of R is p, $s = 3$, $t = 1$ and $\mathcal{J}^2 \subseteq ann(\mathcal{J})$, the annihilator of $\mathcal{J}$.

II. Completely primary finite (CPF) rings

Let R be a completely primary finite ring, $\mathcal{J}$ the set of all zero divisors in R, p a prime, k, n and r be positive integers. Properties of completely primary finite (CPF) rings and those of their groups of units, with different aims and scope, appear in several articles (e.g. [6], [7]), and below we state some of the results without proofs ([6]): $|R| = p^{nr}$, $\mathcal{J}$ is the Jacobson radical of R, $\mathcal{J}^n = (0)$, $|\mathcal{J}| = p^{(n-1)r}$, $R/\mathcal{J} \cong GF(p^r)$, the finite field of p^r elements and $charR = p^k$, where $1 \leq k \leq n$. If $n = k$, it is known that, up to isomorphism, there is precisely one completely primary ring of order p^{kr} having characteristic p^k and residue field $GF(p^r)$. It is called the *Galois ring* $GR(p^{kr},\ p^k)$ and a concrete model is the quotient $\mathbb{Z}_{p^k}[X]/\langle f(x)\rangle$, 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 $GR(p^n,\ p) = \mathbb{F}_{p^n}$. In fact, $R = \mathbb{Z}_{p^n}[b]$, where b is an element of R of multiplicative order $p^r - 1$; $\mathcal{J} = pR$ and $Aut(R) \cong Aut(R/pR)$ (see Proposition 2 in [6]).

Let R be a completely primary ring, $|R/\mathcal{J}| = p^r$ and $charR = p^k$. Then it can be deduced from [6] and [7] that R has a coefficient subring R_o of the form $GR(p^k,\ p^{kr})$ 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 [6]). Furthermore, there exist elements $m_1,\ ...,\ m_h \in \mathcal{J}$ and automorphisms $\sigma_1,\ ...,\ \sigma_h \in Aut(R_o)$ such that $R = R_o \oplus \sum_{i=1}^{h} R_om_i$ (as R_o-modules), $m_ir_o = r_o^{\sigma_i}m_i$, for all $r_o \in R_o$ and any $i = 1,\ ...,\ h$. Moreover, $\sigma_1,\ ...,\ \sigma_h$ are uniquely determined by R and R_o. The maximal ideal of R is $\mathcal{J} = pR_o \oplus \sum_{i=1}^{h} R_om_i$. We call σ_i the *automorphism associated* with m_i and $\sigma_1,\ ...,\ \sigma_h$ the *associated automorphisms* of R with respect to R_o.

Now, let $R_o = \mathbb{Z}_{p^k}[b]$ be a coefficient subring of R of order p^{kr} and characteristic p^k and let $K_o = \langle b\rangle \cup \{0\}$, denote the set of coset representatives of $\mathcal{J}$ in R. Then it is easy to show that every element of R_o can be written uniquely as $\sum_{i=0}^{k-1} \lambda_ip^i$, where $\lambda_i \in K_o$.

Let R be a completely primary finite ring (not necessarily commutative). The following facts are useful (e.g. see [6, §2]): The unit group $U(R)$ of R contains a cyclic subgroup $\langle b\rangle$ of order $p^r - 1$ and a $p-$Sylow subgroup $1 + \mathcal{J}$ of order $p^{(n-1)r}$; hence $U(R)$ is a semi-direct product of $1 + \mathcal{J}$ by $\langle b\rangle$ and $|U(R)| = p^{(n-1)r}(p^r - 1)$; the unit group $U(R)$ is solvable; if G is a subgroup of $U(R)$ of order $p^r - 1$, then G is conjugate to $\langle b\rangle$ in $U(R)$; if $U(R)$ 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; 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).

III. Some known groups of units of CPF rings with $\mathcal{J}^3 = (0)$

Let R be a commutative completely primary finite (CPF) ring with maximal ideal $\mathcal{J}$ such that $\mathcal{J}^3 = (0)$ and $\mathcal{J}^2 \neq (0)$. Then $charR = p^k$, where $1 \leq k \leq 3$ (see [1]). Let $s,\ t,\ \lambda$ be numbers in the generating sets for the R_o-modules $U,\ V,\ W$, respectively, so that

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

and

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

In [3] we have determined the group of units $U(R)$ of the ring R and its generators when $s = 2,\ t = 1,\ \lambda = 0$ and characteristic of R is p; and when $t = s(s+1)/2,\ \lambda = 0$, for a fixed integer s, for all the characteristics of R. It was noted that $U(R)$ and its generators depended on the structural matrices (a_{ij}) and on the parameters $p,\ k,\ r$, and s. In [4] we obtained the structure of $U(R)$ and its generators when $s = 2,\ t = 1,\ \lambda = 0$ and characteristic of R is p^2 and p^3; and the case when $s = 2,\ t = 2,\ \lambda = 0$ and characteristic of R is p. In both papers, [3] and [4], we assumed that $\lambda = 0$ so that the annihilator of the maximal ideal $\mathcal{J}$ coincides with $\mathcal{J}^2$. It was also noted that the earlier strategy (that of considering different types of symmetric matrices) was thus not viable anymore and we followed a different approach; that of considering structural matrices of isomorphic classes of these types of rings with the same invariants $p,\ r,\ k,\ s$, and t.

In [5], we proved that $1 + \mathcal{J}$ is a direct product of its subgroups $1 + pR_o \oplus U \oplus V$ and $1 + W$ and further determined the structure of $1 + W$, in general; we also determined the structure of $U(R)$ and its generators when $s = 3,\ t = 1,\ \lambda \geq 1$ and $\mathrm{char}R = p$. We then generalized the structure of $U(R)$ in the cases when $s = 2,\ t = 1$; $t = s(s+1)/2$, for a fixed integer s, and for all characteristics of R; and when $s = 2,\ t = 2$ and $\mathrm{char}R = p$; determined in [3] and [4], to the case when $ann(\mathcal{J}) = \mathcal{J}^2 + W$ so that $\lambda \geq 1$.

We state the following result which summarizes the structure of the group of units $U(R)$ of the rings R determined in [3], [4] and [5].

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

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

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

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

and if $p = 2$

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

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

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

and

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

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

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

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

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

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

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

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

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

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

The proof follows from Section 3.1 in [3], Propositions 2.2, 2.3, 2.4 and 2.5 in [4], Theorem 4.1 in [3] and Proposition 2.3 in [5].

The above results describe structures of groups of units of completely primary finite rings when $m = 2$, that is, when $\mathcal{J}^2 = (0)$; when $m = k = n$, that is $\mathcal{J}^m = (0)$ and char$R = p^m$; and when $m = 3$, that is, $\mathcal{J}^3 = (0)$, for given parameters. The solution for different parameters when $m = 3$ and $m \geq 4$ is left for further consideration.

In section 4 we extend the above problem to the case when the characteristic of R is p^2, $s \geq 3$ and $1 \leq dim_{R_o/pR_o}(\mathcal{J}^2) < s(s+1)/2$, without considering structural matrices of isomorphic classes of these types of rings.

IV. Group of units of CPF rings of characteristic p^2

We now consider the structure of the group of units of completely primary finite rings with maximal ideals $\mathcal{J}$ such that $\mathcal{J}^3 = (0)$, $\mathcal{J}^2 \neq (0)$, and with characteristic p^2.

IV.1. A construction of commutative rings of characteristic p^2.

Let R_o be the Galois ring $GR(p^2,\ p^{2r})$. Let s, d, t be integers with either $1 \leq 1+t \leq s(s+1)/2$ or $1 \leq d+t \leq s(s+1)/2$. Let V be an R_o/pR_o-space, which when considered as an R_o-module, has a generating set $\{v_1,\ ...,\ v_t\}$ and let U be an R_o-module with an R_o-module generating set $\{u_1,\ \ldots,\ u_s\}$; and suppose that $d \geq 0$ of the u_i are such that $pu_i \neq 0$. Since R_o is commutative, we can think of them as both left and right R_o-modules.

Let (a_{ij}^l) be $1+t$ or $t+d$, $s \times s$ linearly independent symmetric matrices over R_o/pR_o.

On the additive group $R = R_o \oplus U \oplus V$ we define multiplication by the following relations:

$$\begin{aligned} u_iu_j &= a_{ij}^o p + \sum_{l=1}^{d} a_{ij}^l p u_l + \sum_{k=1}^{t} a_{ij}^{d+t} v_k; \\ u_iv_k &= v_ku_i = u_iu_ju_\lambda = pv_k = v_kv_l = v_lv_k = 0; \end{aligned} \tag{IV.1}$$

$$u_i\alpha = \alpha u_i,\ v_k\alpha = \alpha v_k;\ (1 \leq i,\ j,\ \lambda \leq s;\ 1 \leq l \leq d;\ 1 \leq k \leq t);$$

where $\alpha,\ a_{ij}^o,\ a_{ij}^l,\ a_{ij}^{d+k} \in R_o/pR_o$.

By the above relations, R is a commutative completely primary finite ring of characteristic p^2 with Jacobson radical $\mathcal{J} = pR_o \oplus U \oplus V$, $\mathcal{J}^2 = pR_o \oplus V$ or $\mathcal{J}^2 = pU \oplus V$ and $\mathcal{J}^3 = (0)$. We call (a_{ij}^l) the *structural matrices* of the ring R and the numbers $p,\ n,\ r,\ s,\ d$ and t *invariants* of the ring R.

The following result is proved in [1, Theorem 6.1].

Theorem IV.1. *Let R be a ring. Then R is a commutative completely primary finite ring of characteristic p^2 with maximal ideal $\mathcal{J}$ such that $\mathcal{J}^3 = (0)$, $\mathcal{J}^2 \neq (0)$, the annihilator of $\mathcal{J}$ coincides with $\mathcal{J}^2$ if and only if R is isomorphic to one of the rings given by the relations in (IV.1).*

Remark IV.2. *We know that $R = R_o \oplus R_o m_1 \oplus \ldots \oplus R_o m_h$, where the elements $m_i \in \mathcal{J}$; and that $\mathcal{J} = pR_o \oplus R_o m_1 \oplus \ldots \oplus R_o m_h$. Since $\mathcal{J}^3 = (0)$ and $\mathcal{J}^2 = ann(\mathcal{J})$, with $\mathcal{J}^2 \neq (0)$, we can write*

$$\{m_1,\ ...,\ m_h\} = \{u_1,\ ...,\ u_s,\ v_1,\ ....,\ v_t\}$$

where, $u_1, ..., u_s \in \mathcal{J} - \mathcal{J}^2$ and $v_1, ..., v_t \in \mathcal{J}^2$, so that $s + t = h$.

In view of the above considerations and by 1.8 of [1], the non-zero elements of

$$\{1,\ p,\ u_1,\ ...,\ u_s,\ pu_1,\ ...,pu_s,\ v_1, ...,\ v_t\} \tag{IV.2}$$

form a "basis" for R over $K_o = R_o/pR_o$.

Since $pm = 0$, for all $m \in \mathcal{J}^2$, it is easy to check that if $charR = p^2$, then either
(i) $p \in \mathcal{J}^2$; or
(ii) $p \in \mathcal{J} - \mathcal{J}^2$.

These two cases do not overlap, and for clarity of our work, we consider them in turn.

Remark IV.3. *Suppose that $charR = p^2$ and p lies in $\mathcal{J}^2$. In this case, (IV.2) becomes*

$$\{1,\ p,\ u_1,\ ...,\ u_s,\ v_1, ...,\ v_t\};$$

and by Proposition 3.2 of [1], $1 \leq 1 + t \leq s(s+1)/2$. *Hence, every element of R may be written uniquely as*

$$a_o + a_1 p + \sum_{i=1}^{s} b_i u_i + \sum_{k=1}^{t} c_k v_k;\ a_o,\ a_1,\ b_i,\ c_k \in K_o;$$

and therefore,

$$u_i u_j = a_{ij}^o p + \sum_{k=1}^{t} a_{ij}^k v_k,$$

where $a_{ij}^o,\ a_{ij}^k \in R_o/pR_o$. Clearly, $dim_{R_o/pR_o}(\mathcal{J}^2) = 1 + t$.

Remark IV.4. *Suppose that $d \geq 0$ is the number of the elements pu_i in (IV.2) which are not zero. Suppose, without loss of generality, that $pu_1,\ ...,\ pu_d$ are the d non-zero elements. Then, (IV.2) becomes*

$$\{1,\ p,\ u_1,\ ...,\ u_s,\ pu_1,\ ...,pu_d,\ v_1, ...,\ v_t\}; \tag{IV.3}$$

and by Proposition 3.2 of [1], *we have $1 \leq d + t \leq s(s+1)/2$ and hence, every element of R may be written uniquely as*

$$\lambda_o + \lambda_1 p + \sum_{i=1}^{s} \alpha_i u_i + \sum_{l=1}^{d} \beta_l p u_l + \sum_{k=1}^{t} \gamma_k v_k;\ \lambda_o,\ \lambda_1,\ \alpha_i,\ \beta_l,\ \gamma_k \in K_o.$$

Clearly, the products $u_i u_j \in \mathcal{J}^2$. Hence,

$$u_i u_j \quad = \quad \sum_{l=1}^{d} a_{ij}^l p u_l + \sum_{k=1}^{t} a_{ij}^{k+d} v_k,\ \text{where } a_{ij}^l,\ a_{ij}^{k+d} \in R_o/pR_o, \tag{IV.4}$$

and $dim_{R_o/pR_o}(\mathcal{J}^2) = d + t$.

Now, since $pu_l,\ v_k \in \mathcal{J}^2$ $(l = 1,\ ...,\ d;\ k = 1,\ ...,\ t)$, we can write them as sums of products of elements of $\mathcal{J}$. In particular, $pu_l,\ v_k$ can be written as linear combinations of pu_i and u_iu_j with coefficients in R_o/pR_o. Hence, since $pu_l\ ,\ v_k$ $(l = 1,\ ...,\ d;\ k = 1,\ ...,\ t)$ is a basis for $\mathcal{J}^2$ over R_o/pR_o, we conclude that pu_i and u_iu_j $(i,\ j = 1,\ ...,\ s)$ generate $\mathcal{J}^2$.

Clearly, $|R| = p^{2r} \cdot p^{sr} \cdot p^{dr} \cdot p^{tr} = p^{(2+s+d+t)r}$ and $|\mathcal{J}| = p^{(1+s+d+t)r}$.

IV.2. The group of units.

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

$$U(R) = \langle b\rangle \cdot (1 + \mathcal{J}) \cong \langle b\rangle \times (1 + \mathcal{J}); \tag{IV.5}$$

a direct product of the $p-$group $1+\mathcal{J}$ by the cyclic subgroup $\langle b\rangle$. Thus, it suffices to determine the structure of the subgroup $1 + \mathcal{J}$ of the group $U(R)$.

Notice that

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

Proposition IV.5. *(*[3]*, Proposition 3.4) If* $charR = p^2$*, then* $1 + \mathcal{J}$ *contains* $1 + pR_o$ *as its subgroup.*

The structure of $1 + pR_o$ is completely determined by Raghavendran in [6]. For convenience of the reader, we state here the following result. For details, refer to [6, Theorem 9].

We take r elements $\varepsilon_1,\ ...,\ \varepsilon_r$ in R_o with $\varepsilon_1 = 1$ such that $\{\overline{\varepsilon_1},\ ...,\ \overline{\varepsilon_r}\}$ 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 IV.6. ([6, *Theorem* 9) *If* $charR_o = p^2$*, then* $1 + pR_o$ *is a direct product of* r *cyclic groups* $\langle 1 + p\varepsilon_j\rangle$ $(j = 1,\ ...,\ r)$*, each of order* p *for any prime number* p*.*

IV.2.1. Group of units of rings of characteristic p^2 in which $p \in \mathcal{J}^2$. Let R be a commutative completely primary finite ring of characteristic p^2 in which $p \in \mathcal{J}^2$. Then $dim_{R_o/pR_o}(\mathcal{J}^2) = 1+t$. The following results determine the structure of the subgroup $1 + \mathcal{J}$ of the group of units $U(R)$ of the ring R.

Proposition IV.7. *Let* $charR = p^2$*,* $s \geq 3$*,* $1 + t < s(s + 1)/2$*, and suppose that* $p \in \mathcal{J}^2$*. If* p *is odd, then*

$$1 + \mathcal{J} \cong \underbrace{\mathbb{Z}_p^r \times\ ...\ \times \mathbb{Z}_p^r}_{1+s+t},$$

a direct product of $(1 + s + t)r$ *cyclic groups of order* p*.*

Proof. If $p \in \mathcal{J}^2$, 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 $o(a) = p$. This is true because

$$\begin{aligned}(1 + x)^p &= 1 + px + \frac{p(p-1)}{2}x^2 \text{ (since } x^3 = 0)\\ &= 1 + \frac{p(p-1)}{2}x^2 \text{ (since } p \in \mathcal{J}^2 \text{ and } px = 0)\\ &= 1 \text{ (since } p - 1 \text{ is even and } px^2 = 0).\end{aligned}$$

Now let $\varepsilon_1,\ ...,\ \varepsilon_r \in R_o$ with $\varepsilon_1 = 1$ such that $\bar{\varepsilon}_1,\ ...,\ \bar{\varepsilon}_r \in R_o/pR_o \cong GF(p^r)$ form a basis for $GF(p^r)$ over its prime subfield $GF(p)$, for any prime p and positive integer r.

We first note the following results: For each $i = 1,\ ...,\ r$; $j = 1,\ ...,\ s$; and $k = 1,\ ...,\ t$, $(1+\varepsilon_i p)^p = 1$, $(1+\varepsilon_i u_j)^p = 1$, $(1+\varepsilon_i v_k)^p = 1$, and $g^p = 1$ for all $g \in 1+\mathcal{J}$. For integers $l_i,\ m_i,\ n_i \leq p$, we assert that

$$\prod_{i=1}^{r}\{(1+\varepsilon_i p)^{l_i}\}\cdot\prod_{j=1}^{s}\prod_{i=1}^{r}\{(1+\varepsilon_i u_j)^{m_i}\}\cdot\prod_{k=1}^{t}\prod_{i=1}^{r}\{(1+\varepsilon_i v_k)^{n_i}\} = 1,$$

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

If we set $D_i = \{(1+\varepsilon_i p)^l : l = 1,\ ...,\ p\}$, $E_{i,j} = \{(1+\varepsilon_i u_j)^m : m = 1,\ ...,\ p\}$, $(j = 1,\ ...,\ s)$; and $F_{i,k} = \{(1+\varepsilon_i v_k)^n : n = 1,\ ...,\ p\}$, $(k = 1,\ ...,\ t)$, for all $i = 1,\ ...,\ r$; we see that $D_i,\ E_{i,j},\ F_{i,k}$ are all subgroups of the group $1+\mathcal{J}$ and these are all of order p as indicated in their definition. The argument above will show that the product of the $(1+s+t)r$ subgroups $D_i,\ E_{i,j},\ F_{i,k}$ is direct. So, their product will exhaust $1+\mathcal{J}$. This completes the proof.

■

Proposition IV.8. *Let $charR = p^2$, $s \geq 3$, $1+t < s(s+1)/2$, and suppose that $p \in \mathcal{J}^2$. If $p = 2$ and $u_j^2 = 0$, for every $j = 1,\ ...,\ s$; then*

$$1+\mathcal{J} \cong \underbrace{\mathbb{Z}_2^r \times\ ...\ \times \mathbb{Z}_2^r}_{1+s+t},$$

a direct product of $(1+s+t)r$ cyclic groups of order 2.

Proof. If $u_j^2 = 0$, for every $j = 1,\ ...,\ s$; then the highest possible order of any element in $1+\mathcal{J}$ is 2. The proof follows a similar argument to that of the case when p is odd, and may be deduced from the previous proposition.

■

Proposition IV.9. *Let $charR = p^2$, $s \geq 3$, $1+t < s(s+1)/2$, and suppose that $p \in \mathcal{J}^2$. If $p = 2$ and suppose that $l \leq s$ is the number of the u_j such that $u_j^2 \neq 0$. Then*

$$1+\mathcal{J} \cong \underbrace{\mathbb{Z}_4^r \times\ ...\ \times \mathbb{Z}_4^r}_{l} \times \underbrace{\mathbb{Z}_2^r \times\ ...\ \times \mathbb{Z}_2^r}_{m},$$

a direct product of lr cyclic groups of order 4 and mr cyclic groups of order 2, where $l+m = 1+s+t$.

Proof. We first observe that if, without lose of generality, $u_1^2 \neq 0$ while $u_j^2 = 0$, for every $j = 2,\ ...,\ s$, then $(1+\varepsilon_i u_1)^4 = 1$ and the elements $1+\varepsilon_i u_j$, $1+\varepsilon_i v_k$, and $1+\varepsilon_i p$, are all of order 2; and if $u_1^2 \neq 0$, $u_2^2 \neq 0$ while $u_j^2 = 0$ $(j = 3,\ ...,\ s)$, then $(1+\varepsilon_i u_1)^4 = 1$, $(1+\varepsilon_i u_2)^4 = 1$ and the elements $1+\varepsilon_i u_j$, $1+\varepsilon_i v_k$ and $1+\varepsilon_i p$, are all of order 2. Continuing the argument so that every u_j has a non-zero square, we see that $(1+\varepsilon_i u_j)^4 = 1$ and the elements $1+\varepsilon_i v_k$ and $1+\varepsilon_i p$, are all of order 2.

Since $p,\ v_k$ are linear combinations of $u_i u_j$ with coefficients in R_o/pR_o, the products of elements $1+\varepsilon_i u_j$ generate the elements $1+\varepsilon_i v_k$ and $1+\varepsilon_i p$. By induction, we obtain the desired result.

■

As an example to illustrate Proposition IV.9, suppose that $s = 4$ and $t = 2$. Then $|1+\mathcal{J}| = p^{(4+2+1)r}$ and

$$1+\mathcal{J} \cong \begin{cases} \mathbb{Z}_4^r \times \mathbb{Z}_2^r \times \mathbb{Z}_2^r \times \mathbb{Z}_2^r \times \mathbb{Z}_2^r \times \mathbb{Z}_2^r; \\ \mathbb{Z}_4^r \times \mathbb{Z}_4^r \times \mathbb{Z}_2^r \times \mathbb{Z}_2^r \times \mathbb{Z}_2^r; \text{ or} \\ \mathbb{Z}_4^r \times \mathbb{Z}_4^r \times \mathbb{Z}_4^r \times \mathbb{Z}_2^r. \end{cases}$$

IV.2.2. Group of units of rings of characteristic p^2 in which $p \in \mathcal{J} - \mathcal{J}^2$. In this case, $dim_{R_o/pR_o}(\mathcal{J}^2) = d + t$. The following result determines the structure of $1 + \mathcal{J}$ in which $d = s$.

Proposition IV.10. *Let $charR = p^2$, $s \geq 3$, $d + t < s(s+1)/2$, and suppose that $p \in \mathcal{J} - \mathcal{J}^2$. Suppose further that $pu_i \neq 0$, for every $i = 1, \ ..., \ s$. Then*

$$1 + \mathcal{J} \cong \mathbb{Z}_p^r \times \underbrace{\mathbb{Z}_{p^2}^r \times \ ... \ \times \mathbb{Z}_{p^2}^r}_{s} \times \underbrace{\mathbb{Z}_p^r \times \ ... \ \times \mathbb{Z}_p^r}_{t}$$

Proof. If $p \in \mathcal{J} - \mathcal{J}^2$, 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 $o(a) = p^2$, for any prime p.

This is true because, for any ε_i $(i = 1, \ ..., \ r)$,

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

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

$$\begin{aligned} (1 + p\varepsilon_i x)^p &= 1 + p^2\varepsilon_i x + \frac{p(p-1)}{2}(p\varepsilon_i x)^2 \\ &= 1, \text{ since } charR = p^2. \end{aligned}$$

Hence, $(1 + \varepsilon_i x)^{p^2} = 1$. If p is even, then

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

Notice that

$$1 + \mathcal{J} = (1 + pR_o) \times (1 + \sum_{i=1}^{s} R_o u_i + \sum_{k=1}^{t} R_o v_k).$$

The structure of the group $1 + pR_o$ is well known; and it is a direct product of r cyclic groups, each of order p (see Proposition IV.6).

We now determine the structure of $1 + \sum_{i=1}^{s} R_o u_i + \sum_{k=1}^{t} R_o v_k$. Choose $\varepsilon_1, \ ..., \ \varepsilon_r \in R_o$ with $\varepsilon_1 = 1$ such that $\overline{\varepsilon_1}, \ ..., \ \overline{\varepsilon_r} \in R_o/pR_o \cong GR(p^r)$ form a basis for $GF(p^r)$ over $GF(p)$.

For any prime p, since for each $i = 1, \ ..., \ r$, we have that $(1 + \varepsilon_i u_j)^{p^2} = 1$, $(j = 1, \ ..., \ s)$ $(1 + \varepsilon_i v_k)^p = 1$, $(k = 1, \ ..., \ t)$. Also, intersection of $\langle(1 + \varepsilon_i u_j)\rangle$, and $\langle(1 + \varepsilon_i v_k)\rangle$ is trivial. Hence, the direct product of the cyclic groups $\langle(1 + \varepsilon_i u_j)\rangle$, and $\langle(1 + \varepsilon_i v_k)\rangle$ exhaust $(1 + \sum_{i=1}^{s} R_o u_i + \sum_{k=1}^{t} R_o v_k)$. Thus, $1 + \mathcal{J}$ is of the required form, and this completes the proof.

■

Remark IV.11. *Proposition IV.10 is true for the two cases when $u_i^2 = 0$ and when $u_i^2 \neq 0$, for $i = 1, \ ..., \ s$.*

Remark IV.12. *Suppose that $pu_j = 0$ and $u_j^2 = 0$. Then, it is easy to check that $|\langle(1+\varepsilon_i u_j)\rangle| = p$, and this can be proved in a similar manner to Propositions IV.7 and IV.8, cases where $p \in \mathcal{J}^2$.*

Remark IV.13. *If $pu_j = 0$ and $u_j^2 \neq 0$. Then $|\langle(1+\varepsilon_i u_j)\rangle| = p$, if p is odd, or $|\langle(1+\varepsilon_i u_j)\rangle| = p^2$, if p is even, and this can be proved in a similar manner to Propositions IV.7 and IV.9, cases where $p \in \mathcal{J}^2$, for p odd or even, respectively.*

Remark IV.14. *We remark here that the cases for which $d < s$ of $pu_1, \ ..., \ pu_d$ is zero have similar arguments to previous results and one may deduce the structure of $1 + \mathcal{J}$ from the preceding propositions.*

Remark IV.15. *By the above results and by equation (IV.5), the structure of $U(R)$ is now determined.*

Rings with other invariants $p,\ n,\ r,\ s,\ t,\ d$ when $\mathcal{J}^3 = (0)$, and the cases $\mathcal{J}^m = (0),\ \mathcal{J}^{m-1} \neq (0)$, when $m \geq 4$ and $m < k$ are left for further consideration.

References

[1] C. J. Chikunji, *On a class of finite rings*, Comm. Algebra, **27** (1999), no. 10, 5049 – 5081.

[2] C. J. Chikunji, *A classification of cube radical zero completely primary finite rings*, Demonstratio Math., XXXVIII (2005), 7 – 20.

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

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

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

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

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

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