Math. J. Okayama Univ. **45** (2003), 59–71

ON A CLASS OF RINGS OF ORDER P^5

Chiteng'a John CHIKUNJI

Abstract. This paper describes all rings of order p^5, of a certain class of finite rings which satisfy the conditions that (i) the set of all zero-divisors form an ideal $\mathcal{M}$; (ii) $\mathcal{M}^3 = (0)$; and (iii) $\mathcal{M}^2 \neq (0)$.

1. Introduction

Throughout this paper, all rings are finite, associative (however, not necessarily commutative) and have an identity element denoted by 1. It is further assumed that homomorphisms preserve 1, subrings have the same 1 and modules are unital. In what follows Z will denote the ring of all integers, p will be any prime integer ≥ 2. Recall that a finite ring with identity is called a completely primary ring if the set $\mathcal{M}$ of all its zero-divisors forms an ideal. Let R be a finite completely primary ring. Then R contains a subring R_o such that $R_o/pR_o \cong R/\mathcal{M}$, where $pR_o = (p)$, is the radical of R_o (see 2.4 in the body of the paper). We use $ann(\mathcal{M})$ to denote the two-sided annihilator of $\mathcal{M}$ in a ring R; F the Galois field $GF(q)$, where $q = p^r$, for any positive integer r; and if S is any set, $|S|$ will denote the cardinal number of elements in S. The notations $dim(\mathcal{M}/ann(\mathcal{M}))$ and $dim(\mathcal{M}^2)$ will denote the dimensions of $\mathcal{M}/ann(\mathcal{M})$ and $\mathcal{M}^2$ over the residue field R_o/pR_o, respectively. Furthermore, $charR$ will denote the characteristic of any ring R.

In earlier papers, [1] and [2], we formulated the isomorphism problem of a class of finite rings which satisfy the conditions that (i) the set of all zero-divisors form an ideal $\mathcal{M}$; (ii) $\mathcal{M}^3 = (0)$; and (iii) $\mathcal{M}^2 \neq (0)$. These rings are completely primary and we call a ring R which satisfies conditions (i), (ii) and (iii), *a ring with property*(T). This paper describes all the rings of this type of order p^5 and obtains the number of non-isomorphic classes.

2. Preliminary results and definitions

For convenience of the reader, we shall gather in this section all definitions and results which will be used in the sequel. The following results will be assumed:

2.1. *Let R be a finite ring. Then, there is no distinction between left and right zero-divisors (units) and every element in R is either a zero-divisor or a unit* (*see Section* 4 *in* [4]).

Mathematics Subject Classification. 16P10, 13H99.

2.2. *Let R be a finite completely primary ring, $\mathcal{M}$ the set of all the zero-divisors in R, p a prime, k, n and r be positive integers. Then*

(i) $|R| = p^{nr}$;
(ii) $\mathcal{M}$ *is the Jacobson radical of* R;
(iii) $\mathcal{M}^n = (0)$;
(iv) $|\mathcal{M}| = p^{(n-1)r}$;
(v) $R/\mathcal{M} \cong GF(p^r)$, *the finite field of* p^r *elements*; *and*
(vi) $char R = p^k$, *where* $1 \leq k \leq n$.

This is essentially Theorem 2 of [7].

2.3. *Let R be as in 2.2. If $n = k$, then $R = \mathbf{Z}_{p^k}[b]$, where b is an element of R of multiplicative order $p^r - 1$; $\mathcal{M} = pR$ and $Aut(R) \cong Aut(R/pR)$.* Such a ring is called a *Galois ring* and denoted by $GR(p^{kr}, p^k)$.

2.4. *Let R be as in 2.2 and let $char R = p^k$. Then R has a coefficient subring R_o of the form $GR(p^{kr}, p^k)$ which is clearly a maximal Galois subring of R.* This can easily be deduced from the main theorem in [3].

2.5. *Let R and R_o be as in 2.2 and 2.4. 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 [7]).

The following result is due to Wirt [8].

2.6. *Let R and R_o be as in 2.2 and 2.4. Then there exist $m_1, ..., m_h \in \mathcal{M}$ and $\sigma_1, ..., \sigma_h \in Aut(R_o)$ such that*

$$R = R_o \oplus R_om_1 \oplus \ldots \oplus R_om_h \quad (as\ R_o\text{-}modules),$$

$m_ir_o = r_o^{\sigma_i}m_i$, 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.

By using the decomposition of $R_0 \otimes_Z R_0$ in terms of $Aut(R_o)$ and the fact that R is a module over $R_0 \otimes_Z R_0$, one may obtain the proof of 2.6.

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.

2.7. *Let R and R_o be as in 2.2 and 2.4. Let $char R = p^k$. If $m \neq 0 \in \mathcal{M}$ and p^t is the additive order of m, for some positive integer t, then $|R_om| = p^{tr}$.* This follows from the fact that $R_om \cong R_o/p^tR_o$.

2.8. Let R be a completely primary ring described in 2.2 and let R_o be a maximal Galois subring of R. Then, by 2.3, $R_o = \mathbf{Z}_{p^k}[b]$. Let $K_o =< b > \cup\{0\}$. Then, it is easy to show that every element of R_o can be written uniquely as $\sum_{i=0}^{k-1} p^i\lambda_i$, where $\lambda_i \in K_o$. Since $R = R_o \oplus R_om_1 \oplus \ldots \oplus R_om_h$ (by 2.6), it is easy to see that $\mathcal{M} = pR_o \oplus R_om_1 \oplus \ldots \oplus R_om_h$.

3. Rings with property(T)

Let R be a finite completely primary ring such that if $\mathcal{M}$ is the Jacobson radical, then $\mathcal{M}^3 = (0)$ and $\mathcal{M}^2 \neq (0)$. These rings were first studied by the author in [1] and called them "rings with property(T)". Since R is such that $\mathcal{M}^3 = (0)$, by 2.2, $charR$ is either p, p^2 or p^3. By 2.4, R contains a coefficient subring R_o with $charR_o = charR$, and with R_o/pR_o equal to $R/\mathcal{M}$. Moreover, R_o is a Galois ring of the form $GR(p^{kr}, p^k)$, $k = 1, 2$ or 3.

Let $ann(\mathcal{M})$ denote the two-sided annihilator of $\mathcal{M}$ in R, which is of course an ideal of R. As $\mathcal{M}^3 = (0)$, it follows easily that $\mathcal{M}^2 \subseteq ann(\mathcal{M})$.

We know from 2.6 that $R = R_o \oplus \sum_{i=1}^{h} R_o m_i$, where $m_i \in \mathcal{M}$, and that there exist automorphisms $\sigma_1, ..., \sigma_h \in Aut(R_o)$ such that $m_i r_o = r_o^{\sigma_i} m_i$, for all $r_o \in R_o$ and for all $i = 1, ..., h$; and that the number h and the automorphisms σ_i are uniquely determined by R and R_o. Again, since $\mathcal{M}^3 = (0)$, we have that $p^2 m_i = 0$, for all $m_i \in \mathcal{M}$. Further, $pm_i = 0$ for all $m_i \in ann(\mathcal{M})$. In particular, $pm_i = 0$ for all $m_i \in \mathcal{M}^2$.

Let $d \geq 0$ denote the number of the $m_i \in \{m_1, m_2, ..., m_h\}$ with $pm_i \neq 0$. Since $R = R_o \oplus \sum_{i=1}^{h} R_o m_i$ and every element of R_o can be written uniquely as $\sum_{i=0}^{k-1} p^i \lambda_i$, where $\lambda_i \in K_o$, and if $|R| = p^{nr}$, then, since $|K_o| = p^r$, it follows that

$$n = \begin{cases} h+1 & \text{when } charR = p \\ h+d+2 & \text{when } charR = p^2 \\ h+d+3 & \text{when } charR = p^3. \end{cases}$$

Let $K = R/\mathcal{M}$. If we define scalar multiplication on $\mathcal{M}/ann(\mathcal{M})$ by $(r + \mathcal{M}) \cdot (m + ann(\mathcal{M})) = r \cdot m + ann(\mathcal{M})$, where $r \in R$, $m \in \mathcal{M}$, then it is easy to verify that $\mathcal{M}/ann(\mathcal{M})$ is a vector space over K. Also, if $\dim_K(\mathcal{M}/ann(\mathcal{M})) = s$, then $\dim_K(\mathcal{M}^2) \leq s^2$. In particular, if $\dim_K(\mathcal{M}/ann(\mathcal{M})) = 1$, then $\dim_K(\mathcal{M}^2) = 1$.

4. Rings of characteristic P

In this section we assume R to be a completely primary ring of the introduction, of order p^5 and with $charR = p$. The goal is to determine all isomorphism types for R. When $charR = p$, the maximal Galois subring R_o of R is isomorphic to $\mathbf{F}_p$, and it will be convenient to identify $\mathbf{F}_p$ with R_o. Since $|R| = p^5$, the additive group R^+ must then be isomorphic to $\mathbf{F}_p \oplus \mathbf{F}_p \oplus \mathbf{F}_p \oplus \mathbf{F}_p \oplus \mathbf{F}_p$. Hence, there exist elements $x_1,\ x_2,\ x_3,\ x_4 \in \mathcal{M}$ such that $\{1,\ x_1,\ x_2,\ x_3,\ x_4\}$ is a basis for R^+ as a free R_o-module. The multiplication in R is then determined by the products $x_i x_j$. We proceed our argument by cases based upon the dimension, over R_o/pR_o, of the vector space $\mathcal{M}/ann(\mathcal{M})$. Cleary, $R_o/pR_o \cong \mathbf{F}_p$.

4.1. **The case when** $dim(\mathcal{M}/ann(\mathcal{M})) = 1$**.**

Suppose that $dim(\mathcal{M}/ann(\mathcal{M})) = 1$. Then $dim(\mathcal{M}^2) = 1$, and hence, R^+, as a free R_o-module, has a basis $\{1,\ x_1,\ x_2,\ x_3,\ x_4\}$ with $x_i\mathcal{M} = \mathcal{M}x_i$=(0), for every $i = 2,\ 3,\ 4$; and $x_1^2 = ax_2,\ 0 < a \leq p-1$. Thus, up to isomorphism, the ring R is given by the element $a \in \mathbf{F}_p$. If $\{1,\ x_1^{'},\ x_2^{'},\ x_3^{'},\ x_4^{'}\}$ is another basis for R^+ with structural constant $b \in \mathbf{F}_p^*$, then $x_1^{'}$ is a linear combination of $x_1,\ x_2,\ x_3,\ x_4$. Since $\mathcal{M}^3 = (0)$, we may assume that the coefficients of $x_2,\ x_3,\ x_4$ are zero and write $x_1^{'} = \gamma x_1$, so that $\gamma \in \mathbf{F}_p^*$ is the transition element from the basis $\{\overline{x_1}\}$ of $\mathcal{M}/\mathcal{M}^2$ to the basis $\{\overline{x_1^{'}}\}$. Equally, let $\beta \in \mathbf{F}_p^*$ be the transition element from the basis $\{x_2\}$ of $\mathcal{M}^2$ to $\{x_2^{'}\}$. Now $(x_1^{'})^2 = bx_2^{'}$. However, $(x_1^{'})^2 = \gamma^2 x_1^2 = \gamma^2 a x_2 = \gamma^2 a\beta x_2^{'}$, so that $b = \gamma^2 a\beta$. By taking $\gamma = \beta = 1$, we see that the number of isomorphism classes of rings of this type and of order p^5, where $dim(\mathcal{M}/ann(\mathcal{M})) = 1$, is only 1, for any prime p.

4.2. **The case when** $dim(\mathcal{M}/ann(\mathcal{M})) = 2$**.**

In this case, it is easy to see that $dim(\mathcal{M}^2) = 1$ or 2; and hence, R^+, as a free R_o-module, has a basis $\{1,\ x_1,\ x_2,\ y_1,\ y_2\}$ with $y_i\mathcal{M} = \mathcal{M}y_i$= (0), $i = 1,\ 2$; and either

(i) $x_ix_j = a_{ij}y_1$, where $0 \leq a_{ij} \leq p-1$, $1 \leq i,j \leq 2$; if $dim(\mathcal{M}^2)$ =1; or

(ii) $x_ix_j = \sum_{k=1}^{2} a_{ij}^k y_k$, where $0 \leq a_{ij}^k \leq p-1$; if $dim(\mathcal{M}^2) = 2$.

In case (i), the elements a_{ij} form a 2×2 matrix $A = (a_{ij})$. If $\{1,\ x_1^{'},\ x_2^{'},\ y_1^{'},\ y_2^{'}\}$ is another basis for R^+ with corresponding matrix $B = (b_{ij})$, then $x_1^{'},\ x_2^{'}$ are linear combinations of $x_1,\ x_2,\ y_1,\ y_2$. By assuming that the coefficients of $y_1,\ y_2$ are zero, we may write $x_i^{'} = \gamma_{1i}x_1 + \gamma_{2i}x_2$, so that $C = (\gamma_{ij})$ is the transition matrix from the basis $\{\overline{x_1},\ \overline{x_2}\}$ of $\mathcal{M}/\mathcal{M}^2$ to the basis $\{\overline{x_1^{'}},\ \overline{x_2^{'}}\}$. Similarly, let $\beta \in \mathbf{F}_p^*$ be the transition element from the basis $\{y_1\}$ of $\mathcal{M}^2$ to $\{y_1^{'}\}$. Now $x_i^{'}x_j^{'} = b_{ij}y_1^{'}$, and comparing coefficients of $y_1^{'}$, we obtain the equations which, in matrix form is given by the equivalence relation $C^TAC = \beta B$.

Now, consider the matrices $\beta^{-1}C^TAC$. The representatives of the congruence classes of matrices A in $M_2(\mathbf{F}_q)$ may be given by the following: for characteristic $p \neq 2$, we have;

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} g & 0 \\ 0 & 0 \end{pmatrix},$$
$$\begin{pmatrix} g & 0 \\ 2g & g \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & g \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ \gamma & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ \gamma & g \end{pmatrix},$$

where g is a non-square and γ runs over a complete set of coset representatives of $\{\pm 1\}$ in $\mathbf{F}_q^*$; and these are $q + 7$ altogether; and for characteristic

$p = 2$, we have;

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

where $\alpha \in \mathbf{F}_q^*$; and these are $q+4$ in all.

Now, if $|F| = 2$, then there are 5 non-zero congruence classes and since $\beta = 1$ in this case, these matrices also represent equivalence classes. For $|F| = p,\ p \neq 2$, there are $p + 6$ non-zero congruence classes. If $\beta = g$ is an element of $\mathbf{F}_p^*$, it is easy to see that the congruence class $\begin{pmatrix} g & 0 \\ 2g & g \end{pmatrix}$ is equivalent to one of the classes of the form $\begin{pmatrix} 1 & 0 \\ \gamma & 1 \end{pmatrix}$; and the classes $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ and $\begin{pmatrix} g & 0 \\ 0 & 0 \end{pmatrix}$ are equivalent. Therefore, the number of equivalence classes in this case is $p + 4$ and this also gives the number and models for the corresponding rings. Thus, the number of isomorphism classes of rings of this type, characteristic p and of order p^5, where $dim(\mathcal{M}/ann(\mathcal{M})) = 2$ and $dim(\mathcal{M}^2) = 1$ is 5 if $p = 2$ and $p+4$ if $p \neq 2$, and the number of commutative rings of this type is 3 for every prime p.

In case (ii), the elements a_{ij}^k form two linearly independent matrices $A_1 = (a_{ij}^1),\ A_2 = (a_{ij}^2)$ of size 2×2. In [5] page 249 and [6] page 234, Corbas and Williams obtained numbers of equivalence classes of pairs of linearly independent matrices over finite fields and we deduce from their results that the number of isomorphism classes of these rings of characteristic p and of order p^5, where $dim(\mathcal{M}/ann(\mathcal{M})) = 2$ and $dim(\mathcal{M})^2 = 2$, is 10 when $p = 2$ and $3p + 5$ when $p \neq 2$. Of these, 3 are commutative (for any prime p), the others are not.

4.3. **The case when** $dim(\mathcal{M}/ann(\mathcal{M})) = 3$**.**

It is clear in this case that $dim(\mathcal{M}^2) = 1$ since $|R| = p^5$, and hence, R^+ has a basis $\{1,\ x_1,\ x_2,\ x_3,\ y\}$ with $y\mathcal{M} = \mathcal{M}y = (0)$, and $x_i x_j = a_{ij} y$, where $0 \leq a_{ij} \leq p - 1,\ 1 \leq i, j \leq 3$. The elements a_{ij} form a 3×3 non-zero matrix $A = (a_{ij})$. If $\{1,\ x_1',\ x_2',\ x_3',\ y'\}$ is another basis for R^+ with corresponding matrix $B = (b_{ij})$, then $x_1',\ x_2',\ x_3'$ are linear combinations of $x_1,\ x_2,\ x_3,\ y$. As before, since $\mathcal{M}^3 = (0)$, we may assume, that the coefficient of y is zero and write $x_i' = \gamma_{1i}x_1 + \gamma_{2i}x_2 + \gamma_{3i}x_3$, so that $C = (\gamma_{ij})$ is the transition matrix from the basis $\{\overline{x_1},\ \overline{x_2},\ \overline{x_3}\}$ of $\mathcal{M}/\mathcal{M}^2$ to the basis $\{\overline{x_1'},\ \overline{x_2'},\ \overline{x_3'}\}$. Similarly, let $\beta \in \mathbf{F}_p^*$ be the transition element from the basis $\{y\}$ of $\mathcal{M}^2$ to $\{y'\}$. Now $x_i' x_j' = b_{ij} y'$, and comparing coefficients of y', we obtain the equations which, in matrix form, is given by the equivalence relation $C^T A C = \beta B$. As before, we consider the matrices $\beta^{-1} C^T A C = B$.

The congruence classes of matrices A in $M_3(\mathbf{F}_q)$ have the following representatives: when characteristic of $\mathbf{F}_q$ is $p \neq 2$, we have;

$$\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} \varepsilon & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix},$$
$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & \varepsilon & 0 \\ 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \varepsilon \end{pmatrix}, \begin{pmatrix} \mu & 0 & 0 \\ 0 & 0 & 1 \\ 0 & -1 & 0 \end{pmatrix},$$
$$\begin{pmatrix} \mu & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} \mu & 0 & 0 \\ 0 & \varepsilon & 0 \\ 0 & 2\varepsilon & \varepsilon \end{pmatrix}, \begin{pmatrix} \mu & 0 & 0 \\ 0 & 1 & 0 \\ 0 & \gamma & 1 \end{pmatrix}, \begin{pmatrix} \mu & 0 & 0 \\ 0 & 1 & 0 \\ 0 & \gamma & \varepsilon \end{pmatrix},$$
$$\begin{pmatrix} \mu & 0 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix},$$

where $\mu \in \{0,\ 1,\ \varepsilon\}$, with ε an arbitrary but fixed non-square in $\mathbf{F}_q^*$, and γ runs over a complete set of coset representatives of $\{\pm 1\}$ in $\mathbf{F}_q^*$, and their total is $3q + 16$; and when characteristic of $\mathbf{F}_q$ is $p = 2$, we have;

$$\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$
$$\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} \mu & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} \mu & 0 & 0 \\ 0 & 1 & 0 \\ 0 & \gamma & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 1 & 0 \end{pmatrix},$$
$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ \alpha & 1 & 1 \end{pmatrix},$$

where $\mu \in \{0,\ 1\}$, $\gamma \in F^*$ and $X^2 + \alpha X + 1$ is an arbitrary but fixed irreducible polynomial of degree two over F. Their total is $2q + 8$.

Now, suppose $|F| = 2$. Then we can deduce from the above list that the number of non-zero congruence classes is 11. Since in this case $\beta = 1$, these classes are also the equivalence classes, and hence the number of non-isomorphic rings of this type and of characteristic $p = 2$.

If $|F| = p,\ p \neq 2$, then the list above gives $3p + 15$ non-zero congruence classes. As β runs over the elements of $\mathbf{F}_p^*$, the congruence classes

$$\begin{pmatrix} \varepsilon & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \varepsilon \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 \\ 0 & \varepsilon & 0 \\ 0 & 2\varepsilon & \varepsilon \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & \varepsilon & 0 \\ 0 & 2\varepsilon & \varepsilon \end{pmatrix},$$

and $\begin{pmatrix} \varepsilon & 0 & 0 \\ 0 & \varepsilon & 0 \\ 0 & 2\varepsilon & \varepsilon \end{pmatrix}$, become equivalent to $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$, $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, $\begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & \gamma & 1 \end{pmatrix}$, $\begin{pmatrix} \varepsilon & 0 & 0 \\ 0 & 1 & 0 \\ 0 & \gamma & 1 \end{pmatrix}$, and $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & \gamma & 1 \end{pmatrix}$, respectively. Thus, the number of equivalence classes is $3p + 10$.

Collectively, the number of isomorphism classes of rings of this type of characteristic p and of order p^5, where $dim(\mathcal{M}/ann(\mathcal{M})) = 3$ (and hence, $dim(\mathcal{M}^2) = 1$), is 11 when $p = 2$ and $3p + 10$ when $p \neq 2$, and the number of commutative ones is 4, for every prime p. The models for these rings can easily be deduced from the lists of congruence classes given above.

We summarize the results of this section in the following:

Proposition 4.1. *The number of mutually non-isomorphic rings of this type, of characteristic* p *and of order* p^5 *is* 27 *when* $p = 2$ *and* $7p + 20$ *when* $p \neq 2$. *Of these, the number of commutative ones is* 11 *for every prime* p.

5. Rings of characteristic P^2

Let R be a ring of the introduction, of order p^5 and characteristic p^2. All possible isomorphism types for R will be described.

When $char R = p^2$, the maximal Galois subring R_o of R is isomorphic to $\mathbf{Z}_{p^2}$, and it will be convenient to identify $\mathbf{Z}_{p^2}$ and R_o. Since $|R| = p^5$, the additive group R^+ of R must then be isomorphic to one of the following:

$$(1)\ \mathbf{Z}_{p^2} \oplus \mathbf{Z}_p \oplus \mathbf{Z}_p \oplus \mathbf{Z}_p;\ \text{ or } (2)\ \mathbf{Z}_{p^2} \oplus \mathbf{Z}_{p^2} \oplus \mathbf{Z}_p.$$

5.1. The case where $R^+ = \mathbf{Z}_{p^2} \oplus \mathbf{Z}_p \oplus \mathbf{Z}_p \oplus \mathbf{Z}_p$.

It is clear in this case that $\mathcal{M} = pZ_{p^2} \oplus Z_p \oplus Z_p \oplus Z_p$; and as such, we have that $p \in ann(\mathcal{M})$; and hence, either (i) $p \in \mathcal{M}^2$, or (ii) $p \notin \mathcal{M}^2$.

5.1.1. *Case*(i). Suppose that $p \in \mathcal{M}^2$. Let $x, y, z \in R$, such that $\{p,\ x,\ y,\ z\}$ is a basis for the additive group $\mathcal{M}$ as a free $\mathbf{Z}_{p^2}-$module. Obviously, $\{1,\ x,\ y,\ z\}$ is a basis for the additive group R^+ of R (also as a $\mathbf{Z}_{p^2}-$module). Further, each element of R can be written (not necessarily uniquely) in the form $\alpha_o + \alpha_1 x + \beta_1 y + \gamma_1 z$ where $\alpha_o,\ \alpha_1,\ \beta_1,\ \gamma_1 \in \mathbf{Z}_{p^2}$ and $px = py = pz = 0$. Thus $\mathbf{Z}_{p^2}$ serves as a set of scalars for the ring R, as we have noted above.

(i) Now, suppose that $dim(\mathcal{M}/ann(\mathcal{M})) = 1$ over $\mathbf{Z}_{p^2}/p\mathbf{Z}_{p^2}$. Then, obviously, $dim(\mathcal{M}^2) = 1$ and hence, we have that $x^2 = ap$, with $0 < a \leq p - 1$, and the rest of the other products are equal to zero. Thus R possesses the element a as its structural constant. As in 4.1, a change of basis with corresponding structural constant b leads to the relation $b = \gamma^2 a\beta$, with

$\gamma,\ \beta \in (Z_{p^2}/pZ_{p^2})^*$. Here, $\beta = 1$ as any ring homomorphism sends p to itself. Now, the set $H = \{\gamma^2 :\ \gamma \in (Z_{p^2}/pZ_{p^2})^*\}$ is a subgroup of $(Z_{p^2}/pZ_{p^2})^*$ and infact $H =< (\delta + pZ_{p^2})^2 >$, where $\delta \in Z_{p^2}$ of multiplicative order $p^2 - 1$. However,

$$| < (\delta + pZ_{p^2})^2 > | = \frac{p^2-1}{(p^2-1,\ 2)} = \begin{cases} p^2-1 & \text{if } p = 2 \\ \frac{p^2-1}{2} & \text{if } p \neq 2. \end{cases}$$

Thus, for a fixed $\gamma \in< (\delta + pZ_{p^2})^2 >$, the number of rings of this type isomorphic to the ring with structural constant a is

$$\begin{cases} p^2-1 & \text{if } p = 2 \\ \frac{p^2-1}{2} & \text{if } p \neq 2. \end{cases}$$

Thus, the number of isomorphism classes of rings with property(T) of order p^5 and characteristic p^2 in which $p \in \mathcal{M}^2$ and where $dim(\mathcal{M}/ann(\mathcal{M})) = 1$ is 1 when $p = 2$ and 2 when $p \neq 2$. Moreover, these rings are all commutative.

(ii) Next, suppose that $dim(\mathcal{M}/ann(\mathcal{M})) = 2$ over $\mathbf{Z}_{p^2}/p\mathbf{Z}_{p^2}$. Then either $dim(\mathcal{M}^2) = 1$ or 2.

Let us first consider the case where $dim(\mathcal{M}^2) = 1$. In this case, the ring R is defined by one structural matrix A, where A is a 2×2 non-zero matrix with entries in $\mathbf{Z}_{p^2}/p\mathbf{Z}_{p^2}$. As in case(i) of 4.2, we have the relation which, in matrix form is given by the equivalence relation $\beta^{-1}C^TAC = B$. Since any isomorphism between two rings of this type sends the element p to itself, we may take $\beta = 1$ in the above relation. Since $\mathbf{Z}_{p^2}/p\mathbf{Z}_{p^2} \cong \mathbf{F}_p$, we may apply the method of case(i) of 4.2 to conclude that the number of equivalence classes of 2×2 matrices over $\mathbf{Z}_{p^2}/p\mathbf{Z}_{p^2}$ is equal to the number of non-zere congruence classes. Hence, the number of mutually non-isomorphic rings of this type is 5 if $p = 2$, and $p + 6$ if $p \neq 2$. The number of commutative ones is 3 when $p = 2$ and 4 when $p \neq 2$.

We now turn to the case where $dim(\mathcal{M}^2) = 2$. In this case, R has two linearly independent matrices A_1 and A_2 as its structural matrices. From case(ii) of 4.2, we deduce that the number of non-isomorphic rings of this type is 10 if $p = 2$ and $3p + 5$ if $p \neq 2$. Of these, only 3 are commutative for every prime p, the others are not.

(iii) Finally, suppose that $dim(\mathcal{M}/ann(\mathcal{M})) = 3$ over $\mathbf{Z}_{p^2}/p\mathbf{Z}_{p^2}$. Obviously, $dim(\mathcal{M}^2) = 1$, and we can rewrite the basis for $\mathcal{M}$ in the form $\{x_1,\ x_2,\ x_3,\ p\}$ and so $x_ix_j = a_{ij}p$, with $0 \leq a_{ij} \leq p - 1$, $1 \leq i, j \leq 3$. The elements a_{ij} form a 3×3 non-zero matrix $A = (a_{ij})$. By similar calculations as in 4.3, we deduce that the number of isomorphism classes of rings of this type, of characteristic p^2 and of order p^5, where $dim(\mathcal{M}/ann(\mathcal{M})) = 3$ (and hence, $dim(\mathcal{M}^2) = 1$), in which $p \in \mathcal{M}^2$ is 11 when $p = 2$ and $3p + 15$ when

$p \neq 2$ (since $\beta = 1$). Of these, the number of commutative rings is 4 when $p = 2$ and 6 when $p \neq 2$. The models for these rings can easily be deduced from the lists of congruence classes of 3×3 matrices given in 4.3.

This completes our description of rings of this type, of order p^5 and characteristic p^2 in which $p \in \mathcal{M}^2$ and altogether, there are 27 with 11 commutative ones, if $p = 2$ and $7p + 28$ with 15 commutative ones if $p \neq 2$.

5.1.2. *Case*(ii). Suppose now that $p \in ann(\mathcal{M})$ but $p \notin \mathcal{M}^2$. Again, let $x,\ y,\ z \in R$, such that $\{p,\ x,\ y,\ z\}$ is a basis for the additive group of $\mathcal{M}$. Of course, as in the previous case, $\{1,\ x,\ y,\ z\}$ is a basis for R^+ and each element of R can be written (not necessarily uniquely) in the form $\alpha_o + \alpha_1 x + \beta_1 y + \gamma_1 z$, where $\alpha_o,\ \alpha_1,\ \beta_1,\ \gamma_1 \in \mathbf{Z}_{p^2}$ and $px = py = pz = 0$. Thus $\mathbf{Z}_{p^2}$ serves as a set of scalars for the ring R.

(i) Now, suppose that $dim(\mathcal{M}/ann(\mathcal{M})) = 1$ over $\mathbf{Z}_{p^2}/p\mathbf{Z}_{p^2}$. Then, obviously, $dim(\mathcal{M}^2) = 1$ and hence, we have that $x^2 = ay$, with $0 < a \leq p - 1$, and the rest of the other products are equal to zero. Thus R possesses the element a as its structural constant. A change of basis with structural constant b gives the relation $b = \gamma^2 a\beta$. Hence, we may select $\gamma = 1$ and $\beta = a^{-1}$, so that for a fixed $a \in (\mathbf{Z}_{p^2}/p\mathbf{Z}_{p^2})^*$, the number of rings isomorphic to one with structural constant a is $p^2 - 1$, for any prime p. Thus, we have precisely one isomorphism class of rings of this type, of order p^5 and characteristic p^2 in which $p \in ann(\mathcal{M})$ and $p \notin \mathcal{M}^2$, and where $dim(\mathcal{M}/ann(\mathcal{M})) = 1$ and $dim(\mathcal{M}^2) = 1$.

(ii) Next, if $dim(\mathcal{M}/ann(\mathcal{M})) = 2$ over $\mathbf{Z}_{p^2}/p\mathbf{Z}_{p^2}$, it is clear that $dim(\mathcal{M}^2) = 1$ since $p \notin \mathcal{M}^2$, and by similar calculations as in case(ii) of 3.2, we have that the number of isomorphism classes of rings of this type is 5 when $p = 2$ and $p + 4$ when $p \neq 2$. Of these, 3 are commutative for every prime p. Therefore, the total number of distinct rings of this type, of order p^5 and characteristic p^2 in which $p \in ann(\mathcal{M}) - \mathcal{M}^2$ is 6 with 4 commutative ones if $p = 2$ and $p + 5$ with 4 commutative ones if $p \neq 2$.

To summarize the results in the case of rings of this type, of order p^5 and characteristic p^2 in which $p \in ann(\mathcal{M})$, the number of mutually non-isomorphic rings of this type has been shown to be 33 when $p = 2$ and $8p + 33$ otherwise. Only 15 are commutative when $p = 2$ and 19 when $p \neq 2$.

5.2. **The case where $R^+ = \mathbf{Z}_{p^2} \oplus \mathbf{Z}_{p^2} \oplus \mathbf{Z}_p$.**

In this case, it is clear that $p \notin ann(\mathcal{M})$. Let $x,\ y \in R$ such that $\{1,\ x,\ y\}$ is a basis for R^+. Then, it is obvious that $\{p,\ x,\ y\}$ is a basis for the additive group $\mathcal{M}$. Hence, each element of R can be written (not necessarily uniquely) in the form $\alpha_o + \alpha_1 x + \beta_1 y$, where $\alpha_o,\ \alpha_1,\ \beta_1 \in \mathbf{Z}_{p^2}$ and $py = 0$.

Since $p \notin ann(\mathcal{M})$ and $p^2 = 0$, it follows that there is no ring R of this type for which $dim(\mathcal{M}/ann(\mathcal{M})) = 1$. So, $dim(\mathcal{M}/ann(\mathcal{M})) \geq 2$.

(i) Suppose that $dim(\mathcal{M}/ann(\mathcal{M})) = 2$ over $\mathbf{Z}_{p^2}/p\mathbf{Z}_{p^2}$. Then either $dim(\mathcal{M}^2) = 1$ or 2. If $dim(\mathcal{M}^2) = 1$, then $px \neq 0$ and we can find an element $a \in \mathbf{Z}_{p^2}/p\mathbf{Z}_{p^2}$ such that $x^2 = apx$. Thus, R has $\begin{pmatrix} 0 & 1 \\ 1 & a \end{pmatrix}$, as its structural matrix.

Now, a ring R' is isomorphic to the ring R if it has a structural matrix of the form $\beta^{-1}C^T \begin{pmatrix} 0 & 1 \\ 1 & a \end{pmatrix} C$, where $C \in GL(2, \mathbf{Z}_{p^2}/p\mathbf{Z}_{p^2})$, and $\beta \in (\mathbf{Z}_{p^2}/p\mathbf{Z}_{p^2})^*$. Since $p^2 = 0$ in every ring of this type, the above matrix must be of the form $\begin{pmatrix} 0 & \alpha \\ \alpha & \gamma \end{pmatrix}$, $\alpha \in (\mathbf{Z}_{p^2}/p\mathbf{Z}_{p^2})^*$ and $\gamma \in \mathbf{Z}_{p^2}/p\mathbf{Z}_{p^2}$.

Now, if $char(\mathbf{Z}_{p^2}/p\mathbf{Z}_{p^2}) = 2$ and $a \neq 0$, we can select $\beta = a$ and $C = \begin{pmatrix} 1 & 0 \\ 0 & 1/a \end{pmatrix}$; to see that the rings with structural matrices $\begin{pmatrix} 0 & 1 \\ 1 & a \end{pmatrix}$ and $\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$ are isomorphic. Thus, for a fixed $a \in (\mathbf{Z}_{p^2}/p\mathbf{Z}_{p^2})^*$, there exist precisely one ring of this type; namely, the ring with structural matrix $\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$.

If $a = 0$, then it is clear that the ring with structural matrix $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ is not isomorphic to the one with structural matrix $\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$ as these two matrices belong to different equivalence classes (see Section 4). Thus, if $char(\mathbf{Z}_{p^2}/p\mathbf{Z}_{p^2}) = 2$, there are precisely two isomorphism classes of rings of this type.

Next, if $char(\mathbf{Z}_{p^2}/p\mathbf{Z}_{p^2}) \neq 2$, we can select $\beta = 1$ and $C = \begin{pmatrix} 1 & 0 \\ \frac{1-a}{2} & 1 \end{pmatrix}$, to see that the rings with structural matrices $\begin{pmatrix} 0 & 1 \\ 1 & a \end{pmatrix}$, for any $a \in \mathbf{Z}_{p^2}/p\mathbf{Z}_{p^2}$, and $\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$are isomorphic. Therefore, if $char(\mathbf{Z}_{p^2}/p\mathbf{Z}_{p^2}) \neq 2$, there is exactly one ring of this type, up to isomorphism, namely, the ring with structural matrix $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Thus, the number of isomorphism classes of rings of this type is 2 when $p = 2$ and 1 otherwise. There rings are all commutative.

If $dim(\mathcal{M}^2) = 2$, then we can find elements a and $0 \neq c$ in $\mathbf{Z}_{p^2}/p\mathbf{Z}_{p^2}$ such that $x^2 = apx + cy$ and this leads to 10 or $3p + 5$ mutually non- isomorphic rings according as $p = 2$ or $p \neq 2$. Of these, 3 are commutative, the others are not (see case(ii) of 4.2).

(ii) Finally, suppose that $dim(\mathcal{M}/ann(\mathcal{M})) = 3$. Then $dim(\mathcal{M}^2) = 1$ and we can find elements $\alpha,\ \beta,\ \gamma,\ \varepsilon \in \mathbf{Z}_{p^2}/p\mathbf{Z}_{p^2}$ such that $x^2 = \alpha px$, $xy = \beta px$, $yx = \gamma px$, $y^2 = \varepsilon px$. These elements form a 3×3 non-zero matrix A, and since $p^2 = 0$, we apply methods of 4.3, to obtain 11 when $p = 2$ and $3p + 10$ when $p \neq 2$, isomorphism classes of rings of this type. Only 4 are commutative for each prime p.

To summarize the results in the case of rings of this type, of order p^5 and characteristic p^2 in which $p \notin ann(\mathcal{M})$, the number of mutually non-isomorphic rings of this type has been shown to be 23 when $p = 2$ and $6p + 16$ otherwise. Of these, the commutative ones are 9 when $p = 2$ and 8 when $p \neq 2$.

We can now state the following:

Proposition 5.1. *The number of isomorphism classes of rings of this type, of order p^5 and characteristic p^2 is 56 when $p = 2$ and $14p + 49$ when $p \neq 2$. Of these, 24 are commutative when $p = 2$ and 27 when $p \neq 2$. The others are not.*

6. Rings of characteristic P^3

Let R be a ring of this type, of order p^5 and characteristic p^3. In this section, we shall describe all possible isomorphism types of these rings.

When $char R = p^3$, the maximal Galois subring R_o of R is isomorphic to $\mathbf{Z}_{p^3}$, and we shall identify R_o and $\mathbf{Z}_{p^3}$. Since $|R| = p^5$, the additive group R^+ of R must be isomorphic to one of the following:

$$\text{(i) } \mathbf{Z}_{p^3} \oplus \mathbf{Z}_p \oplus \mathbf{Z}_p; \text{ or (ii) } \mathbf{Z}_{p^3} \oplus \mathbf{Z}_{p^2}.$$

6.1. The case where $R^+ = \mathbf{Z}_{p^3} \oplus \mathbf{Z}_p \oplus \mathbf{Z}_p$.

Let $x,\ y \in R$, such that $\{1,\ x,\ y\}$ is a basis for the additive group R^+. Then each element of R can be written (not necessarily uniquely) as $\alpha_o + \alpha_1 x + \alpha_2 y$, where $\alpha_o,\ \alpha_1,\ \alpha_2 \in \mathbf{Z}_{p^3}$. As before, the argument proceeds by cases based upon the dimension, over R_o/pR_o, of the vector space $\mathcal{M}/ann(\mathcal{M})$. Obviously, $R_o/pR_o \cong \mathbf{F}_p$.

(i) Suppose $dim(\mathcal{M}/ann(\mathcal{M})) = 1$. Then $dim(\mathcal{M}^2) = 1$ and hence,

$$px = py = x^2 = xy = yx = y^2 = 0;\ p^2 \neq 0;$$

and this multiplication leads to precisely one ring up to isomorphism for any prime p.

(ii) Suppose $dim(\mathcal{M}/ann(\mathcal{M})) = 2$. Then $dim(\mathcal{M}^2) = 1$ or 2. If $dim(\mathcal{M}^2) = 1$, we can find a non-zero element $a \in \mathbf{F}_p$ such that $x^2 = ap^2$, and the other products are all equal to zero. As in 5.1(i) we have that the number of isomorphism classes of rings of this type is 1 when $p = 2$ and 2 when $p \neq 2$. These rings are all commutative.

If $dim(\mathcal{M}^2) = 2$, we can find elements a and $0 \neq c$ in $\mathbf{F}_p$ such that $x^2 = ap^2 + cy$, and the rest of the products are zero. The structural matrices in that definition of this ring are diagonal matrices of the form $\begin{pmatrix} 1 & 0 \\ 0 & a \end{pmatrix}$ $\begin{pmatrix} 0 & 0 \\ 0 & c \end{pmatrix}$. This leads to precisely one commutative ring for any prime.

(iii) Suppose $dim(\mathcal{M}/ann(\mathcal{M})) = 3$. Then $dim(\mathcal{M}^2) = 1$, and we can find elements $\alpha,\ \beta,\ \gamma,\ \varepsilon \in \mathbf{Z}_p$ such that $x^2 = \alpha p^2$, $xy = \beta p^2$, $yx = \gamma p^2$, $y^2 = \varepsilon p^2$ and the rest of the products are zero. These elements form a 3×3 non-zero matrix $\begin{pmatrix} 1 & 0 & 0 \\ 0 & \alpha & \beta \\ 0 & \gamma & \varepsilon \end{pmatrix}$,and we deduce from 5.1(i) that the number of isomorphism classes of rings of this type is 5 when $p = 2$ and $p + 6$ when $p \neq 2$. The commutative ones are 3 or 4, according as $p = 2$ or $p \neq 2$.

Thus, there are 8 with 6 commutative rings of this type when $p = 2$ and $p + 10$ with 8 commutative ones when $p \neq 2$, and this completes our description of 6.1.

6.2. **The case where $R^+ = \mathbf{Z}_{p^3} \oplus \mathbf{Z}_{p^2}$.**

Let $x \in R$ such that $\{1,\ x\}$ is a basis for R^+. Then each element of R can be written (not necessarily uniquely) in the form $\alpha_o + \alpha_1 x$, where $\alpha_o,\ \alpha_1 \in \mathbf{Z}_{p^3}$. Since $px \neq 0$ in this case, it follows that $dim(\mathcal{M}/ann(\mathcal{M})) > 1$. Suppose $dim(\mathcal{M}/ann(\mathcal{M})) = 2$. Then $dim(\mathcal{M}^2) = 1$ or 2. Again, since $px \neq 0$, $dim(\mathcal{M}^2) \neq 1$. So, $dim(\mathcal{M}^2) = 2$ and therefore, we can find elements a and c in $\mathbf{Z}_p$ such that $x^2 = ap^2 + cpx$. This leads to precisely one commutative isomorphism class of rings of this type, for any prime p.

We have thus proved the following:

Proposition 6.1. *The number of isomorphism classes of rings of this type, of order p^5 and characteristic p^3 is 9 when $p = 2$ and $p + 11$ when $p \neq 2$. Of these, 7 are commutative when $p = 2$ and 9 when $p \neq 2$.*

We now state the main result of this paper.

Theorem 6.2. *The number of isomorphism classes of rings of this type and of order p^5 is 92 when $p = 2$ and $22p + 80$ when $p \neq 2$. Of these, the number of commutative ones is 42 when $p = 2$ and 47 when $p \neq 2$.*

Proof. This follows from Propositions 4.1, 5.1 and 6.1. □

References

[1] C. J. Chikunji, *On a Class of Finite Rings,* Comm. Algebra, **27**(10), 5049–5081 (1999).
[2] C. J. Chikunji, *Classification of a Class of Finite Rings* (submitted to Demonstratio Mathematica)
[3] W. E. Clark, *A coefficient ring for finite non-commutative rings*, Proc. Amer. Math. Sec. **33**, No1(1972), 25–28.
[4] B. Corbas, *Rings with few zero divisors*, Math. Ann. **181**(1969), 1–7.
[5] B. Corbas and G. D. Williams, *Congruence of Two-Dimensional Subspaces of* $M_2(K)$ (*characteristic* $\neq 2$), Pacific J. of Math., **188**(2)(1999), 225–235.
[6] B. Corbas and G. D. Williams, *Congruence of Two-Dimensional Subspaces of* $M_2(K)$ (*characteristic* $= 2$), Pacific J. of Math., **188**(2)(1999), 237–249.
[7] R. Raghavendran, *Finite associative rings*, Compositio Math. **21**, Fac.2 (1969), 195–229.
[8] B. R. Wirt, *Finite non-commutative local rings*, Ph.D. Thesis, Univ. of Oklahoma (1972).

Chiteng'a John Chikunji
Department of Mathematics
University of Transkei
P/BAG X1, UMTATA 5117
Republic of South Africa
e-mail address: chikunji@getafix.utr.ac.za

(*Received July 18, 2003*)