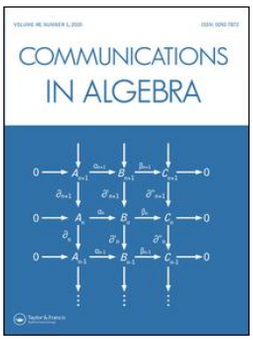

Communications in Algebra

ISSN: 0092-7872 (Print) 1532-4125 (Online) Journal homepage: https://www.tandfonline.com/loi/lagb20

On a class of finite rings

Chiteng'a John Chikunji

To cite this article: Chiteng'a John Chikunji (1999) On a class of finite rings, Communications in Algebra, 27:10, 5049-5081, DOI: 10.1080/00927879908826747

To link to this article: https://doi.org/10.1080/00927879908826747

Published online: 27 Jun 2007.

COMMUNICATIONS IN ALGEBRA, 27(10), 5049–5081 (1999)

ON A CLASS OF FINITE RINGS

Chiteng'a John Chikunji

Department of Mathematics and Statistics,
University of Zambia, Lusaka.

Abstract

In [7], Corbas determined all finite rings in which the product of any two zero-divisors is zero, and showed that they are of two types, one of characteristic p and the other of characteristic p^2.

The purpose of this paper is to address the problem of the classification of finite rings such that

(i) the set of all zero-divisors form an ideal $\mathcal{M}$;

(ii) $\mathcal{M}^3 = (0)$; and

(iii) $\mathcal{M}^2 \neq (0)$.

Because of (i), these rings are called *completely primary* and we shall call a finite completely primary ring R which satisfies conditions (i), (ii) and (iii), *a ring with property(T)*. These rings are of three types, namely, of characteristic p, p^2 and p^3. The characteristic p^2 case is subdivided into cases in which $p \in \mathcal{M}^2$, $p \in ann(\mathcal{M}) - \mathcal{M}^2$ and $p \in \mathcal{M} - ann(\mathcal{M})$, where $ann(\mathcal{M})$ denotes the two-sided annihilator of $\mathcal{M}$ in R.

0 Introduction

Throughout, all rings are finite, associative (but generally not commutative) and have an identity element, denoted by 1. Further, it is assumed that homomorphisms preserve 1, subrings have the same 1 and modules are unital.

We begin with a section of preliminaries, where we gather the required notions about finite completely primary rings. In Section 2, we give a brief review of the types of finite completely primary rings that have been classified in terms of well known structures; see Raghavendran [9] and Corbas [6] and [7].

In Section 3, we consider rings with a certain property(T) and obtain some elementary results concerning these rings. Section 4 describes rings with property(T) and of characteristic p, giving a construction of these rings and proving that this construction indeed describes them all and in Section 5 we consider the problem of enumerating these rings. In particular, we give a method of determining the isomorphism classes of these rings in the case where the maximal Galois subfield lies in the centre. In Section 6, we consider the remaining cases, namely, those of characteristic p^2 and p^3, respectively. In the last Section, we extend the problem of section 5 to these cases; that is, we give formulae for determining the isomorphism classes of these rings in the cases where the maximal Galois subrings lie in the center.

1 Preliminaries

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

The following are the known results.

1.1 *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 [6]).

The following results can be found in [9].

1.2 *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) $charR = p^k$ *where* $1 \leq k \leq n$.

1.3 *Let* R *be as in 1.2. 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 $GR(p^{kr}, p^k)$.

1.4 *Let* R *be as in 1.2 and let* $charR = p^k$. *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].

1.5 *Let* R *be as in 1.2. 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 [9]).

The following result is due to Wirt [13].

1.6 *Let* R *be as in 1.2. Then there exist* $m_1, ..., m_h \in \mathcal{M}$ *and* $\sigma_1, ..., \sigma_h \in Aut(R_o)$ *such that*

$$R = R_o \oplus R_om_1 \oplus \ldots \oplus R_om_h \qquad (as\ R_o - modules\ ),$$

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

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 1.6.

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.

1.7 *Let* R *be as in 1.2 and let* $charR = p^k$. *If* $m \in \mathcal{M}$ *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 $R_om \cong R_o/p^tR_o$.

1.8 Let R be a completely primary ring and let R_o be a maximal Galois subring of R. Then, by 1.3, $R_o = \mathbf{Z}_{p^k}[b]$. 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 1.6), it is easy to see that $\mathcal{M} = pR_o \oplus R_om_1 \oplus \ldots \oplus R_om_h$.

2 Review of well-known structures

We briefly review the types of finite completely primary rings that have been classified in terms of well known structures; see Raghavendran [9] and Corbas [6] and [7].

Raghavendran attacked the problem by taking a finite completely primary ring of order p^{nr}, and characteristic p^k and considering the two extreme cases $k = 1$ and $k = n$. For rings of characteristic p, he was only able to give complete classification in two special cases:

(a) when $\mathcal{M}^2 = (0)$; and

(b) when $\mathcal{M}^{n-1} \neq (0)$ so that $\mathcal{M}$ has index of nilpotence n. In both cases, the rings can be represented as rings of matrices over $GF(p^r)$. Corbas [7] has also given a classification of rings of type (a), but, in fact, his work goes much further and classifies **all** finite rings with $\mathcal{M}^2 = (0)$. These are of two types, one of characteristic p, and the other of characteristic p^2.

Completely primary rings with full characteristic p^n have been of interest for some years. Clark mentions in [3] that Krull worked with these rings as early as 1924, and that Janusz rediscovered them in [8]. Raghavendran has classified these rings as quotients of polynomial rings. It is worth noting that Raghavendran's classification of these rings had already been discovered by both Krull and Janusz, although their considerations have been less detailed. Indeed, the terminology "Galois Rings" which Raghavendran uses for a ring of this type, was introduced by Janusz.

In [9], one more type of completely primary rings is considered and a classification produced, namely, those completely primary rings of order p^{nr}, and maximal ideal $\mathcal{M}$ of index of nilpotence $n - 1$. Raghavendran called them near-Galois rings.

The only other completely primary rings for which a classification has been produced are those finite rings with n zero-divisors and order exactly n^2. Corbas shows in [6] that there are exactly two types of these rings, one being of order p^{2r}, and characteristic p (so that $\mathcal{M}^2 = (0)$), and the other of order p^{2r} and characteristic p^2, i.e. a Galois ring. So both of these types are included in the classifications produced by Raghavendran.

In summary, the types of completely primary rings that have been classified are:

(i) rings of order p^{nr} and characteristic p^k with $\mathcal{M}^2 = (0)$, for any k;

(ii) rings of order p^{nr} and characteristic p with $\mathcal{M}^{n-1} \neq (0)$;

(iii) rings of order p^{nr} and characteristic p^n, i.e. Galois rings; and

(iv) rings of order p^{nr} and characteristic p^{n-1} with $\mathcal{M}^{n-1} \neq (0)$; i.e. near-Galois rings; for any prime p and positive integers n and r.

3 Rings with property(T)

In this section, we obtain some elementary results concerning rings with property(T). Let R be a ring with property(T). Since R is such that $\mathcal{M}^3 = (0)$, then by 1.2 $charR$ is either p, p^2 or p^3. Hence, by 1.4, 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. Because $\mathcal{M}^3 = (0)$, it follows easily that $\mathcal{M}^2 \subseteq ann(\mathcal{M})$.

We know from 1.6 that $R = R_o \oplus R_o m_1 \oplus \ldots \oplus R_o m_h$, where $m_i \in \mathcal{M}$, and that there exist automorphisms $\sigma_1, \ldots, \sigma_h \in Aut(R_o)$ such that $m_i r_o = r_o^{\sigma_i} m_i$, for all $r_o \in R_o$ and for all $i = 1, \ldots, h$; 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 $m_i \in \{m_1, m_2, \ldots, m_h\}$ with $pm_i \neq 0$. Since $R = R_o \oplus R_o m_1 \oplus \ldots \oplus R_o m_h$ 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

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

Lemma 3.1 *Let R be a ring with property(T) and let $K = R/\mathcal{M}$. Then $\mathcal{M}/ann(\mathcal{M})$ is a vector space over K.*

Proof It is easy to verify that $\mathcal{M}/ann(\mathcal{M})$ is a vector space over K on defining scalar multiplication on $\mathcal{M}/ann(\mathcal{M})$ by

$$(r + \mathcal{M}) \cdot (m + ann(\mathcal{M})) = r \cdot m + ann(\mathcal{M}),$$

$r \in R$, $m \in \mathcal{M}$.

Proposition 3.2 *Let R be a ring with property(T) and let $K = R/\mathcal{M}$. If*

$$dim_K(\mathcal{M}/ann(\mathcal{M})) = s, \text{ then } dim_K(\mathcal{M}^2) \leq s^2.$$

Proof We prove this for the case where $\sigma_i = id_{R_o}$, for all $i = 1, ..., h$. The general case follows from this.

Let $\bar{x}_1, \ldots, \bar{x}_s$ be a fixed K-basis for $\mathcal{M}/ann(\mathcal{M})$. Let $c \in \mathcal{M}^2$. Then

$$c = \sum_{k=1}^{t} a_k b_k; \quad a_k, \ b_k \in \mathcal{M},$$

for some integer $t \geq 1$. But

$$a_k = \sum_{i=1}^{s} \lambda_{ik} x_i + \lambda_k, \quad b_k = \sum_{j=1}^{s} \mu_{jk} x_j + \mu_k; \quad \lambda_{ik}, \ \mu_{jk} \in K; \quad \lambda_k, \ \mu_k \in ann(\mathcal{M}).$$

Hence,

$$\begin{aligned} c &= \sum_{k=1}^{t} \Big(\sum_{i,j=1}^{s} \lambda_{ik} \mu_{jk} x_i x_j \Big) \\ &= \sum_{i,j=1}^{s} \Big(\sum_{k=1}^{t} \lambda_{ik} \mu_{jk} \Big) x_i x_j; \text{where } \sum_{k=1}^{t} \lambda_{ik} \mu_{jk} \in K. \end{aligned}$$

Therefore, the products $x_i x_j$ $(i, \ j = 1, \ \ldots, \ s)$ generate $\mathcal{M}^2$ over K. Hence, $dim_K(\mathcal{M}^2)$ is atmost s^2.

Corollary 3.3 *If $dim_K(\mathcal{M}/ann(\mathcal{M})) = 1$, then $dim_K(\mathcal{M}^2) = 1$.*

4 Rings of characteristic p

Let R be a ring with property(T) and characteristic p. In this case, K_o is a field F of order p^r and by choice of b, every element of R may be written uniquely

as $\alpha_o + m$ with $\alpha_o \in F$, $m \in \mathcal{M}$ (see 1.8), and therefore any element of R may be written uniquely as

$$\alpha_o + \sum_{i=1}^{h} \alpha_i m_i \quad (\alpha_o,\ \alpha_i \in F).$$

Note that since $\mathcal{M}^3 = (0)$ and $\mathcal{M}^2 \subseteq ann(\mathcal{M})$ with $\mathcal{M}^2 \neq (0)$, we can write

$$\{m_1, \ldots, m_h\} = \{x_1, \ldots, x_s, y_1, \ldots, y_\lambda, z_1, \ldots, z_t\}$$

where $x_1, \ldots, x_s \in \mathcal{M} - ann(\mathcal{M})$, $y_1, \ldots, y_\lambda \in ann(\mathcal{M}) - \mathcal{M}^2$, and $z_1, \ldots, z_t \in \mathcal{M}^2$. Accordingly, we write

$$\{\sigma_1, \ldots, \sigma_h\} = \{\sigma_1, \ldots, \sigma_s, \tau_1, \ldots, \tau_\lambda, \theta_1, \ldots, \theta_t\},$$

where $s + t + \lambda = h$, and by Proposition 3.2, $1 \leq t \leq s^2$, and $\lambda \geq 0$ Therefore any element of R may be written uniquely as

$$\alpha_o + \sum_{i=1}^{s} \alpha_i x_i + \sum_{\mu=1}^{\lambda} \beta_\mu y_\mu + \sum_{k=1}^{t} \gamma_k z_k \quad (\alpha_o,\ \alpha_i,\ \beta_\mu,\ \gamma_k \in F).$$

Now consider the products $x_i x_j$, where x_i, x_j are the elements of $\mathcal{M}$ given above. Clearly, $x_i x_j \in \mathcal{M}^2$. Therefore,

$$x_i x_j = \sum_{k=1}^{t} a_{ij}^k z_k, \text{ where } a_{ij}^k \in F. \tag{1}$$

But $z_k \in \mathcal{M}^2$ is of the form

$$z_k = \sum_{\nu} a_\nu b_\nu, \quad a_\nu,\ b_\nu \in \mathcal{M};\ \nu \geq 1.$$

But

$$a_\nu = \sum_{i=1}^{s} \beta_{i\nu} x_i + y', \quad b_\nu = \sum_{j=1}^{s} \gamma_{j\nu} x_j + y'', \quad \beta_{i\nu},\ \gamma_{j\nu} \in F,\ \ y',\ y'' \in ann(\mathcal{M}).$$

Hence,

$$z_k = \sum_{i,j=1}^{s} (\sum_{\nu} \beta_{i\nu} \gamma_{j\nu}^{\sigma_i}) x_i x_j; \text{ where } \sum_{\nu} \beta_{i\nu} \gamma_{j\nu}^{\sigma_i} \in F.$$

Since z_k $(k = 1, \ldots, t)$ is a basis for $\mathcal{M}^2$ over F, therefore $x_i x_j$ $(i,\ j = 1, \ldots, s)$ generate $\mathcal{M}^2$. Therefore, the coefficients in (1) form a matrix

$$\mathcal{A} = \begin{pmatrix} a_{11}^1 & a_{11}^2 & \cdots & a_{11}^t \\ a_{12}^1 & a_{12}^2 & \cdots & a_{12}^t \\ \vdots & \vdots & \vdots & \vdots \\ a_{ss}^1 & a_{ss}^2 & \cdots & a_{ss}^t \end{pmatrix}$$

of row rank t. In particular, the matrices (a_{ij}^k) $(k = 1, \ldots, t)$, which are the t columns of the above coefficient matrix, are linearly independent over F. Moreover, since for every $l \in \{1, \ldots, s\}$, $x_l \notin ann(\mathcal{M})$, it follows that there exists a $j \in \{1, \ldots, s\}$ such that $x_l x_j \neq 0$ or $x_j x_l \neq 0$. Or equivalently, for every $l \in \{1, \ldots, s\}$, there exists a $k \in \{1, \ldots, t\}$ and a $j \in \{1, \ldots, s\}$ such that $a_{lj}^k \neq 0$ or $a_{jl}^k \neq 0$.

Definition A set of $s \times s$ matrices $(a_{ij}^1), \ldots, (a_{ij}^t)$ with entries in F are *compatible* if

(i) they are linearly independent over F; and

(ii) they are such that for every $l \in \{1, \ldots, s\}$, there exists a $k \in \{1, \ldots, t\}$ and a $j \in \{1, \ldots, s\}$ such that $a_{lj}^k \neq 0$ or $a_{jl}^k \neq 0$.

We next consider the automorphisms σ_i, θ_k; $(i = 1, \ldots, s;\ k = 1, \ldots, t)$. By using the associativity of R which requires that

$$(x_i x_j)b = x_i(x_j b), \quad 1 \leq i, j \leq s;$$

we have

$$\begin{aligned} \sum_{k=1}^{t} a_{ij}^k b^{\theta_k} z_k &= (b^{\sigma_j})^{\sigma_i} x_i x_j \\ &= b^{\sigma_i \sigma_j} \sum_{k=1}^{t} a_{ij}^k z_k. \end{aligned}$$

Hence,

$$\sum_{k=1}^{t} a_{ij}^k [b^{\theta_k} - b^{\sigma_i \sigma_j}] z_k = 0.$$

But z_k $(k = 1, \ldots, t)$, are linearly independent over F, so that

$$a_{ij}^k [b^{\theta_k} - b^{\sigma_i \sigma_j}] = 0,$$

for all $k = 1, \ldots, t$. Hence, $a_{ij}^k = 0$ or $b^{\theta_k} = b^{\sigma_i \sigma_j}$. If $a_{ij}^k \neq 0$, then $b^{\theta_k} = b^{\sigma_i \sigma_j}$ and since b is a primitive element of F, $\theta_k = \sigma_i \sigma_j$. Since the columns of matrix

$\mathcal{A}$ are linearly independent, they are, in particular, non-zero and so for every $k = 1, \ldots, t$ there exist an $a_{ij}^k \neq 0$ and hence $\theta_k = \sigma_i\sigma_j$. So the σ_i's determine the θ_k's.

Therefore the multiplication in R is now given by

$$(\alpha_o + \sum_{i=1}^{s} \alpha_i x_i + \sum_{\mu=1}^{\lambda} \beta_\mu y_\mu + \sum_{k=1}^{t} \gamma_k z_k) \cdot (\alpha_o' + \sum_{i=1}^{s} \alpha_i' x_i + \sum_{\mu=1}^{\lambda} \beta_\mu' y_\mu + \sum_{k=1}^{t} \gamma_k' z_k)$$

$$= \alpha_o\alpha_o' + \sum_{i=1}^{s} [\alpha_o\alpha_i' + \alpha_i(\alpha_o')^{\sigma_i}]x_i + \sum_{\mu=1}^{\lambda} [\alpha_o\beta_\mu' + \beta_\mu(\alpha_o')^{\tau_\mu}]y_\mu + \sum_{k=1}^{t} [\alpha_o\gamma_k' +$$

$$\gamma_k(\alpha_o')^{\theta_k} + \sum_{i,j=1}^{s} a_{ij}^k \alpha_i(\alpha_j')^{\sigma_i}]z_k.$$

Thus, up to isomorphism, the ring R is given by t compatible matrices $A_k = (a_{ij}^k)$ of size $s \times s$, and by automorphisms σ_i, τ_μ $(i = 1, \ldots, s;\ \mu = 1, \ldots, \lambda)$.

We shall call the compatible matrices A_k the *structural matrices* of the ring R, and if A_k is a singleton with element a, we shall call a the *structural constant* of R.

We can now give the following:

CONSTRUCTION A

Let F be the Galois field $GF(p^r)$. For some integers s, t, λ with $1 \leq t \leq s^2$, $\lambda \geq 0$, let U, V, W be s, λ, t -dimensional F-spaces, respectively. Since F is commutative we can think of them as both left and right vector spaces. Let (a_{ij}^k) be t compatible matrices of size $s \times s$ with entries in F, $\{\sigma_1, \ldots, \sigma_s\}$, $\{\tau_1, \ldots, \tau_\lambda\}$, $\{\theta_1, \ldots, \theta_t\}$ be sets of automorphisms of F (with possible repetitions) and let $\{\sigma_i\}$ and $\{\theta_k\}$ satisfy the additional condition that if $a_{ij}^k \neq 0$, for any k with $1 \leq k \leq t$, then $\theta_k = \sigma_i\sigma_j$.

Consider the additive group direct sum

$$R = F \oplus U \oplus V \oplus W;$$

select bases $\{u_i\}$, $\{v_\mu\}$ and $\{w_k\}$ for U, V and W, respectively, and define a multiplication on R by

$$(\alpha_o, \sum_i \alpha_i u_i, \sum_\mu \beta_\mu v_\mu, \sum_k \gamma_k w_k) \cdot (\alpha_o', \sum_i \alpha_i' u_i, \sum_\mu \beta_\mu' v_\mu, \sum_k \gamma_k' w_k)$$

$$= \Big(\alpha_o\alpha_o', \sum_i [\alpha_o\alpha_i' + \alpha_i(\alpha_o')^{\sigma_i}]u_i, \sum_\mu [\alpha_o\beta_\mu' + \beta_\mu(\alpha_o')^{\tau_\mu}]v_\mu,$$

$$\sum_k [\alpha_o\gamma_k' + \gamma_k(\alpha_o')^{\theta_k} + \sum_{i,j=1}^{s} a_{ij}^k \alpha_i(\alpha_j')^{\sigma_i}]w_k\Big).$$

Then this multiplication turns R into a ring as we see in the following theorem.

Theorem 4.1 *The ring R given by Construction A is a ring with property(T) and of characteristic p. Conversely, every such ring is isomorphic to one given by Construction A.*

Proof We first show that R is in fact a ring. We know that it is an additive abelian group and has multiplicative identity (1, 0, 0, 0), so it remains to check that the multiplication is associative and distributive over addition. The distributive properties can be seen immediately from the definition; however, the check for associativity is more elaborate but as it is elementary, it is not given here. Furthermore,

$$\begin{aligned} |R| &= |F| \cdot |U| \cdot |V| \cdot |W| \\ &= p^r \cdot p^{rs} \cdot p^{r\lambda} \cdot p^{rt} \\ &= p^{(1+s+\lambda+t)r} \\ &= p^{nr}, \text{ if we put } n = 1 + s + \lambda + t; \end{aligned}$$

and $charR = p$.

We now show that R is completely primary and satisfies property(T).

With the obvious identifications, we can think of F, U, V, W as subsets of R. Put $M = U \oplus V \oplus W$. It follows immediately from the way multiplication was

defined that $M^2 \subset W$ and that $M(V \oplus W) = (V \oplus W)M = 0$. Hence, $M^3 = (0)$. Also, from the definition of multiplication, it follows that $RM = MR \subset M$, so that M is an ideal.

Let now $\alpha \in F^*$ and $x \in M$. Since $x^m = 0$ for some $m > 0$, we have

$$(1 + x)(1 - x + x^2 - x^3 + \ldots + (-1)^{m-1}x^{m-1}) = 1$$

Thus, $1 + x$ is invertible for every $x \in M$. Then $\alpha + x = \alpha(1 + \alpha^{-1}x)$ is the product of two invertible elements, and hence is invertible.

Since $|M| = p^{r(s+\lambda+t)}$ and $|F^* + M| = (p^r - 1)(p^{r(s+\lambda+t)})$, it follows that $F^* + M = R - M$ and hence, all the elements outside M are invertible. Hence, $R/M \cong GF(p^r)$ and therefore, R is completely primary and satisfies property(T).

To prove the converse, it is sufficient to notice that the considerations before Construction A establish that all rings of characteristic p satisfying property(T) are like the ones given in Construction A.

We complete this section with a theorem concerning the case where the Galois subfield F lies in the center of the ring R with property(T) and characteristic p.

Theorem 4.2 *Let R be a ring of Construction A. Then the field F lies in the centre of R if and only if $\sigma_i = \tau_\mu = \theta_k = id_F$, for all $i = 1, \ldots, s$, $\mu = 1, \ldots, \lambda$; $k = 1, \ldots, t$.*

Proof If $\sigma_i = \tau_\mu = \theta_k = id_F$, for all $i = 1, \ldots, s$; $\mu = 1, \ldots, \lambda$; $k = 1, \ldots, t$; that F lies in the centre of R follows trivially from the multiplication defined in Construction A.

Hence, suppose F lies in the centre of R. Let $b \in F$ be primitive. Then

$$(0,\ u_i,\ v_\mu,\ w_k) \cdot (b,\ 0,\ 0,\ 0) = (b,\ 0,\ 0,\ 0) \cdot (0,\ u_i,\ v_\mu,\ w_k),$$

that is

$$(0,\ b^{\sigma_i}u_i,\ b^{\tau_\mu}v_\mu,\ b^{\theta_k}w_k) = (0,\ bu_i,\ bv_\mu,\ bw_k).$$

Therefore, $b^{\sigma_i} = b$, $b^{\tau_\mu} = b$, $b^{\theta_k} = b$, and since b is a primitive element of F, it follows that $\sigma_i = \tau_\mu = \theta_k = id_F$; for all $i = 1, \ldots, s$; $\mu = 1, \ldots, \lambda$; $k = 1, \ldots, t$.

Corollary 4.3 *Let R be a ring of Construction A. Then R is commutative if and only if $\sigma_i = \theta_k = \tau_\mu = id_F$; and $a_{ij}^k = a_{ji}^k$, for all $i, j = 1, \ldots, s$; $\mu = 1, \ldots, \lambda$; $k = 1, \ldots, t$.*

This completes the characterization of all rings with property(T) and of characteristic p.

We remark that if R is a ring with property(T), we shall call the integers p, n, r, s, t and λ, *invariants* of R.

It is clear that what we have named invariants are indeed that, that is, isomorphic rings have the same invariants. On the other hand, it is easy to find examples of non-isomorphic rings with property(T) and characteristic p with the same invariants.

5 Enumeration of rings with property(T) and characteristic p

In this section, we consider the problem of finding the number of distinct (up to isomorphism) types of rings with property(T) and of characteristic p.

Let R be a ring with property(T) and characteristic p in which the maximal Galois subfield F lies in the center. Then R is a ring of Construction A with $\sigma_i = \tau_\mu = \theta_k = id_{R_o}$, for all $i = 1, \ldots, s$; $\mu = 1, \ldots, \lambda$; $k = 1, \ldots, t$ (Theorem 4.2), so that R has a multiplication

$$(\alpha_o, \sum_i \alpha_i u_i, \sum_\mu \beta_\mu v_\mu, \sum_k \gamma_k w_k) \cdot (\alpha_o', \sum_i \alpha_i' u_i, \sum_\mu \beta_\mu' v_\mu, \sum_k \gamma_k' w_k)$$

$$= (\alpha_o\alpha_o', \sum_i [\alpha_o\alpha_i' + \alpha_i\alpha_o']u_i, \sum_\mu [\alpha_o\beta_\mu' + \beta_\mu\alpha_o']v_\mu,$$

$$\sum_k [\alpha_o \gamma_k' + \gamma_k \alpha_o' + \sum_{i,j=1}^{s} a_{ij}^k \alpha_i \alpha_j'] w_k)$$

and the only parameters left in defining R are the t compatible matrices (a_{ij}^k) of size $s \times s$ with entries in F.

Notice that since $\mathcal{M}^2 \subseteq ann(\mathcal{M})$, we can write

$$R = F \oplus U \oplus N, \text{ where } N = V \oplus W,$$

and if we denote $v_1, \ldots, v_\lambda$ by $w_{t+1}, \ldots, w_{t+\lambda}$, respectively, then the above multiplication for R becomes

$$(\alpha_o, \sum_i \alpha_i u_i, \sum_{k=1}^{t+\lambda} \gamma_k w_k) \cdot (\alpha_o', \sum_i \alpha_i' u_i, \sum_{k=1}^{t+\lambda} \gamma_k' w_k)$$

$$= (\alpha_o \alpha_o', \sum_i [\alpha_o \alpha_i' + \alpha_i \alpha_o'] u_i, \sum_k [\alpha_o \gamma_k' + \gamma_k \alpha_o' + \sum_{i,j=1}^{s} a_{ij}^k \alpha_i \alpha_j'] w_k),$$

where $a_{ij}^k = 0$, for all $k = t+1, \ldots, t+\lambda$.

It is therefore easy to see that the description of the rings of this type reduces to the case where $ann(\mathcal{M})$ coincides with $\mathcal{M}^2$. Therefore, to enumerate the rings of this type of a given order, say p^{nr}, where $ann(\mathcal{M})$ does not coincide with $\mathcal{M}^2$, we shall first write all the rings of this type of order $\leq p^{nr}$, where $ann(\mathcal{M})$ coincides with $\mathcal{M}^2$.

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

Remark Let R be the ring given by the above multiplication with respect to the compatible matrices $A_k = (a_{ij}^k) \in \mathbf{M}_s(F)$ $(k = 1, \ldots, t)$.
Let $A = \{A_k : k = 1, \ldots, t\}$, and denote the ring R by $R(A)$ or $R(\{A_k\})$. Up to isomorphism, the ring $R(A)$ is given by t compatible matrices $A_k = (a_{ij}^k)$ of size $s \times s$, and as before we call the compatible matrices A_k, the structural matrices of the ring $R(A)$. We also recall that if $|R(A)| = p^{nr}$, the integers p, n, r, s, t are invariants of $R(A)$.

Let now R' be another ring of the same type with the same invariants p, n, r, s, t; with respect to compatible matrices $D_k = (d_{ij}^k)$ over the common

maximal Galois subfield F. Denote this ring by $R(D)$, where $D = \{D_k : k = 1, \ldots, t\}$. Our problem is to determine which choices of A give distinct rings up to isomorphism. This is facilitated by the lemma below.

We take this opportunity to introduce the symbol M^σ to denote $\sigma((a_{ij}))$ if $M = (a_{ij})$.

Lemma 5.1 *With the above notation,*

$$R(A) \cong R(D)$$

if and only if there exist $\sigma \in Aut(F)$, $B = (\beta_{k\rho}) \in GL(t, F)$ *and* $C \in GL(s, F)$ *such that*

$$D_\rho = \sum_{k=1}^{t} \beta_{k\rho} C^T A_k^\sigma C.$$

Proof Suppose there is an isomorphism

$$\phi : R(A) \longrightarrow R(D).$$

Then, $\phi(F)$ is a maximal subfield of $R(D)$ so that there exists an invertible element $w \in R(D)$ such that $w\phi(F)w^{-1} = F$.

Now, consider the map

$$\begin{array}{rccc} \psi: & R(A) & \longrightarrow & R(D) \\ & r & \longmapsto & w\phi(r)w^{-1} \end{array}$$

Then, clearly, ψ is an isomorphism from $R(A)$ to $R(D)$ which sends F to itself.

Also,

$$\psi(0, \sum_i \alpha_i u_i, 0) = (0, \sum_\nu \sum_i \psi(\alpha_i)\alpha_{\nu i} u_\nu', y') \ (y' \in N');$$

and

$$\psi(0, 0, \sum_k \gamma_k w_k) = (0, 0, \sum_\rho \sum_k \psi(\gamma_k)\beta_{\rho k} w_\rho').$$

Therefore,

$$\psi(0, \sum_i \alpha_i u_i, 0) \cdot \psi(0, \sum_i \alpha_i' u_i, 0)$$

$$= \left(0,\ \sum_{\nu}\sum_{i}\psi(\alpha_i)\alpha_{\nu i}u'_{\nu},\ y'\right)\cdot\left(0,\ \sum_{\nu}\sum_{i}\psi(\alpha'_i)\alpha_{\nu i}u'_{\nu},\ y''\right)$$

$$= \left(0,\ 0,\ \sum_{\rho}\sum_{\nu,\mu=1}^{s}\sum_{i,j=1}^{s}\psi(\alpha_i)\psi(\alpha'_j)\alpha_{\nu i}\alpha_{\mu j}d^{\rho}_{\nu\mu}w'_{\rho}\right).$$

On the other hand,

$$\psi\left((0,\ \sum_{i}\alpha_i u_i,\ 0)\cdot(0,\ \sum_{i}\alpha'_i u_i,\ 0)\right) = \psi(0,\ 0,\ \sum_{k}\sum_{i,j=1}^{s}\alpha_i\alpha'_j a^k_{ij}w_k)$$

$$= (0,\ 0,\ \sum_{\rho}\sum_{k=1}^{t}\sum_{i,j=1}^{s}\psi(\alpha_i\alpha'_j)\beta_{\rho k}\psi(a^k_{ij})w'_{\rho}).$$

It follows that

$$\sum_{\nu,\mu=1}^{s}\sum_{i,j=1}^{s}\psi(\alpha_i)\psi(\alpha'_j)\alpha_{\nu i}\alpha_{\mu j}d^{\rho}_{\nu\mu} = \sum_{k=1}^{t}\sum_{i,j=1}^{s}\psi(\alpha_i\alpha'_j)\beta_{\rho k}\psi(a^k_{ij}). \qquad (2)$$

Now, $\psi|_F$ is an automorphism of F; and therefore,

$$\psi(a^k_{ij}) = \sigma(a^k_{ij}),$$

for some $\sigma \in Aut(F)$. Hence, (2) implies that

$$E^T D_\rho E = \sum_{k=1}^{t}\beta_{k\rho}A^{\sigma}_k, \text{ with } E = (\alpha_{\mu j});$$

that is,

$$D_\rho = C^T[\sum_{k=1}^{t}\beta_{k\rho}A^{\sigma}_k]C = \sum_{k=1}^{t}\beta_{k\rho}C^T A^{\sigma}_k C, \text{ where } C = E^{t-1};$$

as required.

Now, suppose there exist $\sigma \in Aut(F)$, $B = (\beta_{k\rho}) \in GL(t,\ F)$ and $C \in GL(s,\ F)$ with

$$D_\rho = \sum_{k=1}^{t}\beta_{k\rho}C^T A^{\sigma}_k C.$$

Consider the map

$$\begin{array}{rccc} \psi: & R(A) & \longrightarrow & R(D) \\ & (\alpha_o,\ \sum_i \alpha_i u_i,\ \sum_k \gamma_k w_k) & \longmapsto & (\alpha^{\sigma}_o,\ \sum_\nu \sum_i \alpha^{\sigma}_i \alpha_{\nu i}u'_{\nu},\ \sum_\rho \sum_k \gamma^{\sigma}_k \beta_{k\rho}w'_{\rho}) \end{array}$$

Then, it is easy to verify that ψ is an isomorphism of the ring $R(A)$ onto the ring $R(D)$.

As a result of this lemma, the set

$$\{R(\{\sum_{k=1}^{t}\beta_{k\rho}C^{T}A_{k}^{\sigma}C\}) : B=(\beta_{k\rho})\in GL(t,\ F),\ C\in GL(s,\ F),\ \sigma\in Aut(F)\}$$

gives all the rings of Construction A which are isomorphic to $R(\{A_k\})$.

Corollary 5.2 *Let A and D be sets of compatible matrices with entries from F. If A and D generate the same space over F, then $R(A)\cong R(D)$.*

Proof This is a direct consequence of Lemma 5.1, with $C=I_s$ and $\sigma=id_F$.

Next, we interpret Lemma 5.1 interms of bilinear forms.

Lemma 5.3 *Let U be an s-dimensional F-space with bases $(u_1,\ \ldots,\ u_s)$ and $(v_1,\ \ldots,\ v_s)$ and B a t-dimensional F-space of bilinear forms on U with bases $(f_1,\ \ldots, f_t)$ and $(g_1,\ \ldots,\ g_t)$. For each $k=1,\ \ldots,\ t$, let $A_k=(a_{ij}^k)$ and $D_k=(d_{ij}^k)$ be matrices of f_k and g_k with respect to $(u_1,\ \ldots,\ u_s)$ and $(v_1,\ \ldots,\ v_s)$, respectively. Then*

$$D_\rho=\sum_{k=1}^{t}\beta_{k\rho}C^{T}A_kC,$$

where $B=(\beta_{k\rho})$ and $C=(\alpha_{ij})$ are the transition matrices from $(f_1,\ \ldots, f_t)$ and $(u_1,\ \ldots,\ u_s)$ to $(g_1,\ \ldots,\ g_t)$ and $(v_1,\ \ldots,\ v_s)$, respectively.

Proof We have

$$v_i=\sum_{\nu=1}^{s}\alpha_{\nu i}u_\nu,\ \text{for } i=1,\ \ldots,\ s;$$

and

$$g_\rho=\sum_{k=1}^{t}\beta_{k\rho}f_k,\ \text{for } \rho=1,\ \ldots,\ t.$$

Now, by the bilinearity of f_k,

$$\begin{aligned} g_\rho(v_i,\ v_j) &= \sum_{k=1}^{t}\beta_{k\rho}f_k(v_i,\ v_j)\\ &= \sum_{k=1}^{t}\beta_{k\rho}\sum_{\nu,\mu=1}^{s}\alpha_{\nu i}\alpha_{\mu j}f_k(u_\nu,\ u_\mu); \end{aligned}$$

that is,

$$d_{ij}^{\rho} = \sum_{k=1}^{t} \beta_{k\rho} \sum_{\nu,\mu=1}^{s} \alpha_{\nu i}\alpha_{\mu j}a_{\nu\mu}^{k},$$

from which the result follows.

Definition If $(A_1, \ldots, A_t)$ and $(D_1, \ldots, D_t)$ are matrices corresponding to bases $(f_1, \ldots, f_t)$ and $(g_1, \ldots, g_t)$ of F-spaces $\mathcal{A}$ and $\mathcal{D}$ of bilinear forms on s-dimensional F-spaces U and V, respectively, then we shall say $\mathcal{D}$ is *equivalent* to $\mathcal{A}$ if there exist invertible matrices $B = (\beta_{k\rho})$ and C such that for each $\rho = 1, \ldots, t$,

$$D_{\rho} = \sum_{k=1}^{t} \beta_{k\rho} C^{T} A_k C.$$

It is readily seen that the relation of being equivalent, defined above, is an equivalence relation on spaces of bilinear forms.

Notice that the formula in Lemma 5.1 matches that in Lemma 5.3 if we take σ to be the identity automorphism on F. In particular, if the rings under consideration are constructed from prime subfields $\mathbf{F}_p$, or if the rings are commutative, then the formulae in the two Lemmata will be the same. Therefore, there is a connection between isomorphism classes of commutative rings with property(T) and characteristic p with the same invariants p, n, r, s, t; and rings with property(T) and characteristic p with prime subfields $\mathbf{F}_p$ with the same invariants p, n, s, t; and equivalence classes of t-dimensional F-spaces of bilinear forms on s-dimensional F-spaces U.

In view of the above, we have the following:

Theorem 5.4 *Two rings with property(T) and characteristic p and of same order, with maximal Galois subfield $\mathbf{F}_p$ and with same invariants p, n, s, t, are isomorphic if and only if the corresponding spaces of bilinear forms are equivalent. Also, two commutative rings with property(T) and characteristic p and of the same order with same invariants p, n, r, s, t are isomorphic if and only if the corresponding spaces of bilinear forms are equivalent.*

6 Rings with property(T) and characteristic p^ν, $\nu = 2, 3$

In this section, we describe the remaining cases of rings with property(T), namely, those of characteristic p^2 and p^3, and give their general construction in Consturction B.

6.1 Rings of characteristic p^2

Let R be a ring with property(T) and characteristic p^2. Then R contains an element b of order $p^r - 1$ such that $b + \mathcal{M}$ is a primitive element of $R/\mathcal{M}$, $\mathcal{M}$ being the unique maximal ideal of R. Let $R_o = \mathbf{Z}_{p^2}[b]$. Then R_o is a Galois subring of R of order p^{2r} and characteristic p^2 (see 1.4 and 1.8). The maximal ideal of R_o is

$$\mathcal{M}_o = pR_o = \mathcal{M} \cap R_o,$$

and

$$R_o/\mathcal{M}_o \cong GF(p^r).$$

Let ψ be the canonical map from R_o onto $R_o/\mathcal{M}_o$. Since b has order $p^r - 1$ and $\mathcal{M}_o \subset \mathcal{M}$, we have that $\psi(b)$ is a primitive element of $R_o/\mathcal{M}_o$. Then, by 1.8, every element of R_o can be written uniquely as $\lambda_o + \lambda_1 p$, where λ_o, $\lambda_1 \in K_o$.

Now, by 1.6, we know that

$$R = R_o \oplus R_o m_1 \oplus \ldots \oplus R_o m_h, \text{ where } m_i \in \mathcal{M}$$

and we know that there exist σ_1, ..., $\sigma_h \in Aut(R_o)$ such that $m_i r = r^{\sigma_i} m_i$, for all $r \in R_o$, and for all $m_i \in \mathcal{M}$. Clearly,

$$\mathcal{M} = pR_o \oplus R_o m_1 \oplus \ldots \oplus R_o m_h.$$

Since $\mathcal{M}^3 = (0)$ and $\mathcal{M}^2 \subseteq ann(\mathcal{M})$, with $\mathcal{M}^2 \neq (0)$, we can write

$$\{m_1, \ldots, m_h\} = \{x_1, \ldots, x_s, y_1, \ldots, y_\lambda, z_1, \ldots, z_t\}$$

where, $x_1, \ldots, x_s \in \mathcal{M} - ann(\mathcal{M})$, $y_1, \ldots, y_\lambda \in ann(\mathcal{M}) - \mathcal{M}^2$ and $z_1, \ldots, z_t \in \mathcal{M}^2$. Accordingly, we write

$$\{\sigma_1, \ldots, \sigma_h\} = \{\sigma_1, \ldots, \sigma_s, \tau_1, \ldots, \tau_\lambda, \theta_1, \ldots, \theta_k\},$$

where $s + \lambda + t = h$.

In view of the above considerations and by 1.8, since $pm = 0$, for all $m \in ann(\mathcal{M})$, we have either

(i) $p \in \mathcal{M}^2$;

(ii) $p \in ann(\mathcal{M}) - \mathcal{M}^2$; or

(iii) $p \in \mathcal{M} - ann(\mathcal{M})$.

We consider these cases separately.

Case (i). $p \in \mathcal{M}^2$.

In this case, $1 \leq 1 + t \leq s^2$; $\lambda \geq 0$, by Proposition 3.2. Hence, every element of R may be written uniquely as

$$\lambda_o + \lambda_1 p + \sum_{i=1}^{s} \alpha_i x_i + \sum_{\mu=1}^{\lambda} \beta_\mu y_\mu + \sum_{k=1}^{t} \gamma_k z_k; \quad \lambda_o,\ \lambda_1,\ \alpha_i,\ \beta_\mu,\ \gamma_k \in K_o.$$

Clearly, $x_i x_j \in \mathcal{M}^2$. Therefore,

$$x_i x_j \quad = \quad a_{ij}^o p + \sum_{k=1}^{t} a_{ij}^k z_k, \text{ where } a_{ij}^o,\ a_{ij}^k \in R_o/pR_o \tag{3}$$

Now, since $p,\ z_k \in \mathcal{M}^2$ $(k = 1,\ \ldots,\ t)$, we can write them as sums of products of elements of $\mathcal{M}$. In particular, $p,\ z_k$ can be written as linear combinations of $x_i x_j$ with coefficients in R_o/pR_o. Hence, since p , z_k $(k = 1,\ \ldots,\ t)$ form a basis for $\mathcal{M}^2$ over R_o/pR_o, we conclude that $x_i x_j$ $(i,\ j = 1,\ \ldots,\ s)$ generate $\mathcal{M}^2$ over R_o/pR_o. Therefore, the coefficients in (3) form a matrix

$$\mathcal{A} = \begin{pmatrix} a_{11}^o & a_{11}^1 & \cdots & a_{11}^t \\ a_{12}^o & a_{12}^1 & \cdots & a_{12}^t \\ \vdots & \vdots & \vdots & \vdots \\ a_{ss}^o & a_{ss}^1 & \cdots & a_{ss}^t \end{pmatrix}$$

of row rank $1 + t$. In particular, the matrices (a_{ij}^k) $(k = 0,\ 1,\ \ldots,\ t)$, which are the $1 + t$ columns of the above coefficient matrix, are linearly independent over R_o/pR_o. Moreover, since for every $l \in \{1,\ \ldots,\ s\}$, $x_l \notin ann(\mathcal{M})$, it follows that there exists a $j \in \{1,\ \ldots,\ s\}$ such that $x_l x_j \neq 0$ or $x_j x_l \neq 0$. Or equivalently, for every $l \in \{1,\ \ldots,\ s\}$, there exists a $k \in \{0,\ 1,\ \ldots,\ t\}$ and a $j \in \{1,\ \ldots,\ s\}$

such that $a_{lj}^k \neq 0$ or $a_{jl}^k \neq 0$. As in Section 4, the $s \times s$ matrices (a_{ij}^o), ..., (a_{ij}^t) with entries in R_o/pR_o are compatible.

Next consider the automorphisms σ_i, θ_k; $(i = 1, \ldots, s;\ k = 1, \ldots, t)$. By using the associativity of R which requires that

$$(x_i x_j)b = x_i(x_j b), \quad 1 \leq i, j \leq s;$$

we have

$$pa_{ij}^o(b + pR_o) + \sum_{k=1}^{t} a_{ij}^k (b + pR_o)^{\theta_k} z_k = (b + pR_o)^{\sigma_i \sigma_j}[pa_{ij}^o + \sum_{k=1}^{t} a_{ij}^k z_k].$$

Hence,

$$pa_{ij}^o[(b + pR_o) - (b + pR_o)^{\sigma_i \sigma_j}] = 0;$$

and

$$\sum_{k=1}^{t} a_{ij}^k [(b + pR_o)^{\theta_k} - (b + pR_o)^{\sigma_i \sigma_j}] z_k = 0.$$

But p, z_k, $(k = 1, \ldots, t)$, are linearly independent over R_o/pR_o; so that

$$a_{ij}^o[(b + pR_o) - (b + pR_o)^{\sigma_i \sigma_j}] = 0;$$

and

$$a_{ij}^k[(b + pR_o)^{\theta_k} - (b + pR_o)^{\sigma_i \sigma_j}] = 0, \quad \text{for all } k = 1, \ldots, t.$$

Hence,

$$a_{ij}^o = 0 \text{ or } (b + pR_o) = (b + pR_o)^{\sigma_i \sigma_j};$$

and

$$a_{ij}^k = 0 \text{ or } (b + pR_o)^{\theta_k} = (b + pR_o)^{\sigma_i \sigma_j}.$$

Suppose that $a_{ij}^o \neq 0$. Then $(b+pR_o) = (b+pR_o)^{\sigma_i \sigma_j}$. But $b+pR_o$ is a primitive element of R_o/pR_o, so that $\sigma_i \sigma_j = id_{R_o}$. Also, if $a_{ij}^k \neq 0$, then $\theta_k = \sigma_i \sigma_j$. Since the columns of matrix $\mathcal{A}$ are linearly independent, they are, in particular, non-zero and so there exist an $a_{ij}^o \neq 0$ and for every $k = 1, \ldots, t$ there exist an $a_{ij}^k \neq 0$, and hence $\sigma_i \sigma_j = id_{R_o}$ and $\theta_k = \sigma_i \sigma_j$. So the σ_i determine the θ_k.

Therefore the multiplication in R is now given by

$$(\alpha_o + \sum_{i=1}^{s} \alpha_i x_i + \sum_{\mu=1}^{\lambda} \beta_\mu y_\mu + \sum_{k=1}^{t} \gamma_k z_k) \cdot (\alpha_o' + \sum_{i=1}^{s} \alpha_i' x_i + \sum_{\mu=1}^{\lambda} \beta_\mu' y_\mu + \sum_{k=1}^{t} \gamma_k' z_k)$$

$$= \alpha_o\alpha_o' + p\sum_{i,j=1}^{s} a_{ij}^o\alpha_i(\alpha_j')^{\sigma_i} + \sum_{i=1}^{s}[(\alpha_o + pR_o)\alpha_i' + \alpha_i(\alpha_o' + pR_o)^{\sigma_i}]x_i +$$

$$\sum_{\mu=1}^{\lambda}[(\alpha_o + pR_o)\beta_\mu' + \beta_\mu(\alpha_o' + pR_o)^{\tau_\mu}]y_\mu + \sum_{k=1}^{t}[(\alpha_o + pR_o)\gamma_k' + \gamma_k(\alpha_o' + pR_o)^{\theta_k}$$

$$+ \sum_{i,j=1}^{s} a_{ij}^k\alpha_i(\alpha_j')^{\sigma_i}]z_k.$$

Thus, up to isomorphism, the ring R is given by $1 + t$ compatible matrices $A_k = (a_{ij}^k)$ of size $s \times s$, and by automorphisms σ_i, τ_μ $(i = 1, \ldots, s;\ \mu = 1, \ldots, \lambda)$ with $\sigma_i\sigma_j = id_{R_o}$ whenever $a_{ij}^k \neq 0$.

As before, we shall call the compatible matrices A_k the structural matrices of the ring R and if A_k is a singleton with element a, we shall call a the structural constant of R.

Case (ii). $p \in ann(\mathcal{M}) - \mathcal{M}^2$.

The argument is the same as in the previous case. However, in this case, the ring R is given by t compatible matrices $A_k = (a_{ij}^k)$ of size $s \times s$, and by automorphisms σ_i, θ_k, τ_μ with $\theta_k = \sigma_i\sigma_j$ whenever $a_{ij}^k \neq 0$ $(i = 1, \ldots, s;\ \mu = 1, \ldots, \lambda;\ k = 1, \ldots, t)$.

Hence, the multiplication in R is given by

$$(\alpha_o + \sum_{i=1}^{s}\alpha_i x_i + \sum_{\mu=1}^{\lambda}\beta_\mu y_\mu + \sum_{k=1}^{t}\gamma_k z_k)\cdot(\alpha_o' + \sum_{i=1}^{s}\alpha_i' x_i + \sum_{\mu=1}^{\lambda}\beta_\mu' y_\mu + \sum_{k=1}^{t}\gamma_k' z_k)$$

$$= \alpha_o\alpha_o' + \sum_{i=1}^{s}[(\alpha_o + pR_o)\alpha_i' + \alpha_i(\alpha_o' + pR_o)^{\sigma_i}]x_i + \sum_{\mu=1}^{\lambda}[(\alpha_o + pR_o)\beta_\mu'$$

$$+\beta_\mu(\alpha_o' + pR_o)^{\tau_\mu}]y_\mu + \sum_{k=1}^{t}[(\alpha_o + pR_o)\gamma_k' + \gamma_k(\alpha_o' + pR_o)^{\theta_k} + \sum_{i,j=1}^{s} a_{ij}^k\alpha_i(\alpha_j')^{\sigma_i}]z_k.$$

Case (iii). $p \in \mathcal{M} - ann(\mathcal{M})$.

Suppose that $d \geq 0$ is the number of the elements px_i which are not zero, where $x_1, \ldots x_s \in \mathcal{M} - ann(\mathcal{M})$. Suppose, without loss of generality, that

$px_1, \ldots, px_d$ are the d non-zero elements. Then, by Proposition 3.2, we have $1 \leq d+t \leq (1+s)^2$; $\lambda \geq 0$. Hence, every element of R may be written uniquely as

$$\lambda_o+\lambda_1 p+\sum_{i=1}^{s}\alpha_i x_i+\sum_{l=1}^{d}\xi_l px_l+\sum_{\mu=1}^{\lambda}\beta_\mu y_\mu+\sum_{k=1}^{t}\gamma_k z_k;\ \lambda_o, \lambda_1, \alpha_i, \xi_l, \beta_\mu, \gamma_k \in K_o.$$

Clearly, the products $x_i x_j \in \mathcal{M}^2$. Hence,

$$x_i x_j = \sum_{l=1}^{d} a_{ij}^{l} px_l + \sum_{k=1}^{t} a_{ij}^{k+d} z_k, \text{ where } a_{ij}^{l}, a_{ij}^{k+d} \in R_o/pR_o. \tag{4}$$

Now, since $px_l, z_k \in \mathcal{M}^2$ $(l = 1, \ldots, d;\ k = 1, \ldots, t)$, we can write them as sums of products of elements of $\mathcal{M}$. In particular, px_l, z_k can be written as linear combinations of px_i and $x_i x_j$ with coefficients in R_o/pR_o. Hence, since px_l , z_k $(l = 1, \ldots, d;\ k = 1, \ldots, t)$ is a basis for $\mathcal{M}^2$ over R_o/pR_o, we conclude that px_i and $x_i x_j$ $(i, j = 1, \ldots, s)$ generate $\mathcal{M}^2$. Therefore, the coefficients in (4) form a matrix

$$\mathcal{A} = \begin{pmatrix} a_{11}^{1} & \cdots & a_{11}^{d} & a_{11}^{d+1} & \cdots & a_{11}^{d+t} \\ a_{12}^{1} & \cdots & a_{12}^{d} & a_{12}^{d+1} & \cdots & a_{12}^{d+t} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{ss}^{1} & \cdots & a_{ss}^{d} & a_{ss}^{d+1} & \cdots & a_{ss}^{d+t} \end{pmatrix}$$

of row rank $d+t$. In particular, the matrices (a_{ij}^{l}) and (a_{ij}^{k+d}) $(l = 1, \ldots, d;\ k = 1, \ldots, t)$, which are the $d + t$ columns of the above coefficient matrix, are linearly independent over R_o/pR_o. Moreover, since for every $h \in \{1, \ldots, s\}$, $x_h \notin ann(\mathcal{M})$, it follows that there exists a $j \in \{1, \ldots, s\}$ such that $x_h x_j \neq 0$ or $x_j x_h \neq 0$. Or equivalently, for every $h \in \{1, \ldots, s\}$, there exists a $\kappa \in \{1, \ldots, t + d\}$ and a $j \in \{1, \ldots, s\}$ such that $a_{hj}^{\kappa} \neq 0$ or $a_{jh}^{\kappa} \neq 0$. As in the previous cases, the $s \times s$ matrices (a_{ij}^{1}), $\ldots$, (a_{ij}^{t+d}) with entries in R_o/pR_o are compatible.

We next consider the automorphisms σ_i, θ_k; $(i = 1, \ldots, s;\ k = 1, \ldots, t)$. By using the associativity of R which requires that

$$(x_i x_j)b = x_i(x_j b), \quad 1 \leq i, j \leq s;$$

it is easy to show that for every $l = 1, \ldots, d$ there exist an $a_{ij}^{l} \neq 0$ and for every

$k = 1, \ldots, t$ there exist an $a_{ij}^{k+d} \neq 0$, and hence $\sigma_l = \sigma_i\sigma_j$ and $\theta_k = \sigma_i\sigma_j$. In particular the σ_i determine the θ_k.

Therefore, the multiplication in R is now given in a suitable manner as in the previous cases with obvious notation. Thus, the compatible matrices $(a_{ij}^1), \ldots, (a_{ij}^{t+d})$, and the automorphisms σ_i, τ_μ determine completely the multiplicative structure of R.

6.2 Rings of characteristic p^3

In this case, let $R_o = \mathbf{Z}_{p^3}[b]$. Then, the argument is similar to that given in the case where $charR = p^2$. However, in this case, $p \in \mathcal{M} - ann(\mathcal{M})$ and $p^2 \in \mathcal{M}^2$ and thus, if $a_{ij}^o \neq 0$, then $\sigma_i\sigma_j = id_{R_o}$; if $a_{ij}^l \neq 0$, with $l = 1, \ldots, d$, then $\sigma_l = \sigma_i\sigma_j$ and if $a_{ij}^{k+d} \neq 0$, with $k = 1, \ldots, t$ then $\theta_k = \sigma_i\sigma_j$.

We can now give the following:

CONSTRUCTION B

Let R_o be the Galois ring $GR(p^{2r}, p^2)$ or $GR(p^{3r}, p^3)$. Let s, d, t, λ be integers with either $1 \leq t \leq s^2$, $1 \leq 1 + t \leq s^2$ or $1 \leq d + t \leq s^2$ if $charR_o = p^2$ or $1 \leq 1 + d + t \leq (1 + s^2)$ if $charR_o = p^3$, and $\lambda \geq 0$. Let V, W be R_o/pR_o-spaces which when considered as R_o-modules have generating sets $\{v_1, \ldots, v_\lambda\}$ and $\{w_1, \ldots, w_t\}$, respectively. 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), for $l = 0, 1, \ldots, t, 1 + t$ or $d + t$, be $s \times s$ compatible matrices with entries in R_o/pR_o if $charR_o = p^2$ or $l = 0, 1, \ldots, d + t$ be $(1 + s) \times (1 + s)$ compatible matrices with entries in R_o/pR_o if $charR_o = p^3$. Let $\{\sigma_1, \ldots, \sigma_s\}$, $\{\tau_1, \ldots, \tau_\lambda\}$, $\{\theta_1, \ldots, \theta_t\}$ be sets of automorphisms of R_o (with possible repetitions) and let $\{\sigma_i\}$, $\{\theta_k\}$ satisfy the additional conditions that

(i) if $a_{ij}^o \neq 0$, then $\sigma_i\sigma_j = id_{R_o}$;

(ii) if $a_{ij}^h \neq 0$, for any h with $h = 1, \ldots, d$, then $\sigma_i\sigma_j = \sigma_h$; and

(ii) if $a_{ij}^{d+k} \neq 0$, for any k with $k = 1, \ldots, t$, then $\theta_k = \sigma_i\sigma_j$.

Consider the additive group direct sum

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

and define a multiplication on R by

$$(\alpha_o, \sum_i \alpha_i u_i, \sum_\mu \beta_\mu v_\mu, \sum_k \gamma_k w_k) \cdot (\alpha_o', \sum_i \alpha_i' u_i, \sum_\mu \beta_\mu' v_\mu, \sum_k \gamma_k' w_k)$$

$$= \Bigg(\alpha_o \alpha_o' + p^f \sum_{i,j=1}^{s} a_{ij}^o [\alpha_i (\alpha_j')^{\sigma_i} + pR_o] ,$$

$$\sum_{i=1}^{s} [\alpha_o \alpha_i' + \alpha_i (\alpha_o')^{\sigma_i} + p \sum_{\nu,\mu=1}^{s} a_{\nu\mu}^i [\alpha_\nu (\alpha_\mu')^{\sigma_i} + pR_o]] u_i ,$$

$$\sum_\mu [(\alpha_o + pR_o)\beta_\mu' + \beta_\mu (\alpha_o' + pR_o)^{\tau_\mu}] v_\mu ,$$

$$\sum_k [(\alpha_o + pR_o)\gamma_k' + \gamma_k (\alpha_o' + pR_o)^{\theta_k} + \sum_{i,j=1}^{s} a_{ij}^{d+k} [\alpha_i (\alpha_j')^{\sigma_i} + pR_o]] w_k \Bigg) ,$$

where $f = 1$ or 2, depending on whether $char R_o = p^2$ or p^3.

Then this multiplication turns R into a ring as we see in the following theorem.

Theorem 6.1 *The ring R given by Construction B is a ring with property(T) and of characteristic p^2 or p^3. Conversely, any ring with property(T) and of characteristic p^2 or p^3, is isomorphic to one given by Construction B.*

Proof We give the proof for the case of rings of characteristic p^3. The other case will then follow by simple modifications.

First we show that R is in fact a ring. We know that it is an additive abelian group and has multiplicative identity (1, 0, 0, 0) where $1 \in R_o$; so it remains to check that the multiplication is associative and distributive over addition. The distributive properties can be seen immediately from the definition; however, the check for associativity is more elaborate but as it is almost elementary, it is not given here. Furthermore,

$$|R| = |R_o| \cdot |U| \cdot |V| \cdot |W|$$

$$= p^{3r} \cdot p^{r\sum_{i=1}^{s} t_i} \cdot p^{\lambda r} \cdot p^{tr}$$
$$= p^{(3+\sum_{i=1}^{s} t_i+\lambda+t)r}$$
$$= p^{nr}, \text{ if we put } n = 3 + \sum_{i=1}^{s} t_i + \lambda + t;$$

(where p^{t_i} is the additive order of u_i), and $charR = p^3$.

We show that R is completely primary and satisfies property(T). With the obvious identifications, we can think of R_o, U, V, and W as subsets of R. Put $M = pR_o \oplus U \oplus V \oplus W$. It follows immediately from the way multiplication was defined that $M^2 \subset p^2R_o + pU + W$ and that

$$M(p^2R_o + pU + V + W) = (p^2R_o + pU + V + W)M = (0).$$

Hence, $M^3 = (0)$. Also, from the definition of multiplication it follows that $RM = MR \subset M$, so that M is an ideal.

Next, let $r_o \in R_o$ with $r_o \notin pR_o$ and let $x \in M$. As in the proof of Theorem 4.1, it is easy to check that $r_o + x$ is invertible.

Since $|M| = p^{(2+\sum_{i=1}^{s} t_i+\lambda+t)r}$ and

$$|(R_o/pR_o)^+ + M| = (p^r - 1)(p^{(2+\sum_{i=1}^{s} t_i+\lambda+t)r})$$

it follows that $K_o + M = R - M$ and hence, all the elements outside M are invertible. Therefore, R is completely primary and satisfies property(T).

Now, let R be a ring with property(T) and characteristic p^3. To show that R is a ring of Construction B, it is sufficient to notice that the considerations before Construction B establish that all the rings of characteristic p^3 satisfying property(T) are like the ones given in Construction B.

Remark As in the previous case, if R is a ring with property(T) and characteristic p^2 or p^3, we shall call the integers p, n, r, d, s, t and λ, *invariants* of R. We remark that p can be any prime; n, r, s can be any positive integers and d, λ can be any integers ≥ 0, while t is subject to the condition that either $1 \leq t \leq s^2$, $1 \leq 1 + t \leq s^2$ or $1 \leq d + t \leq s^2$ if $charR = p^2$; and that p can be

any prime; n, r can be any arbitrary positive integers and s, d, λ can be any integers ≥ 0, while t is subject only to the condition that $1 \leq 1+d+t \leq (1+s)^2$ if $charR = p^3$.

We complete this section with a theorem concerning the case where the Galois subring R_o lies in the center of a ring R with property(T) and characteristic p^2 or p^3.

Theorem 6.2 *Let R be a ring of Construction B. Then the Galois ring R_o lies in the centre of R if and only if $\sigma_i = \tau_\mu = \theta_k = id_{R_o}$, for all i, μ and k.*

Proof This can be proved in a similar manner to Theorem 4.2.

Corollary 6.3 *Let R be a ring of Construction B. Then R is commutative if and only if $\sigma_i = \tau_\mu = \theta_k = id_{R_o}$, and $a_{ij}^h = a_{ji}^h$, for all i, μ, k and h.*

7 Enumeration of Rings with property(T) and of characteristic p^ν, $\nu = 2, 3$

In this section, we consider the problem of finding isomorphism classes of rings with property(T) and characteristics p^2 and p^3. In particular, we consider the case where the maximal Galois subring R_o lies in the centre of R, so that R is a ring of Construction B, with $\sigma_i = \tau_\mu = id_{R_o}$, and hence, $\theta_k = id_{R_o}$ for all i, μ, k (Theorem 6.2).

7.1 Rings of characteristic p^2

In Section 6, we saw that there are three types of rings with property(T) and characteristic p^2, namely, those in which
(i) $p \in \mathcal{M}^2$;
(ii) $p \in ann(\mathcal{M}) - \mathcal{M}^2$; and
(iii) $p \in \mathcal{M} - ann(\mathcal{M})$.

It is clear from the considerations in Section 6 that these rings have great similarities and to avoid repetition, we opted to treat them under one construc-

tion. However, to avoid considerable loss of clarity, we have opted to treat them separately in this section.

We start with the following:

Case (i). The case where p is in $\mathcal{M}^2$

We know that all the rings of this type are rings of Construction B, and so if R is such a ring, the only parameters left in defining R are the $s \times s$ compatible matrices $A_l = (a_{ij}^l)$ over R_o/pR_o, for $l = 0, 1, \ldots, t$.

Since $\mathcal{M}^2 \subseteq ann(\mathcal{M})$, we can write

$$R = R_o \oplus U \oplus N, \text{ where } N = V \oplus W,$$

and if we denote $v_1, \ldots, v_\lambda$ by $w_{t+1}, \ldots, w_{t+\lambda}$, respectively, then the above multiplication for R in Construction B becomes

$$\left(\alpha_o, \sum_i \alpha_i u_i, \sum_{k=1}^{t+\lambda} \gamma_k w_k\right) \cdot \left(\alpha_o', \sum_i \alpha_i' u_i, \sum_{k=1}^{t+\lambda} \gamma_k' w_k\right)$$

$$= \left(\alpha_o\alpha_o' + p\sum_{i,j=1}^{s} a_{ij}^o[(\alpha_i\alpha_j') + pR_o], \quad \sum_{i=1}^{s}[(\alpha_o + pR_o)\alpha_i' + \alpha_i(\alpha_o' + pR_o)]u_i,\right.$$

$$\left.\sum_k[(\alpha_o + pR_o)\gamma_k' + \gamma_k(\alpha_o' + pR_o) + \sum_{i,j=1}^{s} a_{ij}^k[(\alpha_i\alpha_j') + pR_o]]v_k\right),$$

where $a_{ij}^k = 0$, for all $k = t+1, \ldots, t+\lambda$.

It is therefore easy to see that the description of rings of this type reduces to the case where $ann(\mathcal{M})$ coincides with $\mathcal{M}^2$. Therefore, as before, to enumerate rings of this type of a given order, say p^{nr}, where $ann(\mathcal{M})$ does not coincide with $\mathcal{M}^2$, we shall first write all the rings of this type of order $\leq p^{nr}$, where $ann(\mathcal{M})$ coincides with $\mathcal{M}^2$.

As before, we assume that $\lambda = 0$, in what follows.

Let A be the set consisting of the compatible matrices $A_o, \ldots, A_t$ and denote the ring with the above multiplication by $R(A)$ or $R(\{A_k\})$. Let $R(D)$ be

another ring of the same type with the same invariants p, n, r, s, t, where D is the set consisting of the structural matrices for the ring $R(D)$. We assume that $R(A)$ and $R(D)$ are constructed from a common maximal Galois subring R_o. Our problem is to determine which choices of A give distinct rings up to isomorphism. This is facilitated by the following lemma.

Lemma 7.1 *Let $R(A)$ and $R(D)$ be rings with property(T) and of characteristic p^2 in which R_o lies in the centre, with the same invariants p, n, r, s, t, and in which p lies in $\mathcal{M}^2$. Then $R(A) \cong R(D)$ if and only if there exist $\sigma \in Aut(R_o)$, $B = (\beta_{k\rho}) \in GL(1+t,\ R_o/pR_o)$ and $C \in GL(s,\ R_o/pR_o)$, such that*

$$D_\rho = \sum_{k=0}^{t} \beta_{k\rho} C^T A_k^\sigma C.$$

Proof Similar to that for Lemma 5.1.

As a result of this lemma, the set of all rings

$$R\left(\{\sum_{k=0}^{t} \beta_{k\rho} C^T A_k^\sigma C\}\right)$$

where

$$B = (\beta_{k\rho}) \in GL(1+t,\ R_o/pR_o),\ C \in GL(s,\ R_o/pR_o),\ \sigma \in Aut(R_o)$$

gives all the rings of Construction B in which p lies in $\mathcal{M}^2$ isomorphic to $R(\{A_k\})$.

Case (ii). The case where p lies in $ann(\mathcal{M}) - \mathcal{M}^2$

Notice that, in Case (i), we assumed that $p \in \mathcal{M}^2$. However, if now $p \in ann(\mathcal{M})$ while $p \notin \mathcal{M}^2$, the discussion is virtually the same as that given above only that in this case the matrix $B = (\beta_{k\rho})$ will be in $GL(t,\ R_o/pR_o)$. Therefore, we have the following:

Lemma 7.2 *Let $R(A)$ and $R(D)$ be rings with property(T) and of characteristic p^2 in which R_o lies in the centre, with the same invariants p, n, r, s, t, and in which p lies in $ann(\mathcal{M}) - \mathcal{M}^2$. Then $R(A) \cong R(D)$ if and only if there exist $\sigma \in Aut(R_o)$, $B = (\beta_{k\rho}) \in GL(t,\ R_o/pR_o)$ and $C \in GL(s,\ R_o/pR_o)$, such that*

$$D_\rho = \sum_{k=1}^{t} \beta_{k\rho} C^T A_k^\sigma C.$$

As a result of this lemma, the set of all rings

$$R\left(\{\sum_{k=1}^{t}\beta_{k\rho}C^{T}A_{k}^{\sigma}C\}\right)$$

where

$$B=(\beta_{k\rho})\in GL(t,\ R_o/pR_o),\ C\in GL(s,\ R_o/pR_o),\ \sigma\in Aut(R_o)$$

gives all the rings of Construction B in which p lies in $ann(\mathcal{M})-\mathcal{M}^2$ isomorphic to $R(\{A_k\})$.

Case(iii). **The case where p lies in $\mathcal{M}-ann(\mathcal{M})$**

The discussion is the same as in the previous two cases only that in this case $B=(\beta_{k\rho})\in GL(d+t,\ R_o/pR_o)$ and hence,we have the following lemma.

Lemma 7.3 *Let $R(A)$ and $R(D)$ be rings with property(T) and characteristic p^2 in which R_o lies in the centre, with the same invariants p, n, r, s, d, t and in which p does not lie in $ann(\mathcal{M})$. Then $R(A)\cong R(D)$ if and only if there exists a $\sigma\in Aut(R_o)$, $B=(\beta_{k\rho})\in GL(d+t,\ R_o/pR_o)$, $C\in GL(s,\ R_o/pR_o)$, such that*

$$D_\rho=\sum_{k=1}^{d+t}\beta_{k\rho}C^{T}A_{k}^{\sigma}C.$$

Thus, as a result of this lemma, the set of all rings

$$R\left(\{\sum_{k=1}^{t+d}\beta_{k\rho}C^{T}A_{k}^{\sigma}C\}\right)$$

where

$$B=(\beta_{k\rho})\in GL(t+d,\ R_o/pR_o),\ C\in GL(s,\ R_o/pR_o),\ \sigma\in Aut(R_o)$$

gives all the rings of Construction B in which p does not lie in $ann(\mathcal{M})$ isomorphic to $R(\{A_k\})$.

7.2 Rings of characteristic p^3

In this case, R is a ring of Construction B with $\sigma_i=\tau_\mu=id_{R_o}$, and hence, $\theta_k=id_{R_o}$ for all i, μ, k (Theorem 6.2). The following lemma gives a formula to

show when two rings of this type and with the same invariants are isomorphic.

Lemma 7.4 *Let $R(A)$ and $R(D)$ be rings with property(T) and of characteristic p^3 in which R_o lies in the centre, with the same invariants p, n, r, s, d, t. Then $R(A) \cong R(D)$ if and only if there exists a $\sigma \in Aut R_o$, $B = (\beta_{\rho k}) \in GL(1+d+t,\ R_o/pR_o)$, $C \in GL(s,\ R_o/pR_o)$, such that*

$$D_\rho = \sum_{k=0}^{d+t} \beta_{\rho k} C^T A_k^\sigma C, \quad \text{where } M^\sigma \text{ means } (\sigma(a_{ij})),\ \text{if } M = (a_{ij}).$$

Proof Suppose there is an isomorphism

$$\phi : R(A) \longrightarrow R(D).$$

Then, $\phi(R_o)$ is a maximal Galois subring of $R(D)$ so that there exists an invertible element $w \in R(D)$ such that $w\phi(R_o)w^{-1} = R_o$.

Now, consider the map

$$\begin{array}{rccc} \psi : & R(A) & \longrightarrow & R(D) \\ & r & \longmapsto & w\phi(r)w^{-1} \end{array}$$

Then, clearly, ψ is an isomorphism from $R(A)$ to $R(D)$ which sends R_o to itself and $\psi(p) = \alpha_{oo}p$, with $\alpha_{oo} = 1$; $\psi(p^2) = \beta_{oo}p^2$, with $\beta_{oo} = 1$.

Also,

$$\psi(0,\ u_i,\ 0) = (\alpha_{oi}p,\ \sum_{\nu=1}^{s} \alpha_{\nu i} u_\nu',\ y')\ \ (y' \in W');$$

and

$$\psi(0,\ 0,\ w_k) = (\beta_{0k}p^2,\ \sum_{l=1}^{d} \beta_{lk} p u_l',\ \sum_{\rho=1}^{t} \beta_{\rho+d,k} w_\rho').$$

Now, since $pu_j \in \mathcal{M}^2$, for all $j = 1,\ \ldots, d$;

$$\begin{aligned} \psi(pu_j) &= \beta_{oj}p^2 + \sum_{\nu=1}^{d} \beta_{\nu j} p u_\nu' + \sum_{\eta=1}^{t} \beta_{\eta+d,j} w_\eta' \\ &= p\psi(u_j) \\ &= p[\alpha_{oj}p + \sum_{\nu=1}^{s} \alpha_{\nu j} u_\nu' + y''] \\ &= \alpha_{oj}p^2 + \sum_{\nu=1}^{d} \alpha_{\nu j} p u_\nu', \end{aligned}$$

which implies that $\alpha_{oj} = \beta_{oj}$; $\alpha_{\nu j} = \beta_{\nu j}$; for all $\nu = 1, \ldots, d$; and $\beta_{\eta+d,j} = 0$, for all $\eta = 1, \ldots, t$.

Therefore,

$$\psi(0, u_i, 0) \cdot \psi(0, u_j, 0) = (\alpha_{oi}p, \sum_{\nu} \alpha_{\nu i} u_{\nu}', y') \cdot (\alpha_{oj}p, \sum_{\mu} \alpha_{\mu j} u_{\mu}', y'')$$

$$= \left(\sum_{\nu,\mu=0}^{s} \alpha_{\nu i}\alpha_{\mu j} d_{\nu\mu}^{o} p^2, \sum_{l=1}^{d} \sum_{\nu,\mu=0}^{s} \alpha_{\nu i}\alpha_{\mu j} d_{\nu\mu}^{l} p u_l', \sum_{h=1}^{t} \sum_{\nu,\mu=1}^{s} \alpha_{\nu i}\alpha_{\mu j} c_{\nu\mu}^{h+d} w_h' \right).$$

On the other hand,

$$\psi(\ (0, u_i, 0) \cdot (0, u_j, 0)\ ) = \psi(a_{ij}^{o}p^2, \sum_{l=1}^{d} a_{ij}^{l} p u_l, \sum_{h=1}^{t} a_{ij}^{h+d} w_h)$$

$$= (\ \psi(a_{ij}^{o})p^2 + \sum_{l=1}^{d} \beta_{ol}\psi(a_{ij}^{l})p^2 + \sum_{h=1}^{t} \beta_{o,d+h}\psi(a_{ij}^{h+d})p^2,$$

$$\sum_{\tau=1}^{d}\sum_{l=1}^{d} \psi(a_{ij}^{l})\beta_{\tau l} p u_{\tau}' + \sum_{\tau=1}^{d}\sum_{h=1}^{t} \psi(a_{ij}^{h+d})\beta_{\tau,h+d} p u_{\tau}',$$

$$\sum_{k=1}^{t}\sum_{l=1}^{d} \psi(a_{ij}^{l})\beta_{kl} w_k' + \sum_{k=1}^{t}\sum_{h=1}^{t} \beta_{d+k,d+h}\psi(a_{ij}^{d+h}) w_k'\ ).$$

Hence,

$$\sum_{\nu,\mu=0}^{s} \alpha_{\nu i}\alpha_{\mu j} d_{\nu\mu}^{\rho} = \sum_{k=0}^{d+t} \psi(a_{ij}^{k})\beta_{k\rho};\ \rho = 0, 1, \ldots, d+t;$$

But this implies that

$$E^T D_\rho E = \sum_{k=0}^{d+t} \beta_{k\rho} A_k^{\psi};$$

that is,

$$D_\rho = C^T [\sum_{k=0}^{d+t} \beta_{k\rho} A_k^{\psi}] C,\quad C = E^{-1};$$

or

$$D_\rho = \sum_{k=0}^{d+t} \beta_{k\rho} C^T A_k^{\psi} C.$$

Now, $\psi|_{R_o/pR_o}$ is an automorphism of R_o/pR_o. But $Aut(R_o/pR_o) \cong Aut(R_o)$ (see 1.3). Hence, $\psi|_{R_o/pR_o}$ is an automorphism σ of R_o, and therefore $A_k^{\psi} = A_k^{\sigma}$, with $\sigma \in Aut(R_o)$.

Conversely, suppose there exist $C \in GL(s,\ R_o/pR_o)$, $B = (\beta_{k\rho}) \in GL(1 + d + t,\ R_o/pR_o)$ and $\sigma \in Aut(R_o)$ with

$$D_\rho = \sum_{k=0}^{d+t} \beta_{\rho k} C^T A_k^\psi C.$$

Consider the map

$$\begin{array}{rccc} \psi: & R(A) & \longrightarrow & R(D) \\ & (\alpha_o,\ \sum_i \alpha_i u_i,\ \sum_k \gamma_k w_k) & \longmapsto & (\alpha_o^\sigma + \sum_i \alpha_i^\sigma \alpha_{oi} p + \sum_k \gamma_k^\sigma \beta_{ok} p^2, \\ & & & \sum_\nu \sum_i \alpha_i^\sigma \alpha_{\nu i} u_\nu^{'} + \sum_l \sum_k \gamma_k^\sigma \beta_{lk} p u_l^{'}, \\ & & & \sum_\rho \sum_k \gamma_k^\sigma \beta_{d+\rho,d+k} w_\rho^{'}) \end{array}$$

Then, it is route to check that ψ is an isomorphism of the ring $R(A)$ onto the ring $R(D)$.

As a result of this lemma, the set of all rings

$$R\left(\{\sum_{k=0}^{t+d} \beta_{k\rho} C^T A_k^\sigma C\}\right)$$

where

$$B = (\beta_{k\rho}) \in GL(1 + d + t,\ R_o/pR_o),\ C \in GL(s,\ R_o/pR_o),\ \sigma \in Aut(R_o)$$

gives all the rings of Construction B isomorphic to $R(\{A_k\})$.

We have thus formulated the isomorphism problem and it remains to obtain unique representatives of the isomorphism classes.

ACKNOWLEDGMENTS

The author would like to thank the referee for his suggestions and Professors A.O. Morris and D. Theo for their comments and advice.

REFERENCES

[1] **Y. A. Al-Khamees**, Finite completely primary rings, Ph.D. Thesis, University of Reading(1977).

[2] **G. L. C. Bond**, On the automorphism groups of finite completely primary rings, Ph.D. Thesis, University of Reading (1978).

[3] **W. E. Clark**, A coefficient ring for finite non-commutative rings, Proc. Amer. Math. Soc. 33, No.1 (1972), p.25 - 28.

[4] **W. E. Clark & D. A. Drake**, Finite chain rings, Abhandlungen, Math. Sem. Uni. Hamburg 39(1973), p.147 - 153.

[5] **W. E. Clark & J. J. Liang**, Enumeration of finite commutative chain rings, J. Algebra, 27(1973), p.445 - 453.

[6] **B. Corbas**, Rings with few zero divisors, Math. Ann. 181(1969),p.1 -7.

[7] **B. Corbas**, Finite rings in which the product of any two zero divisors is zero, Archiv der Math. XXI(1970), p.466 - 469.

[8] **G. J. Janusz**, Separable algebras over commutative rings, Trans. Amer. Math. Soc. 122(1966), p.461 - 479.

[9] **R. Raghavendran**, Finite associative rings, Compositio Math. 21, Fasc. 2(1969), p.195 - 229.

[10] **R. S. Wilson**, On the structure of finite rings, Compositio Math., Vol. 26, Fasc. 1(1973), p.79 - 93.

[11] **R. S. Wilson**, On the structure of finite rings II, Pacific J. Math. Vol. 51, No.1 (1974), p.317 - 325.

[12] **R. S. Wilson**, Representations of finite rings, Pacific J. Math. Vol. 53, No.2 (1974), p. 643 - 649.

[13] **B. R. Wirt**, Finite non-commutative local rings, Ph.D. Thesis, University of Oklahoma (1972).

[14] **C. J. Chikunji**, Enumeration of finite rings with Jacobson radical of cube zero, (*in preparation*).

Received: October 1997

Revised: July 1998