COLLOQUIUM MATHEMATICUM

VOL. 111 2008 NO. 1

AUTOMORPHISMS OF COMPLETELY PRIMARY FINITE RINGS OF CHARACTERISTIC p

BY

CHITENG'A JOHN CHIKUNJI (Gaborone)

Abstract. A completely primary ring is a ring R with identity $1 \neq 0$ whose subset of zero-divisors forms the unique maximal ideal $\mathcal{J}$. We determine the structure of the group of automorphisms $\mathrm{Aut}(R)$ of a completely primary finite ring R of characteristic p, such that if $\mathcal{J}$ is the Jacobson radical of R, then $\mathcal{J}^3 = (0)$, $\mathcal{J}^2 \neq (0)$, the annihilator of $\mathcal{J}$ coincides with $\mathcal{J}^2$ and $R/\mathcal{J} \cong \mathrm{GF}(p^r)$, the finite field of p^r elements, for any prime p and any positive integer r.

1. Introduction. A ring R is *completely primary* if the subset $\mathcal{J}$ of all its zero-divisors forms an ideal. These rings have been studied extensively by, among others, Raghavendran [5]. It has long been recognized that the group of automorphisms of a ring provides valuable information about the structure of the ring. For instance, Évariste Galois initiated the study of the group of automorphisms of a field, which was later applied by N. H. Abel to prove the celebrated theorem on the insolvability of the general quintic polynomial by radicals. It is known (see, e.g., [5]) that the group of automorphisms of the Galois ring $R_0 = \mathrm{GR}(p^{nr}, p^n)$ is isomorphic to the group of automorphisms of its residue field R_0/pR_0, and is thus a cyclic group of order r. In [1], Alkhamees determined the group of automorphisms of a completely primary finite ring R in which the product of any two zero divisors is zero. This was done for both characteristics of the ring R (i.e. $\operatorname{char} R = p$ and p^2), and for both commutative and non-commutative cases.

In this paper, we seek an explicit description of the group of automorphisms of a completely primary finite ring R of characteristic p, with Jacobson radical $\mathcal{J}$ such that $\mathcal{J}^3 = (0)$, $\mathcal{J}^2 \neq (0)$, the annihilator of $\mathcal{J}$ coincides with $\mathcal{J}^2$ and $R/\mathcal{J} \cong \mathrm{GF}(p^r)$, the finite field of p^r elements, for any prime p and any positive integer r. We leave the consideration of the cases when the characteristic of R is p^2 and p^3 for future work. These rings were studied by the author who gave their constructions for all characteristics; for details of

2000 *Mathematics Subject Classification*: Primary 16P10, 20B25; Secondary 16L99, 12E20.

Key words and phrases: completely primary finite rings, automorphism group, finite field.

the general background, the reader is referred to [2] and [3]. In this paper, these rings are given in terms of the basis of their additive groups and the multiplication tables of basis elements. We use standard notation and terminology; $\mathrm{ann}(\mathcal{J})$ denotes the two-sided annihilator of $\mathcal{J}$, and for any two groups G and H, $G \times_\theta H$ denotes the semidirect product of G by H, where $\theta : H \to \mathrm{Aut}(G)$ is a group homomorphism.

Throughout, we will assume that all rings are finite, associative (but generally not commutative) with identities, denoted by 1, that ring homomorphisms preserve 1, a ring and its subrings have the same 1 and that modules are unital. We freely use the definitions and notations introduced in [2], [3] and [5].

Let R be a completely primary finite ring. The following results will be assumed (see [5]): $|R| = p^{nr}$, $\mathcal{J}$ is the Jacobson radical of R, $\mathcal{J}^n = (0)$, $|\mathcal{J}| = p^{(n-1)r}$, $R/\mathcal{J} \cong \mathrm{GF}(p^r)$, and $\mathrm{char}\, R = p^k$, where $1 \le k \le n$, for some prime p and positive integers $n,\ k,\ r$; the group of units G_R is a semidirect product $G_R = (1 + \mathcal{J}) \times_\theta \langle b \rangle$ of its normal subgroup $1 + \mathcal{J}$ of order $p^{(n-1)r}$ by a cyclic subgroup $\langle b \rangle$ of order $p^r - 1$. If $n = k$, it is known that, up to isomorphism, there is precisely one completely primary ring of order p^{rk} having characteristic p^k and residue field $\mathrm{GF}(p^r)$. It is called the *Galois ring* $\mathrm{GR}(p^{rk}, p^k)$ and a concrete model is the quotient $\mathbb{Z}_{p^k}[X]/(f)$, where f is a monic polynomial of degree r, irreducible modulo p. Any such polynomial will do: the rings are all isomorphic. Trivial cases are $\mathrm{GR}(p^n, p^n) = \mathbb{Z}_{p^n}$ and $\mathrm{GR}(p^n, p) = \mathbb{F}_{p^n}$. In fact, $R = \mathbb{Z}_{p^n}[b]$, where b is an element of R of multiplicative order $p^r - 1$; furthermore, $\mathcal{J} = pR$ and $\mathrm{Aut}(R) \cong \mathrm{Aut}(R/pR)$ (see Proposition 2 in [5]).

Let R be a completely primary ring, $|R/\mathcal{J}| = p^r$ and $\mathrm{char}\, R = p^k$. Then it can be deduced from [4] that R has a coefficient subring R_0 of the form $\mathrm{GR}(p^{kr}, p^k)$, which is clearly a maximal Galois subring of R. Moreover, if R_0' is another coefficient subring of R then there exists an invertible element x in R such that $R_0' = xR_0x^{-1}$ (see Theorem 8 in [5]). Furthermore, there exist $m_1, \dots, m_h \in \mathcal{J}$ and $\sigma_1, \dots, \sigma_h \in \mathrm{Aut}(R_0)$ such that $R = R_0 \oplus \sum_{i=1}^h R_0 m_i$ (as R_0-modules), and $m_i r_0 = r_0^{\sigma_i} m_i$ for all $r_0 \in R_0$ and any $i = 1, \dots, h$ (use the decomposition of $R_0 \otimes_{\mathbb{Z}} R_0$ in terms of $\mathrm{Aut}(R_0)$ and apply the fact that R is a module over $R_0 \otimes_{\mathbb{Z}} R_0$). Moreover, $\sigma_1, \dots, \sigma_h$ are uniquely determined by R and R_0. We call σ_i the automorphism *associated* with m_i and $\sigma_1, \dots, \sigma_h$ the *associated* automorphisms of R with respect to R_0.

2. Cube radical zero completely primary finite rings. We now assume that R is a completely primary finite ring with Jacobson radical $\mathcal{J}$ such that $\mathcal{J}^3 = (0)$ and $\mathcal{J}^2 \ne (0)$. These rings were studied by the author in [2] and [3]. Since R is such that $\mathcal{J}^3 = (0)$, by one of the above results $\mathrm{char}\, R$ is either $p,\ p^2$ or p^3. The ring R contains a coefficient subring R_0

with $\operatorname{char} R_0 = \operatorname{char} R$, and with R_0/pR_0 equal to $R/\mathcal{J}$. Moreover, R_0 is a Galois ring of the form $\mathrm{GR}(p^{kr}, p^k)$, $k = 1,\ 2$ or 3. Let $\operatorname{ann}(\mathcal{J})$ denote the two-sided annihilator of $\mathcal{J}$ in R. Of course $\operatorname{ann}(\mathcal{J})$ is an ideal of R. Because $\mathcal{J}^3 = (0)$, it follows easily that $\mathcal{J}^2 \subseteq \operatorname{ann}(J)$.

We know from the above results that $R = R_0 \oplus \sum_{i=1}^{h} R_0 m_i$, where $m_i \in \mathcal{J}$, and that there exist automorphisms $\sigma_i \in \operatorname{Aut}(R_0)$ $(i = 1, \ldots, h)$ such that $m_i r_0 = r_0^{\sigma_i} m_i$ for all $r_0 \in R_0$ and for all $i = 1, \ldots, h$; and the number h and the automorphisms $\sigma_1, \ldots, \sigma_h$ are uniquely determined by R and R_0. Again, because $\mathcal{J}^3 = (0)$, we have $p^2 m_i = 0$ for all $m_i \in \mathcal{J}$. Further, $pm_i = 0$ for all $m_i \in \operatorname{ann}(\mathcal{J})$. In particular, $pm_i = 0$ for all $m_i \in \mathcal{J}^2$.

2.1. *Rings of characteristic p.* Let $\mathbb{F}$ be the Galois field $\mathrm{GF}(p^r)$. Given two positive integers s, t such that $1 \leq t \leq s^2$, fix s, t-dimensional $\mathbb{F}$-spaces U, V, respectively. Since $\mathbb{F}$ is commutative we can think of them as both left and right vector spaces. Let $(a_{ij}^k) \in \mathbb{M}_{s\times s}(\mathbb{F})$ be t linearly independent matrices, $\{\sigma_1, \ldots, \sigma_s\}$, $\{\theta_1, \ldots, \theta_t\}$ be sets of automorphisms of $\mathbb{F}$ (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 $\theta_k = \sigma_i \sigma_j$.

In the additive group $R = \mathbb{F} \oplus U \oplus V$, we select bases $\{u_i\}$ and $\{v_k\}$ for U and V, respectively, and we define multiplication by the following relations:

$$
\begin{aligned}
&u_i u_j = \sum_{k=1}^{t} a_{ij}^k v_k, \qquad u_i v_k = v_k u_i = u_i u_j u_l = 0, \\
&u_i \alpha = \alpha^{\sigma_i} u_i, \quad v_k \alpha = \alpha^{\theta_k} v_k \quad (1 \leq i, j, l \leq s,\ 1 \leq k \leq t),
\end{aligned}
\tag{1}
$$

where $\alpha, a_{ij}^k \in \mathbb{F}$.

By the above relations, R is a completely primary finite ring of characteristic p with Jacobson radical $\mathcal{J} = U \oplus V$, $\mathcal{J}^2 = V$ and $\mathcal{J}^3 = (0)$ (see [2] and/or [3]). We call the numbers $p,\ n,\ r,\ s,\ t$ *invariants* of the ring R.

Throughout, we need the following result proved in [3, Theorem 4.1]:

THEOREM 2.1. *Let R be a ring. Then R is a cube radical zero completely primary finite ring of characteristic* p *in which the annihilator of $\mathcal{J}$ coincides with $\mathcal{J}^2$ if and only if R is isomorphic to one of the rings given by the above relations.*

3. The group of automorphisms. To determine this group, we first show that the Galois subfield $\mathbb{F} = \mathrm{GF}(p^r)$ and the $\mathbb{F}$-space $V \cong \mathcal{J}^2$ generated by $\{v_1, \ldots, v_k\}$ are invariant under any automorphism $\phi \in \operatorname{Aut}(R)$. Then we compute the image of the rest of the generators under a fixed element of $\operatorname{Aut}(R)$. Let U and V be the $\mathbb{F}$-vector spaces generated by $\{u_1, \ldots, u_s\}$ and $\{v_1, \ldots, v_t\}$, respectively. By (1), the set $\{u_1, \ldots, u_s\}$ is an $\mathbb{F}$-basis of the vector space $\mathcal{J}/\mathcal{J}^2 \cong U$ and the set $\{u_i u_j : 1 \leq i, j \leq s\}$ generates the vector space V over $\mathbb{F}$.

LEMMA 3.1. *Let $\phi \in \mathrm{Aut}(R)$. Then $\phi(\mathbb{F})$ is a maximal subfield of R which is equal to $\mathbb{F}$ and $\phi(V) = V$, where $V \cong \mathcal{J}^2$.*

Proof. It is obvious that $\phi(\mathbb{F})$ is a maximal subfield of R so that there exists an invertible element $x \in R$ such that $x\phi(\mathbb{F})x^{-1} = \mathbb{F}$. Now, consider the map $\psi : R \to R$ given by $r \mapsto x\phi(r)x^{-1}$. Then, clearly, ψ is an automorphism of R which sends $\mathbb{F}$ to itself.

On the other hand, for any $v \in V$, we have $\phi(v) \in V$ because $[\phi(v)]^2 = \phi(v^2) = 0$, and the result follows. ■

3.1. *Preliminary results.* Let R be the ring given by the multiplication in (1) with respect to the linearly independent matrices $A_k = (a_{ij}^k) \in \mathbb{M}_{s\times s}(\mathbb{F})$ $(k = 1, \ldots, t)$ and associated automorphisms $\{\sigma_i\}$ and $\{\theta_k\}$. Then

$$R = \mathbb{F} \oplus \sum_{i=1}^{s} \mathbb{F}u_i \oplus \sum_{k=1}^{t} \mathbb{F}v_k,$$

and $u_i r_0 = r_0^{\sigma_i} u_i$, $v_k r_0 = r_0^{\theta_k} v_k$ for every $r_0 \in \mathbb{F}$.

Let $B = \{u_1, \ldots, u_s, v_1, \ldots, v_t\}$ and let $\tau \in \mathrm{Aut}(\mathbb{F})$. Put $B_\tau = \{w \in B : wb = b^\tau w\}$, where b is an element of $\mathbb{F}$ of order $p^r - 1$, and let $\mathcal{J}_\tau = \sum_{w\in B_\tau}^{\oplus} \mathbb{F}w$. Then, obviously, $\mathcal{J}_\tau$ is an $\mathbb{F}$-submodule of $\mathcal{J}$.

LEMMA 3.2. *Let R be a ring of Theorem* 2.1 *with maximal ideal $\mathcal{J}$. Then $\mathcal{J} = \sum_{\tau\in\mathrm{Aut}(\mathbb{F})}^{\oplus} \mathcal{J}_\tau$ as $\mathbb{F}$-modules.*

Let R be a ring of Theorem 2.1 and let us reindex the associated automorphisms in such a way that $\sigma_1, \ldots, \sigma_r$ are distinct, so that $\theta_1, \ldots, \theta_h$ are distinct as well. Let $\mathcal{J} = U \oplus V$. Obviously,

$$\mathcal{J} = \sum_{i=1}^{s} \mathbb{F}u_i \oplus \sum_{k=1}^{t} \mathbb{F}v_k,$$

where $U = \oplus\sum_{i=1}^{s} \mathbb{F}u_i$ and $V = \oplus\sum_{k=1}^{t} \mathbb{F}v_k$. Now, if $\varphi \in \mathrm{End}_{\mathbb{F}}(\mathcal{J})$, then $\varphi(m) = ma$ $(m \in \mathcal{J}, a \in \mathbb{F})$ and $\mathcal{J}_i = \sum_{\sigma_j=\sigma_i}^{\oplus} \mathbb{F}u_j \oplus \sum_{\theta_l=\sigma_i}^{\oplus} \mathbb{F}v_l$, where σ_j is the automorphism associated with u_i $(i = 1, \ldots, s)$, and $\mathcal{J}_k^2 = \sum_{\theta_m=\theta_k}^{\oplus} \mathbb{F}v_m$, where θ_m is the automorphism associated with v_k and $1 \le k \le r$. It is easy to see that $\mathcal{J}_1, \ldots, \mathcal{J}_r, \mathcal{J}_k^2$ $(1 \le k \le r)$ are the eigenspaces of φ.

Let γ be the number of non-trivial associated automorphisms σ_j of R taken with their multiplicities and $\mathcal{J}_\gamma = \sum_{\sigma_j\ne\mathrm{id}_{\mathbb{F}}}^{\oplus} \mathbb{F}e_j$, and let δ be the number of non-trivial associated automorphisms θ_k of R taken with their multiplicities and $\mathcal{J}_\delta^2 = \sum_{\theta_k\ne\mathrm{id}_{\mathbb{F}}}^{\oplus} \mathbb{F}f_k$. Clearly, $\mathcal{J}_\gamma$ and $\mathcal{J}_\delta^2$ are $\mathbb{F}$-vector spaces of dimensions γ and δ, respectively. Let $\mathcal{J}_\lambda = \sum_{\sigma_j=\mathrm{id}_{\mathbb{F}}}^{\oplus} \mathbb{F}e_j$ and $\mathcal{J}_\mu^2 = \sum_{\theta_k=\mathrm{id}_{\mathbb{F}}}^{\oplus} \mathbb{F}f_k$; then $\mathcal{J}_\lambda = \mathcal{J}_i$ for some $i \in \{1, \ldots, r\}$ or $\mathcal{J}_\lambda = \{0\}$ according as one or none of the associated automorphisms of R is trivial; and

$\mathcal{J}_\mu^2 = \mathcal{J}_k^2$ for some k with $1 \le k \le r$ or $\mathcal{J}_\mu^2 = \{0\}$ according as one or none of the associated automorphisms of R is trivial.

If $\mathcal{J}_\lambda = \mathcal{J}_i$ for some $i \in \{1, \dots, r\}$ and $\mathcal{J}_\mu^2 = \mathcal{J}_k^2$ for some k with $1 \le k \le r$, let us assume that $\mathcal{J}_\lambda = \mathcal{J}_r$ and $\mathcal{J}_\mu^2 = \mathcal{J}_r^2$, respectively. Hence, $\mathcal{J}_\gamma = \oplus \sum_{i=1}^h \mathcal{J}_i$, where $h = r$ or $r-1$; and $\mathcal{J}_\delta^2 = \oplus \sum_{k=1}^l \mathcal{J}_k^2$, where $1 \le l \le r$ or $1 \le l \le r-1$. Clearly, we may assume $\mathcal{J} = \sum_{i=1}^s \mathbb{F} \oplus \sum_{k=1}^t \mathbb{F}$, also $s = \sum_{i=1}^r s_i$ and $t = \sum_{i=1}^r t_k$, where $s_i = \dim_{\mathbb{F}}(\mathcal{J}_i)$ and $t_k = \dim_{\mathbb{F}}(\mathcal{J}_k^2)$.

PROPOSITION 3.3. *Let R be a ring of Theorem* 2.1. *Then $F \oplus \sum_{i=1}^s \mathbb{F}u_i' \oplus \sum_{k=1}^t \mathbb{F}v_k' = R$ if and only if for all $i = 1, \dots, s$ and $k = 1, \dots, t$, $u_i' = e_i + \sum b_{li} v_l$, and $v_k' = f_k$, where $\{e_1, \dots, e_s\}$ is a union of $\mathbb{F}$-bases for $\mathcal{J}_1, \dots, \mathcal{J}_r$ and b_{li} is an element of $\mathbb{F}$ which is zero if u_i' is not in the centre, $Z(R)$, of R, and where $\{f_1, \dots, f_t\}$ is a union of $\mathbb{F}$-bases for $\mathcal{J}_1^2, \dots, \mathcal{J}_k^2$ $(1 \le k \le r)$.*

Proof. Suppose that $R = \mathbb{F} \oplus \sum_{i=1}^s \mathbb{F}u_i' \oplus \sum_{k=1}^t \mathbb{F}v_k'$ and $u_i' r = r^{\sigma_i} u_i'$, $v_k' r = r^{\theta_k} v_k'$ for all $r \in \mathbb{F}$. Because $u_i' \in \mathcal{J} = \sum_{j=1}^s \mathbb{F}u_j \oplus \sum_{l=1}^t \mathbb{F}v_l$ for any $i = 1, \dots, s$, we can write $u_i' = \sum a_{ji} u_j + \sum b_{li} v_l$, where $a_{ji}, b_{li} \in \mathbb{F}$; and because $v_k' \in \mathcal{J}^2 = \sum_{l=1}^t \mathbb{F}v_l$ for any $k = 1, \dots, t$, we can write $v_k' = \sum c_{lk} v_l$, where $c_{lk} \in \mathbb{F}$.

Now,

$$\begin{aligned}\sum a_{ji} r^{\sigma_i} u_j + \sum b_{li} r^{\sigma_i} v_l = r^{\sigma_i} u_i' = u_i' r &= \Big(\sum a_{ji} u_j + \sum b_{li} v_l\Big) r \\ &= \sum a_{ji} r^{\sigma_j} u_j + \sum b_{li} r^{\theta_l} v_l\end{aligned}$$

and

$$\sum c_{lk} r^{\theta_k} v_l = r^{\theta_k} v_k' = v_k' r = \Big(\sum c_{lk} v_l\Big) r = \sum c_{lk} r^{\theta_l} v_l.$$

From these equalities we deduce that if $\sigma_i \ne \sigma_j$ then $a_{ji} = 0$, and if $\theta_k \ne \theta_l$ then $c_{kl} = 0$. In particular, if $\sigma_i \ne \theta_l$ then $b_{li} = 0$. It is also worth noting that $\theta_k = \sigma_i \sigma_j$ because $\mathcal{J}^3 = (0)$, $\mathcal{J}^2 \ne (0)$.

Let $e_i = u_i' - \sum b_{li} v_l$ and $v_k' = f_k$. Then obviously $e_i r = r^{\sigma_i} e_i$ and $f_k r = r^{\theta_k} f_k$ for all $r \in \mathbb{F}$; that is, σ_i, θ_k are the automorphisms associated with e_i, f_k, respectively. Also, it is easy to check that $\oplus \sum_{i=1}^s \mathbb{F}e_i$ is of order p^{sr}, and $\oplus \sum_{k=1}^t \mathbb{F}f_k$ is of order p^{tr}; but clearly, $\sum_{i=1}^s \mathbb{F}e_i \oplus \sum_{k=1}^t \mathbb{F}f_k \subseteq \mathcal{J}$. Hence, $\mathcal{J} = \sum_{i=1}^s \mathbb{F}e_i \oplus \sum_{k=1}^t \mathbb{F}f_k$.

Finally, it is easy to prove that $\mathcal{J}_i = \sum_{\sigma_j = \sigma_i} \mathbb{F}e_j$ and $\mathcal{J}_k^2 = \sum \mathbb{F}f_l$, where σ_j and θ_l are the automorphisms associated with e_j and f_l, respectively, and $i = 1, \dots, r$, $1 \le k \le r$.

The converse is easy to prove. ∎

Corollary 3.4. *Let* $\phi \in \mathrm{Aut}(R)$*. Then for each* $i = 1, \dots, s$ *and each* $k = 1, \dots, t$,

$$\phi(u_i) = \sum_{\sigma_j = \sigma_i} a_{ji} u_j + \sum_{\theta_k = \sigma_i} b_{ki} v_k, \qquad \phi(v_k) = \sum_{\theta_l = \theta_k} c_{lk} v_l,$$

where $a_{ji}, b_{ki}, c_{lk} \in \mathbb{F}$*. In particular, if* $b_{ki} \neq 0$*, then* $\sigma_i = \mathrm{id}_{\mathbb{F}}$.

Proof. Since

$$u_i \in \mathcal{J} = \oplus \sum_{j=1}^{s} \mathbb{F} u_j \oplus \sum_{k=1}^{t} \mathbb{F} v_k \quad \text{for all } i = 1, \dots, s;$$

$$v_k \in \mathcal{J}^2 = \oplus \sum_{l=1}^{t} \mathbb{F} v_l \quad \text{for all } k = 1, \dots, t,$$

we can write

$$\phi(u_i) = \sum a_{ji} u_j + \sum b_{ki} v_k, \qquad \phi(v_k) = \sum c_{lk} v_l,$$

where $a_{ji}, b_{ki}, c_{lk} \in \mathbb{F}$. Now, let $r_0 \in \mathbb{F}$ be such that $u_i r_0 = r_0^{\sigma_i} u_i$ and $v_k r_0 = r_0^{\theta_k} v_k$. Then

$$\phi(u_i r_0) = \phi(r_0^{\sigma_i} u_i) = \phi(r_0^{\sigma_i})\phi(u_i) = \phi(r_0^{\sigma_i})\Big[\sum a_{ji} u_j + \sum b_{ki} v_k\Big].$$

On the other hand,

$$\begin{aligned}\phi(u_i r_0) = \phi(u_i)\phi(r_0) &= \Big[\sum a_{ji} u_j + \sum b_{ki} w_k\Big]\phi(r) \\ &= \sum a_{ji} [\phi(r_0)]^{\sigma_j} u_j + \sum b_{ki} \phi(r_0)^{\theta_k} v_k.\end{aligned}$$

Similarly

$$\phi(r_0^{\theta_k})\Big[\sum c_{lk} v_l\Big] = \sum c_{lk} [\phi(r_0)]^{\theta_l} v_l.$$

From these equalities, we deduce that if $\sigma_j \neq \sigma_i$ then $a_{ji} = 0$, and if $\theta_l \neq \theta_k$ then $c_{lk} = 0$. In particular, if $b_{ki} \neq 0$ then $\sigma_i = \mathrm{id}_{\mathbb{F}}$, since $\theta_k = \sigma_i \sigma_j$ if $a_{ij}^k \neq 0$, and $\mathrm{ann}(\mathcal{J}) = \mathcal{J}^2$. ∎

Corollary 3.5. *Let* $\phi \in \mathrm{Aut}(R)$*. If* $b_{ki} = 0$*, then* $\phi(u_i) = \sum_{\sigma_j = \sigma_i} a_{ji} u_j$ *and* $\phi(v_k) = \sum_{\theta_l = \theta_k} c_{lk} v_l$*, where* $a_{ji}, c_{lk} \in \mathbb{F}$.

3.2. *The main results.* We first establish some notation that will be useful in the rest of the paper.

Notation. Let R be a ring of Theorem 2.1. If $\sigma \in \mathrm{Aut}(\mathbb{F})$ and $x \in G_R$, the group of unit elements in R, define the mappings α_σ, ψ_x from R to R as follows:

$$\alpha_\sigma\Big(a_0 + \sum a_i u_i + \sum b_k v_k\Big) = a_0^\sigma + \sum a_i^\sigma u_i + \sum b_k^\sigma v_k,$$

$$\psi_x\Big(a_0 + \sum a_i u_i + \sum b_k v_k\Big) = x\Big(a_0 + \sum a_i u_i + \sum b_k v_k\Big)x^{-1}.$$

Also, if

$$\varphi\Big(a_0 + \sum a_i u_i + \sum b_k v_k\Big) = a_0 + \sum a_i \varphi_j(u_i) + \sum b_k \phi_l(v_k),$$

where $\varphi_j \in \mathrm{Aut}_{\mathbb{F}}(\mathcal{J}_i)$ (if $u_i \in \mathcal{J}_j$) and $j = 1, \ldots, r$, and $\phi_l \in \mathrm{Aut}_{\mathbb{F}}(\mathcal{J}_k^2)$ (if $v_k \in \mathcal{J}_l^2$) and $1 \le l \le r$, let $\varphi\sigma = \varphi\alpha_\sigma$, and if

$$\beta\Big(a_0 + \sum a_i u_i + \sum b_k v_k\Big) = a_0 + \sum a_i u_i + \sum_{\sigma_i = \mathrm{id}_{\mathbb{F}}} a_{li} a_i v_l + \sum b_k v_k,$$

where $a_{li} \in \mathbb{F}$ and σ_i is the automorphism associated with u_i, let $\beta\sigma = \beta\alpha_\sigma$. Finally, if $A = (a_{ij})$, define $A^\sigma = (a_{ij}^\sigma)$ and let A^{σ_i} denote $(\sigma_1(a_{i1}), \sigma_2(a_{i2}), \ldots, \sigma_t(a_{it}))$ for some automorphisms σ_j, not necessarily distinct.

THEOREM 3.6. *Let R be a ring of Theorem 2.1. Then $\varphi \in \mathrm{Aut}(R)$ if and only if*

$$\varphi\Big(a_0 + \sum_{i=1}^{s} a_i u_i + \sum_{k=1}^{t} b_k v_k\Big) = x a_0^\sigma x^{-1} + \sum_{i=1}^{s} x a_i^\sigma x^{-1} \varphi_j(u_i) + \sum_{\sigma_i = \mathrm{id}_{\mathbb{F}}} a_{li} x a_i^\sigma x^{-1} v_l + \sum_{k=1}^{t} x b_k^\sigma x^{-1} \phi_l(v_k),$$

where $\sigma \in \mathrm{Aut}(\mathbb{F})$, $x \in G_R$, $\varphi_j \in \mathrm{Aut}_{\mathbb{F}}(\mathcal{J}_i)$ (if $u_i \in \mathcal{J}_j$) and $j = 1, \ldots, r$, $\phi_l \in \mathrm{Aut}_{\mathbb{F}}(\mathcal{J}_k^2)$ (if $v_k \in \mathcal{J}_l^2$) and $1 \le l \le r$, $a_{li} \in \mathbb{F}$, and σ_i, θ_k are automorphisms associated with u_i, v_k, respectively, and where θ_k is a composition of the σ_i's.

Proof. Let $\varphi \in \mathrm{Aut}(R)$. Then there exists $x \in G_R$ such that $\varphi(\mathbb{F}) = x\mathbb{F}x^{-1}$, and hence $\varphi(r) = x r^\sigma x^{-1}$ for any $r \in \mathbb{F}$, for some automorphism σ of $\mathbb{F}$. Since

$$R = \varphi(\mathbb{F}) \oplus \sum \varphi(\mathbb{F})\varphi(u_i) \oplus \sum \varphi(\mathbb{F})\varphi(v_k)$$

and conjugation is an automorphism of R,

$$R = \mathbb{F} \oplus \sum \mathbb{F} x^{-1}\varphi(u_i) x \oplus \sum \mathbb{F} x^{-1}\varphi(v_k) x.$$

But $\mathcal{J}^3 = (0)$, $\mathcal{J}^2 \ne (0)$, hence $x^{-1}\varphi(u_i)x = \alpha_i \varphi(u_i)$ and $x^{-1}\varphi(v_k)x = \beta_k \varphi(v_k)$, where $\alpha_i, \beta_k \in \mathbb{F}$ for all $i = 1, \ldots, s$ and $k = 1, \ldots, t$. Thus,

$$R = \mathbb{F} \oplus \sum \mathbb{F}\alpha_i \varphi(u_i) \oplus \sum \mathbb{F}\beta_k \varphi(v_k)$$

and hence

$$R = \mathbb{F} \oplus \sum \mathbb{F}\varphi(u_i) \oplus \sum \mathbb{F}\varphi(v_k).$$

Therefore, for any $i \in \{1, \ldots, s\}$ and any $k \in \{1, \ldots, t\}$, $\varphi(u_i) = \varphi_j(u_i) + \sum a_{li} v_l$ and $\varphi(v_k) = \phi_l(v_k)$, where $\varphi_j \in \mathrm{Aut}_{\mathbb{F}}(\mathcal{J}_i)$ (if $u_i \in \mathcal{J}_j$), $\phi_l \in \mathrm{Aut}_{\mathbb{F}}(\mathcal{J}_k^2)$ (if $v_k \in \mathcal{J}_l^2$), and $a_{li} \in \mathbb{F}$, which is zero if $u_i \notin Z(R)$, the centre of R.

Conversely, let φ be as defined above. We need to check that for every $r = a_0 + \sum a_i u_i + \sum a_k v_k$,

$$\psi : a_0+\sum a_i u_i+\sum a_k v_k \mapsto a_0^\sigma+\sum a_i^\sigma \psi_j(u_i)+\sum_{\sigma_i=\mathrm{id}_{\mathbb{F}}} a_{li}a_i^\sigma v_l+\sum a_k^\sigma \eta_l(v_k),$$

is an automorphism of R, where $\psi_j(u_i) = x^{-1}\varphi_j(u_i)x$, $\eta_l(v_k) = x^{-1}\phi_l(v_k)x$. So let $s = b_0 + \sum b_i u_i + \sum b_k v_k$ be another element in R. Then

$$\psi : b_0+\sum b_i u_i+\sum b_k v_k \mapsto b_0^\sigma+\sum b_i^\sigma \psi_j(u_i)+\sum_{\sigma_i=\mathrm{id}_{\mathbb{F}}} a_{li}b_i^\sigma v_l+\sum b_k^\sigma \eta_l(v_k).$$

Now,

$$\psi(r)\psi(s) = a_0^\sigma b_0^\sigma +\sum[a_0^\sigma b_i^\sigma + a_i^\sigma (b_0^\sigma)^{\sigma_j}]\psi_j(u_i) + \sum_{\sigma_i=\mathrm{id}_{\mathbb{F}}} [a_0^\sigma a_{li} b_i^\sigma + a_{li}a_i^\sigma (b_0^\sigma)]v_l$$
$$+\sum[a_0^\sigma b_k^\sigma + a_k^\sigma (b_0^\sigma)^{\theta_l}]\eta_l(v_k) + \sum_{i=1}^{s} a_i^\sigma (b_q^\sigma)^{\sigma_j}\psi_j(u_i)\psi_q(u_i).$$

On the other hand,

$$\psi(rs) = (a_0b_0)^\sigma +\sum(a_0b_i + a_i b_0^{\sigma_j})^\sigma\psi_j(u_i) + \sum_{\sigma_i=\mathrm{id}_{\mathbb{F}}} a_{li}(a_0b_i + a_i b_0^{\sigma_j})^\sigma v_l$$
$$+\sum(a_0b_k + a_k b_0^{\theta_l})^\sigma\eta_l(v_k) + \sum_{k=1}^{t}\sum_{i,j=1}^{s}(a_i b_j^{\sigma_i} a_{ij}^k)^\sigma \eta_l(v_k).$$

From the above equalities we deduce that $\sigma_i = \sigma_j$, $\sigma_i = \mathrm{id}_{\mathbb{F}}$ if $a_{li} \neq 0$, $\theta_k = \theta_l$, and $\sum_{k=1}^{t}(a_{jq}^k)^\sigma \eta_l(v_k) = \sum_{j,q=1}^{s} \psi_j(u_i)\psi_q(u_i)$.

Now, it is obvious that $\varphi = \psi_x\psi$, and hence φ is an automorphism of R. ■

Remark 3.7. In view of Corollary 3.4, if $\phi \in \mathrm{Aut}(R)$, then $\phi|_{\mathbb{F}}$ is an automorphism $\sigma \in \mathrm{Aut}(\mathbb{F})$; if $b_{ki} = 0$, then $\phi|_U$ is an automorphism $\varphi_i \in \mathrm{Aut}_{\mathbb{F}}(U_i)$ (if $u_j \in U_i$) and $i = 1, \ldots, s$, and $\phi|_V$ is an automorphism $\phi_k \in \mathrm{Aut}_{\mathbb{F}}(V_k)$ (if $v_l \in V_k$) and $k = 1, \ldots, t$.

Remark 3.8. If $A_1, \ldots, A_t$ are linearly independent matrices over $\mathbb{F}$ and $\sigma \in \mathrm{Aut}(\mathbb{F})$, then $A_1^\sigma, \ldots, A_t^\sigma$ are also linearly independent over $\mathbb{F}$.

Remark 3.9. Let $C \in \mathrm{GL}(s, \mathbb{F})$. If $\sigma_j = \theta$ for some fixed $\theta \in \mathrm{Aut}(\mathbb{F})$, for all $j = 1, \ldots, s$, then $C^{\sigma_j} \in \mathrm{GL}(s, \mathbb{F})$.

Example 3.10. Let $C = \left(\begin{smallmatrix}\alpha & 1+\alpha\\ 1 & 1\end{smallmatrix}\right) \in \mathrm{GL}(2, \mathbb{F}_4)$ and suppose that $\sigma_1 = \mathrm{id}_{\mathbb{F}_4}$, $\sigma_2 \neq \mathrm{id}_{\mathbb{F}_4}$ are automorphisms of $\mathbb{F}_4$. Then $C^{\sigma_j} = \left(\begin{smallmatrix}\alpha & \alpha\\ 1 & 1\end{smallmatrix}\right) \notin \mathrm{GL}(2, \mathbb{F}_4)$. However, if $C^{\sigma_j} = C^\theta$, then for $\theta = \mathrm{id}_{\mathbb{F}_4}$ or $\theta \neq \mathrm{id}_{\mathbb{F}_4}$, $C^\theta \in \mathrm{GL}(2, \mathbb{F}_4)$.

Following observations from Remark 3.9 and Example 3.10, we consider determining the groups of automorphisms of the rings of the paper only in the case where σ_j is fixed for all $j = 1, \ldots, s$. Thus, the formulae in Proposition 3.11 will have fixed automorphisms in what follows.

Proposition 3.11. *Let R be a ring of Theorem* 2.1 *with structural matrices $A_k = (a_{ij}^k)$ and with invariants p, n, r, s, t. Then ϕ is an automorphism of R if and only if $\sigma_i = \theta \in \mathrm{Aut}(\mathbb{F})$ (for every $i = 1, \dots, s$) and there exist $\sigma \in \mathrm{Aut}(\mathbb{F})$, $B = (\beta_{k\varrho}) \in \mathrm{GL}(t, \mathbb{F})$ and $C \in \mathrm{GL}(s, \mathbb{F})$ such that $C^T A_\varrho C^\theta = \sum_{k=1}^t \beta_{k\varrho} A_k^\sigma$.*

Proof. Suppose there is an automorphism $\psi : R \to R$. Then $\phi(\mathbb{F})$ is a maximal subfield of R so that there exists an invertible element $x \in R$ such that $x\psi(\mathbb{F})x^{-1} = \mathbb{F}$.

Now, consider the map $\phi : R \to R$ given by $r \mapsto x\psi(r)x^{-1}$. Then, clearly, ϕ is an automorphism of R which sends $\mathbb{F}$ to itself. Also,

$$\phi\Big(\sum_i \alpha_i u_i\Big) = \sum_\nu \sum_i \phi(\alpha_i)\alpha_{\nu i} u_\nu + y \qquad (y \in V),$$

$$\phi\Big(\sum_k \gamma_k v_k\Big) = \sum_\varrho \sum_k \phi(\gamma_k)\beta_{\varrho k} v_\varrho.$$

Therefore,

$$\begin{aligned}\phi\Big(\sum_i \alpha_i u_i\Big) \cdot \phi\Big(\sum_i \alpha'_i u_i\Big) \\ &= \Big(\sum_\nu \sum_i \phi(\alpha_i)\alpha_{\nu i} u_\nu + y\Big) \cdot \Big(\sum_\nu \sum_i \phi(\alpha'_i)\alpha_{\nu i} u_\nu + y'\Big) \\ &= \sum_\varrho \sum_{\nu,\mu=1}^s \sum_{i,j=1}^s \phi(\alpha_i)\alpha_{\nu i}[\phi(\alpha'_j)\alpha_{\mu j}]^{\sigma_\nu} a_{\nu\mu}^\varrho v_\varrho.\end{aligned}$$

On the other hand,

$$\begin{aligned}\phi\Big(\Big(\sum_i \alpha_i u_i\Big) \cdot \Big(\sum_i \alpha'_i u_i\Big)\Big) &= \phi\Big(\sum_k \sum_{i,j=1}^s \alpha_i[\alpha'_j]^{\sigma_i} a_{ij}^k v_k\Big) \\ &= \sum_\varrho \sum_{k=1}^t \sum_{i,j=1}^s \phi(\alpha_i[\alpha'_j]^{\sigma_i})\beta_{\varrho k}\phi(a_{ij}^k) v_\varrho.\end{aligned}$$

It follows that

$$\sum_{\nu,\mu=1}^s \sum_{i,j=1}^s \phi(\alpha_i)\alpha_{\upsilon i}[\phi(\alpha'_j)\alpha_{\mu j}]^{\sigma_\nu} a_{\nu\mu}^\varrho = \sum_{k=1}^t \sum_{i,j=1}^s \phi(\alpha_i[\alpha'_j]^{\sigma_i})\beta_{\varrho k}\phi(a_{ij}^k).$$

Now, $\phi|_{\mathbb{F}}$ is an automorphism σ of $\mathbb{F}$, and so $\phi(a_{ij}^k) = \sigma(a_{ij}^k)$ and $\sigma_\nu = \sigma_i$. Hence, the above equation now implies that $C^T A_\varrho C^\theta = \sum_{k=1}^t \beta_{k\varrho} A_k^\sigma$ with $C = (\alpha_{\mu j})$ and $\sigma_i = \theta$ for every $i = 1, \dots, s$, as required.

Conversely, suppose that the associated automorphisms σ_i equal $\theta \in \mathrm{Aut}(R)$ for every $i = 1, \dots, s$ and there exist $\sigma \in \mathrm{Aut}(\mathbb{F})$, $B = (\beta_{k\varrho}) \in \mathrm{GL}(t, \mathbb{F})$ and $C \in \mathrm{GL}(s, \mathbb{F})$ with $C^T A_\varrho C^\theta = \sum_{k=1}^t \beta_{k\varrho} A_k^\sigma$. Consider the map

$\phi : R \to R$ given by

$$\phi\Big(\alpha_0 + \sum_i \alpha_i u_i + \sum_k \gamma_k v_k\Big) = \alpha_0^\sigma + \sum_\nu \sum_i \alpha_i^\sigma \alpha_{\nu i} u_\nu + \sum_\varrho \sum_k \gamma_k^\sigma \beta_{k\varrho} v_\varrho.$$

Then it is easy to verify that ϕ is an automorphism of the ring R. ∎

Thus, the set $\{\theta, \sigma \in \mathrm{Aut}(\mathbb{F}),\ B = (\beta_{k\varrho}) \in \mathrm{GL}(t, \mathbb{F}),\ C \in \mathrm{GL}(s, \mathbb{F})\}$ determines all the automorphisms of the ring R.

Consider the set of equations $C^T A_\varrho C^\theta = \sum_{k=1}^t \beta_{k\varrho} A_k^\sigma$ given in Proposition 3.11 with $C = (\alpha_{ij}) \in \mathrm{GL}(s, \mathbb{F})$ and for a fixed $\theta \in \mathrm{Aut}(\mathbb{F})$. Then it is easy to see that $C = (\alpha_{ij})$ is the transition matrix between the bases $(\overline{u}_i)$ of $\mathcal{J}/\mathcal{J}^2$. Also, $B = (\beta_{k\varrho})$ is the transition matrix between the bases (v_k) of $\mathcal{J}^2$. By calculating $u_\nu u_\mu$ (the images of the u_i under ϕ) and comparing coefficients of (v_ϱ) (the images of the v_k under ϕ) we obtain equations which, in matrix form, are $C^T A_\varrho C^\theta = \sum_{k=1}^t \beta_{k\varrho} A_k^\sigma$.

The problem of determining the groups of automorphisms of our rings amounts to classifying t-tuples of linearly independent matrices $(A_1, \ldots, A_t)$ under the above relation, $B,\ C$ being arbitrary invertible matrices and $\sigma,\ \theta$ being arbitrary automorphisms.

Let $\mathcal{A}$ be the set of all t-tuples $(A_1, \ldots, A_t)$ of $s \times s$ matrices over $\mathbb{F}$. The group $\mathrm{GL}(s, \mathbb{F})$ acts on $\mathcal{A}$ by "congruence":

$$(A_1, \ldots, A_t) \cdot C = (C^T A_1 C^\theta, \ldots, C^T A_t C^\theta)$$

and on the left via

$$B \cdot (A_1, \ldots, A_t) = (\beta_{11} A_1^\sigma + \cdots + \beta_{1t} A_t^\sigma, \ldots, \beta_{t1} A_1^\sigma + \cdots + \beta_{tt} A_t^\sigma),$$

where $B = (\beta_{k\varrho})$. Thus, these two actions are permutable and define a (left) action of $G = \mathrm{GL}(s, \mathbb{F}) \times \mathrm{GL}(t, \mathbb{F})$ on $\mathcal{A}$:

$$(C, B) \cdot (A_1, \ldots, A_t) = B \cdot (A_1^\sigma, \ldots, A_t^\sigma) \cdot (C^{-1})^\theta$$

for some fixed automorphisms σ and θ. By restriction, G acts on the subset Y consisting of linearly independent t-tuples $A_1, \ldots, A_t$. This amounts to studying the "congruence" action (via C) of $\mathrm{GL}(s, \mathbb{F})$ on the set $\mathcal{Y}$ of t-dimensional subspaces of $\mathbb{M}_{s\times s}(\mathbb{F})$, B just representing a change of basis in a given space. In the same way, the whole action of G on $\mathcal{A}$ may be represented as an action of $\mathrm{GL}(t, \mathbb{F})$ on the set $\mathbf{A}$ of subspaces of dimension $\leq t$. We may call two t-tuples in the same G-orbit *equivalent*.

Theorem 3.12. *Let R be a ring of Theorem* 2.1 *with invariants p, n, r, s, t. Then*

$$\mathrm{Aut}(R) \cong [\mathbb{M}_{t\times s}(\mathbb{F}) \times (U \oplus V)] \times_{\theta_2} [\mathrm{Aut}(\mathbb{F}) \times_{\theta_1} (\mathrm{GL}(s, \mathbb{F}) \times \mathrm{GL}(t,\ \mathbb{F}))].$$

Proof. Let G be the subgroup of $\mathrm{Aut}(R)$ which contains all the automorphisms φ defined by

$$\varphi\Big(r_0+\sum a_iu_i+\sum b_kv_k\Big)=r_0^\sigma+\sum a_i^\sigma\varphi_j(u_i)+\sum b_k^\sigma\phi_l(v_k),$$

where $\sigma\in\mathrm{Aut}(\mathbb{F})$, $\varphi_j\in\mathrm{Aut}_{\mathbb{F}}(U_j)$ (if $u_i\in U_j$) and $j=1,\dots,s$, and $\phi_l\in\mathrm{Aut}_{\mathbb{F}}(V_l)$ (if $v_k\in V_l$) and $l=1,\dots,t$.

Let G_0 be the subgroup of G which contains all the automorphisms α_σ such that

$$\alpha_\sigma\Big(r_0+\sum a_iu_i+\sum b_kv_k\Big)=r_0^\sigma+\sum a_i^\sigma u_i+\sum b_k^\sigma v_k,$$

where $\sigma\in\mathrm{Aut}(\mathbb{F})$. Then $G_0\cong\mathrm{Aut}(\mathbb{F})$. Let G_1 be the subgroup of G which contains all the automorphisms φ such that

$$\varphi\Big(r_0+\sum a_iu_i+\sum b_kv_k\Big)=r_0+\sum a_i\varphi_j(u_i)+\sum b_kv_k,$$

where $\varphi_j\in\mathrm{Aut}_{\mathbb{F}}(U_j)$ (if $u_i\in U_j$) and $i=1,\dots,s$; and let G_2 be the subgroup of G which contains all the automorphisms φ such that

$$\varphi\Big(r_0+\sum a_iu_i+\sum b_kv_k\Big)=r_0+\sum a_iu_i+\sum b_k\phi_l(v_k),$$

where $\phi_l\in\mathrm{Aut}_{\mathbb{F}}(V_l)$ (if $v_k\in V_l$) and $k=1,\dots,t$. Then G_1 and G_2 are subgroups of G and $G_1\times G_2$ is a direct product. Moreover, $G_1\cong\mathrm{Aut}_{\mathbb{F}}(U)\cong\mathrm{GL}(s,\mathbb{F})$ and $G_2\cong\mathrm{Aut}_{\mathbb{F}}(V)\cong\mathrm{GL}(t,\mathbb{F})$.

Finally, let H be the subgroup of $\mathrm{Aut}(R)$ containing all the automorphisms φ defined by

$$\varphi\Big(r_0+\sum a_iu_i+\sum b_kv_k\Big)=x\Big(r_0+\sum a_iu_i+\sum_{\sigma_i=\mathrm{id}_{\mathbb{F}}}\alpha_{li}a_iv_l+\sum b_kv_k\Big)x^{-1},$$

where $x\in 1+\mathcal{J}$, $a_{li}\in\mathbb{F}$ and σ_i is the automorphism associated with u_i. Let H_1 be the subgroup of H which contains all the automorphisms φ defined by

$$\varphi\Big(r_0+\sum a_iu_i+\sum b_kv_k\Big)=r_0+\sum a_iu_i+\sum_{\sigma_i=\mathrm{id}_{\mathbb{F}}}\alpha_{li}a_iv_l+\sum b_kv_k,$$

where $\alpha_{li}\in\mathbb{F}$ and σ_i is the automorphism associated with u_i, and H_2 be the subgroup of H which contains all the automorphisms φ such that

$$\varphi\Big(r_0+\sum a_iu_i+\sum b_kv_k\Big)=x\Big(r_0+\sum a_iu_i+\sum b_kv_k\Big)x^{-1},$$

where $x\in 1+\mathcal{J}\subset G_R$. Then it is easy to check that the direct product $H=H_1\times H_2$ and the semidirect product $G=(G_1\times G_2)\times_{\theta_2}G_0$ are subgroups of $\mathrm{Aut}(R)$, where if $\varphi\in G_1\times G_2$ and $\alpha_\sigma\in G_0$, then $\theta_2(\alpha_\sigma)(\varphi)=\varphi\sigma$.

Let $\varphi\in H\cap G$. Since every element of H either fixes $\mathbb{F}$ elementwise or sends $\mathbb{F}$ to another maximal Galois subring of R and $\varphi\in G$, we see that φ fixes $\mathbb{F}$ elementwise. Let $\varphi=\beta\psi_x$, where $\beta\in H_1$ and $\psi_x\in H_2$.

Since $x \in 1 + \mathcal{J}$, clearly, $\varphi = \beta\psi_x = \beta$. Since $\beta \in G$, $\beta(U) = U$. But the only element of H_1 which fixes U is the identity. Thus, $\varphi = \mathrm{id}_R$ and hence $H \cap G = \mathrm{id}_R$. Now, it is easy to see that $\mathrm{Aut}(R) = H \times_{\theta_1} G$, where if $\beta\psi_x \in H_1$ and $\varphi\alpha_\sigma \in G$, then $\theta_1(\varphi\alpha_\sigma)(\beta\psi_x) = \beta_\sigma\varphi_{\psi\alpha_\sigma}(x)$. It is trivial to check that the mapping $g : H_1 \to \mathbb{M}_{t\times s}(\mathbb{F})$ given by $g(\beta_M) = \sum_{\sigma_i=\mathrm{id}_\mathbb{F}} a_{li}u_i$, where

$$\beta_M\Big(r_0 + \sum a_iu_i + \sum b_kv_k\Big) = r_0 + \sum a_iu_i + \sum_{\sigma_i=\mathrm{id}_\mathbb{F}} a_{li}a_iu_i + \sum b_kv_k,$$

is an isomorphism, and so, combining with $f : H_2 \to U \oplus V$, we obtain an isomorphism $H \cong \mathbb{M}_{t\times s}(\mathbb{F}) \times (U \oplus V)$.

Hence,

$$\mathrm{Aut}(R) \cong [\mathbb{M}_{t\times s}(\mathbb{F}) \times (U \oplus V)] \times_{\theta_2} [\mathrm{Aut}(\mathbb{F}) \times_{\theta_1} (\mathrm{GL}(s,\mathbb{F}) \times \mathrm{GL}(t,\mathbb{F}))],$$

where

$$\theta_1(\sigma)(C,B)\cdot(A_1,\dots,A_t) = B\cdot(A_1^\sigma,\dots,A_t^\sigma)\cdot(C^{-1})^\sigma,$$
$$\theta_2(\sigma,C,B)(A_1,\dots,A_t) = (C^TA_1C^\theta,\dots,C^TA_tC^\theta). \ \blacksquare$$

COROLLARY 3.13. *Let R be a ring of Theorem* 2.1 *with invariants p, n, r, s, t. Then*

$$|\mathrm{Aut}(R)| = q^{t\times s} \times q^{s+t} \times r \times (q^s - q^{s-1})(q^s - q^{s-2})\dots(q^s - 1) \times (q^t - q^{t-1})\dots(q^t - 1).$$

COROLLARY 3.14. *Let R be a ring of Theorem* 2.1 *with invariants p, n, r, s, t. If $\mathbb{F}$ lies in the centre of R, then*

$$\mathrm{Aut}(R) \cong [\mathbb{M}_{t\times s}(\mathbb{F}) \times (U \oplus V)] \times_{\theta_2} [\mathrm{GL}(s,\mathbb{F}) \times \mathrm{GL}(t,\mathbb{F})].$$

COROLLARY 3.15. *Let R be a ring of Theorem* 2.1 *with invariants p, n, r, s, t. If every $\varphi \in \mathrm{Aut}(R)$ is such that $\varphi(\alpha) = \alpha$ for every $\alpha \in \mathbb{F}$, $\varphi(U) = U$ and $\mathbb{F}$ lies in the centre of R, then*

$$\mathrm{Aut}(R) \cong \mathrm{GL}(s,\mathbb{F}) \times \mathrm{GL}(t,\mathbb{F}).$$

REFERENCES

[1] Y. Alkhamees, *Finite rings in which the multiplication of any two zero-divisors is zero*, Arch. Math. (Basel) 37 (1981), 144–149.

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

[3] —, *A classification of cube radical zero completely primary finite rings*, Demonstratio Math. 38 (2005), 7–20.

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

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

Department of Basic Sciences
Botswana College of Agriculture
P/BAG 0027, Gaborone, Botswana
E-mail: jchikunj@bca.bw

Received 23 March 2007;
revised 23 April 2007 (4888)