International Journal of Pure and Applied Mathematics
Volume 74 No. 4 2012, 465-482
ISSN: 1311-8080 (printed version)
url: http://www.ijpam.eu
ijpam.eu

AUTOMORPHISMS OF A CERTAIN CLASS OF COMPLETELY PRIMARY FINITE RINGS

Owino Maurice Oduor
School of Mathematics and Statistics
Maseno University
P.O. Box 333, Maseno, KENYA

Abstract: Automorphisms of algebraic structures have shown much importance in mathematics. The symmetries of an algebraic structure are captured by automorphisms and very many important results have been proved by analyzing the automorphism group of the algebraic structure. In this work we determine the automorphisms of completely primary finite rings satisfying some special properties.

AMS Subject Classification: 13M05, 16P10, 16W20, 20D40, 20D45, 13E10, 13E15, 16N20
Key Words: automorphisms, completely primary finite rings

Notation

R shall denote a completely primary finite ring with identity, while R^* shall denote its corresponding group of units. Unless otherwise stated, $J(R)$ shall denote the Jacobson radical of R and $R/J(R)$ shall denote a Galois field of order p^r where p is a prime integer and r is a positive integer. $R^{'}$ shall denote the coefficient (Galois) subring of R and for each finite subset X of R, $|X|$ denotes the cardinality of X. For any element $x \in R$ we shall denote its order by $o(x)$. For any R, we shall denote its group of automorphisms by $Aut(R)$ and its characteristic by $char R$.

Received: October 31, 2011

1. Introduction

The analysis of the automorphism groups of algebraic structures has yielded well celebrated results. For instance, Evariste Galois characterized general quintic univariate polynomials f over rationals by showing that the roots of such polynomials cannot be expressed in terms of radicals, via the structure of the automorphism group of the splitting field of f. Raghavendran[9] appears to have made the deepest study into the nature of completely primary finite rings while Alkhamees[2, 3] has done considerable work on automorphisms of completely primary finite rings. The study of the automorphisms of the direct products of finite groups has been extensively done by Bidwell, Hillar among others, see e.g [4, 5, 7]. A few expositions on the automorphisms of completely finite rings can also be mentioned. For instance, Alkhamees [2] has determined the automorphisms of finite rings in which the multiplication of two zero divisors is zero. Chikunji [6] has determined the groups of automorphisms of cube radical zero completely primary finite rings. In this study we characterize the group of automorphisms of a certain class of completely primary finite rings. Our result compares perfectly well with Alkhamees' result in [2].

Let R be a completely primary finite ring with a maximal ideal $J(R)$. Then the following results due to Raghavendran [9] shall be assumed throughout this work.

i) $|R| = p^{kr}$ for some prime integer p and positive integers k and r.

ii) $J(R)$ is the Jacobson radical of R

iii) $(J(R))^m = (0)$, where $m \leq k$ and the residue field $R/J(R)$ is a finite field $GF(p^r)$ for some prime integer p and positive integer r.

iv) Char$R = p^n$ where n is a positive integer such that $n \leq m \leq k$.

Remark. If $k = n = m$, then $R = \mathbf{Z}_{p^n}[a]$ where a is an element of R of multiplicative order $p^r - 1$; $J(R) = pR$ and $\text{Aut}(R) \cong \text{Aut}(R/pR)$. Such a ring is denoted by $GR(p^{nr}, p^n)$ and is called a Galois ring. Now, $GR(p^{nr}, p^n) = \mathbf{Z}_{p^n}[y]/(g)$, where $g \in \mathbf{Z}_{p^n}[y]$ is a monic polynomial of degree r whose image in $\mathbf{Z}_p[y]$ is irreducible. The trivial cases are $GR(p^n, p^n) \cong \mathbf{Z}_{p^n}$ and $GR(p^r, p) \cong \text{GF}(p^r)$. Furthermore, every element of R' can be written uniquely as $\sum_{i=0}^{n-1} p^i \alpha_i$, where $\alpha_i \in F_0 =< a > \cup \{0\}$.

The following result due to Wirt [10] shall be useful in the sequel.

v) Let R be a completely primary finite ring with a maximal ideal $J(R)$, then R has a coefficient subring R' of the form (p^{nr}, p^n) which is a maximal Galois subring of R. Moreover, there exist $u_1, ..., u_h \in J(R)$ and $\sigma_1, ..., \sigma_h \in \text{Aut}(R')$ such that $R = R' \oplus \sum_{i=1}^{h} R' u_i$ (as R'-modules), $u_i r = r^{\sigma_i} u_i$, $\forall r \in R'$ and any $i = 1, ..., h$. Moreover, $\sigma_1, ..., \sigma_h$ are uniquely determined by R and R'. The automorphism σ_i is called the automorphism associated with u_i and $\sigma_1, ..., \sigma_h$ are the associated automorphism of R with respect to $R^{'}$.

Finally, the following result due to Raghavendran [9] shall also be assumed.

vi) Let $R^{'}$ be a Galois subring of R. If $S^{'}$ is another Galois subring of R, then there exists an invertible element $z \in R$ such that $S^{'} = zR^{'}z^{-1}$.

2. Construction and Results

Let $R^{'}$ be the Galois ring of the form $GR(p^{nr}, p^n)$. For each $i = 1, ..., h$, let $u_i \in J(R)$, such that U is an h- dimensional $R^{'}$-module generated by $\{u_1, ..., u_h\}$ so that $R = R^{'} \oplus U$ is an additive group. On this group, define multiplication by the following relations:

(i) If $n = 1, 2$, then $pu_i = u_i u_j = u_j u_i = 0, u_i r^{'} = (r^{'})^{\sigma_i} u_i$

(ii) If $n \geq 3$, then

$$p^{n-1}u_i = 0, u_i u_j = p^2\gamma_{ij}, u_i^n = u_i^{n-1}u_j = u_i u_j^{n-1} = 0, u_i r^{'} = (r^{'})^{\sigma_i} u_i,$$

where $r^{'}, \gamma_{ij} \in R^{'}$, $1 \leq i, j \leq h$, p is a prime integer, n and r are positive integers and σ_i is the automorphism associated with u_i. Further, let the generators $\{u_i\}$ for U satisfy the additional condition that if $u_i \in U$, then $pu_i = u_i u_j = 0$.

From the given multiplication in R, we see that if $r^{'} + \sum_{i=1}^{h} \lambda_i u_i$ and $s^{'} + \sum_{i=1}^{h} \gamma_i u_i$, $r^{'}, s^{'} \in R^{'}, \gamma_i, \lambda_i \in F_0$ are elements of R, then

$$(r^{'} + \sum_{i=1}^{h} \lambda_i u_i)(s^{'} + \sum_{i=1}^{h} \gamma_i u_i) = r^{'}s^{'} + \sum_{i=1}^{h} [(r^{'} + pR^{'})\gamma_i + \lambda_i (s^{'} + pR^{'})^{\sigma_i}] u_i.$$

We verify that the given multiplication turns R into a ring with identity $(1, 0, ..., 0)$.

Let $r^{'} + \sum_{i=1}^{h} \lambda_i u_i \in R, r^{'} \in R^{'}, \lambda_i \in F_0$, then we need to find $s^{'} + \sum_{i=1}^{h} \gamma_i u_i$, $s^{'} \in R^{'}, \gamma_i \in F_0$ such that

$$(r^{'} + \sum_{i=1}^{h} \lambda_i u_i)(s^{'} + \sum_{i=1}^{h} \gamma_i u_i) = (s^{'} + \sum_{i=1}^{h} \gamma_i u_i)(r^{'} + \sum_{i=1}^{h} \lambda_i u_i) = r^{'} + \sum_{i=1}^{h} \lambda_i u_i.$$

Now, if

$$r^{'}s^{'} + \sum_{i=1}^{h} [(r^{'} + pR^{'})\gamma_i + \lambda_i (s^{'} + pR^{'})^{\sigma_i}] u_i = r^{'} + \sum_{i=1}^{h} \lambda_i u_i,$$

then $r^{'}s^{'}=r^{'}$ and

$$\sum_{i=1}^{h}[(r^{'}+pR^{'})\gamma_i+\lambda_i(s^{'}+pR^{'})^{\sigma_i}]u_i=\sum_{i=1}^{h}\lambda_i u_i.$$

So $((r^{'}+pR^{'})\gamma_i)u_i=0_R$ and $s^{'}=1_{R^{'}}$ for each $i=1,...,h$. Since $u_i\neq 0$, $(r^{'}+pR^{'})\gamma_i=0_{F_0}$. But $r^{'}\in R^{'}$, so $\gamma_i=0_{F_0}$ for each $i=1,...,h$. Thus $s^{'}+\sum_{i=1}^{h}\gamma_i u_i=(1,0,...,0)$. Similarly, we can show that

$$(s^{'}+\sum_{i=1}^{h}\gamma_i u_i)(r^{'}+\sum_{i=1}^{h}\lambda_i u_i)=r^{'}+\sum_{i=1}^{h}\lambda_i u_i$$

implies $s^{'}+\sum_{i=1}^{h}\gamma_i u_i=(1,0,...,0)$.

Now, we prove that multiplication is associative.

Suppose $r^{'},s^{'},t^{'}\in R^{'}$ and $\lambda_i,\gamma_i,\kappa_i\in F_0$, let $r^{'}+\sum_{i=1}^{h}\lambda_i u_i, s^{'}+\sum_{i=1}^{h}\gamma_i u_i, t^{'}+\sum_{i=1}^{h}\kappa_i u_i\in R$. Then

$$(r^{'}+\sum_{i=1}^{h}\lambda_i u_i)((s^{'}+\sum_{i=1}^{h}\gamma_i u_i)(t^{'}+\sum_{i=1}^{h}\kappa_i u_i))$$

$$=(r^{'}+\sum_{i=1}^{h}\lambda_i u_i)(s^{'}t^{'}+\sum_{i=1}^{h}[(s^{'}+pR^{'})\kappa_i+\gamma_i(t^{'}+pR^{'})^{\sigma_i}]u_i)$$

$$=r^{'}s^{'}t^{'}+\sum_{i=1}^{h}[(r^{'}+pR^{'})\sum_{i=1}^{h}((s^{'}+pR^{'})\kappa_i+\gamma_i(t^{'}+pR^{'})^{\sigma_i})+\lambda_i(s^{'}t^{'}+pR^{'})^{\sigma_i}]u_i$$

$$=r^{'}s^{'}t^{'}+\sum_{i=1}^{h}[(r^{'}s^{'}+pR^{'})\kappa_i+((r^{'}+pR^{'})\gamma_i+\lambda_i(s^{'}+pR^{'})^{\sigma_i})(t^{'}+pR^{'})^{\sigma_i}]u_i$$

$$=(r^{'}s^{'}+\sum_{i=1}^{h}[(r^{'}+pR^{'})\gamma_i+\lambda_i(s^{'}+pR^{'})^{\sigma_i}]u_i)(t^{'}+\sum_{i=1}^{h}\kappa_i u_i)$$

$$=((r^{'}+\sum_{i=1}^{h}\lambda_i u_i)(s^{'}+\sum_{i=1}^{h}\gamma_i u_i))(t^{'}+\sum_{i=1}^{h}\kappa_i u_i).$$

Moreover,

$$(r^{'}+\sum_{i=1}^{h}\lambda_i u_i)((s^{'}+\sum_{i=1}^{h}\gamma_i u_i)+(t^{'}+\sum_{i=1}^{h}\kappa_i u_i))$$

$$= (r' + \sum_{i=1}^{h} \lambda_i u_i)(s' + t' + \sum_{i=1}^{h} (\gamma_i + \kappa_i) u_i)$$

$$= r'(s' + t') + \sum_{i=1}^{h} [(r' + pR')(\gamma_i + \kappa_i) + \lambda_i((s' + t' + pR')^{\sigma_i}] u_i$$

$$= r's' + \sum_{i=1}^{h} [(r' + pR')\gamma_i + \lambda_i (s' + pR')^{\sigma_i}] + r't' + \sum_{i=1}^{h} [(r' + pR')\kappa_i$$
$$+ \lambda_i (t' + pR')^{\sigma_i}]$$

$$= (r' + \sum_{i=1}^{h} \lambda_i u_i)(s' + \sum_{i=1}^{h} \gamma_i u_i) + (r' + \sum_{i=1}^{h} \lambda_i u_i)(t' + \sum_{i=1}^{h} \kappa_i u_i).$$

Similarly, we can show that

$$((r' + \sum_{i=1}^{h} \lambda_i u_i) + (s' + \sum_{i=1}^{h} \gamma_i u_i))(t' + \sum_{i=1}^{h} \kappa_i u_i)$$
$$= (r' + \sum_{i=1}^{h} \lambda_i u_i)(t' + \sum_{i=1}^{h} \kappa_i u_i) + (s' + \sum_{i=1}^{h} \gamma_i u_i)(t' + \sum_{i=1}^{h} \kappa_i u_i).$$

Remark. From the above construction, we see clearly that every element of R may be uniquely written as $\alpha_0 + \alpha_1 p + ... + \alpha_{n-1} p^{n-1} + u$ with

$$\alpha_0, \alpha_1, ..., \alpha_{n-1} \in F_0 =< a > \cup \{0\}$$

and $u \in J(R)$. Therefore the unique expression can be given in the form

$$\alpha_0 + \alpha_1 p + ... + \alpha_{n-1} p^{n-1} + \lambda_1 u_1 + ... + \lambda_h u_h$$

where $\alpha_0, ..., \alpha_{n-1}, \lambda_i \in F_0$, $(i = 1, ..., h)$. The ring R may also be written in basis form, that is $R = \{1, p, ..., p^{n-1}, u_1, ..., u_h\}$ where u_i, $1 \leq i \leq h$ satisfies the multiplication properties given in the construction.

Lemma 1. *The ring given by the construction is commutative iff* $\sigma_i = id_{R'}$ *for each* $i = 1, ..., h$.

Proof. If $\sigma_i = id_{R'}$, then the ring R is commutative via the multiplication defined in its construction. On the other hand, suppose R is commutative. For each $r', s' \in R', \gamma_i, \lambda_i \in F_0$, let $r' + \sum_{i=1}^{h} \lambda_i u_i$ and $s' + \sum_{i=1}^{h} \gamma_i u_i$, be elements of R, then $(r' + \sum_{i=1}^{h} \lambda_i u_i)(s' + \sum_{i=1}^{h} \gamma_i u_i) = (s' + \sum_{i=1}^{h} \gamma_i u_i)(r' + \sum_{i=1}^{h} \lambda_i u_i) \Rightarrow$

$r^{'}s^{'}+\sum_{i=1}^{h}[(r^{'}+pR^{'})\gamma_i+\lambda_i(s^{'}+pR^{'})^{\sigma_i}]u_i = s^{'}r^{'}+\sum_{i=1}^{h}[(s^{'}+pR^{'})\lambda_i+\gamma_i(r^{'}+pR^{'})^{\sigma_i}]u_i$. Since $R^{'}$ is commutative, $r^{'}s^{'} = s^{'}r^{'}$. Now, $(r^{'}+pR^{'})\gamma_i+\lambda_i(s^{'}+pR^{'})^{\sigma_i} = (s^{'}+pR^{'})\lambda_i+\gamma_i(r^{'}+pR^{'})^{\sigma_i}$. So $\lambda_i(s^{'}+pR^{'})^{\sigma_i}-(s^{'}+pR^{'})\lambda_i = \gamma_i(r^{'}+pR^{'})^{\sigma_i}-(r^{'}+pR^{'})\gamma_i$. This is only possible if both sides are zero and since $r^{'}, s^{'} \in R^{'}, \gamma_i, \lambda_i \in F_0$, then $\sigma_i = id_{R'}$ for each $i = 1, ..., h$ □

Remark. If $n = 1$ or 2, then the Construction yields rings in which multiplication of any two zero divisors is zero, that is $(J(R))^2 = (0)$. Such rings have been shown to be completely primary, and their automorphisms have been deeply studied by Alkhamees[2]. Therefore in the next section, we shall study some properties of rings given by Construction I where $n \in \mathbf{Z}$, $n \geq 3$. We show that such rings are completely primary and satisfy the properties *(i)* $J(R) = pR^{'} \oplus U$, *(ii)* $(J(R))^{n-1} = p^{n-1}R^{'}$, *(iii)* $(J(R))^n = (0)$. We shall call a completely primary finite ring R which satisfies the three properties, *a ring with property A.*

Rings with Property A

Proposition 1. *Let $R^{'} = GR(p^{nr}, p^n)$ where $n \geq 3$. Then the ring R given by Construction I is completely primary and of characteristic p^n satisfying;*
(i) $J(R) = pR^{'} \oplus U$
(ii) $(J(R))^{n-1} = p^{n-1}R^{'}$
(iii) $(J(R))^n = (0)$

Proof. With obvious identifications, let $R^{'} \subseteq R$. Since $id_{R'} = id_R$, it is easy to see that $char R = char R^{'}$. Let $J(R) = pR^{'} \oplus U$. First, we show that every element not in $J(R)$ is invertible. Let $a \in R^{'}$, and a not a member of $pR^{'}$ and $s \in J(R)$. We have

$$\begin{aligned}(a+s)^{p^r} &= a^{p^r} + s^{'}(\text{with } s^{'} \in J(R))\\ &= a + s^{''}(\text{with } s^{''} \in J(R)).\end{aligned}$$

But then

$$(a+s^{''})^{p^r-1} = 1 + s^{'''}(\text{with } s^{'''} \in J(R))$$

and $(1+s^{'''})^{p^{n-1}} = 1$. Hence $a+s$ is invertible. Since $|J(R)| = p^{(h+n-1)r}$ and $|(R^{'}/pR^{'})^{*} + J(R)| = (p^r-1)p^{(h+n-1)r}$, it follows that $(R^{'}/pR^{'})^{*} + J(R) = R - J(R)$ and hence all the elements outside $J(R)$ are invertible. Now, from the way multiplication is defined on R, it follows that $(J(R))^{n-1} = p^{n-1}R^{'}$ and that $J(R)(p^{n-1}R^{'}) = (p^{n-1}R^{'})J(R) = (0)$. Hence $(J(R))^n = (0)$.

Also, from the definition of multiplication, it follows that $RJ(R) = J(R)R \subseteq J(R)$, so that $J(R)$ is an ideal. Suppose there is an ideal $K(R) \supseteq J(R)$, then $K(R)$ contains a unit $z \in R$ such that $zz^{-1} = z^{-1}z = 1$. Then $K = R$. Therefore, $J(R)$ is the unique maximal ideal in R since any maximal ideal distinct from $J(R)$ contains a unit. □

In the sequel, we shall assume that a ring and all its subrings have the same identity 1. Since $ann(J(R)) = p^{n-1}R' \oplus U$, we notice that $(J(R))^{n-1} \subseteq ann(J(R))$. We also notice that in such classes of finite rings, the product of any two zero divisors lies in the coefficient (Galois) subring R'. Infact $(J(R))^2 = p^2R'$.

Lemma 2. *Let R be a completely primary finite ring (not necessarily rings considered in this work). Let $J(R)$ be the Jacobson radical of R. If $char R = p^t$ where $t = 1$ or 2, then $1 + J(R) \cong J(R)$.*

Proof. Let $u \in J(R)$. The map $1 + J(R) \to J(R)$ defined by $1 + u \to u$ is clearly an isomorphism. □

However, if $char R = p^s$ where $s \in \mathbf{Z}, s \geq 3$, then the map defined in the proof above is a bijection, but not an isomorphism. For instance, consider the ring $R = \mathbf{Z}_8$. Here $J(R) = 2\mathbf{Z}_8$, $1 + J(R) = 1 + 2\mathbf{Z}_8$. Now, the elements 2 and 6 in $J(R)$ are each of order 4, while the non identity elements in $R^* = 1 + J(R)$ are each of order 2.

Lemma 3. *Let R be the ring with property A, and $J(R)$ be the Jacobson radical of R. Then $1 + (J(R))^{n-1} \cong (J(R))^{n-1}$.*

Proof. We give the proof for the case when $\sigma_i = id_{R'}$, $i = 1, ..., h$. The general case follows from this.

Now, consider the map $\phi : 1 + J^{n-1} \to J^{n-1}$ defined by

$$1 + \sum_{t=1}^{m} x_{1t}x_{2t}...x_{(n-1)t} \to \sum_{t=1}^{m} x_{1t}x_{2t}...x_{(n-1)t},$$

$$(x_{it} \in J, 1 \leq i \leq n-1, 1 \leq t \leq m).$$

Clearly ϕ is a bijection. Moreover, for each $i = 1, ..., n-1$, $1 \leq t \leq m$, let $\sum_{t=1}^{m} x_{1t}x_{2t}...x_{(n-1)t}, \sum_{t=1}^{m} y_{1t}y_{2t}...y_{(n-1)t} \in J^{n-1}$, then

$$\phi((1 + \sum_{t=1}^{m} x_{1t}x_{2t}...x_{(n-1)t})(1 + \sum_{t=1}^{m} y_{1t}y_{2t}...y_{(n-1)t}))$$

$$= \phi(1 + \sum_{t=1}^{m} x_{1t}x_{2t}...x_{(n-1)t} + \sum_{t=1}^{m} y_{1t}y_{2t}...y_{(n-1)t}) \text{ since} J^n = (0)$$
$$= \sum_{t=1}^{m} x_{1t}x_{2t}...x_{(n-1)t} + \sum_{t=1}^{m} y_{1t}y_{2t}...y_{(n-1)t}$$
$$= \phi(1 + \sum_{t=1}^{m} x_{1t}x_{2t}...x_{(n-1)t}) + \phi(1 + \sum_{t=1}^{m} y_{1t}y_{2t}...y_{(n-1)t}).$$

Thus ϕ is an isomorphism. □

Lemma 4. *Let R be the ring with property A and $F = R/J(R)$. Then $J(R)/ann(J(R))$ is a vector space over F. Moreover, if $dim_F(J(R)/ann(J(R))) = d$, then $dim_F((J(R))^{n-1}) \leq d^{n-1}$.*

Proof. Let $r \in R$ and $u \in J(R)$. Define scalar multiplication on

$$J(R)/ann(J(R))$$

by $(r + J(R)).(u + ann(J(R))) = r.u + ann(J(R))$. Then $J(R)/ann(J(R))$ is clearly a vector space.

The case when $\sigma_i = id_{R'}, i = 1, ..., h$.

Suppose $\overline{e_1}, ..., \overline{e_d}$ is a fixed $F-$ basis for $J(R)/ann(J(R))$ and $u \in (J(R))^{n-1}$. Then $u = \sum_{t=1}^{m} w_{1t}w_{2t}...w_{(n-1)t}$, where $w_{it} \in J(R)$, $1 \leq i \leq n-1, 1 \leq t \leq m)$.

Now,

$$w_{1t} = \sum_{l_1=1}^{d} \eta_{1l_1t}e_{l_1} + \varphi_1 t$$

$$w_{2t} = \sum_{l_2=1}^{d} \eta_{2l_2t}e_{l_2} + \varphi_2 t$$

$$\vdots$$

$$w_{(n-1)t} = \sum_{l_{n-1}=1}^{d} \eta_{(n-1)l_{(n-1)}t}e_{l_{(n-1)}} + \varphi_{(n-1)} t$$

where for each $1 \leq i \leq n-1$ and $1 \leq t \leq m$, $\eta_{il_it} \in F$, $\varphi_i t \in ann(J(R))$. So

$$u = \sum_{t=1}^{m} (\sum_{l_1,l_2,...,l_{n-1}=1}^{d} \prod_{i=1}^{n-1} \eta_{il_it}e_{l_i})$$

$$= \sum_{l_1,l_2,...,l_{n-1}=1}^{d} (\sum_{t=1}^{m} (\prod_{i=1}^{n-1} \eta_{il_it}) e_{l_1}...e_{l_{n-1}})$$

where $\sum_{t=1}^{m}(\prod_{i=1}^{n-1}\eta_{il_it}) \in F$. Thus for each $1 \leq i \leq n-1$, $l_i = 1, ..., d$, the products $e_{l_1}...e_{l_{n-1}}$ generate $(J(R))^{n-1}$ over F. Hence $dim_F((J(R))^{n-1}) \leq d^{n-1}$.

The general case follows from this proof. □

Lemma 5. *Let R be the ring with property A and $J(R)$ be its Jacobson radical. Then, for each $1 \leq i \leq n-1$, the quotient space $(J(R))^i/(J(R))^{i+1}$ is a vector space over $R/J(R)$.*

Proof. Let $x \in R$ and $m \in (J(R))^i$. Define the scalar multiplication on $(J(R))^i/(J(R))^{i+1}$ by $(x+J(R))(m+(J(R))^{i+1}) = xm+(J(R))^{i+1}$. It is easy to see that this multiplication turns $(J(R))^i/(J(R))^{i+1}$ into a vector space. □

Remark: Let R be the ring with property A with the invariants p, n, r, k, h. Let $\{u_1, ..., u_h\}$ be the set of generators for U and $\{\sigma_1, ..., \sigma_h\}$ be the associated automorphisms of R with respect to the maximal Galois subring $R^{'}$ of R where σ_j occurs with multiplicity ξ_j, $j = 1, ..., h$.

Now, suppose S is another ring of the same type with the same invariants constructed from the same maximal Galois subring $R^{'}$ and $\{\widehat{\sigma}_1, ..., \widehat{\sigma}_h\}$ are the associated automorphisms of S with respect to $R^{'}$, where $\widehat{\sigma}_i$ occurs with multiplicity $\widehat{\xi}_j$, $j = 1, ..., h$.

We determine the conditions under which the two rings, R and S are isomorphic.

Proposition 2. *With the above notation, $R \cong S$ iff there exists $\theta \in Aut(R^{'})$, possibly distinct from $\{\sigma_1, ..., \sigma_h\} = \{\widehat{\sigma}_1, ..., \widehat{\sigma}_h\}$ and (after possible reindexing), $\xi_j = \widehat{\xi}_j$, $\forall j = 1, ..., h$.*

Proof. Obviously, every element of $R^{'}$ is of the form $\sum_{i=0}^{n-1} a_ip^i$, $a_i \in F_0$. Suppose $\tau : R \to S$ is an isomorphism, then for each $\sum_{i=0}^{n-1} a_ip^i \in R^{'}$, $\tau(\sum_{i=0}^{n-1} a_ip^i)$ belongs to the coefficient subring of S which is $R^{'}$. Now, there exists a unit $z \in (R^{'})^*$ such that $z\tau(\sum_{i=0}^{n-1} a_ip^i)z^{-1} \in R^{'}$ for each $\sum_{i=0}^{n-1} a_ip^i \in R^{'}$. Thus $z\tau(R^{'})z^{-1} = R^{'}$.

Next, consider the map $\theta : R \to S$ defined by $\theta(r) = z\tau(r)z^{-1}$. For each $\alpha_i, \lambda_j \in F_0$ $(1 \leq i \leq n-1, 1 \leq j \leq h)$,

$$\theta(\sum_{i=0}^{n-1} \alpha_ip^i + \sum_{j=1}^{h} \lambda_ju_j) = z\tau(\sum_{i=0}^{n-1} \alpha_ip^i + \sum_{j=1}^{h} \lambda_ju_j)z^{-1}.$$

Clearly θ is bijective.

Now, let

$$\sum_{i=0}^{n-1}\alpha_i p^i+\sum_{j=1}^{h}\lambda_j u_j, \sum_{i=0}^{n-1}\widehat{\alpha_i} p^i+\sum_{j=1}^{h}\widehat{\lambda_j} u_j \in R,$$

where $\alpha_i, \lambda_j, \widehat{\alpha_i}, \widehat{\lambda_j} \in F_0, (1 \leq i \leq n-1, 1 \leq j \leq h)$. Since τ is an isomorphism and using the distributive properties of multiplication in S, we obtain

$$\begin{aligned}
&\theta((\sum_{i=0}^{n-1}\alpha_i p^i+\sum_{j=1}^{h}\lambda_j u_j)+(\sum_{i=0}^{n-1}\widehat{\alpha_i} p^i+\sum_{j=1}^{h}\widehat{\lambda_j} u_j))\\
&\quad=\theta(\sum_{i=0}^{n-1}(\alpha_i+\widehat{\alpha_i})p^i+\sum_{j=1}^{h}(\lambda_j+\widehat{\lambda_j})u_j)\\
&\quad=z(\tau((\sum_{i=0}^{n-1}\alpha_i+\widehat{\alpha_i})p^i+\sum_{j=1}^{h}(\lambda_j+\widehat{\lambda_j})u_j))z^{-1}\\
&\quad=z(\tau(\sum_{i=0}^{n-1}\alpha_i p^i+\sum_{j=1}^{h}\lambda_j u_j)+\tau(\sum_{i=0}^{n-1}\widehat{\alpha_i} p^i+\sum_{j=1}^{h}\widehat{\lambda_j} u_j))z^{-1}\\
&\quad=z(\tau(\sum_{i=0}^{n-1}\alpha_i p^i+\sum_{j=1}^{h}\lambda_j u_j))z^{-1}+z(\tau(\sum_{i=0}^{n-1}\widehat{\alpha_i} p^i+\sum_{j=1}^{h}\widehat{\lambda_j} u_j))z^{-1}\\
&\quad=\theta(\sum_{i=0}^{n-1}\alpha_i p^i+\sum_{j=1}^{h}\lambda_j u_j)+\theta(\sum_{i=0}^{n-1}\widehat{\alpha_i} p^i+\sum_{j=1}^{h}\widehat{\lambda_j} u_j).
\end{aligned}$$

Also,

$$\begin{aligned}
&\theta((\sum_{i=0}^{n-1}\alpha_i p^i+\sum_{j=1}^{h}\lambda_j u_j)(\sum_{i=0}^{n-1}\widehat{\alpha_i} p^i+\sum_{j=1}^{h}\widehat{\lambda_j} u_j))\\
&\quad=\theta(\alpha_0\widehat{\alpha}_0+p\sum_{t=0}^{1}\alpha_t\widehat{\alpha}_{1-t}+...+p^{n-1}\sum_{t=0}^{n-1}\alpha_t\widehat{\alpha}_{n-1-t}\\
&\quad+\sum_{j=1}^{h}((\sum_{i=1}^{n-1}\alpha_i p^i+pR^{'})\widehat{\lambda}_j+\lambda_j(\sum_{i=0}^{n-1}\alpha_i p^i+pR^{'})^{\sigma_j})u_j)\\
&\quad=z(\alpha_0\widehat{\alpha}_0+p\sum_{t=0}^{1}\alpha_t\widehat{\alpha}_{1-t}+...+p^{n-1}\sum_{t=0}^{n-1}\alpha_t\widehat{\alpha}_{n-1-t}
\end{aligned}$$

$$+\sum_{j=1}^{h}((\sum_{i=1}^{n-1}\alpha_i p^i + pR^{'})\widehat{\lambda}_j + \lambda_j(\sum_{i=0}^{n-1}\alpha_i p^i + pR^{'})^{\sigma_j})u_j)z^{-1}$$

On the other hand,

$$\theta(\sum_{i=0}^{n-1}\alpha_i p^i + \sum_{j=1}^{h}\lambda_j u_j)\theta(\sum_{i=0}^{n-1}\widehat{\alpha}_i p^i + \sum_{j=1}^{h}\widehat{\lambda}_j u_j)$$

$$= z(\sum_{i=0}^{n-1}\alpha_i p^i + \sum_{j=1}^{h}\lambda_j u_j)z^{-1}z(\sum_{i=0}^{n-1}\widehat{\alpha}_i p^i + \sum_{j=1}^{h}\widehat{\lambda}_j u_j)z^{-1}$$

$$= z((\sum_{i=0}^{n-1}\alpha_i p^i + \sum_{j=1}^{h}\lambda_j u_j)(\sum_{i=0}^{n-1}\widehat{\alpha}_i p^i + \sum_{j=1}^{h}\widehat{\lambda}_j u_j))z^{-1}$$

$$= z(\alpha_0\widehat{\alpha}_0 + p\sum_{t=0}^{1}\alpha_t\widehat{\alpha}_{1-t} + ... + p^{n-1}\sum_{t=0}^{n-1}\alpha_t\widehat{\alpha}_{n-1-t}$$

$$+\sum_{j=1}^{h}((\sum_{i=1}^{n-1}\alpha_i p^i + pR^{'})\widehat{\lambda}_j + \lambda_j(\sum_{i=0}^{n-1}\alpha_i p^i + pR^{'})^{\sigma_j})u_j)z^{-1}$$

So θ is an isomorphism which sends $R^{'}$ to itself. Thus $\theta|_{R^{'}}$ is an automorphism of $R^{'}$. Now, every element of S is of the form $\sum_{i=0}^{n-1}\alpha_i p^i + \sum_{j=1}^{h}\lambda_j\tau(u_j),\ \lambda_j \in F_0$ and

$$\theta(\sum_{j=1}^{h}\lambda_j u_j)\omega = z\tau(\sum_{j=1}^{h}\lambda_j u_j)z^{-1}\theta(\omega^{'}), z \in (R^{'})^{*}, \omega, \omega^{'} \in R^{'}$$

$$= z\tau(\sum_{j=1}^{h}\lambda_j u_j)z^{-1}z\tau(\omega^{'})z^{-1}, z \in (R^{'})^{*}, \omega^{'} \in R^{'}$$

$$= z\tau(\sum_{j=1}^{h}\lambda_j u_j)\tau(\omega^{'})z^{-1}$$

$$= z\tau(\sum_{j=1}^{h}\lambda_j u_j\omega^{'})z^{-1}$$

$$= \theta(\sum_{j=1}^{h}\lambda_j u_j\omega^{'})$$

$$= \theta(w^{'\sigma_j}(\sum_{j=1}^{h}\lambda_j u_j))$$

$$= \theta(\omega'^{\sigma_j})\theta(\sum_{j=1}^{h}\lambda_j u_j)$$
$$= (\theta(\omega'))^{\sigma_j}\theta(\sum_{j=1}^{h}\lambda_j u_j)$$
$$= \omega^{\sigma_j}\theta(\sum_{j=1}^{h}\lambda_j u_j).$$

So $\sigma_1, ..., \sigma_h \in Aut(R')$ thus $\{\sigma_1, ..., \sigma_h\} = \{\widehat{\sigma_1}, ..., \widehat{\sigma_h}\}$. Moreover, $\widehat{\xi_j} = \xi_j$ after possible reindexing for any $j = 1, ..., h$ since the two rings R and S are constructed from the same maximal Galois subring R'.

Conversely, if the sets $\{\sigma_1, ..., \sigma_h\}$ and $\{\widehat{\sigma}_1, ..., \widehat{\sigma}_h\}$ are equal and for each $j = 1, ..., h$, the multiplicity of σ_j coincides with multiplicity of $\widehat{\sigma}_j$, (after possible reindexing), then for $z \in (R')^*$, $\theta \in Aut(R')$ and $\alpha_i \in F_0 (1 \leq i \leq n-1)$, $\lambda_j \in R', 1 \leq j \leq h$, the map

$$\sum_{i=0}^{n-1}\alpha_i p^i + \sum_{j=1}^{h}\lambda_j u_j \to z((\sum_{i=0}^{n-1}\alpha_i p^i)^{\theta} + \sum_{j=1}^{h}\lambda_j^{\theta} u_j)z^{-1}$$

from R onto S is clearly an isomorphism. □

Finding Ring Isomorphisms

To find an isomorphism θ from R onto S, we consider the ring $T = R \oplus S$ and compute the generator set Γ of $Aut(T)$. See, for example[1, 8], for further details.

Finding Ring Automorphisms

The problem of finding automorphisms of a ring reduces to that of finding non trivial ring automorphisms. We now describe all the automorphisms of the ring with Property A.

Case (i): R is noncommutative.

If R is noncommutative, then there exists $z \in R^*$ which does not commute with the whole of R, thus defines a non trivial automorphism. In this case, let p be a prime integer, then the map $\varphi : R \to R$ defined by

$$\sum_{i=0}^{n-1}a_i p^i + \sum_{j=1}^{h}\lambda_j u_j \to z((\sum_{i=0}^{n-1}a_i p^i)^{\sigma} + (\sum_{j=1}^{h}\lambda_j{}^{\sigma} u_j))z^{-1},\ \sigma \in Aut(R'),\ a_i, \lambda_j \in F_0$$

is a nontrivial automorphism of R.

Case (ii): R is commutative.

Let R be the ring with Property A with Jacobson radical $J(R)$. Clearly $(J(R))^{n-1} \neq (0)$, $(J(R))^n = (0)$. We can concretely express R in terms of its basis elements $\{a, u_1, ..., u_h\}$ so that $p^{n-1}u_i = 0$, $u_i u_j = \gamma_{ij} p^2$, where $\gamma_{ij} \in F_0$, $1 \leq i, j \leq h$ and p is a prime integer. Let $m_i \in F_0$. Each of the elements $p^{n-1}m_i \in (J(R))^{n-1}, (1 \leq i \leq h)$ defines a nontrivial automorphism as follows:

$$\varphi_1 : \begin{cases} u_1 \to u_1 + p^{n-1}m_1 \\ u_2 \to u_2 \\ \quad\vdots \\ u_h \to u_h \end{cases}$$

$$\varphi_2 : \begin{cases} u_1 \to u_1 \\ u_2 \to u_2 + p^{n-1}m_2 \\ \quad\vdots \\ u_h \to u_h \end{cases}$$

$$\vdots$$

$$\varphi_h : \begin{cases} u_1 \to u_1 \\ u_2 \to u_2 \\ \quad\vdots \\ u_h \to u_h + p^{n-1}m_h \end{cases}$$

Notice that $\varphi = \varphi_1\varphi_2...\varphi_h$ defines an automorphism of R restricted to U.

The Group X

Let R be the ring with Property A and ξ be the number of nontrivial associated automorphisms of R with respect to R' taken with their multiplicities η_i ,

$$U_\xi = \sum_{\sigma_j \neq id_{R'}} \oplus R' u_j$$

and

$$U_\eta = \sum_{\sigma_j = id_{R'}} \oplus R' u_j, (1 \leq i, j \leq h).$$

Suppose $z \in 1 + J(R)$ where $z = 1 + c + d$ with $c \in pR' \oplus U_\eta = J(R) \cap Z(R)$, $d \in U_\xi$ and

$$ct_k, dt_k \in pR' \oplus U_\eta, 1 \leq k \leq n-1.$$

Let

$$\pi_z(\sum_{i=0}^{n-1} a_i p^i + \sum_{j=1}^{h} \lambda_j u_j) = z(\sum_{i=0}^{n-1} a_i p^i + \sum_{j=1}^{h} \lambda_j u_j)z^{-1}$$

and $X = \{\pi_z : z \in 1 + J(R)\}$ and define a map $g : X \to U_\xi$ by $g(\pi_z) = d$.

Now, let $\pi_z = \pi_{s_1}$. Since $z \in 1 + J(R)$ and $(J(R))^n = (0)$, we write $z = s_1 . \prod_{k=2}^{n} s_k$ where

$$\prod_{k=2}^{n} s_k = s_1^{-1} z, \prod_{k=2}^{n} s_k \in 1 + J(R).$$

If $s_1 = 1 + c + d$ and

$$\prod_{k=2}^{n} s_k = \prod_{\nu=1}^{n-1} 1 + t_\nu$$

where $d \in U_\xi$, and

$$t_\nu, ct_\nu, dt_\nu \in pR' \oplus U_\eta = J(R) \cap Z(R), 1 \leq \nu \leq n-1,$$

then

$$z = \prod_{\nu=1}^{n} s_\nu = 1 + (c + \widehat{t} + c\widehat{t} + d\widehat{\widehat{t}}) + d$$

where $\widehat{t} = \sum_{\nu=1}^{n-1} t_\nu +$ sums of mixed products of $t_\nu, 1 \leq \nu \leq n-1$ and $\widehat{\widehat{t}} = \widehat{t} - \prod_{\nu=1}^{n-1} t_\nu$.

Thus $g(\pi_z) = g(\pi_{s_1})$ showing that g is well defined. Since R is finite, g is clearly onto.

Moreover,

$$\begin{aligned} g(\pi_{z_1}\pi_{z_2}) &= g(z_1 \pi_{z_2} z_1^{-1}) \\ &= g(z_1 z_2(\sum_{i=0}^{n-1} a_i p^i + \sum_{j=1}^{n} \lambda_j u_j) z_2^{-1} z_1^{-1}) \\ &= g(z_1 z_2(\sum_{i=0}^{n-1} a_i p^i + \sum_{j=1}^{n} \lambda_j u_j)(z_1 z_2)^{-1}) \\ &= g(\pi_{z_1 z_2}) \\ &= d_1 + d_2 \\ &= g(\pi_{z_1}) + g(\pi_{z_2}). \end{aligned}$$

Thus, $g : X \to U_\xi$ is an isomorphism.

Now, let $U = U_1 \oplus ... \oplus U_s$, where each $U_\nu = \sum_{\sigma_k=\sigma_j} \oplus R^{'} u_k$, so that σ_k is the automorphism associated with u_k and $1 \leq \nu \leq s$.

The following is essentially Remark 2 in [2].

Suppose $U_\xi = \sum_{\sigma_j \neq id_{R^{'}}} \oplus R^{'} u_j$, $U_\eta = \sum_{\sigma_j = id_{R^{'}}} \oplus R^{'} u_j$, then

$$U_\eta \cong \begin{cases} U_k \text{ for some } k \in \{1, ..., s\}, \text{ if one of the associated} \\ \quad \text{automorphisms of } R \text{ with respect to } R^{'} \text{ is trivial} \\ (0) \text{ if none of the associated automorphisms of } R \\ \quad \text{with respect to } R^{'} \text{ is trivial} \end{cases}$$

Given that $U_\eta = U_k$ for some $k \in \{1, ..., s\}$, take $U_\eta = U_s$. Then $U_\xi = U_1 \oplus ... \oplus U_m$ where $m = s$ or $m = s - 1$. So, we consider $U = \sum_{j=1}^{h} \oplus R^{'} u_j$, $h = l_1 + ... + l_s$ where each l_ν is the number of elements in the generating sets for U_ν, $(\nu = 1, ..., s)$.

The following lemmata are modifications of Theorem 2 in [2].

We consider R to be the ring with Property A and $G = Aut(R)$.

Lemma 6. *Let $K \leq G$ containing all the automorphisms ϕ defined by*

$$\phi(\sum_{i=0}^{n-1} a_i p^i + \sum_{j=1}^{h} \lambda_j u_j) = (\sum_{i=0}^{n-1} a_i p^i)^\sigma + \sum_{\nu=1}^{s} \sum_{j=1}^{h} \lambda_j^\sigma \phi_\nu(u_j), a_i, \lambda_j \in F_0,$$

$\sigma \in Aut(R^{'})$ and if $u_j \in U_\eta$, then $\phi_\nu \in Aut_{R^{'}/pR^{'}} U_\nu$.

Suppose K_1 is a subgroup of K containing automorphisms ϕ_σ defined by

$$\phi_\sigma(\sum_{i=0}^{n-1} a_i p^i + \sum_{j=1}^{h} \lambda_j u_j) = (\sum_{i=0}^{n-1} a_i p^i)^\sigma + \sum_{j=1}^{h} \lambda_j^\sigma u_j, a_i, \lambda_j \in F_0$$

and K_2 be a subgroup of K containing automorphisms ϕ^* defined by

$$\phi^*(\sum_{i=0}^{n-1} a_i p^i + \sum_{j=1}^{h} \lambda_j u_j) = \sum_{i=0}^{n-1} a_i p^i + \sum_{\nu=1}^{s} \sum_{j=1}^{h} \lambda_j \phi_\nu(u_j), \phi_\nu \in Aut_{R^{'}/pR^{'}} U_\nu$$

if $u_j \in U_\nu$. Then $K = K_2 \times_\tau K_1$ where $\tau : K_1 \to Aut(K_2)$ defined by $\phi_\sigma \to (\phi^* \to \phi^*_\sigma)$ is a group homomorphism.

Proof. Clearly $\phi = \phi^* \phi_\sigma \in K_2 K_1$. So $K = K_2 K_1$. Also K_2 is normal in K since for each $\phi \in K$,$K_2 \phi = \phi K_2$.

Now let $\mu \in K_1 \cap K_2$. Then μ fixes $R^{'}$ elementwise, $\mu(R^{'}) = R^{'}$ and since $U = \sum_{j=1}^{h} R^{'} u_j$, $\mu(U) = U$ (μ fixes U elementwise) and the only such element is the identity. Thus $K_1 \cap K_2 = id_R$. Finally, that the map τ is a group homomorphism follows from the definition. □

Lemma 7. *Let $L \leq G$ containing all automorphisms π defined by*

$$\pi(\sum_{i=0}^{n-1} a_i p^i + \sum_{j=1}^{h} \lambda_j u_j) = z(\sum_{i=0}^{n-1} a_i p^i + \sum_{j=1}^{h} \lambda_j u_j + \sum_{\sigma_j = id_{R'}} p^{n-1} \lambda_j m_j) z^{-1}, z \in R^*$$

$(z = s_1 ... s_n, s_i \in 1 + J(R), 1 \leq i \leq n), m_j, \lambda_j \in F_0$, σ_j is the automorphism associated with u_j.

Suppose L_1 is a subgroup of L containing automorphisms $\overline{\pi}$ defined by

$$\overline{\pi}(\sum_{i=0}^{n-1} a_i p^i + \sum_{j=1}^{h} \lambda_j u_j) = \sum_{i=0}^{n-1} a_i p^i + \sum_{j=1}^{h} \lambda_j u_j + \sum_{\sigma_j = id_{R'}} p^{n-1} \lambda_j m_j, m_j \in F_0,$$

σ_j is the automorphism associated with u_j, and L_2 is a subgroup of L containing automorphisms π_z defined by

$$\pi_z(\sum_{i=0}^{n-1} a_i p^i + \sum_{j=1}^{h} \lambda_j u_j) = z(\sum_{i=0}^{n-1} a_i p^i + \sum_{j=1}^{h} \lambda_j u_j) z^{-1}, z \in R^*.$$

Then $L = L_1 \times L_2$.

Proof. The automorphism $\pi = \pi_z \overline{\pi} \in L_2 L_1$. Also L_1 and L_2 are normal subgroups of L. Now, let $\varrho \in L_1 \cap L_2$. Then $\varrho(R^{'}) = R^{'}$ or another Galois subring of R. From the definition of $\overline{\pi}$ and π_z, the only ϱ which lies in both L_1 and L_2 is id_R. □

Lemma 8. *Let K and L be as defined in Lemmas 6 and 7 respectively. Then $G = L \times_\alpha K$ where $\alpha : K \to Aut(L)$ defined by*

$$\phi^* \phi_\sigma \to (\overline{\pi} \pi_z \to \overline{\pi}_\sigma (\phi^* \phi_\sigma) z (\phi^* \phi_\sigma)^{-1})$$

is a group homomorphism.

Remark: Notice that each element of G is of the form $\pi\phi$, where $\pi \in L$, $\phi \in K$.

Lemma 9. *Let $f : L_1 \to U_\eta$ defined by $f(\overline{\pi}) = \sum_{\sigma_j = id_{R'}} m_j u_j$. Then $L_1 \cong U_\eta$*

Proof. The map f is clearly a bijection. Moreover, if $\overline{\pi}_1, \overline{\pi}_2 \in L_1$ and $m_j, \widehat{m_j} \in F_0$, then

$$f(\overline{\pi_1 \pi_2}) = f(\sum_{i=0}^{n-1} a_i p^i + \sum_{j=1}^{h} \lambda_j u_j + \sum_{\sigma_j = id_{R'}} p^{n-1} \lambda_j m_j + \sum_{\sigma_j = id_{R'}} p^{n-1} \lambda_j \widehat{m_j})$$

$$= f(\sum_{i=0}^{n-1} a_i p^i + \sum_{j=1}^{h} \lambda_j u_j + \sum_{\sigma_{j=id_{R'}}} p^{n-1}\lambda_j(m_j + \widehat{m_j}))$$
$$= \sum_{\sigma_j = id_{R'}} (m_j + \widehat{m_j})u_j$$
$$= \sum_{\sigma_j = id_{R'}} m_j u_j + \sum_{\sigma_j = id_{R'}} \widehat{m_j} u_j$$
$$= f(\overline{\pi_1}) + f(\overline{\pi_2})$$

□

Remark: Using the above Lemma and the fact that $L_2 = X \cong U_\xi$, we obtain $L_1 \times L_2 \cong U_\eta \oplus U_\xi$. Thus $L \cong U$. Since $U = U_1 \oplus ... \oplus U_s$, we can view each of the U_ν $(\nu = 1, ..., s)$ as a vector space over $R^{'}/pR^{'}$ and $Aut(U_\nu)$ corresponds to the set of invertible matrices $GL(l_\nu, R^{'}/pR^{'})$. Now, $K_2 = Aut(U)$ corresponds to the set of the invertible matrices $\prod_{\nu=1}^{s} GL(l_\nu, R^{'}/pR^{'})$. Since $Aut(R^{'}) \cong Aut(R^{'}/pR^{'})$, notice that $K_1 = Aut(R^{'}/pR^{'})$.

We now state the main Theorem which is similar to Theorem 2 in [2].

Theorem 1. *Let R be the ring with Property A. Then the map*

$$Aut(R) \to U \times_\alpha (\prod_{\nu=1}^{s} GL(l_\nu, R^{'}/pR^{'}) \times_\kappa Aut(R^{'}/pR^{'}))$$

is an isomorphism and in particular

$$| \ Aut(R) \ | = (p^r)^h (\prod_{\nu=1}^{s} \prod_{i=0}^{l_\nu - 1} ((p^r)^{l_\nu} - (p^r)^i))r.$$

Proof. Since $AutR^{'} \cong Aut(R^{'}/pR^{'})$, then $r = |AutR^{'}| = |Aut(R^{'}/pR^{'})|$. Now, using the fact that the order of $U = (p^r)^h$, and

$$|GL(l_\nu, R^{'}/pR^{'})| = \prod_{i=0}^{l_\nu - 1} ((p^r)^{l_\nu} - (p^r)^i),$$

the order of the automorphism group of the ring R clearly follows. The rest of the proof follows from Lemmata 6 to 9. □

Acknowledgments

The author would like to express his wholehearted gratitude to DAAD for sponsoring his visit to the African Institute for Mathematical Sciences, South Africa in which this research was done.

References

[1] M. Agrawal, N. Saxena, *Automorphisms of Finite Rings and Applications to Complexity Problems*, Springer LNCS, 3404 (2005).

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

[3] Y. Alkhamees, Finite completely primary rings in which the product of any two zero divisors of a ring is in its coefficient subring, *Internat. J. Math. and Math. Sci.*, **17**, No. 3 (1994), 463-468.

[4] J.N.S. Bidwell, M.J. Curran, D.J. McCaughan, Automorphisms of direct products of finite groups, *Arch. Math.*, **86** (2006), 481-489.

[5] J.N.S. Bidwell, Automorphisms of direct products of finite groups II, *Arch. Math.*, **91** (2008), 111-121.

[6] C.J. Chikunji, Automorphism groups of finite rings of characteristic p^2 and p^3, *Glasnik Matematicki*, **43**, No. 1 (2008), 25-40.

[7] C. Hillar, D. Rhea, *Automorphisms of an Abelian p-Group*, Amer. Math. Monthly, **114** (2007), 917-922.

[8] N. Kayal, N. Saxena, Complexity of ring morphism problems, *Birkhauser Verlag Bassel*, **15**, No. 4 (2006).

[9] R. Raghavendran, Finite associative rings, *Compositio Math.*, **21**, No. 2 (1969), 195-229.

[10] B.R. Wirt, *Finite Non-Commutative Local Rings*, Ph.D. Thesis, University of Oklahoma (1972).