Pure Mathematical Sciences, Vol. 5, 2016, no. 1, 11 - 23
HIKARI Ltd, www.m-hikari.com

AUTOMORPHISMS OF THE UNIT GROUPS OF SQUARE RADICAL ZERO FINITE COMMUTATIVE COMPLETELY PRIMARY RINGS

Ojiema Michael Onyango [1], **Owino Maurice Oduor** [2] **and Odhiambo Paul Oleche** [3]

[1] Department of Mathematics,
Masinde Muliro University of Science and Technology
P.O Box 190-50100, Kakamega (Kenya).
e-mail: michael_ojiema@yahoo.com or mojiema@mmust.ac.ke

[2] Department of Mathematics and Computer Science
University of Kabianga
P.O Box 2030-20200, Kericho (Kenya)
e-mail: morricearaka@yahoo.com

[3] Department of Pure and Applied Mathematics
Maseno University
P.O Box 333, Maseno (Kenya)
e-mail:poleche@maseno.ac.ke

Abstract

Let G be a group. The groups $G^{'}$ for which G is an automorphism group have not been fully characterized. Suppose R is a Completely Primary finite Ring with Jacobson Radical J such that $J^2 = (0)$. In this case, the characteristic of R is p or p^2 and the group of units $R^* = \mathbb{Z}_{p^r-1} \times (I+J)$. The structure of R^* is well known, but its automorphism group is not well documented. Given the group R^*, let $Aut(R^*)$ denote the group of isomorphisms $\phi : R^* \rightarrow R^*$ with multiplication given by the composition of functions. The structure of the automorphism groups of finite groups is intimately connected to the structure of the finite groups themselves. In this note, we determine the structure of $Aut(R^*)$ using well known procedures and to this end, extend the results previously obtained in this area of research.

Mathematics Subject Classification: Primary 20K30; Secondary 16P10.
Keywords: Automorphism Groups, Unit Groups, Square Radical Zero Completely Primary Rings.

1 Introduction

The definition of terms and standard notations can be obtained from [1, 3, 4, 6]. The classification of finite rings has been studied with great success in the recent past ([1, 3, 6] and related studies). Most of the researchers have concentrated in obtaining the structures of the unit groups of Completely Primary Finite Rings. However, the automorphisms of these unit groups have remained uncharacterized. The first general structure result for the automorphisms group of a finite group follows from a classical result of Gauss in number theory. Let $\mathbb{Z}_n$ denote the additive group of integers mod n and $U(\mathbb{Z}_n)$ the multiplicative group of integers mod n. Gauss analyzed the orders of elements in $U(\mathbb{Z}_{p^n})$ for p prime. His results can be summarized as follows:

Theorem 1.1. *(Gauss) Let p be an odd prime and $n \geq 1$ or $p = 2$ and $n \geq 2$. Then*

$$U(\mathbb{Z}_{p^n}) \cong \mathbb{Z}_{p^{n-1}(p-1)}, U(\mathbb{Z}_{2^n}) \cong \mathbb{Z}_2 \times \mathbb{Z}_{2^{n-2}}$$

Notice that $U(\mathbb{Z}_n)$ is precisely the set of generators of $\mathbb{Z}_n$. Since any automorphism $\theta \in \mathbb{Z}_n$ sends 1 to a generator, the valuation map $E : Aut(\mathbb{Z}_n) \mapsto U(\mathbb{Z}_{p^n})$ given by $E(\theta) = E(1)$ is an isomorphism of groups. This sets the stage for prime factorization of the integer n and consequently the classification of the automorphisms of an arbitrary finite abelian group. On the other hand, the automorphisms of cyclic groups are precisely known. In fact, given any prime p and any integer n, the group $Aut(C_p^n) \cong Aut(\mathbb{Z}_p^n)$, the group of n by n invertible matrices over the field $\mathbb{Z}_p$. These and related matrix groups play important roles in the classification of simple groups.

In [6], the authors have constructed a class of Square Radical Zero Commutative Completely Primary finite Rings as follows:

Let R_o be the Galois ring of the form $GR(p^{kr}, p^k)$, such that $k = 1, 2$. For each $i = 1, ..., h$, let $u_i \in J(R)$, such that U is an $h-$ dimensional R_o-module generated by $\{u_1, ..., u_h\}$ so that $R = R_0 \oplus U$ is an additive group. On this group, define multiplication by the following relation

(*) $pu_i = u_iu_j = u_ju_i = 0$, $u_ir_o = (r_o)^{\sigma_i}u_i$

where $r_o \in R_o$, $1 \leq i, j \leq h$, 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 $r_0 + \sum_{i=1}^{h} \lambda_i u_i$ and $s_0 + \sum_{i=1}^{h} \gamma_i u_i$, $r_0, s_0 \in R_0$, $\lambda_i, \gamma_i \in F_o$ are elements of R, then,

$$(r_o + \sum_{i=1}^{h} \lambda_i u_i)(s_o + \sum_{i=1}^{h} \gamma_i u_i) = r_o s_o + \sum_{i=1}^{h} \{(r_o + pR_o)\gamma_i + \lambda_i (s_o + pR_o)^{\sigma_i}\} u_i$$

It is easy to verify that the given multiplication turns the additive abelian group R, into a ring with identity $(1, 0, ..., 0)$. Moreover, $J^2 = (0)$. Accordingly, the characteristic of R is either p or p^2. Furthermore, the group of units R^* of R is given by $R^* = \mathbb{Z}_{p^r-1} \times (1 + J)$, a direct product of abelian groups.

In [4], Hillar and Rhea have given a useful description of the automorphism group of an arbitrary finite abelian group and they found the size of this automorphism group. We extend their work by characterizing $Aut(R^*)$. We find all the elements of $GL_{hr}(\mathbb{Z}_p)$ that can be extended to a matrix in $End(B_p)$ and calculate the distinct ways of extending such elements to the endomorphism. The first complete characterization of the automorphism group of an abelian group was however given by Ranum [2].

2 Preliminaries

Theorem 2.1. *(cf. [6]) The unit group R^* of the commutative completely primary finite ring of characteristic p or p^2 with maximal ideal J such that $J^2 = (0)$ and with invariants p (prime integer), $p \in J$, $r \geq 1$ and $h \geq 1$ is a direct product of cyclic groups as follows:*

(i) If Char $R = p$,then

$$R^* = \mathbb{Z}_{p^r-1} \times (\mathbb{Z}_p^r)^h$$

(ii) If Char $R = p^2$ then,

$$R^* = \mathbb{Z}_{p^r-1} \times \mathbb{Z}_p^r \times (\mathbb{Z}_p^r)^h.$$

The following Lemma is useful in the sequel

Lemma 2.2. *(cf. [4]) Let H and K be finite groups of relatively prime orders. Then, $Aut(H) \times Aut(K) \cong Aut(H \times K)$*

Proposition 2.3. *Let $R^* = \mathbb{Z}_{p^r-1} \times 1 + J$. Since g.c.d$(p^r - 1, \mid 1 + J \mid) = 1$, $Aut(R^*) \cong Aut(\mathbb{Z}_{p^r-1} \times 1 + J) = Aut(\mathbb{Z}_{p^r-1}) \times Aut(1 + J)$*

Proof. Let $\theta : Aut(\mathbb{Z}_{p^r-1}) \times Aut(1+J) \to Aut(\mathbb{Z}_{p^r-1} \times 1+J)$ be a homomorphism. Suppose $\theta_1 \in Aut(\mathbb{Z}_{p^r-1})$ and $\theta_2 \in Aut(1+J)$, then, it is easy to see that an automorphism $\theta(\theta_1, \theta_2)$ of $\mathbb{Z}_{p^r-1} \times (1+J)$ is given by $\theta(\theta_1, \theta_2)(x, y) = (\theta_1(x), \theta_2(y))$

Let $id_1 \in Aut(\mathbb{Z}_{p^r-1})$ and $id_2 \in Aut(1+J)$ be the identity automorphisms of $\mathbb{Z}_{p^r-1}$ and $1+J$ respectively. To show that, θ is indeed a homomorphism, notice that $\theta(id_1, id_2) = Id_{(\mathbb{Z}_{p^r-1}\times 1+J)}$ and that, $\theta(\theta_1\theta_1^{'}, \theta_2\theta_2^{'})(x, y) = (\theta_1\theta_1^{'}(x), \theta_2\theta_2^{'}(y))$

$$= \theta(\theta_1, \theta_2)\theta(\theta_1^{'}, \theta_2^{'})(x, y), \forall \theta_1, \theta_1^{'} \in Aut(\mathbb{Z}_{p^r-1}), \theta_2, \theta_2^{'} \in Aut(1+J)$$

Next, we verify that θ is an isomorphism. Clearly, θ is injective. Thus, we are left with showing surjectivity.

Let $n = p^r - 1 =\mid \mathbb{Z}_{p^r-1} \mid$ and $m =\mid 1+J \mid$ such that $(n, m) = 1$. Write $\phi_{\mathbb{Z}_{p^r-1}}$ and ϕ_{1+J} for the standard projection homomorphism $\phi_{\mathbb{Z}_{p^r-1}} : \mathbb{Z}_{p^r-1} \times 1+J \to \mathbb{Z}_{p^r-1}$ and $\phi_{1+J} : \mathbb{Z}_{p^r-1} \times 1+J \to 1+J$. Fix $\theta^{'} \in Aut(\mathbb{Z}_{p^r-1} \times 1+J)$ and consider the homomorphism $\alpha : 1+J \to \mathbb{Z}_{p^r-1}$ given by $\alpha(y) = \phi_{\mathbb{Z}_{p^r-1}}(\theta^{'}(id_1, y))$. Notice that $\{y^n : y \in 1+J\} \subseteq ker(\alpha)$ since $id_1 = \phi_{\mathbb{Z}_{p^r-1}}(\theta^{'}(id_1, y))^n = \phi_{\mathbb{Z}_{p^r-1}}(\theta^{'}(id_1, y)^n) = \phi_{\mathbb{Z}_{p^r-1}}(\theta^{'}(id_1, y^n)) = \alpha(y^n)$

Also, since $(m, n) = 1$, the set $\{y^n : y \in 1+J\}$ consists of m elements. Consequently, it follows that $ker(\alpha) = 1+J$ and α is the trivial homomorphism. Similarly, $\delta : \mathbb{Z}_{p^r-1} \to 1+J$ given by $\delta(x) = \phi_{1+J}(\theta^{'}(x, id_2))$ is trivial.

Finally, define endomorphisms of $\mathbb{Z}_{p^r-1}$ and $1+J$ by; $\theta^{'}(x) = \phi_{\mathbb{Z}_{p^r-1}}(\theta^{'}(x, id_2))$, $\theta^{'}_{1+J}(y) = \phi_{1+J}(\theta^{'}(id_1, y))$. From this construction and the above argument, we have $\theta^{'}(x, y) = \theta^{'}(x, id_2)\cdot\theta^{'}(id_1, y) = (\theta^{'}_{\mathbb{Z}_{p^r-1}}(x), \theta^{'}_{1+J}(y)) = (\theta^{'}_{\mathbb{Z}_{p^r-1}}, \theta^{'}_{1+J}(x, y))$for all $x \in \mathbb{Z}_{p^r-1}$ and $y \in 1+J$

It remains to prove that $\theta^{'}_{\mathbb{Z}_{p^r-1}} \in Aut(\mathbb{Z}_{p^r-1})$ and $\theta^{'}_{1+J} \in Aut(1+J)$ and for this, it suffices that $\theta^{'}_{\mathbb{Z}_{p^r-1}}$ and $\theta^{'}_{1+J}$ are injective (since both $n, m < \infty$)

Now, suppose that $\theta^{'}_{\mathbb{Z}_{p^r-1}}(x) = id_1$ for some $x \in \mathbb{Z}_{p^r-1}$. Then, $\theta^{'}(x, id_2) = (\theta^{'}_{\mathbb{Z}_{p^r-1}}(x), \theta^{'}_{1+J}(id_2) = (id_1, id_2)$. So, $x = id_1$ by injectivity of $\theta^{'}$. A similar argument shows that $\theta^{'}_{1+J} \in Aut(1+J)$ and this completes the proof. □

Remark 2.4. *From the Lemma and proposition above it is easy to see that since the groups $\mathbb{Z}_{p^r-1}$ and $1+J)$ are of relatively prime orders and $Aut(\mathbb{Z}_{p^r-1}) \cong (\mathbb{Z}_{p^r-1})^*$, it implies that*

(i) when $char(R) = p$ then $Aut(R^*) \cong Aut(\mathbb{Z}_{p^r-1}) \times Aut(\prod^h(\mathbb{Z}_p^r)) \cong (\mathbb{Z}_{p^r-1})^* \times Aut(\prod^h(\mathbb{Z}_p^r))$.

(ii) when $char(R) = p^2$, then $Aut(R^*) \cong (\mathbb{Z}_{p^r-1})^* \times Aut(\prod^{h+1}(\mathbb{Z}_p^r))$.

Lemma 2.5. *Let $Char(R) = p$, p a prime integer and $B_p = 1+J = (\mathbb{Z}_p^r)^r$. Then, $\mid B_p \mid= p^{rh}$.*

Proof. If $B_p = \prod_{i=1}^{h} \mathbb{Z}/p^{e_i}\mathbb{Z}$ such that $1 \leq e_1 \leq e_2 \leq ... \leq e_r$, then, it is well known that $\mid B_p \mid = \mid \prod_{i=1}^{r} \mathbb{Z}/p^{e_i}\mathbb{Z} \mid = p^{\sum_{i=1}^{r} e_i}$. Now, since $e_1 = e_2 = ... = e_r = 1$ and there are $h-$tuples of such r factors of e_r, it follows that $(\sum_{i=1}^{r} e_i)^h = rh$. Thus $\mid B_p \mid = p^{rh}$ as required. □

Remark 2.6. *Now, suppose* $G \cong \prod_{i}^{h} B_p^{'}$ *such that* $B_p^{'} = \underbrace{\mathbb{Z}_p \times \mathbb{Z}_p \times .... \times \mathbb{Z}_p}_{r}$ *over distinct set of primes p then* $Aut(G) = \prod Aut(B_p^{'})$.

In the sequel, we determine $Aut(I + J)$ for both the characteristics of R.

3 The Endomorphism Rings of the group $1 + J$

For a successful characterization of $Aut(R^*)$, it is necessary to first give a description of E_p, the endomorphism ring of $1 + J$. Elements of E_p are group homomorphisms from $1 + J$ into itself with ring multiplication given by composition and addition given naturally by $(A + B)(x) := A(x) + B(x)$ for $A, B \in End(1 + J)$ and $x \in 1 + J$

An element of $1 + J$ is a column vector $(x_1, ..., x_n)^T$ in which each $x_i \in \mathbb{Z}/p^{e_i}\mathbb{Z}$ and $x_i \in \mathbb{Z}$ is an integral represntative

3.1 Characteristic of $R = p, p^2$

Proposition 3.1. *Let R be a finite ring whose additive group* $(R, +)$ *is of type* $(p^{e_1}, p^{e_2}..., p^{e_l}) : e_i \geq e_2 \geq .... \geq e_l$. *Then, R can be identified with a subring of the endomorphism ring say B of the additive group. The ring B can be considered as the ring of all* $l \times l$ *matrices* (a_{ij}) *such that* $1 \leq i,\ j \leq l$ *of the form.*

$$(a_{i,j}) = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1l} \\ p^{e_1-e_2}a_{21} & a_{22} & \cdots & a_{2l} \\ \vdots & \vdots & \vdots & \vdots \\ p^{e_1-e_2}a_{l1} & \cdots & \cdots & a_{ll} \end{pmatrix}$$

such that

$$a_{ij} = \begin{cases} a_{ij}, & i \leq j; \\ p^{e_j-e_i}a_{ij}, & i > j. \end{cases}$$

Definition 3.2. *Define* $R_p = \{(a_{ij}) \in \mathbb{Z}_{n\times n} : p^{e_i-e_j} \mid a_{ij} \forall i, j; 1 \leq j \leq i \leq n\}$

Example 3.3. *Suppose $n = 4$ and since $e_1 = 1, e_2 = 2, e_3 = 3, e_4 = 4$, then $1 + J = \mathbb{Z}_p \times \mathbb{Z}_{p^2} \times \mathbb{Z}_{p^3} \times \mathbb{Z}_{p^4}$*

$$R_p = \begin{pmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ pa_{21} & a_{22} & a_{23} & a_{24} \\ p^2a_{31} & pa_{32} & a_{33} & a_{34} \\ p^3a_{41} & p^2a_{42} & pa_{4,3} & a_{44} \end{pmatrix}$$

Thus generally, when $1 + J = \underbrace{\mathbb{Z}_p \times ... \times \mathbb{Z}_p}_{r}$

$$R_p = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1r} \\ a_{21} & a_{22} & \cdots & a_{2r} \\ \vdots & \vdots & \vdots & \vdots \\ a_{r1} & a_{r2} & \cdots & a_{rr} \end{pmatrix}$$

Lemma 3.4. *R_p forms a ring under matrix multiplication*

Proof. Let $A = (a_{ij}) \in R_p$. The condition that $p^{e_i - e_j} \mid a_{ij}$ for all $i \geq j$ is equivalent to the existence of a decomposition $A = PA^{'}P^{-1}$, in which $A^{'} \in \mathbb{Z}^{n \times n}$ and $P = diag(p^{e_i}, ..., p^{e_n})$ is diagonal

Now, if $A, B \in R_p$, then, $AB = (PA^{'}P^{-1})(PB^{'}P^{-1}) = PA^{'}B^{'}P^{-1} \in R_p$ as required. □

Proposition 3.5. *Let $\phi_i : \mathbb{Z} \to \mathbb{Z}/p^{e_i}\mathbb{Z}$ be defined by $x \mapsto x mod\ p^{e_i}$. Let $\phi : \mathbb{Z}^n \to 1{+}J$ be a homomorphism given by $\phi(x_1, ..., x_n)^T = (\phi_1(x_1), ..., \phi_n(x_n))^T = (x_1, ..., x_n)^T$. Then, E_p is a multiplication by a matrix $A \in R_p$ on a vector of integer representatives followed by an application of ϕ.*

Theorem 3.6. *[4] The map $\psi : R_p \to E_p$ given by $\psi(A)(x_1, ..., x_n)^T = \phi(A(x_1, ..., x_n)^T)$ is a surjective ring homomorphism.*

Proof. We need to verify that $\psi(A)$ is a well defined map from $1 + J$ into itself. Let $A = (a_{ij}) \in R_p$ and suppose that $(x_1, ..x_n)^T = (y_1, ..., y_n)^T$ for $x, y \in \mathbb{Z}$ so that $pe_i \mid x_i - y_i, \forall i$. The k^{th} vector entry of the difference $\phi(A(x_1, ..., x_n)^T) - \phi(A(y_1, ..., y_n)^T)$ is

$$\phi_k(\sum_{i=1}^{n} a_{k_i}x_i) - \phi_k(\sum_{i=1}^{n} a_{k_i}y_i) = \phi_k(\sum_{i=1}^{n} a_{k_i}x_i - \sum_{i=1}^{n} a_{k_i}y_i)$$

$$\sum_{i=1}^{n} \phi_k(\frac{a_{k_i}}{p^{e_k - e_i}}(x_i - y_i)) = 0$$

since $p^{e_k} \mid (x_i - y_i)$ when $k < i$ Next, since ϕ and A are both linear, it follows that $\psi(A)$ is linear. Therefore $\psi(A) \in End(1 + J)$ for all $A \in R_p$.

To prove surjectivity, of ψ, let $\omega_i = (0, ..., g_i, ..., 0)^T$ be the vector with g_i in the i^{th} component and zeros everywhere else. An endomorphism say $M \in E_p$ determined by where it sends each ω_i, however, there is no complete freedom in the mapping of these elements.

Now, suppose, $M(\omega_j) = (x_{1j}, ..., x_{nj})^T = \phi(x_{1j}, ..., x_{nj})^T$ for $x_{i,j} \in \mathbb{Z}$. Then, $0 = M(0) = M(p^{ej}\omega_j) = \underbrace{M\omega_j + ... + M\omega_j}_{p^{e_j}} = (p^{e_j}x_{1j}, ..., p^{e_j}x_{nj})$. Thus $p^{e_j} \mid p^{e_j}x_{ij}$ $\forall i, j$ and therefore $p^{e_i - e_j} \mid x_{ij}$ when $i \geq j$. Forming the matrix $B = (x_{ij}) \in R_p$ gives, $\psi(B) = M$ by construction and this proves that ψ is surjective

Finally, we need to prove that ψ is a ring homomorphism. Clearly, from the definition, $\psi(I) = id_{E_p}$ and that $\psi(A + B) = \psi(A)\psi(B)$. If $A, B \in R_p$, then, a straight forward calculation reveals that $\psi(AB)$ is the endomorphism composition $\psi(A) \circ \psi(B)$ by the properties of the matrix multiplication □

Remark 3.7. *Given this description of $E_p = End(1+J)$, we can, characterize, those endomorphisms giving rise to elements in $Aut(1 + J)$*

Lemma 3.8. *The kernel of ψ is given by the set of matrices $A = (a_{ij}) \in R_p$ such that $p^{e_i} \mid a_{ij}$ for all i, j*

Proof. Let $\omega_j = (0, ..., g_j, ..., 0)^T \in (1 + J)$ be the vector with g_j in the j^{th} component and zeros everywhere else. If $A = (a_{ij}) \in R_p$ has the property that each a_{ij} is divisible by p^{e_i}, then

$$\psi(A)\omega_j = (\phi_1(a_{ij}), ..., \phi_n(a_{nj})) = 0$$

In particular, since $x \in 1 + J$ is a $\mathbb{Z}-$linear combination of ω_j, it follows that $\phi(A)x = 0, \forall x \in 1 + J$. Thus $A \in ker(\psi)$.

Conversely, suppose $A = (a_{ij}) \in ker(\psi)$ is that $\psi(A)\omega_j = 0, \forall \omega_j$. Then, from the above above calculation, each a_{ij} is divisible by p^{e_i} □

Remark 3.9. *It is now clear that E_p which is the endomorphism of $(1 + J)$ is explicitly characterized as a quotient $R_p/ker(\psi)$*

Lemma 3.10. *Let $A \in \mathbb{Z}^{n\times n}$ such that $det(A) \neq 0$. Then, there exists a unique matrix $B \in \mathbb{Q}^{n\times n}$ called the adjugate of A such that $AB = BA = det(A)I$ and moreover, B has integer entries.*

Theorem 3.11. *An endomorphism $M = \psi(A)$ is an automorphism if and only if A(mod)$p \in GL_n(\mathbb{F}_p)$*

Proof. Fix a matrix $A \in R_p$ with $det(A) \neq 0$. It is well known that an adjugate of A say $B \in \mathbb{Z}^{n\times n}$ such that $AB = BA = det(A)I$. We need to show that B is actually an element of R_p.

Let $A = PA^{'}P^{-1}$ for some $A^{'} \in \mathbb{Z}^{n\times n}$ and $B^{'} \in \mathbb{Z}^{n\times n}$ be such that $A^{'}B^{'} =$

$B^{'}A^{'} = det(A^{'})I$. Notice that $det(A) = det(A^{'})$. Let $C = PB^{'}P^{-1}$ and observe that

$$AC = PA^{'}B^{'}P^{-1} = det(A)I = PB^{'}A^{'}P^{-1} = CA.$$

By the uniqueness of B, it follows that $B = C = PB^{'}P^{-1}$ and thus, B is in R_p as desired.

Now, suppose that $p \nmid det(A)$ so that $A(\text{mod})p \in GL_n(\mathbb{F}_p)$ and let $\lambda \in \mathbb{Z}$ be such that λ is inverse of $det(A)$ modulo p^{e_i}(such an integer exists since $(det(A), p^{e_n}) = 1$). Thus we have, $det(A) \cdot \lambda \equiv 1(\text{mod} p^{e_j})$ whenever $1 \leq j \leq n$.

Let B be the adjugate of A. Define an element of R_p by $A^{(-1)} := \lambda \cdot B$, whose image under ψ is the inverse of the endomorphism represented by A :

$$\psi(A^{(-1)}A) = \psi(AA^{(-1)} = \psi(\lambda \cdot det(A)I) = id_{E_p}$$

This proves that $\psi(A) \in Aut(1+)$. Conversely, if $\psi(A) = M$ and $\psi(C) = M^{-1} \in E_p$ exists, then, $\psi(AC - I) = \psi(AC) - id_{E_p} = 0$. Hence, $AC - I \in ker(\psi)$.

From the kernel calculation , it follows that $p \mid AC - I$ entry-wise and so, $AC \equiv I\text{mod}p$. Thus, $1 \equiv det(AC) \equiv det(A)det(C)\text{mod}p$. In particular, $p \nmid det(A)$ □

Proposition 3.12. *Let R be a Square radical zero finite commutative completely primary ring constructed in the previous section. Let the characteristic of R be p so that $1 + J = (\mathbb{Z}_p^r)^h$. Suppose, $B_p = \underbrace{\mathbb{Z}_p \times ... \times \mathbb{Z}_p}_{r} \subseteq 1 + J$, then we can construct R_p of B_p such that*

$$R_p = (a_{ij}) : p^{e_i - e_j} \mid a_{ij}, \forall i, j; 1 \leq j \leq i \leq r = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1r} \\ a_{21} & a_{22} & \cdots & a_{2r} \\ \vdots & \vdots & \vdots & \vdots \\ a_{r1} & a_{r2} & \cdots & a_{rr} \end{pmatrix} = M_r(\mathbb{Z}_p)$$

As a result, the following conditions hold:

(i) $End(B_p) \cong \psi(A) : A = (a_{ij}) \in M_r(\mathbb{Z}_p)$ and $\psi : M_r(\mathbb{Z}_p) \to End(B_p)$

(ii) $Aut(B_p) \in GL_r(\mathbb{Z}_p)$

(iii) $\mid Aut(B_p) \mid = \prod_{i=0}^{r-1}(p^r - p^i)$

Proof. The proof of (i) and (ii) follow from the previous results.

Now, consider $Aut(\underbrace{\mathbb{Z}_p \times ... \times \mathbb{Z}_p}_{r})$. We start with $Aut(\mathbb{Z}_p)$ and $Aut(\mathbb{Z}_p \times \mathbb{Z}_p)$ in order to obtain the size of the automorphism group of B_p. In $\mathbb{Z}_p$, each of the $p-1$ nonidentity elements has order p. Suppose $\mathbb{Z}_p =< a >$, then the map $a \mapsto a^i$ is an element of $Aut(\mathbb{Z}_p)$ provided $i \in [1, p-1]$. Thus $\mid Aut(\mathbb{Z}_p) \mid = p-1 = \Phi(p)$, where Φ is the Eulers'-phi function.

Next, let a and b each generate groups of order p, so that $\mathbb{Z}_p \times \mathbb{Z}_p =< a >< b >$. A homomorphism $\theta : \mathbb{Z}_p \times \mathbb{Z}_p \mapsto \mathbb{Z}_p \times \mathbb{Z}_p$ is an automorphism iff $\mid \theta(a) \mid = \mid \theta(b) \mid = p$ and $< \theta(a) >$ intersects with $< \theta(b) >$ only at identity.

To find $\mid \mathbb{Z}_p \times \mathbb{Z}_p \mid$, we must count the pairs $(\beta, \beta^{'})$ of elements in $\mathbb{Z}_p \times \mathbb{Z}_p$ such that $\theta(a) = \beta$ and $\theta(b) = \beta^{'}$ determines an automorphism. Each of the $p^2 - 1$ nonidentity elements of $\mathbb{Z}_p \times \mathbb{Z}_p$ has order p , so, a given element of $Aut(\mathbb{Z}_p \times \mathbb{Z}_p)$ may map a to any of the $p^2 - 1$ different places.

Let β be nonidentity element. We must count the elements $\beta^{'}$ of $\mathbb{Z}_p \times \mathbb{Z}_p$ such that $\beta^{'} = p$ and $< \beta > \cap < \beta^{'} > \{e\}$. Since each β generates a group of order p and any of the $p^2 - p$ elements of $\mathbb{Z}_p \times \mathbb{Z}_p$ lying outside of $< \beta >$ will generate a group of order p that intersects the group $< \beta >$ only at identity element, it follows that

$$\mid Aut(\mathbb{Z}_p \times \mathbb{Z}_p) \mid = (p^2 - 1)(p^2 - p)$$

For $B_p = \underbrace{\mathbb{Z}_p \times ... \times \mathbb{Z}_p}_{r}$, let $\{g_1, ..., g_r\}$ be a set of generators for B_p, so that

$$\underbrace{\mathbb{Z}_p \times ... \times \mathbb{Z}_p}_{r} =< g_1 > \times < g_2 > \times ... \times < g_r > .$$

Each of the nonidentity elements of B_p has order p. We now count the number of injective maps from the above generators to nonidentity elements that generate groups intersecting only at the identity element.

Suppose that an automorphism of B_p sends g_1 to some element β in B_p, then there are $p^r - p$ elements $\beta^{'}$ such that $< \beta > \cap < \beta^{'} >$. Supposing further that this automorphism is given by $g_1 \mapsto \beta$ and $g_2 \mapsto \beta^{'}$ for some $\beta^{'}$ not in $< \beta >$, there remain $p^r - p^2$ elements $\beta^{''} \in B_p$ that are outside of $< \beta > \times < \beta^{'} >$. Sending g_3 to any such $\beta^{''}$ gives $(< \beta >< \beta^{'} >) \cap < \beta^{''} > = \{e\}$.

Continuing in this manner, it is easy to specify where an automorphism of B_p sends the first n generators and then find $p^r - p^n$ elements in B_p to which the next generators might be sent. Thus

$$\mid Aut(\prod_{i=1}^{r} \mathbb{Z}_p) \mid = \mid Aut(B_p^{'}) \mid = \prod_{i=0}^{r-1} (p^r - p^i)$$

□

Lemma 3.13. *Consider R^* such that $Char(R) = p$, so that $1+J = \underbrace{\mathbb{Z}_p^r \times \mathbb{Z}_p^r \times .... \times \mathbb{Z}_p^r}_{h}$.*

Then

$$\textit{(i)}\ (R_p) = M_{hr}(\mathbb{Z}_p) = \begin{pmatrix} a_{11} & \cdots & a_{1r} & a_{1(r+1)} & \cdots & a_{1(2r)} & \cdots & a_{1(hr)} \\ a_{21} & \cdots & a_{2r} & a_{2(r+1)} & \cdots & a_{2(2r)} & \cdots & a_{2(hr)} \\ \vdots & \ldots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{r1} & \cdots & a_{rr} & a_{r(r+1)} & \cdots & a_{r(2r)} & \cdots & a_{r(hr)} \\ \vdots & \ldots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{(2r)1} & \cdots & a_{(2r)r} & a_{(2r)(r+1)} & \cdots & a_{(2r)(2r)} & \cdots & a_{(2r)(hr)} \\ \vdots & \ldots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{(hr)1} & \cdots & a_{(hr)r} & a_{(hr)(r+1)} & \cdots & a_{(hr)(2r)} & \cdots & a_{(hr)(hr)} \end{pmatrix}$$

(ii)$End(1+J) \cong \psi(A) : A = (a_{ij}) \in M_{rh}(\mathbb{Z}_p)$ *and* $\psi : M_{rh}(\mathbb{Z}_p) \to End(1+J)$

(iii) $Aut(1+J) \in GL_{hr}(\mathbb{Z}_p)$

Lemma 3.14. *Consider* R^* *such that* $Char(R) = p^2$ *so that* $1+J = \underbrace{\mathbb{Z}_p^r \times \mathbb{Z}_p^r \times .... \times \mathbb{Z}_p^r}_{h+1}$.

Then

$$\textit{(i)}\ (R_p) = M_{(h+1)r}(\mathbb{Z}_p) = \begin{pmatrix} a_{11} & \cdots & a_{1r} & a_{1(r+1)} & \cdots & a_{1(2r)} & \cdots & a_{1((h+1)r)} \\ a_{21} & \cdots & a_{2r} & a_{2(r+1)} & \cdots & a_{2(2r)} & \cdots & a_{2((h+1)r)} \\ \vdots & \ldots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{r1} & \cdots & a_{rr} & a_{r(r+1)} & \cdots & a_{r(2r)} & \cdots & a_{r((h+1)r)} \\ \vdots & \ldots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{(2r)1} & \cdots & a_{(2r)r} & a_{(2r)(r+1)} & \cdots & a_{(2r)(2r)} & \cdots & a_{(2r)((h+1)r)} \\ \vdots & \ldots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{((h+1)r)1} & \cdots & a_{(hr)r} & a_{(hr)(r+1)} & \cdots & a_{(hr)(2r)} & \cdots & a_{((h+1)r)((h+1)r)} \end{pmatrix}$$

(ii)$End(1+J) \cong \psi(A) : A = (a_{ij}) \in M_{r(h+1)}(\mathbb{Z}_p)$ *and* $\psi : M_{r(h+1)}(\mathbb{Z}_p) \to End(1+J)$

(iii) $Aut(1+J) \in GL_{(h+1)r}(\mathbb{Z}_p)$

4 Counting the Automorphisms of $1+J$ for both characteristics of R

4.1 For the characteristic of $R = p$

Since $Aut(1+J) \in GL_{hr}(\mathbb{Z}_p)$, we need to find all the elements of $GL_{hr}(\mathbb{Z}_p)$ that can be extended to a matrix in $End(1+J)$ and calculate the distinct ways of extending such an element to an endomorphism. So, we need all such matrices $M_{hr} \in End(1+J)$ that are invertible modulo p

Now, recall that $1+J=(\mathbb{Z}_p^r)^h$ and define the following numbers:

$$\alpha_k = max\{m : e_m = e_k\}, \beta_k = min\{m : e_m = e_k\}$$

Since $e_m = e_k$ for $m = k$, we have the two inequalities $\alpha_k \geq k$ and $\beta_k \leq k$

Note that $\beta_1 = \beta_2 = ... = \beta_{\alpha_1}$ and $\beta_{\alpha_1+1} = ... = \beta_{\alpha_{\alpha_1+1}}$, and so on. So we have

$$\beta_1 = \cdots = \beta_{\alpha_1} < \beta_{\alpha_1+1} < \beta_{\alpha_{\alpha_1}+1} = \cdots$$

Since $e_1 = e_2 = \cdots = e_n = e_{hr} = 1$, it follows that $n = hr$ and α_k coincides with β_k across all the values of i

Suppose the e_i are different, we can introduce the numbers $e_i^{'}, C_i, D_i$ as follows. Define the set of distinct numbers $\{e_i^{'}\}$ such that $\{e_i^{'}\} = \{e_j\}$ and $e_1^{'} < e_2^{'} < \cdots$

Let $l \in \mathbb{N}$ be the size of $\{e_i^{'}\}$. So, $e_1^{'} = e_1$, $e_2^{'} = e_{\alpha_1+1}, \cdots, e_l^{'} = e_n$. Now define

$$D_i = max\{m : e_m = e_i^{'}\}, C_i = min\{m : e_m = e_i^{'} : \{e_i^{'}\}$$

Note that $C_1 = 1$, and $D_l = n$. Also, define $C_{l+1} = n+1$

Now, for both of the considerations, the number of matrices say $A \in R_p$ that are invertible modulo p are upper block triangular matrices which may be expressed in the following three forms

$$A = \begin{pmatrix} m_{11} & & & & & & & & & * \\ \vdots & & & & & & & & & \\ m_{D_11} & \cdots & m_{D_1D_1} & & & & & & & \\ & & & m_{C_2C_2} & & & & & & \\ & & & \vdots & & & & & & \\ & & & m_{D_2C_2} & \cdots & m_{D_2D_2} & & & & \\ & & & & & & \ddots & & & \\ & & & & & & & m_{C_1C_1} & & \\ & & & & & & & \vdots & & \\ 0 & & & & & & & m_{D_lC_l} & \cdots & m_{D_lC_l} \end{pmatrix}$$

or

$$A = \begin{pmatrix} m_{11} & m_{12} & \cdots & m_{1(hr)} \\ \vdots & & & \\ m_{\alpha_11} & & & \\ & m_{\alpha_22} & & \\ & & \ddots & \\ 0 & & & m_{\alpha_{(hr)}hr} \end{pmatrix} = \begin{pmatrix} m_{1\beta_1} & & & & \\ & m_{2\beta_2} & & & \\ & & \ddots & & \\ 0 & & & m_{(hr)\beta_{(hr)}} & \cdots & m_{(hr)(hr)} \end{pmatrix}$$

The number of such A is $\prod_{k=1}^{hr}(p^{\alpha_k} - p^{k-1})$ since we require linearly independent columns. So, the first step of calculating $\mid Aut(1+J) \mid$ is done.

Next, we count the number of extensions of A to $Aut(1+J)$. To extend each entry m_{ij} from $m_{ij} \in \mathbb{Z}/p\mathbb{Z}$ to $a_{ij} \in p^{e_i - e_j}\mathbb{Z}/pe_i\mathbb{Z}$ if $e_i > e_j$, or $a_{ij} \in \mathbb{Z}/pe_i\mathbb{Z}$ if $e_i = e_j$, such that $a_{ij} \equiv m_{ij}(\text{mod})p$, we have pe_j ways to do so for the necessary zeros (that is , when $e_i > e_j$) as any element of $p^{e_i - e_j}\mathbb{Z}/pe_i\mathbb{Z}$ works.

Similarly, there are $pe_i - 1$ ways for the not necessarily zero entries (that is , when $e_i \leq e_j$) as any element of $p\mathbb{Z}/p^{e_i}\mathbb{Z}$ will do.

4.2 For the characteristic of $R = p^2$

This holds by induction from the previous consideration. Thus we have the following results:

Lemma 4.1. *The R be the a finite ring of the class of rings considered in the construction $(*)$ and R^* be its group of units. The following two conditions hold for both of the characteristics of R*

(i)When charR $= p$, the abelian group $1 + J = (\mathbb{Z}_p^r)^h$ has

$$\mid Aut(1+J) \mid = \prod_{k=1}^{hr}(p^{\alpha_k} - p^{k-1}) \prod_{j=1}^{hr}(p^{e_j})^{hr-\alpha_j} \prod_{i=1}^{hr}(p^{e_i - 1})^{hr-\beta_i+1}$$

(ii)When charR $= p^2$, the abelian group $1 + J = (\mathbb{Z}_p^r)^{h+1}$ has

$$\mid Aut(1+J) \mid = \prod_{k=1}^{(h+1)r}(p^{\alpha_k} - p^{k-1}) \prod_{j=1}^{(h+1)r}(p^{e_j})^{hr-\alpha_j} \prod_{i=1}^{(h+1)r}(p^{e_i - 1})^{(h+1)r-\beta_i+1}$$

Theorem 4.2. *Let R^* be the unit group of a class of finite rings described by construction $(*)$. Then*

(i) When Char$(R) = p$, $Aut(R^*) = Aut(\mathbb{Z}_{p^r} - 1) \times Aut(1+J)$

$$\mid Aut(R^*) \mid = \mid \mathbb{Z}_{p^r}^* - 1 \mid \times \mid Aut(B_p) \mid$$

$$= \Phi(p^r - 1) \cdot \prod_{k=1}^{hr}(p^{\alpha_k} - p^{k-1}) \prod_{j=1}^{hr}(p^{e_j})^{hr-\alpha_j} \prod_{i=1}^{hr}(p^{e_i - 1})^{hr-\beta_i+1}$$

(ii) When Char$(R) = p^2$, then

$$\mid Aut(R^*) \mid = \Phi(p^r - 1) \cdot \prod_{k=1}^{(h+1)r}(p^{\alpha_k} - p^{k-1}) \prod_{j=1}^{(h+1)r}(p^{e_j})^{hr-\alpha_j} \prod_{i=1}^{(h+1)r}(p^{e_i - 1})^{(h+1)r-\beta_i+1}$$

Acknowledgements. The first author acknowledges the co-authors for their meaningful and well done PhD supervision and their selflessness in giving scholarly comments and direction. May God bless you. A lot of thanks to Masinde Muliro University of Science and Technology for their financial support towards my research stay at the University of Kwazulu Natal, South Africa.

References

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

[2] A. Ranum (1907), *The group of classes of congruent matrices with application to the group of isomorphisms of any abelian groups* , Trans. Amer. Math. Soc. **8**, 71-91.

[3] C. J. Chikunji (2008), *On unit groups of completely primary finite rings*, Mathematical Journal of Okayama University, **50**, 149-160.

[4] C. Hillar and D. Rhea (2007), *Automorphisms of an abelian $p-$group*, Amer. Math. Monthly, **114**, 917-922.

[5] K.Shoda (1928), *Uber die Automorphismen einer endlichen Abelschen Gruppe*, Math. Ann., **100**, 674-686.

[6] Maurice O. Oduor, Michael O. Ojiema and Mmasi Eliud (2013),*Units of commutative completely primary finite rings of characteristic p^n*, International Journ. of Algebra, **7**(6), 259-266.

Received: February 04, 2016