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

Ojiema, Michael Onyango

http://hdl.handle.net/190/311
Downloaded from DSpace Repository, DSpace Institution's institutional repository
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_ajiema@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

Copyright © Ojiema Michael Onyango, Owino Maurice Oduor and Odhiambo Paul Oleche. This article is distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

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 $\phi : R^* \to R^*$ 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 \( R = R_o \oplus U \) is an additive group. On this group, define multiplication by the following relation

\[
(*) \quad pu_i = u_iu_j = u_ju_i = 0, \quad u_ir_o = (r_o)^{\sigma_i}u_i
\]
where \( r_0 \in R_0, 1 \leq i, j \leq h, p \) is a prime integer, \( n \) and \( r \) are positive integers and \( \sigma_i \) 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, \( pu_i = u_iu_j = 0 \).

From the given multiplication in \( R \), we see that if \( r_0 + \sum_{i=1}^{h} \lambda_i u_i \) and \( s_0 + \sum_{i=1}^{h} \gamma_i u_i \), \( r_0, s_0 \in R_0 \), \( \lambda_i, \gamma_i \in F_0 \) are elements of \( R \), then,

\[
(r_0 + \sum_{i=1}^{h} \lambda_i u_i)(s_0 + \sum_{i=1}^{h} \gamma_i u_i) = r_0s_0 + \sum_{i=1}^{h} \{(r_0 + pR_0)\gamma_i + \lambda_i(s_0 + pR_0)\sigma_i\}u_i
\]

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 \( \text{Aut}(R^*) \). We find all the elements of \( \text{GL}_{hr}(\mathbb{Z}_p) \) that can be extended to a matrix in \( \text{End}(B_p) \) 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 \( \text{Char} R = p \), then

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

(ii) If \( \text{Char} R = p^2 \) then,

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

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, \( \text{Aut}(H) \times \text{Aut}(K) \cong \text{Aut}(H \times K) \)

**Proposition 2.3.** Let \( R^* = \mathbb{Z}_{p^r - 1} \times 1 + J \). Since \( g.c.d(p^r - 1, |1 + J|) = 1 \), \( \text{Aut}(R^*) \cong \text{Aut}(\mathbb{Z}_{p^r - 1} \times 1 + J) = \text{Aut}(\mathbb{Z}_{p^r - 1}) \times \text{Aut}(1 + J) \)
Proof. Let $\theta : \text{Aut}(\mathbb{Z}_{p^r-1}) \times \text{Aut}(1+J) \to \text{Aut}(\mathbb{Z}_{p^r-1} \times 1 + J)$ be a homomorphism. Suppose $\theta_1 \in \text{Aut}(\mathbb{Z}_{p^r-1})$ and $\theta_2 \in \text{Aut}(1+J)$, 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 $\text{id}_1 \in \text{Aut}(\mathbb{Z}_{p^r-1})$ and $\text{id}_2 \in \text{Aut}(1+J)$ be the identity automorphisms of $\mathbb{Z}_{p^r-1}$ and $1+J$ respectively. To show that, $\theta$ is indeed a homomorphism, notice that $\theta(\text{id}_1, \text{id}_2) = \text{Id}_{(\mathbb{Z}_{p^r-1} \times 1+J)}$ and that, $\theta(\theta_1', \theta_2')(x, y) = (\theta_1'(x), \theta_2'(y))$

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

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

Let $n = p^r - 1 = |\mathbb{Z}_{p^r-1}|$ and $m = |1 + J|$ such that $(n, m) = 1$. Write $\phi_{\mathbb{Z}_{p^r-1}}$ and $\phi_{1+J}$ 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 $\theta' \in \text{Aut}(\mathbb{Z}_{p^r-1} \times 1 + J)$ and consider the homomorphism $\alpha : 1 + J \to \mathbb{Z}_{p^r-1}$ given by $\alpha(y) = \phi_{\mathbb{Z}_{p^r-1}}(\theta'(\text{id}_1, y))$.

Notice that $\{y^n : y \in 1 + J\} \subseteq \ker(\alpha)$ since $\text{id}_1 = \phi_{\mathbb{Z}_{p^r-1}}(\theta'(\text{id}_1, y))^n = \phi_{\mathbb{Z}_{p^r-1}}(\theta'(\text{id}_1, y)^n) = \phi_{\mathbb{Z}_{p^r-1}}(\theta'(\text{id}_1, y^n)) = \alpha(y^n)$

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 $\alpha$ is the trivial homomorphism. Similarly, $\delta : \mathbb{Z}_{p^r-1} \to 1 + J$ and $\delta(x) = \phi_{1+J}(\theta'(x, \text{id}_2))$ is trivial.

Finally, define endomorphisms of $\mathbb{Z}_{p^r-1}$ and $1+J$ by; $\theta'(x) = \phi_{\mathbb{Z}_{p^r-1}}(\theta'(x, \text{id}_2))$, $\theta'_{1+J}(y) = \phi_{1+J}(\theta'(\text{id}_1, y))$. From this construction and the above argument, we have $\theta'(x, y) = \theta'(x, \text{id}_2) \cdot \theta'(\text{id}_1, y) = (\theta'_{\mathbb{Z}_{p^r-1}}(x), \theta'_{1+J}(y)) = (\theta'_{\mathbb{Z}_{p^r-1}}, \theta'_{1+J})(x, y)$ for all $x \in \mathbb{Z}_{p^r-1}$ and $y \in 1 + J$.

It remains to prove that $\theta'_{\mathbb{Z}_{p^r-1}} \in \text{Aut}(\mathbb{Z}_{p^r-1})$ and $\theta'_{1+J} \in \text{Aut}(1 + J)$ 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 $\theta'_{\mathbb{Z}_{p^r-1}}(x) = \text{id}_1$ for some $x \in \mathbb{Z}_{p^r-1}$. Then, $\theta'(x, \text{id}_2) = (\theta'_{\mathbb{Z}_{p^r-1}}(x), \theta'_{1+J}((\text{id}_1, \text{id}_2)) = (\text{id}_1, \text{id}_2)$. So, $x = \text{id}_1$ by injectivity of $\theta'$. A similar argument shows that $\theta'_{1+J} \in \text{Aut}(1 + J)$ and this completes the proof. \qed

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 $\text{Aut}(\mathbb{Z}_{p^r-1}) \cong (\mathbb{Z}_{p^r-1})^*$, it implies that

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

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

Lemma 2.5. Let $\text{Char}(R) = p$, $p$ a prime integer and $B_p = 1 + J = (\mathbb{Z}_p^r)^r$. Then, $|B_p| = p^nh$. 
Proof. If \( B_p = \prod_{i=1}^{r} \mathbb{Z}/p^{e_i} \mathbb{Z} \) such that \( 1 \leq e_1 \leq e_2 \leq \ldots \leq e_r \), then, it is well known that \( |B_p| = \prod_{i=1}^{r} |\mathbb{Z}/p^{e_i} \mathbb{Z}| = p^{\sum_{i=1}^{r} e_i} \). Now, since \( e_1 = e_2 = \ldots = e_r = 1 \) and there are \( h \) tuples of such \( r \) factors of \( e_r \), it follows that \( (\sum_{i=1}^{r} e_i)^h = rh \). Thus \( |B_p| = p^{rh} \) as required.

Remark 2.6. Now, suppose \( G \cong \prod_{i=1}^{h} B'_{p} \) such that \( B'_{p} = \mathbb{Z}/p \mathbb{Z} \times \mathbb{Z}/p \mathbb{Z} \times \ldots \times \mathbb{Z}/p \mathbb{Z} \) over distinct set of primes \( p \) then \( \text{Aut}(G) = \prod \text{Aut}(B'_{p}) \).

In the sequel, we determine \( \text{Aut}(I + J) \) for both the characteristics of \( R \).

### 3 The Endomorphism Rings of the group \( 1 + J \)

For a successful characterization of \( \text{Aut}(R^*) \), 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 \( A, B \in \text{End}(1 + J) \) and \( x \in 1 + J \).

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

#### 3.1 Characteristic of \( R = p, p^2 \)

**Proposition 3.1.** Let \( R \) be a finite ring whose additive group \( (R, +) \) is of type \( (p^{e_1}, p^{e_2}, \ldots, p^{e_l}) : e_1 \geq e_2 \geq \ldots \geq e_l \). 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.

\[
(a_{ij}) = \begin{pmatrix}
    a_{11} & a_{12} & \cdots & a_{1l} \\
    p^{e_1-e_2}a_{21} & a_{22} & \cdots & a_{2l} \\
    \vdots & \vdots & \ddots & \vdots \\
    p^{e_1-e_l}a_{l1} & \cdots & \cdots & a_{ll}
\end{pmatrix}
\]

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 $1 + J = \mathbb{Z}_p \times \mathbb{Z}_p^2 \times \mathbb{Z}_p^3 \times \mathbb{Z}_p^4$.

Let $\psi : \mathbb{Z}_p \to \mathbb{Z}_p^4$ be a homomorphism given by $\psi : a \mapsto (pa_{21}, pa_{22}, pa_{31}, pa_{32})$. Thus generally, when $1 + J = \mathbb{Z}_p \times \cdots \times \mathbb{Z}_p$

We need to verify that $\psi(1 + J) = \mathbb{Z}_p$. Let $\phi : \mathbb{Z}_p^4 \to \mathbb{Z}_p^4$ be defined by $\phi((x_1, x_2, x_3, x_4)) = (x_1, x_2, x_3, x_4)$. Then, $E_p$ is a multiplication by a matrix $A \in R_p$ on a vector of integer representatives followed by an application of $\phi$.

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

Proof. Let $A = (a_{ij}) \in R_p$. The condition that $p^{e_i - e_j} | a_{ij}$ 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 $P = \text{diag}(p^{e_1}, \ldots, p^{e_n})$ 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 $\phi : \mathbb{Z}^n \to \mathbb{Z}/p^k\mathbb{Z}$ be defined by $x \mapsto x \mod p^k$. Let $\phi : \mathbb{Z}^n \to 1 + J$ be a homomorphism given by $\phi(x_1, \ldots, x_n)^T = (\phi_1(x_1), \ldots, \phi_n(x_n))^T = (x_1, \ldots, x_n)^T$. Then, $E_p$ is a multiplication by a matrix $A \in R_p$ on a vector of integer representatives followed by an application of $\phi$.

Theorem 3.6. [4] The map $\psi : R_p \to E_p$ given by $\psi(A)(x_1, \ldots, x_n)^T = \phi(A(x_1, \ldots, x_n)^T)$ 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 $(x_1, \ldots, x_n)^T = (y_1, \ldots, y_n)^T$ 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 $\phi(A(x_1, \ldots, x_n)^T) - \phi(A(y_1, \ldots, y_n)^T)$ is

$$
\phi_k\left(\sum_{i=1}^{n} a_{ki}x_i\right) - \phi_k\left(\sum_{i=1}^{n} a_{ki}y_i\right) = \phi_k\left(\sum_{i=1}^{n} a_{ki}x_i - \sum_{i=1}^{n} a_{ki}y_i\right),
$$

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

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


To prove surjectivity, of \( \psi \), let \( \omega_i = (0, \ldots, g_i, \ldots, 0)^T \) 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 \( \omega_i \), however, there is no complete freedom in the mapping of these elements.

Now, suppose, \( M(\omega_j) = (x_{1j}, \ldots, x_{nj})^T = \phi(x_{1j}, \ldots, x_{nj})^T \) for \( x_{ij} \in \mathbb{Z} \). Then, \( 0 = M(0) = M(p^{e_j}\omega_j) = M\omega_j + \cdots + M\omega_j = (p^{e_j}x_{1j}, \ldots, p^{e_j}x_{nj}) \). 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 \( \psi \) is surjective.

Finally, we need to prove that \( \psi \) 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 \( \square \)

**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 \( \psi \) 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 \( \omega_j = (0, \ldots, g_j, \ldots, 0)^T \in (1+J) \) 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

\[
\psi(A)\omega_j = (\phi_1(a_{ij}), \ldots, \phi_n(a_{nj})) = 0
\]

In particular, since \( x \in 1+J \) is a \( \mathbb{Z} \)-linear combination of \( \omega_j \), 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 \( p^{e_i} \) \( \square \)

**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 \( A \equiv \det(A) \in GL_n(F_p) \)

**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 \( A'B' = \)
As a result, the following conditions hold:

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

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

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

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

Now, consider \( \text{Aut}(\mathbb{Z}_p \times \ldots \times \mathbb{Z}_p) \). We start with \( \text{Aut}(\mathbb{Z}_p) \) and \( \text{Aut}(\mathbb{Z}_p \times \mathbb{Z}_p) \) in order to obtain the size of the automorphism group of \( B_p \). In \( \mathbb{Z}_p \), each

\( B' A' = \det(A')I \). 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 \( \lambda \) is inverse of \( \det(A) \) modulo \( p^e \) (such an integer exists since \( (\det(A), p^e) = 1 \)). Thus we have, \( \det(A) \cdot \lambda \equiv 1 \pmod{p^e} \) 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 \( \psi \) is the inverse of the endomorphism represented by \( A \):

\[ \forall A(\psi) = \psi(A^{(-1)}) = \psi(\lambda \cdot \det(A)I) = \text{id}_{E_p} \]

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

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

**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 \( 1 + J = (\mathbb{Z}_p)^h \). Suppose, \( B_p = \mathbb{Z}_p \times \ldots \times \mathbb{Z}_p \subseteq 1 + J \), then

we can construct \( R_p \) of \( B_p \) such that

\[ R_p = (a_{ij}) : p^{e_i - e_j} | a_{ij}, \forall i, j; 1 \leq j \leq i \leq r = \left( \begin{array}{cccc} a_{11} & a_{12} & \cdots & a_{1r} \\ a_{21} & a_{22} & \cdots & a_{2r} \\ \vdots & \vdots & \ddots & \vdots \\ a_{r1} & a_{r2} & \cdots & a_{rr} \end{array} \right) = M_r(\mathbb{Z}_p) \]

As a result, the following conditions hold:

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

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

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

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

Now, consider \( \text{Aut}(\mathbb{Z}_p \times \ldots \times \mathbb{Z}_p) \). We start with \( \text{Aut}(\mathbb{Z}_p) \) and \( \text{Aut}(\mathbb{Z}_p \times \mathbb{Z}_p) \) 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 $\mathbb{Z}_p = \langle a \rangle$, then the map $a \mapsto a^i$ is an element of $\text{Aut}(\mathbb{Z}_p)$ provided $i \in [1, p - 1]$. Thus $|\text{Aut}(\mathbb{Z}_p)| = p - 1 = \Phi(p)$, where $\Phi$ is the Euler’s-Euler function.

Next, let $a$ and $b$ each generate groups of order $p$, so that $\mathbb{Z}_p \times \mathbb{Z}_p = \langle a \rangle \times \langle b \rangle$. A homomorphism $\theta : \mathbb{Z}_p \times \mathbb{Z}_p \to \mathbb{Z}_p \times \mathbb{Z}_p$ is an automorphism iff $|\theta(a)| = |\theta(b)| = p$ and $\langle \theta(a) \rangle \cap \langle \theta(b) \rangle = \langle e \rangle$ only at identity.

To find $|\mathbb{Z}_p \times \mathbb{Z}_p|$, 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 $\text{Aut}(\mathbb{Z}_p \times \mathbb{Z}_p)$ may map $a$ to any of the $p^2 - 1$ different places.

Let $\beta$ be nonidentity element. We must count the elements $\beta'$ of $\mathbb{Z}_p \times \mathbb{Z}_p$ such that $\beta' = p$ and $\langle \beta \rangle \cap \langle \beta' \rangle = \{e\}$. Since each $\beta$ 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 $\langle \beta \rangle$ will generate a group of order $p$ that intersects the group $\langle \beta \rangle$ only at identity element, it follows that

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

For $\mathcal{B}_p = \mathbb{Z}_p \times \cdots \times \mathbb{Z}_p$, let $\{g_1, \ldots, g_r\}$ be a set of generators for $\mathcal{B}_p$, so that

$$\mathbb{Z}_p \times \cdots \times \mathbb{Z}_p = \langle g_1 \rangle \times \langle g_2 \rangle \times \cdots \times \langle g_r \rangle.$$ 

Each of the nonidentity elements of $\mathcal{B}_p$ 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 $\mathcal{B}_p$ sends $g_1$ to some element $\beta$ in $\mathcal{B}_p$, then there are $p^r - p$ elements $\beta'$ such that $\langle \beta \rangle \cap \langle \beta' \rangle$. Supposing further that this automorphism is given by $g_1 \mapsto \beta$ and $g_2 \mapsto \beta'$ for some $\beta'$ not in $\langle \beta \rangle$, there remain $p^r - p^2$ elements $\beta'' \in \mathcal{B}_p$ that are outside of $\langle \beta \rangle \times \langle \beta' \rangle$. Sending $g_3$ to any such $\beta''$ gives $(\langle \beta \rangle \langle \beta' \rangle) \cap \langle \beta'' \rangle = \{e\}$.

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

$$|\text{Aut}(\prod_{i=1}^{r} \mathbb{Z}_p)| = |\text{Aut}(\mathcal{B}_p')| = \prod_{i=0}^{r-1} (p^r - p^i)$$

\[ \square \]

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

\[(R_p) = M_{hr}(\mathbb{Z}_p) = \begin{pmatrix}
  a_{11} & \cdots & a_{1r} & a_{1(r+1)} & \cdots & a_{1(2r)} & \cdots & a_{1(hr)} \\
  a_{21} & \cdots & a_{2r} & a_{2(r+1)} & \cdots & a_{2(2r)} & \cdots & a_{2(hr)} \\
  \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\
  a_{r1} & \cdots & a_{rr} & a_{r(r+1)} & \cdots & a_{r(2r)} & \cdots & a_{r(hr)} \\
  \vdots & \cdots & \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\
  \end{pmatrix}
\]

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

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

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

Then

\[(R_p) = M_{(h+1)r}(\mathbb{Z}_p) = \begin{pmatrix}
  a_{11} & \cdots & a_{1r} & a_{1(r+1)} & \cdots & a_{1(2r)} & \cdots & a_{1((h+1)r)} \\
  a_{21} & \cdots & a_{2r} & a_{2(r+1)} & \cdots & a_{2(2r)} & \cdots & a_{2((h+1)r)} \\
  \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\
  a_{r1} & \cdots & a_{rr} & a_{r(r+1)} & \cdots & a_{r(2r)} & \cdots & a_{r((h+1)r)} \\
  \vdots & \cdots & \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\
  \end{pmatrix}
\]

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

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

4 Counting the Automorphisms of \( 1+J \) for both characteristics of \( R \)

4.1 For the characteristic of \( R = p \)

Since \( \text{Aut}(1+J) \in GL_{hr}(\mathbb{Z}_p) \), we need to find all the elements of \( GL_{hr}(\mathbb{Z}_p) \) that can be extended to a matrix in \( \text{End}(1+J) \) and calculate the distinct ways of extending such an element to an endomorphism. So, we need all such matrices \( M_{hr} \in \text{End}(1+J) \) 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 $\beta_1 = \beta_2 = \ldots = \beta_{\alpha_1}$ and $\beta_{\alpha_1+1} = \ldots = \beta_{\alpha_1+1}$, and so on. So we have

$$\beta_1 = \ldots = \beta_{\alpha_1} < \beta_{\alpha_1+1} < \beta_{\alpha_1+1} = \ldots$$

Since $e_1 = e_2 = \ldots = e_n = e_{hr} = 1$, it follows that $n = hr$ and $\alpha_k$ coincides with $\beta_k$ 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 $e'_1 < e'_2 < \ldots$

Let $l \in \mathbb{N}$ be the size of $\{e'_i\}$. So, $e'_1 = e_1, e'_2 = e_{\alpha_1+1}, \ldots, e'_l = e_n$. 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 $D_1 = n$. 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

$$A = \begin{pmatrix}
 m_{11} & & & * \\
 & \ddots & & \\
 m_{D_11} & \cdots & m_{D_1D_1} & \\
 & & \ddots & \\
 0 & & & \ddots
\end{pmatrix}$$

or

$$A = \begin{pmatrix}
 m_{11} & m_{12} & \cdots & m_{1(hr)} \\
 & \ddots & & \\
 m_{\alpha_11} & & \cdots & \\
 0 & & & \ddots
\end{pmatrix} = \begin{pmatrix}
 m_{1\beta_1} & & & \\
 & m_{2\beta_2} & & \\
 & & \ddots & \\
 0 & & & m_{(hr)\beta_{(hr)}} & \cdots & m_{(hr)(hr)}
\end{pmatrix}$$
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 $\text{char} R = p$, the abelian group $1 + J = (\mathbb{Z}_p^r)^h$ has

$$| \text{Aut}(1 + J) | = \prod_{k=1}^{hr} (p^{ak_k} - p^{k-1}) \prod_{j=1}^{hr} (p^{ej_j})^{hr-\alpha_j} \prod_{i=1}^{hr} (p^{ei_i-1})^{hr-\beta_i+1}$$

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

$$| \text{Aut}(1 + J) | = \prod_{k=1}^{(h+1)r} (p^{ak_k} - p^{k-1}) \prod_{j=1}^{(h+1)r} (p^{ej_j})^{hr-\alpha_j} \prod_{i=1}^{(h+1)r} (p^{ei_i-1})^{(h+1)r-\beta_i+1}$$

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

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

$$| \text{Aut}(R^*) | = | \mathbb{Z}_{p^r}^* - 1 | \times | \text{Aut}(B_n) |$$

$$= \Phi(p^r - 1) \cdot \prod_{k=1}^{hr} (p^{ak_k} - p^{k-1}) \prod_{j=1}^{hr} (p^{ej_j})^{hr-\alpha_j} \prod_{i=1}^{hr} (p^{ei_i-1})^{hr-\beta_i+1}$$

(ii) When $\text{Char}(R) = p^2$, then

$$| \text{Aut}(R^*) | = \Phi(p^r - 1) \cdot \prod_{k=1}^{(h+1)r} (p^{ak_k} - p^{k-1}) \prod_{j=1}^{(h+1)r} (p^{ej_j})^{hr-\alpha_j} \prod_{i=1}^{(h+1)r} (p^{ei_i-1})^{(h+1)r-\beta_i+1}$$
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


Received: February 04, 2016