ON THE REGULAR ELEMENTS OF RINGS IN WHICH THE PRODUCT OF ANY TWO ZERO DIVISORS LIES IN THE GALOIS SUBRING

Owino Maurice Odour\textsuperscript{1}§, Omamo Aggrey Libendi\textsuperscript{2}, Musoga Christopher\textsuperscript{3}

\textsuperscript{1}Department of Mathematics and Computer Science
University of Kabianga
P.O. Box 2030-20200, Kericho, KENYA
\textsuperscript{2,3}Department of Mathematics
Masinde Muliro University of Science and Technology
P.O. Box 190-50100, Kakamega, KENYA

Abstract: Suppose $R$ is a completely primary finite ring in which the product of any two zero divisors lies in the Galois (coefficient) subring. We construct $R$ and find a generalized characterization of its regular elements.

AMS Subject Classification: 13M05, 16P10, 16U60, 13E10, 16N20

Key Words: unit groups, completely primary finite rings

1. Introduction

Unless otherwise stated, $J(R)$ shall denote the Jacobson radical of a completely primary finite ring $R$. We shall denote the coefficient (Galois) subring of $R$ by $R'$. The set of all the regular elements in $R$ shall be denoted by $V(R)$. The rest of the notations shall be adopted from [1].

An element $x \in R$ is called regular if there exists $y \in R$ such that $x = x^2y$. The element $y$ is called a von Neumann inverse of $x$, see e.g [2]. It is well known that in any local ring, a regular element is either a unit or zero. Further details on the classes of completely primary finite rings considered in this work may be

Received: January 28, 2013
§Correspondence author
obtained in [3] and [4].

2. The Construction

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 $n = 2$, then $u_i u_j = pu_{ij}, u_i^3 = u_i u_j^2 = 0, u_i r' = (r')^{\sigma_i} u_i$

(ii) If $n \geq 3$, then $\beta_{ij} u_i = 0, u_i u_j = p^{n-1} \beta_{ij}, u_i^n = u_i^{n-1} u_j = u_i u_j^{n-1} = 0, u_i r' = (r')^{\sigma_i} u_i,$

where $r', \alpha_{ij} \in R', \beta_{ij} \in R'/pR', 1 \leq i, j \leq h$ and $\sigma_i$ is the automorphism associated with $u_i$. Further, let $pu_i = u_i u_j = 0$, when $u_i \in U$.

From the given multiplication in $R$, we notice that $r', s' \in R', \gamma_i, \lambda_i \in F_0$ are elements of $R$, then

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

\[
= r' s' + p^{n-1}\sum_{i,j=1}^{h} \xi_{ij}(\lambda_i (\gamma_j)^{\sigma_i} + pR') + \sum_{i=1}^{h}[(r' + pR')^{\sigma_i}][\gamma_i + \lambda_i (s' + pR')^{\sigma_i}]u_i
\]

where $r', s' \in R', \lambda_i, \gamma_i \in F_0, \xi_{ij} \in R'/pR'$. It is easy to verify that the given multiplication turns $R$ into a ring with identity $(1, 0, ..., 0)$. We also notice that $p^{n-1} \in (J(R))^2$ when $\text{char} R = \text{char} R' = p^n, n \geq 2$. Specifically, $p \in (J(R))^2$ when $n = 2$.

3. Preliminary Results

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

**Proof.** It is evident \(\square\)

**Remark:** If $n = 2$, then the construction yields rings satisfying the properties

$J(R) = pR' \oplus U$
\[(J(R))^2 = pR'
\]
\[(J(R))^3 = (0).\]

On the other hand, if \( n \geq 3 \), then \( J(R) = pR' \oplus U \)

\[(J(R))^{n-1} = p^{n-1}R'\]
\[(J(R))^n = (0).\]

Now, consider a commutative ring \( R \) from the class of rings described by the construction, we notice that

\[R = \bar{R} \oplus \sum_{i=1}^{h} \bar{R}'u_i\]

\[J(R) = pR' \oplus \sum_{i=1}^{h} R'u_i.\]

So

\[1 + J(R) = 1 + pR' \oplus \sum_{i=1}^{h} R'u_i.\]

Further, \( V(R) = R^* \cup \{0\} = (R^*/1 + J(R)).(1 + J(R)) \cup \{0\} = < a > .(1 + J(R)) \cup \{0\} \cong < a > \times (1 + J(R)) \cup \{0\}. \) It therefore suffices to determine the structure of \( 1 + J(R) \).

**Proposition 1.** For each prime integer \( p \), \( 1 + pR' \) is a subgroup of \( 1 + J(R) \).

**Proposition 2.** For each prime integer \( p \), \( 1 + pR' \oplus R'u_1 \) is a subgroup of \( 1 + J(R) \).

**Proposition 3.** For each \( 1 \leq j \leq h \), \( 1 + \sum_{j=1}^{h} \oplus R'u_j \) is a subgroup of \( 1 + J(R) \).

Since the two sided annihilator \( \text{ann}(J(R)) = p^{n-1}R' \), we state the following result

**Proposition 4.** \( 1 + \text{ann}(J(R)) \leq 1 + pR' \leq 1 + J(R). \)

**Proof.** It suffices to prove that \( 1 + \text{ann}(J(R)) \leq 1 + pR' \). Clearly \( 1 + \text{ann}(J(R)) = 1 + p^{n-1}R', \forall n \geq 2. \) Now, for \( r', s' \in R \), let \( 1 + p^{n-1}r', 1 + p^{n-1}s' \in 1 + \text{ann}(J(R)). \) Then

\[(1 + p^{n-1}r')(1 + p^{n-1}s')^{-1}\]
\[
= (1 + p^{n-1}r')(1 - p^{n-1}s') \\
= 1 + p^{n-1}(r' - s') \in 1 + \text{ann}(J(R))
\]

\[\square\]

**Proposition 5.** Let \( p = 2 \). Then the 2-group \( 1 + J(R) \) is a direct product of the subgroups \( 1 + pR' \oplus R'u_1 \) by \( 1 + \sum_{i=1}^h R'u_i \), with \( h \geq 2 \).

**Proposition 6.** Let \( p \neq 2 \). The \( p \)-group \( 1 + J(R) \) is a direct product of the subgroups \( 1 + pR' \) by \( 1 + \sum_{i=1}^h R'u_i \).

**Proposition 7.** Let \( U \) be a finitely generated \( R' \)-module. If \( U \) is generated by \( \{u_1, \ldots, u_h\} \), then \( \{u_1, u_1 + u_2, \ldots, u_{h-1} + u_h\} \) also generates \( U \).

**Proof.** If \( U \) is a finitely generated \( R' \)-module, then there exist \( \alpha_1, \ldots, \alpha_h \in R' \), such that every \( u \in U \) can be expressed in the form \( u = \sum_{i=1}^h \alpha_i u_i \). But \( \sum_{i=1}^h \alpha_i u_i = (\alpha_1 - \alpha_2 + \ldots + (-1)^{h+1}\alpha_h)u_1 + (\alpha_2 - \alpha_3 + \ldots + (-1)^h\alpha_h)(u_1 + u_2) + \ldots + (\alpha_{h-1} - \alpha_h)(u_{h-2} + u_{h-1}) + \alpha_h(u_{h-1} + u_h) \). Since all the coefficients \( \alpha_1 - \alpha_2 + \ldots + (-1)^{h+1}\alpha_h, \alpha_2 - \alpha_3 + \ldots + (-1)^h\alpha_h, \ldots, \alpha_{h-1} - \alpha_h \) and \( \alpha_h \) belong to \( R' \), it follows that \( \{u_1, u_1 + u_2, \ldots, u_{h-1} + u_h\} \) generates \( U \).

**Proposition 8.** Let \( R \) be a commutative finite ring from the class of finite rings described by the construction. If \( U \) is generated by \( \{u_1, \ldots, u_h\} \), then it is also generated by \( \{u_1, u_1 + u_2, \ldots, u_1 + u_2 + \ldots + u_h\} \).

### 4. Main Results

**Proposition 9.** Let \( R \) be a commutative finite ring from the class of finite rings described by the construction. If \( h \geq 1 \) and \( \text{char}R = p^2 \), then

\[1 + J(R) \cong \begin{cases} 
\mathbb{Z}_p \times (\mathbb{Z}_p)^{h-1} & \text{if } p = 2 \\
\mathbb{Z}_p \times (\mathbb{Z}_p)^h & \text{if } p \neq 2 
\end{cases}\]

**Proof.** Let \( \lambda_1, \ldots, \lambda_r \in R' \) with \( \lambda_1 = 1 \) such that \( \lambda_1, \ldots, \lambda_r \in \mathbb{R}'/pR' \) form a basis for \( \mathbb{R}'/pR' \) regarded as a vector space over its prime subfield \( GF(p) \). Since the two cases do not overlap, we treat them in turn.

**Case (i):** \( p = 2 \).

We notice that, for every \( \nu = 1, \ldots, r \) and \( u_1 \in J(R) - (J(R))^2 \),

\[(1 + \lambda_\nu u_1)^2 = 1 + 2\lambda_\nu^2 + 2\lambda_\nu u_1 \]

\[= 1 + 2\lambda_\nu^2 , \text{since } 2 \in (J(R))^2 \text{and } 2u_1 = 0.\]
Now,

$$(1 + 2\lambda_{\nu}^2)(1 + \lambda_{\nu}u_1) = 1 + 2\lambda_{\nu}^2 + (\lambda_{\nu} + 2\lambda_{\nu}^3)u_1 = 1 + 2\lambda_{\nu}^2 + \lambda_{\nu}u_1,$$

since $2 \in (J(R))^2$ and $2u_1 = 0$.

But then,

$$(1 + 2\lambda_{\nu}^2 + \lambda_{\nu}u_1)(1 + \lambda_{\nu}u_1) = 1 + 2^2\lambda_{\nu}^2 + 2(\lambda_{\nu} + \lambda_{\nu}^3)u_1 = 1,$$

since $2 \in (J(R))^2$ and $2u_1 = 0$.

Also, for each $u_i \in J(R) - (J(R))^2, 1 \leq i \leq h - 1$, $(1 + \lambda_{\nu}u_i + \lambda_{\nu}u_{i+1})^2 = 1 + 2(2\lambda_{\nu}^2) + 2\lambda_{\nu}(u_i + u_{i+1}) = 1$, since $(J(R))^3 = (0)$ so that $2^3 = 0, 2u_i = 2u_{i+1} = 0$, as $2 \in (J(R))^2$.

So, for each $\nu = 1, \ldots, r$ and $1 \leq i \leq h - 1$, $(1 + \lambda_{\nu}u_i)^4 = 1$, $(1 + \sum_{i=1}^{h-1} \lambda_{\nu}(u_i + u_{i+1}))^2 = 1$.

For positive integers $\alpha_{\nu}, \beta_{i\nu}$ with $\alpha_{\nu} \leq 4, \beta_{i\nu} \leq 2$ $(1 \leq i \leq h - 1, 1 \leq \nu \leq r)$, we notice that the equation

$$\prod_{\nu=1}^{r} \{(1 + \lambda_{\nu}u_1)^{\alpha_{\nu}}\} \prod_{i=1}^{h-1} \prod_{\nu=1}^{r} \{(1 + \lambda_{\nu}(u_i + u_{i+1}))^{\beta_{i\nu}}\} = \{1\}$$

will imply $\alpha_{\nu} = 4$ and $\beta_{i\nu} = 2, 1 \leq i \leq h - 1$. If we set

$$T_{\nu} = \{(1 + \lambda_{\nu}u_1)^{\alpha} \mid \alpha = 1, \ldots, 4\},$$

$$S_{i\nu} = \{(1 + \lambda_{\nu}(u_i + u_{i+1})^{\beta_i} \mid \beta_i = 1, 2\}$$

we see that $T_{\nu}$, $S_{i\nu}$ are all cyclic subgroups of the group $1 + J(R)$ and they are of the orders indicated in their definition. Since

$$\prod_{\nu=1}^{r} |1 + \lambda_{\nu}u_1| \cdot \prod_{i=1}^{h-1} \prod_{\nu=1}^{r} |1 + \lambda_{\nu}(u_i + u_{i+1})| = 2^{(h+1)r}$$

and the intersection of any pair of the cyclic subgroups gives the identity group, the product of the $hr$ subgroups $T_{\nu}$, $S_{i\nu}, 1 \leq i \leq h - 1$ is direct. Therefore, their product exhausts the group $1 + J(R)$.

Case (ii): $p$ is odd.

If $\nu = 1, \ldots, r$ and $u_i \in J(R) - (J(R))^2, 1 \leq i \leq h - 1$,

$$(1 + p\lambda_{\nu})^p = 1 + p^2\lambda_{\nu} + \frac{p(p - 1)}{2}(p\lambda_{\nu})^2 + \ldots + (p\lambda_{\nu})^p$$
Also,

\[(1 + \lambda_{\nu} u_1)^p = (1 + \sum_{i=1}^2 \lambda_{\nu} u_i)^p = ... = (1 + \sum_{i=1}^h \lambda_{\nu} u_i)^p = 1.\]

For positive integers \(\alpha_{\nu}, \beta_{i\nu}\) with \(\alpha_{\nu} \leq p, \beta_{i\nu} \leq p\) \((1 \leq i \leq h, 1 \leq \nu \leq r)\), we notice that the equation

\[
\prod_{\nu=1}^r \{(1 + p\lambda_{\nu})^{\alpha_{\nu}}\} \cdot \prod_{i=1}^h \prod_{\nu=1}^r \{(1 + \sum_{j=1}^i \lambda_{\nu} u_j)^{\beta_{i\nu}}\} = \{1\}
\]

will imply \(\alpha_{\nu} = \beta_{i\nu} = p, 1 \leq i \leq h\). If we set

\[
T_{\nu} = \{(1 + p\lambda_{\nu})^\alpha \mid \alpha = 1, ..., p\},
\]

\[
S_{i\nu} = \{(1 + \sum_{j=1}^i \lambda_{\nu} u_j)^{\beta_i} \mid \beta_i = 1, ..., p\}
\]

we see that \(T_{\nu}, S_{i\nu}\) are all cyclic subgroups of the group \(1 + J(R)\) and they are of the orders indicated in their definition. Since

\[
\prod_{\nu=1}^r |1 + p\lambda_{\nu}| \cdot \prod_{i=1}^h \prod_{\nu=1}^r |1 + \sum_{j=1}^i \lambda_{\nu} u_j| = p^{(h+1)r}
\]

and the intersection of any pair of the cyclic subgroups gives the identity group, the product of the \((h + 1)r\) subgroups \(T_{\nu}, S_{i\nu}, 1 \leq i \leq h\) is direct. Therefore, their product exhausts the group \(1 + J(R)\).

\[\square\]

**Proposition 10.** Let \(R\) be a commutative finite ring from the class of finite rings given by the construction. If \(h \geq 1, r > 1\) and \(\text{char } R = p^3\), then

\[
1 + J(R) \cong \begin{cases} 
\mathbb{Z}_2^r \times \mathbb{Z}_4^r \times (\mathbb{Z}_2^r)^{h-1} & \text{if } p = 2 \\
\mathbb{Z}_p^r \times (\mathbb{Z}_{p^3}^r)^h & \text{if } p \neq 2 
\end{cases}
\]

**Proof.** Let \(\lambda_1, ..., \lambda_r \in R'\) with \(\lambda_1 = 1\) such that \(\overline{\lambda_1}, ..., \overline{\lambda_r} \in R'/pR'\) form a basis for \(R'/pR'\) regarded as a vector space over its prime subfield \(GF(p)\). We treat the two cases in turn.

**Case (i):** \(p = 2\).

We notice that for every \(\nu = 1, ..., r\) and \(u_1 \in J(R) - (J(R))^2\),

\[
(-1 + 4\lambda_{\nu})^2 = 1 - 2^3\lambda_{\nu} + 2^4\lambda_{\nu}^2
\]
ON THE REGULAR ELEMENTS OF RINGS IN WHICH...

= 1, since \(\text{char} R = 2^3\).

Also

\[(1 + \lambda_{\nu} u_1)^2 = 1 + 2^2 \lambda_{\nu}^2 + 2\lambda_{\nu} u_1\]

\[= 1 + 2^2 \lambda_{\nu}^2, \text{since } 2u_1 = 0.\]

But then,

\[(1 + 2^2 \lambda_{\nu}^2)^2 = 1 + 2^4 \lambda_{\nu}^2 + 2^4 \lambda_{\nu}^4\]

\[= 1, \text{since } \text{char} R = 2^3.\]

It is also easy to see that, for each \(\nu = 1, \ldots, r, 1 \leq i \leq h-1, (1+\lambda_{\nu}(u_i+u_{i+1}))^2 = 1.\)

For positive integers \(\alpha_{\nu}, \beta_{\nu}, \kappa_{i\nu}\) with \(\alpha_{\nu} \leq 2, \beta_{\nu} \leq 4, \kappa_{i\nu} \leq 2, (1 \leq i \leq h-1, 1 \leq \nu \leq r)\), we notice that the equation

\[\prod_{\nu=1}^{r} \{(-1 + 4\lambda_{\nu})^{\alpha_{\nu}}\} \cdot \prod_{\nu=1}^{r} \{(1 + \lambda_{\nu} u_1)^{\beta_{\nu}}\} \cdot \prod_{i=1}^{h-1} \prod_{\nu=1}^{r} \{(1 + \lambda_{\nu}(u_i + u_{i+1}))^{\kappa_{i\nu}}\} = \{1\}\]

will imply \(\alpha_{\nu} = 2\) and \(\beta_{\nu} = 4, \kappa_{i\nu} = 2, 1 \leq i \leq h - 1.\) If we set

\[H_{\nu} = \{(-1 + 4\lambda_{\nu})^{\alpha} | \alpha = 1, 2\},\]

\[T_{\nu} = \{(1 + \lambda_{\nu} u_1)^{\beta} | \beta = 1, \ldots, 4\},\]

\[S_{i\nu} = \{(1 + \lambda_{\nu}(u_i + u_{i+1}))^{\kappa_{i}} | \kappa_{i} = 1, 2\}\]

we see that \(H_{\nu}, T_{\nu}, S_{i\nu}\) are all cyclic subgroups of the group \(1 + J(R)\) and they are of the orders indicated in their definition. Since

\[\prod_{\nu=1}^{r} \{-1 + 4\lambda_{\nu}\} \cdot \prod_{\nu=1}^{r} \{1 + \lambda_{\nu} u_1\} \cdot \prod_{i=1}^{h-1} \prod_{\nu=1}^{r} \{1 + \lambda_{\nu}(u_i + u_{i+1})\} = 2^{(h+2)r}\]

and the intersection of any pair of the cyclic subgroups gives the identity group, the product of the \((h+1)r\) subgroups \(H_{\nu}, T_{\nu}, S_{i\nu}, 1 \leq i \leq h - 1\) is direct. Therefore, their product exhausts the group \(1 + J(R)\).

**Case (ii):** \(p\) is odd.

Here, we notice that

\[(1 + p\lambda_{\nu})^2 = 1, (1 + \lambda_{\nu} u_1)^p = (1 + \sum_{i=1}^{2} \lambda_{\nu} u_i)^p = \ldots = (1 + \sum_{i=1}^{h} \lambda_{\nu} u_i)^p = 1.\]
Now, for positive integers \( \alpha_i, \beta_i \) with \( \alpha_i \leq p^2, \beta_i \leq p \), \( 1 \leq i \leq h, 1 \leq \nu \leq r \), we notice that the equation

\[
\prod_{\nu=1}^{r} \{(1 + p\lambda_{\nu})^{\alpha_{\nu}}\} \prod_{i=1}^{h} \prod_{\nu=1}^{r} \{(1 + \sum_{j=1}^{i} \lambda_{\nu}u_{j})^{\beta_{\nu}}\} = \{1\}
\]

will imply \( \alpha_i = p^2, \beta_{i\nu} = p \) for \( 1 \leq \nu \leq r \) and \( 1 \leq i \leq h \). The rest of the proof is similar to Case (ii) in the previous Proposition.

**Proposition 11.** Let \( R \) be a commutative finite ring from the class of finite rings described by the construction. If \( h \geq 1, r = 1 \) and \( \text{char}R = p^n, n \geq 4 \), then

\[
1 + J(R) \cong \begin{cases} 
Z_2 \times Z_2 \times Z_{2^{n-2}} \times (Z_2)^h & \text{if } p = 2 \\
Z_{p^{n-1}} \times (Z_p)^h & \text{if } p \neq 2 
\end{cases}
\]

**Proof.** Case (i): \( p = 2 \).

Consider the element \( 1 + 2t + u_1 \), where \( t = n - 4, n \geq 4 \), then \( o(1 + 2t + u_1) = 2^{n-2} \). The elements \(-1 + 2^{n-1}\) and \(-1 + 2^{n-2} + u_1\) are each of order 2. Also, the elements \( 1 + u_1 + u_2, 1 + u_2 + u_3, ..., 1 + u_{h-1} + u_h \) are each of order 2. Now, the mentioned elements generate cyclic subgroups of \( 1 + J(R) \). Since \( |< 1 + 2t + u_1 >| \cdot |< -1 + 2^{n-1} >| \cdot |< -1 + 2^{n-2} + u_1 >| \cdot \prod_{j=2}^{h} |< 1 + u_{j-1} + u_j >| = 2^{n+h-1} \), and the intersection of any pair of the cyclic subgroups gives the identity group, \( < 1 + 2t + u_1 > \times < -1 + 2^{n-1} > \times < -1 + 2^{n-2} + u_1 > \times < 1 + u_1 + u_2 > \times ... \times < 1 + u_{h-1} + u_h > \) is a direct product.

Case (ii): \( p \neq 2 \).

Here, the element \( 1 + p \) is of order \( p^{n-1} \) while the elements \( 1 + u_1, 1 + \sum_{i=1}^{2} u_i, ... , 1 + \sum_{i=1}^{h} u_i \) are each of order \( p \). The given elements generate cyclic subgroups of the group \( 1 + J(R) \). Since

\[
|< 1 + p >| \cdot \prod_{i=1}^{h} |< 1 + \sum_{i=1}^{t} u_i >| = 2^{n+h-1},
\]

and the intersection of any pair of the cyclic subgroups gives the identity group, \( < 1 + p > \times < 1 + u_1 > \times < 1 + \sum_{i=1}^{2} u_i > \times ... \times < 1 + \sum_{i=1}^{h} u_i > \) is a direct product. \( \square \)

**Proposition 12.** Let \( R \) be a commutative finite ring from the class of finite rings described by the construction. If \( h \geq 1, r > 1 \) and \( \text{char}R = p^4 \), then

\[
1 + J(R) \cong \begin{cases} 
Z_2 \times Z_2 \times Z_1 \times Z_2^{-1} \times Z_8^{-1} \times (Z_2)^h & \text{if } p = 2 \\
Z_{p^3} \times (Z_p)^h & \text{if } p \neq 2 
\end{cases}
\]
ON THE REGULAR ELEMENTS OF RINGS IN WHICH...

Let \( \lambda_1, \ldots, \lambda_r \in R' \) with \( \lambda_1 = 1 \) such that \( \overline{\lambda_1}, \ldots, \overline{\lambda_r} \in R'/pR' \) form a basis for \( R'/pR' \) regarded as a vector space over its prime subfield \( GF(p) \). We treat the two cases in turn.

Case (i): \( p = 2 \).

Clearly,

\[
(-1 + 2^3 \lambda_1)^2 = 1, \quad (-1 + 2^2 \lambda_1 + \lambda_1 u_1)^2 = 1, \quad (-1 + 2^3 (\lambda_1 + \lambda_2) + \lambda_2 u_1)^4 = 1,
\]

\[
(1 + 2^2 (\lambda_1 + \lambda_2) + \lambda_2 u_1)^2 = (1 + 2^2 (\lambda_1 + \lambda_3) + (\lambda_2 + \lambda_3) u_1)^2 = \ldots =
\]

\[
(1 + 2^2 (\lambda_1 + \lambda_r) + (\lambda_2 + \ldots + \lambda_r) u_1)^2 = 1, \quad (1 + 2 \lambda_r + \lambda_r u_1)^8 = 1,
\]

\[
(1 + \lambda_r u_{j-1} + \lambda_r u_j)^2 = 1, \quad 2 \leq j \leq h.
\]

For positive integers \( \alpha, \beta, \kappa, \gamma, \tau, \omega \) with \( \alpha \leq 2, \beta \leq 2, \kappa \leq 4, \gamma \leq 2, \tau \leq 8, \omega \leq 2 \), \( \tau \leq 2, s \leq r, 1 \leq \nu \leq r, 1 \leq i \leq h - 1 \), we notice that the equation

\[
\{(-1 + 2^3 \lambda_1)^\alpha \} \{(-1 + 2^2 \lambda_1 + \lambda_1 u_1)^\beta \} \{(-1 + 2^3 (\lambda_1 + \lambda_2) + \lambda_2 u_1)^\kappa \} \prod_{\nu=2}^r \{(1 + 2^2 (\lambda_1 + \lambda_\nu) + \sum_{i=2}^\nu \lambda_i u_1)^\gamma \nu \} \prod_{i=1}^h \prod_{\nu=1}^r \{(1 + \lambda_\nu (u_i + u_{i+1}))^{\omega \nu} \} = \{1\},
\]

will imply \( \alpha = \beta = 2, \kappa = 4, \gamma = 2, \tau = 8, \omega = 2 \) for every \( \nu = 1, \ldots, r \), \( \nu = 2, \ldots, r \) and \( i = 1, \ldots, h - 1 \). If we set

\[
E = \{(-1 + 2^3 \lambda_1)^\alpha \mid \alpha = 1, 2\},
\]

\[
F = \{(-1 + 2^2 \lambda_1 + \lambda_1 u_1)^\beta \mid \beta = 1, 2\},
\]

\[
G = \{(-1 + 2^3 (\lambda_1 + \lambda_2) + \lambda_2 u_1)^\kappa \mid \kappa = 1, \ldots, 4\},
\]

\[
H_\nu = (1 + 2^2 (\lambda_1 + \lambda_\nu) + \sum_{i=2}^\nu \lambda_i u_1)^\gamma \nu \mid \gamma = 1, 2\},
\]

\[
K_\nu = \{(1 + 2 \lambda_\nu + \lambda_\nu u_1)^\tau \nu \mid \tau \nu \leq 8\},
\]

\[
L_{i\nu} = \{(1 + \lambda_\nu (u_i + u_{i+1}))^{\omega i} \}
\]

we see that \( E, F, G, H_2, \ldots, H_r, K_2, \ldots, K_r, L_{1\nu}, \ldots, L_{(h-1)\nu} \) are all cyclic subgroups of the group \( 1 + J(R) \) and they are of the orders indicated in their definition.

Since

\[
| -1 + 8 \lambda_1 | \cdot | -1 + 4 \lambda_1 + \lambda_1 u_1 | \cdot | -1 + 8 (\lambda_1 + \lambda_2) + \lambda_2 u_1 |.
\]

\[
\prod_{\nu=2}^r | 1 + 4 (\lambda_1 + \lambda_\nu) + \sum_{i=2}^\nu \lambda_i u_1 | \cdot \prod_{\nu=2}^r | 1 + 2 \lambda_\nu + \lambda_\nu u_1 |.
\]

\[
\prod_{i=1}^{h-1} \prod_{\nu=1}^r | 1 + \lambda_\nu (u_i + u_{i+1}) | = 2^{(h+1)r},
\]
and the intersection of any pair of the cyclic subgroups gives the identity group, the product of the $1 + (h + 1)r$ subgroups $E, F, G, H_2, ..., H_r, K_2, ..., K_r, L_{1\nu}, ..., L_{(h-1)\nu}$ is direct. Therefore, their product exhausts $1 + J(R)$.

Case (ii): $p \neq 2$.

Here the proof is similar to that of Case (ii) in the previous Proposition, with some slight modification. \[ \square \]

**Proposition 13.** Let $R$ be a commutative finite ring from the class of finite rings described by the construction. If $h \geq 1$, $r > 1$ and $\text{char} R = p^n$, $n \geq 5$, then

$$1 + J(R) \cong \begin{cases} Z_2 \times Z_2 \times Z_{2^{n-2}} \times Z_r^{r-1} \times Z_8^{r-1} \times (Z_2')^{h-1} & \text{if } p = 2 \\
 \prod_{p-1} (Z_p') & \text{if } p \neq 2 \end{cases}$$

**Proof.** Let $\lambda_1, ..., \lambda_r \in R'$ with $\lambda_1 = 1$ such that $1, ..., 1 \in R'/pR'$ form a basis for $R'/pR'$ regarded as a vector space over its prime subfield $GF(p)$. We treat the two cases in turn.

Case (i): $p = 2$.

Clearly,

$$(-1 + 2^{n-1})^2 = 1, (-1 + 2^{n-1} \lambda_1 + 2^{n-1} \lambda_2)^2 = 1, (1 + 2 \lambda_1 + \lambda_1 u_1) = 1,$$

$$1 + \sum_{i=2}^r \lambda_i u_1)^{2^{n-3}} = 1, (1 + 4 \lambda_\nu + \lambda_\nu u_1)^{2^{n-2}} = 1,$$  

$$\nu = 2, ..., r, (1 + \lambda_\nu(u_i + u_{i+1}))^{2^{n-3}} = 1, 1 \leq i \leq h - 1$$

For positive integers $\alpha, \beta, \kappa_\nu, \gamma_\nu, \tau_\nu, \omega_\nu$ with $\alpha \leq 2, \beta \leq 2^{n-2}, \kappa_\nu \leq 2, \gamma_\nu \leq 2^{n-3}, \tau_\nu \leq 2^{n-2}, \omega_\nu \leq 2, 1 \leq \nu \leq r, 1 \leq i \leq h - 1$ we notice that the equation $\{(1 + 2^{n-1} \lambda_1)^\alpha\}, \{(1 + 2 \lambda_1 + \lambda_1 u_1)^\beta\}, \{(1 + 2^{n-1} - 2^{n-2})^\kappa\}, \{(1 + \lambda_\nu(u_i + u_{i+1}))^{\omega_\nu}\}$ imply $\nu = 2, ..., r$ and $i = 1, ..., h - 1$.

If we set

$$E = \{(-1 + 2^{n-1} \lambda_1)^\alpha | \alpha = 1, 2\}$$

$$F = \{(1 + 2 \lambda_1 + \lambda_1 u_1)^\beta | \beta = 1, ..., 2^{n-2}\}$$

$$G = \{(-1 + 2^{n-1} \lambda_2)^\kappa | \kappa = 1, 2\}$$

$$H_\nu = (1 + \sum_{i=2}^r \lambda_i u_1)^\gamma_\nu | \gamma_\nu = 1, ..., 2^{n-3}\},$$

$$K_\nu = \{(1 + 4 \lambda_\nu + \lambda_\nu u_1)^\tau_\nu | 1, ..., 2^{n-2}\},$$

$$L_\nu = \{(1 + \lambda_\nu(u_i + u_{i+1}))^{\omega_i} | \omega_i = 1, 2\}$$
we see that $E, F, G, H_2, ..., H_r, K_2, ..., K_r, L_1, ..., L_{(h-1)}$ are all cyclic subgroups of the group $1 + J(R)$ and they are of the orders indicated in their definition.

Since

$$|< -1 + 2^{n-1} \lambda_1 >| \cdot |< 1 + 2\lambda_1 + \lambda_1 u_1 >| \cdot \prod_{\nu=2}^r |< -1 + 2^{n-1}(\lambda_1 + \lambda_2) >| \cdot \prod_{\nu=2}^r |< 1 + \sum_{i=2}^\nu \lambda_i u_1 >| \cdot \prod_{\nu=2}^r |< 1 + 4\lambda_\nu + \lambda_\nu u_1 >| \cdot \prod_{i=1}^{h-1} \prod_{\nu=1}^r |< 1 + \lambda_\nu (u_i + u_{i+1}) >| = 2^{(h+n-1)r},$$

and the intersection of any pair of the cyclic subgroups gives the identity group, the product of the $1 + (h+1)r$ subgroups $E, F, G, H_2, ..., H_r, K_2, ..., K_r, L_1, ..., L_{(h-1)}$ is direct. Therefore, their product exhausts $1 + J(R)$.

Case (ii): $p \neq 2$.

Here the proof is similar to that of Case (ii) in the previous Proposition, with some slight modification. \(\Box\)

We now state the main result.

**Theorem 1.** The regular elements of the rings described by the construction is given as follows:

i) If $\text{char} R = p^2$, then

$$V(R) \cong \begin{cases} \mathbb{Z}_{2r-1} \times \mathbb{Z}_4^r \times (\mathbb{Z}_2^r)^{h-1} \cup \{0\} & \text{if } p = 2 \\ \mathbb{Z}_{p^r-1} \times \mathbb{Z}_p^r \times (\mathbb{Z}_p^r)^{h} \cup \{0\} & \text{if } p \neq 2 \end{cases}$$

ii) If $\text{char} R = p^3$, then

$$V(R) \cong \begin{cases} \mathbb{Z}_{2r-1} \times \mathbb{Z}_2^r \times \mathbb{Z}_4^r \times (\mathbb{Z}_2^r)^{h-1} \cup \{0\} & \text{if } p = 2 \\ \mathbb{Z}_{p^r-1} \times \mathbb{Z}_p^r \times (\mathbb{Z}_p^r)^{h} \cup \{0\} & \text{if } p \neq 2 \end{cases}$$

iii) If $\text{char} R = p^4$, then

$$V(R) \cong \begin{cases} \mathbb{Z}_{2r-1} \times \mathbb{Z}_2^r \times \mathbb{Z}_2 \times \mathbb{Z}_4^r \times (\mathbb{Z}_2^r)^{h-1} \cup \{0\} & \text{if } p = 2 \text{ and } r = 1 \\ \mathbb{Z}_{2r-1} \times \mathbb{Z}_2^r \times \mathbb{Z}_2 \times \mathbb{Z}_4^r \times \mathbb{Z}_2^{r-1} \times \mathbb{Z}_8^{r-1} \times (\mathbb{Z}_2^r)^{h-1} \cup \{0\} & \text{if } p = 2 \text{ and } r > 1 \\ \mathbb{Z}_{p^r-1} \times \mathbb{Z}_p^r \times (\mathbb{Z}_p^r)^{h} \cup \{0\} & \text{if } p \neq 2 \end{cases}$$
iv) If $\text{char} R = p^n$, $n \geq 5$, then

$V(R) \cong \begin{cases} 
Z_{2^{r-1}} \times Z_2 \times Z_2 \times Z_{2^{n-2}} \times (Z_2)^{h-1} \cup \{0\} & \text{if } p = 2 \text{ and } r = 1 \\
Z_{p^{r-1}} \times Z_2 \times Z_2 \times Z_{2^{n-2}} \times Z_{2^{n-3}}^{-1} \times Z_{2^{n-2}}^{-1} \times (Z_2)^{h-1} \cup \{0\} & \text{if } p = 2 \text{ and } r > 1 \\
Z_{p^{r-1}} \times Z_{p^{n-1}} \times (Z_p)^h \cup \{0\} & \text{if } p \neq 2
\end{cases}$

Acknowledgments

The first author expresses his wholehearted gratitude to DAAD for sponsoring his visit to the African Institute for Mathematical Sciences, South Africa which hosted him during this research.

References


