Earthline Journal of Mathematical Sciences
E-ISSN: 2581-8147
Volume 14, Number 6, 2024, Pages 1229-1237
https://doi.org/10.34198/ejms.14624.12291237

Unit Groups of a Finite Extension of Galois Rings

Oduor Maurice Owino

Department of Mathematics, Actuarial and Physical Sciences, University of Kabianga,
P.O. Box 2030-20200, Kericho, Kenya
e-mail: moduor@kabianga.ac.ke

Abstract

Let R_o be a Galois ring. It is well known that every element of R_o is either a zero divisor or a unit. Galois rings are building blocks of completely primary finite rings which have yielded interesting results towards classification of finite rings. Recent studies have revealed that every finite commutative ring is a direct sum of completely primary finite rings. In fact, extensive account of finite rings have been given in the recent past. However, the classification of finite rings into well known structures still remains an open problem. For instance, the structure of the group of units of R_o is known and some results have been obtained on the structure of its zero divisor graphs. In this paper, we construct a finite extension of R_o (a special class of completely primary finite rings) and classify its group of units for all the characteristics.

1 Introduction

In this paper, we consider finite, associative, commutative rings with identities. It is assumed that all ring homomorphisms preserve identity and a ring with its subrings have the same identity. In the sequel, $\mathbb{Z}$ denotes the ring of all integers, $\mathbb{Z}_n$ denotes the ring of integers modulo n, $R_o = GR(p^{kr}, p^k)$ denotes the Galois ring of order p^{kr} and characteristic p^k. The unit group of a ring R is denoted by

Received: September 3, 2024; Revised & Accepted: October 4, 2024; Published: October 8, 2024
2020 Mathematics Subject Classification: 13M05, 16U60.
Keywords and phrases: unit groups, Galois rings, finite extension.

$U(R)$ while its Jacobson radical is denoted by $J(R)$. The other notations used in this paper are standard.

Now, for a prime integer p and positive integers k and r, let R_o be a Galois ring of order p^{kr} and characteristic p^k. Let U be a finitely generated free R_o-module with generators $u_1, ..., u_h$, such that $pu_i = 0$ for $k = 1, 2$ and $p^j u_i = 0$ for $1 \leq i \leq h$ and $1 \leq j < k$, so that $R = R_o \oplus U = R_o \oplus R_o u_1 \oplus \cdots \oplus R_o u_h$ is an additive abelian group, where every element of R_o is expressible uniquely as

$$\sum_{f=0}^{k-1} p^f \lambda_f, \quad \lambda_f \in R_o/pR_o.$$

On R, define multiplication by

$$(r_o, \sum_{i=1}^{h} r_i u_i)(r_o^{'}, \sum_{i=1}^{h} r_i^{'} u_i) = (r_o r_o^{'}, \sum_{i=1}^{h} [(r_o + pR_o) r_i^{'} + r_i (r_o^{'} + pR_o)] u_i).$$

It is easy to verify that the multiplication turns R into a commutative completely primary finite ring with identity $(1, 0, ..., 0)$.

A similar construction was given in [3] and [7] and the group of units and the group of automorphisms of R were determined with the restriction $u_i\big|_U$ so that $pu_i = u_i u_j = 0, 1 \leq i, j \leq h$. Related studies on such finite rings were conducted in [5] and [6]. Studies on completely primary finite rings have attracted much attention in the recent past. This is because of their significant contribution towards the classification of finite rings, since every finite ring is expressible as a direct sum of completely primary finite rings. Raghavendran [9] and Wilson [11] have extensively studied finite rings even though their classification into well known structures is still an open problem. The units of Galois rings were studied by Raghavendran [9] while their zero divisor graphs were studied by the author in [4] and [10] among others. Gilmer in [2] determined all local rings R where $U(R)$ is cyclic. Pearson and Schneider in [8] found all rings whose unit groups are generated by 2 elements. In this paper, we lift the restriction of u_i on U so that $pu_i = u_i u_j = 0$ and consider the order $o(u_i) = p^j$ or $p^j u_i = 0, i = 1, ..., h$ and $1 \leq j \leq k - 1$ when char $R = p^k$. We determine the generators and the structure of the group of units $U(R)$.

2 Rings in which the Product of any Two Zero Divisors is Zero

Let $R_o = GR(p^{kr}, p^k)$, where $k = 1, 2$ and U be an R_o-module generated by $u_1, ..., u_h$, where $pu_i = 0, i = 1, ..., h$, so that $R = R_o \oplus U = R_o \oplus R_o u_1 \oplus \cdots \oplus R_o u_h$ is an additive abelian group on R, define multiplication as given in Section 1. Then R is a commutative ring with identity, $|R| = p^{(k+h)r}$. The set of the zero divisors of R is a unique maximal ideal

$$Z(R) = pR_o \oplus U = pR_o \oplus R_o u_1 \oplus \cdots \oplus R_o u_h = J(R),$$

the Jacobson radical of R and $(J(R))^2 = (0)$. Since $R_o \subseteq R$ and the degree $[R : R_o] = p^{hr}$, R is a finite extension of R_o. Now, if $|R| = p^{nr}$, then since $|R_o/pR_o| = p^r$, it follows that $n = k + h$ where $k = \text{char } R$.

2.1 The unit group $U(R)$

From the ring constructed in Section 1, R is commutative and consequently $U(R)$ is an Abelian group.

The following result is well known (see, e.g., [1], Proposition 2.1]).

Lemma 1. *Let R be a ring constructed in Section 1. If char $= p^t, t = 1, 2$, then $U(R)$ is cyclic iff $1 + J(R)$ is cyclic. Moreover, $U(R) = \langle b \rangle \cdot (1 + J(R)) \cong \langle b \rangle \times (1 + J(R))$, a direct product of the p-group $1 + J(R)$ by the cyclic subgroup $< b >$ where $b \in R$ and the order $o(b) = p^r - 1$.*

A complete classification of $U(R)$ requires that the structure of $1 + J(R)$ be completely determined. $1+J(R)$ is an abelian p-subgroup of $U(R)$ with a filtration

$$1 + J(R) \supseteq 1 + (J(R))^2 = \langle 1 \rangle$$

and the filtration quotient

$$1 + J(R)/1 + (J(R))^2 = 1 + J(R)$$

isomorphic to the additive group

$$J(R)/(J(R))^2 = J(R)$$

since

$$(J(R))^2 = (0).$$

The following results are useful in determining the structure of $1 + J(R)$. Their proofs are straightforward and may be obtained from [7].

Lemma 2. *Let p be a prime integer. Then $1 + pR_o$ is a subgroup of $1 + J(R)$.*

Proposition 1. *For each $i = 1, 2, ..., h$, $1 + \sum_{i=1}^{h} R_o u_i$ is a subgroup of $1 + J(R)$.*

Proposition 2. *The group $1 + J(R)$ is a direct product of the subgroups $1 + pR_o$ by $1 + \sum_{i=1}^{h} \oplus R_o u_i$.*

Next, we summarize the unit group $U(R)$ of the ring constructed in Section 1, where $charR = p$ or p^2.

Proposition 3. *The unit group U(R) of a ring constructed in Section 1 of characteristic p or p^2 is a direct product of cyclic groups as follows:*

$$U(R) \cong \begin{cases} \mathbb{Z}_{p^r-1} \times \underbrace{\mathbb{Z}_p^r \times \cdots \times \mathbb{Z}_p^r}_{h} & if \quad charR = p \\ \mathbb{Z}_{p^r-1} \times \underbrace{\mathbb{Z}_p^r \times \cdots \times \mathbb{Z}_p^r}_{h+1} & if \ \ charR = p^2. \end{cases}$$

.

3 Rings in which the Set of Zero Divisors, $J(R)$ satisfies $(J(R))^k = (0), (J(R))^{k-1} \neq (0), k \geq 3$

For $k \geq 3$, let $R_o = GR(p^{kr}, p^k)$ be a Galois ring and U be R_o module generated by $u_1, ..., u_h$ where $p^j u_i = 0, 1 \leq i \leq h, 1 \leq j \leq k-1$, so that $R = R_o \oplus U$ is an additive abelian group. Using the multiplication in the construction given in Section 1, the set of the zero divisors

$$J(R) = pR_o \oplus R_o u_1 \oplus \cdots \oplus R_o u_h, \quad p^j u_i = 0, \quad 1 \leq j < k,$$

$$(J(R))^{k-1} = p^{k-1} R_o$$

and

$$(J(R))^k = (0).$$

It is also evident that

$$0 \to R_o \xrightarrow{.p^j} R_o \xrightarrow{g} R_o/p^j R_o \to 0$$

is a short exact sequence since the image $\mathrm{Im}(.p^j) = p^j R_o = (p^j) =$ kernel of g. Further $|R| = p^{(k+jh)r}$ and $[R : R_o] = p^{jhr}$. Now, $J(R)$ has the following filtration

$$J(R) \supset (J(R))^2 \supset \cdots \supset (J(R))^{k-1} \supset (J(R))^k = (0)$$

and the p-group $1 + J(R)$ has the following normal subgroups:

$$\langle 1 \rangle = 1 + (J(R))^k \lhd 1 + (J(R))^{k-1} \lhd \cdots \lhd 1 + (J(R))^3 \lhd 1 + (J(R))^2 \lhd 1 + J(R).$$

It is easy to see that $(J(R))^j/(J(R))^{j+1} \cong 1+(J(R))^j/1+(J(R))^{j+1}$, $1 \leq j \leq k-1$.

3.1 The unit group $U(R)$

We determine the group of units of the ring R constructed in Section 1, when characteristic char $R = p^k, k \geq 3$.

The following result due to Raghavendran [9] on the structure of the units of the Galois ring $R_o = GR(p^{kr}, p^k)$ shall be useful.

Theorem 1. *Let $R_o = GR(p^{kr}, p^k)$ be a Galois ring. Then $U(R_o)$ is a direct product of the cyclic group of order $p^r - 1$ by the group $1 + pR_o$ of order $p^{(k-1)r}$ whose structure is described as follows:*
(a) If (i) p is odd,or (ii) $p = 2$ and $k \leq 2$, then $1 + pR_o$ is the direct product of r

cyclic groups each of order p^{k-1}.
(b) When $p = 2$ and $k \geq 3$, the group $1 + pR_0$ is the direct product of a cyclic group of order 2, a cyclic group of order 2^{k-2} and $r-1$ cyclic groups each of order 2^{k-1}.

We notice that char $R_o =$ char $R = p^k, 1 \leq k < k + jh$;

$$J(R) = pR_o \oplus R_o u_1 \oplus \cdots \oplus R_o u_h$$

$$(J(R))^2 = p^2 R_o \oplus pR_o u_1 \oplus \cdots \oplus pR_o u_h$$

$$.$$

$$.$$

$$.$$

$$(J(R))^{k-1} = p^{k-1} R_o$$

$$(J(R))^k = (0).$$

Further, $|R| = p^{(k+jh)r}, |J(R)| = p^{(k+jh-1)r}$. Hence $R/J(R) \cong \mathbb{F}_{p^r}$. Also

$U(R) \cong \mathbb{Z}_{p^r-1} \times (1 + J(R)), |U(R)| = |R| - |J(R)| = p^{(k+jh)r} - p^{(k+jh-1)r}$

and $|1 + J(R)| = p^{(k+jh-1)r}$.

Now, let $\epsilon_1, ..., \epsilon_r$ be elements of R_0 with $\epsilon_1 = 1$ so that the set $\{\overline{\epsilon_1}, ..., \overline{\epsilon_r}\}$ forms a basis of R_o/pR_o regarded as a vector space over its prime subfield $\mathbb{F}_p$.

Proposition 4. *Let R be a ring constructed in Section 1. Suppose that $k \geq 3$ and $1 \leq j < k$, then*

$$U(R) \cong \begin{cases} \mathbb{Z}_{2^n-1} \times \mathbb{Z}_2 \times \mathbb{Z}_{2^{k-2}} \times \mathbb{Z}_{2^{k-1}}^{r-1} \times \underbrace{\mathbb{Z}_{2^j}^r \times \cdots \times \mathbb{Z}_{2^j}^r}_{h} & \text{if} \quad p = 2 \\ \mathbb{Z}_{p^r-1} \times \mathbb{Z}_{p^{k-1}}^r \times \underbrace{\mathbb{Z}_{p^j}^r \times \cdots \times \mathbb{Z}_{p^j}^r}_{h} & \text{if } p \text{ is odd.} \end{cases}$$

Proof. The unit group $U(R) \cong \mathbb{Z}_{p^r-1} \times (1 + J(R))$. The structure of $U(R)$ is completely determined when the structure of $1 + J(R)$ is known. Since $p^j u_i = 0, 1 \leq j < k, 1 \leq i \leq h$, it easily follows that $1 + R_o u_1 \oplus \cdots \oplus R_o u_h$ is a subgroup of $1 + J(R)$ and $(1 + pR_o) \cap (1 + R_o u_1 \oplus \cdots \oplus R_o u_h) = \langle 1 \rangle$. Therefore $1 + J(R)$ is a direct product of $1 + pR_o$ by $1 + R_o u_1 \oplus \cdots \oplus R_o u_h$.

Since $1 + pR_o$ is completely determined by Theorem 1, we determine the structure of $1 + R_o u_1 \oplus \cdots \oplus R_o u_h$. For each $\nu = 1, ..., r, (1 + \epsilon_\nu u_1)^{p^j} = 1, (1+\epsilon_\nu u_2)^{p^j} = 1, ..., (1+\epsilon_\nu u_h)^{p^j} = 1$ and $a^{p^j} = 1$ for all $a \in 1+R_o u_1 \oplus \cdots \oplus R_o u_h$ since $p^j u_i = 0, 1 \leq j < k, 1 \leq i \leq h$.

For positive integers $\beta_{\nu_i} \leq p^j (1 \leq \nu \leq r, 1 \leq i \leq h)$, we assert that the equation

$$\prod_{\nu=1}^{r} \cdot \prod_{i=1}^{h} \{(1 + \epsilon_\nu u_j)^{\beta_{\nu_i}}\} = \langle 1 \rangle$$

will imply $\beta_{\nu_i} = p^j$. Setting $H_{\nu_i} = \{(1 + \epsilon_\nu u_i)^{\beta_{\nu_i}} | \beta_{\nu_i} = 1, ..., p^j\}$ for all $\nu = 1, ..., r$ and $1 \leq i \leq h$, we see that all the H_{ν_i} are cyclic subgroups of $1 + R_o u_1 \oplus ... \oplus R_o u_h$ and are all of order p^j as indicated in their definition. Therefore the product of the hr subgroups H_{ν_i} is direct and exhausts $1 + R_o u_1 \oplus \cdots \oplus R_o u_h$. □

4 Main Result

The following is the main result proved in this paper.

Theorem 2. *Let R be a Galois ring extension as constructed in Section 1. If $R = R_o \oplus R_o u_1 \oplus \cdots \oplus R_o u_h$, where $u_1, ..., u_h$ are the generators of the R_o module U and char $R = p^k$, so that $p^j u_i = 0$, for prime integer p, $1 \leq j < k$ and*

$1 \leq i \leq h$, *then*

$$U(R) \cong \begin{cases} \mathbb{Z}_{p^r-1} \times \underbrace{\mathbb{Z}_p^r \times \cdots \times \mathbb{Z}_p^r}_{h} & \textit{if} \quad char R = p \\ \mathbb{Z}_{p^r-1} \times \underbrace{\mathbb{Z}_p^r \times \cdots \times \mathbb{Z}_p^r}_{h+1} & \textit{if} \quad char R = p^2 \\ \mathbb{Z}_{2^r-1} \times \mathbb{Z}_2 \times \mathbb{Z}_{2^{k-2}} \times \mathbb{Z}_{2^{k-1}}^{r-1} \times \underbrace{\mathbb{Z}_{2^j}^r \times \cdots \times \mathbb{Z}_{2^j}^r}_{h} & \textit{if} \quad char R = p^k, p = 2, k \geq 3 \\ \mathbb{Z}_{p^r-1} \times \mathbb{Z}_{p^{k-1}}^r \times \underbrace{\mathbb{Z}_{p^j}^r \times \cdots \times \mathbb{Z}_{p^j}^r}_{h} & \textit{if} \quad char R = p^k, p \textit{ is odd}, k \geq 3 \end{cases}$$

Proof. Follows from Theorem 1, Proposition 3 and Proposition 4. □

References

[1] Chitenga, J. C. (2005). Unit groups of cube radical zero commutative completely primary finite rings. *International Journal of Mathematics and Mathematical Sciences, 2005*(4), 579-592. https://doi.org/10.1155/IJMMS.2005.579

[2] Gilmer Jr., R. W. (1963). Finite rings having a cyclic multiplicative group of units. *American Journal of Mathematics, 85*(4), 447-452. https://doi.org/10.2307/2373134

[3] Owino, M. O. (2012). Automorphisms of a certain class of completely primary finite rings. *International Journal of Pure and Applied Mathematics, 74*(4), 465-482.

[4] Owino, M. O. (2016). On the zero divisor graphs of Galois rings. *African Journal of Pure and Applied Sciences (IMHOTEP), 3*, 85-94.

[5] Owino, M. O. (2009). Unit groups of certain classes of commutative finite rings. *Journal of Mathematical Sciences, 20*(3), 275-280.

[6] Owino, M. O., Chiteng'a, J. C., & Omolo, N. O. (2009). Unit groups of $k+1$ index radical zero commutative finite rings. *International Journal of Pure and Applied Mathematics, 57*(1), 57-67.

[7] Owino, M. O., Ojiema, M. O., & Mmasi, E. (2013). Units of commutative completely primary finite rings of characteristic p^n. *International Journal of Algebra, 7*(6), 259-266. https://doi.org/10.12988/ija.2013.13026

[8] Pearson, K. R., & Schneider, J. E. (1979). Rings with a cyclic group of units. *Journal of Algebra, 16*, 243-251. https://doi.org/10.1016/0021-8693(70)90030-X

[9] Raghavedran, R. (1969). Finite associative rings. *Compositio Mathematica, 21*, 195-229.

[10] Rotich, G. T., Owino, M. O., & Olwamba, L. O. (2019). On the adjacency matrices of the Anderson-Livingston zero divisor graphs of Galois rings. *International Journal of Algebra, 13*(4), 153-160. https://doi.org/10.12988/ija.2019.9211

[11] Wilson, R. S. (1969). On the structure of finite rings. *Compositio Mathematica, 26*, 195-229.