International Journal of Algebra, Vol. 7, 2013, no. 6, 259 - 266
HIKARI Ltd, www.m-hikari.com

Units of Commutative Completely Primary Finite Rings of Characteristic p^n

Owino Maurice Oduor[1], **Ojiema Michael Onyango**[2] **and Mmasi Eliud**[3]

[1] Department of Mathematics and Computer Science
Kabianga University, P.O. Box 2030-20200, Kericho, Kenya
morricearaka@yahoo.com

[2], [3] Department of Mathematics and Computer Science
Masinde Muliro University of Science and Technology
P.O. Box 190-50100, Kakamega, Kenya
michael ojiema@yahoo.com, eliudmmasi@gmail.com

Abstract

The characterization of the group of units of any commutative ring has not been done in general, and previous studies have restricted the classes of rings or groups under consideration. In this work, we determine the structures of the groups of units of commutative completely primary finite rings R of characteristic p^n for some prime integer p and positive integer n.

Mathematics Subject Classification: Primary 13M05, 16P10, 16U60, Secondary 13E10, 16N20

Keywords: 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 rest of the notations shall be adopted from [1].
The characterization of a finite abelian group is precisely known and it has

been represented as a direct product of cyclic groups. In this form, vital characteristics of a finite group, such as exponent, rank and order are quite conclusive. On the other hand, the characterization of the group of units of any commutative ring has not been done in general, even though it is well known that if R is a finite field, then R^*, the group of units of R, is cyclic. Moreover, when R is a finite commutative ring, then it is known from the Fundamental Theorem of finite abelian groups that R^* is isomorphic to a direct product of cyclic groups. There is no known general solution to the problem, even though solutions to some special cases have been obtained with a restriction on R. For the previous related work, reference can be made to [2],[3] or [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 $n = 1, 2$, then $pu_i = u_iu_j = u_ju_i = 0, u_ir^{'} = (r^{'})^{\sigma_i}u_i$
(ii) If $n \geq 3$, then

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

where $r^{'}, \gamma_{ij} \in R^{'}$, $1 \leq i, j \leq h$, p is a prime integer, n and r are positive integers and σ_i is the automorphism associated with u_i. Further, let the generators $\{u_i\}$ for U satisfy the additional condition that if $u_i \in U$, then $pu_i = u_iu_j = 0$. From the given multiplication in R, we see that if $r^{'} + \sum_{i=1}^{h} \lambda_iu_i$ and $s^{'} + \sum_{i=1}^{h} \lambda_iu_i, r^{'}, s^{'} \in R^{'}, \gamma_i, \lambda_i \in F_0$ are elements of R, then

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

It is easy to verify that the given multiplication turns R into a ring with identity $(1, 0, ..., 0)$. We also notice that $p \in J(R)$.

3 Preliminary Results

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

Remark: If n =1 or 2, then the construction yields rings in which multiplication of any two zero divisors is zero, that is, $(J(R))^2 = (0)$. Such rings are well known to be completely primary.

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

In the sequel, the rings that satisfy the above three properties shall be called, *rings with property A*.

Lemma 2. *Let R be a commutative ring with property A, then R^* is cyclic iff $1 + J(R)$ is cyclic. Moreover,*

$$R^* =< a > .(1 + J(R)) \cong< a > \times(1 + J(R)),$$

a direct product of the $p-$ group $1+J(R)$ by the cyclic subgroup $< a >$, where $o(a) = p^r - 1$.

Proof. Easily follows from the fact that R is a commutative completely primary finite ring. □

In order to completely classify R^*, we need to determine the structure of $1 + J(R)$.
Since R^* is abelian, $1 + J(R)$ is a normal subgroup of R^*.
In particular, let R be a ring with property A. Then $1 + J(R)$ is an abelian $p-$ subgroup of the unit group R^*. The group $1 + J(R)$ has a filtration

$$1 + J(R) \supset 1 + (J(R))^2 \supset ... \supset 1 + (J(R))^n = \{1\}$$

with filtration quotients

$$1+J(R)/1+(J(R))^2, 1+(J(R))^2/1+(J(R))^3, ..., 1+(J(R))^n/1 = 1+(J(R))^n$$

isomorphic to the additive groups

$$J(R)/(J(R))^2, (J(R))^2/(J(R))^3, ..., (J(R))^n$$

respectively.
We now state some Lemmata used in the determination of the structure of $1 + J(R)$.

Lemma 3. *For each prime integer p, $1 + pR^{'}$ is a subgroup of $1 + J(R)$.*

Proof. Easy □

Lemma 4. *For each $1 \leq j \leq h$, $1+\sum_{j=1}^{h} \oplus R^{'}u_j$ is a subgroup of $1+J(R)$.*

Proof. Easy □

Lemma 5. *Let $ann(J(R))$ be the two sided annihilator of $J(R)$. Then $1 + ann(J(R))$ is a subgroup of $1 + J(R)$.*

Proof. Obviously, $1 + ann(J(R)) = 1 + \sum_{j=1}^{h} \oplus R^{'} u_j$ when $charR = p$ or $1 + ann(J(R)) = 1 + p^{n-1}R^{'} \oplus \sum_{j=1}^{h} R^{'} u_j$ when $charR = p^t, t \geq 2$. We give the proof when $charR = p^t, t \geq 2$ as the other case easily follows from this (see the previous Lemma).Now, let $1 + p^{n-1}r^{'} + \sum_{j=1}^{h} \lambda_j u_j, 1 + p^{n-1}s^{'} + \sum_{j=1}^{h} \widehat{\lambda_j} u_j \in 1 + ann(J), \lambda_j, \widehat{\lambda_j} \in F_0, r^{'}, s^{'} \in R^{'}, 1 \leq j \leq h$. Then
$(1 + p^{n-1}r^{'} + \sum_{j=1}^{h} \lambda_j u_j)(1 + p^{n-1}s^{'} + \sum_{j=1}^{h} \widehat{\lambda_j} u_j)^{-1}$
$= (1 + p^{n-1}r^{'} + \sum_{j=1}^{h} \lambda_j u_j)(1 - p^{n-1}s^{'} - \sum_{j=1}^{h} \widehat{\lambda_j} u_j)$
$= 1 + p^{n-1}(r^{'} - s^{'}) + \sum_{j=1}^{h}(\lambda_j - \widehat{\lambda_j}) u_j$ an element of $1 + ann(J(R))$. □

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

Proof. Clearly $1+pR^{'}$ and $1+\sum_{i=1}^{h} \oplus R^{'} u_i$ are normal subgroups of $1+J(R)$. Also, $(1 + pR^{'}) \cap (1 + \sum_{i=1}^{h} \oplus R^{'} u_i) = \{1\}$. Finally

$$\begin{aligned} &\mid 1 + pR^{'} \mid \quad \mid 1 + \sum_{i=1}^{h} \oplus R^{'} u_i \mid \\ &= p^{(n-1)r} . p^{rh} \\ &= p^{(n+h-1)r} \\ &= \mid 1 + J(R) \mid . \end{aligned}$$

□

Remark: Since $U \subseteq ann(J(R)) = p^{n-1}R^{'} \oplus \sum_{i=1}^{h} \oplus R^{'} u_i$ or $\sum_{i=1}^{h} \oplus R^{'} u_i$ we notice that $pu_i = 0$ for each $u_i \in U, (1 \leq i \leq h)$.

4 Main Results

Proposition 2. *Let R be a commutative finite ring from the class of finite rings described by the construction. If U is generated by $\{u_1, ..., u_h\}$, then it is also generated by $\{u_1, u_1 + u_2, ..., u_1 + u_2 + ... + u_h\}$.*

Proposition 3. *Let R be a commutative finite ring from the class of finite rings described by the construction. If $h \geq 1$ and $charR = p$, then $1 + J(R) \cong (\boldsymbol{Z}_p^r)^h$.*

Proof. See e.g [4] □

Proposition 4. *Let R be a commutative finite ring from the class of finite rings described by the construction. If $h \geq 1$ and $charR = p^2$, then $1 + J(R) \cong \boldsymbol{Z}_p^r \times (\boldsymbol{Z}_p^r)^h$.*

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 note that for every $\nu = 1, ..., r$ $(1 + p\lambda_\nu)^p = 1$, $(1 + \lambda_\nu u_1)^p = 1$, $(1 + \sum_{i=1}^{2} \lambda_\nu u_i)^p = 1$,...,$(1+\sum_{i=1}^{h} \lambda_\nu u_i)^p = 1$. For positive integers α_ν , $\beta_{1\nu}$,..., $\beta_{h\nu}$ 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

$$\prod_{\nu=1}^{r}\{(1 + p\lambda_\nu)^{\alpha_\nu}\}.\prod_{\nu=1}^{r}\{(1 + \lambda_\nu u_1)^{\beta_{1\nu}}\}.$$
$$\prod_{\nu=1}^{r}\{(1 + \sum_{i=1}^{2} \lambda_\nu u_i)^{\beta_{2\nu}}\}...\prod_{\nu=1}^{r}\{(1 + \lambda_\nu u_i)^{\beta_{h\nu}} = \{1\}$$

will imply $\alpha_\nu = \beta_{i\nu} = p$ for every $\nu = 1, ..., r$ and $1 \leq i \leq h$. If we set

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

$$S_{1\nu} = \{(1 + \lambda_\nu u_1)^{\beta_1} \mid \beta_1 = 1, ..., p\}$$

$$S_{2\nu} = \{(1 + \sum_{i=1}^{2} \lambda_\nu u_i)^{\beta_2} \mid \beta_2 = 1, ..., p\}$$

$$\vdots$$

$$S_{h\nu} = \{(1 + \sum_{i=1}^{h} \lambda_\nu u_i)^{\beta_h} \mid \beta_h = 1, ..., p\}$$

we see that T_ν, $S_{1\nu}, ..., S_{h\nu}$ are all cyclic subgroups of the group $1 + J(R)$ and they are each of order p. Since

$$\prod_{\nu=1}^{r} |< 1 + p\lambda_\nu >| . \prod_{\nu=1}^{r} |< 1 + \lambda_\nu u_1 >| . \prod_{\nu=1}^{r} |< 1 + \sum_{i=1}^{2} \lambda_\nu u_i >|$$
$$... \prod_{\nu=1}^{r} |< 1 + \sum_{i=1}^{h} \lambda_\nu u_i >|= p^{(h+1)r}$$

and the intersection of any pair of the cyclic subgroups gives the identity group, the product of the $(h + 1)r$ subgroups T_ν, $S_{1\nu}$, $S_{2\nu}$,...,$S_{h\nu}$ is direct. So their product exhausts the group $1 + J(R)$. □

Proposition 5. *Let R be a ring with Property A. If $h \geq 1$,then*

$$1+J(R) \cong \begin{cases} \boldsymbol{Z}_2 \times \boldsymbol{Z}_{2^{n-2}} \times \boldsymbol{Z}_{2^{n-1}}^{r-1} \times (\boldsymbol{Z}_2^r)^h \text{ if } p=2 \\ \\ \boldsymbol{Z}_{p^{n-1}}^r \times (\boldsymbol{Z}_p^r)^h \text{ if } p \neq 2 \end{cases}$$

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 $GF(p)$. Since the two cases do not overlap, we consider them separately.

Case (i): $p = 2$.

Suppose $\nu = 1, ..., r$ and y is an element of $R^{'}$ such that $x^2 + x + \overline{y} = \overline{0}$ over $R^{'}/pR^{'}$ has no solution in the field $R^{'}/pR^{'}$, we obtain the following results:

$$-1 + 2^{n-1}\lambda_1 \in 1 + pR^{'}, (-1 + 2^{n-1}\lambda_1)^2 = 1, (1+4y)^{2^{n-2}} = 1$$

and $z^{2^{n-1}} = 1$ for each $z \in 1 + pR^{'}$. Also $(1+2\lambda_\nu)^{2^{n-1}} = 1$ for $\nu = 2, ..., r$,

$$(1+\lambda_\nu u_1)^2 = 1, (1+\sum_{i=1}^{2}\lambda_\nu u_i)^2 = 1, ..., (1+\sum_{i=1}^{h}\lambda_\nu u_i)^2 = 1$$

for every $\nu = 1, ..., r$. Now, consider positive integers α, β, κ_ν , $\tau_{1\nu}$,...,$\tau_{h\nu}$ with $\alpha \leq 2$, $\beta \leq 2^{n-2}$, $\kappa_\nu \leq 2^{n-1}$ for $2 \leq \nu \leq r$), and $\tau_{i\nu} \leq 2$ for every $\nu = 1, ..., r$ and $1 \leq i \leq h$. We notice that the equation

$$(-1+2^{n-1}\lambda_1)^\alpha.(1+4y)^\beta.\prod_{\nu=2}^{r}\{(1+2\lambda_\nu)^{\kappa_\nu}\}.\prod_{\nu=1}^{r}\{(1+\lambda_\nu u_1)^{\tau_{1\nu}}\}.$$
$$\prod_{\nu=1}^{r}\{(1+\sum_{i=1}^{2}\lambda_\nu u_i)^{\tau_{2\nu}}\}...\prod_{\nu=1}^{r}\{(1+\sum_{i=1}^{h}\lambda_\nu u_i)^{\tau_{h\nu}}\} = \{1\}$$

will imply $\alpha = 2$, $\beta = 2^{n-2}$, $\kappa_\nu = 2^{n-1}$ for $\nu = 2, ..., r$ and $\tau_{i\nu} = 2$ for each $\nu = 1, ..., r$ and $1 \leq i \leq h$. If we set

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

$$Q = \{(1+4y)^\beta \mid \beta = 1, ..., 2^{n-2}\},$$

$$T_\nu = \{(1+2\lambda_\nu)^\kappa \mid \kappa = 1, ..., 2^{n-1}\}, \nu = 2, ..., r$$

$$S_{1\nu} = \{(1+\lambda_\nu u_1)^{\tau_1} \mid \tau_1 = 1, 2\}$$

$$S_{2\nu} = \{(1+\sum_{i=1}^{2}\lambda_\nu u_i)^{\tau_2} \mid \tau_2 = 1, 2\}$$

$$\vdots$$

$$S_{h\nu} = \{(1 + \sum_{i=1}^{h} \lambda_\nu u_i)^{\tau_h} \mid \tau_h = 1, 2\}$$

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

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

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

Case (ii):p is odd

For every $\nu = 1, ..., r$, $(1 + p\lambda_\nu)^{p^{n-1}} = 1$, $(1 + \lambda_\nu u_1)^p = 1$, $(1 + \sum_{i=1}^{2} \lambda_\nu u_i)^p = 1$,...,$(1+\sum_{i=1}^{h} \lambda_\nu u_i)^p = 1$. For positive integers α_ν , $\beta_{1\nu}$,...,$\beta_{h\nu}$ with $\alpha_\nu \le p^{n-1}$, $\beta_{i\nu} \le p$ $(1 \le i \le h)$, we notice that the equation

$$\prod_{\nu=1}^{r}\{(1 + p\lambda_\nu)^{\alpha_\nu}\}.\prod_{\nu=1}^{r}\{(1 + \lambda_\nu u_1)^{\beta_{1\nu}}\}\prod_{\nu=1}^{r}\{(1 + \sum_{i=1}^{2} \lambda_\nu u_i)^{\beta_{2\nu}}\}$$
$$...\prod_{\nu=1}^{r}\{(1 + \sum_{i=1}^{h} \lambda_\nu u_i)^{\beta_{h\nu}} = \{1\}$$

will imply $\alpha_\nu = p^{n-1}$, $\beta_{i\nu} = p$ for every $\nu = 1, ..., r$ and $1 \le i \le h$. If we set

$$T_\nu = \{(1 + p\lambda_\nu)^{\alpha} \mid \alpha = 1, ..., p^{n-1}\},$$
$$S_{1\nu} = \{(1 + \lambda_\nu u_1)^{\beta_1} \mid \beta_1 = 1, ..., p\}$$
$$S_{2\nu} = \{(1 + \sum_{i=1}^{2} \lambda_\nu u_i)^{\beta_2} \mid \beta_2 = 1, ..., p\}$$
$$\vdots$$
$$S_{h\nu} = \{(1 + \sum_{i=1}^{h} \lambda_\nu u_i)^{\beta_h} \mid \beta_h = 1, ..., p\}$$

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

$$\prod_{\nu=1}^{r} |< 1 + p\lambda_\nu >| \,.\prod_{\nu=1}^{r} |< 1 + \lambda_\nu u_1 >| \,.\prod_{\nu=1}^{r} |< 1 + \sum_{i=1}^{2} \lambda_\nu u_i >|$$
$$...\prod_{\nu=1}^{r} |< 1 + \sum_{i=1}^{h} \lambda_\nu u_i >| = p^{(n+h-1)r}$$

and the intersection of any pair of the cyclic subgroups gives the identity group, the product of the $(h+1)r$ subgroups T_ν, $S_{1\nu}$, $S_{2\nu}$,...,$S_{h\nu}$ is direct. The product exhausts the group $1+J(R)$ and this completes the proof. □

We now state the main result.

Theorem 1. *The unit group R^* of the commutative completely primary finite ring R of characteristic p^n with maximal ideal $J(R)$ such that $(J(R))^2 = (0)$ when $n = 1, 2$; and $(J(R))^n = (0)$, $(J(R))^{n-1} \neq (0)$, when $n \geq 3$, and with invariants p (prime integer), $p \in J(R)$, $r \geq 1$ and $h \geq 1$ is a direct product of cyclic groups as follows:*
i) If $char R = p$, then

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

ii) If $char R = p^2$, then

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

iii) If $char R = p^n; n \geq 3$, then

$$R^* \cong \begin{cases} \boldsymbol{Z}_{2^r-1} \times \boldsymbol{Z}_2 \times \boldsymbol{Z}_{2^{n-2}} \times \boldsymbol{Z}_{2^{n-1}}^{r-1} \times (\boldsymbol{Z}_2^r)^h \text{ if } p = 2 \\ \\ \boldsymbol{Z}_{p^r-1} \times \boldsymbol{Z}_{p^{n-1}}^r \times (\boldsymbol{Z}_p^r)^h \text{ if } p \neq 2 \end{cases}$$

Acknowledgement. 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

[1] Chikunji C.J, *Unit groups of cube radical zero commutative completely primary finite rings*, International Journal of Mathematics and Mathematical sciences **2005:4** (2005),5799-592.

[2] Chikunji C.J ,*Unit groups of cube radical zero commutative completely primary finite rings* International Journal of Mathematics and Mathematical sciences, **4** (2005), 579-592.

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

[4] M.O. Oduor, C.J. Chikunji and N.O. Ongati, *Unit groups of $n+1$ index radical zero commutative finite rings*, IJPAM, **57:1** (2009), 57-67.

Received: January 5, 2013