International Journal of Pure and Applied Mathematics

Volume 54 No. 4 2009, 497-502

ON THE STRUCTURES OF QUOTIENT GROUPS

Omolo N. Ongati[1] [§], Owino Maurice Oduor[2]

[1,2]Department of Mathematics and Applied Statistics
Maseno University
P.O. Box 333, Maseno, KENYA

[1]e-mail: omolo_ongati@yahoo.com
[2]e-mail: morricearaka@yahoo.com

Abstract: Let J be the Jacobson radical of a commutative completely primary finite ring R such that $J^k \neq (0)$ and $J^{k+1} = (0)$. Then $R/J \cong GF(p^r)$, the finite field of p^r elements, and the characteristic of R is p^k where $k \geq 2$ and p is some prime integer. In this paper, we determine the structures of the quotient groups $1 + J^i/1 + J^{i+1}$ for every characteristic of R and $1 \leq i \leq k-1$.

AMS Subject Classification: 13M05, 16U60
Key Words: quotient groups, completely primary finite rings

1. Introduction

Throughout this paper, all the rings are finite and commutative with identities, denoted by $1 \neq 0$ and ring homomorphisms preserve identity. Upon consideration of s, t and λ to be the number of elements in the generating sets for U, V and W respectively, Chikunji in [1] determined in general the structure of $1 + W$ of the unit group of $R = R_0 \oplus U \oplus V \oplus W$ and the structure of the R^* of R when $s = 3$, $t = 1$, $\lambda \geq 1$ and the char$R = p$. Furthermore the author generalized the solution of the cases when $s = 2$, $t = 1$; $t = s(s+1)/2$ for a fixed s, and $p \leq \text{char}R \leq p^3$; and when $s = 2$, $t = 2$ and char$R = p$ to the case when the annihilator, ann$(J) = J^2 + W$, so that $\lambda \geq 1$.

Received: May 22, 2009

[§]Correspondence author

Let R be a completely primary finite ring with maximal ideal J such that $J^{k+1} = (0)$, $J^k \neq (0)$, $k \geq 1$. Then the residue field R/J is a finite field $GF(p^r)$, for some prime integer p and positive integer r. The characteristic of R is p^k for some positive integer k. Let $R_0 = GR(p^{kr}, p^k)$ be the Galois ring of characteristic p^k and order p^{kr}. A concrete model is the quotient $\mathbf{Z}_{p^k}[x]/(f)$ where $f \in \mathbf{Z}_{p^k}[x]$ is a monic polynomial of degree r irreducible modulo p. Then it can be deduced from the main theorem in [2] that R has a coefficient subring R_0 of the form $GR(p^{kr}, p^k)$ which is clearly a maximal Galois subring of R. A trivial case is $GR(p^k, p^k) = \mathbf{Z}_{p^k}$. We construct commutative finite rings with unique maximal ideal J such that $J^{k+1} = (0)$ and $J^k \neq (0)$ for the cases when $\mathrm{char}R = p^2$ and $\mathrm{char}R = p^k : k \geq 3$. Then we determine the structures of the quotient groups of the rings constructed.

The following results are fundamental to the study of unit groups of the rings to be considered in this paper.

1.1. *Let R be a finite ring. Then every left unit is a right unit and every left zero divisor is a right zero divisor. Furthermore, every element of R is either a zero divisor or a unit* (see [3]).

1.2. *If a ring has two or more zero divisors (including zero), then R is a finite ring* (see [4]).

2. A Class of Finite Rings

Let R_0 be the Galois ring of the form $GR(p^{kr}, p^k)$ and let $u_i \in J$, where $1 \leq i \leq h-1$ so that $R = R_0 \oplus R_0u_1 \oplus ... \oplus R_0u_{h-1}$ is an additive group. On the additive group, define multiplication by the following relations: $u_iu_j = 0$ $(1 \leq i, j \leq h-1)$; $r_0u_i = u_ir_0$, $r_0 \in R_0$; $p^{k-1}u_i \neq 0$. From the given definition of multiplication in R, we see clearly that if $(r_0, r_1, ..., r_{h-1})$ and $(s_0, s_1, ..., s_{h-1})$ are any two elements in R, then

$$(r_0, r_1, ..., r_{h-1})(s_0, s_1, ..., s_{h-1}) = (r_0s_0, r_0s_1 + r_1s_0, ..., r_0s_{h-1} + r_{h-1}s_0).$$

It is then easy to show that the given multiplication turns the additive group into a ring.

When char $R = p^k$, where $k \in \mathbf{Z}^+$, we determine the structures of the quotient groups of the ring R.

3. Quotient Groups

It is an established fact that a ring R defined by the construction in Section 2 satisfies the following property: the subset of all its zero divisors forms a unique maximal ideal J and $1+J$ is a normal subgroup of its group of units R^*. Suppose $k \geq 2$, then the ideals J, J^2, J^3,...,J^k and J^{k+1} in R, form a chain

$$J \supset J^2 \supset J^3 \supset ... \supset J^{k+1} = (0)$$

and consequently, the subgroups $1+J$, $1+J^2$,$1+J^3$,...,$1+J^k$, $1+J^{k+1} = \{1\}$ forms a filtration

$$1+J \supset 1+J^2 \supset 1+J^3 \supset ... \supset 1+J^k \supset 1+J^{k+1} = \{1\}.$$

Let R be a ring defined in Section 2 and J be the Jacobson radical of the ring such that for $k \geq 2$, $J^k \neq (0)$ and $J^{k+1} = (0)$.

We begin by showing that for $j = 1, 2, ..., k-1$, the quotient J^j/J^{j+1} is a vector space over the quotient ring R/J.

Lemma 1. *Let J be the Jacobson radical of a ring R defined in Section 2. Then the quotient J^j/J^{j+1}, $j = 1, 2, ..., k-1$ is a vector space over $GF(p) \subseteq R/J$.*

Proof. Given that J is a maximal ideal in R, the quotient ring R/J is a field. For every prime integer p, let $\mathbf{F}_p$ be a prime subfield of R/J. Let $y_1, y_2 \in J^j$ such that $y_1 + J^{j+1}$ and $y_2 + J^{j+1}$ belong to J^j/J^{j+1}, then for each $a \in \mathbf{F}_p$,

$$a((y_1 + J^{j+1}) + (y_2 + J^{j+1})) = a((y_1 + y_2) + J^{j+1}) = (a(y_1 + y_2)) + J^{j+1},$$

which belongs to J^j/J^{j+1}. □

Now,

$$| R | = | R/J | . | J/J^2 | ... | J^{k-1}/J^k | . | J^k |$$

$$= p^{(1+\overbrace{h + ... + h}^{k-1 \text{ times}} + h - 1)r} = p^{khr}, \quad h \geq 2.$$

Thus R is indeed finite.

Remark. Finiteness of R implies that J is nilpotent, say $J^{k+1} = (0)$.

Notice that $1 + J^{j+1}$ is a normal subgroup of $1 + J^j$ and by Lagrange's theorem $| 1 + J^j/1 + J^{j+1} | = p^{hr}$, where $j = 1, ..., k-1$. We now determine the structure of $1 + J^j/1 + J^{j+1}$ for $j = 1, 2, ..., k-1$. We begin with the case, when char $R = p^2$.

Proposition 1. *Let R be a ring defined in Section 2. Suppose J is the*

Jacobson radical of R, then for $k = 2$, the quotient group $1 + J/1 + J^2 \cong \underbrace{\boldsymbol{Z}_p^r \times ... \times \boldsymbol{Z}_p^r}_{h \text{ copies}}$ for every prime integer p.

Proof. Let $\tau_1, ..., \tau_r \in R_0$ such that $\overline{\tau_1}, ..., \overline{\tau_r} \in R_0/pR_0$ form a basis for R_0/pR_0 regarded as a vector space over its prime subfield $\mathbf{F}_p$. Consider the element $(1 + p\tau_l)1 + J^2 \in 1 + J/1 + J^2$. Then

$$\begin{aligned}((1 + p\tau_l)1 + J^2)^p &= (1 + p\tau_l)^p 1 + J^2 \\ &= (1 + p^2\tau_l + ... + p^p\tau_l{}^p)1 + J^2 = 1 + J^2 \text{ since } \operatorname{char} R = p^2 .\end{aligned}$$

Next, consider the element $(1 + \tau_l u_1)1 + J^2 \in 1 + J/1 + J^2$. Then

$$\begin{aligned}((1 + \tau_l u_1)1 + J^2)^p &= (1 + \tau_l u_1)^p 1 + J^2 \\ &= (1 + p\tau_l u_1)1 + J^2 = 1 + J^2 \text{ since } 1 + p\tau_l u_1 \in 1 + J^2 .\end{aligned}$$

Similarly, $((1 + \tau_l u_1 + \tau_l u_2)1 + J^2)^p = 1 + J^2$. Continuing in a similar manner up to the element $(1 + \tau_l u_1 + \tau_l u_2 + ... + \tau_l u_{h-1})1 + J^2$ we obtain $((1 + \tau_l u_1 + \tau_l u_2 + ... + \tau_l u_{h-1})1 + J^2)^p = 1 + J^2$. For positive integers a_l, b_{1l}, b_{2l},...,$b_{(h-1)l}$ with $a_l \leq p$, $b_{il} \leq p$ where $1 \leq i \leq h - 1$, we assert that

$$\prod_{l=1}^{r}\{(1 + p\tau_l)1 + J^2)^{a_l}\}.\prod_{l=1}^{r}\{(1 + \tau_l u_1)1 + J^2)^{b_{1l}}\}.\prod_{l=1}^{r}\{(1 + \tau_l u_1 + \tau_l u_2)$$

$$1 + J^2)^{b_{2l}}\}...\prod_{l=1}^{r}\{(1 + \tau_l u_1 + \tau_l u_2 + ... + \tau_l u_{h-1})1 + J^2)^{b_{(h-1)l}}\} = 1 + J^2$$

will imply $a_l = p$, $b_{il} = p$ for every $l = 1, ..., r$ and $1 \leq i \leq h - 1$. If we set

$$T_l = \{((1 + p\tau_l)1 + J^2)^a \mid a = 1, ..., p\},$$

$$S_{1l} = \{((1 + \tau_l u_1)1 + J^2)^{b_1} \mid b_1 = 1, ..., p\},$$

$$S_{2l} = \{((1 + \tau_l u_1 + \tau_l u_2)1 + J^2)^{b_2} \mid c_2 = 1, ..., p\},$$

$$\vdots$$

$$S_{(h-1)l} = \{((1 + \tau_l u_1 + \tau_l u_2 + ... + \tau_l u_{h-1})1 + J^2)^{b_{h-1}} \mid b_{h-1} = 1, ..., p\},$$

we see that T_l, S_{1l}, S_{2l},...,$S_{(h-1)l}$ are all cyclic subgroups of the group $1+J/1+J^2$ and they are of the orders indicated by their definition. Since

$$\prod_{l=1}^{r} |< (1+p\tau_l)1+J^2 >| .\prod_{l=1}^{r} |< 1+\tau_l u_1 >| .\prod_{l=1}^{r} |< (1+\tau_l u_1+\tau_l u_2)1+J^2 >|$$

$$... \prod_{l=1}^{r} |< (1 + \tau_l u_1 + \tau_l u_2 + ... + \tau_l u_{h-1})1 + J^2 >| = p^{rh}$$

and the intersection of any pair of the cyclic subgroups gives the identity group $1 + J^2$, the product of the hr subgroups T_l, S_{1l}, S_{2l},...,$S_{(h-1)l}$ is direct. So their product exhausts the group $1 + J/1 + J^2$. □

Proposition 2. *Let R be a ring defined in Section 2. Suppose J is the Jacobson radical of R, then for $k \geq 3$, the quotient group $1 + J^j/1 + J^{j+1} \cong \underbrace{\boldsymbol{Z}_p^r \times ... \times \boldsymbol{Z}_p^r}_{h \text{ copies}}$ for every prime integer p.*

Proof. Let $\tau_1, ..., \tau_r \in R_0$ such that $\overline{\tau_1}, ..., \overline{\tau_r} \in R_0/pR_0$ form a basis for R_0/pR_0 regarded as a vector space over its prime subfield $\mathbf{F}_p$.

Suppose $j = 1$. Then the proof is obviously the one given for Proposition 1.

Suppose $j \geq 2$.

Let $y \in R_0$. Consider the element $(1 + p^j\tau_l + p^{j-1}\tau_l y u_1)1 + J^{j+1} \in 1 + J^j/1 + J^{j+1}$. Then

$$\begin{aligned}((1 + p^j\tau_l + p^{j-1}\tau_l y u_1)1 + J^{j+1})^p &= (1 + p^j\tau_l + p^{j-1}\tau_l y u_1)^p 1 + J^{j+1} \\ &= (1 + p^j\tau_l y u_1)1 + J^{j+1} = 1 + J^{j+1} \text{ since } 1 + p^j\tau_l y u_1 \in 1 + J^{j+1}.\end{aligned}$$

Next, consider the element $(1+p^{j-1}\tau_l y u_1)1+J^{j+1} \in 1+J^j/1+J^{j+1}$. Then

$$\begin{aligned}((1 + p^{j-1}\tau_l y u_1)1 + J^{j+1})^p &= (1 + p^{j-1}\tau_l y u_1)^p 1 + J^{j+1} \\ &= (1 + p^j\tau_l y u_1)1 + J^{j+1} = 1 + J^{j+1} \text{ since } 1 + p^j\tau_l y u_1 \in 1 + J^{j+1}.\end{aligned}$$

Similarly, $((1 + p^{j-1}\tau_l y u_1 + p^{j-1}\tau_l y u_2)1 + J^{j+1})^p = 1 + J^{j+1}$. Continuing in a similar manner up to the element $(1 + p^{j-1}\tau_l y u_1 + p^{j-1}\tau_l y u_2 + ... + p^{j-1}\tau_l y u_{h-1})1+J^{j+1}$ we obtain $((1+p^{j-1}\tau_l y u_1+p^{j-1}\tau_l y u_2+...+p^{j-1}\tau_l y u_{h-1})1+J^{j+1})^p = 1+J^{j+1}$. Now, for positive integers a_l, b_{1l},...,$b_{(h-1)l}$ with $a_l \leq p$, $b_{il} \leq p$ for every $l = 1, ..., r$ and $1 \leq i \leq h-1$, we assert that

$$\prod_{l=1}^{r}\{(1 + p^j\tau_l + p^{j-1}\tau_l y u_1)1 + J^{j+1})^{a_l}\}.\prod_{l=1}^{r}\{((1 + p^{j-1}\tau_l y u_1)1 + J^{j+1})^{b_{1l}}\}$$

$$\prod_{l=1}^{r}\{((1 + p^{i-1}\tau_l y u_1 + p^{i-1}\tau_l y u_2)1 + J^{j+1})^{b_{2l}}\}...$$

$$\prod_{l=1}^{r}\{(1 + p^{j-1}\tau_l y u_1 + p^{j-1}\tau_l y u_2 + ... + p^{j-1}\tau_l y u_{h-1})1 + J^{j+1})^{b_{(h-1)l}}\}$$

$$= 1 + J^{j+1}$$

will imply $a_l = p$, $b_{il} = p$ for every $l = 1, ..., r$ and $1 \leq i \leq h-1$. If we set

$$T_l = \{((1 + p^j\tau_l + p^{j-1}\tau_l y u_1)1 + J^{j+1})^a \mid a = 1, ..., p\},$$

$$S_{1l} = \{((1 + p^{j-1}\tau_l y u_1)1 + J^{j+1})^{b_1} \mid b_1 = 1, ..., p\},$$

$$S_{2l} = \{((1 + p^{j-1}\tau_l y u_1 + p^{j-1}\tau_l y u_2)1 + J^{j+1})^{b_2} \mid b_2 = 1, ..., p\}$$

$$\vdots$$

$$S_{(h-1)l} = \{((1 + p^{j-1}\tau_l y u_1 + p^{j-1}\tau_l y u_2 + ... + p^{j-1}\tau_l y u_{h-1})1 + J^{j+1})^{b_{h-1}} \mid b_{h-1} = 1, ..., p\},$$

we see that T_l, S_{1l}, S_{2l},...,$S_{(h-1)l}$ are all cyclic subgroups of the group $1+J^j/1+J^{j+1}$ and they are of the orders indicated by their definition. Since

$$\prod_{l=1}^{r} |< (1 + p^j\tau_l + p^{j-1}\tau_l y u_1)1 + J^{j+1} >| . \prod_{l=1}^{r} |< (1 + p^{j-1}\tau_l y u_1)1 + J^{j+1} >| .$$

$$\prod_{l=1}^{r} |< (1 + p^{j-1}\tau_l y u_1 + p^{j-1}\tau_l y u_2)1 + J^{j+1} >|$$

$$... \prod_{l=1}^{r} |< (1 + p^{j-1}\tau_l y u_1 + p^{j-1}\tau_l y u_2 + ... + p^{j-1}\tau_l y u_{h-1})1 + J^{j+1} >|$$

$$= p^{rh}$$

and the intersection of any pair of the cyclic subgroups gives $1 + J^{i+1}$, the product of the hr subgroups T_l, S_{1l}, S_{2l},...,$S_{(h-1)l}$ is direct. So their product exhausts the group $1 + J^j/1 + J^{j+1}$. □

References

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

[2] W.E. Clark, A coefficient ring for finite non-commutative rings, *Proc. Amer. Math. Soc.*, **33** (1972), 25-28.

[3] B. Corbas, Rings with finite zero divisors, *Math. Ann.*, **181** (1969), 1-7.

[4] B. Corbas, Finite rings in which the product of any two zero divisors is zero, *Math. Ann.* (1970), 466-469.