On the Regular Elements of a Class of Commutative Completely Primary Finite Rings

Article · January 2015

DOI: 10.12988/ija.2015.516

Maurice Owino Oduor
University of Kabianga

International Journal of Algebra, Vol. 9, 2015, no. 3, 101 - 107
HIKARI Ltd, www.m-hikari.com
http://dx.doi.org/10.12988/ija.2015.516

On the Regular Elements of a Class of Commutative Completely Primary Finite Rings

Owino Maurice Oduor

Department of Mathematics and Computer Science
University of Kabianga
P.O. Box 2030-20200, Kericho, Kenya

Musoga Christopher

Department of Mathematics
Masinde Muliro University of Science and Technology
P.O. Box 190-50100, Kakamega, Kenya

Abstract

In this paper, a class of completely primary finite rings of characteristic p^k has been constructed . The objective is to investigate the inverses of regular elements in the class of rings.

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

Keywords: Completely primary finite rings, Regular elements, Von-Neumann inverses

1 Introduction

The classification of finite rings still remains elusive . Every element in a finite ring with identity is either a zero divisor or a unit. It is well known that every commutative finite ring is a direct sum of completely primary finite rings . The study on the structures of units and zero divisors has not been exhausted. An element $a \in R$ is said to be Von-Neumann regular if there exists an element $b \in R$ such that $a = a^2 b$, where b is the Von-Neumann Inverse of a , See e.g [3]. An element of R is regular if it is either a unit or zero.This article investigates the inverses of regular elements in R.

Unless otherwise stated, $J(R)$ shall denote the Jacobson radical of a completely primary finite ring R. The set of all the regular elements in R shall be denoted by $V(R)$. The rest of the notations used in this article are standard and reference may be made to [1], [2], [4] and [6].

2 Regular elements of Galois Rings

Let R be a completely primary finite ring with a unique maximal ideal J. Then R is of order p^{nr}; J is the Jacobson radical of R; $J^m = (0)$ where $m \leq n$ and the residue field $R/J \cong F_{p^r}$ is a finite field for some prime integer p and positive integer r. The characteristic of R is p^k where k is an integer such that $1 \leq k \leq m$. If $k = m = n$, then $R = \mathbb{Z}_{p^k}[b]$ where b is an element of R of multiplicative order $p^r - 1$; $J = pR$ and $\mathrm{Aut}(R) \cong \mathrm{Aut}(R/pR)$. Such a ring is called a Galois ring , denoted by $GR(p^{kr}, p^k)$. Now,$GR(p^{kr}, p^k) = \mathbb{Z}_{p^k}[x]/(f)$ where $f \in \mathbb{Z}_{p^k}[x]$ is a monic polynomial of degree r whose image in $\mathbb{Z}_p[x]$ is irreducible.

The results on trivial Galois rings can be obtained from [3]. The proofs have been made more elaborate. Consider the trivial Galois ring $GR(p^k, p^k) = \mathbb{Z}_{p^k}$. Then for each natural number p^k, the function $\varphi(p^k)$ is the number of integers x such that $1 \leq x \leq p^k$ and g.c.d (x, p^k)=1, $\varpi(p^k)$ is the number of distinct primes dividing p^k, $\tau(p^k)$ is the number of divisors of p^k and $\sigma(p^k)$ is the sum of the divisors of p^k.

Proposition 1 (See [3])**.** *Let p and k be a prime and a positive integer respectively.An element a is regular in $GR(p^k, p^k)$ iff $a^{p^k - p^{k-1}+1} \equiv a (mod\ p^k)$*

Proof. Suppose a is a regular element in $\mathbb{Z}_{p^k}$. If $a \equiv 0(\mathrm{mod}\ p^k)$, then $a^{p^k - p^{k-1}+1} \equiv a(\mathrm{mod}\ p^k)$. Now , let a be a unit(mod p^k). Using Euler's theorem, $a^{p^k - p^{k-1}} \equiv 1(\mathrm{mod}\ p^k)$. Therefore $a^{p^k - p^{k-1}+1} \equiv a(\mathrm{mod}\ p^k)$.
Conversely , $a \equiv a^{p^k - p^{k-1}+1} \equiv a^2 a^{p^k - p^{k-1}-1}(\mathrm{mod}\ p^k)$, so that a is a regular element.

Corollary 1 (See [3])**.** *Let $0 \neq a$ be a regular element in $GR(p^k, p^k)$, then $a^{p^k - p^{k-1}-1}$ is a Von-Neumann inverse of a in $GR(p^k, p^k)$.*

Proposition 2 (See [3])**.** *Let $R = GR(p^k, p^k)$. Then $V(p^k) = p^k - p^{k-1} + 1 = \varphi(p^k) + 1 = p^k(1 - \frac{1}{p} + \frac{1}{p^k})$*

Proof. Since $GR(p^k, p^k)$ is local , every regular element in the ring is either zero or a unit . Now, the number of all the units of the ring is $p^k - p^{k-1}$ and the zero element in the ring is unique . Thus the result easily follows.

Proposition 3 (See [3]). *Let p and k be a prime and a positive integer respectively. Then $V(p^k) = \sum_{t\|p^k} \varphi(t)$ and $V(p^k)/\varphi(p^k) = \sum_{t\|p^k} 1/\varphi(t)$.*

Proof. In $GR(P^k, p^k)$, the unitary divisors are 1 and $p^k \equiv 0(\text{mod } p^k)$. By definition, $\varphi(1)$=1. But $V(p^k) = p^k - p^{k-1} + 1 = \varphi(p^k) + 1 = \varphi(p^k) + \varphi(1)$. Further, $\frac{V(p^k)}{\varphi(p^k)} = \frac{p^k - p^{k-1}+1}{p^k - p^{k-1}} = 1 + \frac{1}{p^k - p^{k-1}}$

$$= \frac{1}{\varphi(1)} + \frac{1}{\varphi(p^k)}.$$

The summatory function $F(p^k)$ is given by
$F(p^k) = \sum_{t|p^k} V(t) = \sum_{i=0}^{k} V(p^i) = V(1) + \sum_{i=1}^{k} V(p^i)$

$$= V(1) + \sum_{i=1}^{k} [(p^i - p^{i-1}) + 1]$$

$$= 1 + (p + p^2 + ... + p^k) - (1 + p + p^2 + ... + p^{k-1}) + k$$

$$= p^k + k.$$

Theorem 2 (See [3]). *Let $R = GR(p^k, p^k)$, then $\sigma(p^k) + \varphi(p^k) \leq p^k \tau(p^k)$.*

Proof. Let k=1, then $\sigma(p) = p+1$ and $\varphi(p) = p-1$ so that $\sigma(p)+\varphi(p) = 2p$. Since p has only two divisors, that is 1 and p, then $2p = p\tau(p)$.
Thus $\sigma(p) + \varphi(p) = p\tau(p)$.
Now , suppose $k > 1$, then $\sigma(p^k) = \sum_{i=0}^{k} p^i$ and $\varphi(p^k) = p^k - p^{k-1}$, so that $\sigma(p^k) + \varphi(p^k) = 1 + p + ... + p^k + p^k - p^{k-1}$

$$= 2p^k + p^{k-2} + ... + p + 1 < (k+1)p^k.$$

But p^k has $(k+1)$ divisors, so that $(k+1)p^k = p^k\tau(p^k)$.
Thus $\sigma(p^k) + \varphi(p^k) < p^k\tau(p^k)$.

Lemma 1 (See [3]). *Let $R = GR(p,p) = \mathbb{F}_p$. Then $\sigma(p) + V(p) > p\tau(p)$*

Proof. Clearly $\sigma(p) = p + 1$ and $V(p) = p$.
So $\sigma(p) + V(p) = 2p + 1 > 2p = p\tau(p)$.

Theorem 3 (See [3]). *Let $R = GR(p^k, p^k)$. If $k > 1$, then $\sigma(p^k)+V(p^k) < p^k\tau(p^k)$*

Proof. Clearly $1 + \frac{1}{p} + \frac{1}{p^2} + ... + \frac{1}{p^k} < k = (k+1) - 1 = \tau(p^k) - 1$
So $\frac{\sigma(p^k)}{p^k} = \frac{1+p+p^2+...+p^k}{p^k} < \tau(p^k) - 1$.
Now, $\sigma(p^k) < p^k(\tau(p^k) - 1) = p^k\tau(p^k) - p^k$.
Since $V(p^k) < p^k$, we obtain $\sigma(p^k) < p^k\tau(p^k) - V(p^k)$.

Lemma 2. *Let $R_0 = GR(p^r, p)$ for some prime integer p and positive integer r. Then $V(R_0) = R_0$.*

Proof. Clearly $V(R_0) \subseteq R_0$ because every element in $V(R_0)$ belongs to R_0. On the other hand , let $a \in R_0$. Then a is either a unit or zero. Thus $a \in V(R_0)$. So $R_0 \subseteq V(R_0)$. This completes the proof.

We now characterize the VonNeumann inverses of regular elements in $GR(p^r, p)$.

Lemma 3. *Let $R_0 = GR(p^r, p)$, for some prime integer p and positive integer r. If $a \neq 0$ is regular in R_0, then $a^{-1} \equiv a^{(V(p))^r - 2}(\mathrm{mod}\ p)$.*

Proof. Clearly $V(p) = p$. Since R_0 is a field of order p^r, every nonzero element in R_0 is invertible. Let $0 \neq a \in R_0$, then by Euler's theorem, $a^{p^r - 1} \equiv 1(\mathrm{mod}\ p)$.
Multiplying both sides by a^{-1}, we obtain $a^{p^r - 2} \equiv a^{-1}(\mathrm{mod}\ p)$.
Since $\equiv$ is symmetric , the result follows.

Lemma 4. *Let $R = GR(p^{kr}, p^k)$ where p is a prime integer , k and r are positive integers. Then $V(R) = R^* \cup \{0\}$ and $\mid V(R) \mid = p^{(k-1)r}(p^r - 1) + 1$*

Proof. Let $a \in R^* \cup \{0\}$, then a is either a unit or zero. Since R is local, a is a regular element, that is $a \in V(R)$. So $R^* \cup \{0\} \subseteq V(R)$. On the other hand, let $a \in V(R)$, then there exists an element $b \in R$ such that $a = a^2b$,that is $a(1 - ab) = 0$. If a is a unit, then $1 - ab = 0$, so that $ab = 1$ and b is the VonNeumann inverse of a. If a is a nonunit, then ab is a nonunit. But $ab = a^2b^2 = aabb = abab = (ab)^2$ because R is commutative. So $ab = (ab)^2$. $\Rightarrow ab(1 - ab) = 0$. Since $1 - ab$ is a unit, $ab = 0$. so that $a = 0$ because b is its VonNeumann inverse.
Thus $V(R) \subseteq R^* \cup \{0\}$. Now $R^* = (R^*/1 + J) \times 1 + J \cong \mathbb{Z}_{p^r - 1} \times 1 + J$. But $\mid 1 + J \mid = \mid J \mid = \mid pGR(p^{kr}, p^k) \mid = p^{(k-1)r}$. Therefore $\mid R^* \mid = (p^r - 1)(p^{(k-1)r})$. Since $V(R) = R^* \cup \{0\}$, the last statement easily follows.

Proposition 4. *Let $R_0 = GR(p^{kr}, p^k)$. Suppose a is a regular element in R_0, then its VonNeumann inverse is given as $a^{-1} \equiv a^{p^{(k-1)r}(p^r - 1) - 1}(\mathrm{mod}\ p^k)$.*

Proof. If a is regular in R, then $a \equiv a^{|R^*|+1} \equiv a^{p^{(k-1)r}(p^r-1)+1} \equiv a^2 a^{p^{(k-1)r}(p^r-1)-1}(\mathrm{mod}\ p^k)$. So that $a^{-1} \equiv a^{p^{(k-1)r}(p^r-1)-1}(\mathrm{mod}\ p^k)$.

3 Regular elements of completely primary finite rings of characteristic p^k

Let R_0 be the Galois ring of the form GR(p^{kr}, p^k). For each $i = 1, ..., h$, let $u_i \in J(R)$ such that U is h-dimensional R_0-module generated by $u_1, ..., u_h$ so that $R = R_0 \oplus U = R_0 \oplus \sum_{i=1}^{h} \oplus (R_0/pR_0)^i$ is an additive group. On this group, define multiplication as follows:

$(r_0, \overline{r_1}, \overline{r_2}, ..., \overline{r_h})(s_0, \overline{s_1}, \overline{s_2}, ..., \overline{s_h}) = (r_0 s_0, r_0\overline{s_1} + \overline{r_1}s_0, r_0\overline{s_2} + \overline{r_2}s_0, ..., r_0\overline{s_h} + \overline{r_h}s_0)$.

It is well known that this multiplication turns R into a completely primary finite ring with identity $(1, \overline{0}, \overline{0}, ..., \overline{0})$.
The structure of the group of units of this ring is well known and reference may be made to [5].

Theorem 4. *Let R be the ring constructed in this section, it's regular elements are classified as follows;*

(i)If char $R = p$, then $V(R) \cong \mathbb{Z}_{p^r-1} \times (\mathbb{Z}_p^r)^h \cup \{0\}$

(ii)If char $R = p^2$, then $V(R) \cong \mathbb{Z}_{p^r-1} \times \mathbb{Z}_p^r \times (\mathbb{Z}_p^r)^h \cup \{0\}$

(iii)If char $R = p^k, k \geq 3$, then

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

Proof. This is a consequence of Theorem 1 in [5].

Proposition 5. *Let $R_0 = GR(p^k, p^k)$ and $U = R_0/pR_0 \oplus .... \oplus R_0/pR_0$ be an R-module generated by h elements so that* $R = R_0 \oplus U = R_0 \oplus \underbrace{R_0/pR_0 \oplus .... \oplus R_0/pR_0}_{hsummands}$.
If s_0 is regular in R_0, then its VonNeumann inverse $s_0^{-1} = s_0^{p^k - p^{k-1} - 1}$, and $(s_0, s_1, s_2, ..., s_h)^{-1} = (s_0^{p^k - p^{k-1} - 1}, -s_1 t_0 s_0^{-1}, ..., -s_h t_0 s_0^{-1})$.

Proof. For the inverse of s_0, refer to Proposition 4.
Now let $(t_0, t_1, t_2, ..., t_h) = (s_0, s_1, s_2, ..., s_h)^{-1}$, then $(s_0, s_1, ..., s_h) = (s_0, s_1, s_2, ..., s_h)^2$ $(t_0, t_1, t_2, ..., t_h) = (s_0^2, s_0 s_1 + s_1 s_0, ..., s_0 s_h + s_h s_0)(t_0, t_1, ..., t_h) = (s_0^2 t_0, s_0^2 t_1 + (s_0 s_1 + s_1 s_0)t_0, ..., s_0^2 t_h + (s_0 s_h + s_h s_0)t_0)$
So $s_0 = s_0^2 t_0$. $\Rightarrow s_0 t_0 = 1$
$\Rightarrow t_0 = s_0^{-1} = s_0^{p^k - p^{k-1} - 1}$.
For $i = 1, ..., h, s_i = s_0^2 t_i + (s_0 s_i + s_i s_0)t_0$
$\Rightarrow s_0^2 t_i = s_i - (s_0 s_i + s_i s_0)t_0$
$t_i = \frac{s_i - 2s_0 s_i t_0}{s_0^2}$ because R is commutative.

$t_i = \frac{s_i}{s_0^2} - \frac{2s_i t_0}{s_0} = \frac{s_i t_0}{s_0} - \frac{2s_i t_0}{s_0}$
$= \frac{-s_i t_0}{s_0} = -s_i t_0 s_0^{-1}$
$= -s_i s_0^{-2}$.
So $(s_0, s_1, s_2, ..., s_h)^{-1} = (s_0^{p^k - p^{k-1} - 1}, -s_1 s_0^{-2}, ..., -s_h s_0^{-2})$

Theorem 5. *Let $R = R_0 \oplus R_0 u_1 \oplus ..... + R_0 u_h$, then $r \in R$ is regular iff either it is zero or a unit in R.*

Proof. $V(R) = R^* \cup \{0\} = (R^*/1 + J(R)).(1 + J(R)) \cup \{0\}$

$$= < a > .(1 + J(R)) \cup \{0\}$$

$$\cong < a > \times (1 + J(R)) \cup \{0\}$$

$$\cong \mathbb{Z}_{p^r - 1} \times (1 + J(R)) \cup \{0\}.$$

4 Main Result

Proposition 6. *Let $R_0 = GR(p^{kr}, p^k)$ and $U = R_0/pR_0 \oplus ...... \oplus R_0/pR_0$ be an R-module generated by h elements so that $R = R_0 \oplus U = R_0 \oplus \underbrace{R_0/pR_0 + ... \oplus R_0/pR_0}_{hsummands}$. If s_0 is regular in R_0, then its VonNeumann inverse is $s_0^{-1} = s_0^{p^{(k-1)r}(p^r - 1) - 1}$ and $(s_0, s_1, ..., s_h)^{-1} = (s_0^{p^{(k-1)r}(p^r-1)-1}, -s_1 t_0 s_0^{-1}, ..., -s_h t_0 s_0^{-1})$*

Proof. Follows from Propositions 4 and 5.

References

[1] A. Osba, M. Henriksen, A. Osama and F. Smith, *The Maximal Regular Ideals of some commutative Rings*, Comment. Math. Univ. Carolinea, vol **47**,1, (2006),1-10.

[2] A. Osba, M. Henriksen and A. Osama, *Combining Local and VonNeumann Regular Rings*, Comm. Algebra, **32** (2004), 2639 - 2653. http://dx.doi.org/10.1081/agb-120037405

[3] A. Osama and A.O. Emad, *On the Regular Elements in $\mathbb{Z}_n$*, Turkish Journal of Mathematics, **32**,(2008),31-39.

[4] C.J. Chikunji, *Unit Groups of Cube Radical Zero Commutative Completely Primary finite Rings*, International Journal of Mathematics and Mathematical Sciences, **4** (2005), 579-592. http://dx.doi.org/10.1155/ijmms.2005.579

[5] M.O. Oduor, M.O. Ojiema and E. Mmasi, *Units of commutative completely primary finite rings of characteristic* p^n, IJPAM, Vol. **7** (2013), 259-266.

[6] M.O. Oduor, A.L. Omamo and C. Musoga, *On the Regular Elements of Rings in which the product of any two zero divisors lies in the Galois subring*, IJPAM, Vol. **86** (2013), 7-18.
http://dx.doi.org/10.12732/ijpam.v86i1.2

Received: February 14, 2015; Published: March 12, 2015