PUBLICATIONS DE L'INSTITUT MATHÉMATIQUE
Nouvelle série, tome 95 (109) (2014), 215–220 DOI: 10.2298/PIM1409215C

UNIT GROUPS OF FINITE RINGS WITH PRODUCTS OF ZERO DIVISORS IN THEIR COEFFICIENT SUBRINGS

Chiteng'a John Chikunji

Communicated by Siniša Crvenković

Abstract. Let R be a completely primary finite ring with identity $1 \neq 0$ in which the product of any two zero divisors lies in its coefficient subring. We determine the structure of the group of units G_R of these rings in the case when R is commutative and in some particular cases, obtain the structure and linearly independent generators of G_R.

1. Introduction

All rings considered in this paper are associative (but not necessarily commutative) with identity element $1 \neq 0$. Let R be a completely primary finite ring with unique maximal ideal $\mathcal{J}$. It is easy to see (cf. [3]) that $|R| = p^{nr}$, $|\mathcal{J}| = p^{(n-1)r}$, and the characteristic of R is p^k, for some prime p and positive integers n, k and r with $1 \leqslant k \leqslant n$. If $k = n$, then R is of the form $\mathbb{Z}_{p^n}[x]/(f)$ and $R = \mathbb{Z}_{p^n}[b]$, where $\mathbb{Z}_{p^n}$ is the ring of integers modulo p^n, $f(x)$ is a monic polynomial over $\mathbb{Z}_{p^n}$ and irreducible modulo p, and b is an element of R of multiplicative order $p^r - 1$. These rings are uniquely determined by the integers p, n, r; they are called Galois rings and we shall denote them by $GR(p^n, p^{nr})$.

Let R be a commutative completely primary finite ring. It is well known that any two coefficient subrings of R are conjugate (cf. [2]). Also if R_0 is a coefficient subring of R, then there exist $u_1, \dots, u_h$ in $\mathcal{J}$ such that

$$R = R_0 \oplus R_0u_1 \oplus \cdots \oplus R_0u_h \ \ \text{(as } R_0\text{-modules)}$$

and $u_ir = ru_i$, for all r in R_0 and for all $i = 1, \dots, h$. (This is a direct consequence of Theorems 2-2 and 2-4 in [4]).

Throughout this paper, for a given commutative completely primary finite ring R with maximal ideal $\mathcal{J}$, let $\mathbb{F} = R/\mathcal{J}$, and let $\mathbb{F}^*$ and G_R denote the multiplicative group of units of $\mathbb{F}$ and R, respectively.

2010 *Mathematics Subject Classification:* Primary 16P10, 16U60; Secondary 20K01, 20K25.
Key words and phrases: Completely primary finite rings, Galois rings.

Let $R_0 = GR(p^n, p^{nr})$, R be a commutative completely primary finite ring with $\mathcal{J}^2$ contained in R_0 and let $u_1, \ldots, u_h$ be elements in $\mathcal{J}$. Since $R_0 \cap R_0 u_i = 0$ and the product of any two zero divisors is in R_0, we have that $pu_i = 0$ for all $i = 1, \ldots, h$. But $u_i u_j$ is an element of pR_0; thus $u_i u_j$ is an element of $p^{n-1}R_0$, for all $i = 1, \ldots, h$. Suppose that $u_i u_j$, $u_i u_k$ are non-zero elements of pR_0 with $j \neq k$. Then $u_i u_j R_0 = u_i u_k R_0 = p^{n-1} R_0$ and we get $u_i u_j = u_i u_k \alpha$, where α is an element of $\langle b \rangle$. Thus, $u_j - u_k \alpha$ is an element of $\operatorname{ann}(u_i)$, the annihilator of u_i, and subsequently it is contained in $pR_0 \oplus R_0 u_1 \oplus \cdots \oplus R_0 u_h$ $(j \neq k)$. This implies that u_j is an element of $pR_0 \oplus R_0 u_1 \oplus \cdots \oplus R_0 u_h$, which is a contradiction. Therefore, for all $i = 1, \ldots, h$, either $u_i u_j$ is zero for all $j = 1, \ldots, h$ or $u_i u_j$ is non-zero for only one $j = 1, \ldots, h$. We assume w is the number of u_i such that $u_i u_j$ is zero for all $j = 1, \ldots, h$ and λ is the number of the other u_i. Let us reindex $u_1, \ldots, u_h$ in such way that for each $i = 1, \ldots, \lambda$, there exists only one $j = 1, \ldots, h$ with $u_i u_j = p^{n-1}\alpha_{ij}$, where α_{ij} is an element of $\langle b \rangle$, and let θ be the function from $\{1, \ldots, \lambda\}$ to $\{1, \ldots, h\}$ determined by $\theta(i) = j$. Clearly, θ is injective.

Let s be the number of i in $\{1, \ldots, \lambda\}$ such that $\theta(i) = i$ and t be $\lambda - s$. We reindex $u_1, \ldots, u_\lambda$ such that $\theta(i) = i$ for all $i = 1, \ldots, s$ and suppose $\alpha_{i\theta(i)} = \beta_i$ for all $i = 1, \ldots, s$. Put $v_e = u_e$ for all $i = 1, \ldots, s$ and $v_e = u_e \alpha_e$ for all $i = s+1, \ldots, h$, where if e is in the image of θ, say $e = \theta(i)$, then $\alpha_e = 1$. Thus, $u_i u_{\theta(i)} = p^{n-1}$ for all $i = s+1, \ldots, \lambda$. Hence, either $u_i^2 = 0$, $u_i^2 = p^{n-1}$ or $u_i^2 = \alpha p^{n-1}$, $\alpha \in \langle b \rangle - \{0, 1\}$; and $u_i u_j = 0$ for all $i \neq j$.

2. Construction A

Let R_0 be a Galois ring of the form $GR(p^n, p^{nr})$ and $\mathbb{F}$ be R_0/pR_0. Let U be an $\mathbb{F}$-space which when considered as an R_0-module has a generating set $\{u_1, \ldots, u_h\}$ such that $pu_i = 0$ for all $i = 1, \ldots, u_h$. Also assume that s, t, w are non-negative integers such that $h = s + t + w$ and suppose that θ is an injective function from $\{s+1, \ldots, s+t\}$ to $\{s+1, \ldots, h\}$. On the additive group

$$R = R_0 \oplus R_0 u_1 \oplus \cdots \oplus R_0 u_h,$$

define the multiplication as follows:

$$\begin{aligned} u_i u_j &= 0, \text{ for } i \neq j \ \ (1 \leqslant i, j \leqslant h); \\ u_i^2 &= \alpha_i p^{n-1}, \text{ for } i = 1, \ldots, s; \\ u_i^2 &= p^{n-1}, \text{ for } i = s+1, \ldots, s+t; \\ u_i^2 &= 0, \text{ for } i = s+t+1, \ldots, h; \\ u_i r^* &= r^* u_i, \text{ for all } i = 1, \ldots, h; \end{aligned}$$

where α_i are non-trivial elements of $\mathbb{F}^*$ and r^* is the image of r under the canonical homomorphism from R_0 to $\mathbb{F} \cong R_0/pR_0$.

It can easily be verified that R is an associative ring with identity $1 \neq 0$.

THEOREM 2.1. *Let R be a commutative completely primary finite ring. Then the product of any two zero divisors is an element of its coefficient subring R_0 if and only if R is one of the rings given by Construction A.*

The proof follows from the discussion before Construction A; the converse that $\mathcal{J}^2$ lies in R_0 is easy to check.

These rings were studied by Alkhamees [1], who gave their complete general construction for both commutative and non-commutative cases.

We notice that $\mathrm{char}R = p^n$; $\mathcal{J} = pR_0 \oplus R_0u_1 \oplus \cdots \oplus R_0u_h$, $\mathcal{J}^2 = pR_0$, and $\mathcal{J}^n = 0$. Also, notice that $|R| = p^{(n+h)r}$, $|\mathcal{J}| = p^{(n+h-1)r}$ and hence, $R/\mathcal{J} \cong \mathbb{F}_{p^r}$.

3. The group of units of R

There are many important results on the group of units of certain finite rings. For example, it is well known that the multiplicative group of the finite field $GF(p^r)$ is a cyclic group of order p^r-1, and the multiplicative group of the finite ring $\mathbb{Z}/p^k\mathbb{Z}$, the ring of integers modulo p^k, for p a prime number, and k a positive integer, is a cyclic group of order $p^{k-1}(p-1)$.

Let G_{R_0} denote the group of units of the Galois ring $R_0 = GR(p^n, p^{nr})$. Then G_{R_0} has the following structure [3]:

Theorem 3.1. *$G_{R_0} = \langle b\rangle \times (1 + pR_0)$, where $\langle b\rangle$ is the cyclic group of order p^r-1 and $1 + pR_0$ is of order $p^{(n-1)r}$ whose structure is described below.*

(i) *If (a) p is odd, or (b) $p = 2$ and $n \leqslant 2$, then $1+pR_0$ is the direct product of r cyclic groups each of order $p^{(n-1)}$.*

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

We now determine the structure of the group of units of this paper. We first recall that

$$G_R = \langle b\rangle \times (1 + \mathcal{J}), \quad |G_R| = |R| - |\mathcal{J}| = p^{(n+h)r} - p^{(n+h-1)r}$$

and in fact $|1 + \mathcal{J}| = p^{(n+h-1)r}$.

To simplify the problem, we split our study into two cases, namely,

(1) the case when $u_j^2 = 0$ for every $j = 1, \dots, h$; and
(2) the case when $u_j^2 = \alpha_j p^{n-1}$, where $\alpha_j \in \mathbb{F}^*$ for every $j = 1, \dots, h$.

We shall use the information from the two cases in order to obtain the general structure of G_R (see Theorem 4.1). We treat the cases separately.

Let $\varepsilon_1, \varepsilon_2, \dots \varepsilon_r$ be elements of R_0 with $\varepsilon_1 = 1$ so that $\overline{\varepsilon_1}, \overline{\varepsilon_2}, \dots, \overline{\varepsilon_r} \in R_0/pR_0 \cong GF(p^r)$ form a basis of $GF(p^r)$ over its prime subfield $GF(p)$.

3.1. The case when $u_i^2 = 0$ for every $i = 1, \dots, h$.

In this subsection, we determine the structure of the group of units G_R of the ring R in the case when $u_i^2 = 0$ for every $i = 1, \dots, h$.

Proposition 3.1. *Let R be a ring given by construction A and suppose that $u_j^2 = 0$ for every $j = 1, \dots, h$. Then*

$$G_R \cong \begin{cases} \mathbb{Z}_{2^r-1} \times \mathbb{Z}_2 \times \mathbb{Z}_{2^{n-2}} \times \mathbb{Z}_{2^{n-1}}^{r-1} \times \underbrace{\mathbb{Z}_2^r \times \cdots \times \mathbb{Z}_2^r}_{h} & \text{if } p = 2, \\ \mathbb{Z}_{p^r-1} \times \mathbb{Z}_{p^{n-1}}^r \times \underbrace{\mathbb{Z}_p^r \times \cdots \times \mathbb{Z}_p^r}_{h} & \text{if } p \text{ is odd.} \end{cases}$$

Proof. We know that

$$R = R_0 \oplus R_0u_1 \oplus \cdots \oplus R_0u_h, \quad \mathcal{J} = pR_0 \oplus \mathbb{F}u_1 \oplus \cdots \oplus \mathbb{F}u_h,$$

where $u_i \in \mathcal{J}$, $\mathbb{F} \cong R_0/pR_0$, $\mathcal{J}^{n-1} \neq (0)$, and $\mathcal{J}^n = (0)$. Moreover,

$$G_R \cong (\langle b \rangle) \times (1 + \mathcal{J}),$$

where $\langle b \rangle$ is a cyclic group of order $p^r - 1$, for every prime number p. We need to determine the structure and linearly independent generators of $1 + \mathcal{J}$ in order to complete the proof.

Since $pu_j = 0$ for all $j = 1, \dots, h$, $u_iu_j = 0$ for all $1 \leqslant i, j \leqslant h$, and $u_j^2 = 0$ for every $j = 1, \dots, h$, one easily sees that $(1 + R_0u_i) \cap (1 + R_0u_j) = \{1\}$. Moreover, $(1 + pR_0) \cap (1 + R_0u_j) = \{1\}$, for all $j = 1, \dots, h$. Further, it is easy to verify that $1 + R_0u_1 \oplus \cdots \oplus R_0u_h$ is a subgroup of $1 + \mathcal{J}$ and hence,

$$1 + \mathcal{J} = (1 + pR_0) \times (1 + R_0u_1 \oplus \cdots \oplus R_0u_h),$$

a direct product.

The structure of $1 + pR_0$ is well known, for example, see Theorem 3.1. We now determine the structure of $1 + R_0u_1 \oplus \cdots \oplus R_0u_h$. For any prime p and for each $i = 1, \dots, r$, we see that $(1 + \varepsilon_ju_1)^p = 1$, $(1 + \varepsilon_ju_2)^p = 1, \dots, (1 + \varepsilon_ju_h)^p = 1$, and $g^p = 1$ for all $g \in 1 + R_0u_1 \oplus \cdots \oplus R_0u_h$.

For integers $l_{ij} \leqslant p$, we asset that $\prod_{i=1}^r \prod_{j=1}^h \{(1 + \varepsilon_iu_j)^{l_{ij}} = 1$, will imply $l_{ij} = p$, for all $i = 1, \dots, r$ and $j = 1, \dots, h$.

If we set $E_{ij} = \{(1 + \varepsilon_iu_j)^{l_{ij}} : l_{ij} = 1, \dots, p\}$ for all $i = 1, \dots, r$, then we see that E_{ij} are all subgroups of $1 + R_0u_1 \oplus \cdots \oplus R_0u_h$ and that these are all of order p as indicated in their definition.

The argument above will show that the product of the hr subgroups E_{ij} is direct. Thus, their product will exhaust $1 + R_0u_1 \oplus \cdots \oplus R_0u_h$, and this completes the proof. □

3.2. The case when $u_j^2 = \alpha_jp^{n-1}$ for every $j = 1, \dots, h$; where $\alpha_j \in \mathbb{F}^*$. We now consider the second case.

Proposition 3.2. *Let R be a ring given by construction A and suppose that $u_j^2 = \alpha_jp^{n-1}$ for every $j = 1, \dots, h$, where $\alpha_j \in \mathbb{F}^*$. Then*

$$1 + \mathcal{J} \cong \begin{cases} \mathbb{Z}_2 \times \mathbb{Z}_{2^{n-3}} \times \mathbb{Z}_{2^{n-2}}^{r-1} \times \mathbb{Z}_4^r \times \underbrace{\mathbb{Z}_2^r \times \cdots \times \mathbb{Z}_2^r}_{h-1} & \text{if } p = 2, \\ \mathbb{Z}_{p^{n-1}}^r \times \underbrace{\mathbb{Z}_p^r \times \cdots \times \mathbb{Z}_p^r}_{h} & \text{if } p \text{ is odd.} \end{cases}$$

PROOF. The argument of the proof is similar to the proof of Proposition 3.2. Since $pu_j = 0$ for all $j = 1, \dots, h$, $u_i u_j = 0$ for all $1 \leqslant i, j \leqslant h$, and $u_j^2 = \alpha p^{n-1}$ for every $j = 1, \dots, h$, and a fixed α, one easily verifies that if $p = 2$, $(1 + \varepsilon_i u_j)^4 = 1$, for every $i = 1, \dots, r$ and $j = 1, \dots, h$; and if p is odd, $(1 + \varepsilon_i u_j)^p = 1$, for every $i = 1, \dots, r$ and $j = 1, \dots, h$. This difference, in turn, breaks into two cases to consider.

Suppose first that p is an odd prime number. For each $i = 1, \dots, r$ and $j = 1, \dots, h$, we see that for elements $1 + p\varepsilon_i$, $1 + \varepsilon_i u_j$ in $1 + \mathcal{J}$, $(1 + p\varepsilon_i)^{p^{n-1}} = 1$ and $(1 + \varepsilon_i u_j)^p = 1$.

For positive integers $m_i \leqslant p^{n-1}$ and $l_{ij} \leqslant p$, we assert that the equation

$$\prod_{i=1}^{r}\{(1 + p\varepsilon_i)^{m_i}\} \cdot \prod_{i=1}^{r}\prod_{j=1}^{h}\{(1 + \varepsilon_i u_j)^{l_{ij}}\} = 1,$$

will imply $m_i = p^{n-1}$, for all $i = 1, \dots, r$, and $l_{ij} = p$, for all $i = 1, \dots, r$ and $j = 1, \dots, h$.

If we set

$$E_i = \{(1 + p\varepsilon_i)^{m_i} : m_i = 1, 2, \dots, p^{n-1}\},$$
$$F_{ij} = \{(1 + \varepsilon_i u_j)^{l_{ij}} : l_{ij} = 1, \dots, p\},$$

we see that E_i, and F_{ij}, are all cyclic subgroups of $1 + \mathcal{J}$ and that these are all of the precise orders indicated by their definition.

The argument above shows that the product of the $(1 + h)r$ subgroups E_i, F_{ij} is direct. So, their product will exhaust $1 + \mathcal{J}$; and we see that the proof for the case when p is odd is complete.

We now assume that $p = 2$. We remark that there exists at least one element β in R_0 such that the equation $x^2 + x + \bar{\beta} = \bar{0}$ over R_0/pR_0 has no solution in R_0/pR_0. We then note that for elements $(-1 + 2^{n-1}\varepsilon_1)$, $(1 + 4\beta)^2 = (1 + 8\beta + 16\beta^2)$, $(1 + \varepsilon_i u_j)$ and $(1 + \varepsilon_i u_j + \varepsilon_i u_{j+1})$ in $1 + \mathcal{J}$, $(-1 + 2^{n-1}\varepsilon_1)^2 = 1$, $(1 + 8\beta + 16\beta^2)^{2^{n-3}} = 1$, $(1 + \varepsilon_i u_j)^4 = 1$ for all $i = 1, \dots, r$; and $j = 1, \dots, h$; and for a $u_j^2 = \alpha 2^{n-1}$ with α fixed for every $j = 1, \dots, h$; $(1 + \varepsilon_i u_j + \varepsilon_i u_{j+1})^2 = 1$, for all $i = 1, \dots, r$ and $j = 1, \dots, h - 1$.

For positive integers $k \leqslant 2$, $l \leqslant 2^{n-3}$, $m_i \leqslant 4$ and $n_{ij} \leqslant 2$, we assert that the equation

$$(-1 + 2^{n-1}\varepsilon_1)^k \cdot (1 + 8\beta + 16\beta^2)^l \cdot \prod_{i=1}^{r}\{(1 + \varepsilon_i u_1)^{m_i}\} \cdot \prod_{i=1}^{r}\prod_{j=1}^{h-1}\{(1 + \varepsilon_i u_j + \varepsilon_i u_{j+1})^{n_{ij}}\} = 1,$$

will imply $k = 2$, $l = 2^{n-3}$, $m_i = 4$ for all $i = 1, \dots, r$; and $n_{ij} = 2$ for all $i = 1, \dots, r$ and $j = 1, \dots, h - 1$.

If we set

$$E_1 = \{(-1 + 2^{n-1}\varepsilon_1)^k : k = 1, 2\},$$
$$E_2 = \{(1 + 8\beta + 16\beta^2)^l : l = 1, \dots, 2^{n-3}\},$$

$$E_{i1} = \{(1+\varepsilon_i u_1)^{m_i} : m_i = 1, \dots, 4\},$$
$$F_{ij} = \{: (1+\varepsilon_i u_j + \varepsilon_i u_{j+1})^{n_{ij}} : n_{ij} = 1, 2\},$$

then we see that E_1, E_2, E_{i1}, F_{ij} are all cyclic subgroups of $1+\mathcal{J}$ and that these are all of the precise orders indicated by their definition.

The argument above shows that the product of the $2+hr$ subgroups E_1, E_2, E_{i1}, F_{ij} is direct. So, their product will exhaust $1+\mathcal{J}$, and we see that the proof for the case when $p=2$ is complete.

This completes the proof of the theorem. $\square$

4. Conclusion

We now state the structure of the group of units G_R of the ring R in general.

THEOREM 4.1. *Let R be a ring given by construction A and suppose that $u_j^2 = \alpha_j p^{n-1}$, for every $j = 1, \dots, s$, where $\alpha_j \in \mathbb{F}^*$ and for $j = s+1, \dots, h$, $u_j^2 = 0$. Then*

$$1+\mathcal{J} \cong \begin{cases} \mathbb{Z}_2 \times \mathbb{Z}_{2^{n-3}} \times \mathbb{Z}_{2^{n-2}}^{r-1} \times \mathbb{Z}_4^r \times \underbrace{\mathbb{Z}_2^r \times \cdots \times \mathbb{Z}_2^r}_{s-1} \times \underbrace{\mathbb{Z}_2^r \times \cdots \times \mathbb{Z}_2^r}_{h-s} & \text{if } p = 2, \\ \mathbb{Z}_{p^{n-1}}^r \times \underbrace{\mathbb{Z}_p^r \times \cdots \times \mathbb{Z}_p^r}_{h} & \text{if } p > 2, \end{cases}$$

and hence,

$$G_R \cong \begin{cases} \mathbb{Z}_{2^r-1} \times (1+\mathcal{J}) & \text{if } p = 2, \\ \mathbb{Z}_{p^r-1} \times (1+\mathcal{J}) & \text{if } p \text{ is odd.} \end{cases}$$

PROOF. Follows from Propositions 3.2 and 3.3. $\square$

References

1. Y. Alkhamees, *Finite completely primary rings in which the product of any two zero divisors of a ring is in its coefficient subring*, Internat. J. Math. Math. Sci. **17**:3 (1994), 463–468.
2. W. E. Clark, *A coefficient ring for finite non-commutative rings*, Proc. Amer. Math. Soc. **33** (1972), 25–28.
3. R. Raghavendran, *Finite associative rings*, Compositio Math. **21** (1969), 195–229.
4. B. R. Wirt, *Finite non-commutative rings*, PhD Thesis, University of Oklahoma, 1972.

Department of Basic Sciences
Botswana College of Agriculture
Gaborone
Botswana
jchikunj@bca.bw

(Received 27 08 2012)