Internat. J. Math. & Math. Sci.
VOL. 17 NO. 3 (1994) 463-468

FINITE COMPLETELY PRIMARY RINGS IN WHICH THE PRODUCT OF ANY TWO ZERO DIVISORS OF A RING IS IN ITS COEFFICIENT SUBRING

YOUSIF ALKHAMEES

Department of Mathematics
King Saud University
P.O. Box 2455
Riyadh 11451, Saudi Arabia

(Received June 6, 1990 and in revised form August 30, 1993)

ABSTRACT. According to general terminology, a ring R is completely primary if its set of zero divisors J forms an ideal. Let R be a finite completely primary ring. It is easy to establish that J is the unique maximal ideal of R and R has a coefficient subring S (i.e. R/J isomorphic to S/pS) which is a Galois ring. In this paper we give the construction of finite completely primary rings in which the product of any two zero divisors is in S and determine their enumeration. We also show that finite rings in which the product of any two zero divisors is a power of a fixed prime p are completely primary rings with either $J^2=0$ or their coefficient subring is Z_{2^n} with n=2 or 3. A special case of these rings is the class of finite rings, studied in [2], in which the product of any two zero divisors is zero.

KEY WORDS AND PHRASES. Finite completely primary ring, Galois ring.
1992 AMS SUBJECT CLASSIFICATION CODES 16 A 10,16 A 44,16 A 48.

1. INTRODUCTION.

All rings considered in this paper are associative with identity. Let R be a finite completely primary ring. It is easy to see (cf. [5]) that $|R|=p^{mr}$, $|J|=p^{(m-1)r}$, and the characteristic of R is p^n, for some prime p and positive integers m,n and r with $1\leq n\leq m$. If n=m, then R is of the form $Z_{p^n}[x]/(g)$ and $R=Z_{p^n}[a]$, where Z_{p^n} is the ring of integers modulo p^n, g is monic polynomial over Z_{p^n} and irreducible modulo p and a is an element of R of multiplicative order p^r-1. In this case Aut R, the automorphism group of R, is cyclic and is of order r. These rings are uniquely determined by the triplet p, n, r ; they are called Galois rings and are denoted by $GR(p^n,r)$.

Let R be a finite completely primary ring. It is already known that any two coefficient subrings of R are conjugate (cf. [4]). Also if S is a coefficient subring of R; then there exist $\pi_1, \ldots, \pi_m$ in J and $\sigma_1, \ldots, \sigma_m$ in Aut S such that

$$R = S \oplus \sum_{i=1}^{m}{}^{\oplus} S\pi_i \quad (\text{as } S\text{ - modules}) \quad \text{and} \quad \pi_i r = r^{\sigma_i} \pi_i$$

for all r in S and for all i=1, ..., m. (This result is a direct consequence of theorems 2-2 and 2-4 in [6]). Moreover the automorphisms $\sigma_1, \ldots, \sigma_m$ are uniquely determined by R and S (cf. [2]). Thus we call $\sigma_1, \ldots, \sigma_m$ the associated automorphisms of R and the automorphism σ_i is called the automorphism associated with π_i. Throughout this paper, for a given finite completely primary ring R, we denote by T_R the set of all $(S, \pi_1, \ldots, \pi_m)$ which come from the above description. In addition, let F=R/J, and let F^* and G_R denote the multiplicative group of units of F and R respectively.

2. THE CONSTRTUCTION.

CONSTRUCTION A: Let S be a Galois ring of the form $GR(p^n,r)$ and F be S/pS. Also assume that s, t, w, m are non-negative integers such that m=s+t+w and suppose that f is an injective function from {s+1, ..., s+t} to {s+1, ..., m}. On the additive group $R=S\oplus F^m$, define the multiplication as follows:

$$(r_o,r_1,\ldots,r_m)(s_o,s_1,\ldots,s_m)=(r_o s_o+p^{n-1}\sum_{i=1}^{s}u_i r_i s_i^{\sigma_i}+p^{n-1}\sum_{i=s+1}^{s+t}r_i s_i^{\sigma_i},\ r_o^* s_1+r_1 s_o^{*\sigma_1},\ \ldots,\ r_o^* s_m+r_m s_o^{*\sigma_m})$$

where u_i are elements of F, σ_i automorphisms of F such that $\sigma_i^2=id_F$ for all i=1, ..., s and $\sigma_{f(i)}=\sigma_i^{-1}$ for all i=s+1,..., s+t and r^* is the image of r under the canonical homomorphism from S to F.

It can be easily verified that R is a ring and it is commutative if and only if $\sigma_i=id_F$ for all i=1, ..., m.

THEOREM 1: Let R be a finite completely primary ring. Then the product of any two zero divisors is an element of its coefficient subring S if and if it is one of the rings given by construction A.

PROOF: Let R be a finite completely primary ring with J^2 contained in S and $(S, \pi_1', \ldots, \pi_m')$ be an element of T_R. Since $S\cap S\pi_i'=0$ and the product of any two zero divisors is in S, $p\pi_i'=0$ for all i=1, ..., m. But $\pi_i'\pi_j'$ is an element of pS; thus $\pi_i'\pi_j'$ is an element of $p^{n-1}S$ for all i,j=1, ..., m. Suppose $\pi_i'\pi_j',\pi_i'\pi_k'$ are non-zero elements of pS with j≠k. Then $\pi_i'\pi_j'S=\pi_i'\pi_k'S=p^{n-1}S$ and we get $\pi_i'\pi_j'=\pi_i'\pi_k'\alpha$, where α is an element of <a>. Thus $\pi_j'-\pi_k'\alpha$ is an element of ann π_i' and subsequently it is contained in

$$pS\oplus\sum_{h=1,\,h\neq j,k}^{m}{}^{\oplus}\ S\pi_h'.$$

This implies that π_j' is an element of

$$pS\oplus\sum_{h=1,\,h\neq j}^{m}{}^{\oplus}\ S\pi_h',$$

which contradicts the assumption that $(S, \pi_1', \ldots, \pi_m')$ is an element of T_R. Therefore for all i=1, ..., m, either $\pi_i'\pi_j'$ is zero for all j=1, ..., m or $\pi_i'\pi_j'$ is non-zero for only one j=1, ..., m. Similarly, we prove that for all i=1, ..., m, either $\pi_j'\pi_i'$ is zero for all j=1, ..., m or $\pi_j'\pi_i'$ is non-zero for exactly one j. Assume w is the number of π_i' such that $\pi_i'\pi_j'$ is zero for all j=1, ..., m and λ is the number of other π_i'. Let us reindex $\pi_1', \ldots,\pi_m'$ in such a way that for each i=1,...,λ there exists only one j=1, ..., m with $\pi_i'\pi_j'=p^{n-1}\alpha_{ij}$,where α_{ij} is an element of <a>, and let f be the function from {1, ..., λ} to {1, ..., m} determined by f(i)=j. Clearly f is injective. Also, for all i=1, ..., m

$$p^{n-1}a\alpha_{if(i)}=\pi_i'\pi_{f(i)}'a=a^{\sigma_i\sigma_{f(i)}}\pi_i'\pi_{f(i)}'=p^{n-1}a^{\sigma_i\sigma_{f(i)}}\alpha_{if(i)},$$

which implies that $\sigma_{f(i)}=\sigma_i^{-1}$ for all i=1, ..., λ. Let s be the number of i in {1, ..., λ} such that f(i)=i and t be λ-s. We reindex $\pi_1', \ldots, \pi_\lambda'$ such that f(i)=i for all i=1, ..., s and suppose $\alpha_{if(i)}=u_i$ for all i=1, ..., s. Put $\pi_e=\pi_e'$ for all i=1, ...,s and $\pi_e=\pi_e'\alpha_e$ for all i=s+1, ..., m, where if e is in the image of f, say $e=f^j(i)$, then

$$\alpha_e=\prod_{h=1}^{j}(\alpha_{f^{h-1}(i)f^h(i)})^{g(h)},\ \text{where}\ g(h)=(-1)^{j+h+1}\prod_{d=h}^{j-1}\sigma_{f^d(i)},\ \text{and}\ \alpha_e=1\ \text{otherwise}.$$

It is easy to see that $(S, \pi_1, \ldots, \pi_m)$ is an element of T_R with $\pi_i\pi_{f(i)}=p^{n-1}$ for all i=s+1, ...,λ. Now it follows that R is isomorphic to one of the rings given by construction A.

The converse is easy to check.

3. FINITE RINGS IN WHICH THE PRODUCT OF ANY TWO ZERO DIVISORS IS A POWER OF A FIXED PRIME.

LEMMA 1: Let R be a finite ring of characteristic p^n in which the product of any two zero divisors is a power of p. Then R is completely primary.

PROOF: Let x and y be zero divisors in R. To show that x+y is a zero divisor, we can use the distributive properties to write $(x+y)^{2n}$ as a sum of products, each containing 2n factors (which are x's or y's). Since each xy or yx is of the form p^{λ_i}, each of the summands of $(x+y)^{2n}$ is product of the form $p^{\lambda_1}p^{\lambda_2}\dots p^{\lambda_n}=0$. Therefore x+y is zero divisor and hence R is completely primary.

PROPOSITION 1: Let R be a finite ring of characteristic p^n in which the product of any two zero divisors is a power of p. Then R is completely primary with either $J^2=0$ or the coefficient subring of R is Z_{2^n}, where n=2,3.

PROOF: Suppose $J^2\neq 0$; then there exist x,y in J with $xy=p^\lambda\neq 0$. Since for any unit α in R, αx is a zero divisor, we have $(\alpha x)y=p^\mu$. On the other hand, $xy=p^\lambda$ implies that $\alpha xy=\alpha p^\lambda$ and so $\alpha p^\lambda=p^\mu$. Without loss of generality, we can assume $\mu\geq\lambda$ and deduce that $p^\lambda(\alpha-p^{\mu-\lambda})=0$. Since $p^\lambda\neq 0$, we have $\alpha-p^{\mu-\lambda}$ is an element of J. If $\mu\neq\lambda$, this would imply that α is an element of J which is not possible; hence $\mu=\lambda$ and α is an element of 1+J. However α is an arbitrary unit and therefore $G_R=1+J$. Since $R=G_R\cup J$ (disjoint union), we have

$$|R| = |G_R|+|J| = |1+J|+|J| = 2|J|$$

Thus 2 divides |R| and consequently char R is 2^n. If $n\geq 4$, then 2,6 are zero divisors of R with (2)(6)=12 which is not a power of 2. Also n=1 implies that $J^2=0$. Thus n=2,3. Let $S=Z_{2^n}[a]$ be a coefficient subring of R, where a is an element of R of multiplicative order 2^r-1 and let x,y be elements of J with $xy=2^\lambda\neq 0$. But $(ax)y=2^\mu$ implies $a2^\lambda=2^\mu$ and hence a=1. Thus the coefficient subring of R is Z_{2^n} with n=2,3.

4. THE ENUMERATION.

NOTATIONS: Retaining the above notations, assume k is the number of elements in {s+t+1, ..., m} which are not in the image of f. Let all the π_i in which i is not in the image of f be renamed as $\theta_1, \dots, \theta_k$ and assume $\tau_1, \dots, \tau_k$ are the respective automorphisms associated with them. Thus we suppose that $(S, \pi_1, \dots, \pi_{m-k}, \theta_1, \dots, \theta_k)$ is an element of T_R and $\sigma_1, \dots, \sigma_{m-k}, \tau_1, \dots, \tau_k$ are the automophisms associated with $\pi_1, \dots, \pi_{m-k}, \theta_1, \dots, \theta_k$ respectively. We call (p, n, r, s, t, k, m, f) the invariants of R. In what follows we shall use these notations.

PROPOSITION 2: Let R be a finite completely primary ring in which the product of any two zero divisors is an element of its coefficient subring. Then $(S, \pi_1', \dots, \pi_{m-k}', \theta_1', \dots, \theta_k')$ is an element of T_R if and only if

$$\pi_i' = \lambda_i\pi_i + \sum_{\tau_j=\sigma_i}\xi_{ij}\theta_j + p^{n-1}\xi_i \quad \text{(after possible reindexing)},$$

$$\theta_i' = \sum_{\tau_j=\tau_i}\mu_j\theta_j + p^{n-1}\omega_i \quad \text{(after possible reindexing)}.$$

where λ_i are elements of F^* and $\xi_{ij}, \xi_i, \mu_j, \omega_i$ are elements of F such that ξ_i is zero if σ_i is not the trivial automorphism and ω_i is zero if τ_i is not the trivial automorphism.

PROOF: Using the fact that $\pi_i'a=a^{\sigma_i}\pi_i'$, we deduce that for all i=1, ..., m-k, we have

$$\pi_i' = \sum_{\sigma_j=\sigma_i}\lambda_{ij}\pi_i + \sum_{\tau_j=\sigma_i}\xi_{ij}\theta_j + p^{n-1}\xi_i .$$

where λ_{ij}, ξ_{ij} and ξ_i are elements of F such that ξ_i is zero if σ_i is not the trivial automorphism. For all i=1,...,s+t, $|\mathrm{ann}\ \pi_{f(i)}|=|J|/p^r$ and so $\pi_j'\pi_{f(i)}=0$ for all but one j, say j=h. Thus $\pi_h'\pi_{f(i)}$ is a non-zero element of $p^{n-1}S$, $\pi_h'\pi_j=0$ for all j≠f(i) and $\sigma_h=(\sigma_{f(i)})^{-1}=\sigma_i$. Thus $\lambda_{hj}=0$ for all j except j=h. Let us put $\lambda_{hh}=\lambda_i$ and redenote π_h' by π_i'. Therefore

$$\pi_i' = \lambda_i\pi_i + \sum_{\tau_j=\sigma_i}\xi_{ij}\theta_j + p^{n-1}\xi_i .$$

We can prove the rest of the proposition by using a similar argument.

THEOREM 2: Let R,R' be finite completely primary rings constructed over the same coefficient subring S and having the same associated automorphisms. Suppose that $(J(R))^2$ and $(J(R'))^2$ are contained in S and R,R' have the same invariants p, n, r, s, t, k, m, f. Also suppose that $(S, \pi_1', ..., \pi_{m-k}', \theta_1', ..., \theta_k')$ is an element of $T_{R'}$ with $\pi_i'^2=p^{n-1}v_i$ for all i=1, ..., s. Then R is isomorphic to R' if and only if there exist isomorphisms ϕ_i from $S\oplus S\pi_i$ to $S\oplus S\pi_i'$ (after possible reindexing) for all i=1, ..., m-k such that $\phi_i(\pi_i)=\lambda_i\pi_i'$, where λ_i are elements of F^* such that

$$\lambda_i\lambda_i^{\sigma_i} = u_i^{p^j}v_i^{-1} \text{ and } \lambda_h\lambda_{f(h)}^{\sigma_h} = 1$$

for all i=1, ..., s and h=s+1, ..., s+t, o≤j<r.

PROOF: Let ψ be an isomorphism from R to R'. Then $\psi(S)$ is a coefficient subring of R' and hence there exists a unit x in R' such that $\psi(S)=xSx^{-1}$. Let ϕ be the composition of the conjugation by x and ψ. Clearly ϕ is an isomorphism from R to R' which sends S to itself and thus $(S, \phi(\pi_1), ..., \phi(\pi_{m-k}), \phi(\theta_1), ..., \phi(\theta_k))$ is an element of $T_{R'}$. Therefore for all i=1, ..., m-k

$$\phi(\pi_i) = \lambda_i\pi_i' + \sum_{\tau_j=\sigma_i}\xi_{ij}\theta_j' + p^{n-1}\xi_i$$

where λ_i are elements of F^* and ξ_{ij},ξ_i are elements of F such that ξ_i is zero if σ_i is not the trivial automorphism. For all i=1, ..., s

$$p^{n-1}u_i^{p^j} = p^{n-1}\phi(u_i) = \phi(\pi_i^2) = (\phi(\pi_i))^2 = (\lambda_i\pi_i')^2 = p^{n-1}\lambda_i^{\sigma_i}\lambda_i .$$

Thus

$$\lambda_i\lambda_i^{\sigma_i} = u_i^{p^j}v_i^{-1} \text{ for some } 0\le j<r.$$

Also for all i=s+1, ..., s+t

$$p^{n-1} = \phi(\pi_i^2) = (\phi(\pi_i))^2 = (\lambda_i\pi_i')^2 = \lambda_i\lambda_i^{\sigma_i}\pi_i'^2 = p^{n-1}\lambda_i\lambda_i^{\sigma_i}.$$

It is easy to see that, for all i=1, ..., s+t, the mappings ϕ_i from $S\oplus S\pi_i$ to $S\oplus S\pi_i'$ determined by $\phi_i(\pi_i)=\lambda_i\pi_i'$ are isomorphisms.

Conversely,let ϕ_i be the isomorphisms from $S\oplus S\pi_i$ to $S\oplus S\pi_i'$ defined in the statement of the theorem, where i=1, ..., m-k. It is easy to check that the mapping ϕ determined by

$$\phi(r_o+\sum r_i\pi_i + \sum r_i\theta_i) = r_o + \sum r_i\ \phi_i(\pi_i) + \sum r_i\theta_i'$$

is an isomorphism from R to R'.

NOTATIONS: Let R be a finite completely primary ring in which the product of any two zero divisors is in its coefficient subring and let p, n, r, s, t, k, m, f be invariants of R. Assume ρ is the permutation on the maximal subset of {s+1, ..., s+t} which is stable under f and c is the number of cycles of ρ. Finally, let

$$a^{\sigma_i} = a^{p^{r_i}} \text{ for all } i = 1, \ldots, s,$$

and N_i be the number of mutually non-isomorphic rings of the form $S\oplus S\pi_i$ with the same associated automorphisms σ_i, where $\pi_i^2=p^{n-1}u_i$. Then from theorem 2 in [3], we have

$$N_i = \begin{cases} 1 & \text{if p is even and } \sigma_i \text{ is the trivial automorphism,} \\ 2 & \text{if p is odd and } \sigma_i \text{ is the trivial automorphism,} \\ p^{r/2}+1 & \text{if } \sigma_i \text{ is not the trivial automorphism.} \end{cases}$$

THEOREM 3: The number of mutually non-isomorphic finite completely primary rings in which the product of any two zero divisors is in its coefficient subring, having the same invariants p, n, r, s, t, k, m, f and with the same associated automorphisms is

$$(p^r-2)^{t-c}\prod_{i=1}^{s} N_i .$$

PROOF: If u_i,v_i are elements of F^*, define $u_i\_v_i$ if and only if

$$u_i^{p^j}v_i^{-1} = \lambda_i^{p^{r_i}+1}$$

for all i=1, ..., s, where $0\le j<r$. By using similar method as in the proof of theorem 2 in [3], one can deduce that the number of equivalence classes of this equivalent relation is N_i. Define $\pi_i\_\pi_i'$ if and only if $\pi_i=\lambda_i\pi_i'$ for all i=s+1, ..., s+t, where λ_i is an element of F^* such that $\lambda_i\lambda_{f(i)}=1$. Let n_i be the number of the equivalence classes of this equivalent relation. Then $n_i=1$ if i is not in the image of f and $n_i=p^r-2$ if i is in the image of f. But when f restricted to {s+1, ..., s+t} the number of elements in the image of f is t-c. Thus

$$\prod_{i=s+1}^{s+t} n_i = (p^r - 2)^{t-c}.$$

In view of the last theorem the required number is

$$\left(\prod_{i=1}^{s} N_i\right)\left(\prod_{i=s+1}^{s+t} n_i\right) = (p^r - 2)^{t-c} \prod_{i=1}^{s} N_i .$$

COROLLARY: The finite ring of characteristic p^n in which the product of any two zero divisors is a power of p is completely determined by its associated automorphisms and its invariants.

REMARK: Let R be a finite ring which has a p-ring as its coefficient subring and the product of any two zero divisors of R is in its coefficient subring. By using similar argument as in the proof of lemma 1, one can prove that R is completely primary. Thus the construction and the enumeration of such rings is determined.

ACKNOWLEDEMENT: The author would like to thank B. Corbas for his suggestions which enabled the author to make some improvements in the contents of the paper.

REFERENCES

1. Y. AlKhamees, On the structure of finite completely primary rings, J. Coll. Sci., King Saud Uni. 13(1)(1982), 149-153.
2. __________, Finite rings in which the multiplication of any two zero divisors is zero, Arch. Math. Vol. 37(1981), 144-149.
3. __________, Near Galois rings, Proceedings of the conference on Algebra and Geometry, Kuwait (1981), 1-6.
4. W. E. Clark, A coefficient ring for finite non-commutative rings, Proc. Amer. Math. Soc. 33(1)(1972), 25-27.
5. R. Raghavendran, Finite associative rings, Compositio Math. 21(2)(1969), 195-229.
6. B. R. Wirt, Finite non-commutative local rings, Ph.D. Thesis, Uni. of Oklahoma, (1972).