COMPOSITIO MATHEMATICA

R. RAGHAVENDRAN

A class of finite rings

Compositio Mathematica, tome 22, nº 1 (1970), p. 49-57

<http://www.numdam.org/item?id=CM_1970__22_1_49_0>

COMPOSITIO MATHEMATICA, Vol. 22, Fasc. 1, 1970, pag. 49-57
Wolters-Noordhoff Publishing
Printed in the Netherlands

A class of finite rings

by

R. Raghavendran

Introduction

In a paper published not long ago Gilmer [2] determined completely the structure of every finite commutative ring with an identity element whose multiplicative group of units is cyclic; and showed that there exists at least one noncommutative ring with this property by giving the example of the ring R_0 (say) of all 2×2 upper triangular matrices over the field $GF(2)$. By way of generalisation, Eldridge and Fischer [1] proved certain results of which only the following are of immediate concern to us here. If R is any ring with a cyclic group of units whose left ideals satisfy the descending chain condition, they showed that R will be necessarily finite; if, in addition, R is not commutative, they showed that R will be the direct sum of a commutative ring with the ring R_0 described above.

For convenience, we shall use throughout this paper the term Gilmer ring to denote any finite (associative, but not necessarily commutative) ring with an identity element, whose multiplicative group of units is cyclic.

The method of procedure of Eldridge and Fischer may now be described as follows. They prove a series of lemmas which lead to the conclusion that a Gilmer ring will be commutative except in a certain situation; and then they determine the structure of the ring in this particular case. At one stage of this process they make use of the classification given in Gilmer [2].

In this paper we redetermine the structures of all Gilmer rings *ab initio*, and in a manner almost independent of that of Gilmer. Our discussion is based on a lemma (Lemma 1) and some simple remarks (given in § (1.2)). The discussion depends on [2] only to the extent of using an argument of Gilmer which, however, forms an essential part of the proof of Lemma 1 of this paper.

The author wishes to thank Professor V. Ganapathy Iyer for his encouragement and guidance during the preparation of this paper.

Thanks are due to N. Ganesan for having shown the author a preprint of the paper [1] sent to him by Eldridge prior to its publication.

Section 1

(1.1) We begin by describing the notations used throughout this paper. The symbol R will be used to denote any finite (associative) ring with an identity element $1 \neq 0$. The symbol J will be used to denote the Jacobson radical of the ring under consideration. We use the notation G_R for the multiplicative group of units of the ring R. The symbol S will be used to denote the subring of R generated by its identity element. The symbol X is used to denote an indeterminate. As is usual, Z denotes the ring of all integers and p denotes any positive prime integer. For any set A with a finite number of elements, we use $|A|$ to denote the number of elements in that set.

We now describe a notation which plays an important role in this paper. For any particular prime p, we use the symbol $N(p)$ to denote the set of all the nilpotent elements x (of the ring under consideration) which satisfy the condition $px = 0$.

(1.2) In this subsection we mention some simple results which will be useful to us later.

(i) If R is a ring of order $p_1^{n_1} \cdot \cdots \cdot p_k^{n_k}$ where the p_i are distinct primes and the n_i are positive integers, it is well known that R is expressible, in a unique manner, as the direct sum of rings R_i, where $|R_i| = p_i^{n_i}$, $i = 1, \cdots, k$.

(ii) (Gilmer [2, Th. 1].) Let the ring R be the direct sum of nontrivial rings $R_1, \cdots, R_k$. Then it is obvious that each ring R_i has an identity element, and that the group G_R is the direct product of the groups G_{R_i}, $i = 1, \cdots, k$. *So the group G_R will be cyclic if, and only if, both the following conditions are satisfied*: (1) *each G_{R_i} is a cyclic group, and* (2) *the integers $|G_{R_i}|$ are prime to each other in pairs.*

(iii) In view of the above remark we see that, in considering Gilmer rings, we may restrict our attention to indecomposable ones – whose orders are necessarily prime-powers.

(iv) If a ring R is the direct sum of two nontrivial rings, it can be easily verified that the additive group generated by the zero divisors of R will be the whole of R.

(v) *Let K be a nil ideal in the ring R. If the quotient ring R/K is a field, then K will consist of all the nonunits of R; also R will be an* *indecomposable ring*. For, it can be easily verified that an element x will be a unit in R if, and only if, the element $x+K$ is a unit in the quotient ring R/K. So if R/K is a field, then all the nonunits of R will belong to K (and exhaust K), and the remark (iv) above shows that R will be indecomposable (because K is a proper subset of R).

(vi) *If R is a Gilmer ring with radical J, then the quotient ring R/J will also be a Gilmer ring.* For, as J is a nil ideal, the argument in (v) above shows that the canonical mapping will map the group G_R onto the group of units of the ring R/J.

(vii) Let A be the ring of all $n \times n$ matrices over a division ring. If $n \geqq 2$ we know that the group G_A will be nonabelian. So A will be a Gilmer ring if, and only if A is a (finite) field.

(viii) *If R is a Gilmer ring with radical J, then the quotient ring R/J will be a direct sum of fields.* For, by Wedderburn-Artin structure theorem, R/J will be the direct sum of a finite number of ideals $A_1, \cdots, A_k$ where each A_i, regarded by itself, is a total matrix ring over some division ring. The desired result now follows by using, in succession, the remarks (vi), (ii) and (vii) above.

(Note: A celebrated theorem of Wedderburn asserts that every finite division ring is necessarily commutative. However, we do not need this result here.)

(ix) (Koh [4]) *If a ring A has exactly n left zero divisors and $n > 1$, then $|A| \leqq n^2$.* For, let z be a nonzero left zero divisor and let K be the kernel of the homomorphism $a \to az$ $(a \in A)$ of the additive group of A onto that of Az. As every element of both the sets K and Az is a left zero divisor in A, we have $|K| \leqq n$ and $|Az| \leqq n$. Then the fact $|A| = |K| \cdot |Az|$ gives the desired result.

(1.3) The object of this paper is to prove the following comprehensive result.

THEOREM 1. (Gilmer [2], Eldridge and Fischer [1].)

Each one of the following rings is an indecomposable Gilmer ring.

(a) *$GF(p^m)$, where p is any prime and $m \geqq 1$.*

(b) *$Z/(p^m)$, where p is an odd prime and $m \geqq 2$.*

(c) *$F[X]/(X^2)$, where F is any prime field of finite order.*

(d) $Z/(4)$.

(e) *$F[X]/(X^3)$, where $F = GF(2)$.*

(f) $Z[X]/(4, 2X, X^2-2)$.

(g) *The ring of all 2×2 upper triangular matrices over the field $GF(2)$.*

Conversely, every indecomposable Gilmer ring is isomorphic to one, and only one, of the rings described above. Also, if a Gilmer ring is the direct sum of k ($\geqq 2$) indecomposable rings, then at least $k-1$ of these component rings are fields with characteristic 2.

Proof. First we prove the direct part of the theorem. If the ring R is of type (a) or type (b) or type (d) it is well known that the group G_R is cyclic. Suppose now that R is of type (c) and that u is the coset $X+(X^2)$ in $F[X]$. It is easily seen that the nonunits of R constitute the ideal Ru of order p, so that $J = Ru$ and $R/J \cong GF(p)$. The group G_R of order $p(p-1)$ is the direct product of the group $1+J$ (of order p, a prime) and the group G_F (of order $p-1$). As the groups $1+J$ and G_F are cyclic, it follows that the group G_R is cyclic. Next we will dispose of the types (e) and (f) together. Suppose that R is of type (e) or of type (f) and that u denotes the coset $X+A$ in the appropriate polynomial ring, where $A = (X)$ if R is of type (e) and $A = (4, 2X, X^2-2)$ if R is of type (f). If $K = \{0, u, u^2, u^2+u\}$, we have $R = K \cup \{1+K\}$ and as $2u = u^3 = 0$, we can easily verify that K is a nil ideal in R; and also that $G_R = 1+K$ is cyclic, with $1+u$ as a generator. If R is of any one of the types (a) to (f) we note that R/J is a field; so all these rings are indecomposable (by § (1.2) (v)).

Suppose finally that R is of type (g). Here the group G_R (of order 2) is cyclic. Let, if possible, R be expressed as the direct sum of two nontrivial rings R_1, R_2. As $|R| = 8$, we may suppose that $|R_1| = 4$ and $|R_2| = 2$; as R_1, R_2 would have identity elements, both of them must be commutative. As this contradicts the fact that R is noncommutative, we see that the ring (g) is indecomposable.

This completes the proof of the direct part of the theorem. The first statement in the converse part will be proved later. Assuming this result for the moment, we see that the second statement follows from the remark (ii) of § (1.2) and the observation that $|G_R|$ is odd for an indecomposable Gilmer ring R only if R is a finite field with characteristic 2.

(1.4) With the ultimate objective of proving the first statement in the converse part of Theorem 1 we prove five lemmas, the first of which is to be found below. The decisive trick used in its proof is due to Gilmer (refer [2, Th. 3]).

Lemma 1. *Let R be any Gilmer ring and let, for a prime p, the set $N(p)$ (defined in § (1.1)) contain a nonzero element u. Then the following results hold.*

(i) *If* $x^2 = 0$ *for all elements* x *in* $N(p)$, *then*
$N(p) = \{mu : m = 0, 1, \cdots, p-1\}$.
So $|N(p)| = p$ *in this case.*

(ii) *If* $u^2 \neq 0$, *then* $p = 2$ *and*
$N(2) = \{0, u, u^2, u^2+u : u^3 = 0 = 2u\}$.
So $|N(2)| = 4$ *in this case.*

Proof. We shall first prove (ii). Let x be any fixed element of $N(p)$ with $x^2 \neq 0$, and let k $(\geqq 3)$ be the least positive integer such that $x^k = 0$. It can be easily verified that the set

$$A = \{1+(a+bx)x^{k-2} : a, b = 0, 1, \cdots, p-1\}$$

consists of p^2 distinct elements. If $p(k-2)$ were greater than or equal to k, then every element y of the set A will satisfy the equation $y^p = 1$, since $px = 0$ and p is a prime. This is in contradiction to the fact that, for any positive integer n, the number of solutions of the equation $y^n = 1$ in any Gilmer ring is at the most equal to n. So if $k > 2$ we must have $k > p(k-2) \geqq 2(k-2)$, and we get $k = 3$ and $p = 2$. As this implies that $x^3 = 0$ and so $(1+x)^4 = 1$ for all x in the set $N(2)$, we get $|N(2)| \leqq 4$. Since 0, u, u^2 and u^2+u are distinct elements of the set $N(2)$, we see that the proof of (ii) is complete. The proof of (i) will now be obvious.

Section 2

(2.1) The following lemma describes the structures of all Gilmer rings whose orders are powers of odd primes.

Lemma 2. *Let R be a Gilmer ring whose order is a power of an odd prime p. Then R will be isomorphic to a ring of one, and only one, of the types* (a), (b), (c) *mentioned in Theorem* 1.

Proof. In the course of this proof we use many of the results stated in § (1.2). Suppose first that R is semisimple, so that $R = R_1 \oplus \cdots \oplus R_k$ where each R_i is a field. (Refer § (1.2) (viii).) As $p-1$ $(\geqq 2)$ will be a factor of each $|G_{R_i}|$, it follows (from § (1.2) (ii)) that we can have only $k = 1$, so that $R = R_1$ is a field. Thus R will be of type (a) in case R is semisimple.

We suppose hereafter that R has radical $J \neq (0)$. The quotient ring R/J is a semisimple Gilmer ring (refer § (1.2) (vi)) and is therefore a field. All the nonunits of R belong to the nil ideal J (refer § (1.2) (v)). Now we have to distinguish between two cases.

CASE (1). Here we suppose that R has characteristic p. Then $J \subseteqq N(p)$ and as $J \neq (0)$, we have $|J| = |N(p)| = p$ and $J^2 = (0)$ (from Lemma 1, since the prime p is odd). As R has only p left zero divisors and as $|R|$ is a power of p, (using § (1.2) (ix)) we can conclude that $|R| = p^2$. If u is any nonzero element of J one can easily verify that $R = \{a \cdot 1+bu : a, b = 0, 1, \cdots, p-1; p \cdot 1 = u^2 = 0\}$, by showing that the set on the right side of this equation has p^2 distinct elements. Thus $R = F[X]/(X^2)$ with $F = GF(p)$ and so R is of type (c) in this case.

CASE (2). Here we suppose that R has characteristic p^m with $m > 1$. The subring S (refer § (1.1)) is isomorphic to $Z/(p^m)$ so that $N(p) \subset S$. We now assert that $S = R$. Suppose the contrary that R contains an element x which does not belong to S. As $p^m \cdot x = 0 \in S$, there exists an integer α with $0 \leqq \alpha \leqq m-1$ such that $p^\alpha \cdot x \notin S$ while $p^{\alpha+1} \cdot x \in S$. As $S \cong Z/(p^m)$ there is an element y in S such that $p^{\alpha+1} \cdot x = p^{\alpha+1} \cdot y$. If we write $z = p^\alpha(x-y)$, we have $z \notin S$ and $pz = 0$. As every unit in R has additive order p^m $(m > 1)$, and as every nonunit of R belongs to J, we find that $z \in J$. As J is a nil ideal and $pz = 0$, we have $z \in N(p)$. But this is in contradiction to the facts: $z \notin S$, $N(p) \subset S$. This contradiction proves our assertion that $S = R$ and hence shows that R is of type (b) in this case.

As the very method of proof shows that the above three rings are mutually nonisomorphic the proof of the lemma is complete.

Section 3

(3.1) In this section we determine completely the structures of all indecomposable Gilmer rings whose orders are powers of 2, and thus complete the proof of Theorem 1. For this purpose we require some preliminary results which are given in the following lemma.

LEMMA 3. (Eldridge and Fischer [1, Lemmas 5 and 6])

Let R be any Gilmer ring whose order is a power of 2 and let J be its Jacobson radical. Then the following results hold.

(i) *The characteristic of R is either 2 or 4.*

(ii) *Every nilpotent element of R belongs to J.*

(iii) *If the characteristic of R is 2, then*
either $J = (0)$,
or $J = \{0, u : u^2 = 0\}$,
or $J = \{0, u, u^2, u^2+u : u^3 = 0\}$.

(iv) *If the characteristic of R is 4, then*
either $J = \{0, 2\}$,
or $J = \{0, 2, u, u+2 : 2u = u^2-2 = 0\}$.

Proof. The characteristic of R is 2^k for some positive integer k, and so the subring S (defined in § (1.1)) $\cong Z/(2^k)$. As $G_S = S \cap G_R$ and therefore G_S is cyclic, we get $k = 1$ or 2 from a well known result. This proves (i). The result (ii) follows from § (1.2) (viii).

We will now show that $J = N(2)$. That $N(2) \subseteqq J$ follows from (ii); for proving the reverse inclusion we need consider only the case where the characteristic of R is 4. If x is any element of J, $2(1+x) \neq 0$, because $(1+x)$ is a unit; then $(1+2x)^2 = 1$ and $1+2x \neq -1$ imply that $1+2x = 1$. This proves the desired result that $J \subseteqq N(2)$, and the result (iii) follows from Lemma 1.

Again suppose that the characteristic of R is 4. As the element 2.1 is nilpotent, we have $J \neq (0)$ and if $|J| = 2$ then $J = \{0, 2\}$. If $J = \{0, u, u^2, u^2+u\}$ we can only have $2 = u^2$ since $2^2 = 0 \neq (u)^2 = (u^2+u)^2$. This completes the proof of the lemma.

(3.2) Remarks. (i) From the proof of the direct part of Th. 1 we see that all the cases mentioned in the results (iii) and (iv) of the above lemma are possible.

(ii) For proving the results (iii) and (iv) of the above lemma Eldridge and Fischer depend upon the classification of all commutative Gilmer rings given in [2].

(3.3) The following two lemmas give the structures of all indecomposable Gilmer rings whose orders are powers of 2.

Lemma 4. *Let R be a Gilmer ring whose order is a power of* 2 *and let J be its Jacobson radical. If the quotient ring R/J is a field, then R will be isomorphic to a ring of one, and only one, of the types* (a), (c), (d), (e), (f) *mentioned in Theorem* 1.

Proof. If $J = (0)$ then $R \cong R/J$ is a field (by our hypothesis) so that R will be of type (a) in this case. Hereafter we suppose that $J \neq (0)$. From the results (iii), (iv) of the previous lemma we see that we have to discuss four cases. We now assert that $R = J \cup \{1+J\}$ in all these cases. Granting this assertion for the moment and using the results (iii) and (iv) of the previous lemma we get the following results: when $|J| = 2$, $R = J \cup \{1+J\}$ will be of type (c) or of type (d) according as the characteristic of R is 2 or 4, and when $|J| = 4$, R will be of type (e) or of type (f) according as the characteristic of R is 2 or 4.

So the proof of the lemma will be complete if we show that

$R = J \cup \{1+J\}$ in case $J \neq (0)$. Suppose first that $|J| = 4$ so that $J = \{0, u, u^2, u^2+u : 2u = u^3 = 0\}$. (Note: This is valid even when the characteristic of R is 4.) Let g be a generator of the cyclic group of units of R and let $gu^2 = v$. As $v \in J$, $v \neq 0$ and $vu = 0$, we see that $(gu^2 =) \, v = u^2$, so that $(g-1)$ is a zero divisor in R. As all the nonunits of R belong to J (for R/J is a field) we have $g = 1+w$ for some w in J, and hence $g^4 = (1+w)^4 = 1$. This shows that $|G_R| \leqq 4$. But as $\{1+J\}$ is a subgroup of order 4 in G_R we get $G_R = 1+J$. So we have $R = J \cup G_R = J \cup \{1+J\}$, in the case $|J| = 4$. As the proof for the case $|J| = 2$ is quite similar, the proof of the lemma is complete.

Lemma 5. *Let R be an indecomposable Gilmer ring whose order is a power of 2 and let J be its Jacobson radical. If the ring R/J is not a field, R will be isomorphic to the ring* (g) *of Theorem* 1.

Proof. By § (1.2) (viii), the ring R/J is the direct sum of k $(\geqq 1)$ fields; our conditions on R imply that $k \geqq 2$, and hence that $J \neq (0)$. By Lemma 3, there exists a unique nonzero element v (say) in the entire ring R such that $v^2 = 0$. Lifting idempotent elements from the quotient ring R/J, we can get k mutually orthogonal nonzero idempotents $e_1, \cdots, e_k$ in the ring R such that $e_1 + \cdots + e_k = 1$ and such that $(Re_i + J)/J = (e_iR+J)/J$ is a field for each i; and then we consider the Peirce decompositions $R = Re_1 \oplus \cdots \oplus Re_k$ and $R = e_1R \oplus \cdots \oplus e_kR$. (Refer Jacobson [3, Ch. III, Sections 7 and 8].) If $e_iRe_j = (0)$ for all i, j with $i \neq j$, it will follow that R is decomposable into the direct sum of k $(\geqq 2)$ nonzero ideals $Re_i = e_iRe_i = e_iR$, a contradiction to our hypothesis. If $e_iRe_j \neq (0)$ for a pair i, j, with $i \neq j$, then $e_iRe_j = \{0, v\}$, since $(e_iRe_j)^2 = (0)$. If $(0) \neq e_iRe_j = e_\alpha Re_\beta$, it follows easily that $\alpha = i$ and $\beta = j$. So we may suppose that $e_1Re_2 = \{0, v\}$ and that $e_iRe_j = (0)$ for all other pairs i, j with $i \neq j$. Now if $k \geqq 3$, R will be the direct sum of the nonzero ideals $R(e_1+e_2) = (e_1+e_2)R$, and e_iRe_i for $i \geqq 3$, a contradiction. So we must have $k = 2$.

We have $J = e_1Je_1 + e_1Je_2 + e_2Je_2$. If $e_1Je_1 \neq (0)$ we can find a nonzero element z in e_1Je_1 such that $z^2 = 0$. But this will imply $e_1ze_1 = z = v \in e_1Re_2$, a contradiction since $v \neq 0$. So $e_iJe_i = (0)$ for $i = 1, 2$ and we find that $J = e_1Je_2 = e_1Re_2 = \{0, v\}$. The supposition that the characteristic of R is 4 will lead to $v = 2$, a contradiction because $v = e_1ve_2$ does not commute with e_1. So we have proved that the characteristic of R is 2 and that $|J| = 2$. (Refer Lemma 3.)

Now $J = e_1Re_2 \subset Re_2$. If J_2 is the Jacobson radical of Re_2, then $J_2 = J$. (For, as J is a nil ideal in Re_2, $J \subseteqq J_2$ and the reverse inclusion follows from Lemma 3 (ii)). As $Re_2/J_2 = Re_2/J$ is a field, we get $|Re_2| = 4$, and similarly that $|e_1R| = 4$ (by using § (1.2) (ix)). As $Re_1 = e_1Re_1$ is a proper subset of e_1R, we find that $|R| = 8$.

If $F = \{0, 1\}$, then F is a subfield of R, and as every element of R is uniquely expressible in the form ae_1+be_2+cv with a, b, c in F, and as the mapping

$$(ae_1+be_2+cv) \rightarrow \begin{pmatrix} a & c \\ 0 & b \end{pmatrix} \qquad (a, b, c \in F)$$

is easily verified to be an isomorphism, we see that R is isomorphic to the ring of all 2×2 upper triangular matrices over the field $GF(2)$. This completes the proof of the lemma.

(3.4) The result (v) of § (1.2) shows that the rings considered in Lemmas 2 and 4 are all indecomposable. So the Lemmas 2, 4 and 5 together prove the first statement in the converse part of Theorem 1.

The proof of Theorem 1 is now complete.

REFERENCES

K. E. Eldridge and I. Fischer

[1] *DCC* rings with a cyclic group of units, Duke Math. J. 34, 243—248 (1967).

R. W. Gilmer

[2] Finite rings having a cyclic multiplicative group of units, Amer. J. Math. 85, 247—252 (1963).

N. Jacobson

[3] Structure of Rings, Colloquium Publication volume XXXVII of the Amer. Math. Soc., (1956).

K. Koh

[4] On "Properties of Rings with a Finite Number of Zero Divisors", Math. Annalen 171, 79—80 (1967).

(Oblatum 12–IX–68)

Department of Mathematics
Annamalai University
Annamalainagar, Madras State, India