COMPOSITIO MATHEMATICA

ROBERT S. WILSON

On the structure of finite rings

Compositio Mathematica, tome 26, nº 1 (1973), p. 79-93
<http://www.numdam.org/item?id=CM_1973__26_1_79_0>

COMPOSITIO MATHEMATICA, Vol. 26, Fasc. 1, 1973, pag. 79-93
Noordhoff International Publishing
Printed in the Netherlands

ON THE STRUCTURE OF FINITE RINGS

by

Robert S. Wilson *

Introduction

In this paper we shall concern ourselves primarily with completely primary finite rings and shall obtain results about other types of rings by means of the Peirce decomposition and other methods. Recall that an Artinian ring R with radical J is called primary if R/J is simple and is called completely primary if R/J is a division ring The deepest study into the nature of completely primary finite rings appears to have been made by Raghavendran [5]. We first state some of his major results.

In what follows Z will denote the rational integers, and if S is a finite set, $\#(S)$ will denote the number of elements in S.

THEOREM A. *Let R be a completely primary finite ring with radical J and let $R/J \cong GF(p^r)$. Then*

(1) $\#(R) = p^{nr}$ *and* $\#(J) = p^{(n-1)r}$ *for some prime p and some positive integer n,*

(2) $J^n = (0)$;

(3) *The characteristic of R is p^k for some positive integer $k \leqq n$.*

This is essentially Theorem 2 of [5]. Of special interest is the case $k = n$. To consider this case Raghavendran introduced the following class of rings.

DEFINITION. Let $f(x) \in Z[x]$ be a monic polynomial of degree r which is irreducible modulo p. Then the ring $Z[x]/(p^n, f)$ is called the *Galois ring* of order p^{nr} and characteristic p^n, and will be denoted by $G_{n,r}$; the prime p will be clear from the context. That $G_{n,r}$ is well defined independently of f the monic polynomial of degree r follows from §§ (3.4), (3.5) of [5] where it is shown that any two completely primary rings R of characteristic p^n with radical J such that $\#(R) = p^{nr}$ and $\#(R/J) = p^r$ are isomorphic. Note that $GF(p^r) \cong G_{1,r}$ and $Z/(p^k) \cong G_{k,1}$. The importance of this class of rings is illustrated in

* Written while the author was an NSF Trainee at the University of California at Santa Barbara, California, working on his dissertation under the direction of Professor Adil Yaqub.

THEOREM B. *Let R, p, r, be as in Theorem A. Then*

(1) *R will contain a subring isomorphic to $G_{k,r}$ if and only if the characteristic of R is p^k.*

(2) *If R_2, R_3 are any two subrings of R both isomorphic to $G_{k,r}$ then there will be an invertible element a in R such that* $R_2 = a^{-1}R_3a$. This is Theorem 8 of [5].

In § 1 we obtain some alternate characterizations of Galois rings, show that any Galois ring is the homomorphic image of a principal ideal domain, and compute the tensor product of two Galois rings.

Since the additive group of a finite ring is a finite Abelian group, the additive structure of a finite ring is in a sense completely determined by the fundamental theorem of finite Abelian groups as a direct sum of cyclic groups of prime power order. In § 2 we use the results from § 1 to establish a connection between the multiplicative structure of the ring and the cyclic decomposition of its additive group.

In § 3 we prove that any completely primary finite ring for which p, n, r, and k are as in Theorem A is the homomorphic image of a ring of $m \times m$ matrices over $G_{k,r}(p)$ for some $m \leqq n$ in which p divides all entries below the main diagonal of each matrix. As a result we can also prove that any finite nilpotent ring of characteristic p^k is the homomorphic image of a ring of matrices over $Z/(p^k)$ in which p divides all entries on and below the main diagonal of each matrix. We thus obtain characterizations of completely primary finite rings and finite nilpotent rings of prime power characteristic. It should be pointed out here that some time ago Szele [6] reduced all problems on the structure of nilpotent Artinian rings to problems about nilpotent finite rings of prime power characteristic, and therefore, our result taken together with [6] yields a characterization of all nilpotent Artinian rings.

1. Remarks on Galois rings

We first remark that any finite ring is the direct sum of finite rings of prime power characteristic. This follows from noticing that when we decompose the additive group of the ring into a direct sum of subgroups of distinct prime power orders, that the component subgroups are ideals. See [2] for further information on this question.

So without loss of generality (up to direct sum formation), we need only consider rings of prime power order. For the remainder of this paper the letter p will denote an arbitrary fixed rational prime and unless otherwise stated, all rings considered will be of characteristic p^k for some positive integer k. If x is an element of such a ring we call the smallest positive integer e such that $p^e x = 0$ the *order of* x.

In this section we prove some results on Galois rings which will be used in what follows.

PROPOSITION 1.1. Any Galois ring is the homomorphic image of a local PID whose unique maximal ideal is generated by the rational prime p.

PROOF. $G_{n,r}$ is a ring of Witt vectors of length n [5; p. 212, § (3.5)]. Hence $G_{n,r}$ is the homomorphic image of the ring of Witt vectors $W(K)$ of infinite length, $K = GF(p^r)$, a discrete valuation ring whose unique maximal ideal is generated by the rational prime p ([8], pp. 234–236).

COROLLARY 1. *Any ideal of $G_{k,r}$ is of the form $p^i G_{k,r}\, i = 0, 1, \cdots, k$.*

COROLLARY 2. *Any finite $G_{k,r}$-module M is a direct sum of cyclic $G_{k,r}$-modules. If*

$$M = \sum_{i=1}^{s}{}^{\cdot}\, G_{k,r}x_i = \sum_{j=1}^{t}{}^{\cdot}\, G_{k,r}y_j$$

are two decompositions of M into cyclic submodules then $s = t$ and the orders of the x_i are (perhaps after reindexing) equal to the orders of the y_j.

PROOF. If $W(K)$ is the PID mapping onto $G_{k,r}$ by Proposition 1.1 then R possesses the structure of a torsion $W(K)$-module. As is well known, the proof of the fundamental theorem of finite abelian groups (see [3]) translates into a fundamental theorem for finitely generated torsion modules over PID'S, and applying this latter theorem to the $W(K)$-module structure of R we see that R is a direct sum of cyclic torsion $W(K)$-modules. As $p^k W(K)$ annihilates R we conclude that R is a direct sum of cyclic $G_{k,r}$-modules.

REMARK. An important example of a finite ring of characteristic p^k which contains $G_{k,r}$ is $G_{k,m}$ where m is a multiple of r by Proposition 1 of § (3.8) of [5]. As a consequence of Corollary 1 the elements of $G_{k,m}$ of order i for $i < k$ are precisely the elements of $pG_{k,m}$. If on the other hand, we view $G_{k,m}$ as a direct sum of cyclic $G_{m,r}$-modules and count elements of order p^i for $i < k$ we conclude that $G_{k,m}$ is free over $G_{k,r}$ on m/r generators.

We shall make repeated use of

PROPOSITION 1.2. *Let k_1, k_2, r_1, r_2 be positive integers. Let $k =$* min *(k_1, k_2),* and space *$d = gcd(r_1, r_2)$, and $m = lcm(r_1, r_2)$. Then*

$$G_{k_1,r_1} \underset{Z}{\otimes} G_{k_2,r_2} \cong \sum_{1}^{d}{}^{\cdot}\, G_{k,m}.$$

PROOF. We first note that

$$(1) \qquad G_{k_1,r_1} \underset{Z}{\otimes} G_{k_2,r_2} \cong G_{k,r_1} \underset{Z/(p^k)}{\otimes} G_{k,r_2}.$$

Now by Proposition 1, § (3.8) of [5] every subring of $G_{k,r}$ is isomorphic to $G_{k,s}$ where s divides r and, conversely for every positive integer s which divides r, $G_{k,r}$ contains a subring isomorphic to $G_{k,s}$. Therefore both G_{k,r_1} and G_{k,r_2} contain subrings isomorphic to $G_{k,d}$. We thus have G_{k,r_1} and G_{k,r_2} as left and right $G_{k,d}$-modules. Therefore

$$(2) \qquad G_{k,r_1} \underset{Z/(p^k)}{\otimes} G_{k,r_2} \cong$$

$$G_{k,r_1} \underset{G_{k,d}}{\otimes} (G_{k,d} \underset{Z/(p^k)}{\otimes} G_{k,d}) \underset{G_{k,d}}{\otimes} G_{k,r_2}$$

so we first seek to determine $G_{k,d} \otimes_{Z/(p^k)} G_{k,d}$. It is straightforward to show that

$$G_{k,d} \cong \frac{(Z/(p^k))[x]}{(\bar{f}(x))}$$

where $\bar{f}(x) \in (Z/(p^k))[x]$ is the image of a polynomial of degree d, $f(x) \in Z[x]$ which is irreducible mod p. Let $\bar{\bar{f}}(x)$ be the image of $f(x)$ and hence of $\bar{f}(x)$ in $(Z/(p))[x]$. As $f(x)$ is supposed to be irreducible of degree d mod p it follows that $\bar{\bar{f}}(x)$ splits into distinct linear factors over $GF(p^d)$. Therefore by Theorem 6 of [5] $\bar{f}(x)$ splits into d distinct linear factors over $G_{k,d}$. Say $(x-\bar{a}_1), \cdots, (x-\bar{a}_d)$. Then

$$\begin{aligned} &G_{k,d} \underset{Z/(p^k)}{\otimes} G_{k,d} \\ &\cong \frac{(Z/(p^k))[x]}{(\bar{f}(x))} \underset{Z/(p^k)}{\otimes} G_{k,d} \\ &\cong G_{k,d}[x]/(\bar{f}(x)) \cong \sum_{i=1}^{d}{}^{\cdot}\, G_{k,d}[x]/(x-\bar{a}_i) \\ &\cong \sum_{1}^{d}{}^{\cdot}\, G_{k,d}. \end{aligned}$$

From (2) we thus have

$$\begin{aligned} G_{k,r_1} \underset{Z/(p^k)}{\otimes} G_{k,r_2} &\cong G_{k,r_1} \underset{G_{k,d}}{\otimes} \Big(\sum_{1}^{d}{}^{\cdot}\, G_{k,d}\Big) \underset{G_{k,d}}{\otimes} G_{k,r_2} \\ &\cong \sum_{1}^{d}{}^{\cdot}\, G_{k,r_1} \underset{G_{k,d}}{\otimes} G_{k,r_2}. \end{aligned}$$

Thus to prove the lemma we need only show that

$$(3) \qquad G_{k,r_1} \underset{G_{k,d}}{\otimes} G_{k,r_2} \cong G_{k,m}.$$

We first prove (3) in case $k = 1$, i.e., for the case of fields. Since $m = lcm(r_1, r_2)$ it follows that $GF(p^m)$ contains a subfield isomorphic to $GF(p^{r_1})$ and a subfield isomorphic to $GF(p^{r_2})$ so we may consider $GF(p^{r_1})$, $GF(p^{r_2}) \subset GF(p^m)$ with $GF(p^{r_1}) \cap GF(p^{r_2}) = GF(p^d)$. Let

$$F = \{ \sum_i a_i b_i \in GF(p^m) | a_i \in GF(p^{r_1}),\ b_i \in GF(p^{r_2})\}.$$

F being a subring of finite field is a finite field with p^s elements for some positive integer s. Since $GF(p^{r_1})$, $GF(p^{r_2}) \subset F$ we have that r_1 and r_2 both divide s. Therefore m divides s. Since $F \subset GF(p^m)$ we conclude that $F = GF(p^m)$ and hence any element in $GF(p^m)$ can be represented in the form $\sum_i a_i b_i$ with $a_i \in GF(p^{r_1})$, $b_i \in GF(p^{r_2})$. We now define a map from $GF(p^{r_1}) \otimes_{GF(p^d)} GF(p^{r_2})$ to $GF(p^m)$ by

$$\sum_i a_i \otimes b_i \to \sum_i a_i b_i .$$

By the remarks above, this map is onto, and by counting dimensions over $GF(p^d)$ we conclude that it is an isomorphism, and we conclude that

$$GF(p^m) \cong GF(p^{r_1}) \underset{GF(p^d)}{\otimes} GF(p^{r_2}).$$

We now consider the diagram

$$\begin{array}{ccc} G_{k,r_1} \times G_{k,r_2} & \xrightarrow{\otimes} & G_{k,r_1} \underset{G_{k,d}}{\otimes} G_{k,r_2} \\ & \searrow^{\varphi} & \downarrow h \\ & & GF(p^{r_1}) \underset{GF(p^d)}{\otimes} GF(p^{r_2}) \cong GF(p^m) \end{array}$$

where $\varphi(a, b) = \psi_1(a) \otimes \psi_2(b)$ with ψ_i being the map

$$G_{k,r_2} \to G_{k,r_i}/J_i \cong GF(p^{r_i})$$

J_i the radical of G_{k,r_1} $i = 1, 2$. It is clear that φ is bilinear over $G_{k,d}$ and multiplicative in each variable so there exists an induced homomorphism h from $G_{k,r_1} \otimes_{G_{k,d}} G_{k,r_2}$ onto $GF(p^r)$. $G_{k,r_1} \otimes_{G_{k,d}} G_{k,r_2}$ is thus a completely primary ring homomorphic to $GF(p^m)$ of characteristic p^k. Since G_{k,r_1} and G_{k,r_2} are free over $G_{k,d}$ on r_1/d respectively r_2/d generators, it follows that $G_{k,r_1} \otimes_{G_{k,d}} G_{k,r_2}$ is free over $G_{k,d}$ on $(r_1/d)(r_2/d) = m/d$ generators and hence

$$\#\left(G_{k,r_1} \underset{G_{k,d}}{\otimes} G_{k,r_2}\right) = \#(G_{k,d})^{m/d} = (p^{kd})^{m/d} = p^{km}$$

and therefore (3) is established and the proposition is proved.

2. The additive structure of finite rings

As in the last section, all rings will be of characteristic p^k for some positive integer k.

In this section we delve deeper into the additive structure of completely primary finite rings. In particular, we will later need information about completely primary finite rings viewed as $(G_{k,r}, G_{k,r})$-modules. As is well known, if A and B are commutative rings, an abelian group M admits an (A, B)-module structure if and only if it admits a left $A \otimes_Z B$-module structure: the scalar multiplications being related by the rule

$$amb = (a \otimes b)m, \ a \in A, \ b \in B, \ m \in M.$$

We are thus led to consider the structure of a $G_{k_1,r_1} \otimes_Z G_{k_2,r_2}$-module.

THEOREM 2.1. *Let M be a $G_{k_1,r_1} \otimes_Z G_{k_2,r_2}$-module, and let* $k = \min(k_1, k_2)$, $d = gcd(r_1, r_2)$, $m = lcm(r_1, r_2)$. *Then M is a direct sum of $G_{k_1,r_1} \otimes G_{k_2,r_2}$-submodules which are cyclic left $G_{k,m}$-modules, and given any two decompositions of M into $G_{k_1,r_1} \otimes_Z G_{k_2,r_2}$-submodules.*

$$M = \sum_{q=1}^{s}{}^{\cdot}\, G_{k,m} a_q = \sum_{q=1}^{t}{}^{\cdot}\, G_{k,m} b_q,$$

$s = t$ and the order of a_q is (after a possible reordering of the b_q) the order of b_q.

PROOF. We know from Proposition 1.2 that

$$G_{k_1,r_1} \underset{Z}{\otimes} G_{k_2,r_2} \cong \sum_{1}^{d}{}^{\cdot}\, G_{k,m},$$

so we consider M as a $\sum_1^{d\cdot} G_{k,m}$-module. Let $e_1, \ldots, e_d$ be an orthogonal system of primitive idempotents for $\sum_1^{d\cdot} G_{k,m}$, i.e.,

$$e_1 + \cdots + e_d = 1, \ e_i e_j = 0 \text{ for all } i \neq j.$$

Then $M = 1M = (e_1 + \cdots + e_d)M = e_1 M + \cdots + e_d M$. We wish to show that this sum is direct. Let $m \in e_i M \cap e_j M$ for $i \neq j$. Then $m \in e_i M$ implies that $e_i m = m$ and $m \in e_j M$ implies that $e_j m = m$. Therefore

$$m = e_i m = e_i(e_j m) = (e_i e_j)m = Om = 0$$

and the sum is direct.

But e_i is the multiplicative identity of the i^{th} component of the direct sum $\sum_1^{d\cdot} G_{k,m}$ and hence the structure of $e_i M$ as a $\sum_1^{d\cdot} G_{k,m}$-module is the same as its structure as a $G_{k,m}$-module with scalar multiplication defined by $ge_i m = (g, \cdots, g)e_i m$ and the result now follows from Corollary 2 of Proposition 1.1.

COROLLARY. *Let R be a finite ring with* 1 *of characteristic p^k and let $e_1, \cdots, e_m$ be a complete set of primitive idempotents for R. Let e_iRe_i have characteristic p^{k_i} and suppose that $e_iRe_i/e_iJe_i \cong GF(p^{r_i})$. Let $k_{ij} = \min (k_i, k_j)$, $d_{ij} = gcd\ (r_i, r_j)$ and $m_{ij} = lcm(m_i, m_j)$. Then in the Peirce decomposition of R* [4; pp. 48, 50]

$$R = \sum_{i,j=1}^{m} {}^{\cdot}\ e_iRe_j$$

e_iRe_j is isomorphic as a $(G_{k_i,r_i}, G_{k_j,r_j})$-module to a direct sum of cyclic left $G_{k_{ij},m_{ij}}$-modules and the orders of the generators for one decomposition are the orders of the generators obtained in any other such decomposition.

PROOF. Since e_iRe_i is completely primary of characteristic p^{k_i} and radical e_iJe_i such that $e_iRe_i/e_iJe_i \cong GF(p^{r_i})$, it follows from Theorem B that e_iRe_i contains a subring isomorphic to G_{k_i,r_i}. Since e_iRe_j is a (e_iRe_i, e_jRe_j)-module it is thus a $(G_{k_i,r_i}, G_{k_j,r_j})$-module and hence a left $G_{k_1,r_i} \otimes_Z G_{k_j,r_j}$-module. The result now follows from Theorem 2.1.

PROPOSITION 2.2. *Let R be a completely primary finite ring of characteristic p^k with radical J such that $R/J \cong GF(p^r)$. Then there exists an independent generating set $b_1, b_2, \cdots, b_m$* of R *as a left $G_{k,r}$-module such that*:

(1) $b_1 = 1$; $b_2, \cdots, b_m \in J$.

(2) $G_{k,r}b_i$ is a $(G_{k,r}, G_{k,r})$-submodule of R.

PROOF. We first note that $G_{k,r} \cdot 1$ is a $(G_{k,r}, G_{k,r})$-submodule. Moreover, $G_{k,r} \cdot 1$ is $(G_{k,r}, G_{k,r})$-module isomorphic to a direct summand of $G_{k,r} \otimes_Z G_{k,r}$ by Proposition 1.2. Now $G_{k,r}$ being the homomorphic image of a PID is a quasi-Frobenius ring (Exercise 2c of § 58 of [1]). As is well known and easy to see, a direct sum of quasi-Frobenius rings is also quasi-Frobenius. Hence $G_{k,r} \otimes_Z G_{k,r} \cong \sum_1^{r} {}^{\cdot}\ G_{k,r}$ is quasi-Frobenius. Therefore $G_{k,r}$ is a direct summand of $G_{k,r} \otimes_Z G_{k,r}$ and hence a projective $G_{k,r} \otimes_Z G_{k,r}$-module. But projective modules over quasi-Frobenius rings are also injective, so $G_{k,r}$ is an injective $G_{k,r} \otimes_Z G_{k,r}$-module, hence an injective $(G_{k,r}, G_{k,r})$-module, i.e., $G_{k,r} \cdot 1$ is a $(G_{k,r}, G_{k,r})$-module direct summand of R. Therefore there exists another $(G_{k,r}, G_{k,r})$-submodule M of R such that $R = G_{k,r} \cdot 1 \dot{+} M$. We now need to show that M can be generated by nilpotents. We first obtain a left $G_{k,r}$-module decomposition $R = G_{k,r} \cdot 1 \dot{+} L$ where L is generated by nilpotents. Let

$$R = \sum_{i=1}^{m} {}^{\cdot}\ G_{k,r}b_i \qquad b_1 = 1$$

be a left $G_{k,r}$-module decomposition of R. Let e_i be the order of b_i. If $e_i \leqq k-1$ then $b_i \in \{x \in R | p^{k-1}x = 0\}$ which is a proper ideal of R and hence contained in the unique maximal ideal J. Thus we conclude that if $e_i \leqq k-1$ then $b_i \in J$. Next suppose $e_i = k$. Let $\varphi : R \to R/J \cong GF(p^r)$ be the cannonical surjection. Since φ takes $G_{k,r}$ onto $GF(p^r)$ it follows that there is a $g_i \in G_{k,r}$ such that $\varphi(g_i) = \varphi(b_i)$, i.e., $\varphi(b_i - g_i) = 0$ which implies that $b_i - g_i \in J$. We thus obtain a new set $\{1, b'_2, \cdots, b'_m\}$ where $b'_i = b_i - g_i$ if $e_i = k$ and $b'_i = b_i$ if $e_i \leqq k-1$, and $b'_2, \ldots, b'_m \in J$. It is straightforward to verify that $1, b'_2, \ldots, b'_m$ is an independent generating set of R as a left $G_{k,r}$-module. We thus have that $pG_{k,r} \dotplus \sum_{i=2}^{m} G_{k,r}b'_i$ is a decomposition of J. Next, since J is an ideal of R and hence a $(G_{k,r}, G_{k,r})$-submodule, we let $J = \sum_{i=1}^{s} G_{k,r}a_i$ be a decomposition of J into a direct sum of $(G_{k,r}, G_{k,r})$-submodules which are cyclic left $G_{k,r}$-modules as in Theorem 2.1. Then *a fortiori* the latter decomposition is a left $G_{k,r}$-module decomposition of J so we know that $s = m$ and the orders of a_i is the order of b'_i after a possible reindexing. Let f_i be the order of a_i. Assume that the a_i are ordered such that $f_1 = \cdots = f_t = k, f_{t+1}, \cdots, f_m \leqq k-1$. We wish to prove that $1, a_1, \cdots, a_t$ are independent over $G_{k,r}$. Suppose that there is a linear dependence relation among them. Such a relation can be written

$$g_0 = \sum_{i=1}^{t} g_i a_i g_0, g_1, \cdots, g_t \in G_{k,r}.$$

If $g_0 = 0$ then the relation becomes

$$\sum_{i=1}^{t} g_i a_i = 0.$$

But the a_i are supposed to be independent so $g_i a_i = 0$, $i = 1, \cdots, t$, and the relation is trivial. So suppose that $g_0 \in p^{f_0} G_{k,r}$ but not in $p_0^{f_0+1} G_{k,r}$ with $f_0 \leqq k-1$. Then

$$0 = p^{k-f_0} g_0 = \sum_{i=1}^{t} p^{k-f_0} g_i a_i$$

and hence $p^{k-f_0} g_i a_i = 0$ $i = 1, \cdots, t$. and as $f_i = k$ for $i = 1, \cdots, t$ we conclude that $p^{k-f_0} g_i = 0$ $i = 1, \cdots, t$. Thus $g_i \in p^{f_0} G_{k,r}$ $i = 1, \cdots, t$. Let $g_i = p^{f_0} g'_i$ $i = 1, \cdots, t$ and let $g_0 = p^{f_0} g'_0$. Since $g_0 \notin p^{f_0+1} G_{k,r}$ we see that $g'_0 \notin pG_{m,r}$ and hence g'_0 is a unit. We can thus rewrite the integral dependence relation as

$$p^{f_0}(1 - \sum_{i=1}^{t} g_0'^{-1} g'_i a_i) = 0.$$

But $a_1, \ldots, a_m \in J$ so $(1 - \sum_{i=1}^{t} g_0'^{-1} g'_i a_i)$ is a unit, and thus we have

$p^{f_0} = 0$. Hence $f_0 = k$ and $g_0 = 0$ which forces the relation to be trivial. Therefore $G_{k,r} \dotplus \sum_{i=1}^{t} G_{k,r} a_i$ is a $(G_{k,r}, G_{k,r})$-module which is isomorphic to a direct sum of $t+1$ injective $(G_{k,r}, G_{k,r})$-modules, and is hence itself injective. Therefore we can write R as a $(G_{k,r}, G_{k,r})$-module direct sum

$$R \cong (G_{k,r} \dotplus \sum_{i=1}^{t} G_{k,r} a_i) \dotplus M_1 .$$

Now if we express $M_1 = \sum_{j=1}^{m-t-1} {}^{\cdot}\, G_{k,r} c_j$ as a direct sum of $(G_{k,r})$-submodules we have that

$$R \cong G_{k,r} \dotplus \sum_{i=1}^{t}{}^{\cdot}\, G_{k,r} a_i \dotplus \sum_{j=1}^{m-t-1} G_{k,r} c_j$$

is a cyclic decomposition of R as a left $G_{k,r}$-module. But since the orders of the a_i's are the same as the orders of the b_i''s we conclude from the uniqueness of a cyclic decomposition that there are only $t+1$ generators of order k in any decomposition and therefore all of the c_j's have order $\leqq k-1$. Therefore $M_1 \subset \{x \in R | p^{k-1}x = 0\} \subset J$ and by setting $M = \sum_{i=1}^{t}{}^{\cdot}\, G_{k,r} a_i \dotplus M_1$ we obtain the desired decomposition.

§ 3. Characterizations of completely primary and nilpotent finite rings

THEOREM 3.1. *Let R be a completely primary finite ring of characteristic p^k with radical J such that $R/J \cong GF(p^r)$, and let R have an independent generating set consisting of m generators over $G_{k,r}$. Then R is the homomorphic image of a ring T of $m \times m$ matrices over $G_{k,r}$ in which every entry below the main diagonal of every matrix in T is a multiple of p, and, moreover, every main diagonal entry of every matrix of T which is in the preimage of J is also a multiple of p.*

PROOF. We must first obtain the correct independent generating set of R over $G_{k,r}$. Let e be the smallest positive integer such that $J^e = (0)$. Let us consider the set of independent generating sets of R which satisfy the conditions of Proposition 2.2. Suppose that q_1 is the maximum number of elements of any of these generating sets which are in J^{e-1}. Say $b_2, \cdots, b_{q_1+1}$ are in J^{e-1} and are elements of some generating set satisfying Proposition 2.2. We now consider all such independent generating sets which include $b_2, \cdots, b_{q_1+1}$. Suppose q_2 is the maximum number of elements in any of these generating sets which are in J^{e-2}. Say $b_{q_1+2}, \cdots, b_{q_2+q_1+1}$ are in J^{e-2} and are elements of some generating set satisfying Proposition 2.2 which also contain $b_2, \cdots, b_{q_1+1}$. We continue choosing elements or our generating set in this way: at the i^{th} step we have already chosen $1, b_2, \cdots, b_{q_{i-1}+\cdots+q_2+q_1+1}$ and we suppose that the maximum number of elements in J^{e-1} in any generating set satisfying Proposition 2.2 which also includes $b_2, \cdots, b_{q_{i-1}+\cdots+q_1+1}$ is q_i. We choose $b_{q_{i-1}+\cdots+q_1+2}, \cdots, b_{q_i+\cdots+q_1+1} \in J^{e-i}$ which are elements of some generating set satisfying the conditions of Proposition 2.2 which also contain $b_2, \cdots, b_{q_i-1+\cdots+q_1+1}$. After $e-1$ steps we have that $p, b_2, \cdots, b_{q_{e-1}+\cdots+q_1+1}$ generate all of J and hence $1, b_2, \cdots, b_m$ is a generating set satisfying the conditions of Proposition 2.2.

Next let $M = \sum_{i=1}^{m} G_{k,r}c_i$ be a free $G_{k,r}$-module on generators $c_1, \cdots, c_n$. Let e_i be the order of b_i. We embed R into M by identifying $b_i \to p^{k-e_i}c_i$. It is easy to check that this map is an isomorphism of R into M. We next consider R as a subring of the ring of endomorphisms of R considered as a left $G_{k,r}$-module $\mathrm{Hom}_{G_{k,r}}(R, R)$ via the right regular representation, i.e., we consider $x \in R$ to be the endomorphism defined by $x : a \to ax$ for all $a \in R$. We shall thus write all maps in $\mathrm{Hom}_{G_{k,r}}(R, R)$ and in $\mathrm{Hom}_{G_{k,r}}(M, M)$ on the right. Let $T = \{\alpha \in \mathrm{Hom}_{G_{k,r}}(M, M) |$ there exists an $a \in R$ such that for all $x \in R$, $(x)\alpha = xa\}$. Given an $\alpha \in \mathrm{Hom}_{G_{k,r}}(M, M)$, if there exists an $a \in R$ such that $(x)\alpha = xa$ for all $x \in R$ then a is uniquely determined by the fact that $(1)\alpha = 1a = a$. It is straightforward to check that T is a ring and that the map $v : T \to R$ defined by $v : \alpha \to (1)\alpha$ is a ring homomorphism. Since $R \subset M$, we consider any $x \in R$ to be a homomorphism over $G_{k,r}$ into M by $x : a \to ax \in R \subset M$, and since M is a free module over a quasi-Frobenius ring it is injective and the homomorphism x can be extended to an endomorphism of M. We conclude that v is onto. We want to prove that T satisfies the conditions of the theorem.

The matrix representation we obtain for T is the matrix representation obtained over M with respect to the basis $c_1, \cdots, c_m$ i.e., if

$$(c_i)\alpha = \sum_{j=1}^{m} \gamma_{ij}(\alpha)c_j \quad \gamma_{ij}(\alpha) \in G_{k,r} \quad i = 1, \cdots, n$$

then the map from T to $M_m(G_{k,r})$ given by $\alpha \to [\gamma_{ij}(\alpha)]$ is an isomorphism. However, this matrix representation depends on the order in which we index the c_i. We index the c_i by specifying the order of the b_i. We take $b_1 = 1$. We then assume that if e_i is the order of b_i that $e_2 \leqq e_3 \leqq \cdots \leqq e_m$. Next let f_i be the positive integer such that $b_i \in J^{f_i}$ but $b_i \notin J^{f_i+1}$. We call f_i the radical index of b_i. We shall further assume that if $e_i = e_j$ with $i \geqq j$ then $f_i \geqq f_j$. We prove that the matrix representation of T with respect to this ordering of the basis $c_1, \cdots, c_m$ of M is of the desired type.

Let $\alpha \in T$. We must compute the action of α on each c_i. $p^{k-c_i}c_i = b_i \in R$ so let $a = (1)\alpha \in R$. $a = \sum_{q=1}^{m} g_q b_q$. Hence

$$(p^{k-e_i}c_i)\alpha = b_i \sum_{q=1}^{m} g_q b_q = \sum_{q=1}^{m} b_i g_q b_q.$$

Now $b_i \in G_{k,r}b_i$ which is a $(G_{k,r}, G_{k,r})$ submodule of R. Hence $b_i g_q \in G_{k,r}b_i$; say $b_i g_q = g_q^{(i)} b_i$ for some $g_q^{(i)} \in G_{k,r}$. So $(p^{k-e_i}c_i)\alpha = \sum_{q=1}^m g_q^{(i)} b_i b_q$.

We now let $b_i b_q = \sum_{j=1}^m \gamma_{ij}^{(q)} b_j$. Then

$$(p^{k-e_i}c_i)\alpha = \sum_{j=1}^m \Big(\sum_{q=1}^m g_q^{(i)} \gamma_{ij}^{(q)} p^{k-e_j}\Big) c_j .$$

Now suppose that $i \geqq j$. Then $e_i \geqq e_j$. If $e_i > e_j$ then p^{k-e_i} properly divides p^{k-e_j}. We conclude that if $i > j$ so that $e_i > e_j$ then the i, j^{th} entry of the matrix representation of α is a multiple of p for all $\alpha \in T$. So we restrict our attention to those i, j such that $i \geqq j$ but $e_i = e_j$. In this case

$$p^{k-e_j}\gamma_{ij}(\alpha) = p^{k-e_j} \sum_{q=1}^m g_q^{(i)} \gamma_{ij}^{(q)}$$

and thus $\gamma_{ij}(\alpha) - \sum_{q=1}^m g_q^{(i)} \gamma_{ij}^{(q)}$ is a multiple of p^{e_j}. Therefore if $\sum_{q=1}^m g_q^{(i)} \gamma_{ij}^{(q)} \in pG_{k,r}$ then so is $\gamma_{ij}(\alpha)$. To show then that every entry below the main diagonal of each matrix on T is a multiple of p, it will suffice to show that for all $q = 1, \cdots, m$, $\gamma_{ij}^{(q)}$ is a multiple of p for all $i > j$ such that $e_i = e_j$. Moreover if $\alpha \in T$ is in the preimage of J then $g_1^{(i)} = 0$ for all $i = 1, \cdots, m$, and, therefore, to show that the main diagonal entries $\gamma_{jj}(\alpha)$ are all multiples of p it will suffice to show that $\gamma_{jj}^{(q)}$ is a multiple of p for all $q = 2, \cdots, m$.

If $q = 1$ then $b_i b_1 = b_i$ and so $\gamma_{ij}^{(1)} = \delta_{ij}$ and thus $\gamma_{ij}^{(1)}$ is a multiple of p for all $i > j$. So the proof of the theorem will be complete if we can show that for all $q = 2, \cdots, m$ $\gamma_{ij}^{(q)}$ is a multiple of p for all $i \geqq j$ such that $e_i = e_j$.

We shall assume that there is a $q \geqq 2$ for which there exists an $i \geqq j$ such that $e_i = e_j$ but $\gamma_{ij}^{(q)}$ is not a multiple of p, and we shall derive a contradiction. Since $q \geqq 2$ $b_q \in J$ so the radical index of $b_i b_q$ is strictly greater than the radical index of b_i which is, by hypothesis, greater than or equal to the radical index of b_j. So from the construction of the generating set $1, b_2, \ldots, b_m$ of R over $G_{k,r}$ we will have our contradiction if we can show that $1, b_2, \cdots, b_{j-1}, b_i b_q, b_{j+1}, \cdots, b_m$ is a generating set of R over $G_{k,r}$ satisfying the conditions of Proposition 2.2.

$$b_i b_q = \sum_{t=1}^m \gamma_{it}^{(q)} b_t$$

and p does not divide $\gamma_{ij}^{(q)}$ so it follows that $1, b_2, \cdots, b_{j-1}, b_i b_q, b_{j+1}, \cdots, b_m$ is a generating set of R over $G_{k,r}$. To show independence, we first note that $p^{e_j}(b_i b_q) = p^{e_i}(b_i b_q) = 0$ so the order of $b_i b_q$ is less than or equal to e_j. However, $\gamma_{ij}^{(q)}$ is not a multiple of p and so we conclude that $p^s(b_i b_q) = \sum_{t=1}^{m} \gamma_{it}^{(q)} p^s b_t \neq 0$ if $s < e_j$ and thus the order of $b_1 b_q$ is the order of b_j. Now since $1, b_2, \cdots, b_{j-1}, b_i b_q, b_{j+1}, \cdots, b_m$ is a generating set the map from the external direct sum

$$\sum_{t=1}^{j-1}{}^{\cdot}\, G_{k,r} b_t \dot{+} G_{k,r} b_i b_q \dot{+} \sum_{t=j+1}^{m} G_{k,r} b_s$$

to R given by

$$(g_1, g_2 b_2, \cdots, g_{j-1} b_{j-1}, g_{j+1} b_{j+1}, \cdots, g_m b_m) \to \sum_{t=1}^{j-1} g_t b_t + g_j b_i b_q + \sum_{t=j+1}^{m} g_t b_t$$

is onto. But as the order of $b_i b_q$ is e_j we conclude that

$$^{\#}\Big(\sum_{t=1}^{j-1}{}^{\cdot}\, G_{k,r} b_t \dot{+} G_{k,r} b_i b_q \dot{+} \sum_{t=j+1}^{m} G_{k,r} b_t\Big) = {}^{\#}R$$

which is equivalent to saying that $1, b_2, \cdots, b_{j-1}, b_i b_q, b_{j+1}, \cdots, b_m$ are independent. Moreover, if $g \in G_{k,r}$, then since $G_{k,r} b_q$ is a $(G_{k,r}, G_{k,r})$-submodule, there exists a $g' \in G_{k,r}$ such that $b_q g = g' b_q$. Similarly given g' there exists a $g'' \in G_{k,r}$ such that $b_i g' = g'' b_i$. Hence $(b_i b_q) g = g''(b_i b_q)$ and we conclude that $G_{k,r} b_i b_q$ is a $(G_{k,r}, G_{k,r})$-submodule of R and, therefore, $1, b_2, \cdots, b_{j-1}, b_i b_q, b_{j+1}, \cdots, b_m$ satisfies the conditions of Proposition 2.2 and the proof is complete.

As a consequence of this result we obtain the following classification of finite nilpotent rings.

THEOREM 3.2. *Let R be a finite nilpotent ring with characteristic n, and let $n = p_1^{k_1} \cdots p_r^{k_r}$ be the prime power factorization of n. Then R is a direct sum*

$$R = \sum_{i=1}^{r}{}^{\cdot}\, R_i$$

where R_i is a homomorphic image of a ring T_i of matrices over $Z/(p_i^{k_i})$ in which every entry on or below the main diagonal of each matrix in T_i is a multiple of p_i.

PROOF. As was noted at the beginning of § 1, a finite ring with characteristic n is a direct sum of rings of characteristic $p_i^{k_i}$. Moreover, each direct summand of a finite nilpotent ring must itself be nilpotent. So we need only consider the case where $n = p^k$ for some prime p.

We embed R into the radical of a completely primary finite ring as follows. Let $\bar{R} = Z/(p^k) + R$ be the usual embedding of R as an ideal into a ring with 1, i.e., the elements of $\bar{R}$ are ordered pairs (n, r) $n \in Z/(p^k)$, $r \in R$ with addition defined coordinate-wise and multiplication defined by

$(n_1, r_1)(n_2, r_2) = (n_1 n_2, n_1 r_2 + n_2 r_1 + r_1 r_2)$. It is easy to see that (n, r) is a unit in $\bar{R}$ if and only if n is not a multiple of p. Hence the nonunits of $\bar{R}$ form an ideal J and $\bar{R}$ is completely primary with R isomorphic to a subring of J. $\bar{R}$ is of characteristic p^k and $\bar{R}/J \cong Z/(p)$ and the result follows immediately from Theorem 3.1.

NOTE. The special cases of Theorem 3.1 in which $k = 1$ and either $J^2 = (0)$ or $J^{n-1} \neq (0)$ where $^{\#}R = p^{nr}$ have been proved in Theorems 3 and 4 of [5]. The special case of Theoıem 3.2 in which $n = p$ for some prime p follows from a very old result which can be found on page 202 of [4].

In [6] Szele essentially reduced all questions about nilpotent Artinian rings to questions about finite nilpotent rings of prime power characteristic. Let p be a prime. A nilpotent Artinian p-ring is a nilpotent Artinian ring R in which for every $x \in R$ there exists a positive integer $k(x)$ such that $p^{k(x)}x = 0$. Szele proved that any nilpotent Artinian ring is a direct sum of a finite number of nilpotent Artinian p-rings and that a nilpotent Artinian p-ring is a direct sum of a finite nilpotent ring of characteristic p^k for some positive integer k and a null ring whose additive group is a direct sum of a finite number of quasi-cyclic groups, i.e., groups isomorphic to the additive group mod 1 of all rationals with p-power denominators. If we combine this result with Theorem 3.2 we obtain the following

COROLLARY. *Any nilpotent Artinian ring is isomorphic to a direct sum of a ring of the type described in Theorem* 3.2 *and a null ring whose additive group is a direct sum of quasi-cyclic groups.*

REMARK. It could be asked whether completely primary and nilpotent finite rings are in general not only homomorphic images of subrings of matrix rings as described in Theorems 3.1 and 3.2 but in fact isomorphic to subrings of such matrix rings. If the ring is of prime characteristic (or of square free characteristic in the case of nilpotent rings) the answer is yes. If $p^k = p$ then $G_{1,r} \cong GF(p^r)$ and R itself is thus a free module over $G_{1,r}$ so we could take both M and T in the proof of Theorem 3.1 to be R. However, in general, the answer to this question is negative as the following example shows.

Let $\varphi : Z/(4) \to Z(2)$ be the usual homomorphism; i.e., $\varphi(0) = \varphi(2) = 0$, $\varphi(1) = \varphi(3) = 1 \in Z/(2)$. We consider the set of matrices with entries in both $Z/(4)$ and $Z/(2)$ of the form

$$\begin{bmatrix} a & b & \varphi(c) \\ 2d & a+2e & f \\ 2g & 2h & a+2i \end{bmatrix}.$$

as $a, b, c, d, e, f, g, h, i \in Z(4)$. Call this set of mixed matrices R and define addition in R coordinatewise and multiplication by

$$\begin{bmatrix} a & b & \varphi(c) \\ 2d & a+2e & f \\ 2g & 2h & a+2i \end{bmatrix} \begin{bmatrix} j & k & \varphi(l) \\ 2m & j+2n & p \\ 2q & 2r & j+2s \end{bmatrix} =$$

$$\begin{bmatrix} aj+2(bm+cq) & ak+bj+2bn+2cr & \varphi(al+bp+cj) \\ 2(dj+am+fq) & aj+2(dk+ej+an+fr) & 2dl+ap+2ep+fj+2fs \\ 2(gj+aq) & 2(gk+hj+ar) & aj+2(gl+hp+as+ij) \end{bmatrix}.$$

The reader can check that these operations are well defined and that R with these operations is a completely primary finite ring of characteristic 4 whose radical J consists of all matrices of the form

$$\begin{bmatrix} 2a & b & \varphi(c) \\ 2d & 2e & f \\ 2g & 2h & 2i \end{bmatrix}.$$

such that $R/J \cong GF(2)$, and that J is a nilpotent finite ring of characteristic 4. Consider the element

$$\begin{bmatrix} 0 & 0 & \varphi(1) \\ 0 & 0 & 0 \\ 2 & 0 & 0 \end{bmatrix} \in J \subset R.$$

Note that

$$2\begin{bmatrix} 0 & 0 & \varphi(1) \\ 0 & 0 & 0 \\ 2 & 0 & 0 \end{bmatrix} = 0$$

so if R or J were isomorphic to a subring of $M_n(Z/(4))$ for some n then we would have

$$\begin{bmatrix} 0 & 0 & \varphi(1) \\ 0 & 0 & 0 \\ 2 & 0 & 0 \end{bmatrix} \in 2M_n(Z/(4))$$

and hence

$$\begin{bmatrix} 0 & 0 & \varphi(1) \\ 0 & 0 & 0 \\ 2 & 0 & 0 \end{bmatrix}^2 \in 4M_n(Z/(4)) = (0).$$

But

$$\begin{bmatrix} 0 & 0 & \varphi(1) \\ 0 & 0 & 0 \\ 2 & 0 & 0 \end{bmatrix}^2 = \begin{bmatrix} 2 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 2 \end{bmatrix} \notin (0)$$

a contradiction.

NOTE. The author wishes to thank the referee for his helpful suggestions.

REFERENCES

CHARLES W. CURTIS and IRVING REINER
[1] *Representation theory of finite groups and associative algebras.* (Interscience 1962).

L. FUCHS
[2] Ringe und ihre additive Gruppe. Publ. Math. Debrecen 4 (1956), 488–508.

E. HECKE
[3] *Vorlesungen über algebraische Zahlentheorie.* (Chelsea 1948).

NATHAN JACOBSON
[4] *Structure of rings.* (Amer. Math. Soc. Colloq. Publ. XXXVII 1964).

R. RAGHAVENDRAN
[5] Finite associative rings. Compositio Math. **21** (1969), 195–229.

T. SZELE
[6] Nilpotent Artinian rings. Publ. Math. Debrecen 4 (1955), 71–78.

OSCAR ZARISKI and PIERRE SAMUEL
[7] *Commutative algebra* (Van Nostrand 1959).

NATHAN JACOBSON
[8] *Lectures on abstract algebra*, Vol. III (Van Nostrand, 1964).

(Oblatum 5–X–71)

University of California
Santa Barbara, California 93106
University of Texas
Austin, Texas 78712