PACIFIC JOURNAL OF MATHEMATICS
Vol. 53, No. 2, 1974

REPRESENTATIONS OF FINITE RINGS

ROBERT S. WILSON

In this paper we extend the concept of the Szele representation of finite rings from the case where the coefficient ring is a cyclic ring to the case where it is a Galois ring. We then characterize completely primary and nilpotent finite rings as those rings whose Szele representations satisfy certain conditions.

1. **Preliminaries.** We first note that any finite ring is a direct sum of rings of prime power order. This follows from noticing that when one decomposes the additive group of a finite ring into its pime power components, the component subgroups are, in fact, ideals. So without loss of generality, up to direct sum formation, one needs only to consider rings of prime power order. For the remainder of this paper p will denote an arbitrary, fixed prime and all rings will be of order p^n for some positive integer n. Of the two classes of rings that will be studied in this paper, completely primary finite rings are always of prime power order, so for the completely primary case, there is no loss of generality at all. However, nilpotent finite rings do not need to have prime power order, but we need only classify finite nilpotent rings of prime power order, the general case following from direct sum formation.

If R is finite ring (of order p^n) then the characteristic of R will be p^k for some positive integer k. If $x \in R$ then we define the order of x to be the smallest positive integer e such that $p^e x = 0$. Thus $0 < e \leqq k$.

We now define a very important class of finite rings.

DEFINITION 1.1. Let $f(x) \in Z[x]$, when Z denotes the rational integers, be monic of degree r and irreducible modulo p. Then the ring $Z[x]/(p^k, f(x))$ is called the Galois ring of order p^{kr} and characteristic p^k, and will be denoted by $G_{k,r}$. Basically, then, a Galois ring is an irreducible algebraic extension of degree r of the cyclic ring $Z/(p^k)$, and any two irreducible algebraic extensions of $Z/(p^k)$ of degree r are isomorphic [2, § 3]. Note that $G_{1,r} \cong GF(p^r)$ and $G_{k,1} \cong Z/(p^k)$. This class of rings was introduced independently by Raghavendran [2] and Janusz [1] both of whom called them Galois rings. The importance of Galois rings, at least in our case, is that if R is a completely primary finite ring of characteristic p^k with Jacobson radical J such that $R/J \cong GF(p^r)$ then R contains a unique (up to inner isomorphism) copy of $G_{k,r}$ ([2, Th. 8]). Thus the com-

pletely primary finite ring R is a $G_{k,r}$-bimodule. The author has developed a structure theory for finite $G_{k,r}$-bimodules and facts that we will need are listed below.

PROPOSITION 1.2. *Let M be a finite $G_{k,r}$-bimodule. Then there exist elements $m_1, \cdots, m_n \in M$ such that*

(i) $M = \sum_{i=1}^{n} \oplus G_{k,r} m_i$

(ii) $G_{k,r} m_i = m_i G_{k,r}$ $i = 1, \cdots, n$.

Moreover, if $M = \sum_{j=1}^{q} \oplus G_{k,r} m_j'$ is another such decomposition of M then $q = n$ and the orders of the m_j' are (after possible reindexing) the orders of the m_i.

This is essentially Theorem 2.1 of [5].

2. **The Szele representation.** The representations we are interested in will be right regular representations with Galois rings as coefficient rings. Thus we adopt the convention of writing maps on the right and scalars on the left. We next introduce the following class of rings. Let $k = k_1 \geqq k_2 \geqq \cdots k_n > 0$ be a nonincreasing sequence of positive integers. Let $\phi_j: G_{k,r} \to G_{k_j,r}$ be the map induced by the cannonical homomorphism $G_{k,r} \to G_{k,r}/p^{k_j} G_{k,r}$ followed by the isomorphism $G_{k,r}/p^{k_j} G_{k,r} \cong G_{k_j,r}$. Let R denote the set of all rectangular arrays $[a_{ij}]$ where $a_{ij} \in G_{k_j,r} (i, j = 1, \cdots, n)$ where for entries below the main diagonal we have a_{ij} is a multiple of $p^{k_j - k_i}$ in $G_{k_j,r}$. Let $S = \{[b_{ij}] \in M_n(G_{k,r}) \mid b_{ij} \in p^{k_j - k_i} G_{k,r} \text{ if } i > j\}$. Define a map $\Phi: S \to R$ by $\Phi: [b_{ij}] \to [(b_{ij})\phi_j]$. Clearly Φ is onto. We define addition and multiplication in R by stipulating that Φ preserves addition and multiplication. R is then a ring. The only thing which is not immediate is that multiplication is well-defined. But that follows from our condition that a_{ij} is a multiple of $p^{k_j - k_i}$ whenever $i > j$. This construction is due to Szele [3] who did it for cyclic rings, however, as we shall see there is no reason why we cannot do it over more general rings. We shall call such a ring and subrings thereof rings of Szele matrices. The class of rings are of interest when studying finite rings because of the following result.

LEMMA 2.1. *Let R be a finite ring of characteristic p^k which contains a copy of $G_{k,r}$. Then the right regular representation of R over $G_{k,r}$ can be realized as a ring of Szele matrices.*

Thus we have immediately

COROLLARY 2.2. *Any finite ring with unit (of prime power of order) is a subring of a ring of Szele matrices over a Galois ring.*

These results were proved by Szele in case the coefficient Galois ring is taken to be a cyclic ring. Any finite ring will of course contain a cyclic ring and it is quite possible that the cyclic subring will be the largest Galois subring so, in a sense, our result does not represent much of a step forward in the study of general finite rings. However, in the study of completely primary finite rings, one can obtain a tractable, complete characterization if one studies the Szele representation over the largest Galois subring.

Proof of Lemma 2.1. Proposition 1.2 supplies all of the necessary tools to follows Szele's original proof except that, in general, Galois subrings do not need to be contained in the center. However, we circumvent that difficulty be writing maps on the right and scalars on the left. $G_{k,r} \subset R$ so R is a $G_{k,r}$-bimodule. Let $b_1, \cdots, b_n$ be a basis of R over $G_{k,r}$ satisfying the conditions of Proposition 1.2. Let k_i be the order of b_i and suppose that the b_i are arranged such that $k = k_1 \geqq k_2 \geqq \cdots \geqq k_n > 0$. Let $a \in R$, $b_i a \in R$ $i = 1, \cdots, n$ so we may write

$$b_i a = \sum_{j=1}^{n} \alpha_{ij} b_j \quad \alpha_{ij} \in G_{k,r} i = 1, \cdots, n .$$

Note that

$$0 = p^{k_i} b_i a = \sum_{j=1}^{n} p^{k_i} \alpha_{ij} b_j \quad \text{for all} \quad i = 1, \cdots, n .$$

Since the b_j's are independent over $G_{k,r}$ we conclude that $p^{k_i}\alpha_{ij} b_j = 0$ for all $i, j = 1, \cdots, n$. Thus $p^{k_i}\alpha_{ij}$ is a multiple of p^{k_j}. So if $i > j$ we have that α_{ij} is a multiple of $p^{k_j - k_i}$ for all $a \in R$. So the map ψ given by $\psi: a \to [(\alpha_{ij})\phi_j]$ is a map from R into a ring of Szele matrices. It is straightforward to check that ψ is a ring homomorphism and since k_j is the order of b_i it follows that ψ is one to one, and the lemma is proved.

3. Completely primary and nilpotent finite rings. In [5], the author proves that a completely primary (resp. nilpotent) finite ring is isomorphic to a subring of a homomorphic image of a ring of matrices which are upper triangular (resp. strictly upper triangular) modulo p. We now characterize this homomorphic image by means of the Szele representation over Galois rings.

THEOREM 3.1. *Let R be a completely primary finite ring of characteristic p^k with radical J such that $R/J \cong GF(p^r)$. Then R is isomorphic to a ring of Szele matrices over $G_{k,r}$ in which every matrix is upper triangular modulo p, and if the matrix $[(a_{ij})\phi_j]$*

$(a_{ij} \in G_{k,r})$ is in this ring then there are automorphisms $\sigma_2, \cdots, \sigma_n$ of $GF(p^r)$ such that $(a_{jj})\phi_1 = ((a_{11})\phi_1)\sigma_j$ (i.e., *the main diagonal entries of the matrices are all related by automorphisms modulo p*).

The converse is also true. Any such ring is completely primary, so this result characterizes completely primary finite rings.

Proof. We first note that if a completely primary ring has an representation as a ring of Szele matrices which is upper triangular modulo p then the main diagonal entries must be related by automorphisms modulo p. For then the radical of the ring is the set of all matrices in the ring which are strictly upper triangular modulo p so the map $R \longrightarrow R/J \cong GF(p^r)$ can be realized by the map

$$\begin{bmatrix} (a_{11})\phi_k & \cdots & (a_{1n})\phi_{k_n} \\ \vdots & & \vdots \\ (a_{n1})\phi_k & \cdots & (a_{nn})\phi_{k_n} \end{bmatrix} \longrightarrow ((a_{11})\phi_1, \cdots, (a_{nn})\phi_1) \in GF(p^r) \oplus \cdots \oplus GF(p^r) .$$

However, the image of this map is a one dimensional algebra over $GF(p^r)$ so the entry $(a_{jj})\phi_1$ is uniquely determined by the value of $(a_{11})\phi_1$; i.e., $(a_{jj})\phi_1$ is a function of $(a_{11})\phi_1$ say $(a_{jj})\phi_1 = ((a_{11})\phi_1)\sigma_j$ for some function σ_j $j = 2, \cdots, n$. The σ_j are seen to be homomorphisms from $GF(p^r)$ to $GF(p^r)$ and that part of the result follows. For the rest of the result, the particular matrix representation we choose depends upon the choice of independent generating set we make for R over $G_{k,r}$. For R completely primary as in the hypothesis of the theorem, the author showed [5, Prop. 2.2] that in addition to conditions (i) and (ii) of Proposition 1.2 we can also assume (iii) $b_1 = 1$, and $b_2, \cdots, b_n \in J$.

We now 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 (i), (ii), and (iii). Suppose that q_1 is the maximum number of elements of any of these generating sets which are in J^{e-1}. Say $\{1, b_2, \cdots, b_{q_1+1}, c_{q_1+2}, \cdots, c_n\}$ is such a generating set with $b_2, \cdots, b_{q_1+1} \in J^{e-1}$. Suppose q_2 is the maximum number of elements in J^{e-2} included in any set of the form $\{1, b_2, \cdots, b_{q_1+1}, c_{q_1+2}, \cdots, c_n\}$ which satisfies the conditions (i), (ii), and (iii). Choose a generating set $\{1, b_2, \cdots, b_{q_1+1}, b_{q_1+2}, \cdots, b_{q_1+q_2+1}, \cdots, d_n\}$ with $b_{q_1+1}, \cdots, b_{q_1+q_2+1} \in J^{e-2}$. We continue choosing elements of our generating set in this way: At the ith step we have already chosen $1, b_2, \cdots, b_{q_{i-1}+\cdots+q_1+1}$ and we suppose that the maximum number of elements in J^{e-i} in any generating set satisfying (i), (ii), and (iii) which includes all of the above elements 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 (i), (ii),

and (iii) which also contain the elements we have chosen in the previous steps. 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 $1, b_2, \cdots, b_n$ is a generating set satisfying the conditions (i), (ii), and (iii). Also, this matrix representation depends on the order in which we index the b_i. We take $b_1 = 1$. We then assume that if k_i is the order of b_i that $k = k_1 \geqq k_2 \geqq \cdots \geqq k_n$. Next let f_i be the largest positive integer such that $b_i \in J^{f_i}$. We call f_i the radical index of b_i. We shall further assume that if $k_i = k_j$ with $i \geqq j$ then $f_i \geqq f_j$. We prove that the Szele representation of R with respect to this ordering of the basis $b_1, \cdots, b_n$ of R is of the desired type.

Again let $a \in R$ and write $b_i a = \sum_{j=1}^n \alpha_{ij} b_j$. Since we have that $k = k_1 \geqq k_2 \geqq \cdots \geqq k_n$ we already know that if $i > j$ with $k_i < k_j$ then α_{ij} is a multiple of $p^{k_j - k_i}$. So we need only restrict our attention to those i, j such that $i > j$ but $k_i = k_j$. Let us express $a = \sum_{q=1}^n g_q b_q (g_q \in G_{k,r} q = 1, \cdots, n)$. Then $b_i a = \sum_{q=1}^n b_i g_q b_q$. But by (ii), $b_i G_{k,r} = G_{k,r} b_i (i = 1, \cdots, n)$ so $b_i g_q \in G_{k,r} b_i$. Let $b_i g_q = g_q^{(i)} b_i$. Then $b_i a = \sum_{q=1}^n g_q^{(i)} b_i b_q$. Next let

$$b_i b_q = \sum_{j=1}^n \gamma_{ij}^{(q)} b_j \quad \gamma_{ij}^{(q)} \in G_{k,r} \qquad i, j, q = 1, \cdots, n$$

then

$$b_i a = \sum_{j=1}^n \left(\sum_{q=1}^n g_q^{(i)} \gamma_{ij}^{(q)} \right) b_j .$$

From this we conclude $(\alpha_{ij})\phi_j$, the i, jth entry of the Szele representation of a is $(\sum_{q=1}^n g_q^{(i)} \gamma_{ij}^{(q)})\phi_j$. Thus if we seek to show that for an arbitrary $(\alpha_{ij})\phi_j$ is a multiple of p for some i, j it suffices to show that $\gamma_{ij}^{(q)}$ is a multiple of q for each $q = 1, \cdots, n$.

We have thus reduced the problem to showing that if $i > j$ with $k_i = k_j$ then $\gamma_{ij}^{(q)}$ is a multiple of p for each $q = 1, \cdots, n$. 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 $q = 2, \cdots, n$ $\gamma_{ij}^{(q)}$ 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 seek a contradiction. Since $q \geqq 2$, $b_q \in J$ so the radical index of $b_i b_q$ is strictly greater than f_i which is the radical index of b_i which is, by hypothesis, greater than or equal to the radical index of γ_j. So from the construction of the generating set $1, b_2, \cdots, b_m$ of R over $G_{k,r}$ we will have our contradiction if we can show that $1, b_2, \cdots, b_{j-1}, b_i b_q, \cdots, b_m$ is a generating set of R over $G_{k,r}$ satisfying the conditions (i), (ii), and (iii).

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

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 $p^{k_j}(b_ib_q) = p^{k_i}(b_ib_q) = 0$ so that order of b_ib_q is less than or equal to k_j. However, $\gamma_{ij}^{(q)}$ is not a multiple of p and so we conclude that $p^s b_ib_q = \sum_{t=1}^{m} \gamma_{it}^{(q)} p^s b_t \neq 0$ if $s < k_j$ and thus the order of b_ib_q is the order of b_j. Now since $1, b_2, \cdots, b_{j-1}, b_ib_q, b_{j+1}, \cdots, b_m$ is a generating set the map from the external direct sum

$$\sum_{t=1}^{i-1} \oplus G_{k,r}b_t \oplus G_{k,r}b_ib_q \oplus \sum_{t=j+1}^{m} \oplus G_{k,r}b_t$$

to R given by

$$(g_1, g_2b_2, \cdots, g_{j-1}b_{j-1}, g_jb_ib_q, g_{j+1}b_{j+1}, \cdots, g_mb_m)$$
$$\longrightarrow \sum_{t=1}^{j-1} g_tb_t + g_jb_ib_q + \sum_{t=j+1}^{m} g_tb_t$$

is onto. But as the order of b_ib_q is k_j we conclude that

$$\#\left(\sum_{t=1}^{j-1} \oplus G_{k,r}b_t \oplus G_{k,r}b_ib_q \oplus \sum_{t=j+1}^{m} G_{k,r}b_t\right) = \#R$$

which is equivalent to saying that $1, b_2, \cdots, b_{j-1}, b_ib_q, b_{j+1}, \cdots, b_m$ 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 $b_qg = g'b_q$. Similarly, given g' there exists a $g'' \in G_{k,r}$ such that $b_ig' = g''b_i$. Hence, $(b_ib_q)g = g''(b_ib_q)$ and we conclude that $G_{k,r}b_ib_q$ is a $(G_{k,r}, G_{k,r})$-submodule of R and, therefore, $1, b_2, \cdots, b_{j-1}, b_ib_q, b_{j+1}, \cdots, b_m$ satisfies the conditions of (i), (ii), and (iii) and the proof is complete.

As a result we obtain the following classification of finite nilpotent rings (of prime power order).

THEOREM 3.2. *Let R be a finite nilpotent ring of characteristic p^k. Then R is isomorphic to a ring of Szele matrices (over $Z/(p)^k$ which are all strictly upper triangular modulo p.*

Proof. 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 into a ring with 1 over $Z/(p^k)$. $\bar{R}$ is completely primary because the nonunits of $\bar{R}$ are the elements of $pZ/(p^k) + R$ and hence form and ideal J with $R \subset J$. $\bar{R}$ J. $\bar{R}/J \cong Z(p^k)$. We apply Theorem 3.1 to obtain Szele representation of $\bar{R}$ which is upper triangular modulo p. The radical of $\bar{R}$ will be contained in the set of Szele matrices which are strictly upper traiangular modulo p and the result follows.

REMARK 3.3. In [4] Szele reduced the problem of classifying nilpotent Artinian rings to the problem of classifying finite nilpotent rings of prime power order by showing that any nilpotent Artinian ring is a direct sum or a particular type of extension of a finite nilpotent ring of prime power order by a direct sum of null rings over quasi-cycle groups. Thus Theorem 3.2 yields a classification of nilpotent Artinian rings which can by easily recovered by anyone with a knowledge of the results in [4].

REMARK 3.4. The question can be asked as to whether the author's previous representations [5] of completely primary and nilpotent finite rings are in fact the preimages under the map Φ defined in § 2 of the Szele representation. The answer is no. Although the same generating sets were used in both representations (although they were ordered slightly differently) the author's previous representation is essentially the homological dual of the preimage of the Szele representation.

NOTE. The author would like to acknowledge a helpful remark by Professor K. R. McLean concerning Remark 3.3.

REFERENCES

1. G. J. Janusz, *Separable algebras over commutative rings*, Trans. Amer. Math. Soc., **122** (1966), 461-479.
2. R. Raghavendran, *Finite associative rings*, Compositio Math., **21** (1969), 195-229.
3. T. Szele, *Ein Satz über die Struktur der endlichen Ringe*, Acta Sci. Math., (Szeged) **11** (1948), 246-250.
4. ———, *Nilpotent Artinian rings*, Publ. Math. Debrecen, **4** (1955), 71-78.
5. R. S. Wilson, *On the structure of finite rings*, Compositio Math., **26** (1973), 79-93.

Received May 8, 1973 and in revised form July 15, 1973.

UNIVERSITY OF TEXAS