

THE INTEGRAL REPRESENTATION RING $a(R_k G)$

BY

T. A. HANNULA⁽¹⁾

0. Notation.

p = an odd prime.

G = cyclic group of order p with generator g .

R = a commutative ring with identity 1, in which the principal ideal $(p \cdot 1)$ is a nonzero maximal ideal.

$R_k = R/(p^k)$, using only those k for which $(p^k) \neq (p^{k-1})$.

$\mathfrak{M} = \{M \mid M = R_k\text{-free } R_k G\text{-module of finite } R_k\text{-rank}\}$.

$[M:R_k] = R_k\text{-rank of } M = \text{number of elements in an } R_k\text{-basis of } M$.

$I_n = n \times n$ identity matrix.

1. The integral representation ring $a(R_k G)$. The *integral representation ring* $a(R_k G)$ (see Reiner [6]) is generated by the symbols $[M]$, one for each isomorphism class of modules in \mathfrak{M} , subject to the relations

$$(1.1) \quad [M] + [M'] = [M \oplus M'] \quad \text{and} \quad [M][M'] = [M \otimes_{R_k} M'],$$

where $M \otimes M'$ is the $R_k G$ -module with $g(m \otimes m') = gm \otimes gm'$. We note that $a(R_k G)$ is a commutative ring with identity $[R_k]$, R_k the trivial $R_k G$ -module. The Krull-Schmidt theorem holds for elements of \mathfrak{M} , so $a(R_k G)$ is a free \mathbb{Z} -module with \mathbb{Z} -basis the nonisomorphic indecomposable elements of \mathfrak{M} .

J. A. Green [2] has investigated $a(R_k G)$ when $k=1$ and G is a cyclic p -group. Some of his results have been simplified in [4]. We will, therefore, assume that $k > 1$ and also that p is odd, unless otherwise stated.

The indecomposable modules in \mathfrak{M} have been determined in [1], for $k > 1$ and p an odd prime, when R is the ring of integers \mathbb{Z} . In this case, the study of these modules is equivalent to the study of the representations of G by matrices over \mathbb{Z}_k . Similar results for the general case have been obtained in [3] by somewhat different methods. We collect these results for later use in this paper.

Since $R_1 = R/(p)$ is a field of characteristic p , and G is a cyclic group of order p , there are exactly p nonisomorphic indecomposable $R_1 G$ -modules, namely the modules $S_i = R_1[x]/(x-1)^i$ for $i=1, 2, \dots, p$, with g acting on S_i as multiplication by x . For each $M \in \mathfrak{M}$, define \bar{M} to be the $R_1 G$ -module M/pM ; then we have from [1] and [3]:

Received by the editors May 19, 1967.

⁽¹⁾ This paper is based on the author's Ph.D thesis written under the supervision of Professor Irving Reiner at the University of Illinois.

(1.2) Every $M \in \mathfrak{M}$ has the form $M = M_1 \oplus M_{p-1} \oplus M_p$, where M_i is an $R_k G$ -module with \bar{M}_i a direct sum of copies of S_i , $i = 1, p-1, p$.

In the sequel we shall refer to such a module M_i as a T_i -module. From (1.2) it follows that a basis of $a(R_k G)$ will be known once the indecomposable T_i -modules are classified to within isomorphism for $i = 1, p-1$, and p . Again from [1] and [3] we have

(1.3) $R_k G$ is an indecomposable $R_k G$ -module, and each T_p -module is a free $R_k G$ -module.

Further,

(1.4) A T_1 -module M affords a matrix representation $g \rightarrow I_n + p^{k-1}B$, where B is an $n \times n$ matrix over R_k . Here, $n = [M : R_k]$.

Thus each T_1 -module M has the property that $(g-1)M \subseteq p^{k-1}M$.

Let \bar{B} be the result of reducing the entries of B modulo p ; then one can easily show that

(1.5) Two T_1 -modules M_1 and M_2 are isomorphic if and only if \bar{B}_1 and \bar{B}_2 are similar over the field R_1 .

(1.6) A T_1 -module M is indecomposable if and only if \bar{B} is indecomposable under similarity transformations.

The T_{p-1} -modules have been classified in [1] and [3] as follows:

(1.7) Let $A = (g-1)R_k G =$ augmentation ideal in $R_k G$. Then

(i) M is a T_{p-1} -module if and only if there exists a T_1 -module N such that $M \cong N \otimes A$.

(ii) For T_1 -modules N_1 and N_2 , $N_1 \otimes A \cong N_2 \otimes A$ if and only if $N_1 \cong N_2$.

(iii) The T_{p-1} -module $N \otimes A$ is indecomposable if and only if the T_1 -module N is indecomposable.

II. Multiplication in $a(R_k G)$. From (1.2) it follows that as a Z -module,

$$a(R_k G) = a(T_1) \oplus a(T_{p-1}) \oplus a(T_p),$$

where $a(T_i)$ has as Z -basis the indecomposable T_i -modules. Clearly $a(T_1)$ is a subring of $a(R_k G)$. For any $M \in \mathfrak{M}$ with R_k -basis $\{m_i\}$, the set $\{g^j \otimes g^j m_i\}$ is an R_k -basis for $R_k G \otimes M$. Hence $R_k G \otimes M = \sum^\oplus R_k G(1 \otimes m_i)$, and thus is $R_k G$ -free. It follows that $a(T_p)$ is an ideal and, by (1.3), $a(T_p) = Z\alpha_p$, where $\alpha_p = [R_k G]$. Let $\alpha_{p-1} = [A]$; then by (1.7) $a(T_{p-1}) = a(T_1)\alpha_{p-1}$. Further, it is well known that

$$(2.0) \quad \alpha_{p-1}^2 = 1 + (p-2)\alpha_p.$$

It now follows that multiplication in $a(R_k G)$ will be determined by that in $a(T_1)$. In order to investigate multiplication in $a(T_1)$, we replace $a(T_1)$ by the representation ring $a(R_1[x])$. This is generated by the symbols $[V]$, one for each isomorphism class of $R_1[x]$ -modules with finite R_1 -basis, subject to the relations

$$(2.1) \quad [V] + [V'] = [V \oplus V'] \quad \text{and} \quad [V][V'] = [V \otimes_{R_1} V'],$$

where $V \otimes V'$ is an $R_1[x]$ -module with x acting as $x \otimes 1 + 1 \otimes x$.

To see that $a(T_1) \cong a(R_1[x])$, define a mapping $\beta: a(T_1) \rightarrow a(R_1[x])$ by $\beta([N]) = [V]$, where N affords the representation $g \rightarrow I + p^{k-1}B$, and V is an $R_1[x]$ -module for which the linear transformation "multiplication by x " is represented by \bar{B} relative to some R_1 -basis. It is clear from (1.4), (1.5), and the well-known facts about $R_1[x]$ -modules, that β is an isomorphism between the additive groups of $a(T_1)$ and $a(R_1[x])$. If $g \rightarrow I + p^{k-1}B_i$ is a representation of G afforded by N_i , $i=1, 2$, then since $k > 1$, $g \rightarrow I + p^{k-1}(B_1 \otimes I + I \otimes B_2)$ is a representation of G afforded by $N_1 \otimes N_2$. Hence β preserves multiplication.

For convenience, denote $R_1[x]/(f(x))^r$ by $R_1(f, r)$. Thus to determine multiplication in $a(R_1[x])$, we need only find the decomposition of $W = R_1(f, r) \otimes_{R_1} R_1(g, s)$. Moreover, we may assume that $R_1(f, r)$ and $R_1(g, s)$ are indecomposable, and thus that $f(x)$ and $g(x)$ are irreducible over R_1 . Letting Ω be an algebraic closure of R_1 , we have

$$(2.2) \quad \Omega \otimes_{R_1} W \cong \sum_{i,j}^{\oplus} \Omega(\alpha_i, p^i r) \otimes \Omega(\beta_j, p^j s),$$

where $f(x) = \prod (x - \alpha_i)^{p^i}$ and $g(x) = \prod (x - \beta_j)^{p^j}$ in $\Omega[x]$, and $\Omega(\gamma, m) = \Omega[x]/(x - \gamma)^m$.

Let $N_m = m \times m$ matrix with 1's immediately below the main diagonal and 0's everywhere else, $B(m, n) = (\lambda I_m + N_m)^n$, λ an indeterminate over Ω , and $\{\lambda^{d_n}\}$, the set of nonunit invariant factors of $B(m, n)$. Then the decomposition of (2.2) into indecomposable factors is obtained by means of

(2.3) LEMMA. *The $\Omega[x]$ -module $\Omega(\alpha, m) \otimes \Omega(\beta, n)$, with x acting as $x \otimes 1 + 1 \otimes x$, has the decomposition*

$$(2.3.1) \quad \Omega(\alpha, m) \otimes \Omega(\beta, n) = \sum_n^{\oplus} \Omega(\alpha + \beta, d_n).$$

Moreover, there are $\min(m, n)$ summands on the right side of (2.3.1).

Proof. Relative to suitable Ω -bases, the action of x on $\Omega(\alpha, m)$ and $\Omega(\beta, n)$ is given by the matrices $\alpha I_m + N_m$ and $\beta I_n + N_n$, respectively. Thus the action of x on $\Omega(\alpha, m) \otimes \Omega(\beta, n)$ is given by the matrix

$$\begin{aligned} Y(m, n) &= (\alpha I_m + N_m) \otimes I_n + I_m \otimes (\beta I_n + N_n) \\ &= ((\alpha + \beta)I_m + N_m) \otimes I_n + I_m \otimes N_n. \end{aligned}$$

The Jordan canonical form of $Y(m, n)$ is determined by the invariant factors of $Y(m, n) - zI_{mn}$ as a matrix over $\Omega[z]$, z an indeterminate over Ω . Use the definition $A \otimes B = (A b_{ij})$, and let $\lambda = \alpha + \beta - z$. An easy induction shows that $Y(m, n) - zI$ is equivalent to the matrix

$$\begin{bmatrix} I_{m(n-1)} & 0 \\ 0 & B(m, n) \end{bmatrix},$$

where $B(m, n) = (\lambda I_m + N_m)^n$.

Since $\det(B(m, n)) = \lambda^{mn}$, each invariant factor of $B(m, n)$ is of the form λ^{d_i} for some nonnegative integer d_i . Thus the Jordan canonical form of $Y(m, n)$ is

$$\sum_h^{\oplus} ((\alpha + \beta)J_{d_h} + N_{d_h}),$$

where the sum is over those h for which $d_h > 0$. Thus

$$\Omega(\alpha, m) \otimes \Omega(\beta, n) = \sum_{d_h > 0}^{\oplus} \Omega(\alpha + \beta, d_h).$$

Since \otimes is commutative, we may assume $m \leq n$. Moreover, since $(N_m)^m = 0$, the binomial expansion of $(\lambda I_m + N_m)^n$ shows that $(\lambda I_m + N_m)^n$ is a multiple of λ . Hence all the invariant factors are multiples of λ . Thus there are $m = \min(m, n)$ summands on the right side of (2.3.1).

We refer the reader to papers by Green [3], Ralley [5], and Srinivasan [7] for methods of determining these invariant factors.

Now let V be an $R_1[x]$ -module with finite R_1 -basis, and suppose that

$$(2.4.1) \quad \Omega \otimes V \cong \sum_{\alpha, t}^{\oplus} n(\alpha, t)\Omega(\alpha, t),$$

with $n(\alpha, t)\Omega(\alpha, t)$ denoting a direct sum of $n(\alpha, t)$ copies of $\Omega(\alpha, t)$. Further, let

$$(2.4.2) \quad V = \sum_{q, s}^{\oplus} n(q, s)R_1(q, s),$$

with $q(x)$ irreducible, $q(x) = \prod (x - \alpha_q)^{p^{e(q)}}$, with α_q ranging over the distinct roots of $q(x)$. It follows that

$$(2.4.3) \quad \Omega \otimes V = \sum_{q, s, \alpha_q}^{\oplus} n(q, s)\Omega(\alpha_q, p^{e(q)}s).$$

On comparing (2.4.1) and (2.4.3), we have:

(2.4) LEMMA. *If a decomposition for $\Omega \otimes V$ is given by (2.4.1) and one for V by (2.4.2), then*

$$(2.4.4) \quad \begin{aligned} n(q, s) &= n(\alpha, t), & \text{when } q(x) &= \text{Irr}(\alpha, R_1) \text{ and } t = p^{e(q)}s, \\ n(\alpha, t) &= 0, & \text{when } q(x) &= \text{Irr}(\alpha, R_1) \text{ and } t \neq p^{e(q)}s. \end{aligned}$$

Now let $f(x) = \prod (x - \alpha_i)^{p^i}$, $\alpha_i \in \Omega$, α_i distinct; $g(x) = \prod (x - \beta_j)^{p^j}$, $\beta_j \in \Omega$, β_j distinct; $C = \{\alpha_i + \beta_j\}$; $\{\lambda^{d_h}\}$ = set of invariant factors of $B(p^t r, p^u s)$; $\{q_k(x)\}$ = set of distinct irreducible polynomials over R_1 of the elements in C ; $p^{e(k)}$ = degree of inseparability of $q_k(x)$ over R_1 ; and $n(\gamma)$ = number of pairs (α_i, β_j) such that $\gamma = \alpha_i + \beta_j$.

(2.5) THEOREM. *With the above notation, $n(\gamma) = n(\gamma')$ whenever γ and γ' are conjugate over R_1 . If we let $n_k = n(\gamma)$ for any root γ of $q_k(x)$, then*

$$(2.5.1) \quad R_1(f, r) \otimes R_1(g, s) \cong \sum_{h,k} n_k R_1(q_k, d_h/p^{e(k)}).$$

Proof. We have

$$(2.5.2) \quad \Omega \otimes (R_1(f, r) \otimes R_1(g, s)) \cong \sum_{i,j}^{\oplus} \Omega(\alpha_i, p^i r) \otimes \Omega(\beta_j, p^j s).$$

Hence by Lemma 2.3,

$$(2.5.3) \quad \Omega \otimes (R_1(f, r) \otimes R_1(g, s)) \cong \sum_{i,j,h}^{\oplus} \Omega(\alpha_i + \beta_j, d_h).$$

Collecting like terms yields

$$(2.5.4) \quad \Omega \otimes (R_1(f, r) \otimes R_1(g, s)) \cong \sum_{\gamma \in C}^{\oplus} \sum_h^{\oplus} n(\gamma) \Omega(\gamma, d_h).$$

By Lemma 2.4, we know that the number of times $\Omega(\gamma, d_h)$ occurs is the same for each γ such that $q_k(\gamma) = 0$. This is $n(\gamma)m_h$, where m_h is the number of times d_h occurs as an invariant factor of $B(p^i r, p^j s)$. Thus $n(\gamma)$ is constant, say n_k , for each root γ of $q_k(x)$. Applying Lemma 2.4, we find that (2.5.1) holds.

(2.6) COROLLARY. *If $f(x)$ and $g(x)$ are separable over R_1 , then*

- (1) $\prod_{i,j} (x - (\alpha_i + \beta_j)) = \prod_k q_k^{n_k}(x)$,
- (2) $R_1(f, r) \otimes R_1(g, s) \cong \sum_{k,h} n_k R_1(q_k, d_h)$.

Proof. (1) follows immediately from the hypothesis, and (2) then follows from the theorem.

III. Nilpotent elements in $a(R_kG)$. We now turn our attention to the possible existence of nilpotent elements in $a(R_kG)$. Recall that an element r of a ring is nilpotent if there exists a positive integer n such that $r^n = 0$.

(3.1) THEOREM. *If $a(R_kG)$ has a nonzero nilpotent element, then so does $a(T_1)$.*

Proof. If $a(R_kG)$ has nonzero nilpotents, then there exists a $z \in a(R_kG)$ such that $z \neq 0$, but $z^2 = 0$. Let $z = z_1 + z_{p-1} + z_p$, $z_i \in a(T_i)$. Moreover, $z_{p-1} = z'_1 \cdot \alpha_{p-1}$ for some $z'_1 \in a(T_1)$, and $z_p = n\alpha_p$ for some integer n . Using (2.0), we have

$$(3.1.1) \quad 0 = z_1^2 + (z'_1)^2 + (p-2)(z'_1)^2 \alpha_p + z_p^2 + 2z_1 z'_1 \alpha_{p-1} + 2z_1 z_p + 2z_{p-1} z_p.$$

It follows from (3.1.1), and results in §I, that

$$(3.1.2) \quad z_1^2 + (z'_1)^2 = 0, \quad 2z_1 z'_1 \alpha_{p-1} = 0.$$

Again using (2.0), we obtain $2z_1 z'_1 + 2(p-2)z_1 z'_1 \alpha_p = 0$. Thus $z_1 z'_1 = 0$. It now follows from (3.1.2) that $z_1^2 = 0$ and $(z'_1)^2 = 0$. Therefore, if $a(T_1)$ has no nonzero nilpotent

elements, then $z_1=0$ and $z'_1=0$. Hence $z=nz_p$. But $z^2=0$, so $n=0$. Thus $z=0$, contrary to assumption.

We now replace $a(T_1)$ by $a(R_1[x])$ and embed $a(R_1[x])$ in $a(\Omega[x])$ by identifying $[V]$ with $[\Omega \otimes V]$.

If $v \in a(\Omega[x])$, then $v = \sum_{\alpha,r} n(\alpha, r)v(\alpha, r)$, $n(\alpha, r) \in Z$, and $v(\alpha, r) = [\Omega[x]/(x - \alpha)^r]$. If $n(\alpha, r) \neq 0$ for some r , call α a root of v . Let $H(v)$ be the additive subgroup of Ω generated by the roots of v . Then we may write $H(v) = \Omega_0 u_1 + \dots + \Omega_0 u_t$, Ω_0 = prime subfield of Ω . If $H(v) \neq 0$, define $H'(v) = \sum_{i < t} \Omega_0 u_i$ and $w = [\Omega[x]/(x - u_t)]$. Using Lemma 2.3, we see that $w^p = [\Omega[x]/(x)]$, the multiplicative identity of $a(\Omega[x])$. (Recall that x acts as $x \otimes 1 + 1 \otimes x$ on a tensor product.) Further, each $\alpha \in H(v)$ has the form $\alpha = h' + iu_t$ for some $h' \in H'(v)$ and some i , $0 \leq i \leq p-1$. It follows that $v(\alpha, r) = w^i v(h', r)$. Using this factorization, and collecting like powers of w , we have

$$v = v_0 + wv_1 + \dots + w^{p-1}v_{p-1},$$

with each v_i having all its roots in $H'(v)$. It is clear that $v=0$ if and only if each $v_i=0$.

Let C denote the field of complex numbers and let $A(\Omega[x]) = C \otimes_Z a(\Omega[x])$. Obviously $a(\Omega[x])$ can be embedded in $A(\Omega[x])$. Let ρ be any complex p th root of 1 and let $v(\rho) = v_0 + \rho wv_1 + \rho^2 w^2 v_2 + \dots + \rho^{p-1} w^{p-1} v_{p-1}$. It is clear that if $v^n = \sum_{i=0}^{p-1} w^i v_i^n$, then $(v(\rho))^n = \sum_{i=0}^{p-1} (\rho w)^i v_i^n$. It thus follows that

(3.2) LEMMA. *If v is nilpotent in $a(\Omega[x])$, then for any p th-root of unity ρ in C , $v(\rho)$ is nilpotent in $A(\Omega[x])$.*

(3.3) THEOREM. *If $v \in a(\Omega[x])$ and $v \neq 0$, then v is not nilpotent.*

Proof. We proceed by induction on the rank t of $H(v)$. If $t=0$, then $v = \sum a_r v(o, r)$ with $a_r \in Z$ and $v(o, r) = [\Omega[x]/x^r]$. By Lemma 2.3, we know that $v(o, r)v(o, s) = \sum_t b_{rst} v(o, t)$, with each b_{rst} a nonnegative integer, and $\sum_t b_{rst} = \min(r, s)$. Thus $v^2 = \sum_{r,s} a_r a_s v(o, r)v(o, s) = \sum_{r,s,t} a_r a_s b_{rst} v(o, t)$. If $v^2=0$, then for each t , $\sum_{r,s} a_r a_s b_{rst} = 0$. Summing on t , we obtain $\sum_{r,s} a_r a_s \min(r, s) = 0$. If n is an integer such that $a_m = 0$ for all $m > n$, we find that

$$0 = \sum_{r=1}^n \sum_{s=1}^n a_r a_s \min(r, s) = \left(\sum_{i=1}^n a_i \right)^2 + \left(\sum_{i=2}^n a_i \right)^2 + \dots + a_n^2.$$

Hence each $a_r = 0$ and thus $v=0$.

Let $t \geq 1$, and now assume that whenever the rank of $H(v_0)$ is less than t and $v_0 \neq 0$, then v_0 is not nilpotent. Let $v \in a(\Omega[x])$, $v \neq 0$, and let the rank of $H(v)$ be t . Replacing v by $w^i v$ for some i , $0 \leq i \leq p-1$, we may assume that

$$v = v_0 + wv_1 + \dots + w^{p-1}v_{p-1}$$

with roots of each v_i in $H'(v)$ and $v_0 \neq 0$. By the induction assumption v_0 is not nilpotent. If v is nilpotent and ρ is a primitive p th root of 1 in C , then $\sum_{j=0}^{p-1} v(\rho^j)$ is

nilpotent in $A(\Omega[x])$, since $A(\Omega[x])$ is commutative and each $v(\rho^j)$ is nilpotent by Lemma 3.2. But

$$\begin{aligned} \sum_{j=0}^{p-1} v(\rho^j) &= v + v(\rho) + \cdots + v(\rho^{p-1}) \\ &= \sum (w^i v_i) + \sum (\rho w)^i v_i + \cdots + \sum (\rho^{p-1} w)^i v_i \\ &= \beta_0 v_0 + \beta_1 w v_1 + \cdots + \beta_{p-1} w^{p-1} v_{p-1} \end{aligned}$$

where $\beta_i = \sum_{j=0}^{p-1} (\rho^j)^i$ for each i , $0 \leq i \leq p-1$. Since $\beta_0 = p$ and $\beta_i = 0$ for $1 \leq i \leq p-1$, we see that $p v_0$ is nilpotent. But $H(p v_0) \subseteq H'(v)$, thus $p v_0 = 0$ by the induction assumption. But in this case $v_0 = 0$, which contradicts v_0 being nonzero. Thus v cannot be nilpotent and the induction step is completed.

(3.4) COROLLARY. *The ring $a(R_1[x])$ has no nonzero nilpotent elements, whence neither does $a(T_1)$.*

(3.5) COROLLARY. *The ring $a(R_k G)$ has no nonzero nilpotent elements.*

REFERENCES

1. V. S. Drobotenko, E. S. Drobotenko, Z. P. Zhilinskaya and E. V. Pogorilyak, *Representations of cyclic groups of prime order p over rings of residue classes mod p^s* , Ukrain. Mat. Ž. 17 (1965), 28–42.
2. J. A. Green, *The modular representation algebra of a finite group*, Illinois J. Math. 6 (1962), 607–619.
3. T. A. Hannula, *Group representations over integers modulo a prime power*, Ph.D Thesis, Univ. of Illinois, Urbana, 1967.
4. T. A. Hannula, T. G. Ralley and I. Reiner, *Modular representation algebras*, Bull. Amer. Math. Soc. 73 (1967), 100–101.
5. T. G. Ralley, *Decomposition of products of modular representations*, Bull. Amer. Math. Soc. 72 (1966), 1012–1013.
6. I. Reiner, *The integral representation ring of a finite group*, Michigan Math. J. 12 (1965), 11–22.
7. B. Srinivasan, *The modular representation ring of a cyclic p -group*, Proc. London Math. Soc. (3) 14 (1964), 677–688.

UNIVERSITY OF MAINE,
ORONO, MAINE