ON REPRESENTATIONS OF FINITE GROUPS OVER VALUATION RINGS

BY

ALFREDO JONES[1]

Let G be a finite group. Given a ring R, by RG we denote the group ring of G with coefficients in R. By an RG-module M we understand a left RG-module M that has a finite basis over R. Thus the RG-modules afford the representations of G by matrices with entries in R. If R' is a ring extension of R we write $R' \otimes M$ to denote $R' \otimes_R M$, and if G is a subgroup of H we let $M^H = RH \otimes_{RG} M$. Given a prime p let Z_p be the ring of p integral rationals and Q^*, with valuation ring Z^*, the p-adic completion of the rationals, Q.

In this note we study the representations of a finite group G over Z_p. If p is prime to the order of G, it is known that every representation of G over Z_p is a unique direct sum of indecomposable representations, and that the indecomposables are the Q-irreducible representations of G (see [2]). In the present paper we wish to consider the case when p divides the order of G.

In the first section we show that, if G is cyclic of order p and ξ is a root of unity of order prime to p, then the representations of G over $Z_p[\xi]$ can be determined by extending the method used by Reiner to study the rational integral representations of this group (see [2]). With this result it is possible to construct the representations over Z_p of any commutative group with a p-Sylow subgroup of order p.

In Section 2 we consider the problem of the uniqueness of the decomposition into indecomposables. We say that the Krull-Schmidt Theorem holds for RG-modules if in any decomposition of an RG-module into a direct sum of indecomposable submodules the indecomposable summands are uniquely determined up to RG-ismorphism. It is known that the Krull-Schmidt Theorem holds for $Z^* G$-modules for every finite group G (see [2]). In [4] Reiner raised the question of whether the theorem holds for $Z_p G$-modules. This was answered by Berman and Gudivok [1] who gave an example of a cyclic group for which the theorem fails.[2] In Theorem 2 of the present paper we prove that for G abelian, if p divides the order of G, then the Krull-Schmidt Theorem holds for $Z_p G$-modules if and only if the indecomposable representations of G over Z_p are indecomposable over Z^*, and that this is equivalent to a condition on the exponent of G. It is shown that this condition is also sufficient for the Krull-Schmidt Theorem to hold when G is a nilpotent group of odd order. This section is essentially independent of the first one, but some representations introduced in Section 1 are used in the proof of Theorem 2.

Received December 21, 1963.

[1] This research was partially supported by the U. S. Army Research Office.

[2] The author is grateful to Professor Berman for communicating this example to him.

1. In this section we use the following notation. θ denotes a root of unity of prime order p, and ξ a root of unity of order q, prime to p. Let $S = Z_p[\xi]$, and $R = S[\theta]$. If s is the order of p in the integers modulo q, Φ the Euler function, and $h = \Phi(q)/s$, then there are h primes $\delta_1, \cdots, \delta_h$ in R, such that $R\delta_i \neq R\delta_j$ for $i \neq j$, $\delta_1 \cdots \delta_h = \theta - 1$, and $R(\theta - 1)^{p-1} = Rp$. nS denotes the direct sum of n copies of S.

Let G be a cyclic group of order p, and g a generator of G. S can be considered as an SG-module by letting $gc = c$ for all $c \in S$. R becomes an SG-module if we define $g\alpha = \theta\alpha$ for all $\alpha \in R$. Now let $\gamma \in R$, $\gamma \mid (\theta - 1)$, $R\gamma \neq R(\theta - 1)$. We can construct an SG-module by taking the S-module $Sy \oplus R$, direct sum of a free S-module and R, and defining

$$gy = y + \gamma, \qquad g\alpha = \theta\alpha, \qquad \alpha \in R.$$

We denote this module (γ, R). We shall now prove that every indecomposable SG-module is of one of the types described above.

THEOREM 1. *Every SG-module M is isomorphic to a direct sum*

$$(\gamma_1, R) \oplus \cdots \oplus (\gamma_r, R) \oplus n_0 S \oplus n_1 R,$$

where $\gamma_i \mid \gamma_{i+1}$, $1 \leq i < r$, $\gamma_r \mid (\theta - 1)$, $R\gamma_r \neq R(\theta - 1)$. The integers n_0, n_1 are uniquely determined by the isomorphism class of M, and $\gamma_1, \cdots, \gamma_r$ are determined up to units of R.

Proof. We shall duplicate a proof done by Reiner of a similar result for ZG-modules (see [2, p. 506]).

Let $\sigma = 1 + g + \cdots + g^{p-1}$, and let (σ) be the ideal generated by σ in SG. Then $SG/(\sigma) \cong R$. Given an SG-module M, let

$$M_\sigma = \{m \in M; \sigma m = 0\}.$$

Then M_σ can be made into an R-module by defining $\theta m = gm$ for all $m \in M_\sigma$. M_σ is finitely generated and torsion-free as an R-module.

Since $(g - 1)M \subset M_\sigma$, by the invariant factor theorem for modules over principal ideal domains, there exist $b_1, \cdots, b_n \in M$, $\gamma_1, \cdots, \gamma_n \in R$, such that $\gamma_i \mid \gamma_{i+1}$, $1 \leq i < n$, and

$$M_\sigma = Rb_1 \oplus \cdots \oplus Rb_n, \qquad (g - 1)M = R\gamma_1 b_1 \oplus \cdots \oplus R\gamma_n b_n.$$

$\gamma_1, \cdots, \gamma_n$ are uniquely determined up to units of R by the modules M_σ, $(g - 1)M$. From $(g - 1)M \supset (\theta - 1)M_\sigma$ it follows that $\gamma_n \mid (\theta - 1)$. Assume $R\gamma_r \neq R(\theta - 1)$ and $\gamma_{r+1} = \cdots = \gamma_n = \theta - 1$.

M_σ is an S-pure submodule of M; hence there exists an S-submodule X of M such that $M = X \oplus M_\sigma$. Now consider

$$L = (g - 1)M/(\theta - 1)M_\sigma \cong R\gamma_1/R(\theta - 1) \oplus \cdots \oplus R\gamma_r/R(\theta - 1).$$

Since $(g - 1)M = (g - 1)X + (\theta - 1)M_\sigma$, the natural homomorphism $(g - 1)M \to L$ maps $(g - 1)X$ onto L. Hence the composition of the map

$$x \to (g - 1)x + (\theta - 1)M_\sigma, \qquad x \in X,$$

with the above isomorphism defines a homomorphism ϕ from X onto $R\gamma_1/R(\theta - 1) \oplus \cdots \oplus R\gamma_r/R(\theta - 1)$. Let

$$\phi = \phi_1 + \cdots + \phi_r, \qquad \phi_i : X \to R\gamma_i/R(\theta - 1), \quad 1 \le i \le r.$$

Let $x_1, \cdots, x_t$ be an S-basis for X. Define $\beta_i = (\theta - 1)/\gamma_i$, $i \le i \le r$, and let $\beta_1 = \delta_1 \cdots \delta_u$, $u \le h$. For $i \le u$ we write $\delta_i \mid \phi_1(x)$ if

$$\phi_1(x) \in R\gamma_1 \delta_i/R(\theta - 1).$$

Suppose that for some $j \le u$ we have

$$\delta_i \nmid \phi_1(x_1), \qquad 1 \le i < j,$$
$$\delta_j \mid \phi_1(x_1).$$

Then there exists some x_k such that $\delta_j \nmid \phi_1(x_k)$; otherwise

$$\phi_1(X) \subset R\gamma_1 \delta_j/R(\theta - 1) \subsetneq R\gamma_1/R(\theta - 1).$$

So if we let $c = \varepsilon(\delta_1 \cdots \delta_{j-1})^{p-1} \in S$, where ε is a unit of R, then

$$\delta_i \nmid \phi_1(x_1 + cx_k), \qquad 1 \le i \le j.$$

Thus we can get an S-basis $x, x_2, \cdots, x_t$ of X, such that

$$\phi_1(x) = \alpha\gamma_1 + R(\theta - 1),$$

where α is prime to β_1.

Since $R\gamma_1 = S\gamma_1 + R(\theta - 1)$, there exists $c \in S$, prime to β_1, such that $\alpha\gamma_1 - c\gamma_1 \in R(\theta - 1)$. If c is not a unit then for some $\delta \mid \gamma_1$, $c = c'\varepsilon\delta^{p-1}$, ε unit of $R, c' \in S$; therefore $c'' = c'(\varepsilon\delta^{p-1} + p/\varepsilon\delta^{p-1})$ has one prime factor less than c, and $\alpha\gamma_1 - c''\gamma_1 \in R(\theta - 1)$. We can then assume that c is a unit of S. Let $\bar{\gamma}_1 = \gamma_1 + R(\theta - 1)$; then if $x_1' = c^{-1}x$ we have $\phi_1(x_1') = \bar{\gamma}_1$. Now for every i, $1 < i \le t$, $\phi_1(x_i) = \bar{d}_i \bar{\gamma}_i$ for some $d_i \in S$; hence $\phi_1(x_i - d_i x_1) = 0$. Therefore, letting $x_1' = x_i - d_i x_1$, $1 < i \le t$, we obtain an S-basis $x_1', \cdots, x_t'$ of X, such that

$$\phi_1(x_1') = \bar{\gamma}_1, \qquad \phi_1(x_2') = \cdots = \phi_1(x_t') = 0.$$

Let $\beta_2 = \delta_1 \cdots \delta_v$. We shall now prove that for every δ_j, $i \le j \le v$, there exists some x_k', $2 \le k \le t$, such that $\delta_j \nmid \phi_2(x_k')$. Assume this is false; then

$$\phi_2(Sx_2' \oplus \cdots \oplus Sx_t') \subset R\gamma_2 \delta_j/R(\theta - 1).$$

Now let

$$\phi\left(\textstyle\sum_{i=1}^t c_i x_i'\right) \in R\gamma_2/R(\theta - 1), \qquad c_i \in S, \quad 1 \le i \le t.$$

Then $\phi_1(\sum_{i=1}^t c_i x_i') = \phi_1(c_1 x_1') = 0$, so $\beta_1 \mid c_1$; hence $\beta_i \mid c_1$, $1 \le i \le r$, and from this $\phi_i(c_1 x_i') = 0$, $1 \le i \le t$; consequently

$$\phi\left(\textstyle\sum_{i=1}^t c_i x_i'\right) = \phi\left(\textstyle\sum_{i=2}^t c_i x_i'\right) \in R\gamma_2 \delta_j/R(\theta - 1) \subsetneq R\gamma_2/R(\theta - 1),$$

which is a contradiction.

As before, we can now construct a new basis $x_1'', \cdots, x_t''$ of X, such that

$$\phi_2(x_2'') = \bar{\gamma}_2, \qquad \phi_2(x_1'') = \phi_2(x_3'') = \cdots = \phi_2(x_t'') = 0.$$

It is easily verified that with the method used to construct this basis we get

$$\phi_1(x_1'') = \phi_1(x_1') = \bar{\gamma}_1, \qquad \phi_1(x_2'') = \phi_1(x_2') = \cdots = \phi_1(x_t'') = \phi_1(x_t') = 0.$$

Repeating this process we obtain a basis $z_1, \cdots, z_t$ of X, such that

$$\phi(z_i) = \phi_i(z_i) = \bar{\gamma}_i, \qquad 1 \leq i \leq r,$$

$$\phi(z_i) = 0, \qquad r < i \leq t.$$

Hence there exist $m_i \in M_\sigma$, $1 \leq i \leq t$, such that

$$(g - 1)z_i = \gamma_i b_i + (\theta - 1)m_i, \qquad 1 \leq i \leq r,$$

$$(g - 1)z_i = (\theta - 1)m_i, \qquad r < i \leq t.$$

If we let $y_i = z_i - m_i$, $1 \leq i \leq t$, then

$$(g - 1)y_i = \gamma_i b_i, \qquad 1 \leq i \leq r,$$

$$(g - 1)y_i = 0, \qquad r < i \leq t,$$

and

$$M = Sy_1 \oplus \cdots \oplus Sy_t \oplus Rb_1 \oplus \cdots \oplus Rb_n .$$

Therefore

$$M \cong (\gamma_1, R) \oplus \cdots \oplus (\gamma_r, R) \oplus (t - r)S \oplus (n - r)R.$$

Consider now

$$M = (\gamma_1, R) \oplus \cdots \oplus (\gamma_r, R) \oplus n_0 S \oplus n_1 R,$$

$$\gamma_i \mid \gamma_{i+1}, \qquad 1 \leq i < r,$$

$$\gamma_r \mid (\theta - 1), \qquad R\gamma_r \neq R(\theta - 1).$$

It is easily verified that the invariant factors of the pair of modules M_σ, $(g - 1)M$ are

$$\gamma_1, \cdots, \gamma_r, \gamma_{r+1} = \cdots = \gamma_n = \theta - 1.$$

Since under any isomorphism of SG-modules, $M \cong M'$, M_σ is mapped onto M_σ' and $(g - 1)M$ onto $(g - 1)M'$, the numbers $\gamma_1, \cdots, \gamma_r$ and $n - r = n_1$ are determined by the isomorphism class of M. Therefore, given the S-rank of M, n_0 is also determined.

Now let G be a commutative group, $G = G_1 \times G_2$, where G_1 has exponent q prime to p and G_2 has ordered p, and let ξ be a root of unity whose order divides q. Then $Z_p[\xi]$ can be made into an irreducible $Z_p\, G_1$-module with the elements of G_1 acting by multiplication by the powers of ξ. Denote

$$gx = \xi^{\alpha(g)}x, \quad \text{for} \quad x \in Z_p[\xi],\ g \in G_1 .$$

Then, given an indecomposable $Z_p[\xi]G_2$-module N, define a $Z_p\, G$-module N_α to be the additive group N with the elements of G acting by

$$g_1 g_2 n = \xi^{\alpha(g_1)} g_2 n, \quad \text{for} \quad g_1 \in G_1,\ g_2 \in G_2,\ n \in N.$$

It is easily verified that N_α is an indecomposable $Z_p\, G$-module and that, if N' is another indecomposable $Z_p[\xi]G_2$-module, then $N_\alpha \cong N'_\alpha$ if and only if $N \cong N'$.

Given any indecomposable $Z_p\, G$-module M let M_{G_1} be the $Z_p\, G_1$-module obtained by restricting the operators to G_1. Since p is prime to the order of G_1, M_{G_1} is the direct sum of irreducible submodules. Multiplication by the elements of G_2 permutes isomorphic components of M_{G_1}. Since M is indecomposable, it follows that all the components of M_{G_1} are isomorphic. The irreducible $Z_p\, G_1$-modules are of the form $Z_p[\xi]$, therefore $M_{G_1} \cong Z_p[\xi] \otimes M'$ for some Z_p-module M', where $g(x \otimes m) = gx \otimes m$ for $x \in Z_p[\xi]$, $m \in M'$. Now considering the action of G_2 on M, $N = Z_p[\xi] \otimes M'$ can be made into an indecomposable $Z_p[\xi]G_2$-module, and M can be obtained from N in the manner described above.

2. THEOREM 2. *Let G be a commutative group. If p divides the order of G, then the Krull-Schmidt Theorem holds for $Z_p\, G$-modules if and only if G has exponent qp^n where either $q = 1$ or p is a primitive root modulo q. The theorem also holds if G is a nilpotent group of odd order satisfying this condition.*

Proof. To show that the theorem holds when the given condition is satisfied we shall prove that for every irreducible QG-module M, $Q^* \otimes M$ is an irreducible Q^*G-module. It follows that every irreducible Q^*G-module can be obtained from a QG-module by tensoring with Q^*, and this implies that every Z^*G-module comes from a $Z_p\, G$-module (see [2]). From this, and the fact that for $Z_p\, G$-modules Z^*-isomorphism implies Z_p-isomorphism, it follows that for every indecomposable $Z_p\, G$-module M, $Z^* \otimes M$ is indecomposable. Then the Krull-Schmidt Theorem for $Z_p\, G$-modules is a consequence of the theorem for Z^*G-modules.

Let G be a commutative group satisfying the condition. Every irreducible QG-module M is of the form $M \cong Q[X]/(f)$, where f is a cyclotomic polynomial of some order dividing qp^n, and where the elements of G act by multiplication by X and the powers of X. By the hypothesis on qp^n, f is irreducible over Q^*, hence $Q^* \otimes M$ is an irreducible Q^*G-module.

Suppose G has exponent qp^n where p is not a primitive root modulo q, then, since G has a homomorphic image that is cyclic of order qp, it is sufficient to show that the theorem fails when G is cyclic of order qp.

Using the notation of Theorem 1, $\theta - 1$ has a proper divisor δ in R, so letting $\gamma = (\theta - 1)/\delta$ we get

$$(1, R) \oplus S \oplus R \cong (\delta, R) \oplus (\gamma, R).$$

Let $\delta = \delta_0 + \delta_1 \theta + \cdots + \delta_{p-2}\, \theta^{p-2}$ and $\gamma = \gamma_0 + \gamma_1 \theta + \cdots + \gamma_{p-2}\, \theta^{p-2}$.

Let $\tilde{\xi}$ be a matrix over Z_p which represents multiplication by ξ in S, and denote

$$U = \begin{bmatrix} 0 & 0 & \cdots & 0 & -\tilde{\xi} \\ \tilde{\xi} & 0 & \cdots & \cdot & \cdot \\ 0 & \tilde{\xi} & \cdots & \cdot & \cdot \\ \cdot & \cdot & \cdots & \cdot & \cdot \\ 0 & 0 & \cdots & \tilde{\xi} & -\tilde{\xi} \end{bmatrix}.$$

We then obtain two different decompositions of a Z_p-representation of G into indecomposables by mapping the generator of G into

$$\begin{bmatrix} \tilde{\xi} & 0 & \cdots & 0 \\ \tilde{\xi} & & & \\ 0 & & U & \\ \cdot & & & \\ 0 & & & \end{bmatrix} \oplus \tilde{\xi} \oplus U \sim \begin{bmatrix} \tilde{\xi} & 0 & \cdots & 0 \\ \tilde{\xi}\tilde{\delta}_0 & & & \\ \cdot & & U & \\ \cdot & & & \\ \tilde{\xi}\tilde{\delta}_{p-2} & & & \end{bmatrix} \oplus \begin{bmatrix} \tilde{\xi} & 0 & \cdots & 0 \\ \tilde{\xi}\tilde{\gamma}_0 & & & \\ \cdot & & U & \\ \cdot & & & \\ \tilde{\xi}\tilde{\gamma}_{p-2} & & & \end{bmatrix}.$$

Let G be any finite group and M^* an irreducible Q^*G-module. Let $| G |$ denote the order of G and let $| G | M^*$ be the direct sum of $| G |$ copies of M^*. It can be shown from Artin's Theorem on induced characters (see [2, p. 281]) that there exist cyclic subgroups $\{H_i\}$ of G, and for each H_i a Q^*H_i-module M_i^* and integers n_i, $n_i' \geq 0$, such that

$$| G | M^* \oplus \sum n_i(M_i^*)^G \cong \sum n_i(M_i^*)^G.$$

Suppose that the exponent of G satisfies the given condition; then this condition is also satisfied by all the subgroups H_i, so by the first part of our proof every Q^*H_i-module comes from a QH_i-module. It follows that there exists a QG-module N such that $| G | M^* = Q \otimes N$. Now let M be an irreducible QG-module and suppose that $Q^* \otimes M \cong \sum M_i^*$ where $\{M_i^*\}$ are irreducible Q^*G-modules. Applying the above considerations to these modules we get QG-modules $\{N_i\}$ such that $| G | M_i^* = Q^* \otimes N_i$; hence $| G | M \cong \sum N_i$, so the irreducible components of the modules $\{N_i\}$ are all isomorphic to M. From this it follows that the modules $\{M_i^*\}$ are all isomorphic.

If we now assume G nilpotent and of odd order, by the results of Roquette [5], $\mathrm{Hom}_{Q^*G}(Q^* \otimes M, Q^* \otimes M)$ is commutative so we conclude that $Q^* \otimes M$ must be irreducible.

References

1. S. D. Berman and P. M. Gudivok, *Integral representations of finite groups*, Dokl. Akad. Nauk SSSR, vol. 145 (1962), pp. 1199–1201.
2. C. W. Curtis and I. Reiner, *Representation theory of finite groups and associative algebras*, New York, Interscience, 1963.
3. A. Heller and I. Reiner, *Representations of cyclic groups in rings of integers I*, Ann. of Math. (2), vol. 76 (1962), pp. 73–92.

4. I. REINER, *The Krull-Schmidt Theorem for integral group representations*, Bull. Amer. Math. Soc., vol. 67 (1961), pp. 365–367.
5. P. ROQUETTE, *Realisierung von Darstellungen endlicher nilpotenter Gruppen*, Arch. Math., vol. 9 (1958), pp. 241–250.
6. H. WEYL, *Algebraic theory of numbers*, Princeton, Princeton University Press, 1940.

CORNELL UNIVERSITY
ITHACA, NEW YORK