INTEGRAL REPRESENTATIONS OF NON-ABELIAN GROUPS OF ORDER pq

Lena Chang Pu

1. INTRODUCTION

The problem of representing a finite group G by matrices over an integral domain R can be studied through the classification of finitely generated RG-modules that are torsion-free over R. (By an RG-module, we mean a finitely generaged RG-module that is torsion-free over R.) However, such classification is rather difficult, since several powerful theorems (such as the Jordan-Hölder Theorem, the Krull-Schmidt Theorem, and Maschke's Theorem) do not hold for RG-modules in general.

For the case where G is a cyclic group of prime order p and Z is the ring of rational integers, a complete set of nonisomorphic indecomposable ZG-modules was determined by Diederichsen [2] and Reiner [6]. Recently, M. P. Lee [5] obtained a full set of indecomposable ZG-modules for any dihedral group G of order 2p. The present work gives a complete classification of the integral representations of non-abelian groups of order pq, p and q being distinct primes. In this case, the defining relations for G are as follows:

$$a^q = b^p = 1 \quad \text{and} \quad ab = b^r a,$$

where $p > q$, q divides $p - 1$, and r is a primitive qth root of unity modulo p. The results of this paper include Lee's as a special case.

For any rational prime ℓ, define $Z_\ell = \{t/s: t, s \in Z, (s, \ell) = 1\}$. With each ZG-module M we associate a Z'G-module $M' = Z' \otimes_Z M$, where

$$Z' = Z_p \cap Z_q = \{t/s: t, s \in Z, (s, pq) = 1\}.$$

Then, since p and q are the only primes dividing (G: 1), M is indecomposable as a ZG-module if and only if M' is indecomposable as a Z'G-module [8]. We first determine a full set of $2 + q + 2^{q-1} + 2^q$ nonisomorphic indecomposable Z'G-modules. Using these, we obtain a full set of indecomposable ZG-modules. We compute the number of such modules in terms of the class number of certain algebraic number fields and the indices of certain unit groups.

Finally, using the results of M. Rosen [9], we establish a homomorphism ϕ from the projective class group of ZG onto the direct product of two ideal class groups. We then give a necessary and sufficient condition for this homomorphism to be an isomorphism, and we show that ϕ is not always an isomorphism.

Received August 3, 1964.

This research was supported in part by the Office of Naval Research. The author wishes to thank Professor I. Reiner for his valuable suggestions.

2. Z'G-MODULES

Let M be a Z'G-module, and let

$$\Phi_p(b) = 1 + b + b^2 + \cdots + b^{p-1} \in Z'G.$$

Define $M_0 = \{m \in M: \Phi_p(b)m = 0\}$. Then M_0 is a Z'G-submodule of M, and the short exact sequence of Z'G-modules

$$0 \to M_0 \to M \to M/M_0 \to 0$$

splits over Z'.

Since $\Phi_p(b)(b - 1)m = 0$ for all $m \in M$, we see that $(b - 1)m \in M_0$. Hence b acts trivially on M/M_0, and we can determine the structure of M/M_0 as a Z'G-module by simply considering it as a $Z'\langle a\rangle$-module ($\langle a\rangle$ denotes the cyclic group generated by a). By the results of Reiner [6], the only indecomposable $Z'\langle a\rangle$-modules are Z', $Z'[\theta]$, and $Z'\langle a\rangle$, where θ is a primitive qth root of unity.

Next, let $\zeta m = bm$ for $m \in M$. Then M_0 can be considered as an S'-module, where $S' = Z'[\zeta]$. Since $ab = b^r a$ and $r^q \equiv 1 \pmod p$, we have the relations $a \cdot \zeta m = abm = b^r am = \zeta^r am$ for $m \in M_0$. Hence a acts as a semilinear transformation on the S'-module M_0, with the induced Z'-automorphism σ on S' given by $\sigma: \zeta \to \zeta^r$.

Definition 1. Let Λ be the free S'-module generated by the elements of $\langle a\rangle$. Define multiplication in Λ by

$$\xi_1 a^n \cdot \xi_2 a^m = \xi_1 \xi_2^{\sigma^n} a^{m+n} \qquad (\xi_1, \xi_2 \in S');$$

then Λ is the *twisted group ring* of $\langle a\rangle$ with coefficients in S'.

By a Λ-module, we mean a left Λ-module that is finitely generated and torsion-free over S'. Each Λ-module may be considered as a Z'G-module (annihilated by $\Phi_p(b)$) on which b acts as multiplication by ζ. The converse is also true, since $Z'G/(\Phi_p(b))$ and Λ are isomorphic to each other as rings.

Therefore the problem of determining all indecomposable Z'G-modules is now reduced to finding all nonisomorphic indecomposable Z'G-extensions of Λ-modules by $Z'\langle a\rangle$-modules, after the Λ-modules themselves are determined.

Definition 2. Let $K = Q(\zeta)$; an S'-ideal A of K is said to be *ambiguous* if and only if $A^\sigma = A$.

Let A be an ambiguous S'-ideal in K, and define $a \cdot \xi = \xi^\sigma$ for all $\xi \in A$. Then A is an irreducible Λ-module, and every irreducible Λ-module is of this type. Since every Λ-module is Λ-projective [9], a Λ-module is indecomposable, if and only if it is irreducible. Also, it is easy to see that two indecomposable Λ-modules A and B are Λ-isomorphic if and only if there exists a nonzero $\rho \in K$ such that $\rho^\sigma = \rho$ and $B = \rho A$.

We note that the only prime ideals in S' are those lying over p or q. Moreover, $pS' = (\zeta - 1)^{p-1}S'$ and $qS' = Q_1 \cdot Q_2 \cdots Q_{p-1}$, where the Q_i are distinct prime ideals in S'. Hence $P = (\zeta - 1)S'$ is the only prime ideal of S' fixed under σ, that is, $P^\sigma = P$. Since p^q and S' are Λ-isomorphic, it is easily seen that S', P, P^2, $\cdots$ P^{q-1} constitute a complete set of nonisomorphic indecomposable Λ-modules [9].

Throughout this section, let M_0 be a Λ-module, and M_1 a $Z'\langle a\rangle$-module. For simplicity, we write Ext for $\mathrm{Ext}^1_{Z'G}$. Then

$$\mathrm{Ext}(M_1, M_0) \subset \mathrm{Hom}_{Z'}(Z'G, \mathrm{Hom}_{Z'}(M_1, M_0)).$$

If $f \in \mathrm{Ext}(M_1, M_0)$, then

$$f_{\rho\tau}(m_1) = \rho f_\tau(m_1) + f_\rho(\tau m_1)$$

for all $\rho, \tau \in G$ and all $m_1 \in M_1$. Each $f \in \mathrm{Ext}(M_1, M_0)$ determines a $Z'G$-extension module M, denoted by $(M_0, M_1; f)$, such that M and $M_0 \oplus_{Z'} M_1$ are Z'-isomorphic with the action of $\rho \in G$ given by $\rho(m_0, m_1) = (\rho m_0 + f_\rho(m_1), \rho m_1)$. Hence to find all extensions of M_0 by M_1, we must first determine $\mathrm{Ext}(M_1, M_0)$. However, since Ext is an additive functor, it suffices to determine $\mathrm{Ext}(M_1, M_0)$ explicitly for indecomposable M_0 and M_1.

Consider the exact sequence

$$(1) \qquad 0 \to I \xrightarrow{i} Z'G \xrightarrow{j} Z' \to 0$$

of $Z'G$-modules, where $j(a) = j(b) = 1$ and I is the augmentation ideal in $Z'G$. One easily finds that $I = Z'G(b-1) + Z'\langle a\rangle(a-1)$.

THEOREM 1. *Let* $S' = Z'[\zeta]$, $P = (\zeta - 1)S'$. *Then*

(i) $\mathrm{Ext}(Z', P) \cong S'/P$,

(ii) $\mathrm{Ext}(Z', S') = 0$,

(iii) $\mathrm{Ext}(Z', P^m) = 0$ *for* $2 \le m \le q-1$.

Proof. Let $\mathfrak{A}$ denote the Λ-module P^m for some m $(0 \le m \le q-1,\ P^0 = S')$. Then it follows from (1) that

$$0 \to \mathrm{Hom}_{Z'G}(Z', \mathfrak{A}) \xrightarrow{j^*} \mathrm{Hom}_{Z'G}(Z'G, \mathfrak{A}) \xrightarrow{i^*} \mathrm{Hom}_{Z'G}(I_1, \mathfrak{A}) \to \mathrm{Ext}(Z', \mathfrak{A}) \to 0$$

is an exact sequence of Z'-modules. Clearly, the $i^*(\mathrm{Hom}(Z'G, \mathfrak{A}))$ are isomorphic to $\mathfrak{A}$ as Z'-modules, the isomorphism being given by $i^*(f) \to f(1)$. Let

$$\mathfrak{A}^* = \mathfrak{A} \otimes_{Z'} Q;$$

then $\mathfrak{A}^* \cong K = Q(\zeta)$ (as QG-modules). Further, the augmentation ideal I^* in QG is $I \otimes_{Z'} Q$. Thus, for each $f \in \mathrm{Hom}(I, \mathfrak{A})$, $f \otimes 1$ lies in $\mathrm{Hom}(I^*, \mathfrak{A}^*)$ and can be extended uniquely to f^* on QG, since $\mathfrak{A}^*$ is an injective QG-module. Let $f^*(1) = \alpha_f$. Then $\alpha_f \in \mathfrak{A}^*$, $f(x) = x\alpha_f$ for each $x \in I$, and α_f is uniquely determined by f. Now define $\mathfrak{A}' = \{\alpha \in \mathfrak{A}^*: (a-1)\alpha \in \mathfrak{A}$ and $(b-1)\alpha \in \mathfrak{A}\}$; then $\mathrm{Hom}(I, \mathfrak{A})$ and $\mathfrak{A}'$ are Z'-isomorphic. Indeed, $f \to \alpha_f$ is the desired isomorphism. Thus,

$$(2) \qquad \mathrm{Ext}(Z', \mathfrak{A}) \cong \mathfrak{A}'/\mathfrak{A} \text{ as } Z'\text{-modules}.$$

Now we shall show that $\mathfrak{A}' \cong S'$ for $m = 1$ and that $\mathfrak{A}' \cong \mathfrak{A}$ for $m \ne 1$ $(0 \le m \le q-1)$. To this end, we recall that $a\alpha = \alpha^\sigma$ and $b\alpha = \zeta\alpha$ for each $\alpha \in \mathfrak{A}'$. Thus $\mathfrak{A}/(\zeta - 1) \supset \mathfrak{A}' \supset \mathfrak{A}$. Further, for $\alpha \in \mathfrak{A}/(\zeta-1)$, $\alpha \in \mathfrak{A}'$ if and only if $\alpha^\sigma - \alpha \in \mathfrak{A}$. But $\alpha \in \mathfrak{A}/(\zeta - 1)$ implies $\alpha = (\zeta - 1)^{m-1}u_0$ for some $u_0 \in S'$. Thus $\alpha \in \mathfrak{A}'$ if and only if

$$(\zeta - 1)^m \eta^m u_0^\sigma \equiv (\zeta - 1)^m \eta u_0 \pmod{P^{m+1}},$$

where $\eta = (\zeta - 1)^{\sigma - 1} = 1 + \zeta + \zeta^2 + \cdots + \zeta^r$. Hence $\alpha \in \mathfrak{A}'$ if and only if $\eta^m u_0^\sigma \equiv \eta u_0 \pmod{P}$. Now $u_0^\sigma \equiv u_0 \pmod{P}$ for each $u_0 \in S'$, and $\eta \equiv r \pmod{P}$. Thus $\alpha \in \mathfrak{A}'$ if and only if $(r^m - r)u_0 \equiv 0 \pmod{P}$.

If $m \neq 1$, then since r is a primitive qth root of unity (mod p), $r^m - r \notin P$. This implies $u_0 \in P$, and thus $\alpha \in \mathfrak{A}'$ if and only if $\alpha \in \mathfrak{A}$, that is, $\mathfrak{A}' \cong \mathfrak{A}$.

If $m = 1$, then $r^m - r = r - r = 0 \in P$. Thus in this case u_0 is arbitrary in S', and $\mathfrak{A}' \cong S'$.

Using (2), we have the desired result.

Similarly, using the fact that the different of K/K_0 is $(\zeta - 1)^{q-1} S'$, where K_0 is the field of fixed elements under σ, we may obtain the following results, where, as before, θ denotes a primitive qth root of unity:

$$(3)\qquad \begin{cases} \mathrm{Ext}(Z'[\theta], P) = 0, \\ \mathrm{Ext}(Z'[\theta], S') \cong S'/P, \\ \mathrm{Ext}(Z'[\theta], P^m) \cong S/P \qquad (2 \leq m \leq q - 1), \\ \mathrm{Ext}(Z'\langle a \rangle, P^m) \cong S'/P \qquad (0 \leq m \leq q - 1). \end{cases}$$

Remark 1. Theorem 1 and (3) remain valid when Z' is replaced by Z_p or Z_q. We further note that since p is a unit in Z_q, $\mathrm{Ext}^1_{Z_qG}(M_1, M_0) = 0$ for any Λ_q-module M_0 and $Z_q\langle a \rangle$-module M_1, where $\Lambda_q = \Lambda \otimes_{Z'} Zq$.

Remark 2 (Reiner [1, (81.8)]). Let M_0, M_1 be indecomposable, and let

$$f, g \in \mathrm{Ext}(M_1, M_0).$$

Since $\mathrm{Hom}_{Z'G}(M_1, M_0) = 0$, we have the isomorphism $(M_0, M_1; f) \cong (M_0, M_1; g)$ if and only if there exist $\psi \in \mathrm{Hom}_{Z'}(M_1, M_0)$ and automorphisms ϕ_0 and ϕ_1 of M_0 and M_1, respectively, such that

$$\phi_0 f_\rho(m_1) - g_\rho(\phi_1(m_1)) = \rho\psi(m_1) - \psi(\rho m_1)$$

for all $\rho \in G$ and $m_1 \in M_1$.

Now, suppose M_0, M_1 are indecomposable; using the relation $ab = b^r a$, we obtain

$$(4)\qquad (\zeta^r - 1) f_a(m_1) = (f_b(m_1))^\sigma - \eta f_b(a m_1) \qquad (m_1 \in M_1),$$

where $\eta = (\zeta - 1)^{\sigma - 1}$. Since a and b form a basis for G, it is clear from (4) that f_ρ is completely determined by f_b. Let $f, g \in \mathrm{Ext}(M_1, M_0)$ satisfy the condition in Remark 2 for $\rho = b$ and all $m_1 \in M_1$. Then clearly the condition is satisfied for all $\rho \in G$, and $(M_0, M_1; f) \cong (M_0, M_1; g)$.

If M_1 is cyclic with generator $\overline{m}$, we obtain from (4) the relation

$$f_b(a\overline{m}) \equiv \eta^{-1} (f_b(\overline{m}))^\sigma \pmod{PM_0}.$$

Hence $f_b(m_1)$ is determined modulo PM_0 by $f_b(\overline{m})$, for each $m_1 \in M_1$, if $M_1 = Z\langle a\rangle \cdot \overline{m}$. In the case where M_1 is indecomposable, M_1 is cyclic with generator 1. (We recall that the only indecomposable $Z'\langle a\rangle$-modules are Z', $Z'[\theta]$, and $Z'\langle a\rangle$.)

With the above discussion, the following proposition follows immediately, since $\mathrm{Hom}_{Z'G}(M_1, M_0) = 0$.

PROPOSITION 1. *Let* $f, g \in \mathrm{Ext}(M_1, M_0)$. *Then* $(M_0, M_1; f) \cong (M_0, M_1; g)$ *if and only if there exist automorphisms* ϕ_0 *and* ϕ_1 *of* M_0 *and* M_1, *respectively, such that*

$$\phi_0 f_b(m_1) - g_b(\phi_1(m_1)) \equiv 0 \pmod{PM_0}$$

for all $m_1 \in M_1$. *Further, if* M_1 *is cyclic with generator* 1, *then*

$$(M_0, M_1; f) \cong (M_0, M_1; g)$$

if and only if

$$\phi_0(f_b(1)) - g_b(\phi_1(1)) \equiv 0 \pmod{PM_0}.$$

Again, let M_0, M_1 be indecomposable. Then any automorphism of M_0 is a multiplication by a unit in $R_0' = K_0 \cap S'$. We recall that $\mathrm{Ext}(M_1, M_0)$ is either Z/pZ or 0. Further, each nonzero element in Z/pZ is represented by a unit in $Z' \subset R_0'$. Thus by Proposition 1, the following result is clear.

PROPOSITION 2. *Suppose* M_0, M_1 *are indecomposable and* $\mathrm{Ext}(M_1, M_0) \neq 0$; *then there exists a unique indecomposable* $Z'G$-*extension of* M_0 *by* M_1.

Now let Z_p be the ring of p-adic integers in Q, Q_p the p-adic completion of Q, and Z_p^* the p-adic valuation ring in Q_p. Then, since q divides p - 1 and (by Hensel's Lemma) Z_p^* contains every qth root of unity. Further, by Swan [10] or Reiner [7], the Krull-Schmidt Theorem holds for Z_p^*G-modules.

Definition 3. A Z_p^*G-module N is *induced* from a Z_pG-module M if and only if N and $Z_p^* \otimes_{Z_p} M$ are isomorphic as Z_p^*G-modules.

Remark 3 (A. Jones [4]). A Z_pG-module M is indecomposable if and only if $Z_p^* \otimes_{Z_p} M$ has no induced direct summand.

Thus we should like first to determine all indecomposable Z_p^*G-modules. Let $K^* = Q_p(\zeta)$, and let $S_p^* = Z_p^*[\zeta]$ be the ring of integers in K^*. Then clearly

$$S_p^*,\ P^* = (\zeta - 1)S_p^*,\ P^{*2},\ \cdots,\ P^{*q-1}$$

form a complete set of indecomposable Z_p^*G-modules on which b acts as multiplication by ζ and a acts as $\sigma: \zeta \to \zeta^r$.

Let $\theta_0 = 1, \theta_1, \cdots, \theta_{q-1}$ be the qth roots of unity in Z_p^*, ordered so that $\theta_i \equiv r^i \pmod p$. We denote by W_i the Z_p^*G-module Z_p^* on which b acts trivially and a acts as multiplication by θ_i. It is easily found that $\{W_i\colon 0 \leq i \leq q-1\}$ is a complete set of indecomposable Z_p^*G-modules on which b acts trivially.

Remark 4. Let $H = \langle b\rangle$, $b^p = 1$. Since the Krull-Schmidt Theorem holds for Z_p^*G-modules and since p does not divide (G: H), it follows [3] that every indecomposable Z_p^*G-module is isomorphic to a direct summand of L^G for some indecomposable Z_p^*H-module L. Let M be an indecomposable Z_p^*G-module such that

$$M \mid H \cong L_1 \oplus \cdots \oplus L_n,$$

where each L_i is an indecomposable Z_p^*H-module. Then M is a direct summand of some L_i^G.

Since Z_p^*, $Z_p^*[\zeta]$, and Z_p^*H form a full set of indecomposable Z_p^*H-modules, Remark 4 yields the Z_p^*G-isomorphisms

$$(5) \qquad \begin{cases} Z_p^{*G} \cong W_0 \oplus W_1 \oplus \cdots \oplus W_{q-1}, \\ \{Z_p^*[\zeta]\}^G \cong S_p^* \oplus P^* \oplus P^{*2} \oplus \cdots \oplus P^{*q-1}. \end{cases}$$

As in the proof of Theorem 1 we have for each e $(0 \leq e \leq q-1)$ the relations

$$(6) \qquad \begin{cases} \operatorname{Ext}(W_{e-1}, P^{*e}) \cong S_p^*/P^* \cong Z/pZ, \\ \operatorname{Ext}(W_i, P^{*e}) = 0 \quad \text{for each } i \neq e-1 \quad (0 \leq i \leq q-1). \end{cases}$$

Further, we may easily show (as in Proposition 2) that for each e there exists a unique indecomposable extension of P^{*e} by W_{e-1}, which we denote by V_e.

Let $\Lambda_p = Z_p \otimes_{Z'} \Lambda$. Then (see [9]) the sequence of Z_pG-modules

$$0 \to \Lambda_p \to Z_pG \to Z_p\langle a \rangle \to 0$$

is exact, and

$$\Lambda_p \cong S_p \oplus \tilde{P} \oplus \tilde{P}^2 \oplus \cdots \oplus \tilde{P}^{q-1},$$

where $\tilde{P} = (\zeta - 1)S_p$. From this and Remark 1 we obtain

$$(7) \qquad \{Z_p^*H\}^G \cong Z_p^*G \cong V_0 \oplus V_1 \oplus \cdots \oplus V_{q-1}.$$

By Remark 4, the following collection of Z_p^*G-modules is a complete set of indecomposables:

$$\{W_i: 0 \leq i \leq q-1\}, \qquad \{P^{*e}: 0 \leq e \leq q-1, \quad P^{*0} = S_p^*\}, \qquad \{V_e: 0 \leq e \leq q-1\}.$$

Let $\{N_t: 1 \leq t \leq 2^q\}$ be the set of all distinct direct sums (including zero) of subsets of $\{\tilde{P}^0, \tilde{P}^1, \tilde{P}^2, \cdots, \tilde{P}^{q-1}\}$, arranged so that none of $N_1, N_2, \cdots, N_{2^q - 1}$ contains $\tilde{P}^1$ as a direct summand.

THEOREM 2. *For each* t $(1 \leq t \leq 2^{q-1})$ *there exists a unique indecomposable* Z_pG-*extension of* N_t *by* $Z_p[\theta]$.

Proof. Let $X = (N_t, Z_p[\theta]; f)$ be an extension of N_t by $Z_p[\theta]$. Then (say)

$$N_t = \sum_{i=1}^{k}{}^{\oplus} \tilde{P}^{e_i} \quad \text{and} \quad f = \sum_{i=1}^{k} f_i,$$

where $f_i \in \operatorname{Ext}(Z_p[\theta], \tilde{P}^{e_i})$ $(1 \leq i \leq k)$. If some f_i is 0, then clearly $\tilde{P}^{e_i}$ splits off as a direct summand of X. On the other hand, suppose $f_i \neq 0$ for each i; tensoring with Z_p^*, we have the isomorphism

$$X^* \cong (N_t^*, Z_p[\theta]^*; \sum_{i=1}^{k} 1 \otimes f_i).$$

Since $1 \otimes f_i \neq 0$ for each i $(1 \leq i \leq k)$, the following is a decomposition of X^* into indecomposable summands:

$$X^* \cong \sum_{i=1}^{k}{}^{\oplus} (P^{*e_i}, W_{e_{i-1}}; 1 \otimes f_i) \oplus \sum_j{}^{\oplus} W_j,$$

where j ranges over all integers between 1 and q - 1 distinct from each e_i. If X is decomposable, then, since $Z_p[\theta]$ is irreducible, some $\tilde{P}^{e_i}$ must split off as a direct summand. It follows that P^{*e_i} is a direct summand of X^*. However, this contradicts the Krull-Schmidt Theorem for Z_p^*G-modules, so X is indecomposable.

To show the uniqueness of the extension for each $e \neq 1$, we recall that

$$\text{Ext}^1_{Z_pG}(Z_p[\theta], \tilde{P}^e) \cong Z/pZ.$$

Assume, for fixed t, that X is indecomposable, so that $f_i \neq 0$ for each i; then, since $1 \in Z_p[\theta]$, we see that

$$(f_i)_b(1) = s_i m_i \quad \text{for some } m_i \text{ and some } s_i \; (m_i \in \tilde{P}^{e_i},\; m_i \notin \tilde{P}^{e_i+1},\; 1 \leq s_i \leq p-1).$$

By Proposition 1, to determine the isomorphism class of X one need only consider the behavior of f_b at 1. Define ϕ: $N_t \to N_t$ by

$$\phi(\alpha_1, \alpha_2, \cdots, \alpha_k) = (s_1\alpha_1, s_2\alpha_2, \cdots, s_k\alpha_k) \quad (\alpha_i \in \tilde{P}^{e_i}).$$

Since s_i is a unit in Z_p for each i, ϕ is clearly an automorphism of N_t. Let $X_t = (N_t, Z_p[\theta]; g)$, where

$$g = \sum_{i=1}^{k} g_i \quad \text{in} \quad \sum_{i=1}^{k}{}^{\oplus} \text{Ext}(Z_p[\theta], \tilde{P}^{e_i})$$

and $(g_i)_b(1) = m_i$. Then obviously $\phi g_b(1) - f_b(1) \equiv 0 \pmod{\tilde{P} N_t}$. Thus, by Proposition 1, $X \cong X_t$. This proves the theorem.

Consider the set $\mathcal{T}$ of Z_pG-modules

$$\mathcal{T} = \{Z_p, S_p, \tilde{P}, \tilde{P}^2, \cdots, \tilde{P}^{q-1}, [\tilde{P}, Z_p], X_1, \cdots, X_{2^{q-1}}\},$$

where $[\tilde{P}, Z_p]$ denotes the unique indecomposable Z_pG-extension of $\tilde{P}$ by Z_p. So far we have shown that each module in $\mathcal{T}$ is indecomposable. Clearly no two modules in $\mathcal{T}$ are Z_pG-isomorphic. Further, with the repeated use of Remark 3, we can easily (although with some tedium) obtain the following theorem.

THEOREM 3. *The set* $\mathcal{T}$ *of* $2^{q-1} + q + 2$ *distinct* Z_pG-*modules is a complete set of nonisomorphic indecomposable* Z_pG-*modules.*

This completes the investigation of the localization at the prime p.

When localized at q, p is a unit in Z_p. Using Remark 1, we can then easily show that

$$\{Z_q, Z_q[\theta], Z_q\langle a\rangle, S_q = Z_q[\zeta]\}$$

forms a complete set of indecomposable Z_qG-modules.

Remark 5 (Reiner [8]). A Z'G-module M is decomposable if and only if there exist nontrivial decompositions

$$Z_pM = L_p \oplus X \quad \text{and} \quad Z_qM = L_q \oplus Y$$

such that $Q \otimes_{Z_p} L_p \cong Q \otimes_{Z_q} L_q$.

Let $\{N_t: 1 \le t \le 2^q\}$ be defined as before, with $P = (\zeta - 1)S'$ replacing $\tilde{P}$. Recall that N_t does not contain P for $1 \le t \le 2^{q-1}$, and write

$$N_t = \sum_{i=1}^{k}{}^{\oplus} P^{e_i}.$$

THEOREM 4. *For each* t $(1 \le t \le 2^{q-1})$ *there exists a unique indecomposable* Z'G-*extension* X_t' *of* N_t *by* $Z'[\theta]$. *Furthermore, for each* t $(1 \le t \le 2^q)$ *there exists a unique indecomposable* Z'G-*extension* Y_t' *of* N_t *by* $Z'\langle a\rangle$.

Proof. Use Remark 5 and the fact that each nonzero element in Z/pZ is represented by a unit in Z'.

Let [P, Z'] denote the unique indecomposable extension of P by Z'.

THEOREM 5. *The set of* Z'G-*modules*

$$\{Z', S', P, \cdots, P^{q-1}, [P, Z'], X_1', \cdots, X_{2^{q-1}}', Y_1', \cdots, Y_{2^q}'\}$$

is a complete set of nonisomorphic indecomposable Z'G-*modules. The number of indecomposables is thus* $2 + q + 2^{q-1} + 2^q$.

Proof. Use Remark 5 and the information we obtained on the indecomposable Z_pG- and Z_qG-modules. We omit the details.

3. ZG-MODULES

Let $S = Z[\zeta]$, where ζ is a primitive pth root of unity; further, let σ be the Q-automorphism of $K = Q(\zeta)$ of order q defined by the relation $\sigma: \zeta \to \zeta^r$, where $r^q \equiv 1 \pmod p$. Let Λ be the twisted group ring of $\langle a\rangle$ with coefficients in S (we note that the Λ in Section 2 has coefficients in S'). Let K_0 denote the field of fixed elements in K under σ, and let $R_0 = K_0 \cap S$. Let $P = (\zeta - 1)S$ (the P in Section 2 is $(\zeta - 1)S'$), $P_0 = P \cap R_0$. Let $K' = Q(\theta)$, let θ be a primitive qth root of unity, and let R' be the ring of algebraic integers in K'. Finally, let h_0 and h' denote the ideal class number of R_0 and R', respectively. Then the following three results are obtained as in Section 2.

(I) *Each* ZG-*module is a* ZG-*extension of a* Λ-*module by a* $Z\langle a\rangle$-*module.*

(II) *Let* $A_1 = R_0, A_2, \cdots, A_{h_0}$ *be a set of representatives for the ideal classes in* R_0; *let* P^e *be considered as a* Λ-*module by* $a \cdot \xi = \xi^\sigma$ $(\xi \in P^e)$. *Then*

$$\{P^e A_j: 1 \leq e \leq q - 1,\ 1 \leq j \leq h_0\}$$

is a complete set of nonisomorphic indecomposable Λ*-modules.*

(III) *Let* $C_1, C_2, \cdots, C_{h'}$ *be a set of representatives for the ideal classes of* $R' = Z[\theta]$. *Each* C_i *is considered as a* $Z\langle a\rangle$*-module by* $a \cdot \xi = \theta\xi$ $(\xi \in C_i)$. *Further, for each* i, *fix* $\gamma_i \in C_i$ *such that* $\gamma_i \notin (\theta - 1)C_i$. *Denote by* (C_i, γ_i) *the* $Z\langle a\rangle$*-module* $C_i \oplus Z$, *where* $a(\xi, n) = (\theta\xi + \gamma_i, n)$ *for each* $\xi \in C_i$ *and each* $n \in Z$. *Then, since* $\langle a\rangle$ *is a cyclic group of prime order* q,

$$\{Z, C_1, C_2, \cdots, C_{h'}, (C_1, \gamma_1), (C_2, \gamma_2), \cdots, (C_{h'}, \gamma_{h'})\}$$

is a complete set of nonisomorphic, indecomposable $Z\langle a\rangle$*-modules.*

Now let $\{N_t: 1 \leq t \leq 2^q\}$ be defined as in Section 2, with $P = (\zeta - 1)S$. Write $N_t = \sum_{i=1}^{k\,\oplus} P^{e_i}$. Let $B_1, B_2, \cdots, B_k$ be a set of R_0-ideals, and let $[B]$ denote the R_0-ideal class of $\prod_{i=1}^{k} B_i$. Let

$$N_{t,[B]} = \sum_{i=1}^{k\,\oplus} P^{e_i} B_i .$$

Then by a result of M. Rosen [9], a full set if invariants of the isomorphism class of $N_{t,[B]}$ consists of $e_1, \cdots, e_k$ and $[B]$.

PROPOSITION 3. *For each* t $(1 \leq t \leq 2^{q-1})$, *each* R_0*-ideal class* $[B]$, *and each* R'*-ideal class* $[C]$, *there exists an indecomposable* ZG*-extension of* $N_{t,[B]}$ *by* C. *Further, for each* t $(1 \leq t \leq 2^q)$ *there exists an indecomposable* ZG*-extension of* $N_{t,[B]}$ *by* (C, γ), *where* $\gamma \in C$ *and* $\gamma \notin (\theta - 1)C$.

Proof. A ZG-module M is indecomposable if and only if $Z' \otimes M$ is indecomposable as a Z'G-module [8]. From this and our results for Z'G-modules we can easily show, for each R_0-ideal class $[B]$, the existence of an indecomposable ZG-extension of $N_{t,[B]}$ by $Z[\theta]$ for each t $(1 \leq t \leq 2^{q-1})$, and the existence of an indecomposable extension of $N_{t,[B]}$ by $Z\langle a\rangle$ for each $t \leq t \leq 2^q$). For any other ideal class $[C]$ in R', we may take the representative C to be an integral ideal such that $C \cap Z = (s)$ and $(s, p) = 1$. If $f \in \mathrm{Ext}^1_{ZG}(Z[\theta], N_{t,[B]})$ is such that $(N_{t,[B]}, Z[\theta]; f)$ is indecomposable, then, using the restriction of f to the above chosen ideal C, we find that $(N_{t,[B]}, C: f|C)$ is also indecomposable. Furthermore, since $(s, p) = 1$, (C, γ) and (C, s) are isomorphic as $Z\langle a\rangle$-modules. Define $\rho: (C, s) \to Z\langle a\rangle$ such that $\rho(c, n) = (c, ns)$ for all $c \in C$ and all $n \in Z$. Then ρ is a $Z\langle a\rangle$-map, embedding (C, s) in $Z\langle a\rangle$. Using this embedding ρ, we may easily show the existence of an indecomposable ZG-extension of $N_{t,[B]}$ by (C, s).

Let $\overline{Z} = Z/pZ$, $\overline{Z}^* = \overline{Z} - \{0\}$. Let U be the set of units in R_0. Then, since $\overline{R}_0 = R_0/P_0 \cong \overline{Z}$, $\overline{U}$ is a multiplicative subgroup of $\overline{Z}^*$.

PROPOSITION 4. *For each* R_0*-ideal class* $[B]$, *there exist exactly* $(\overline{Z}^*: \overline{U})$ *nonisomorphic indecomposable* ZG*-extensions of* PB *by* Z.

Proof. We may assume B to be integral and relatively prime to $P_0 = P \cap R_0$. Let $f \in \mathrm{Ext}^1_{ZG}(Z, PB)$, and let $M_{f,[B]} = (PB, Z; f)$. Then clearly $M_{f,[B]}$ is indecomposable as a ZG-module if and only if $f \neq 0$.

Let $f_b(1) = \ell m_0$, where $m_0 \in PB$, $m_0 \notin P^2 B$, and $\ell \in \overline{Z}^*$. Let

$$g \in \mathrm{Ext}^1_{ZG}(Z, PB)$$

be such that $g_b(1) = sm_0$ for some $s \in \overline{Z}^*$. We shall show that then

$$(PB, Z; f) \cong (PB, Z; g)$$

if and only if there exists $u \in U$ such that $s \equiv \bar{u}\ell \pmod p$. By Proposition 1, $M_{f,[B]} \cong M_{g,[B]}$ if and only if there exist automorphisms ϕ_0 of PB and ϕ_1 of Z such that $\phi_0 f_b(1) - g_b(\phi_1(1))$ is in $P^2 B$. However, the only ZG-automorphisms of Z are the identity map and the map ϕ: $\phi(1) = -1$. The ZG-automorphisms of PB are given as multiplications by units in R_0. Hence $M_{f,[B]} \cong M_{g,[B]}$ if and only if there exists a unit $u \in R_0$ such that

$$uf_b(1) - g_b(\phi(1)) = u\ell m_0 \pm sm_0 \in P^2 B.$$

That is, $M_{f,[B]} \cong M_{g,[B]}$ if and only if $\bar{u}\ell \equiv \pm s \pmod p$. Since $\pm 1 \in \overline{U}$, there are exactly $(\overline{Z}^*: \overline{U})$ nonisomorphic indecomposable ZG-extensions of PB by Z.

Define $\eta = (\zeta - 1)^{1-\sigma}$ (note that this is the reciprocal of the value assigned to η in (4) of Section 2). Then η is a unit in S. Further, let $\eta^{(i)} = \eta^{1+\sigma+\sigma^2+\cdots+\sigma^{i-1}}$.

Using (4), we obtain for M_0 a Λ-module,

$$(8)\quad \begin{cases} \text{(i)}\ f_b(\theta^i \cdot 1) = f_b(a^i \cdot 1) \equiv \eta^{(i)} a^i f_b(1) \pmod{PM_0}, \\ \qquad\qquad \text{where } f \in \mathrm{Ext}(Z[\theta], M_0) \\ \text{(ii)}\ f_b(a^i \cdot 1) = \eta^{(i)} a^i f_b(1), \text{ where } f \in \mathrm{Ext}(Z\langle a\rangle, M_0). \end{cases}$$

Now let

$$\beta = \sum_{i-0}^{q-2} z_i \theta^i \quad \left(\text{or } \beta = \sum_{i=0}^{q-1} z_i a^i,\ z_i \in Z \right)$$

be a unit in $Z[\theta]$ (or in $Z\langle a\rangle$, respectively). Then by (8) we have the congruence

$$f_b(\beta \cdot 1) \equiv \sum_i z_i \eta^{(i)} a^i f_b(1) \pmod{PM_0}.$$

Suppose $M_0 = P^e B$ for some e $(0 \le e \le q - 1)$, and suppose B is an R_0-ideal relatively prime to P; then a^i acts on M_0 as σ^i. Thus

$$f_b(\beta \cdot 1) \equiv \sum_i z_i \eta^{(i)} (f_b(1))^{\sigma^i} \pmod{P^{e+1} B}.$$

Since $P^e/P^{e+1} \cong S/P \cong \overline{Z}$, σ induces the identity map on P^e/P^{e+1}. Hence $(f_b(1))^{\sigma^i} \equiv f_b(1) \pmod{p^{e+1} B}$ and

$$f_b(\beta \cdot 1) \equiv \left(\sum_{i=1}^{q-1} z_i \eta^{(i)} \right) f_b(1) \pmod{P^{e+1} B}.$$

Define

$$\overline{U}_\theta = \{u_\beta \in \overline{Z}^*: u_\beta \equiv \sum_{i=0}^{q-2} z_i \eta^{(i)} \pmod{P},$$

$$\text{where } \beta = \sum_{i=0}^{q-2} z_i \theta^i \text{ is a unit in } Z[\theta]\}.$$

Also, define

$$\overline{U}_a = \{ u_\beta \in \overline{Z}^*: u_\beta \equiv \sum_{i=0}^{q-1} z_i \eta^{(i)} \pmod{P},$$

where $\beta = \Sigma_{i=0}^{q-1} z_i a^i$ is a unit in $Z\langle a \rangle\}$. Then clearly $\overline{U}_\theta$ and $\overline{U}_a$ are multiplicative subgroups of $\overline{Z}^*$. The following Lemma can easily be obtained.

LEMMA 1. *Let* $M = \sum_{i=1}^{k}{}^{\oplus} P^{e_i}$, *where* $0 \leq e_i \leq q - 1$ *for each* i. *Let* ϕ *be a* ZG-*automorphism of* M. *Then there exist* $\alpha_1, \alpha_2, \cdots, \alpha_k$ *in* R_0 *and a unit* $u \in R_0$ *such that*

(i) $u \equiv \alpha_1 \alpha_2 \cdots \alpha_k \pmod{P_0}$, *where* $P_0 = P \cap R_0$,

(ii) $\phi(x_1, x_2, \cdots, x_k) \equiv (\alpha_1 x_1, \alpha_2 x_2, \cdots, \alpha_k x_k) \pmod{PM}$ *for each* $(x_1, x_2, \cdots, x_k) \in M$.

LEMMA 2. *Let* $\operatorname{diag}(\overline{\beta}_1, \overline{\beta}_2, \cdots, \overline{\beta}_k)$ *be a* $k \times k$ *diagonal matrix over* $\overline{R}_0 = R_0/P_0$. *Let* β_i *be a coset representative of* $\overline{\beta}_i$ *for each* i. *Suppose there exists a unit in* R_0 *such that* $\Pi_{i=1}^{k} \beta_i \equiv u \pmod{P_0}$. *Then the matrix*

$$\operatorname{diag}(\overline{\beta}_1, \overline{\beta}_2, \cdots, \overline{\beta}_k)$$

can be lifted to a nonsingular matrix $(\alpha_{ij})_{1<i,\, j<k}$ *over* R_0 *such that*

(i) $\alpha_{ii} \equiv \beta_i \pmod{P_0}$ *for each* i $(1 \leq i \leq k)$, *and*

(ii) $\alpha_{ij} \equiv 0 \pmod{P_0}$ *for each* (i, j) *with* $j < i$.

Again the proof is rather straightforward, and we omit it.

We remark that by the proof of Lemma 1 the matrix (α_{ij}) defined in Lemma 2 represents a ZG-automorphism of M. Thus Lemma 2 gives us the converse to Lemma 1.

For each positive integer n, define

$$\overline{U}_\theta^{(n)} = \{s^n: s \in \overline{U}_\theta\} \quad \text{and} \quad \overline{U}_a^{(n)} = \{s^n: s \in \overline{U}_a\}.$$

THEOREM 6. *Let* [B] *be an* R_0-*ideal class such that* $[B] = [\Pi_{i=1}^{k} B_i]$. *For each* t $(1 \leq t \leq 2^{q-1})$, *let*

$$N_{t,[B]} = \sum_{i=1}^{k} {}^{\oplus}\, P^{e_i} B_i \neq 0.$$

Then for each $Z[\theta]$*-ideal class* $[C]$, *there are exactly* $(\overline{Z}^*: \overline{U}\,\overline{U}_\theta^{(k)})$ *nonisomorphic indecomposable* ZG*-extensions of* $N_{t,[B]}$ *by* C.

Proof. Let $(N_{t,[B]}, Z[\theta]; f)$ be indecomposable. By the result of (8), if $\beta = \Sigma_{i=0}^{q-1} z_i\, \theta^i$ is a unit in $Z[\theta]$, then

$$f_b(\beta \cdot 1) \equiv \sum_{i=0}^{q-2} z_i \eta^{(i)} a^i f_b(1) \pmod{PN_{t,[B]}}.$$

We may assume B_i to be relatively prime to $P_0 = P \cap R$ for each i. Furthermore, $f_b(1) = (s_1 m_1, s_2 m_2, \cdots, s_k m_k)$, where $s_i \in \overline{Z}^*$ and $m_i \in P^{e_i}$, $m_i \notin P^{e_i+1}$. We recall that σ induces the identity map on P^{e_i}/P^{e_i+1} for each i, and that a acts as the automorphism σ on $N_{t,[B]}$. Thus

$$f_b(\beta \cdot 1) \equiv \left(\sum_{i=0}^{q-2} z_i \eta^{(i)}\right) f_b(1) \pmod{PN_{t,[B]}}.$$

(Recall that $\eta = (\zeta - 1)^{1-\sigma}$ and $\eta^{(i)} = \eta^{1+\sigma+\cdots+\sigma^{i-1}} \equiv r^i \pmod{P}$.) Let $s_\beta = \Sigma_{i=0}^{q-2} z_i \eta^{(i)}$. Then

$$s_\beta \in \overline{U}_\theta, \qquad s_\beta \equiv \sum_{i=0}^{q-2} z_i r^i \pmod{P}, \qquad f_b(\beta \cdot 1) \equiv s_\beta f_b(1) \pmod{PN_{t,[B]}}.$$

Moreover, suppose $(N_{t,[B]}, Z[\theta]; g)$ is also an indecomposable extension. Then $g_b(1) = (\ell_1 m_1, \cdots, \ell_k m_k)$, where $\ell_i \in \overline{Z}^*$ for each i. By Proposition 1 the two extensions are isomorphic if and only if there exists an automorphism ϕ of $N_{t,[B]}$ such that $\phi g_b(1) - f_b(\beta \cdot 1) \in PN_{t,[B]}$. But by Lemmas 1 and 2, ϕ is a ZG-automorphism of $N_{t,[B]}$ if and only if there exist $\alpha_1, \alpha_2, \cdots, \alpha_k$ in R_0 and a unit $u \in R_0$ such that $\Pi_{i=1}^k \alpha_i \equiv u \pmod{P_0}$ and

$$\phi g_b(1) \equiv (\alpha_1 \ell_1 m_1, \alpha_2 \ell_2 m_2, \cdots, \alpha_k \ell_k m_k) \pmod{PN_{t,[B]}}.$$

Hence the two extensions are isomorphic if and only if there exist $\overline{s}_\beta \in \overline{U}_\theta$, $\overline{u} \in \overline{U}$, $\alpha_1, \alpha_2, \cdots, \alpha_k$ in R_0 such that

(I) $\overline{\alpha}_i \ell_i = \overline{s}_\beta \cdot s_i \in \overline{Z}^*$ for each i $(1 \le i \le k)$ and

(II) $\prod_{i=1}^{k} \overline{\alpha}_i = \overline{u}$.

We shall show that the above conditions are satisfied if and only if

$$\prod_{i=1}^{k} \ell_i \equiv \prod_{i=1}^{k} s_i \pmod{\overline{U} \cdot \overline{U}_\theta^{(k)}}.$$

The "only-if" part is trivial. To show the sufficiency, suppose

$$\prod_{i=1}^{k} \ell_i \equiv \prod_{i=1}^{k} s_i \pmod{\overline{U}\cdot\overline{U}^{(k)}};$$

then there exist $\bar{u} \in \overline{U}$ and $\bar{s}_\beta \in \overline{U}_\theta$ such that

$$\prod_{i=1}^{k} \ell_i = \bar{u}\cdot\bar{s}_\beta^k \prod_{i=1}^{k} s_i .$$

Let $\alpha_i \in R_0$ be such that $\overline{\alpha}_i = \bar{s}_\beta \cdot s_i \cdot \ell_i^{-1}$ for each i $(2 \leq i \leq k)$. Further, let $\alpha_1 \in R_0$ be such that

$$\overline{\alpha}_1 = \bar{u}^{-1}\cdot\left(\prod_{i=2}^{k} \overline{\alpha}_i\right)^{-1} .$$

A simple calculation shows that conditions (I) and (II) are satisfied by the choice of the α_i.

Hence we have exactly $(\overline{Z}^*: \overline{U}\cdot\overline{U}_\theta^{(k)})$ indecomposable extensions of $N_{t,[B]}$ by $Z[\theta]$.

For each ideal class [C] in $Z[\theta]$, choose C as in Proposition 3 and use the natural embedding of C in $Z[\theta]$ to get the desired result.

PROPOSITION 5. *For each* t $(1 \leq t \leq 2^q)$ *let* $N_{t,[B]} \neq 0$ *be defined as in Theorem* 6. *Then for each ideal class* [C] *in* $Z[\theta]$, *there are exactly* $(\overline{Z}^*: \overline{U}\,\overline{U}_a^{(k)})$ *nonisomorphic indecomposable* ZG-*extensions of* $N_{t,[B]}$ *by* (C, s), *where* $s \in C$ *and* $s \notin (\theta - 1)C$. (We recall that (C, s) denotes the $Z\langle a\rangle$-module C + Z such that $a(\xi, y) = (\theta\xi + s, y)$ for $\xi \in C$ and $y \in Z$.)

The proof is similar to that of Theorem 6.

Now let $n = (\overline{Z}^*: \overline{U})$, $n_\theta^{(k)} = (\overline{Z}^*: \overline{U}\cdot\overline{U}_\theta^{(k)})$, and $n_a^{(k)} = (\overline{Z}^*: \overline{U}\cdot\overline{U}_a^k)$. Let h_0 be the class number of R_0 and h' that of $Z[\theta]$. Then we observe that there are

(1) $1 + qh_0 + h'$ irreducible ZG-modules,

(2) h' indecomposable ZG-modules of the form (C, s),

(3) nh_0 indecomposables, from Proposition 4,

(4) $\sum_{k=1}^{q-1} \binom{q-1}{k} h_0 h' n_\theta^{(k)}$ indecomposables, from Theorem 6,

(5) $\sum_{k=1}^{q} \binom{q}{k} h_0 h' n_a^{(k)}$ indecomposables, from Proposition 5.

These form a complete set of nonisomorphic indecomposable ZG-modules.

For q = 2, it is easy to see that the cyclotomic units u_i,

$$\pm u_i = \pm\sqrt{(1-\zeta^i)(1-\zeta^{-i})(1-\zeta)^{-1}(1-\zeta^{-1})^{-1}} \qquad \left(0 \leq i \leq \frac{P-1}{2}\right)$$

form a complete set of representatives for $\overline{Z}^*$. Thus, in this case,

$$n = n_\theta^{(1)} = n_a^{(1)} = n_a^{(2)} = 1 .$$

Furthermore, $Z[\theta] = Z$, hence $h' = 1$. Thus, for a dihedral group G of order 2p, there are exactly $7h_0 + 3$ nonisomorphic indecomposable ZG-modules. We remark that the result of M. P. Lee [5] coincides with this special case of our result.

We refer the readers to the example given at the end of Section 4, from which we see that $\overline{Z}^*$ is not always represented by units in R_0.

PROPOSITION 6. *If* q^2 *does not divide* $(p - 1)$, *then* $n_\theta^{(k)} = n_a^{(k)} = 1$ *for each* k $(1 \leq k \leq q - 1)$.

This is proved by exhibiting enough units in R_0, $Z[\theta]$, and $Z\langle a \rangle$.

4. PROJECTIVE ZG-MODULES

Throughout this section we retain the notation of Section 3.

A ZG-module M is projective if and only if $\operatorname{Ext}^1_{ZG}(M, N) = 0$ for every ZG-module N. Let M and M' be projective modules. Define $M \sim M'$ whenever there exist free modules F and F' such that $M \oplus F \cong M' \oplus F'$. This gives an equivalence relation on the set of projective modules; the equivalence classes form an additive abelian group under direct sums, called the *projective class group* of ZG and denoted by $PCG\{ZG\}$. If M is projective, then by a result of Swan [10], $M = F \oplus I$, where F is free and I is an ideal in ZG. Thus each projective class is represented by a projective ideal I in ZG. We note that the class containing all free ZG-modules is the identity element in $PCG\{ZG\}$.

Let I be a projective ideal in ZG. Then, by a result of Swan [10], I is indecomposable, and

$$\operatorname{Rank}_Z I = \operatorname{Rank}_Z ZG .$$

Define $I_0 = \{x \in I: \Phi_p(b)x = 0\}$ and $I_1 \cong I/I_0$. Then I_0 is a projective Λ-module and

$$I_0 = \sum_{e=0}^{q-1} \oplus P^e A_e ,$$

where the A_e are ideals in R_0. By a result of M. Rosen [9, Theorem 3, Section 3, Chap. II], $A_e \neq 0$ for each e. Furthermore, I_1 is of the form (C, γ), where C is an ideal in $Z[\theta]$, $\gamma \in C$, and $\gamma \notin (\theta - 1)C$. Let $A = \Pi_{e=0}^{q-1} A_e$; then (see [9]) [A] is an invariant of I_0, and [C] is an invariant of I_1. Thus the mapping ϕ given by $\phi(I) = ([A], [C])$ is well-defined from the projective ideals of ZG to $ICG\{R_0\} \times ICG\{Z[\theta]\}$ (ICG stands for the ideal class group). Clearly, ϕ is a homomorphism on $PCG\{ZG\}$. Furthermore, by Proposition 5, ϕ is onto.

Let I be a projective ideal in ZG. Then, as we remarked before

$$I_0 \cong \sum_{e=0}^{q-1} \oplus P^e A_e \qquad \text{and} \qquad I_1 = (C, \gamma)$$

for some R_0-ideals A_e and some $Z[\theta]$-ideal C. Suppose $\phi(I)$ is the identity; then $\Pi_{e=0}^{q-1} A_e$ and C are principal ideals in R_0 and $Z[\theta]$, respectively. Hence $I \in \operatorname{Ker} \phi$ if and only if

$$I_0 \cong S \dot{+} P \dot{+} \cdots \dot{+} P^{q-1} \cong \Lambda \quad \text{and} \quad I_1 \cong Z\langle a \rangle .$$

The main object of this section is to give a necessary and sufficient condition for the homomorphism ϕ to be an isomorphism.

For each positive integer k, let $n_a^{(k)}$ be defined as in Section 2.

THEOREM 7. *The homomorphism* ϕ *is an isomorphism from* $RCG\{ZG\}$ *to* $ICG\{R_0\} \times ICG\{Z[\theta]\}$ *if and only if* $n_a^{(q)} = 1$, *that is, if and only if* $\overline{Z}^* = \overline{U} \cdot \overline{U}_a^{(q)}$.

Proof. Let $I \in PCG\{ZG\}$. Then $I \in \operatorname{Ker} \phi$ if and only if I is an indecomposable extension of Λ by $Z\langle a \rangle$. Hence ϕ is an isomorphism if and only if ZG is the unique indecomposable extension of Λ by $Z\langle a \rangle$. Thus by Proposition 5, ϕ is an isomorphism if and only if $(\overline{Z}^*: \overline{U}\, \overline{U}_a^{(q)}) = 1$. This proves the theorem.

Finally we give the following counter-example to show that $\overline{Z}^*$ is not always represented by units in R_0 and that the homomorphism ϕ is not always an isomorphism.

Example. Let q = 3, p = 7. The defining relations of the group G are $a^3 = b^7 = 1$ and $ab = b^2 a$. Let $K = Q(\zeta)$, where ζ is a primitive 7th root of unity. Then σ is the Q-automorphism of K sending ζ onto ζ^2. Let K_0 be the field of fixed elements under σ. Then $(K_0: Q) = 2$, and ± 1 are the only roots of unity in R_0, the set of algebraic integers in K_0. Furthermore, the roots of unity form a set of fundamental units in R . Hence $U = \{-1, 1\}$. But $(\overline{Z}^*: 1) = 6$, and thus $(\overline{Z}^*: \overline{U}) = 3 > 1$.

Since $(p - 1)/q = 2$, we have the relations $\overline{U}_a^{(q)} = \{\pm 1\}$ and $\overline{U} \cdot \overline{U}_a^{(q)} = \overline{U}$. Hence $(\overline{Z}^*: \overline{U} \cdot \overline{U}_a^{(q)}) = (\overline{Z}^*: \overline{U}) = 3 > 1$. This shows that ϕ in Theorem 7 is not always an isomorphism. In fact, in this case, using Proposition 6 in Section 3, we can show that there are exactly $3 + 18\, h_0$ nonisomorphic indecomposable ZG-modules.

REFERENCES

1. C. W. Curtis and I. Reiner, *Representation theory of finite groups and associative algebras*, Interscience, New York, 1962.
2. F. E. Diederichsen, *Über die Ausreduktion ganzzahliger Gruppendarstellungen bei arithmetischer Äquivalenz*, Abh. Math. Sem. Univ. Hamburg 13 (1940), 357-412.
3. D. G. Higman, *Indecomposable representations at characteristic* p. Duke Math. J. 21 (1954), 377-381.
4. A. Jones, *Groups with a finite number of indecomposable integral representations*, Michigan Math. J. 10 (1963), 257-261.
5. M. P. Lee, *Integral representations of dihedral groups of order* 2p, Trans. Amer. Math. Soc. 110 (1964), 213-231.
6. I. Reiner, *Integral representations of cyclic groups of prime order*, Proc. Amer. Math. Soc. 8 (1957), 142-146.

7. I. Reiner, *The Krull-Schmidt Theorem for integral group representations*, Bull. Amer. Math. Soc. 67 (1961), 365-367.

8. ———, *Failure of the Krull-Schmidt Theorem for integral representations*, Michigan Math. J., 9 (1962), 225-231.

9. M. Rosen, *Representations of twisted group rings*, Ph.D. thesis, Princeton University (1963).

10. R. G. Swan, *Induced representations and projective modules*, Ann. of Math. (2) 71 (1960), 552-578.

University of Illinois