INTEGRAL REPRESENTATIONS OF DIHEDRAL GROUPS OF ORDER $2p$

BY
MYRNA PIKE LEE(1)

Introduction. Information about the integral representations of finite groups has been obtained to varying extents. For Z the ring of rational integers and G the cyclic group of prime order, the ZG-modules were studied by Diederichsen [3] and Reiner [11], who showed that there were finitely many indecomposable ZG-modules and determined them completely. The finiteness of the number of indecomposables in the case where G is cyclic of order p^2 was shown, for $p = 2$, by Troy [16] and for any p by Heller and Reiner [5] and by Knee [8], while Oppenheim [10] and Knee [8] established the finiteness of the number of indecomposables for G cyclic, of square free order. Heller and Reiner [5; 6] and Jones [7] established that the number of indecomposable ZG-modules is finite if and only if all p-Sylow subgroups of G are cyclic of order at most p^2. Here, as well as throughout this paper, we shall mean by a ZG-module one which is finitely generated and Z-free.

In this paper we shall classify all finitely-generated S-free SG-modules where G is the dihedral group of order $2p$, p an odd prime, and S is Z or Z_{2p} the semi-local ring formed by the intersection of Z_p and Z_2, respectively the rings of p-integral and 2-integral elements in Q the rational field. $Z_{2p} = \{r/s \in Q: (s, 2p) = 1\}$. Taking θ to be a primitive pth root of unity, we shall denote by $K = Q(\theta)$ the cyclotomic field of degree $p-1$ over Q and by $K_0 = Q(\theta + \theta^{-1})$ the real subfield of K. R_0 and R shall be the integral closures of S in K_0 and K, respectively. Letting $\mathfrak{h}$ denote the group of automorphisms of K with fixed field K_0, we may form Λ the twisted group ring of $\mathfrak{h}$ with coefficients in R.

§1 of this paper is devoted to a characterization of R-projective Λ-modules of finite R-rank. The results of this section are then applied in the second section to show that there are precisely $7h + 3$ nonisomorphic, indecomposable SG-modules where h is the ideal class number of R_0. In §3 it is shown that although a Krull-Schmidt theorem is not obtainable for SG-modules, invariants may be obtained which determine an SG-module up to $Z_{2p}G$-isomorphism. The final section deals with projective SG-modules. Here an isomorphism is established between the projective class group of SG and the ideal class group of R_0.

Presented to the Society, February 22, 1962; received by the editors September 12, 1962.

(1) The author was supported, in part, by the Office of Naval Research while doing this research.

The author would like to express her gratitude to Professor Irving Reiner for his help and guidance during the preparation of the thesis, upon which this paper is based. The many helpful suggestions of S. Takahashi and M. Rosen are also gratefully acknowledged.

1. **Modules of the twisted group ring.** The group $\mathfrak{h}$ of automorphisms of K having fixed field K_0 is of order 2 with generator a where $a\theta = \theta^{-1}$ the complex conjugate of θ. We shall henceforth denote θ^{-1} by $\bar{\theta}$. It follows that $ax = \bar{x}$ for every $x \in K$. The twisted group ring of $\mathfrak{h}$ with coefficients in R is given by $\Lambda = R + Ra$ where $a(r_1 + r_2 a) = \bar{r}_1 a + \bar{r}_2$ for $r_1 + r_2 a \in \Lambda$.

Every Λ-module can be regarded as an R-module. We shall call a Λ-module M R-projective if M is a projective R-module.

PROPOSITION 1.1. *Every R-projective Λ-module is Λ-projective.*

Proof. Let M be any Λ-module which is R-projective. Let $\phi : R \to \Lambda$ be the natural map. Define $M_\phi = \Lambda \otimes_R M$ where $a(\lambda \otimes m) = a\lambda \otimes m$ for $\lambda \in \Lambda$, $m \in M$. Since M is R-projective, M_ϕ is Λ-projective [1, p. 30]. Consider the exact sequence of Λ-modules

$$0 \to \ker g \to M_\phi \xrightarrow{g} M \to 0 \tag{1.1}$$

where $g(\lambda \otimes m) = \lambda m$. Take $\rho = \theta/(\theta + \bar{\theta})$, a unit in R such that $\rho + \bar{\rho} = 1$ and define $f : M \to M_\phi$ by $f(m) = (1 \otimes \rho m) + (a \otimes \rho a m)$. f is a Λ-homomorphism. For any $m \in M$, $gf(m) = g(1 \otimes \rho m) + g(a \otimes \rho(am)) = \rho m + a\rho a m = \rho m + \bar{\rho} m = m$, whence the sequence (1.1) splits. It follows that M is isomorphic as a Λ-module to a direct summand of the projective Λ-module M_ϕ and is thus Λ-projective.

Any ideal I in Λ, considered as an R-module, is a submodule of the free R-module Λ. Since R is dedekind, R is an hereditary ring and I is thus R-projective. By Proposition 1.1 I is Λ-projective. This establishes

PROPOSITION 1.2. *Λ is an hereditary ring.*

It follows that every submodule of a free Λ-module is a direct sum of modules, each isomorphic to a left ideal in Λ [1, p. 13]. It remains for us to characterize the ideals in Λ.

DEFINITION. An R-ideal A in K is said to be ambiguous if and only if $A = \bar{A}$, that is, if and only if whenever $x \in A$, $\bar{x} \in A$.

Since a is the automorphism of K given by $ax = \bar{x}$ for each $x \in K$, an ambiguous ideal in K can be considered as an ideal of Λ of R-rank one under the action of a given by $ar = \bar{r}$ for $r \in A$. Conversely, any Λ-module I of R-rank one is isomorphic as an R-module to an R-ideal A in K. Since $ax \in I$ for each $x \in I$, the isomorphism is an isomorphism of Λ-modules if and only if $ar = \bar{r} \in A$ for each $r \in A$. We have thus shown

Proposition 1.3. *An ideal I in Λ has R-rank one if and only if I is Λ-isomorphic to an ambiguous R-ideal in K.*

Now assume I is any ideal in Λ having R-rank two. Consider $I^* = K_0 \otimes_{R_0} I$. I^* is a module over $\Lambda^* = K_0 \otimes_{R_0} \Lambda \cong K + Ka$, where $ax = \bar{x}a$ for $x \in K$. Since $K_0 \subset K$ is the fixed field of a, Λ^* is the crossed product algebra of K over K_0 with respect to $\mathfrak{h}$. It follows that Λ^* is a simple algebra over K_0 and, in fact, a simple ring with minimum condition. Thus any Λ^*-module is isomorphic to a direct sum of minimal left ideals of Λ^* and all minimal left ideals of Λ^* are isomorphic. In particular, if K is made a Λ^*-module by defining $(x_1 + x_2 a)x = x_1 x + x_2 \bar{x}$ where $x \in K$ and $x_1 + x_2 a \in \Lambda^*$, we see that K, being a field, is an irreducible Λ^*-module. It follows that any Λ^*-module is isomorphic to a direct sum of copies of K, that is, there exists a K-basis for I^*, (e_1, e_2), such that $I^* \cong Ke_1 \oplus Ke_2$. Let $I_2 = I \cap Ke_2$. I_2 is invariant under the action of a and is thus a Λ-submodule of I having R-rank one. By Proposition 1.3 I_2 is isomorphic to an ambiguous R-ideal in K. I/I_2, considered as the quotient of two Λ-modules, is a Λ-module of R-rank one and hence is isomorphic to an ambiguous R-ideal in K. As such it is Λ-projective. It follows that the exact sequence of Λ-modules,

$$0 \to I_2 \to I \to I/I_2 \to 0$$

splits and I/I_2 is isomorphic to a direct summand of I. Hence I is isomorphic to a direct sum of two ambiguous R-ideals in K. We have shown

Theorem 1.1. *Every ideal I in Λ is Λ-isomorphic to either an ambiguous R-ideal in K or a direct sum of two ambiguous R-ideals in K, depending on whether I has R-rank one or two.*

Let us now characterize ambiguous R-ideals in K.

Definition. Two ideals A and B in K will be called real-equivalent if and only if there exists an $\alpha \in K_0$ such that $A = B\alpha$.

Real-equivalence is an equivalence relation on the set of ambiguous R-ideals in K. We have immediately

Lemma 1.1. *Two ambiguous ideals in K yield isomorphic ideals in Λ if and only if they are real-equivalent.*

Proof. Let A and B be ambiguous R-ideals in K which are Λ-modules under the action $ax = \bar{x}$ for $x \in A$, $ay = \bar{y}$ for $y \in B$. Let ϕ be a Λ-isomorphism of A and B. Since ϕ is an R-isomorphism, it must be given by multiplication by an element $\alpha \in K$, that is, $B = A\alpha$ and $\phi(x) = x\alpha \in B$ for $x \in A$. Isomorphism as Λ-modules implies α is real since $a\phi(x) = \phi(ax)$ if and only if $\bar{x}\alpha = \overline{x\alpha}$, that is, if and only if $\alpha = \bar{\alpha}$ which implies $\alpha \in K_0$. The converse is trivial.

Since for any ideal $A \subset K$ we may find an element $z \in S \subset K_0$ such that $Az \subset R$, we may now restrict our attention to ambiguous ideals in R.

LEMMA 1.2. *An ideal in R is ambiguous if and only if it can be written in the form* $(1-\theta)^{\varepsilon}WR$ *where W is an ideal in* R_0 *and* $\varepsilon = 0$ *or* 1.

Proof. Let $A \subset R$ be an ambiguous ideal and consider its factorization into prime ideals in R. If P is a prime ideal and $P \mid A$, then $\bar{P} \mid A$, and we have the following two possibilities:

(i) $P \neq \bar{P}$. In this case P and $\bar{P}$ occur to the same exponent in the factorization of A, so that A has a factor $(\bar{P}P)^e$ for some integer $e > 0$. We can write $\bar{P}P = VR$ for some ideal $V \subset R_0$.

(ii) $P = \bar{P}$. Then since $\bar{P}P = VR$ for some ideal $V \subset R_0$, $P^2 = VR$ and V cannot have more than one type of prime ideal divisor in R_0. If V is not prime in R_0, then $V = W^2$ where $W \subset R_0$, W is a prime ideal and $P = WR$. If, on the other hand, V is prime in R_0, $VR = P^2$ implies that V ramifies from K_0 to K. The only prime which so ramifies is p, whence $P = (1-\theta)R$ and $P^2 = VR$.

Combining (i) and (ii) establishes the lemma in one direction.

Conversely, for any $Y \subset R_0$, $Y = \bar{Y}$. Then $YR = \overline{YR}$ and since $(1-\theta)/(1-\bar{\theta})$ is a unit in R, $\overline{(1-\theta)YR} = (1-\bar{\theta})YR = (1-\bar{\theta})\cdot[(1-\theta)/(1-\bar{\theta})]YR$ implies that $\overline{(1-\theta)YR} = (1-\theta)YR$.

We note that $(1-\theta)^{\varepsilon}YR$ and $(1-\theta)^{\varepsilon}XR$ are real-equivalent for $\varepsilon = 0$ or $\varepsilon = 1$ if and only if X and Y are in the same ideal class of R_0, and further that XR and $(1-\theta)YR$ are never real-equivalent for any ideals X and $Y \subset R_0$. We thus have

THEOREM 1.2. *There are precisely* $2h$ *nonisomorphic, indecomposable,* Λ*-modules of R-rank* 1. *These arise from the ambiguous ideals of R where h is the ideal class number of* R_0.

If $\{U_i : 1 \leqq i \leqq h\}$ is a complete set of representatives of the h distinct ideal classes of R_0, then $\{U_iR,\ (1-\theta)U_iR\colon 1 \leqq i \leqq h\}$ is a complete set of representatives of the classes of real-equivalent ambiguous R-ideals in K. We note we may choose the set of U_i for $i = 1, \cdots, h$ such that $U_i \dotplus U_j = R_0$ for $i \neq j$. Further, since $(1-\theta)U_iR = (\bar{\theta}-\theta)U_iR$, we may choose our $2h$ nonisomorphic, indecomposable, Λ-modules to be given by U_iR and $(\bar{\theta}-\theta)U_iR$ for $1 \leqq i \leqq h$ where $a\cdot u = \bar{u}$ for $u \in U_iR$ and $a(\bar{\theta}-\theta)u = -(\bar{\theta}-\theta)\bar{u}$ for $(\bar{\theta}-\theta)u \in (\bar{\theta}-\theta)U_iR$.

Our above remarks have already established

PROPOSITION 1.4. *If I and J are ideals in* Λ *of R-rank one, then* $I \cong (\bar{\theta}-\theta)^{\varepsilon_i}U_iR$ *and* $J \cong (\bar{\theta}-\theta)^{\varepsilon_j}U_jR$, $1 \leqq i, j \leqq h$, *where* ε_i *and* ε_j *are each either* 0 *or* 1. *I and J are* Λ*-isomorphic if and only if* $i = j$.

LEMMA 1.3. *If* U_i *and* U_j *are representatives of distinct ideal classes of* R_0, $(\bar{\theta}-\theta)^{\varepsilon_i}U_iR \dotplus (\bar{\theta}-\theta)^{\varepsilon_j}U_jR \cong (\bar{\theta}-\theta)^{\varepsilon_i}R \dotplus (\bar{\theta}-\theta)^{\varepsilon_j}U_iU_jR$ *where* ε_i *and* ε_j *may each be taken to be either* 0 *or* 1.

Proof. U_i and U_j may be chosen such that $U_i \dotplus U_j = R_0$. Then there exist

$\alpha \in U_i$ and $\beta \in U_j$ such that $\alpha + \beta = 1$. The map ϕ defined by $\phi(x,y) = (x + y, \beta x - \alpha y)$ for $(x,y) \in (\bar{\theta} - \theta)^\varepsilon U_i R \dot{+} (\bar{\theta} - \theta)^\varepsilon U_j R$ where ε is fixed as 0 or 1 is a Λ-isomorphism of $(\bar{\theta} - \theta)^\varepsilon U_i R \dot{+} (\bar{\theta} - \theta)^\varepsilon U_j R$ and $(\bar{\theta} - \theta)^\varepsilon R \dot{+} (\bar{\theta} - \theta)^\varepsilon U_i U_j R$. If $\varepsilon_i \neq \varepsilon_j$, since $(\bar{\theta} - \theta)^2 U_j$ is a member of the same ideal class of R_0 as U_j, we can choose U_i such that $U_i \dot{+} (\bar{\theta} - \theta)^2 U_j = R_0$. Then there are $\alpha \in U_i$ and $\beta \in (\bar{\theta} - \theta)^2 U_j$ such that $\alpha + \beta = 1$. The map ϕ of $U_i R \dot{+} (\bar{\theta} - \theta) U_j R$ onto $R \dot{+} (\bar{\theta} - \theta) U_i U_j R$ given by $\phi(x,y) = (x + y, \beta x - \alpha y)$ for $x \in U_i R$ and $y \in (\bar{\theta} - \theta) U_j R$ is a Λ-isomorphism of the two direct sums.

We remark at this point that if S is the semilocal ring Z_{2p}, then R_0 and R, being dedekind domains with only finitely many prime ideals, are principal ideal domains and $h = 1$. In light of this remark Lemma 1.3 is trivially true for the case where $S = Z_{2p}$.

Lemma 1.4. *If $M \cong \sum_{i=1}^n (\bar{\theta} - \theta)^{\varepsilon_i} U_i R$ where each $\varepsilon_i = 0$ or 1 and U_i is an ideal in R_0, then the class of $\prod_{i=1}^n U_i$ in R_0 is an invariant of M.*

Proof. Considering $\mathrm{Hom}_\Lambda(R,M)$ as an R_0-module, we see that $\mathrm{Hom}_\Lambda(R,M) \cong \mathfrak{A}_1 \oplus \cdots \oplus \mathfrak{A}_n$ where $\mathfrak{A}_i$, $1 \leq i \leq n$, are ideals in R_0 and the class of $\prod_{i=1}^n \mathfrak{A}_i$ in R_0 is an invariant of $\mathrm{Hom}_\Lambda(R,M)$. On the other hand, Hom is an additive functor so that

$$\mathrm{Hom}_\Lambda(R,M) \cong \sum_{i=1}^n \mathrm{Hom}_\Lambda(R,(\bar{\theta} - \theta)^{\varepsilon_i} U_i R).$$

If $f \in \mathrm{Hom}_\Lambda(R,(\bar{\theta} - \theta)^{\varepsilon_i} U_i R)$, f is determined by $f(1) \in (\bar{\theta} - \theta)^{\varepsilon_i} U_i R$. Since $af(1) = f(a \cdot 1) = f(1)$; $f(1) \in K_0$ hence $\mathrm{Hom}_\Lambda(R,(\bar{\theta} - \theta)^\varepsilon U_i R) \cong (\bar{\theta} - \theta)^\varepsilon U_i R \cap K_0$ under the mapping $f \to f(1)$. But $(\bar{\theta} - \theta)^{\varepsilon_i} U_i R \cap K_0 = \rho_i R_0 U_i$ where $\rho_i R_0$ is a principal ideal in R_0. Thus $\mathrm{Hom}_\Lambda(R,M) \cong \sum_{i=1}^n \rho_i R_0 U_i$. It follows that the class of $\prod \mathfrak{A}_i$ in R_0 is the same as the class of $\prod U_i$ in R_0 and the class of $\prod U$ in R_0 is an invariant of M.

We note that if $M = \Lambda$, $f \in \mathrm{Hom}_\Lambda(R,\Lambda)$ is determined by $f(1) = r + \bar{r}a$ for $r \in R$. The mapping $r \to r + \bar{r}a = f(1)$ is an isomorphism of $\mathrm{Hom}_\Lambda(R,\Lambda)$ and R as R_0-modules. Since $af(1) = f(a \cdot 1) = f(1)$, $\mathrm{Hom}_\Lambda(R,\Lambda) \cong R \cap K_0 = R_0$. It follows that the class of principal ideals in R_0 is an invariant of Λ, that is,

$$\Lambda \cong (\bar{\theta} - \theta)^{\varepsilon_1} R \dot{+} (\bar{\theta} - \theta)^{\varepsilon_2} R \tag{1.2}$$

where each of $\varepsilon_1, \varepsilon_2$ are 0 or 1.

It is now clear that any R-projective Λ-module of R-rank n is isomorphic as a Λ-module to a direct sum of ambiguous ideals in R of the two types $U_i R$ and $(\bar{\theta} - \theta) U_i R$. Note that if we choose basis elements e_1 and e_2 such that $ae_1 = e_1$ and $ae_2 = -e_2$, we may replace $U_i R$ and $(\bar{\theta} - \theta) U_i R$ by the modules $U_i R e_1$ and $U_i R e_2$ where a acts semi-linearly on an element of $U_i R$. The action of a considered as a semi-linear transformation on a Λ-module M having v factors of the type U_iRe_1 and $n-v$ of the type U_iRe_2 is given by the diagonal matrix $\mathbf{M} = \operatorname{diag}[I_v, -I_{n-v}]$ where I_v is the $v \times v$ identity matrix and I_{n-v} is the $n-v \times n-v$ identity matrix. We must determine when the two R-projective Λ-modules M and N are isomorphic. Clearly, since isomorphism as Λ-modules implies isomorphism as R-modules, M and N must have the same R-rank n. Lemma 1.4 tells us the class of $\prod U_{i_v}$ in R_0 is the same for M and N. Now let v and u be the numbers of summands of type U_iRe_1 in M and N, respectively. Let $\mathbf{M} = \operatorname{diag}[I_v, -I_{n-v}]$ and $\mathbf{N} = \operatorname{diag}[I_u, -I_{n-u}]$ and suppose $u \neq v$. M is Λ-isomorphic to N if and only if there exists a unimodular matrix $\mathbf{C}$ over R such that $\bar{\mathbf{C}}\mathbf{M}\mathbf{C}^{-1} = \mathbf{N}$ where $\bar{\mathbf{C}} = [\bar{\gamma}_{ij}]$ if $\mathbf{C} = [\gamma_{ij}]$. Let P be the maximal prime ideal in the local ring R_P, the integral closure of Z_p in K. $(\bar{\theta} - \theta)$ is not a unit in R_P, whence $\bar{\theta} \equiv \theta \bmod P$, and $\bar{\mathbf{C}} \equiv \mathbf{C} \bmod P$. If $\mathbf{C}$ is unimodular over R, $\mathbf{C}$ is unimodular over R_P and $\mathbf{C}\mathbf{M}\mathbf{C}^{-1} \equiv \mathbf{N} \bmod P$ where $\mathbf{C}$ is unimodular over R_P/P. But R_P/P is a field of characteristic $p \neq 2$ and such a $\mathbf{C}$ cannot exist. Hence, M is not Λ-isomorphic to N. It follows that the number of summands of M of type U_iR is an invariant.

Consolidating the results of this section we see that we have established

THEOREM 1.3. *If M is any R-projective Λ-module of R-rank n,*

$$M \cong \sum_{\nu=1}^{v} U_{i_\nu}R \dotplus \sum_{\mu=1}^{n-v} (\bar{\theta} - \theta) U_{i_\mu}R,$$

where U_{i_ν}, U_{i_μ} are ideals in R_0 and the action of a is given by conjugation. M is determined up to Λ-isomorphism by n, v, and the ideal class of $(\prod_\nu U_{i_\nu})(\prod_\mu U_{i_\mu})$ in R_0.

2. **Indecomposable SG-modules.** Let G be the dihedral group generated by a and b under the defining relations $a^2 = b^p = 1$ and $ab = b^{p-1}a$. We note that SG is the twisted group ring $S[b] + S[b]a$. Taking $\Phi_p(X)$ to be the cyclotomic polynomial of degree $p-1$ and $R = S[\theta]$, we see that the correspondence $b \to \theta$ induces an SG-isomorphism between $SG/\Phi_p(b)SG$ and $R + Ra = \Lambda$, where b acts on Λ as multiplication by θ and $a\lambda = \bar{\lambda}a$ for $\lambda \in \Lambda$.

Let M be any finitely generated, S-torsion free, SG-module. Define $M_0 = \{m \in M : \Phi_p(b)m = 0\}$. M_0 is a pure SG-submodule of M annihilated by $\Phi_p(b)$ and we can therefore consider M_0 as a Λ-module. Being a finitely generated, R-torsion free Λ-module, M_0 is Λ-projective. It follows from §1 that M_0 is Λ-isomorphic, and hence SG-isomorphic, to a direct sum of ambiguous ideals in R, $M_0 \cong A_1 \dotplus \cdots \dotplus A_n$ where $A_i = (\bar{\theta} - \theta)^\varepsilon U_iR$ for $\varepsilon = 0$ or 1 and a and b act on A_i by conjugation and multiplication by θ, respectively. M_0 is determined up to SG-isomorphism by the number of ideals of each of the two types U_iR and $(\bar{\theta} - \theta)U_jR$, and the ideal class of $\prod_{i=1}^{n} Zl_i$ in R_0.

On the other hand, since $(b-1)$ annihilates M/M_0, M/M_0 is an $S[a]$-module.

It follows from [11] that $M/M_0 \cong S^{(r)} \dotplus S'^{(s)} \dotplus L^{(t)}$, where S, S' and L are defined as SG-modules by

$$S: \quad ax = x, \; x \in S,$$
$$S': \quad \{x \in S\} \quad \text{with } ax = -x \text{ for } x \in S',$$
$$L: \quad \{(x_1e_1 + x_2e_2): \; x_i \in S\} \text{ with } ax_1e_1 = x_1e_2, \; ax_2e_2 = x_2e_1,$$

the action of b being trivial. M/M_0 is determined up to SG-isomorphism by the numbers (r), (s) and (t) of each type of summand.

It is readily seen that the problem of classifying SG-modules reduces to one of determining the extensions of $S^{(r)} \dotplus S'^{(s)} \dotplus L^{(t)}$ by $A_1 \dotplus \cdots \dotplus A_n$.

For any pair of SG-modules X and Y, we can obtain from the S-module $X \dotplus Y$, an SG-module denoted by $(X,Y;F)$ by choosing a pair of homomorphisms $F_g \in \mathrm{Hom}_S(Y,X)$ such that $g(x,y) = (gx + F_g(y), gy)$ where $g = a,b$. The pair (F_a, F_b) determine a map $F \in \mathrm{Hom}_S(SG, \mathrm{Hom}_S(Y,X))$ which will be called a binding homomorphism of X and Y. Clearly, due to the defining relations of G, an $F \in \mathrm{Hom}_S(SG, \mathrm{Hom}_S(Y,X))$ is a binding homomorphism if and only if

$$\text{(i)} \qquad aF_a(y) + F_a(ay) = 0,$$

$$\text{(2.1) (ii)} \qquad \sum_{i=0}^{p-1} b^{p-1-i}F_b(b^iy) = 0,$$

$$\text{(iii)} \qquad aF_b(y) + F_a(by) = b^{p-1}F_a(y) - b^{p-1}F_b(b^{p-1}ay),$$

for $y \in Y$. The totality of all binding homomorphisms of X and Y $B(Y,X)$ is an additive subgroup of $\mathrm{Hom}_S(SG, \mathrm{Hom}_S(Y,X))$.

Definition. If X and Y are SG-modules and F, $F' \in B(Y,X)$, we shall say F and F' are strongly equivalent, denoted by $F \approx F'$, if there exists an $E \in \mathrm{Hom}_S(Y,X)$ such that $F_g(y) - F'_g(y) = gE(y) - Eg(y)$ for all $y \in Y$, and $g \in G$. We will say F and F' are equivalent, denoted by $F \sim F'$ if $(X,Y;F) \cong_{SG} (X,Y;F')$.

Clearly, $F \approx F'$ implies $F \sim F'$. We remark further that if $(X,Y;F)$ is an SG-module with $F \approx 0$, then $(X,Y;F) \cong X \dotplus Y$ (SG-direct sum).

We refer the reader to [13] for the proof of the following

Proposition 2.1. *Let X and Y be arbitrary SG-modules and $F, F' \in B(Y,X)$. If there exist SG-isomorphisms α of X onto X and β of Y onto Y such that $\alpha F \approx F'\beta$, then $F \sim F'$. Further, if* $\mathrm{Hom}_{SG}(X,Y) = 0$, *the converse is also true.*

Strong equivalence is an equivalence relation under which $B(Y,X)$ may be partitioned into classes of strongly equivalent binding homomorphisms. These classes form an S-module customarily denoted by $\mathrm{Ext}^1_{SG}(Y,X)$. In order to determine the extensions of M/M_0 by M_0, we shall first consider separately the extensions of S, S', and L by A_i. We shall adopt the notation Hom and Ext for Hom_{SG} and Ext^1_{SG}. Further, since in considering $A_i = (\bar\theta - \theta)^e U_i R$, the class of U_i in R_0 is of no consequence, we shall merely write A_i or A_i', depending on whether $\varepsilon = 0$ or $\varepsilon = 1$. Note that for $x \in A_i$, $ax = \bar{x}$, while for $x \in A_i'$, $ax = -\bar{x}$.

Treating SG as a left SG-module we obtain the exact sequences

$$\text{(i)} \qquad 0 \to I \xrightarrow{\psi_1} SG \xrightarrow{\phi_1} S \to 0,$$

$$\text{(2.2) (ii)} \qquad 0 \to I' \xrightarrow{\psi_2} SG \xrightarrow{\phi_2} S' \to 0,$$

$$\text{(iii)} \qquad 0 \to SG(b-1) \xrightarrow{\psi_3} SG \xrightarrow{\phi_3} L \to 0.$$

(i) is obtained by taking $\phi_1 : SG \to S$ to be defined by $\phi_1(a) = \phi_1(b) = 1$. It is easily verified that $I = SG(b-1) + S(a-1)$. Taking $\phi_2(a) = -1$, $\phi_2(b) = 1$, we see that $I' = SG(b-1) + S(a+1)$. To obtain (iii) we observe that if $Y = S\Phi_p(b) + Sa\Phi_p(b)$, then $\tau(\Phi_p(b)) = e_1, \tau(a\Phi_p(b)) = e_2$ is an SG-isomorphism of Y and L. Taking $\eta : SG \to Y$ given by $\eta(z) = z\Phi_p(b)$ for $z \in SG$, we see that $SG(b-1)$ is the kernel of η and

$$0 \to SG(b-1) \xrightarrow{\psi_3} SG \xrightarrow{\eta} Y \to 0$$

is exact. We need only take $\phi_3 = \tau\eta$ to obtain (iii).

LEMMA 2.1. *There exist S-isomorphisms*
(i) $\operatorname{Ext}(S, A_i) \cong (0) \cong \operatorname{Ext}(S', A_i')$,
(ii) $\operatorname{Ext}(L, A_i) \cong A_i/(\theta - 1)A_i \cong \operatorname{Ext}(S', A_i)$,
(iii) $\operatorname{Ext}(L, A_i') \cong A_i'/(\theta - 1)A_i' = \operatorname{Ext}(S, A_i')$.

Proof. (We shall prove the lemma only for $\operatorname{Ext}(S, A_i)$ and $\operatorname{Ext}(S, A_i')$. The proofs of the other results are similar.) Since SG is a free SG-module, we obtain from (2.2) the exact sequences

$$\text{(i)} \quad \cdots \to \operatorname{Hom}(SG, A_i) \xrightarrow{\psi_1^*} \operatorname{Hom}(I, A_i) \to \operatorname{Ext}(S, A_i) \to 0,$$

$$\text{(i}'\text{)} \quad \cdots \to \operatorname{Hom}(SG, A_i') \xrightarrow{\psi_1^*} \operatorname{Hom}(I, A_i') \to \operatorname{Ext}(S, A_i') \to 0,$$

where ψ_1^* arises from the inclusion map ψ_1 in (2.2) by $(\psi_1^* f)x = f(\psi_1(x))$ for $x \in I$ and $f \in \operatorname{Hom}(SG, A_i)$ or $\operatorname{Hom}(SG, A_i')$, as the case may be. It follows that $\operatorname{Ext}(S, A_i) \cong \operatorname{Hom}(I, A_i)/$image of ψ_1^* in (i) and $\operatorname{Ext}(S, A_i') \cong \operatorname{Hom}(I, A_i)/$image of ψ_1^* in (i′). An $f \in \operatorname{Hom}(I, A_i')$ is determined by its action on $(a-1)$ and $(b-1)$. If $f(a-1) = x$ and $f(b-1) = y$ where $x, y \in A_i'$, then $(b-1)(f(a-1)) = f((b-1)(a-1))$ and $(b-1)(a-1) = [a(b^{p-2} + b^{p-3} + \dots + 1) - 1](b-1)$ imply that $(\theta - 1)x = \theta\bar{y} - y$. It follows that x depends wholly on the choice of y, enabling us to specify f by specifying $f(b-1) = y$. Further, since $y \equiv \bar{y} \bmod (1-\theta)A_i'$, we have $y(\theta - 1) \equiv 0 \bmod (1-\theta)A_i'$ and we see that our choice of y may be arbitrary in A_i'. By associating f with $f(b-1) = y$ we obtain $\operatorname{Hom}(I, A_i') \cong A_i'$. Now consider $\psi_1^*(\operatorname{Hom}(SG, A_i'))$. Certainly $\operatorname{Hom}(SG, A_i') \cong A_i'$. If $h \in \operatorname{Hom}(SG, A_i')$,

$(\psi_1^* h)(b-1) = h(b-1) = (b-1)h(1)$ and the image of ψ_1^* in (i′) is isomorphic to $(b-1)A_i'$. Since b acts as multiplication by θ, $\mathrm{Ext}(S,A_i') \cong A_i'/(\theta-1)A_i'$.

Replacing A_i' by A_i and again using the relationship $(b-1)(f(a-1)) = f((b-1)(a-1))$ for $f \in \mathrm{Hom}(I,A_i)$, we obtain $(\theta-1)x = -\theta\bar{y} - y$. Then $y(1+\theta) \equiv 0 \bmod (\theta-1)A_i$ from which it follows that $y \in (\theta-1)A_i$ and $\mathrm{Hom}(I,A_i) \cong (\theta-1)A_i$. Thus $\mathrm{Ext}(S,A_i) \cong (\theta-1)A_i/(\theta-1)A_i \cong (0)$.

Since $A_i'/(\theta-1)A_i' \cong A_i/(\theta-1)A_i \cong S/pS$, we see that the number of extensions of S, S' or L by A_i or A_i' is, in all cases, either 1 or p. If there is only one extension we have a decomposable SG-module. In the case where the number of extensions is p, taking representatives of $A_i'/(\theta-1)A_i'$ to be given by $\{jn_0 : 0 \leqq j \leqq p-1,\ n_0 \in A_i', n_0 \notin (\theta-1)A_i'\}$, we shall denote the representatives of the p inequivalent classes of binding homomorphisms so obtained by $F^{(j)}$, $j = 0,\cdots,p-1$. We now consider $(A_i',S;F^{(j)})$ for $j=0,\cdots,p-1$. An $F \in B(S,A_i')$ is determined by the action of the pair (F_a,F_b) on $1 \in S$. From (2.1(iii)) and the defined actions of a and b on S and A_i', we have $\overline{-F_b(1)} + \bar{\theta}F_b(1) = (\bar{\theta}-1)F_a(1)$. It follows that $F_a(1)$ and hence F_1 is determined by $F_b(1)$. We shall choose $F_b^{(j)}(1) = jn_0$ for $j=0,\cdots,p-1$ and show that $F^{(j)} \sim F^{(1)}$ for $0 \leqq j \leqq p-1$. Both S and A_i' are irreducible SG-modules, hence $\mathrm{Hom}(S,A_i') = 0$ and, by Proposition 2.1, we need only find SG-automorphisms α and β of A_i' and S such that $\alpha F^{(1)} \approx F^{(j)}\beta$. This will be the case if and only if $(\alpha F^{(1)} - F^{(j)}\beta)(1) \in (\theta-1)A_i'$. Take β to be the identity automorphism of S and α to be left multiplication by the $u = (x\bar{x})^{1/2}$ with $x = (\theta^j - 1)/(\theta-1)$ so that u is a unit of R_0 and hence of R. Then $\alpha F_b^{(1)}(1) - F_b^{(j)}\beta(1) = (u-j)n_0$ which, since $u \equiv \bmod(\theta-1)$ implies that $(u-j)n_0 \in (\theta-1)A_i'$ for $0 < j \leqq p-1$. It follows that there exists up to isomorphism at most one indecomposable module arising from an extension of S by A_i'.

To establish that $(A_i',S;\ F^{(1)})$ is indeed indecomposable we note that by Proposition 2.1 if $F^{(1)} \sim F^{(0)}$ there would exist SG-automorphisms α and β of A_i' and S such that $(\alpha F_b^{(1)} - F_b^{(0)}\beta)(1) \in (\theta-1)A_i'$. But $F^{(0)} \approx (0)$ implies that $\alpha(n_0) \in (\theta-1)A_i'$. Since α must be multiplication by a unit of R, $n_0 \in (\theta-1)A_i'$ a contradiction of our original choice of $F^{(1)}$. We have shown

PROPOSITION 2.2. *There exists one indecomposable SG-module arising from an extension of S by* A_i'. *This module, denoted by* $(A_i',S;F)$, *is defined by* $\{(x,y): x \in A_i', y \in S\}$ *where the action of G is given by* $a(x,y) = (\bar{x} + F_a(y), y)$, $b(x,y) = (\theta x + F_b(y), y)$.

$$F_b(y) = yn_0,\ F_a(y) = y(-\bar{n}_0 + \bar{\theta}n_0)/(\bar{\theta}-1) \ \textit{for}\ n_0 \in A_i',\ n_0 \notin (\theta-1)A_i'.$$

In a similar manner, employing the same automorphisms α and β, we can show the existence of precisely one indecomposable SG-module of each of the types $(A_i,S';F)$, $(A_i,L;F)$ and $(A_i',L;F)$. In the case of the last two types we need only note the class of $F^{(j)}$, $0 \leqq j \leqq p-1$, in $B(L,A_i)$ or $B(L,A_i')$ under strong equivalence is uniquely determined by $(F_a^{(j)}(e_1), F_b^{(j)}(e_2)) = (jn_0, jn_0)$ where $n_0 \in A_i$, $n_0 \notin (\theta - 1)A_i$ and $n_0 \notin P_i$ for any prime ideal factor P_i of $2R$. In view of the existence of only one indecomposable module for each extension of S, S' or L by A_i or A_i', we shall hereafter drop the F and refer to the nontrivial extension only by the pair of modules involved.

We shall now determine the extensions of M/M_0 by M_0 which yield indecomposable SG-modules M. Note that if M is any finitely generated Z-free ZG-module, we can form the associated $Z_{2p}G$-module $M_{2p} = Z_{2p} \otimes_Z M$. When $S = Z_{2p}$, the class number h of R_0 is one and $A_i = R$, $A_i' = (\bar{\theta} - \theta)R = R'$ for $1 \leqq i \leqq h$. In this case M_0 simplifies to the form $R^{(u)} \dotplus R'^{(v)}$. Since a theorem due to Reiner [14] tells us that M is a decomposable ZG-module if and only if M_{2p} is decomposable as a $Z_{2p}G$-module, we shall for the remainder of this section, except where it is expressly stated to the contrary, assume $S = Z_{2p}$.

Let M be an indecomposable SG-module. M is the extension of $S^{(s)} \dotplus S'^{(t)} \dotplus L^{(w)}$ by $R^{(u)} \dotplus R'^{(v)}$. Since M is indecomposable, we cannot have all of (s), (t), and (w) equal to 0 unless one of (u) and (v) is 0 and the other is 1. Similarly if $(v) = (u) = 0$ one and only one of (s), (t) and (w) is equal to 1 and the other two are 0. Assuming now that neither all of (s), (t) and (w) nor all of (u) and (v) are 0, we have

Case 1. $w \neq 0$. There are two subcases: (i) $s = t = 0$ and (ii) either one or both of s and t are nonzero.

(i) If $s = t = 0$, M arises from the extension of $L^{(w)}$ by $R^{(u)} \dotplus R'^{(v)}$. Letting $\sum_{i=1}^{w} SGx_i$ be a free SG-module with basis $\{x_1, \cdots, x_w\}$, and adding w copies of the exact sequence (2.2.(iii)), we obtain the exact sequence

$$0 \to \sum_{i=1}^{w} SG(b-1)x_i \xrightarrow{\tau} \sum_{i=1}^{w} SGx_i \to \sum_{i=1}^{w} Lx_i \to 0.$$

Then $\mathrm{Ext}(L^{(w)}, R^{(u)} \dotplus R'^{(v)}) \cong \mathrm{Hom}(\sum SG(b-1)x_i, R^{(u)} \dotplus R'^{(v)})/\text{image of } \tau^*$. Let $\{a_1, \cdots, a_u\}$ and $\{b_1, \cdots, b_v\}$ be bases for $R^{(u)}$ and $R'^{(v)}$ respectively such that $R^{(u)} = Ra_1 \oplus \cdots \oplus Ra_u$ and $R'^{(v)} = R'b_1 \oplus \cdots \oplus R'b_v$. An

$$F \in \mathrm{Hom}(\sum SG(b-1)x_i, R^{(u)} \dotplus R'^{(v)})$$

is given by

$$F((b-1)x_i) = \sum_{j=1}^{u} r_{ji}a_j + \sum_{k=1}^{v} r'_{ki}b_k, \qquad 1 \leqq i \leqq w,\ r_{ji} \in R,\ r'_{ki} \in R'.$$

The class of F in $\mathrm{Ext}(L^{(w)}, R^{(u)} \dotplus R'^{(v)})$ corresponds to a pair of matrices $F_\rho = (\rho_{ji})$ and $F'_\rho = (\rho'_{ki})$ where the entries ρ_{ji} and ρ'_{ki} are in $\mathrm{Ext}(L,R)$ and $\mathrm{Ext}(L,R')$, respectively. In particular, since there is, up to isomorphism, only one indecomposable module arising from each extension, ρ_{ji} and ρ'_{ki} can be taken to be either 0 or 1.

A change of basis of $R^{(u)}$, leaving a_j fixed for some $j \neq 1$ and replacing a_1

by $a_1 - \lambda a_j$, will replace ρ_{ji} by $(\rho_{ji} - \lambda\rho_{1i})$, $1 \leqq i \leqq w$. On the other hand, since, a change of basis of $L^{(w)}$ leaving $x_1, x_3, \cdots, x_w$ unchanged, but replacing x_2 by $x_2 - \lambda x_1$, replaces $(b-1)x_2$ by $(b-1)x_2 - \lambda(b-1)x_1$ and hence ρ_{j2} and ρ'_{k2} by $\rho_{j2} - \lambda\rho_{j1}$ and $\rho'_{k2} - \lambda\rho'_{k1}$, respectively. We will identify F with its class in $\operatorname{Ext}(L^{(w)}, R^{(u)} \dotplus R'^{(v)})$ and speak of $F(x_i)$ rather than $F((b-1)x_i)$.

Consider first the $(u \times w)$ matrix $F_\rho = (\rho_{ji})$. There must be a nonzero element $\rho_{1i} = 1$ in the first row of F_ρ, since otherwise a factor of Ra_1 would split off and M would be decomposable. Renumber the basis elements of $L^{(w)}$ if necessary, to place this element in the $(1,1)$ position. We may assume hereafter $\rho_{11} = 1$. A change of basis of $R^{(u)}$ which results in replacing ρ_{j1} by $\rho_{j1} - \lambda\rho_{11}$ where $\lambda = \rho_{j1}$ is either 1 or 0 for $2 \leqq j \leqq u$ can be performed. F_ρ now will have all entries in its first column, with the exception of ρ_{11}, equal to 0. By changing the basis of $L^{(w)}$ we may now make the $(1,2), \cdots, (1,w)$ entries 0. Repeating this process we may diagonalize F_ρ to obtain $F_\rho = \operatorname{diag}[I_m, 0]$. If $m < u$, a factor $Ra_{m+1} \oplus \cdots \oplus Ra_u$ would be a direct summand of M, contradicting the indecomposability of M. Therefore, we may assume $m = u$, and

$$(2.3)\qquad \begin{aligned} F(x_i) &= a_i + \sum_{k=1}^{v} \rho'_{ki} b_k, \qquad 1 \leqq i \leqq u, \\ F(x_i) &= \sum_{k=1}^{v} \rho'_{ki} b_k, \qquad u+1 \leqq i \leqq w. \end{aligned}$$

We note that although the diagonalization process will change the values o coefficients of the b_k's, these coefficients are elements of $\operatorname{Ext}(L, R')$ and, as such, may be taken to be 0 and 1; thus we retain the notation ρ'_{ki} for these coefficients

Now consider $F_{\rho'}$. If $v = 0$ (2.3) tells us that $M = (R, L)^{(u)} \oplus L^{(w-u)}$ contradicting the indecomposability of M. Thus assume $v \neq 0$. There exists a nonzero entry in the last column of $F_{\rho'}$ since otherwise L or (R, L) would be a direct summand of M, depending on whether $u < w$ or $u = w$. We may renumber the basis elements $b_1, \cdots, b_v$ such that $\rho'_{1w} = 1$. A change of basis of $R'^{(v)}$, replacing b_1 by $b_1 - \lambda b_k$ where $\lambda = \rho'_{kw}$, $2 \leqq k \leqq v$ will reduce the entries of the last column of $F_{\rho'}$ to 0 for $2 \leqq k \leqq v$, that is, $F(x_w) = \delta_{uw} a_u + b_1$ where $\delta_{uw} = 0$ if $u < w$, $\delta_{uw} = 1$ if $u = w$. A change of basis of $L^{(w)}$, replacing x_i by $(x_i - \rho'_{1w} x_w)$ for $1 \leqq i \leqq w - 1$ will give us

$$(2.4)\qquad \begin{aligned} F(x_i) &= a_i - \delta_{uw}\rho'_{1i} a_u + \sum_{k=2}^{v} \rho'_{ki} b_k, \qquad 1 \leqq i \leqq u, \\ F(x_i) &= \delta_{uw}\rho'_{1i} a_u + \sum_{k=2}^{v} \rho'_{ki} b_k, \qquad u+1 \leqq i \leqq w-1. \\ F(x_w) &= \delta_{uw} a_u + b_1. \end{aligned}$$

If $u \neq w$, $\delta_{uw} = 0$ and (2.4) becomes

$$F(x_i) = a_i + \sum_{k=2}^{v} \rho'_{ki} b_k, \qquad 1 \leqq i \leqq u,$$

$$F(x_i) = \sum_{k=2}^{v} \rho'_{ki} b_k, \qquad u+1 \leqq i \leqq w-1,$$

$$F(x_w) = b_1,$$

whence a factor (R', L) is a direct summand of M. If $u = w$, $\delta_{uw} = 1$ and (2.4) is given by

$$F(x_i) = a_i - \rho'_{1i} a_n + \sum_{k=2}^{v} \rho'_{ki} b_k, \qquad 1 \leqq i \leqq w-1,$$

$$F(x_w) = aw + b_1.$$

Replacing a_i by $a'_i = a_i - \rho'_{1i} a_n$ for $1 \leqq i \leqq n-1$ and taking $a'_n = a_n$ we finally obtain

$$F(x_i) = a'_i + \sum_{k=2}^{v} \rho'_{ki} b_k, \qquad 1 \leqq i \leqq w-1,$$

$$F(x_w) = a'_n + b_1$$

whence $(L, R \dotplus R')$ is a direct factor of M. In either case M is now decomposable. Thus if M is an indecomposable module obtained by an extension of $L^{(w)}$ by $R^{(u)} \dotplus R'^{(v)}$, we have $\max(u, v, w) = 1$. We have already seen M is indecomposable if $w = 1$ and one or both of u, v are equal to 0; or if $w = 0$ and one of u and v is 0. That M is indecomposable when $u = v = w = 1$ follows from the indecomposability of the group ring (cf. [15]) and the fact that SG has S-rank $2p$.

(ii) If $w \neq 0$ and one or both of s and t is nonzero, then M is an extension of $S^{(s)} \dotplus S'^{(t)} \dotplus L^{(w)}$ by $R^{(u)} \dotplus R'^{(v)}$. Noting that by Lemma 2.1 $\mathrm{Ext}(S, R) = \mathrm{Ext}(S', R') = 0$, we see that the class of an $F \in \mathrm{Ext}(S^{(s)} \dotplus S'^{(t)} \dotplus L^{(w)}, R^{(u)} \dotplus R'^{(v)})$ is determined by the four matrices

$$(2.5) \qquad \begin{aligned} F_\tau &= (\tau_{ij})_{(u \times t)}, \\ F_{\tau'} &= (\tau'_{ij})_{(v \times s)}, \\ F_\rho &= (\rho_{ij})_{(u \times w)}, \\ F_{\rho'} &= (\rho'_{ij})_{(v \times w)} \end{aligned}$$

with entries in $\mathrm{Ext}(S', R)$, $\mathrm{Ext}(S, R')$, $\mathrm{Ext}(L, R)$ and $\mathrm{Ext}(L, R')$, respectively. In particular, these entries may be taken to be 0 or 1.

We suppose first that M is the indecomposable module arising from an extension of $S \oplus L$ by R'. The matrix representation of M has the form

$$\begin{bmatrix} R' & 1 & 1 \\ & S & 0 \\ & & L \end{bmatrix}.$$

But L is the extension of S' by S [11] whence, noting that Ext $(S', R') = 0$, it follows after suitable manipulation of bases that M is determined by the two matrices $F = (\tau'_{ij}), i = 1, j = 1,2$ and $E = (\rho'_{11})$ with nonzero entries in $\mathrm{Ext}_{SG}(S, R')$ and $\mathrm{Ext}_{S[a]}(S', S)$, respectively; that is, M now has a representation of the form

$$\begin{bmatrix} R' & 1 & 1 & 0 \\ & S & 0 & 0 \\ & & S & 1 \\ & & & S' \end{bmatrix}$$

and F is the matrix corresponding to an extension of $S^{(2)}$ by R'. If $S^{(2)} = Sz_1 \oplus Sz_2$ and $R' = R'b_1$, $F(z_1) = b_1$ and $F(z_2) = b_1$. A change of bases to z'_i where $z'_1 = z_1$ and $z'_2 = z_2 - z_1$ makes $F = (1\ 0)$ whence M becomes $(R', S) \oplus L$. A similar argument will show that the extension of $S' \oplus L$ by R cannot be indecomposable. To return to the more general situation we suppose we have the four matrices indicated in (2.5). Let the bases for $R^{(u)}$, $R'^{(v)}$ and $L^{(w)}$ be as in (i) and take $S^{(s)} = Sy_1 \oplus \cdots \oplus Sy_s$. Then identifying maps with matrices

$$(2.6)\qquad \begin{aligned} F(y_l) &= \sum_{k=1}^{v} \tau'_{kl} b_k, & 1 \leqq l \leqq s, \\ F(x_j) &= \sum_{i=1}^{u} \rho_{ij} a_i + \sum_{k=1}^{v} \rho'_{kj} b_k, & 1 \leqq j \leqq w. \end{aligned}$$

There exists a nonzero element $\tau'_{k1} = 1$ in the first column of $F_{\tau'}$ since otherwise Sy_1 would be a direct summand of M. Renumbering the b_k such that $\tau'_{11} = 1$ and using the same process as in (i), we may diagonalize $F_{\tau'}$ to obtain, $F(y_l) = b_l$ for $1 \leqq l \leqq m$. If $m < s$, $Sy_{m+1} \oplus \cdots \oplus Sy_s$ would be a direct summand of M. We may therefore assume $m = s$. (2.6) becomes

$$F(y_l) = b_l, \qquad 1 \leqq l \leqq s, \qquad s \leqq v,$$

$$F(x_j) = \sum_{k=1}^{v} \rho'_{kj} b_k + \sum_{i=1}^{u} \rho_{ij} a_i, \qquad 1 \leqq j \leqq w.$$

We note as in (i) that although ρ'_{kj} may change under the diagonalization the values remain 0 or 1. Now consider $F_{\rho'}$. Again the absence of a nonzero element $\rho'_{1k} = 1$ in the first row would cause $(R'b_1, Sy_1)$ to be a direct summand of M.

Renumbering the x_j, if necessary, we place ρ'_{1k} in the $(1,w)$ position. Fixing x_w and replacing x_j by $x_j - \rho_{1j}x_w$ for $1 \leqq j \leqq w-1$, we obtain

$$F(y_l) = b_l,$$

$$F(x_j) = \sum_{k=2}^{v} \rho'_{kj}b_k + \sum_{i=1}^{u} \rho_{ij}a_i, \qquad 1 \leqq j \leqq w-1,$$

$$F(x_w) = b_1 + \sum_{k=2}^{v} \rho_{kw}b_k + \sum_{i=1}^{u} \rho_{iw}a_i.$$

Thus an extension of $S \oplus L$ by R' appears in M. As we have already seen, we may then split off (R', S), making M decomposable.

Case 2, $w = 0$. Then M is an extension of $S^{(s)} \dotplus S'^{(t)}$ by $R^{(u)} \dotplus R'^{(v)}$.

The class of an $F \in \operatorname{Ext}(S^{(s)} \dotplus S'^{(t)}, R^{(u)} \dotplus R'^{(v)})$ is seen to be given by a pair of matrices $F_\tau = (\tau_{ij})$ and $F_{\tau'} = (\tau'_{ij})$ where $\tau_{ij} \in \operatorname{Ext}(S, R')$ and $\tau'_{ij} \in \operatorname{Ext}(S', R)$. Use of the methods in Case 1 quickly results in the diagonalization of both of these matrices to obtain the result that M is decomposable.

Allowing S to be Z or Z_{2p} and returning to the notation $A'_i = (\bar\theta - \theta)U_iR$ $A_i = U_iR$ where U_i is a representative of an ideal class of R_0, we see we have established the existence of five types of indecomposable SG-modules arising from nontrivial extensions of M/M_0 by M_0:

(2.7) (U_iR, S'), (U_iR, L), $((\bar\theta - \theta)U_iR, S)$, $((\bar\theta - \theta)U_iR, L)$, $(R \dotplus (\bar\theta - \theta)U_jR, L)$.

We can now state the following

Proposition 2.3. *There exist h nonisomorphic, indecomposable, SG-modules of each of the five types listed in* (2.7). *These are obtained by allowing U_i to range through the complete set of representatives of the h ideal classes of R_0.*

Proof. The existence of isomorphisms $(U_iR, S') \cong (U_jR, S')$, $((\bar\theta - \theta)U_iR, S) \cong ((\bar\theta - \theta)U_jR, S)$ or $((\bar\theta - \theta)^\varepsilon U_iR, L) \cong ((\bar\theta - \theta)^\varepsilon U_jR, L)$ for $\varepsilon = 0$ or 1 would imply by Proposition 2.1 the existence of SG-isomorphisms and hence of Λ-isomorphisms of $(\bar\theta - \theta)^\varepsilon U_iR$ and $(\bar\theta - \theta)^\varepsilon U_jR$ for $\varepsilon = 0$ or 1. We have noted in §1 that such isomorphisms will exist if and only if U_i and U_j are in the same ideal class of R_0. Similarly, if $(R \dotplus (\bar\theta - \theta)U_iR, L) \cong (R \dotplus (\bar\theta - \theta)U_jR, L)$ where U_i and U_j are in distinct ideal classes of R_0, we have a Λ-isomorphism of $R \dotplus (\bar\theta - \theta)U_iR$ and $R \dotplus (\bar\theta - \theta)U_jR$. Lemma 1.4 tells us that this is impossible. We now have

Theorem 2.1. *There exist precisely $7h + 3$ nonisomorphic, indecomposable, SG-modules where h is the ideal class number of R_0. If $\{U_i : i = 1, \cdots, h\}$ is a full set of representatives of ideal classes of R_0, h of these indecomposables come from each of the following types of modules*: U_iR, $(\bar\theta - \theta)U_iR$, (U_iR, S'),

$((\bar\theta-\theta)U_iR,S)$, (U_iR,L), $((\bar\theta-\theta)U_iR,L)$ and $(R\dotplus(\bar\theta-\theta)U_iR,L)$, by taking $i=1,\cdots,h$. The additional three modules are S, S' and L.

3. **Nonuniqueness of decomposition.** The decomposition of an SG-module, into indecomposables is certainly nonunique in the case where $S=Z$ and $h\neq 1$ since here we already have by Lemma 1.3

$$U_iR\dotplus U_jR\cong R\dotplus U_iU_jR.$$

Let us therefore consider the situation which occurs when $S=Z_{2p}$. Since $h=1$, there exists only one ideal class of R_0 so that nonuniqueness is not immediate.

If M is any SG-module, we may form the associated Z_pG and Z_2G-modules $M_p=Z_p\otimes_S M$ and $M_2=Z_2\otimes_S M$, respectively. For any two SG-modules M and M', $M\cong M'$ if and only if $M_p\cong M'_p$ and $M_2\cong M'_2$.

Under extension of the ground ring from S to Z_p, L decomposes into the direct sum $Z_p\oplus Z'_p$ and it follows that $(R,L)_p\cong(R_p,Z_p)\oplus Z'_p$, $(R',L)_p\cong(R'_p,Z_p)\oplus Z'_p$ and $(R\dotplus R',L)_p\cong(R_p,Z'_p)\oplus(R_p,Z'_p)$. In extending S to Z_2, we find that although Z_2, Z'_2, L_2, R_2 and R'_2 remain indecomposable, in each case our extensions of Z_2, Z'_2 and L_2 by R_2 and R'_2 split into direct sums of the modules involved. Thus if M is an SG-module which has the decomposition $M\cong(R,L)\oplus(R',L)$ and M' is an SG-module having the decomposition $M'\cong L\oplus(R\dotplus R',L)$,

$$M_p\cong(R_p,Z'_p)\oplus Z_p\oplus(R'_p,Z_p)\oplus Z'_p\cong M'_p$$

and

$$M_2\cong R_2\oplus L_2\oplus R'_2\oplus L_2\cong M'_2,$$

whence $M\cong M'$ as SG-modules.

Although the decomposition of SG-modules into sums of indecomposables does not even preserve the S-rank of the summands, we may still obtain certain invariants for a direct sum decomposition. We shall make use of

THEOREM 3.1 (KRULL-SCHMIDT). *In any decomposition of a Z_pG-module M_p into a direct sum of indecomposables, the indecomposable summands are uniquely determined by M_p up to Z_pG-isomorphism and order of occurrence.*

Proof. Let Q^* denote the p-adic completion of Q and Z^* the ring of integral elements in Q^*. For any Z_pG-module M_p, we may form the associated Z^*G-module $M_p^*=Z^*\otimes_{Z_p}M_p$. We have (Maranda [9]; see also [2]).

(3.1) $M_p^*\cong M_p'^*$ as Z^*G-modules if and only if $M_p\cong M'_p$ as Z_pG-modules.

Further, since QR_p, QZ_p, QR'_p and QZ'_p are irreducible QG-modules which remain irreducible under extension to Q^*G-modules, a theorem due to Heller [4] tells us that M_p is decomposable if and only if M_p^* is decomposable as a Z^*G-module, The Krull-Schmidt theorem holds for Z^*G-modules (see [12]). The result now follows from (3.1).

Now consider the following chart, which shall represent a direct sum decomposition of M. The left-hand column gives the number of summands of each type of indecomposable SG-module appearing in the decomposition. The two columns on the right are corresponding decompositions for M_p and M_2.

Number of Summands	M	M_p	M_2
s_1	S	Z_p	Z_2
s_2	S'	Z'_p	Z'_2
l	L	$Z_p \oplus Z'_p$	L_2
r_1	R	R_p	R_2
r_2	R'	R'_p	R'_2
u_1	(R,S')	(R_p,Z'_p)	$R_2 \oplus Z'_2$
u_2	(R',S)	(R'_p,Z_p)	$R'_2 \oplus Z_2$
v_1	(R,L)	$(R_p,Z'_p) \oplus Z_p$	$R_2 \oplus L_2$
v_2	(R',L)	$(R'_p,Z_p) \oplus Z'_p$	$R'_2 \oplus L_2$
t	$(R \dotplus R',L)$	$(R_p,Z'_p) \oplus (R'_p,Z_p)$	$R_2 \oplus R'_2 \oplus L_2$

Theorem 3.1 tells us that the number of various types of indecomposable summands in a decomposition of M_p is invariant. We thus have as invariants for M_p and hence for M

$$s_1 + l + v_1,\ s_2 + l + v_2,\ r_1,\ r_2,\ u_1 + v_1 + t,\ u_2 + v_2 + t.$$

From the structure of M/M_0 as an $S[a]$-module, we see that the total number each of S, S' and L appearing in summands of M is also an invariant of M, whence we have the additional invariants $s_1 + u_2$ and $s_2 + u_1$. It is a simple exercise to verify that these eight invariants determine M up to SG-isomorphism if $S = Z_{2p}$. We can now easily show, taking S to be either Z or Z_{2p},

THEOREM 3.2. *Any finitely generated, S-free, SG-module M can be written*

$$M \cong S^{(s_1)} \dotplus S'^{(s_2)} \dotplus L^{(l)} \dotplus (U_{i_\delta}R)^{(r_1)} \dotplus ((\bar\theta - \theta)U_{i_\varepsilon}R^{(r_2)} \dotplus (U_{i_\zeta}R,S')^{(u_1)}$$
$$\dotplus\ ((\bar\theta - \theta)U_{i_\eta}R,S)^{(u_2)} \dotplus (U_{i_\lambda}R,L)^{(v_1)} \dotplus ((\bar\theta - \theta)U_{i_\mu}R,L)^{(v_2)}$$
$$\dotplus\ (R \dotplus (\bar\theta - \theta)U_{i_\nu}R,L)^{(t)},$$

where $1 \leqq i \leqq h$, *and the invariants*: $s_1 + l + v_1$, $s_2 + l + v_2$, $u_1 + v_1 + t$, $u_2 + v_2 + t$, $s_2 + u_1$, $s_1 + u_2$, r_1, r_2, *and the ideal class of*

$$(\prod_{\delta} U_{i_\delta})(\prod_{\varepsilon} U_{i_\varepsilon})(\prod_{\eta} U_{i_\eta})(\prod_{\zeta} U_{i_\zeta})(\prod_{\lambda} U_{i_\lambda})(\prod_{\mu} U_{i_\mu})(\prod_{\nu} U_{i_\nu})$$

in R_0 determine M up to $Z_{2p}G$-isomorphism.

4. **The group ring and projective modules.** SG considered as a left SG-module is indecomposable [15] of S rank $2p$ and hence must be a module of the form $(R \dot{+} (\bar{\theta} - \theta)U_iR, L)$. It is necessary only to determine the class of U_i in R_0. Since $SG/\Phi_p(b)SG \cong \Lambda$, we see that $\Lambda \cong R \dot{+} (\bar{\theta} - \theta)U_iR$.

In §1 (1.2) we remarked that the class of ideals in R_0 which is an invariant of Λ is the class of principal ideals in R_0. It follows immediately that $SG \cong (R \dot{+} (\bar{\theta} - \theta)R, L)$.

To simplify the notation throughout the rest of this section, we shall denote $R \dot{+} (\bar{\theta} - \theta)U_iR$ by M_i for $1 \leqq i \leqq h$, having renumbered the U_i, if necessary, such that the ideal class of U_1, $[U_1] = [R_0]$ the class of principal ideals in R_0. Thus $R \dot{+} (\bar{\theta} - \theta)R = M_i$. We shall denote $(R \dot{+} (\bar{\theta} - \theta)U_i, L)$, that is, (M_i, L), by X_i for $1 \leqq i \leqq h$. M_{ij} will be used to indicate $R \dot{+} (\bar{\theta} - \theta)U_iU_jR$ and $X_{ij} = (M_{ij}, L)$.

Let $\mathscr{F}$ denote the class of all finitely generated, free SG-modules and let $\mathscr{P}$ be the class of all finitely generated, projective SG-modules. Then $\mathscr{F} \subset \mathscr{P}$, and we may define an equivalence relation on $\mathscr{P}$ as follows:

Definition. P_1 and P_2 in $\mathscr{P}$ are equivalent if and only if there exist F_1 and F_2 in $\mathscr{F}$ such that $P_1 \dot{+} F_1 \cong P_2 \dot{+} F_2$, as SG-modules.

We shall denote the equivalence class of P in $\mathscr{P}$ by $\{P\}$. By $\{0\}$ we shall mean the set of all $P \in \mathscr{P}$ such that $P \dot{+} F \in \mathscr{F}$ for some $F \in \mathscr{F}$; and by $-\{P\}$, the class of all $P' \in \mathscr{P}_\rho$ such that $P \dot{+} P' \in \mathscr{F}$. The set of classes of $\mathscr{P}$ under this relation form a group called the projective class group. We have

Theorem 4.1. (*Swan* [15]; *see also* [2].) *If P is a projective SG-module, P can be written $P = P_0 \dot{+} F$ where F is a free SG-module and P_0 is a projective ideal of SG.*

If P_0 is a projective ideal of SG, $QP_0 \cong QG$. Then P_0 must have S-rank $2p$. The h nonisomorphic left ideals of SG, X_i, $1 \leqq i \leqq h$, constitute a complete set of indecomposable SG-modules having S-rank $2p$. We shall show each X_i to be a projective ideal of SG.

X_i is projective if and only if $\mathrm{Ext}(X_i, A) = 0$ for each SG-module A. $\mathrm{Ext}(X_i, A) = 0$ if and only if $Z_q \otimes_S \mathrm{Ext}(X_i, A) = 0$ for each prime $q \mid [G:1]$.

But $Z_q \otimes_S X_i \cong Z_qG$ and $\mathrm{Ext}_{Z_qG}(Z_qG, Z_qA) = 0$ whence, since $Z_q \otimes_S \mathrm{Ext}(X_i, A) \cong \mathrm{Ext}_{Z_qG}(Z_q \otimes_S X_i, Z_q \otimes_S A)$, it follows that X_i is projective.

Lemma 4.1. *$X_i \dot{+} X_j \cong X_1 \dot{+} X_{ij}$ for $1 \leqq i, j \leqq h$.*

Proof. If $X_i = (M_i, L;\ F^{(i)})$ and $X_j = (M_j, L;\ F^{(j)})$ where $F^{(i)} \in B(L, M_i)$ and $F^{(j)} \in B(L, M_j)$, then

$$X_i \dotplus X_j \cong (M_i \dotplus M_j,\ L \dotplus L; F)$$

where $F_g(l_1,l_2) = (F_g^{(i)}(l_1), F_g^{(j)}(l_2))$ defines an $F \in B(L \dotplus L, M_i \dotplus M_j)$. The map ϕ of $M_i \dotplus M_j$ onto $M_1 \dotplus M_{ij}$ given by

$$\phi((r_1,m_i),(r_2,m_j)) = ((r_1, m_i + m_j),\ (r_2, \alpha m_i - \beta m_j)),$$

where $(r_1,m_i) \in M_i$ and $(r_2,m_j) \in M_j$ and α and β are elements of U_i and U_j, respectively, chosen so that $\alpha + \beta = 1$, is an SG-isomorphism. It follows that the map ψ of $(M_i \dotplus M\ , L \dotplus L; F)$ onto $(M_1 \dotplus M_{ij}, L \dotplus L;\ F')$ given by $\psi(M_i \dotplus M_j, L \dotplus L; F) = (\phi(M_i \dotplus M_j), L \dotplus L;\ \phi F)$ is also an SG-isomorphism, F', of course, being $\phi F \in B(L \dotplus L, M_1 \dotplus M_{ij})$. Since $(M_1 \dotplus M_{ij}, L \dotplus L; F')$ is decomposable, it may be written as a direct sum of indecomposables involving only R, $(\bar\theta - \theta)R$, $(\bar\theta - \theta)U_iU_jR$ and L, or S and S'. Since it is isomorphic to a direct sum of projective modules, we must have $(M_1 \dotplus M_{ij},\ L \dotplus L) \cong (M_1, L) \dotplus (M_{ij}, L)$ implying that $X_i \dotplus X_j \cong X_1 \dotplus X_{ij}$.

Lemma 4.2. *$X_i \dotplus X_j \cong X_k \dotplus X_l$ if and only if $[U_i][U_j] = [U_k][U_l]$.*

Proof. By Lemma 4.1, $X_i \dotplus X_j \cong X_1 \dotplus X_{ij} \cong (M_1 \dotplus M_{ij}, L \dotplus L)$. Thus if $X_i \dotplus X_j \cong X_k \dotplus X_l$, there exists an SG-isomorphism of $M_1 \dotplus M_{ij}$ onto $M_1 \dotplus M_{kl}$. By Lemma 1.4, $[U_i][U_j] = [U_k][U_l]$. The converse is an immediate consequence of Lemma 4.1.

If P is any projective SG-module, by Theorem 4.1 $P = X_i \dotplus F$ for some $1 \leqq i \leqq h$ and $\{X_i\}$, the projective class of X_i is the same as $\{P\}$. If $X_1 \dotplus X_i \cong X_1 \dotplus X_j$, by Lemma 4.2 $[U_i] = [U_j]$. Then by Proposition 2.3 $X_i \cong X_j$. Since $X_1 \cong SG$ and $\{0\} = \{X_1\}$, it follows that

Proposition 4.1. *$X_i \dotplus F_i \cong X_j \dotplus F_j$, where F_i, F_j are free SG-modules of equal SG-rank, if and only if $X_i \cong X_j$.*

Further, $X_i \in \{0\}$ if and only if $X_i \dotplus F = F'$. But this is the case if and only if $X_i \dotplus F \cong X_1 \dotplus F''$ and by Proposition 4.1 $X_i \cong X_1$ and conversely, that is,

Proposition 4.2. *$X_i \in \{0\}$ if and only if X_i is a free SG-module.*

We are now able to establish the main result of this section.

Theorem 4.2. *There are h projective classes of SG-modules given by $\{X_i\}$ for $i = 1, \cdots, h$. In particular, the projective class group of SG is isomorphic to the ideal class group of R_0.*

Proof. Let ρ be a mapping of the projective class group of SG into the ideal class group of R_0 given by $\rho: \{X_i\} \to [U_i]$. By Proposition 4.1 $X_i \dotplus F_i \cong X_j \dotplus F_j$ implies $[U_i] = [U_j]$, so ρ is well defined. Since $X_i \dotplus X_j = X_1 \dotplus X_{ij}$ and $\{X_1\} = \{0\}$, we have $\rho: \{X_i \dotplus X_j\} \to [U_i][U_j]$. But $\rho(\{X_i\}) \cdot \rho(\{X_j\}) = [U_i][U_j]$; hence ρ is a homomorphism. ρ is obviously onto. That it is 1–1 follows from Proposition 4.1; thus ρ is the desired isomorphism.

References

1. E. Cartan and S. Eilenberg, *Homological algebra*, Princeton Univ. Press, Princeton, N. J., 1956.

2. C. W. Curtis and I. Reiner, *Theory of group representations*, Interscience, New York, 1962.

3. F. E. Diederichsen, *Über die Ausreducktion ganzzahliger Gruppendarstellungen bei arithmetischer Äquivalenz*, Abh. Math. Sem. Univ. Hamburg **13** (1940), 357–412.

4. A. Heller, *On group representations over a valuation ring*, Proc. Nat. Acad. Sci. U.S.A. **47** (1961), 1194–1197.

5. A. Heller and I. Reiner, *Representations of cyclic groups in rings of integers*. I, Ann. of Math. (2) **76** (1962), 73–93.

6. ———, *Representations of cyclic groups in rings of integers*. II, Ann. of Math. (2) **77** (1963), 318–328.

7. A. Jones, *Indecomposable integral representations*, Thesis, Univ. of Illinois, Urbana, Ill 1962.

8. D. Knee, *The indecomposable representations of finite cyclic groups*, Notices Amer. Math. Soc. **9** (1962), 32.

9. J.-M. Maranda, *On P-adic integral representations of finite groups*, Canad. J. Math. **5** (1953), 344–355.

10. J. Oppenheim, *Integral representations of cyclic groups of square free order*, Thesis, Univ. of Illinois, Urbana, Ill., 1962.

11. I. Reiner, *Integral representations of cyclic groups of prime order*, Proc. Amer. Math. Soc. **8** (1957), 142–146.

12. ———, *The Krull-Schmidt theorem for integral group representations*, Bull. Amer. Math. Soc. **67** (1961), 365–367.

13. ———, *On the class number of representations of an order*, Canad. J. Math. **11** (1959), 660–672.

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

15. R. G. Swan, *Induced representations and projective modules*, Ann. of Math. (2) **70** (1960), 552–578.

16. A. Troy, *Integral representutions of cyclic groups order p^2*, Thesis, Univ. of Illinois, Urbana, Ill., 1961.

Brown University,
Providence, Rhode Island