PACIFIC JOURNAL OF MATHEMATICS
Vol. 17, No. 3, 1966

COHOMOLOGY OF CYCLIC GROUPS OF PRIME SQUARE ORDER

J. T. PARR

Let G be a cyclic group of order p^2, p a prime, and let U be its unique proper subgroup. If A is any G-module, then the four cohomology groups

$$H^0(G, A) \quad H^1(G, A) \quad H^0(U, A) \quad H^1(U, A)$$

determine all the cohomology groups of A with respect to G and to U. This article determines what values this ordered set of four groups takes on as A runs through all finitely generated G-modules.

Reduction. Let G be any finite group. A finitely generated G-module M is quotient of a finitely generated G-free module L. The kernel K is Z-free, and since the cohomology of L is zero with respect to all subgroups of G, K is a dimension shift of M. The standard dimension shifting module $P = ZG/(S_G)$ is Z-free, so $K \otimes P$ is a Z-free G-module having the same cohomology as M with respect to all subgroups of G.

PROPOSITION 1. If G is any finite p-group and M any Z-free G-module, the cohomology of M is that of $R \otimes M$ where R is the ring of p-adic integers.

Proof. Because M is Z-free, $0 \rightarrow M \rightarrow R \otimes M \rightarrow R/Z \otimes M \rightarrow 0$ is a G-exact sequence. $R/Z \otimes M$ is divisible and p-torsion free, so its cohomology is zero, and $M \rightarrow R \otimes M$ induces isomorphism on all cohomology groups.

If M is Z-free and finitely generated, $R \otimes M$ is an R-torsion free, finitely generated RG-module. So we see that if G is any finite p-group, every finitely generated G-module has the same cohomology as a finitely generated, R-torsion free RG-module.

2. Exact sequences. Let G be generated by an element g of order p^2 and let U be its subgroup of order p. Heller and Reiner [2] have determined all indecomposable finitely generated R-torsion free RG-modules:

(a) R with trivial action
(b) $B = R(\omega)$, ω a primitive pth root of 1, $g\omega^j = \omega^{j+1}$
(c) $C = R(\theta)$, θ a primitive p^2th root of 1, $g\theta^j = \theta^{j+1}$

Received December 27, 1963.

(d) $E = RH$, H a cyclic group of order p generated by h, $gh^j = gh^{j+1}$

(e)—(i) a module M such that there exists an exact sequence

(e) $0 \to R \to M \to C \to 0$

(f) $0 \to E \to M \to C \to 0$

(g) $0 \to B \to M \to C \to 0$

(h) $0 \to R \oplus E \to M \to C \to 0$

(i) $0 \to R \oplus B \to M \to C \to 0$

We compute the cohomology of the modules in (a)—(d) directly, and find their sets of four groups to be

(a)	Z_{p^2}	0	Z_p	0
(b)	0	Z_p	$(p-1)Z_p$	0
(c)	0	Z_p	0	pZ_p
(d)	Z_p	0	pZ_p	0

The exact cohomology sequences arising from the exact sequences (e)—(i) restrict the cohomology possibilities to

(e)	Z_{p^2}	Z_p	Z_p	pZ_p
	Z_{p^2}	Z_p	0	$(p-1)Z_p$
	Z_p	0	Z_p	pZ_p
	Z_p	0	0	$(p-1)Z_p$
(f)	0	0	nZ_p	nZ_p
	Z_p	Z_p	nZ_p	nZ_p
		$n = 0, \cdots, p$		
(g)	0	$2Z_p$	nZ_p	$(n+1)Z_p$
	0	Z_{p^2}	nZ_p	$(n+1)Z_p$
		$n = 0, \cdots, p-1$		
(h)	Z_{p^2}	0	$(n+1)Z_p$	nZ_p
	$2Z_p$	0	$(n+1)Z_p$	nZ_p
	$Z_{p^2} + Z_p$	Z_p	$(n+1)Z_p$	nZ_p
		$n = 0, \cdots, p$		
(i)	Z_{p^2}	Z_{p^2}	nZ_p	nZ_p
	Z_{p^2}	$2Z_p$	nZ_p	nZ_p
	Z_p	Z_p	nZ_p	nZ_p
		$n = 0, \cdots, p$		

In § 4 we shall determine which of these combinations actually occur.

3. Enlargements.

An R-enlargement of C by A is an R-split RG-exact sequence $0 \to A \to M \to C \to 0$ [1]. Two enlargements involving M and M' are equivalent if there exists an RG-homomorphism $u: M \to M'$ such that

$$\begin{tikzcd}[row sep=small] & & M \arrow[dd, "\mu"] \arrow[dr] & & \\ 0 \arrow[r] & A \arrow[ur] \arrow[dr] & & C \arrow[r] & 0 \\ & & M' \arrow[ur] & & \end{tikzcd} \qquad \text{commutes .}$$

The R-split exact sequence gives M the R-structure of $A \oplus C$. The first summand is determined by the sequence, but the second is not; choose any one of the possible R-submodules for the second summand. Because the sequence is a G-sequence, $g(a, 0) = (ga, 0)$ and the second component of $g(0, c)$ is gc. Denote the first component of $g(0, c)$ by $f(c)$; $g(0, c) = (f(c), gc)$. So f is a function from C into A, and is an R-homomorphism because g is an R-homomorphism. The equation $g^{p^2}(0, c) = ((N_G f)(c), c) = (0, c)$ gives us that f is a -1-cocycle of the G-module $\mathrm{Hom}_R(C, A)$ where G acts by $(gf)(c) = gf(g^{-1}c)$. Clearly, every -1-cocycle defines an action by G on $A \oplus C$ which makes an R-enlargement of $0 \to A \to A \oplus C \to C \to 0$. If two -1-cocycles f_1 and f_2 differ by a coboundary, $f_1 - f_2 = (g - 1)f_3$, then

$$u(a, c) = (a + [(1 - g)f_3](g^{-1}c), c)$$

defines an RG-isomorphism u of $A \oplus C$ with G-module structure given by f_1 onto $A \oplus C$ with G-module structure given by f_2; the RG-modules corresponding to f_2 and f_1 are isomorphic. So to investigate all enlargement modules M of C by A we need only look at those corresponding to a set of representative cocycles of $H^{-1}(G, \mathrm{Hom}_R(C, A))$.

Since the modules R, B, C, and E are R-free, the exact sequences (e)—(i) are R-split, and M is an enlargement in each case of C by another module.

For the application of this section, we shall need the following propositions.

PROPOSITION 2. If A is an RG-module on which U acts trivially, then $N_G \mathrm{Hom}_R(C, A) = 0$.

Proof. Let $f \in \mathrm{Hom}_R(C, A)$. We easily compute that $(N_G f)(\theta^j) = g^j(N_G f)(1)$, and using the facts that θ satisfies

$$x^{p(p-1)} + x^{p(p-2)} + \cdots + x^p + 1 = 0$$

and that g^p acts trivially on A, we find by writing it out that $(N_G f)(1) = 0$, which then implies that $N_G f = 0$.

Abbreviate $p(p - 1) = m$. Since C is the R-direct sum of the R-submodules generated by θ^i, $i = 0, 1, \cdots, m - 1$, then $\mathrm{Hom}_R(C, A)$ is the direct sum of subgroups F_i, where F_i is the set of all R-homomorphisms from C to A which have value zero for all θ^j except possibly for $j = i$.

PROPOSITION 3. If A is any RG-module, every element of $\mathrm{Hom}_R(C, A)$ is equivalent mod the -1-coboundary group $(g-1)\mathrm{Hom}_R(C, A)$ to some element of F_{m-1}.

Proof. If $f \in F_0$, then $g^{-1}f \in F_{m-1}$, and $g^{-1}f - f = (g^{-1}-1)f = (g-1)(g^{p^2-2} + \cdots + g + 1)f$. If $f \in F_i$, then $gf \in F_{i+1} + F_0$ differs from f by $(g-1)f$. The proof succeeds by repeated application of these cases to the F_i-components of an arbitrary f.

COROLLARY. *If M is one of the modules described in* (e)—(i), *M is an enlargement module of C by A $(A = R, B, E, R \oplus B, R \oplus E)$ corresponding to an element of F_{m-1}.*

Because we are concerned only with indecomposable modules, the following proposition will spare us some unnecessary computations later on.

PROPOSITION 4. Let M be an enlargement module of C by $A \oplus D$ corresponding to $f \in \mathrm{Hom}_R(C, A \oplus D) \cong \mathrm{Hom}_R(C, A) \oplus \mathrm{Hom}_R(C, D)$, and let $f = f_1 + f_2$ be the corresponding decomposition of f. Then if either f_1 or f_2 represents a G-split enlargement of C by A or D, M is decomposable as a G-module.

Proof. Suppose f_1 represents an RG-split enlargement of C by A. Let N be $A \oplus C$ with action of C defined by f_1. Since the enlargement splits there is an RG-homomorphism $w: N \rightarrow A$ such that $A \rightarrow N \rightarrow A$ is the identity of A. Let u be the restriction of w to the given copy of C in N. That w is an RG-homomorphism right inverse to the inclusion of A in N requires that $gu(c) = f_1(c) + u(gc)$.

Let M be $A \oplus D \oplus C$ with action of G defined by f. Then $v(a + d + c) = a + u(c)$ defines an RG-homomorphism right inverse to the inclusion of A in M, so M is decomposable as an RG-module.

4. Computations.

In this section we determine which of the possibilities for the cohomology of (e)—(i) actually occur.

PROPOSITION 5. Let A be an RG-module left fixed by U, and let M be an enlargement module of C by A corresponding to $f \in F_{m-1}$. Then

i) $H^0(G, M) = A^G/(N_G A + N_{G/U} f(\theta^{m-1}))$

ii) $H^0(U, M)$ is isomorphic to the quotient of $A/N_U A$ with respect to the cyclic G/U-submodule generated by the class of $f(\theta^{m-1})$.

Proof. M^G is just the copy of A^G canonically (by the given exact sequence) contained in M, M^U the copy of A^U. Since A is a submodule, the norms of elements of the copy of A are the images of the norms in A. Computation shows

$$N_G(0, \theta^i) = N_G(0, 1) = (N_{G/U} f(\theta^{m-1}), 0)$$
$$N_U(0, \theta^i) = g^i N_U(0, 1) = g^i (f(\theta^{m-1}), 0)$$

whence the result.

We are now able to settle case (e).

(e) M is an enlargement module of C by R. By Proposition 5, $H^0(G, M)$ is Z_{p^2} if $f(\theta^{m-1})$ is a multiple of p and Z_p if not; and $H^0(U, M)$ is Z_p if $f(\theta^{m-1})$ is a multiple of p and 0 if not. This, together with the information in Section 3, shows that the only cohomology this module M might have is

	Z_{p^2}	Z_p	Z_p	pZ_p
or	Z_p	0	0	$(p-1)Z_p$.

For the remaining cases, we shall need one more proposition.

PROPOSITION 6. Let H be a group of order p generated by h. Let A be a cyclic Z_pH-module of Z_p-dimension n. Then

(i) $(h-1)^j A$ has dimension $n-j$, $j = 0, \cdots, n$.

(ii) a is a generator for A if and only if $a \notin (h-1)A$.

(iii) a is a generator for A if and only if $(h-1)^{n-1}a$ is nonzero.

Proof. (i) We have a properly descending chain

$$A \supset (h-1)A \supset \cdots \supset (h-1)^{n-1}A \supset (h-1)^n A = 0$$

of Z_p-spaces, and we can see by counting that the dimension of $(h-1)^j A$ is $n-j$.

(ii) The above chain exhibits all submodules of A.

(iii) If a generates A, $(h-1)^{n-1}a$ generates $(h-1)^{n-1}A$, which is not zero. If not, $a \in (h-1)A$, so $(h-1)^{n-1}a = 0$.

(f) M is an enlargement module of C by E. $E/pE = \bar{E}$ is a cyclic $Z_p(G/U)$-module of Z_p-dimension p. Let M be represented by $f \in F_{m-1}$, and $f(\theta^{m-1}) = e$. By Proposition 5, $H^0(G, M)$ is the quotient of $H^0(G, E)$ by the subgroup generated by $N_{G/U}\bar{e} = (\bar{g}-1)^{p-1}\bar{e}$, hence zero if $N_{G/U}\bar{e}$ is not zero, Z_p if it is. Using proposition 6 iii, we see

$$H^0(G, M) \cong 0 \text{ if } \bar{e} \text{ generates } \bar{E} \text{ over } Z_p(G/U)$$
$$\cong Z_p \text{ if not .}$$

$H^0(U, M)$ is the quotient of $H^0(U, E) \cong \bar{E}$ by the $Z_p(G/U)$-submodule generated by $\bar{e}$. Let n be the largest integer with $\bar{e} \in (g-1)^n \bar{E}$. By Proposition 6 ii then, $\bar{e}$ generates $(g-1)^n \bar{E}$, which is of dimension $p-n$, so the quotient has dimension n. The cohomology of M is

$$\begin{array}{ccccl} 0 & 0 & 0 & 0 & \text{if } n=0 \\ Z_p & Z_p & nZ_p & nZ_p & \text{if } n=1,\cdots,p\,. \end{array}$$

(g) M is an enlargement module of C by B. $N_G M \subset M^G = B^G = 0$. So $H^0(G, M) = 0$ and $H^1(G, M) \cong H^{-1}(G, M)$ is the quotient of M modulo $(g-1)M$. Let M correspond to $f \in F_{m-1}$ and denote $f(\theta^{m-1}) = b$.

Case 1. $b \in (g-1)B$. Then $H^1(G, M) \cong 2Z_p$
Case 2. $b \notin (g-1)B$. Then $H^1(G, M) \cong Z_{p^2}$.

By Proposition 6 again,

$$\begin{aligned} H^1(G, M) &\cong 2Z_p \text{ if } \bar{b} \text{ does not generate } B/pB \\ &\cong Z_{p^2} \text{ if it does}\,. \end{aligned}$$

Similarly as in (f), if n is the greatest integer with $\bar{b} \in (\bar{g}-1)^n(B/pB)$, then $H^0(U, B) \cong nZ_p$. The cohomology is thus

$$\begin{array}{ccccl} 0 & Z_{p^2} & 0 & Z_p & \text{if } n=0 \\ 0 & 2Z_p & nZ_p & (n+1)Z_p & \text{if } n=1,\cdots,p-1\,. \end{array}$$

(h) M is an enlargement module of C by $R \oplus E$. Let M correspond to $f \in F_{m-1}$ and write $f(\theta^{m-1}) = r + e$, $r \in R$, $e \in E$. We may assume r is not divisible by p, because if it were, M would be decomposable (Proposition 4).

Computation based on Proposition 5 shows

$$\begin{aligned} H^0(G, M) &\cong 2Z_p \quad \text{if } N_{G/U}e \text{ is divisible by } p \\ &\cong Z_{p^2} \quad \text{if not,} \end{aligned}$$

and that

$$\begin{aligned} H^0(U, M) &\cong (n+1)Z_p \quad \text{if } n=0,\cdots,p-1 \\ &\cong pZ_p \qquad \text{if } n=p \end{aligned}$$

where n is the largest integer with $\bar{e} \in (g-1)^n \bar{E}$. So the cohomology of M may be

$$\begin{array}{ccccl} Z_{p^2} & 0 & Z_p & 0 & \text{or} \\ 2Z_p & 0 & (n+1)Z_p & nZ_p & n=1,\cdots,p-1\,. \end{array}$$

(i) M is an enlargement module of C by $R \oplus B$. Let $f \in F_{m-1}$ represent the enlargement and write $f(\theta^{m-1}) = r + b$, $r \in R$, $b \in B$. Again we may assume r is not divisible by p.

$H^0(G, M) \cong Z_p$ by Proposition 5.

Let j be the largest integer with $\bar{b} \in (g-1)^j \bar{B}$.

$$\begin{aligned} H^0(U, M) &= (j+1)Z_p \quad \text{if} \quad j = 0, \cdots, p-2 \\ &= (p-1)Z_p \quad \text{if} \quad j = p-1 \,. \end{aligned}$$

So the cohomology of M is

$$Z_p \qquad Z_p \qquad nZ_p \qquad nZ_p \qquad n = 1, \cdots, p-1 \,.$$

5. **Summary.** If M is any finitely generated G-module, then the cohomology of M is the direct sum of a finite number of the following:

	$H^0(G, A)$	$H^1(G, A)$	$H^0(U, A)$	$H^1(U, A)$	
1.	Z_{p^2}	0	Z_p	0	
2.	0	Z_{p^2}	0	Z_p	
3.	Z_p	0	pZ_p	0	
4.	0	Z_p	0	pZ_p	
5.	Z_p	0	0	$(p-1)Z_p$	
6.	0	Z_p	$(p-1)Z_p$	0	
7.	Z_p	Z_p	nZ_p	nZ_p	$n = 1, \cdots, p$
8.	$2Z_p$	0	$(n+1)Z_p$	nZ_p	$n = 1, \cdots, p-1$
9.	0	$2Z_p$	nZ_p	$(n+1)Z_p$	$n = 1, \cdots, p-1$

Given any direct sum of finitely many of the above, there is a finitely generated G-module with that cohomology.

BIBLIOGRAPHY

1. Samuel Eilenberg, *Topological methods in abstract algebra,* Bull. Amer. Math. Soc. **55** (1949), 3-35.
2. A. Heller and I. Reiner, *Representations of cyclic groups in rings of integers I.* Ann. of Math. **76** (1962), 73-92.