

EXPONENTS AND THE COHOMOLOGY OF FINITE GROUPS

JONATHAN PAKIANATHAN

(Communicated by Ralph Cohen)

ABSTRACT. We will provide an example of a p -group G which has elements of order p^3 in some of its integral cohomology groups but which also has the property that p^2 annihilates $\bar{H}^i(G; \mathbb{Z})$ for all sufficiently high i . This provides a counterexample to a conjecture of A. Adem which states that if a finite group K has an element of order p^n in one of its integral cohomology groups, then it has such an element in infinitely many of its cohomology groups.

1. INTRODUCTION

Throughout this paper, we will use the integers \mathbb{Z} as coefficients for cohomology groups unless otherwise specified and will write $H^*(\cdot)$ for $H^*(\cdot; \mathbb{Z})$.

It is well known that for G a finite group, the integral cohomology groups $H^*(G)$ are finitely generated in each dimension and are annihilated by $|G|$ in positive dimensions. (Here $|G|$ stands for the order of G .) Thus if we define $\bar{H}(G) = \bigoplus_{i=1}^{\infty} H^i(G)$, we have $|G| \cdot \bar{H}(G) = 0$.

Definition 1.1. Given a group G , we define the exponent of G as $\exp(G) = \min\{n \geq 1 : g^n = 1, \forall g \in G\}$. We use the convention that $\exp(G) = \infty$ if the set that we are minimizing over is empty.

Definition 1.2. For a finite group G , $e(G)$ is defined to be $\exp(\bar{H}(G))$. It follows easily that $e(G) \mid |G|$.

Let p be a prime and let P be a finite p -group. It is known that the value of $e(P)$ (which will be a power of p) contains information about the structure of P . In particular there is the following theorem of A. Adem:

Theorem 1.3 (A. Adem). *If P is a finite p -group, then $e(P) = p$ if and only if P is a nontrivial elementary abelian p -group.*

(Also note that if P is a p -group, then $e(P) = 1$ if and only if $P = 1$. See for example page 149 of [B].)

For a general p -group P , finding $e(P)$ can be quite difficult. Therefore we define another related quantity which is sometimes easier to calculate.

Definition 1.4. For P a finite p -group, $e_{\infty}(P) = \min\{n \geq 1 : n\bar{H}(P) \text{ is finite}\}$.

Notice that $e_{\infty}(P)$ will be a power of p and $e_{\infty}(P) \mid e(P) \mid |P|$.

Received by the editors March 16, 1998 and, in revised form, August 13, 1998.
1991 *Mathematics Subject Classification.* Primary 20J06, 17B50; Secondary 17B56.

Remark 1.5. It is easy to see that for $C = \mathbb{Z}/p^n\mathbb{Z}$, the cyclic group of order p^n , one has $\exp(C) = e_\infty(C) = e(C) = |C| = p^n$.

A question one is lead to ask is, does $e_\infty(P) = e(P)$? This is part of a conjecture of A. Adem stated on page 438 of [C]:

Conjecture 1.6. If S is a finite group, and $H^i(S)$ contains elements of order p^n for some i , then it does so for infinitely many i . In particular for a p -group P , $e_\infty(P) = e(P)$.

This conjecture is true in certain cases as is seen in the next proposition:

Proposition 1.7. *Let P be a p -group.*

If $e_\infty(P) = 1$, then $e(P) = 1$ and $P = 1$.

If $e_\infty(P) = p$, then $e(P) = p$ and P is elementary abelian.

Proof. The first part follows from standard Nakayama-Rim Theory. (See page 140 of [B].) The second part follows essentially from the theorem of A. Adem stated before. (See [A] or [Le].) □

However, it turns out the conjecture is false in general (at least when p is odd). The main purpose of this paper is to provide a counterexample to the conjecture, which will be done in the next section. However before doing this, let us prove a few basic properties of $e_\infty(P)$.

Proposition 1.8. *If $P_1 \leq P_2$ where P_2 is a p -group, then $e_\infty(P_1) | e_\infty(P_2)$.*

Proof. By the Evens-Venkov Theorem, $H^*(P_1)$ is a finitely generated $H^*(P_2)$ -module, say with generators $x_1, \dots, x_n \in H^*(P_1)$. Let $t = \max\{\dim(x_i) : 1 \leq i \leq n\}$ and $s \in \mathbb{N}$ be such that $e_\infty(P_2) \cdot H^i(P_2) = 0$ for $i > s$. Then it is easy to see that for $j > s + t$, we have $e_\infty(P_2) \cdot H^j(P_1) = 0$. Thus $e_\infty(P_2) \cdot \bar{H}(P_1)$ is finite and $e_\infty(P_1) | e_\infty(P_2)$. □

Corollary 1.9. *If P is a finite p -group, then*

$$\exp(P) | e_\infty(P) | e(P) | |P|.$$

Furthermore, there are examples of p -groups which show that these quantities are different in general.

Proof. For the first part, it only remains to show $\exp(P) | e_\infty(P)$. Notice there is a cyclic subgroup C of P of size $\exp(P)$. Thus by Proposition 1.8, one has $\exp(P) = |C| = e_\infty(C) | e_\infty(P)$. Thus we have the first part. When P is elementary abelian of rank greater than one, then $e(P) = p$ is not equal to $|P|$. When P is extraspecial with $\exp(P) = p$, then by the theorem of A. Adem quoted before, we can see $e_\infty(P) \neq p$ and hence $e_\infty(P)$ is not equal to $\exp(P)$. Finally, the counterexample in the next section gives an example of a p -group P where $e_\infty(P)$ is not equal to $e(P)$. □

Definition 1.10. Let $S(p^n)$ be the Sylow p -group of the symmetric group on p^n letters.

Remark 1.11. $\exp(S(p^n)) = e_\infty(S(p^n)) = e(S(p^n)) = p^n$.

Proof. The cyclic group $\mathbb{Z}/p^n\mathbb{Z}$ acts faithfully on itself by left multiplication and hence embeds in the symmetric group on p^n letters. Thus $S(p^n)$ has a cyclic subgroup of order p^n and hence $p^n \mid \exp(S(p^n))$. So in light of Corollary 1.9, it remains only to show that $e(S(p^n)) \mid p^n$. This follows by an induction. When $n = 1$, $S(p^n)$ is cyclic of order p , so this case follows. The induction proceeds by noting that $S(p^n)$ is isomorphic to the wreath product of $S(p^{n-1})$ with $\mathbb{Z}/p\mathbb{Z}$. Thus $S(p^n)$ has a subgroup of index p which is isomorphic to the direct product of p copies of $S(p^{n-1})$, and hence $e(S(p^n)) \mid pe(S(p^{n-1})) \mid pp^{n-1} = p^n$ by an easy transfer argument. \square

This allows us to prove the following lemma (given in [Le]; we include a proof for completeness).

Lemma 1.12. *Let P be a finite p -group. If the intersection of all subgroups of P of index p^n is trivial, then $e_\infty(P) \mid p^n$.*

Proof. Let H_1, \dots, H_k be the distinct subgroups of index p^n in P . Then for each $1 \leq i \leq k$, P acts on the left cosets of H_i and this gives us a homomorphism

$$\phi_i : P \rightarrow S(p^n),$$

with kernel lying in H_i . Putting these homomorphisms together we get a homomorphism from P into L which is the direct product of k copies of $S(p^n)$. This is injective, as its kernel is the intersection of the kernels of the ϕ_i maps for all $1 \leq i \leq k$, which is trivial by assumption. Thus P can be considered a subgroup of L and from the remark above, $e_\infty(L) = p^n$ and hence the lemma follows from Proposition 1.8. \square

Neither Lemma 1.12 nor Proposition 1.8 is true if we replace $e_\infty(\cdot)$ with $e(\cdot)$. For example, the group $G(\mathfrak{sl}_2)$, provided as a counterexample in the next section, embeds in a direct product L of a few copies of $S(p^2)$ because the intersection of its index p^2 subgroups is trivial. Of course $e(L) = p^2$, however $e(G(\mathfrak{sl}_2)) = p^3$.

2. THE COUNTEREXAMPLE

Throughout this section, p will be an odd prime. We will be looking at a certain central extension:

$$1 \rightarrow W \rightarrow G \rightarrow V \rightarrow 1,$$

where V, W are elementary abelian p -groups. It is well known that there is a bracket $\langle \cdot, \cdot \rangle : V \rightarrow W$ and a p -power map $\phi : V \rightarrow W$ which are defined using the commutator and p -power in the group G (see [BrP]). These are an alternating bilinear form and a linear map respectively. We will assume as in [BrP] that ϕ is an isomorphism and hence identify V and W . It was shown there that such groups G are in natural correspondence with bracket algebras (Lie algebras minus the Jacobi identity) over \mathbb{F}_p . In particular, to every such bracket algebra, there exists a unique such group corresponding to it. To get the corresponding bracket algebra one just forms $[\cdot, \cdot] : V \rightarrow V$ by composing $\langle \cdot, \cdot \rangle$ with the inverse of ϕ . Hence either V or W can be considered as the bracket algebra.

Now recall that we have the Lie algebra \mathfrak{sl}_2 which is a 3-dimensional algebra over \mathbb{F}_p . We can choose a basis $\{h, x_+, x_-\}$ where the bracket is given by:

$$\begin{aligned} [h, x_+] &= 2x_+, \\ [h, x_-] &= -2x_-, \\ [x_+, x_-] &= h. \end{aligned}$$

Let $G = G(\mathfrak{sl}_2)$ be the group associated to this Lie algebra as mentioned above. It follows easily then that G has exponent p^2 and order p^6 . It was shown in the last section of [BrP] that $e(G) = p^3$ and in fact there are elements of order p^3 in $H^4(G)$.

We will show that the intersection of all subgroups of index p^2 in G is trivial and hence that $e_\infty(G) \mid p^2$ by Lemma 1.12. One can conclude that $e_\infty(G) = p^2$, as G is not elementary abelian. Since we know as previously remarked that $e(G) = p^3$, this means $H^*(G)$ is annihilated by p^2 in all sufficiently high dimensions but not in all positive dimensions, and hence gives us the counterexample we sought!

So it remains to show that the intersection of all subgroups of index p^2 in G is trivial. We have

$$1 \rightarrow W \rightarrow G \rightarrow V \rightarrow 1$$

where W and V can both be identified with \mathfrak{sl}_2 . Note the preimage of any 1-dimensional subspace of V is a subgroup of index p^2 in G and the intersection of these is in W , so the intersection of all index p^2 subgroups lies in W . To show the intersection of the index p^2 subgroups is in fact trivial, we need a lemma:

Lemma 2.1. *Every 2-dimensional sub(Lie)algebra S of \mathfrak{sl}_2 considered as a subset in V has a subgroup K of index p^2 in G lying over it. Furthermore the intersection of K and W is just $\phi(S)$ where ϕ is the p -power map mentioned before.*

Proof. Let \hat{x} and \hat{y} be a basis for the 2-dimensional subalgebra and lift them to $x, y \in G$. Let K be the subgroup they generate; then K maps down to the subalgebra under the projection map to V and hence lies over it. It remains to show K has index p^2 . Any element t in K can be written as a product of x, y, x^{-1}, y^{-1} in some combination or other. As the commutator of x and y is central we can move all the x 's to the leftmost and all the y 's to the right of them, leaving a bunch of commutators of x 's and y 's and their inverses on the right. However if we let L be the image under the ϕ p -power map of the subalgebra S , then L is generated by x^p and y^p so is in K , is central and contains these commutators. This means that each commutator can be written as a product of some power of x^p and some power of y^p and as these are central, we can move them to join the other powers of x and y respectively. The upshot is that any $t \in K$ can be written $t = x^l y^s$ for some l, s integers. However x, y have order p^2 so we see the order of K is at most p^4 , but we see easily that it has order at least p^4 so K has order p^4 and is of index p^2 . The intersection of K with W is obviously L . □

If we view W as \mathfrak{sl}_2 , then we have already argued that the intersection of all subgroups of index p^2 in G lies in W . To show this intersection is trivial, in light of the lemma above, it suffices to show that the intersection of 2-dimensional Lie subalgebras in \mathfrak{sl}_2 is trivial. We do this next and then will be done.

Note $\{h, x_+\}$ generates a 2-dimensional subalgebra of \mathfrak{sl}_2 and so does $\{h, x_-\}$. Their intersection is the 1-dimensional subspace spanned by h . So we only need to

show that there is a 2-dimensional subalgebra which does not contain h . Now let $\alpha = 4^{-1}$ in \mathbb{F}_p . Consider S the subspace generated by $\{h + x_+, -\alpha h + x_-\}$. Then we have:

$$\begin{aligned} [h + x_+, -\alpha h + x_-] &= 2\alpha x_+ - 2x_- + h \\ &= 2\alpha(x_+ + h) - 2(x_- - \alpha h) + (1 - 4\alpha)h \\ &= 2\alpha(h + x_+) - 2(-\alpha h + x_-) \end{aligned}$$

as $4\alpha = 1$.

So we see S is a 2-dimensional sub(Lie)algebra of \mathfrak{sl}_2 . However it is easy to see that h is not in S . Thus we are done as mentioned before.

REFERENCES

- [A] A. Adem, *Cohomological exponents of $\mathbb{Z}G$ -lattices*, J. Pure and Appl. Alg. **58** (1989). MR **90b**:20046
- [BrP] W. Browder, J. Pakianathan, *Cohomology of uniformly powerful p -groups*, preprint.
- [B] K. S. Brown, *Cohomology of Groups*, Springer Verlag GTM 87, New York-Heidelberg-Berlin, 1994. MR **96a**:20072
- [C] G. Carlsson, R. L. Cohen, H. R. Miller, D. C. Ravenel, *Algebraic Topology*, Springer Verlag Lecture Notes in Mathematics 1370, New York-Heidelberg-Berlin, 1989. MR **90a**:55003
- [Le] I. J. Leary, *A bound on the exponent of the cohomology of BC -bundles*, Proceedings of the 1994 Barcelona Conference on Algebraic Topology: Progress in Mathematics, Vol. **136** (1996) pp. 255-260, Birkhauser-Verlag. MR **97k**:55018

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF WISCONSIN, MADISON, WISCONSIN 53706
E-mail address: pakianat@math.wisc.edu