NILPOTENCY DEGREE OF COHOMOLOGY RINGS
IN CHARACTERISTIC \( p \)

PHAM ANH MINH

(Communicated by Stephen D. Smith)

Dedicated to Professor Huỳnh Mùi on his sixtieth birthday

Abstract. Let \( p \) be an odd prime number. The purpose of this paper is to provide a \( p \)-group \( G \) whose mod-\( p \) cohomology ring has a nilpotent element \( \xi \in H^*(G) \) satisfying \( \xi^p \neq 0 \).

1. Statement of the main result

For every \( p \)-group \( G \), denote by \( H^*(G) \) the mod-\( p \) cohomology algebra of \( G \). We are now interested in the nilpotency degrees of elements of \( H^*(G) \). For the case \( p = 2 \), in [1], [4], it was shown that, given any positive integer \( n \), there exists a \( 2 \)-group whose cohomology ring has elements of nilpotency degree \( n + 1 \). It was also noted in [1] that, for \( p \) odd, we did not have any example of elements of \( H^*(G) \) having nilpotency degrees greater than \( p \).

Recently, such an example was given in [8] for \( p = 3 \). In this case, \( G \) is chosen to be an extension of \( E \times A \) by \( \mathbb{Z}/p \), where \( E \) is the extraspecial 3-group of order \( 3^3 \) and of exponent 3, and \( A \) the elementary abelian 3-group of rank 4.

The purpose of this paper is to generalize the result in [8] to the case of any odd prime \( p \). Let \( \mathfrak{S}_{p^2,p} \) be the Sylow subgroup of the symmetric group on \( p^2 \) letters (so \( \mathfrak{S}_{p^2,p} = \mathbb{Z}/p \wr \mathbb{Z}/p \), the wreath product of \( \mathbb{Z}/p \) and \( \mathbb{Z}/p \)) and let \( Z \) be the center of \( \mathfrak{S}_{p^2,p} \). Define \( \mathfrak{R} = \mathfrak{S}_{p^2,p}/Z \) (so \( \mathfrak{R} = E \) for \( p = 3 \)) and let \( \mathfrak{A}_k \) be the elementary abelian \( p \)-group of rank \( 2k \). We shall prove

Theorem. For \( k \geq 2p - 2 \), there exists a \( p \)-group \( G \) given by a central extension

\[
0 \to \mathbb{Z}/p \to G \to \mathfrak{R} \times \mathfrak{A}_k \to 1
\]

whose mod-\( p \) cohomology ring has a nilpotent element \( \xi \in H^2(G) \) satisfying \( \xi^p \neq 0 \).

We shall use the following notation. For homogeneous elements \( X, Y, \ldots \) of a graded ring \( R \), \( |X| \) denotes the degree of \( X \) and \( (X, Y, \ldots) \) the ideal of \( R \) generated by \( X, Y, \ldots \). \( p \) is assumed from now on to be an arbitrary odd prime number. If \( S \) is a subset of a group \( G \), then \( \langle S \rangle \) denotes the subgroup of \( G \) generated by \( S \). With some abuse of notation, for every \( \zeta \in H^*(G) \) and for every subgroup \( K \) of \( G \), we consider \( \zeta \) as an element of \( H^*(K) \) via the restriction map; also, for every extension \( T \) of \( G \), \( \zeta \) is considered as an element of \( H^*(T) \) via the inflation maps.

Received by the editors August 15, 2001 and, in revised form, September 18, 2001.

2000 Mathematics Subject Classification. Primary 20J06; Secondary 20D15, 55R40.

©2002 American Mathematical Society
2. The groups $\mathfrak{R}$ and $\mathfrak{U}$

Let $\mathfrak{U}$ be the $p$-group of order $p^{p+2}$ given by

$$\mathfrak{U} = \langle a, a_1, \ldots, a_{p+1} | a^p = a_1^p = \cdots = a_{p+1}^p = a_i a_j = a_1^p a_2^{p(p-1)/2} a_p,$$

$$= a_2^p a_{p+1} = 1, [a, a_\ell] = a_\ell 1, 1 \leq i, j \leq p, 1 \leq \ell \leq p \rangle.$$  

Then $\mathfrak{U}$ is a 2-generator $p$-group of maximal class and $\mathfrak{R} = \mathfrak{U}/\langle a_p, a_{p+1} \rangle$ (see e.g. [2 Section 4]). Set $\mathfrak{U} = \mathfrak{U}/(a_p, a_{p+1}), g_i = a_i (a_p, a_{p+1}) \in \mathfrak{R}, 1 \leq i \leq p - 1$, and $K = \langle g_1, \ldots, g_{p-1} \rangle$. We then have extensions of groups

$$(\mathfrak{U}) \quad 0 \to \mathbb{Z}/p \to \mathfrak{U} \rightarrow \mathfrak{U}/\langle a \rangle \to 1,$$

$$(\mathfrak{F}) \quad 0 \to \mathbb{Z}/p \to \mathfrak{F} \rightarrow \mathfrak{R} \to 1,$$

$$(\mathfrak{R}) \quad 0 \to (\mathbb{Z}/p)^{p-1} \cong K \to \mathfrak{R} \to \langle a \rangle \to 1.$$ 

Let $x \in H^1(\langle a \rangle)$ be the dual of $a$ and consider $x$ as an element of $H^1(\mathfrak{R})$ via the inflation map. Define $x_1 \in H^1(\mathfrak{R})$ satisfying $x_1(g_1) = 1, x_1(a) = 0$ ($x_1$ is well-defined, as $\mathfrak{R}$ is a 2-generator $p$-group and $\mathfrak{R} = \langle a, g_1 \rangle$). $x, x_1$ is then a basis of $H^1(\mathfrak{R})$. Set $y = \beta x, y_1 = \beta x_1$ with $\beta$ the Bockstein homomorphism. Let $w$ be the element of $H^2(\mathfrak{R})$ classifying the extension $(\mathfrak{F})$ and set $U = w + y_1$. We have

**Lemma 1.** (i) $U|_K = 0$;

(ii) $U^p + xy^p - \beta U - y^p - 1 = 0$;

(iii) $x \cdot U = x y_1$;

(iv) $U^p = y^p - 1 y_1$.

**Proof.** Set $f = p_1(a_1)$. Since $f^p = j(-1)$ and $p_2^{-1}(K)$ is abelian, $w|_K = -y_1$. Hence $U|_K = 0$. (ii) follows from [5 Remark 1] (see also [7 Theorem 1.1]) and the fact that $U|_K = 0$.

Note that the term $E_2(\mathfrak{U})$ of the Hochschild- Serre spectral sequence corresponding to the extension $(\mathfrak{F})$ is of form

$$E_2(\mathfrak{F}) = H^*(\mathfrak{R}) \otimes H^*(j(\mathbb{Z}/p)).$$

Let $w'$ be the element of $H^2(\mathfrak{F})$ classifying the extension $(\mathfrak{U})$ and let $u$ be the element of $H^2(\mathbb{Z}/p)$ satisfying $d_2(u) = w$. Since $\langle a_p, a_{p+1} \rangle = p_1^{-1}(\text{Im} j)$ is of exponent $p$, $w'$ restricts trivially on $j(\mathbb{Z}/p)$. So $w'$ represents a non-zero element of $E_2^{-1,1}(\mathfrak{U}) \oplus E_2^{0,0}(\mathfrak{U})$. Note that $X|_{(a_j, j(\mathbb{Z}/p))}$ (resp. $X|_{(a_j, j(\mathbb{Z}/p))}$) is a scalar multiple of $y$ (resp. $y_1$), for any $X \in E_2^{0,0}(\mathfrak{U}) \subset \text{Im} \, \text{Inf}^{\mathfrak{R}}$. As $[a, a_\ell] = a_\ell 1$ and $[a, a_p] = 1$, it follows that $w'$ represents a non-zero element $\theta$ of $E_2^{-1,1}(\mathfrak{U})$ and $w' \{|_{J(\mathbb{Z}/p)} \} \neq 0, w' \{|_{J(\mathbb{Z}/p)} \} = 0$. So $\theta$ is a non-zero scalar multiple of $x \otimes u$. This means that $x d_2(u) = xw = 0$. Hence $x \cdot U = x(w + y_1) = xy_1$.

Finally, as

$$y \cdot U - x \cdot \beta U = \beta(x \cdot U) = \beta(xy_1) \quad \text{by (iii)}$$

$$= yy_1.$$
we have, by (ii),
\[
0 = U^p + xy^{p-2} \cdot \beta U - y^{p-1} \cdot U \\
= U^p + y^{p-2}(x \cdot \beta U - y \cdot U) \\
= U^p - y^{p-2} \cdot y y_1 \\
= U^p - y^{p-1} y_1.
\]

The lemma is proved. \(\square\)

Remarks. 1. It is known that \(\text{Inf}^p_{\mathfrak{S}_{p^2}, p} : H^2(\mathfrak{S}) \to H^2(\mathfrak{S}_{p^2}, p)\) is surjective (this comes from the fact that \(\mathfrak{S}_{p^2}, p\) is a terminal \(p\)-group; see \[3\]). Furthermore, as \(H^*(\mathfrak{S}_{p^2}, p)\) is detected by elementary abelian subgroups (\[9\]) and \(U|_{(a)} = 0, U|_K = 0\), it follows that \(\text{Inf}^p_{\mathfrak{S}_{p^2}, p}(U) = 0\). Hence \(U\) is nothing other than the cohomology class classifying the central extension \(1 \to Z \to \mathfrak{S}_{p^2}, p \to \mathfrak{S} \to 1\).

2. The group \(U\) can be obtained from algebraic number theory, as follows. Let \(\vartheta\) be a primitive \(p\)th root of unity and let \(\mathbb{Z}_p\) be the ring of \(p\)-adic integers. Then
\[
\mathbb{Z}_p[\vartheta] = \bigoplus_{j=0}^{p-2} \vartheta^j \mathbb{Z}_p.
\]

Let \(\langle a \rangle\) be the cyclic group of order \(p\). Multiplication by \(\vartheta\) induces an action of \(\langle a \rangle\) on \(\mathbb{Z}_p[\vartheta]\), hence on \(\mathfrak{S} = \mathbb{Z}_p[\vartheta]/((\vartheta - 1)^{p+1})\). We can check that the map
\[
\{a, a_1, \ldots, a_{p+1}\} \to \langle a \rangle \ltimes \mathfrak{S}
\]
which maps \(a\) to \(a\), \(a_i\) to \((\vartheta - 1)^{i-1}, 1 \leq i \leq p+1\), can be extended to a homomorphism of groups from \(U\) to \(\langle a \rangle \ltimes \mathfrak{S}\) which is bijective. So \(U \cong \langle a \rangle \ltimes \mathfrak{S}\).

3. PROOF OF THE THEOREM

Pick a basis \(c_1, \ldots, c_{2k}\) of the elementary abelian \(p\)-group \(\mathfrak{A}_k\) of rank \(2k\). Let \(u_1, \ldots, u_{2k}\) be the basis of \(H^1(\mathfrak{A}_k)\), dual to that of \(\mathfrak{A}_k\). Define \(v_i = \beta u_i, 1 \leq i \leq 2k\). Set \(G = \mathfrak{S} \ltimes \mathfrak{A}_k\). By K"unneth formula,
\[
H^*(G) = H^*(\mathfrak{S}) \otimes H^*(\mathfrak{A}_k) \\
= H^*(\mathfrak{S}) \otimes \Lambda[u_1, \ldots, u_{2k}] \otimes \mathbb{F}_p[v_1, \ldots, v_{2k}].
\]

Let
\[
z = y + u_1 u_2 + \cdots + u_{2k-1} u_{2k}, \\
\alpha = u_1 u_2 + \cdots + u_{2k-1} u_{2k}, \\
\gamma = u_3 u_4 + \cdots + u_{2k-1} u_{2k}
\]
be elements of \(H^*(G)\). Set \(\Lambda = \Lambda[u_1, \ldots, u_{2k}]\) and \(\Lambda' = \Lambda[u_3, \ldots, u_{2k}]\). For \(i \geq 0\), let \(\Lambda_i\) be the degree \(i\)-part of \(\Lambda\). We have

Lemma 2. Let \(0 \neq X\) be a homogeneous element of \(H^*(G)\) and let \(n, k\) be positive integers.

(i) If \(n \leq \min(p - 1, k)\) and \(X \cdot \alpha^n = 0\), then \(|X| \geq \min(2p - 2n, k - n + 1)\).

(ii) If \(X : z = 0\):

(iiia) \(|X| \geq \min(2p - 2, k)\);

(iiib) \(|X| > 2p - 1\), provided that \(k \geq 2p - 2\) and \(X \in (v_1, \ldots, v_{2k})\).
Proof. (i) By induction on \( k \). It obviously holds for \( k = 1 \). Assume that it holds for \( k - 1 \). Without loss of generality, we may assume that \( X \in \Lambda \). If \( n = k \leq p - 1 \), then \( 0 = X \cdot \alpha^n = k! X \cdot u_1 \cdots u_{2k} \) implies \( |X| \geq 1 \). We may then suppose that \( n \leq k - 1 \).

Write \( X = X_1 + X_2 \cdot u_1 u_2 + X_3 \cdot u_1 + X_4 \cdot u_2 \) with \( X_i \) homogeneous in \( \Lambda' \). So \( 0 = X \cdot \alpha^n = X \cdot (\gamma + u_1 u_2)^n \) implies

\[
\begin{align*}
X_1 \cdot \gamma^n &= 0, \\
(nX_1 + X_2 \cdot \gamma) \cdot \gamma^{n-1} &= 0, \\
X_3 \cdot \gamma^n &= X_4 \cdot \gamma^n = 0.
\end{align*}
\]

If \( X_3 \neq 0 \) or \( X_4 \neq 0 \), it follows from (3) and the inductive hypothesis that \( \min(|X_3|, |X_4|) \geq \min(2p - 2n, k - n) \), hence

\[ |X| = \min(|X_3|, |X_4|) + 1 \geq \min(2p - 2n + 1, k - n + 1). \]

So we may suppose that \( X_3 = X_4 = 0 \). By (2) and by the inductive hypothesis,

\[ |nX_1 + X_2 \cdot \gamma| \geq \min(2p - 2n + 2, k - n + 1). \]

Hence \( |X| = |nX_1 + X_2 \cdot \gamma| \geq \min(2p - 2n, k - n + 1) \). If \( nX_1 + X_2 \cdot \gamma \neq 0 \), then \( nX_1 + X_2 \cdot \gamma = 0 \) implies \( X_1 = -X_2 \cdot \gamma \).

By (1), \( X_2 \cdot \gamma^{n+1} = 0 \). By the inductive hypothesis, \( |X_2| \geq \min(2p - 2n - 2, k - n - 1) \).

Hence \( |X| = |X_2| + 2 \geq \min(2p - 2n, k - n + 1) \). (i) is then proved.

(ii) Write \( X = \sum_{i=0}^{m} X_i \cdot Y_i \) with \( Y_i \in \Lambda_1, X_i \in H^*(\mathfrak{g}) \otimes \bF[v_1, \ldots, v_{2k}] \) and \( X \cdot Y_m = 0 \). By (i), it follows that \( |X| = \min(|X_1|, |Y_m|) \geq \min(2p - 2k) \).

Suppose that \( k \geq 2p - 2, |X| \leq 2p - 1 \), and \( X \in (v_1, \ldots, v_{2k}) \). Fix \( i \) with \( 1 \leq i \leq 2k \) and write \( X = v_i' X' + X'' \) with \( X'' \) free of \( v_i \). Then \( X' \cdot z = 0 \). As \( |X'| \leq 2p - 3 \), it follows from (ia) that \( X' = 0 \). \( X \) is then free of \( v_i \). Hence the lemma is proved.

The lemma is proved. \( \square \)

Suppose from now on that \( k \geq 2p - 2 \). We have

**Lemma 3.** If \( X \) is homogeneous in \( H^*(\mathfrak{g}) \) of degree \( \leq 2p - 5 \) and \( X \cdot \beta z \in (z) \), then \( X \in (z, \beta z) \).

**Proof.** Write \( X \cdot \beta z = A \cdot z \) with \( A \) homogeneous in \( H^*(\mathfrak{g}) \). Then \( A \cdot \beta z = 0 \). As \( |A \cdot \beta z| = |X| + 4 \leq 2p - 1 \), and \( A \cdot \beta z \in (v_1, \ldots, v_{2k}) \), it follows from Lemma 2(ii) that \( A \cdot \beta z = 0 \). By [5] Lemma 2.1, \( A \in (\beta z, u_1 \cdots u_{2k}) \). Then \( A \in (\beta z) \), as \( |A| \leq 2p - 4 \). Write \( A = B \cdot \beta z \). Then we have \( (X - B \cdot \beta z) = 0 \). Again, by [5] Lemma 2.1, \( X - B \cdot \beta z \in (\beta z) \). Therefore \( X \in (z, \beta z) \). The lemma is proved. \( \square \)

For every \( 1 \leq j \leq p - 1 \), let \( B_j \) be a set of elements of \( \Lambda_{2j} \) such that the disjoint union \( B_j \cup \{\alpha^j\} \) forms a basis of \( \Lambda_{2j} \). We then have a decomposition

\[ H^*(\mathfrak{g}) \otimes \Lambda_{2j} = H^*(\mathfrak{g}) \otimes ((B_j) \oplus \{\alpha^j\}), 1 \leq j \leq p - 1. \]

For \( 1 \leq i < p - 1 \) and for \( 0 \neq b \in \langle B_i \rangle, \mu \in Z/p \), as \( |b - \mu \alpha^j| = 2i < 2p - 2 \), it follows from Lemma 2 that \( (b - \mu \alpha^j) \cdot \alpha \neq 0 \). Let \( \alpha^j \) be chosen such that, for every \( 1 \leq i < p - 1 \),

\[ \{b \cdot \alpha | 0 \neq b \in \langle B_i \rangle \} \subset \langle B_{i+1} \rangle. \]

**Lemma 4.** \( y^{p-1} y_1 \notin (z, \beta z) \).
Proof. Note that, as $\mathfrak{R}$ is of exponent $p$, $y^{p-1}y_1|_{(a_1)} \neq 0$. So $y^{p-1}y_1 \neq 0$.

Suppose that $y^{p-1}y_1 = A \cdot z + B \cdot \beta z$ with $A, B$ homogeneous in $H^*(G)$. Write $A = A' + A''$ with $A' \in H^*(\mathfrak{R}) \otimes \Lambda$, $A'' \in (v_1, \ldots, v_{2k})$. It follows that $y^{p-1}y_1 = A' \cdot z$ and $A'' \cdot z + B \cdot \beta z = 0$. Hence, without loss of generality, we may assume that $y^{p-1}y_1 = A \cdot z$ with $A \in H^*(\mathfrak{R}) \otimes \Lambda$. By the decomposition (4), we have

$$A = A_{2p-2} + \sum_{i=1}^{p-1} (A_{2p-2i-2} \cdot \alpha^i + \sum_{b \in B_i} A_{2p-2i-2b} \cdot b)$$

with $A_j, A_j, b \in H^*(\mathfrak{R})$. By (5), it follows that

$$A_{2p-2}y = y^{p-1}y_1,$$

$$(A_{2p-2} + A_{2p-4}) \cdot \alpha = 0,$$

$$\ldots$$

$$(A_2 + A_0y) \cdot \alpha^{p-1} = 0.$$

Therefore, for every $i \geq 1$, $A_{2i} = -A_{2i-2}$. So $y^{p-1}y_1 = A_0y^p$. As $y^{p-1}y_1|_{(a)} = 0$, this implies $A_0 = 0$. Hence $y^{p-1}y_1 = 0$, a contradiction. Thus $y^{p-1}y_1 \notin (z, \beta z)$. The lemma is proved.

Let $\{E_r, d_r\}$ be the Hochschild-Serre spectral sequence corresponding to the central extension

$$0 \rightarrow \mathbb{Z}/p^i \rightarrow G \rightarrow G \rightarrow 1$$

classified by $z \in H^2(G)$. Pick $s$ (resp. $t$) in $H^1(i(\mathbb{Z}/p))$ (resp. $H^2(i(\mathbb{Z}/p))$) satisfying $d_2(s) = z$ (resp. $d_3(t) = \beta z$). It is known that

$$E_2 = H^*(G) \otimes H^*(i(\mathbb{Z}/p)),$$

$$E_3 = H^*(G)/(z) \otimes \mathbb{F}_p[t] \oplus \text{Ann}_H^*(G)(z) \otimes \mathbb{F}_p[t]s.$$

We have

**Lemma 5.** There exists no element $\eta \in E_2^{p-n-1}, n \geq 3$, satisfying $d_n(\eta) = y^{p-1}y_1$.

**Proof.** Suppose that $\eta$ is an element of $E_2^{2p-2r-1, 2r-1}, r \geq 2$, represented by $X \otimes t^{2r-1} \otimes s \in E_2^{2p-2r-1, 2r-1}$. Then $0 = d_2(X \otimes t^{2r-1} \otimes s) = X \cdot z \otimes t^{2r-1}$. So $X \cdot z = 0$. Since $|X| = 2p - 2r \leq 2p - 4$, $X = 0$ by Lemma 2. Hence $0 = d_2(\eta) \neq y^{p-1}y_1$.

Suppose now that $\eta \in E_3^{2p-2r-1, 2r} \otimes t^{2r-1}$ is represented by $X \otimes t^r \in E_3^{2p-2r-1, 2r} \otimes t^{2r-1}, r \geq 2$. If $r = 1$, then $y_1^{2p-1}y_2 \neq X \cdot \beta z = -d_3(X \otimes t)$ by Lemma 4. If $r \geq 2$, then $-rX \cdot \beta z \otimes t^{r-1} = d_3(X \otimes t^r) = 0$ in $E_3$. So $X \cdot \beta z = 0$. As $|X| = 2p - 2r - 1 \leq 2p - 5$, $X \in (z, \beta z)$ by Lemma 3. This implies $X \otimes t^r = 0$ in $E_4$ unless $r = p - 1$ and $X \in (\beta z)$. But $r = p - 1$ also implies $|X| = 2p - 2r - 1 = 1$ and $X \in (\beta z)$, hence $X = 0$. So $0 = d_{2r+1}(\eta) \neq y^{p-1}y_1$. The lemma is proved.

**Proof of the Theorem.** Set $\xi = \text{Inf}_G^*(U)$. By Lemma 1, $\xi^p = y^{p-1}y_1$. Since $z$ vanishes in $H^*(G)$, $y^p = -\alpha^p = 0$ in $H^*(G)$. So $\xi^{2p} = y^{2^{p-2}}y_2^p = 0$. Hence $\xi$ is nilpotent. Besides, Lemmas 4 and 5 show that $y^{p-1}y_1 \notin \ker \text{Inf}_G^*$, which means that $\xi^p = y^{p-1}y_1 \neq 0$. The Theorem is proved.
REFERENCES


DEPARTMENT OF MATHEMATICS, COLLEGE OF SCIENCES, UNIVERSITY OF HUE, HUE, VIETNAM

E-mail address: paminh@dng.vnn.vn