NILPOTENCY DEGREE OF COHOMOLOGY RINGS
IN CHARACTERISTIC TWO

GEORGE S. AVRUNIN AND JON F. CARLSON

ABSTRACT. In this paper, we consider the cohomology ring of a finite 2-group
with coefficients in a field of characteristic two. We show that, for any posi-
tive integer n, there exists a 2-group whose cohomology ring has elements of
nilpotency degree $n + 1$ and all smaller degrees.

1. INTRODUCTION

It is well known that the cohomology rings of finite groups with coefficients
in fields of positive characteristic can contain nilpotent elements. But these
cohomology rings are difficult to determine, so we do not know the detailed
structure of very many examples. In particular, nothing appears to be known
about the possible nilpotency degrees of elements in these rings. In this paper,
we construct a family of finite groups G_n such that, for any field K of charac-
teristic two, the cohomology ring $H^*(G_n, K)$ contains elements of nilpotency
degree j for all $j \leq n + 1$. Unfortunately, our methods do not generalize to
the case of odd characteristic. Indeed, if K is a field of odd characteristic p,
we know of no examples of elements of $H^*(G, K)$ having nilpotency degree
greater than p.

2. THE GROUP G_n

Fix an integer $n > 1$ and a field K of characteristic two. We describe a group
$G = G_n$ in terms of an abelian normal subgroup N, the quotient Q, and the
2-cohomology class corresponding to the central extension $N \rightarrowtail G \twoheadrightarrow Q$.

Let $N = \langle a_1, \ldots, a_n \rangle$ and $Q = \langle z_1, \ldots, z_n \rangle$ be elementary abelian 2-
groups of rank n. Then the cohomology rings $H^*(N, K)$ and $H^*(Q, K)$
are polynomial rings in n indeterminates over K. We write $H^*(N, K) =
K[\alpha_1, \ldots, \alpha_n]$ and $H^*(Q, K) = K[\zeta_1, \ldots, \zeta_n]$, where α_i is the element of
$\mathrm{Hom}(N, K) = H^1(N, K)$ dual to a_i and ζ_j is the element of $\mathrm{Hom}(Q, K)$
dual to z_j.

Let $E_*^{*,*}$ be the Lyndon-Hochschild-Serre spectral sequence for the coho-
mology of the extension with coefficients in K. Since N is central in G,

Q acts trivially on $H^*(N, K)$ and $E_2^{r,s} = H^r(Q, H^s(N, K)) \cong H^r(Q, K) \otimes_K H^s(N, K)$. If $\chi \in Z^2(Q, N)$ is a cocycle representing the class of the extension $N \rightarrowtail G \twoheadrightarrow Q$, then the differential $d_2^{0,1} : H^1(N, K) \to H^2(Q, H^0(N, K)) = H^2(Q, K)$ is given by $d_2^{0,1}([\mu]) = [\mu \circ \chi]$. Specifying appropriate values for the $d_2^{0,1}(\alpha_i)$ thus determines the class of χ and so the structure of G.

For $i = 1, \ldots, n$, define an element $\tau_i \in H^2(Q, K)$ by

$$
\tau_i = \begin{cases} \zeta_1^2 & \text{for } i = 1, \\ \zeta_{i-1}\zeta_i + \zeta_i^2 & \text{for } i = 2, \ldots, n. \end{cases}
$$

Now define $d_2^{0,1}$ by $d_2^{0,1}(\alpha_i) = \tau_i$.

A corresponding χ describing the extension $N \rightarrowtail G \twoheadrightarrow Q$ is then given by

$$
\chi\left(\sum \varepsilon_i z_i, \sum \varepsilon_i' z_i\right) = \varepsilon_1 \varepsilon_1' a_1 + (\varepsilon_1 \varepsilon_2' + \varepsilon_2 \varepsilon_2') a_2 + \cdots + (\varepsilon_{n-1} \varepsilon_n' + \varepsilon_n \varepsilon_n') a_n,
$$

where the $\varepsilon_i, \varepsilon_i' \in \mathbb{F}_2$. The group G is thus a group of order 2^{2n} generated by elements $u_1, \ldots, u_n$ subject to the relations $u_i^4 = 1$, $[u_i, u_{i-1}] = u_i^2$, and $[u_i, u_j] = 1$ if $j \neq i - 1, i + 1$.

3. THE SPECTRAL SEQUENCE

Let $R = K[x_1, \ldots, x_n]$ be a polynomial ring in n indeterminates over K. Using the somewhat nonstandard, but convenient, notation of [2], we define the Koszul complex of R as follows.

Definition 3.1. For each $i = 0, \ldots, n$, let $\mathscr{K}_i(R)$ be the free R-module with basis consisting of the symbols $b(S)$ indexed by the set of all subsets $S \subseteq \{1, \ldots, n\}$ with $|S| = i$. Define $\delta_i : \mathscr{K}_i(R) \to \mathscr{K}_{i+1}(R)$ by

$$
\delta_i(f \cdot b(S)) = \sum_{j \notin S} x_j f \cdot b(S \cup \{j\}), \quad \text{for all } f \in R.
$$

Then $\delta_{i+1}\delta_i = 0$ and

$$
\mathscr{K}(R): 0 \to \mathscr{K}_0(R) \xrightarrow{\delta_0} \mathscr{K}_1(R) \xrightarrow{\delta_1} \cdots \xrightarrow{\delta_{n-1}} \mathscr{K}_n(R) \to 0
$$

is the *Koszul complex* of R.

Except for the indexing, $\mathscr{K}(R)$ is the standard projective resolution of K as R-module [3], and we know its cohomology.

Lemma 3.1. *The cohomology* $H^*(\mathscr{K}(R))$ *is* $H^n(\mathscr{K}(R)) = K$.

Definition 3.2. Let A be a finitely generated R-module. The *Koszul complex of* A, $\mathscr{K}(A)$, is defined to be $\mathscr{K}(A) = A \otimes_R \mathscr{K}(R)$.

Now make $H^*(Q, K) = K[\zeta_1, \ldots, \zeta_n]$ into an R-module by setting $x_i \cdot f(\zeta_1, \ldots, \zeta_n) = \tau_i f(\zeta_1, \ldots, \zeta_n)$. By [6, Proposition 3.1], $H^*(Q, K)$ is a free R-module. It follows that $H^i(\mathscr{K}(H^*(Q, K)))$ is zero unless $i = n$, and we see that $H^n(\mathscr{K}(H^*(Q, K)))$ is isomorphic to $H^*(Q, K)/I$, where I is the ideal generated by the τ_i, as in the previous section.

Consider an element $\mu = f(\zeta_1, \ldots, \zeta_n) \otimes \alpha_1^{e_1} \cdots \alpha_n^{e_n}$ in $E_2^{p, e_1 + \cdots + e_n}$. Since d_2 is a derivation, $d_2(\alpha_i^{e_i})$ is zero when e_i is even. Thus,

$$d_2(\mu) = \sum f(\zeta_1, \ldots, \zeta_n)\tau_i \otimes \alpha_1^{e_1} \cdots \alpha_i^{e_i - 1} \cdots \alpha_n^{e_n},$$

where the sum is taken over those i such that e_i is odd. If the e_i are all even, we see that the complex

$$0 \to H^*(Q, K) \otimes \alpha_1^{e_1+1} \cdots \alpha_n^{e_n+1} \xrightarrow{d_2} \sum_i H^*(Q, K) \otimes \alpha_1^{e_1+1} \cdots \alpha_i^{e_i} \cdots \alpha_n^{e_n+1} \xrightarrow{d_2}$$

$$\cdots \xrightarrow{d_2} \sum_i H^*(Q, K) \otimes \alpha_1^{e_1} \cdots \alpha_i^{e_i+1} \cdots \alpha_n^{e_n} \xrightarrow{d_2} H^*(Q, K) \otimes \alpha_1^{e_1} \cdots \alpha_n^{e_n} \to 0$$

is isomorphic to the Koszul complex $\mathscr{K}(H^*(Q, K))$. Since E_2 is a direct sum of such complexes and the cohomology of each complex is $H^*(Q, K)/I$ in degree n, we have proved

Theorem 3.2. $E_3^{*,*} \simeq H^*(Q, K)/I \otimes K[\alpha_1^2, \ldots, \alpha_n^2]$.

Corollary 3.3. $E_\infty^{*,*} = E_3^{*,*}$.

Proof. We have seen that each α_i^2 survives to E_3, and we note that $\alpha_i^2 = \beta(\alpha_i)$, where β is the Bockstein operator. Since the transgression commutes with the Steenrod operations [4, II.9.c], we have $d_3(\alpha_i^2) = \beta(\tau_i)$, which is zero in E_3. It follows that each α_i^2 survives to infinity, and then that all the higher differentials in the spectral sequence are zero. □

4. THE QUOTIENT $H^*(Q, K)/(\tau_1, \ldots, \tau_n)$

We now exhibit elements of the ring $E_3^{*,0} = E_2^{*,0}/d_2(E_2^{*,1})$ having nilpotency degrees $2, \ldots, n+1$. Since $E_3^{*,0} = E_\infty^{*,0}$ is a subring of $H^*(G, K)$, we will therefore produce elements of the same nilpotency degrees in the cohomology ring $H^*(G, K)$.

Let I be the ideal generated by the elements $\tau_1, \ldots, \tau_n$. Then I is the image of d_2 in $E_2^{*,0}$. We use Gröbner bases to show that, modulo I, the element ζ_i is nilpotent of degree $i + 1$.

We recall some basic definitions and results. Let k be a field and let $k[x_1, \ldots, x_m]$ be the polynomial ring in m indeterminates over k. Fix any order of the monomials $x_1^{i_1} \cdots x_m^{i_m}$ such that

    (1) If $a < b$ then $ac < bc$ for any monomials a, b, and c, and
    (2) $a < ab$ for all monomials a and $b \neq 1$.

We can write any $f \in k[x_1, \ldots, x_m]$ as a k-linear combination of monomials. The nonzero term $a_{(i_1, \ldots, i_m)} x_1^{i_1} \cdots x_m^{i_m}$ such that $x_1^{i_1} \cdots x_m^{i_m}$ is as large as possible with respect to the order $<$ is called the *principal term* of f. The monomial $x_1^{i_1} \cdots x_m^{i_m}$ is called the *principal monomial* of f.

Now let B be a finite set of polynomials. A polynomial f is said to be *reduced* with respect to B if the principal monomial of f is not divisible by the principal monomial of any element of B. By subtracting multiples of elements of B from f, we can obtain a reduced polynomial that is congruent to f modulo the ideal generated by the elements of B; such a polynomial is

a *reduction of* f with respect to B. A set of generators B for an ideal I is called a *Gröbner basis* for I if, for every polynomial $f \in I$, every reduction of f with respect to B is zero. (In such a case, we say f *reduces to zero with respect to* B.) We will need the following theorems [1].

Theorem 4.1. *Let f and g be any two nonzero polynomials, and let f_p and g_p be their principal terms. The S-polynomial of f and g, $S(f, g)$, is*

$$S(f, g) = \frac{h}{f_p} f - \frac{h}{g_p} g,$$

where h is the least common multiple of f_p and g_p. A set of generators B is a Gröbner basis if and only if $S(f, g)$ reduces to zero with respect to B for every $f, g \in B$.

Theorem 4.2. *Let B be a Gröbner basis for an ideal I, and let $f \in k[x_1, \ldots, x_m]$. Then $f \in I$ if and only if f reduces to zero with respect to B.*

Now consider $H^*(Q, K) = K[\zeta_1, \ldots, \zeta_n]$. We order the monomials lexicographically with $\zeta_n > \zeta_{n-1} > \cdots > \zeta_1$. Then, for each $i = 1, \ldots, n$, the principal term of τ_i is ζ_i^2.

Proposition 4.3. *The set $\{\tau_1, \ldots, \tau_n\}$ is a Gröbner basis for the ideal $I = (\tau_1, \ldots, \tau_n)$.*

Proof. We have $S(\tau_i, \tau_j) = \zeta_j^2 \tau_i + \zeta_i^2 \tau_j$, which reduces to zero. □

Proposition 4.4. *For $j = 1, \ldots, n$, $\zeta_j^j \notin I$ and $\zeta_j^{j+1} \in I$.*

Proof. The element $\zeta_1 \cdots \zeta_j$ is congruent to ζ_j^j modulo $(\tau_1, \ldots, \tau_n)$, so it suffices to show that $\zeta_1 \cdots \zeta_j$ does not belong to I. But $\zeta_1 \cdots \zeta_j$ is reduced with respect to the Gröbner basis $\{\tau_1, \ldots, \tau_n\}$.

Clearly, $\zeta_1^2 = \tau_1 \in I$. For $j > 1$, we have

$$\zeta_j^{j+1} = \zeta_{j-1}^j \zeta_j + \left(\sum_{k=0}^{j-1} \zeta_{j-1}^{j-1-k} \zeta_j^k \right) \tau_j,$$

so ζ_j^{j+1} does belong to I. □

Thus, the image of ζ_j in $E_3^{1,0} = E_\infty^{1,0}$ has nilpotency degree $j + 1$.

We sketch another argument. The quotient $K[\zeta_1, \ldots, \zeta_n]/I$ is a finite-dimensional algebra, so the set $\{\tau_1, \ldots, \tau_n\}$ is a system of parameters and the corresponding variety is a complete intersection. Then $K[\zeta_1, \ldots, \zeta_n]/I$ has dimension exactly 2^n. This is a consequence of Bézout's Theorem. Unfortunately, we know of no really good reference. The reader is referred to [5] for a general treatment or to [7, Appendix 6] for something more specific.

From this, it is easy to see that the set consisting of the monomials $\zeta_1^{i_1} \cdots \zeta_n^{i_n}$ for which each i_k is either zero or one is a basis for $K[\zeta_1, \ldots, \zeta_n]/I$, and this implies that the element $\zeta_1 \cdots \zeta_j$ is not in I for $j = 1, \ldots, n$. Since ζ_j^j is congruent to $\zeta_1 \cdots \zeta_j$ modulo I, ζ_j^j does not belong to I.

References

1. B. Buchberger, *Theoretical basis for the reduction of polynomials to canonical forms*, ACM SIGSAM Bull. **39** (1976), 19–29.

2. Jon F. Carlson, *Projective resolutions and degree shifting for cohomology and group rings*, preprint, Proceedings of the Tsukuba Workshop on Representations of Algebras, August, 1990 (to appear).

3. Saunders Mac Lane, *Homology*, Grundlehren Math. Wiss., vol. 114, Springer-Verlag, Berlin, 1963.

4. Jean-Pierre Serre, *Homologie singulière des espaces fibrés*, Ann. of Math. (2) **54** (1951), 425–505.

5. _____, *Algèbre locale—multiplicités*, Lecture Notes in Math., vol. 11, Springer-Verlag, Berlin, 1965.

6. Richard P. Stanley, *Invariants of finite groups and their applications to combinatorics*, Bull. Amer. Math. Soc. (N.S.) **1** (1979), 475–511.

7. Oscar Zariski and Pierre Samuel, *Commutative algebra*, vol. II, Van Nostrand, New York, 1960.

DEPARTMENT OF MATHEMATICS AND STATISTICS, UNIVERSITY OF MASSACHUSETTS, AMHERST, MASSACHUSETTS 01003
E-mail address: avrunin@math.umass.edu

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF GEORGIA, ATHENS, GEORGIA 30602
E-mail address: jfc@math.uga.edu