Proceedings of the Edinburgh Mathematical Society (2013) **56**, 151–175
DOI:10.1017/S001309151200017X

NILPOTENCE IN GROUP COHOMOLOGY

NICHOLAS J. KUHN

Department of Mathematics, University of Virginia, Charlottesville, VA 22904, USA (njk4x@virginia.edu)

Abstract We study bounds on nilpotence in $H^*(BG)$, the mod p cohomology of the classifying space of a compact Lie group G. Part of this is a report of our previous work on this problem, updated to reflect the consequences of Peter Symonds's recent verification of Dave Benson's Regularity Conjecture. New results are given for finite p-groups, leading to good bounds on nilpotence in $H^*(BP)$ determined by the subgroup structure of the p-group P.

Keywords: group cohomology; classifying spaces; invariant theory

2010 *Mathematics subject classification:* Primary 20J06
Secondary 55R40

1. Introduction

Fixing a prime p, let $H^*(BG)$ denote the mod p cohomology ring of the classifying space of a compact Lie group G. This is a graded commutative $\mathbb{F}_p$-algebra of great interest as it is the home for mod p characteristic classes of principal G bundles. Furthermore, when G is finite, this ring identifies with $\mathrm{Ext}^*_{\mathbb{F}_p[G]}(\mathbb{F}_p, \mathbb{F}_p)$, and so contains much detailed module theoretic information.

Precise calculation of $H^*(BG)$ can be daunting, particularly when G is a finite p-group. In this paper we study nilpotence in $H^*(BG)$. We offer some updates of our previous work in [**17**], together with new results in the finite p-group case.

We should be more precise about what we mean by 'nilpotence'.

Let $\mathrm{Rad}(G)$ be the nilradical of the graded $\mathbb{F}_p$-algebra $H^*(BG)$. One can define an 'algebraic' nilpotence degree as follows.

Definition 1.1. Define $d^{\mathrm{alg}}(G)$ to be the maximal d such that $\mathrm{Rad}(G)^d \neq 0$.

As the mod p cohomology of a topological space, $H^*(BG)$ is in the category $\mathcal{U}$, the category of modules over the mod p Steenrod algebra $\mathcal{A}_p$ which satisfy the unstable condition. Following Henn *et al.* in [**15**], one can define a 'topological' nilpotence degree as follows. Let $\Sigma^d M$ denote the dth suspension (upward shift) of a graded module M.

Definition 1.2. Define $d^{\mathcal{U}}(G)$ to be the maximal d such that $H^*(BG)$ contains a non-zero submodule of the form $\Sigma^d M$, with $M \in \mathcal{U}$.

This definition is clearly just dependent on the $\mathcal{A}_p$ module structure of $H^*(BG)$, but results in [**15**] allow for comparison with $d^{\mathrm{alg}}(G)$. As will be reviewed in § 2,

$$d^{\mathrm{alg}}(G) \leqslant \begin{cases} d^{\mathcal{U}}(G) & \text{if } p = 2, \\ d^{\mathcal{U}}(G) + r(G) & \text{if } p \text{ is odd.} \end{cases}$$

Here $r(G)$ is the maximal rank of an elementary abelian p-subgroup of G.

Our goal here is to describe how to calculate $d^{\mathcal{U}}(G)$, and, in particular, to give good group theoretic upper bounds. We note that $d^{\mathcal{U}}(\mathbb{Z}/p) = 0$ and $d^{\mathcal{U}}(G \times H) = d^{\mathcal{U}}(G) + d^{\mathcal{U}}(H)$. Furthermore, by transfer arguments, $d^{\mathcal{U}}(G) \leqslant d^{\mathcal{U}}(P)$ if P is a p-Sylow subgroup of a finite group G, and a similar inequality holds for a general compact Lie group G, with P now the evident extension of a maximal torus T by a p-Sylow subgroup of $N_G(T)/T$.

1.1. A general bound on $d^{\mathcal{U}}(G)$

Notation 1.3. Throughout the paper, we let E denote an elementary abelian p-group, i.e. a group isomorphic to $(\mathbb{Z}/p)^r$ for some r. We let $E^{\#}$ denote the dual of E. As mentioned above, $r(G)$ will denote the maximal rank of $E < G$. Let $C(G) < G$ be the maximal central elementary abelian p-subgroup, and let $c(G)$ denote its rank.

We recall from [**17**] the definition of a key invariant.

Definition 1.4. Via restriction, $H^*(\mathrm{BC}(G))$ is a finitely generated $H^*(BG)$-module, and we let $e(G)$ denote the top degree of a generator.

Theorem 1.5. *If G is compact Lie, then*

$$\max_{\substack{E<G,\\ r(E)=r(G)}} \{e(C_G(E)) - \dim(C_G(E))\} \leqslant d^{\mathcal{U}}(G) \leqslant \max_{E<G} \{e(C_G(E)) - \dim(C_G(E))\}.$$

Here $\dim(G)$ denotes the dimension of a Lie group G as a manifold, and so it is 0 if G is finite.

In the theorem, the indexing for the upper bound can be restricted to E which contain $C(G)$. Thus, the lower bound equals the upper bound when $c(G) = r(G)$, i.e. G is *p-central* (a group in which every element of order p is central) and, in that case, $d_0^{\mathcal{U}}(G) = e(G) - \dim G$.

The proof of Theorem 1.5 is given in § 2. Most of this is a review and slight reorganization of work in [**17**], with results extended to all compact Lie groups. Some of our results were previously conditional on the verification of Dave Benson's Regularity Conjecture [**3**], which conjectured the vanishing of certain local cohomology groups. Happily, this is now a theorem of Peter Symonds's [**24**], and we make very precise how the vanishing of local cohomology groups allows for improvement on Theorem 1.5.

1.2. Bounds for finite p-groups

Further investigations of $e(P)$ when P is a finite p-group led to some good bounds on cohomology nilpotence determined by subgroup structure.

https://doi.org/10.1017/S001309151200017X Published online by Cambridge University Press

The following monotonicity theorem at first surprised us, as it is false for arbitrary finite groups.

Theorem 1.6. *Let Q be a subgroup of a p-group P. Then $e(Q) \leqslant e(P)$.*

An immediate first consequence is that the upper bound given in Theorem 1.5 simplifies.

Theorem 1.7. *If P is a p-group, then $d^{\mathcal{U}}(P) \leqslant e(P)$.*

We then make further use of Theorem 1.6. The theorem, when combined with an explicit calculation of the e-invariant of the p-Sylow subgroups of the symmetric groups, leads to the next estimate of $e(P)$.

Theorem 1.8. *Suppose a p-group P acts faithfully on a set S with no fixed points. Then*

$$e(P) \leqslant \begin{cases} |S|/2 - |S/P| & \text{if } p = 2, \\ 2|S|/p - |S/P| & \text{if } p \text{ is odd.} \end{cases}$$

Here $|S|$ is the cardinality of S.

Another new general bound on $e(P)$ is the following.

Theorem 1.9. *Let $A < P$ be an abelian subgroup of maximal order in a p-group P. Then $e(P) \leqslant c(P)(2|P|/|A| - 1)$.*

The last two theorems are nicely illustrated by the following example.

Example 1.10. Let P be a 2-Sylow subgroup of the finite group $\mathrm{SU}(3,4)$. P is a 2-central group of order 64, of exponent 4, with $C(P) = [P,P] \simeq \mathbb{Z}/2 \times \mathbb{Z}/2$; see [**18**, § 6.3] for a useful description of this group. Both theorems give us the estimate $e(P) \leqslant 14$, which, in fact, computation shows equals $e(P)$, and thus $d^{\mathcal{U}}(P)$.

To use Theorem 1.8, let $a, b \in P$ be elements of order 4 with $a^2 \neq b^2$. Then P acts faithfully on $S = P/\langle a \rangle \coprod P/\langle b \rangle$ with no fixed points, so $e(P) \leqslant 32/2 - 2 = 14$.

To use Theorem 1.9, the centralizer of any element of order 4 is isomorphic to $\mathbb{Z}/4 \times \mathbb{Z}/4$; thus, $e(P) \leqslant 2[2(64/16) - 1] = 14$.

Theorem 1.9 is proved using Chern classes of representations, and would be a special case of the next conjecture, where we let $n(G)$ denote the minimal dimension (over $\mathbb{C}$) of a faithful complex representation of G.

Conjecture 1.11. *If G is compact Lie, then $e(G) \leqslant 2n(G) - c(G)$.*

If this conjecture were true, one could easily deduce that $d^{\mathcal{U}}(G) \leqslant 2n(G) - c(G)$; see Remark 3.11. This should be compared with the estimate in [**15**]: $d^{\mathcal{U}}(G) \leqslant n(G)^2$.

Section 3 contains the proofs of Theorems 1.8 and 1.9, a discussion of the conjecture and the beginning of our most subtle argument: the proof of Theorem 1.6. Proved by induction on the order of P, in § 3 it is reduced to a problem about invariants of arbitrary $\mathbb{Z}/p$ actions on sub-Hopf algebras of polynomial algebras over $\mathbb{F}_p$; see Problem 3.13. This we then deal with in § 4, proving results in invariant theory which appear to be new, and should be of independent interest.

https://doi.org/10.1017/S001309151200017X Published online by Cambridge University Press

Remark 1.12. We note that our paper [**17**] has tables of examples made using Jon Carlson's cohomology website [**9**]. Thousands more examples are now similarly accessible using the cohomology website of David Green and Simon King [**13**]. Their implementation includes the calculation of the restriction of $H^*(BP)$ to $H^*(\mathrm{BC}(P))$, so that $e(P)$ can be immediately read off from their data. For example, one can see that if P is the 2-Sylow subgroup of the third Conway group, and P therefore has order 1024, then $e(P) = 7$ and so, combining Theorem 1.7 with the fine points of Theorem 2.22, we see that $d^{\mathcal{U}}(P) \leqslant 6$.

2. Old results revisited

In this section, we prove the bounds for $d^{\mathcal{U}}(G)$ given in Theorem 1.5. The main steps are as follows, where terminology and notation will be defined in due course:

- $d^{\mathcal{U}}(G) = \max\{d_0(\mathrm{Cess}^*(BC_G(E))) \mid E < G\}$ (see Proposition 2.8);
- $d_0(\mathrm{Cess}^*(BG)) = e_{\mathrm{prim}}(G)$ (see Corollary 2.14);
- $e_{\mathrm{prim}}(G) \leqslant e_{\mathrm{indec}}(G)$ (see Corollary 2.20);
- $e_{\mathrm{indec}}(G) \leqslant e(G) - \dim G$ (see Theorem 2.22 for this and a bit more).

The last inequality refines using local cohomology as follows:

- $e_{\mathrm{indec}}(G) = e(G) + \max\{e \mid H_{\mathfrak{m}}^{c(G),-c(G)+e}(H^*(BG)) \neq 0\}$ (see Theorem 2.29);
- $H_{\mathfrak{m}}^{s,t}(H^*(BG)) = 0$ if $s + t > -\dim G$; this is Symonds's Theorem [**24**].

2.1. The basic ring structure of $H^*(BG)$

We begin by recalling a fundamental example. If $E = (\mathbb{Z}/p)^r$ and if $H^1(E) \simeq E^{\#}$ has basis $x_1, \dots, x_r$, then

$$H^*(BE) \simeq \begin{cases} \mathbb{F}_2[x_1, \dots, x_r] & \text{if } p = 2, \\ \Lambda(x_1, \dots, x_r) \otimes \mathbb{F}_p[y_1, \dots, y_r] & \text{if } p \text{ is odd,} \end{cases}$$

where $y_i = \beta(x_i)$ (β is the Bockstein homomorphism). Furthermore, addition $E \times E \to E$ induces a primitively generated Hopf algebra structure on $H^*(BE)$.

More generally, $H^*(BG)$ can be difficult to compute explicitly, particularly when G is a more interesting finite p-group. For example, if P is the 2-Sylow subgroup of $SU_3(4)$, as in Example 1.10, a minimal presentation of the algebra $H^*(BP)$ has 26 generators (in degrees up to 11) and 270 relations (in degrees up to 22); see [**10**, Group #187], or [**13**, Group #145].

In spite of this, some basic ring structure has been known for a long time. In the late 1960s, Quillen [**21**] showed that $H^*(BG)$ is noetherian of Krull dimension $r(G)$; equivalently, $H^*(BG)$ is a finitely generated module over a polynomial subalgebra on $r(G)$ generators. A decade later, Duflot [**11**] showed that its depth is at least $c(G)$; equivalently, $H^*(BG)$ is a free module over a polynomial subalgebra on $c(G)$ generators.

https://doi.org/10.1017/S001309151200017X Published online by Cambridge University Press

Remark 2.1. The extreme situation, when $c(G) = r(G)$, happens precisely when G is p-central. Then $H^*(BG)$ will be Cohen–MacCauley: the depth of $H^*(BG)$ will equal its Krull dimension. In general, there is no group theoretic criterion characterizing either groups G such that the depth of $H^*(BG)$ equals the lower bound $c(G)$, or groups G such that the depth of $H^*(BG)$ equals the upper bound $r(G)$.

Quillen's idea was to probe $H^*(BG)$ by its restrictions to its elementary abelian p-subgroups. The product over all such restrictions gives a ring homomorphism

$$q_0 \colon H^*(BG) \to \prod_{E<G} H^*(BE).$$

Recall that, given $K < G$, the restriction map $H^*(BG) \to H^*(BK)$ makes $H^*(BK)$ into a finitely generated $H^*(BG)$-module. Thus, the codomain of q_0, a ring whose Krull dimension is clearly $r(G)$, is finitely generated over $H^*(BG)$. Quillen then shows that $\ker(q_0)$ is nilpotent, which then immediately implies the result about Krull dimension.

2.2. The nilpotent filtration of $\mathcal{U}$

As the mod p cohomology of a topological space, $H^*(BG)$ is an unstable algebra over the mod p Steenrod algebra $\mathcal{A}_p$. When $p = 2$, we recall that an $\mathcal{A}_p$-module M is unstable if $Sq^k x = 0$ whenever $k > |x|$. When p is odd, the condition is that $\beta^e P^k x = 0$ if $2k + e > |x|$. M is an unstable algebra if, in addition, it is a graded commutative algebra satisfying both the Cartan and restriction formulae.

The 1980s featured much remarkable work on $\mathcal{K}$ and $\mathcal{U}$, the categories of unstable algebras and modules, with the algebras $H^*(BE)$ playing a special role (see [**23**] for an introduction to the extensive literature).

In the 1995 paper [**15**], Henn *et al*. revisited Quillen's work from this new perspective. Following [**15**], we have the following definition.

Definition 2.2. If M is an unstable $\mathcal{A}_p$-module, let $d_0(M)$ be the maximal d such that M contains a non-zero submodule of the form $\Sigma^d N$, with N unstable. If no such maximum exists, let $d_0(M) = \infty$, and let $d_0(\mathbf{0}) = -\infty$.

Thus, the invariant $d^{\mathcal{U}}(G)$ of the introduction is $d_0(H^*(BG))$.

An alternative definition, easily shown to be equivalent to the one above, is that $d_0(M)$ is the length of the nilpotent filtration [**22**] of M,

$$\cdots \subset \operatorname{nil}_d M \subset \operatorname{nil}_{d-1} \subset \operatorname{nil}_1 M \subset \operatorname{nil}_0 M = M,$$

where $\operatorname{nil}_d M$ is the large submodule in the localizing subcategory of $\mathcal{U}$ generated by the d-fold suspensions.

Three elementary properties of $d_0(M)$ are stated in the next lemma.

https://doi.org/10.1017/S001309151200017X Published online by Cambridge University Press

Lemma 2.3.

(a) *If M is non-zero in degree d, but zero in all higher degrees, then $d_0(M) = d$.*

(b) *If $0 \to M_1 \to M_2 \to M_3 \to 0$ is a short exact sequence in $\mathcal{U}$, then $d_0(M_1) \leqslant d_0(M_2)$ and $d_0(M_2) \leqslant \max\{d_0(M_1), d_0(M_3)\}$.*

(c) $d_0(H^*(B\mathbb{Z}/p)) = 0$.

The next properties are considerably deeper. References for (a) are [**16**, Proposition 2.5] or [**15**, Proposition I.3.6]. Property (b) concerns Lannes's functor [**20**] $T_E\colon \mathcal{U} \to \mathcal{U}$, the left adjoint to the functor $M \rightsquigarrow H^*(BE) \otimes M$, and a reference is [**17**, Proposition 3.12]. Property (c) is due to Henn [**14**].

Proposition 2.4.

(a) $d_0(M \otimes N) = d_0(M) + d_0(N)$.

(b) $d_0(T_E M) = d_0(M)$.

(c) *$d_0(M) < \infty$ if M is a finitely generated module over an noetherian unstable algebra K with structure map $K \otimes M \to M$ in $\mathcal{U}$.*

2.3. The comparison between $d^{\mathbf{alg}}(G)$ and $d^{\mathcal{U}}(G)$

Note that Proposition 2.4 (c) implies that $d^{\mathcal{U}}(G) < \infty$, so that the nilpotent filtration of $H^*(BG)$ has finite length.

In [**15**], Henn *et al.* show how to generalize Quillen's map q_0 to realize the nilpotent filtration of $H^*(BG)$. For each $d \geqslant 0$, let

$$q_d\colon H^*(BG) \to \prod_E H^*(BE) \otimes H^{\leqslant d}(BC_G(E))$$

be the map of unstable algebras with components induced by the group homomorphisms $E \times C_G(E) \to G$. Here $M^{\leqslant d}$ denotes the quotient of a graded module M by all elements of degree more than d.

They observe that $\ker q_d = \mathrm{nil}_{d+1} H^*(BG)$, and so we have the following.

Proposition 2.5. *$d^{\mathcal{U}}(G)$ is the minimal d such that q_d is monic.*

If I is a nilpotent ideal in a graded noetherian ring, let $d^{\mathrm{alg}}(I)$ be the maximal d such that $I^d \neq 0$. Thus, the invariant $d^{\mathrm{alg}}(G)$ of the introduction is $d^{\mathrm{alg}}(\mathrm{Rad}(G))$. Note that

$$d^{\mathrm{alg}}(H^*(BE) \otimes \tilde{H}^{\leqslant d}(BC_G(E))) = \begin{cases} d^{\mathrm{alg}}(\tilde{H}^{\leqslant d}(BC_G(E))) & \text{if } p = 2, \\ d^{\mathrm{alg}}(\Lambda(E^{\#}) \otimes \tilde{H}^{\leqslant d}(BC_G(E))) & \text{if } p \text{ is odd.} \end{cases}$$

Corollary 2.6. *With $d = d^{\mathcal{U}}(G)$,*

$$d^{\mathrm{alg}}(G) \leqslant \begin{cases} \max\limits_E\{d^{\mathrm{alg}}(\tilde{H}^{\leqslant d}(BC_G(E)))\} \leqslant d & \text{if } p = 2, \\ \max\limits_E\{d^{\mathrm{alg}}(\tilde{H}^{\leqslant d}(BC_G(E))) + r(E)\} \leqslant d + r(G) & \text{if } p \text{ is odd.} \end{cases}$$

https://doi.org/10.1017/S001309151200017X Published online by Cambridge University Press

2.4. Central essential cohomology

The following definition from [**17**] is a variant of Carlson's Depth Essential Cohomology [**10**].

Definition 2.7. Let $\mathrm{Cess}^*(BG)$ be the kernel of the map

$$H^*(BG) \to \prod_{C(G) \lneqq E} H^*(BC_G(E)).$$

This is an unstable $\mathcal{A}$-module. $\mathrm{Cess}^*(BG) = H^*(BG)$ exactly when the product is over the empty set, i.e. G is p-central. $\mathrm{Cess}^*(BG)$ can also be zero: as we shall see, $\mathrm{Cess}^*(BG) \neq 0$ if and only if the depth of $H^*(BG) = c(G)$.

Proposition 2.8. $d^{\mathcal{U}}(G) = \max\{d_0(\mathrm{Cess}^*(BC_G(E))) \mid E < G\}$.

To prove this, we first need the following consequence of the calculation of $T_E H^*(BG)$ due to Lannes [**19**].

Proposition 2.9. *For all $E < G$, $H^*(BC_G(E))$ is a summand of $T_E H^*(BG)$, and thus $d^{\mathcal{U}}(C_G(E)) \leqslant d^{\mathcal{U}}(G)$.*

Proof of Proposition 2.8. This follows by downward induction on the rank of $C(G)$. From the exact sequence

$$0 \to \mathrm{Cess}^*(BG) \to H^*(BG) \to \prod_{C(G) \lneqq E} H^*(BC_G(E)),$$

one sees that

$$d^{\mathcal{U}}(G) \leqslant \max\{d_0(\mathrm{Cess}^*(BG)), d^{\mathcal{U}}(C_G(E)) \mid C(G) \lneqq E < G\}.$$

But this inequality is an equality by Proposition 2.9. □

2.5. Primitives in central essential cohomology

For the rest of this section, we fix a compact Lie group G, and let $C = C(G)$.

By an unstable $H^*(BC)$-comodule, we shall mean an unstable module M having an $H^*(BC)$-comodule structure map $\Delta\colon M \to H^*(BC) \otimes M$ that is in the category $\mathcal{U}$. Examples of interest to us include $H^*(BG)$, $H^*(BC_G(E))$ for all $E < G$ and $\mathrm{Cess}^*(BG)$, where the comodule structures are all induced by the group homomorphism $C \times G \to G$ sending (c, g) to cg.

Definition 2.10. If M is an unstable $H^*(BC)$-comodule, we define its associated module of primitives to be

$$P_C M = \{x \in M \mid \Delta(x) = 1 \otimes x\} = \mathrm{Eq}\Big\{M \underset{i}{\overset{\Delta}{\rightrightarrows}} H^*(C) \otimes M\Big\}.$$

If $P_C M$ is finite dimensional, we let $e_{\mathrm{prim}}(M)$ be its largest non-zero degree, or $-\infty$ if $M = \mathbf{0}$.

Note that $P_C M$ is again an unstable module.

https://doi.org/10.1017/S001309151200017X Published online by Cambridge University Press

Lemma 2.11. *If M is an unstable $H^*(BC)$-comodule, and P_CM is finite dimensional, then $d_0(M) = e_{\rm prim}(M)$.*

Proof. Assume P_CM is finite dimensional with largest non-zero degree $e = e_{\rm prim}(M)$. Then $e = d_0(P_CM)$. Since P_CM is an unstable submodule of M, $d_0(P_CM) \leqslant d_0(M)$. Finally, the composite

$$M \xrightarrow{\Delta} H^*(BC) \otimes M \twoheadrightarrow H^*(BC) \otimes M^{\leqslant e}$$

will be monic, so that

$$d_0(M) \leqslant d_0(H^*(BC) \otimes M^{\leqslant e}) = d_0(M^{\leqslant e}) = e.$$

□

Proposition 2.12. *$P_C\mathrm{Cess}^*(BG)$ is finite dimensional.*

Proof. Theorem 8.5 of [**17**] implies that if $P_C\mathrm{Cess}^d(BG) \neq 0$, then $d \leqslant d^{\mathcal{U}}(G)$. □

Remark 2.13. The careful reader will discover that [**17**, Theorem 8.5] has a rather delicate proof, using related results in [**18**], all based on careful analysis of formulae in [**15**]. It would be nice to have a simpler proof of the proposition. In the next subsection we shall see (Corollary 2.19) that $P_C\mathrm{Cess}^*(BG)$ is finite dimensional if and only if $\mathrm{Cess}^*(BG)$ has Krull dimension equal to $c(G)$. When G is finite, this Krull dimension calculation is verified [**17**, Proposition 8.2] using a result of Carlson [**8**].

We let $e_{\rm prim}(G)$ denote $e_{\rm prim}(\mathrm{Cess}^*(BG))$.

Corollary 2.14. $d_0(\mathrm{Cess}^*(BG)) = e_{\rm prim}(G)$.

2.6. Duflot algebras

Let $c = c(G)$, the rank of $C = C(G)$, so that

$$H^*(BC) \simeq \begin{cases} \mathbb{F}_2[x_1, \dots, x_c] & \text{if } p = 2, \\ \Lambda(x_1, \dots, x_c) \otimes \mathbb{F}_p[y_1, \dots, y_c] & \text{if } p \text{ is odd.} \end{cases}$$

The image of the restriction homomorphism $i^*\colon H^*(BG) \to H^*(BC)$ will be a sub-Hopf algebra of $H^*(BC)$. After a change of basis for $H^1(BC)$, it will have the form

$$\mathrm{im}(i^*) = \begin{cases} \mathbb{F}_2[x_1^{2^{j_1}}, \dots, x_c^{2^{j_c}}] & \text{if } p = 2, \\ \mathbb{F}_p[y_1^{p^{j_1}}, \dots, y_b^{p^{j_b}}, y_{b+1}, \dots, y_c] \otimes \Lambda(x_{b+1}, \dots, x_c) & \text{if } p \text{ is odd,} \end{cases}$$

with the j_i forming a sequence of non-increasing non-negative integers (see [**6**, Remark 1.3] and [**1**].) In the odd prime case, $c - b$ has group theoretic meaning as the rank of the largest subgroup of C splitting off G as a direct summand.

https://doi.org/10.1017/S001309151200017X Published online by Cambridge University Press

As in [**17**], we shall say that G has *type* $[a_1, \dots, a_c]$, where

$$(a_1, \dots, a_c) = \begin{cases} (2^{j_1}, \dots, 2^{j_c}) & \text{if } p = 2, \\ (2p^{j_1}, \dots, 2p^{j_b}, 1, \dots, 1) & \text{if } p \text{ is odd.} \end{cases}$$

Recall that $e(G)$ is defined to be the largest degree of an $H^*(BG)$-module generator of $H^*(BC)$, i.e. the top degree of the finite-dimensional Hopf algebra $H^*(BC) \otimes_{H^*(BG)} \mathbb{F}_p$. Note that this number is determined by the type of G:

$$e(G) = \sum_{i=1}^{c} (a_i - 1).$$

Since $\mathrm{im}(i^*)$ is a *free* commutative algebra, one can split the epimorphism of rings $i^* \colon H^*(BG) \twoheadrightarrow \mathrm{im}(i^*)$, and make the next definition.

Definition 2.15. A *Duflot algebra* of $H^*(BG)$ is a subalgebra $A \subseteq H^*(BG)$, such that $i^* \colon A \to \mathrm{im}(i^*)$ is an isomorphism.

Remark 2.16. It seems unclear whether a Duflot algebra can always be chosen to also be closed under Steenrod operations. Nor does it seem that it can always be chosen to be a sub-$H^*(BC)$-comodule of $H^*(BG)$.

2.7. Indecomposables in central essential cohomology

For the rest of the section, now also fix a Duflot algebra $A \subseteq H^*(BG)$.

Definition 2.17. If M is an A-module, we define the A-indecomposables to be $Q_A M = M \otimes_A \mathbb{F}_p$. If $Q_A M$ is finite dimensional, we let $e_{\mathrm{indec}}(M)$ be its largest non-zero degree, or $-\infty$ if $M = \mathbf{0}$.

Observe that everything in the exact sequence

$$0 \to \mathrm{Cess}^*(BG) \to H^*(BG) \to \prod_{C \lneq E} H^*(BC_G(E))$$

is both an A-module and an $H^*(BC)$-comodule. These structures are sufficiently compatible 'up to filtration' that one can prove the following.

Proposition 2.18. *The following hold.*

(a) $\mathrm{Cess}^*(BG)$ *is a free* A*-module.*

(b) *The composite* $P_C \mathrm{Cess}^*(BG) \hookrightarrow \mathrm{Cess}^*(BG) \twoheadrightarrow Q_A \mathrm{Cess}^*(BG)$ *is monic.*

(c) *The sequence*

$$0 \to Q_A \mathrm{Cess}^*(BG) \to Q_A H^*(BG) \to \prod_{C \lneq E} Q_A H^*(BC_G(E))$$

is exact.

See [**17**, Proposition 8.1].

https://doi.org/10.1017/S001309151200017X Published online by Cambridge University Press

Corollary 2.19. *$Q_A\mathrm{Cess}^*(BG)$ is finite dimensional if and only if $P_C\mathrm{Cess}^*(BG)$ is finite dimensional. In this case, $e_{\mathrm{prim}}(\mathrm{Cess}^*(BG)) \leqslant e_{\mathrm{indec}}(\mathrm{Cess}^*(BG))$.*

Proof. For notational simplicity, let $M = \mathrm{Cess}^*(BG)$. The proposition immediately implies that if Q_AM is finite dimensional, so is P_CM, and the stated inequality will hold. Conversely, suppose P_CM is finite dimensional. Recall that the composite (of A-modules)

$$M \xrightarrow{\Delta} H^*(BC) \otimes M \to H^*(BC) \otimes M^{\leqslant e_{\mathrm{prim}}(M)}$$

is monic. As $H^*(BC) \otimes M^{\leqslant e_{\mathrm{prim}}(M)}$ is certainly a finitely generated A-module, so is M. □

We let $e_{\mathrm{indec}}(G)$ denote $e_{\mathrm{indec}}(\mathrm{Cess}^*(BG))$.

Corollary 2.20. *$\mathrm{Cess}^*(BG)$ is a finitely generated free A-module, and $e_{\mathrm{prim}}(G) \leqslant e_{\mathrm{indec}}(G)$.*

Remark 2.21. As we observed computationally in [**17**, Appendix A], $e_{\mathrm{prim}}(G) = e_{\mathrm{indec}}(G)$ for all finite 2-groups G of order dividing 32. We suspect that this pattern will not continue, but it would be nice to have an explicit example for which the inequality of the corollary is strict.

2.8. Local cohomology and Symonds's Theorem

The last step in our proof of Theorem 1.5 is the verification of the next bound.

Theorem 2.22. *For all G, $e_{\mathrm{indec}}(G) \leqslant e(G) - \dim G$. The inequality is strict unless G is p-central. If G is p-central, then $d_{\mathcal{U}}(G) = e_{\mathrm{prim}}(G) = e_{\mathrm{indec}}(G) = e(G) - \dim G$.*

We first note that, even when p is odd, it suffices to prove this when the Duflot algebra A is a polynomial algebra, i.e. when G has no $\mathbb{Z}/p$ direct summands, as $d_{\mathcal{U}}(G\times E) = d_{\mathcal{U}}(G)$, $e_{\mathrm{prim}}(G \times E) = e_{\mathrm{prim}}(G)$, $e_{\mathrm{indec}}(G \times E) = e_{\mathrm{indec}}(G)$ and $e(G \times E) = e(G)$.

We need to begin with a quick summary of definitions and properties of local cohomology. A general reference for this is [**5**].

Let $\mathfrak{m}$ be a maximal ideal in a graded noetherian ring R. For M an R-module,

$$M \mapsto H^{s,*}_{\mathfrak{m}}(M)$$

is defined to be the sth right derived functor of

$$M \mapsto H^{0,*}_{\mathfrak{m}}(M) = \text{the } \mathfrak{m}\text{-torsion part of } M.$$

Proposition 2.23. *$H^{s,*}_{\mathfrak{m}}(M) \neq 0$ only if $\mathrm{depth}_{\mathfrak{m}}M \leqslant s \leqslant \dim M$. Furthermore, if $s = \mathrm{depth}_{\mathfrak{m}}M$ or $s = \dim M$, then $H^{s,*}_{\mathfrak{m}}(M) \neq 0$.*

This is the content of [**5**, Corollary 6.2.8].

We need some related results about how local cohomology interacts with regular M-sequences. Let $|z|$ denote the degree of $z \in R$.

https://doi.org/10.1017/S001309151200017X Published online by Cambridge University Press

Lemma 2.24. *Fix (s,t), and suppose that $H_{\mathfrak{m}}^{s',t'}(M)=0$ for $s'<s$ and for (s,t') with $t'>t$. If $z\in R$ is an M-regular element, then $H_{\mathfrak{m}}^{s',t'}(M/(z))=0$ for $s'<s-1$ and for $(s-1,t')$ with $t'>t+|z|$, and, furthermore,*

$$H_{\mathfrak{m}}^{s-1,t+|z|}(M/(z))\simeq H_{\mathfrak{m}}^{s,t}(M).$$

Proof. By assumption, z is not a zero divisor of M, so there is a short exact sequence of R-modules

$$0\to\Sigma^{|z|}M\xrightarrow{z}M\to M/(z)\to 0.$$

The lemma then follows from the associated long exact sequence, which has the form

$$\cdots\to H_{\mathfrak{m}}^{s'-1,t'+|z|}(M)\to H_{\mathfrak{m}}^{s'-1,t'+|z|}(M/(z))\to H_{\mathfrak{m}}^{s',t'}(M)\to H_{\mathfrak{m}}^{s',t'+|z|}(M)\to\cdots.$$

□

By induction on the length of a regular sequence, the lemma has the following corollary.

Corollary 2.25. *With assumptions on (s,t) and M as in the lemma, if $z_1,\dots,z_s$ is an M-regular sequence, then $H_{\mathfrak{m}}^{0,t'}(M/(z_1,\dots,z_s))=0$ for $t'>t+|z_1|+\cdots+|z_s|$, and*

$$H_{\mathfrak{m}}^{0,t+|z_1|+\cdots+|z_s|}(M/(z_1,\dots,z_s))\simeq H_{\mathfrak{m}}^{s,t}(M).$$

We now apply this in the case when $R=M=H^*(BG)$ and $\mathfrak{m}=\tilde{H}^*(BG)$. Let $c=c(G)$ and $r=r(G)$. If $z_1,\dots,z_c$ are algebra generators for the Duflot algebra A, then $|z_1|+\cdots+|z_s|=c+e(G)$, and $M/(z_1,\dots,z_c)=Q_AM$, and the corollary tells us the following.

Proposition 2.26. *Suppose $H_{\mathfrak{m}}^{c(G),-c(G)+e'}(H^*(BG))=0$ for all $e'>e$. Then*

$$H_{\mathfrak{m}}^{0,e(G)+e'}(Q_AH^*(BG))=0$$

for all $e'>e$, and

$$H_{\mathfrak{m}}^{0,e(G)+e}(Q_AH^*(BG))=H_{\mathfrak{m}}^{c,-c+e}(H^*(BG)).$$

Now we note the following.

Proposition 2.27. $Q_A\mathrm{Cess}^*(BG)=H_{\mathfrak{m}}^{0,*}(Q_A\mathrm{Cess}^*(BG))=H_{\mathfrak{m}}^{0,*}(Q_AH^*(BG))$.

Our argument is similar to that proving [**17**, Proposition 8.9]. We need the following lemma.

Lemma 2.28 (Kuhn [17, Lemma 8.8]). *Assume $c<r$. Given any sequence $z_1,\dots,z_c\in H^*(G)$ that generates the polynomial algebra A, there exists $z\in H^*(BG)$ such that, for all proper inclusions $C<E$, $z_1,\dots,z_c,z$ restricts to a regular sequence in $H^*(BC_G(E))$.*

https://doi.org/10.1017/S001309151200017X Published online by Cambridge University Press

Proof of Proposition 2.27. As $Q_A\mathrm{Cess}^*(BG)$ is finite dimensional, we clearly have

$$Q_A\mathrm{Cess}^*(BG) = H^{0,*}_{\mathfrak{m}}(Q_A\mathrm{Cess}^*(BG)).$$

By Proposition 2.18, we have an exact sequence

$$0 \to Q_A\mathrm{Cess}^*(BG) \to Q_AH^*(BG) \to \prod_{C \lneqq E} Q_AH^*(BC_G(E)),$$

and this induces an exact sequence

$$0 \to H^{0,*}_{\mathfrak{m}}(Q_A\mathrm{Cess}^*(BG)) \to H^{0,*}_{\mathfrak{m}}(Q_AH^*(BG)) \to \prod_{C \lneqq E} H^{0,*}_{\mathfrak{m}}(Q_AH^*(BC_G(E))).$$

But the last term here is 0, because if $z \in H^*(BG)$ is chosen as in the lemma, then z will act regularly on each $Q_AH^*(BC_G(E))$ with $C(G) \lneqq E$. □

The last two propositions combine to prove the next theorem.

Theorem 2.29. $e_{\mathrm{indec}}(G) = e(G) + \max\{e \mid H^{c(G),-c(G)+e}_{\mathfrak{m}}(H^*(BG)) \neq 0\}$.

Proof of Theorem 2.22. Symonds [**24**] has proved that

$$H^{s,t}_{\mathfrak{m}}(H^*(BG)) = 0 \quad \text{if } s + t > -\dim G.$$

Combined with Theorem 2.29, this immediately implies the first part of the theorem: for all compact Lie groups G,

$$e_{\mathrm{indec}}(G) \leqslant e(G) - \dim G.$$

Furthermore, this inequality will be strict if and only if

$$H^{c(G),-c(G)-\dim(G)}_{\mathfrak{m}}(H^*(BG)) = 0.$$

To deduce more, we need to recall why Symonds's result (in the finite group case) had been conjectured by Benson. As constructed by Greenlees and Benson [**4**], there is a spectral sequence

$$H^{s,t}_{\mathfrak{m}}(H^*(BG)) = E_2^{s,t} \Rightarrow \tilde{H}_{-s-t}(EG_+ \wedge_G S^{\mathrm{Ad}(G)}; \mathbb{F}_p),$$

where $S^{\mathrm{Ad}(G)}$ is the one point compactification of the adjoint representation, so Benson was conjecturing that some evident vanishing at the level of E_∞ had already happened at E_2.

By Symonds's Theorem, the group $H^{c(G),-c(G)-\dim(G)}_{\mathfrak{m}}(H^*(BG))$ consists of permanent cycles, as the differentials leaving this group will take values in groups that are zero. As this group is certainly not in the image of non-zero boundary maps, it will thus be a quotient of

$$\tilde{H}_{\dim(G)}(EG_+ \wedge_G S^{\mathrm{Ad}(G)}; \mathbb{F}_p) \simeq \begin{cases} \mathbb{F}_p & \text{if } \mathrm{Ad}(G) \text{ is } \mathbb{F}_p\text{-oriented,} \\ 0 & \text{otherwise.} \end{cases}$$

https://doi.org/10.1017/S001309151200017X Published online by Cambridge University Press

In the oriented case, $H_{\mathfrak{m}}^{r(G),-r(G)-\dim(G)}(H^*(BG)) \simeq \mathbb{F}_p$, by a generalization to all compact Lie groups of Benson's argument [**2**] in the finite group case. (The generalization is straightforward, using the transfer map $H^*(BE) \to H^{*+\dim(G)}(BG)$ associated to an inclusion $E < G$.)

Thus, in both the oriented and non-oriented cases, we see that

$$H_{\mathfrak{m}}^{c(G),-c(G)-\dim(G)}(H^*(BG)) = 0$$

unless $c(P) = r(P)$, i.e. G is p-central. In the p-central case, G will be oriented and $e_{\mathrm{indec}}(G) = e(G)$. But, arguing as in [**17**], one can do better: the top class in $Q_A H^*(BG)$ will be represented by an $H^*(BC)$-primitive, so $e_{\mathrm{prim}}(G) = e_{\mathrm{indec}}(G)$. □

We end this section by noting that our results above include a proof of Carlson's Depth Conjecture in the case of minimal depth, generalizing results in [**12**, **17**]. Note that

$$e_{\mathrm{indec}}(G) \neq -\infty \Leftrightarrow e_{\mathrm{indec}}(G) \geqslant 0 \Leftrightarrow Q_A \mathrm{Cess}^*(G) \neq 0 \Leftrightarrow \mathrm{Cess}^*(G) \neq 0$$

and

$$H_{\mathfrak{m}}^{c(G),*}(H^*(BG)) \neq 0 \Leftrightarrow H^*(BG) \text{ has depth precisely } c(G).$$

Therefore, Theorem 2.29 tells us most of the following, and Symonds's Theorem tells us the rest.

Theorem 2.30. *For G compact Lie, $H^*(BG)$ has depth precisely $c(G)$ if and only if $H^*(BG)$ is not detected by restriction to the cohomology rings $H^*(BC_G(E))$ for $E < G$ of rank greater than $c(G)$. In this case, $H_{\mathfrak{m}}^{c(G),t}(H^*(BG)) \neq 0$ for some $-c(G)-\dim(G) \leqslant t \leqslant -c(G) - e(G)$.*

Corollary 2.31. *If G is compact Lie, and $e(G) < \dim(G)$, then $H^*(BG)$ has depth greater than $c(G)$ and is detected by restriction to the cohomology rings $H^*(BC_G(E))$ for $E < G$ of rank greater than $c(G)$.*

3. New results for finite p groups

We now prove various new results about $e(P)$ when P is a finite p-group. We begin with a proof of Theorem 1.9, with part of the discussion relevant for all compact Lie groups G. We shall next deduce Theorems 1.7 and 1.8, while assuming Theorem 1.6. Finally, we shall reduce Theorem 1.6 to a problem in invariant theory, to be solved in the subsequent section.

3.1. Upper bounds for $e(P)$ coming from Chern classes

We use Chern classes of representation to get group theoretic upper bounds for $e(P)$ when P is a finite p-group. With $C = C(P)$, we need to get a lower bound on $\mathrm{im}(i^*)$, the image of restriction

$$i^* \colon H^*(BP) \to H^*(BC).$$

https://doi.org/10.1017/S001309151200017X Published online by Cambridge University Press

To set up notation and unify exposition, let $c = c(P)$ and let

$$H^*(BC) \simeq \begin{cases} \mathbb{F}_2[x_1, \dots, x_c] & \text{if } p = 2, \\ \Lambda(x_1, \dots, x_c) \otimes \mathbb{F}_p[y_1, \dots, y_c] & \text{if } p \text{ is odd,} \end{cases}$$

where $y_i \in H^2(BC)$ denotes $\beta(x_i)$ for all primes (so that $y_i = x_i^2$ when $p = 2$). Note that each element y_i is the Chern class of a unique one-dimensional complex representation ω_i of C.

Now let $A < P$ be a maximal abelian subgroup, so that A certainly contains C. Each ω_i extends, possibly non-uniquely, to a one-dimensional representation $\tilde{\omega}_i$ of A. Now let $\rho_i = \mathrm{Ind}_A^P(\tilde{\omega}_i)$, a representation of P of dimension $[P\colon A] = |P|/|A|$.

By construction, the restriction of ρ_i to C will be $|P|/|A|\omega_i$, which has top Chern class $y_i^{|P|/|A|}$. We have proved the next theorem, a precise form of Theorem 1.9.

Theorem 3.1. *The Hopf algebra* $\mathrm{im}(i^*)$ *contains* $\mathbb{F}_p[y_1^{|P|/|A|}, \dots, y_c^{|P|/|A|}]$. *Thus,* $e(P) \leqslant c(P)(2|P|/|A| - 1)$.

Remark 3.2. Let $e_{\mathrm{grp}}(P) = c(P)(2|P|/|A| - 1)$, where $A < P$ is an abelian subgroup of maximal order; thus, the theorem says that $e(P) \leqslant e_{\mathrm{grp}}(P)$. With arguments similar, but simpler, to ones we shall use in the proof of Theorem 1.6, it is not hard to prove that this invariant of p-groups has the following monotonicity property:

$$\text{if } Q < P, \text{ then } e_{\mathrm{grp}}(Q) \leqslant e_{\mathrm{grp}}(P).$$

This property suffices to deduce that if P is a finite p-group, then $d^{\mathcal{U}}(P) \leqslant e_{\mathrm{grp}}(P)$:

$$d^{\mathcal{U}}(P) \leqslant \max_{E<G}\{e(C_G(E))\} \leqslant \max_{E<G}\{e_{\mathrm{grp}}(C_G(E))\} \leqslant e_{\mathrm{grp}}(P).$$

3.2. Conjectural upper bounds for $e(G)$ coming from Chern classes

We continue in the spirit of the last subsection, and discuss how one might use Chern classes to prove Conjecture 1.11. This says that, if $n(G)$ is the minimal dimension of a faithful representation of a compact Lie group G, then $e(G) \leqslant 2n(G) - c(G)$.

With $C = C(G)$, the calculation of $e(G)$ requires understanding of the Hopf algebra $\mathrm{im}(i^*)$, the image of the restriction

$$i^*\colon H^*(BG) \to H^*(BC).$$

Definition 3.3.

(a) If ρ is a representation of C, let $\mathcal{H}(\rho) \subset H^*(BC)$ be the smallest Hopf algebra containing its Chern classes.

(b) When ρ is faithful, so can be viewed as an inclusion of C into a unitary group U, $\mathcal{H}(\rho)$ will contain the image of $H^*(BU) \to H^*(BC)$, and thus $H^*(BC)$ will be a finitely generated $\mathcal{H}(\rho)$ module. In this case, let $e(\rho)$ be the top degree of $Q_{\mathcal{H}(\rho)}H^*(BC)$.

https://doi.org/10.1017/S001309151200017X Published online by Cambridge University Press

(c) If G is a compact Lie group with $C = C(G)$, let $\mathcal{H}(G)$ be the smallest Hopf algebra containing all of the $\mathcal{H}(\rho)$, where ρ ranges over all representations of G, restricted to C, and let $e_{rep}(G)$ be the top degree of $Q_{\mathcal{H}(\mathcal{G})}H^*(BC)$.

It is clear that for any representation ρ of G,

$$\mathcal{H}(\rho) \subseteq \mathcal{H}(G) \subseteq \mathrm{im}(i^*),$$

so we learn the following.

Proposition 3.4. $e(G) \leqslant e_{rep}(G) \leqslant e(\rho)$.

Thus, Conjecture 1.11 would follow immediately from the next conjecture, which just concerns Chern classes of representations of elementary abelian groups.

Conjecture 3.5. *Let C be an elementary abelian p-group of rank c. If ρ is a faithful n-dimensional complex representation of C, then $e(\rho) \leqslant 2n - c$.*

In turn, this conjecture would be consequence of a conjectural identification of the Hopf algebra $\mathcal{H}(\rho)$. To describe this, and for later purposes, we digress to describe a natural parametrization of the sub-Hopf algebras of a polynomial algebra.

3.3. Sub-Hopf algebras of a polynomial algebra

Let $S^*(V)$ be the symmetric algebra generated by an $\mathbb{F}_p$-vector space V. If $y_1, \ldots, y_c$ form a basis for V, then $S^*(V) = \mathbb{F}_p[y_1, \ldots, y_c]$. We describe a natural parametrization of the *full* sub-Hopf algebras of $S^*(V)$: sub-Hopf algebras $\mathcal{H} \subseteq S^*(V)$ having Krull dimension c.

We need the following notation: given a subspace $W < V$, $W^{(k)} \subset S^{p^k}(V)$ denotes the span of the p^kth powers of the elements in W.

Definition 3.6. Suppose $\mathcal{F}$ is a finite filtration of the $\mathbb{F}_p$-vector space V:

$$V(0) \subseteq V(1) \subseteq \cdots \subseteq V(n) = V.$$

Let $\mathcal{H}(\mathcal{F}) \subseteq S^*(V)$ be the Hopf algebra

$$\mathcal{H}(\mathcal{F}) = S^*(V(0) + V(1)^{(1)} + \cdots + V(n)^{(n)}).$$

Proposition 3.7. *Filtrations of V correspond bijectively to the full sub-Hopf algebras of $S^*(V)$, under the correspondence $\mathcal{F} \rightsquigarrow \mathcal{H}(\mathcal{F})$.*

Sketch proof. If $\mathcal{H} \subseteq S^*(V)$ is a full sub-Hopf algebra, then there are natural numbers $j_1, \ldots, j_c$, and a basis $\{y_1, \ldots, y_c\}$ of V, such that $\mathcal{H} = \mathbb{F}_p[y_1^{p^{j_1}}, \ldots, y_c^{p^{j_c}}]$. Then $\mathcal{H} = \mathcal{H}(\mathcal{F})$, where the filtration $\mathcal{F}$ of V has kth subspace $V(k)$ equal to the span of the y_i satisfying $j_i \leqslant k$. More intrinsically, $V(k)^{(k)} = \mathcal{H} \cap V^{(k)}$. □

https://doi.org/10.1017/S001309151200017X Published online by Cambridge University Press

Definition 3.8. If $\mathcal{F}$ is the filtration $V(0) \subseteq \cdots \subseteq V(n) = V$, let

$$e(\mathcal{F}) = \sum_{k=0}^{n} c_k(\mathcal{F})(2p^k - 1),$$

where $c_k(\mathcal{F})$ is the rank of $V(k)/V(k-1)$.

With this definition, if C is an elementary abelian p-group, $V = \beta(H^1(BC)) \subseteq H^2(BC)$ and $\mathcal{F}$ is a filtration of V, then $e(\mathcal{F})$ is the top degree of a generator of $H^*(BC)$, viewed as an $\mathcal{H}(\mathcal{F})$-module.

We now return to our discussion of Conjecture 3.5. So, suppose ρ is a faithful n-dimensional complex representation of C, where C has rank c. This will be a sum of line bundles, possibly with multiplicities, and so will correspond to the following data:

- a finite set of distinct elements $v_1, \ldots, v_m \in V$ which span V;
- multiplicities $n_1, \ldots, n_m \in \mathbb{N}$ such that $n_1 + \cdots + n_m = n$.

From this data, we define a filtration $\mathcal{F}_\rho$ of V by letting $V(k)$ be the span of the v_j such that p^{k+1} does not divide n_j.

Lemma 3.9. $\mathcal{H}(\rho) \subseteq \mathcal{H}(\mathcal{F}_\rho)$.

Proof. Let $\mathrm{ch}(\rho)$ denote the total Chern class. We shall have

$$\mathrm{ch}(\rho) = \prod_{j=1}^{m}(1+v_j)^{n_j} = \prod_{k} \prod_{v_j \in V(k)-V(k-1)} (1+v_j^{p^k})^{n_j/p^k}.$$

As $v_j^{p^k} \in \mathcal{H}(\mathcal{F}_\rho)$ for $v_j \in V(k) - V(k-1)$, we see that all the homogenous components of $\mathrm{ch}(\rho)$ are in $\mathcal{H}(\mathcal{F}_\rho)$ as well. □

We conjecture equality in the last lemma.

Conjecture 3.10. $\mathcal{H}(\rho) = \mathcal{H}(\mathcal{F}_\rho)$.

As the estimate $e(\mathcal{F}_\rho) \leqslant 2n - c$ is not hard to check, this conjecture implies Conjecture 3.5, and thus Conjecture 1.11.

Remark 3.11. Note that, for any $E < G$, $n(C_G(E)) \leqslant n(G)$ and $c(C_G(E)) \geqslant c(G)$. Thus, if Conjecture 1.11 were true, we could deduce

$$d^{\mathcal{U}}(G) \leqslant \max_{E<G}\{e(C_G(E))\} \leqslant \max_{E<G}\{2n(C_G(E)) - c(C_G(E))\} \leqslant 2n(G) - c(G).$$

3.4. Proofs of Theorems 1.7 and 1.8 assuming Theorem 1.6

Here we assume Theorem 1.6, which says that if P is a p-group, and $Q < P$, then $e(Q) \leqslant e(P)$, and we deduce Theorem 1.7 and Theorem 1.8.

Proof of Theorem 1.7. This is immediate: $d^{\mathcal{U}}(P) \leqslant \max_{E<P}\{e(C_P(E))\} \leqslant e(P)$. □

https://doi.org/10.1017/S001309151200017X Published online by Cambridge University Press

Proof of Theorem 1.8. Suppose a p-group P acts faithfully on a set S with no fixed points. We wish to show that $e(P) \leqslant |S|/2 - |S/P|$ when $p = 2$, and $e(P) \leqslant 2|S|/p - |S/P|$ when p is odd.

Note that S/P is the set of orbits of S, so S has a decomposition into orbits

$$S = \coprod_{i=1}^{|S/P|} S_i,$$

with $|S_i| = p^{r_i}$, and each $r_i \geqslant 1$. Then P admits an embedding

$$P \subseteq \prod_{i=1}^{|S/P|} W(r_i),$$

where $W(r)$ denotes the Sylow subgroup of the symmetric group Σ_{p^r}.

Assuming Theorem 1.6, we would then have the bound

$$e(P) \leqslant \sum_{i=1}^{|S/P|} e(W(r_i)).$$

The next proposition will thus complete the proof of Theorem 1.8. □

Proposition 3.12. *When $p = 2$, $e(W(r)) = 2^{r-1} - 1$. When p is odd, $e(W(1)) = 0$, and, for $r \geqslant 1$, $e(W(r)) = 2p^{r-1} - 1$.*

Proof. We begin by identifying $C(r) = C(W(r))$. We claim that $C(r) \simeq \mathbb{Z}/p$. This is easily proved by induction on r, as $W(r+1)$ is the semidirect product

$$W(r+1) = W(r)^p \rtimes \mathbb{Z}/p,$$

so that

$$C(r+1) = (C(r)^p)^{\mathbb{Z}/p},$$

the diagonal copy of $C(r)$ in $C(r)^p$.

Now we determine $\mathrm{im}(i(r)^*) \subset H^*(\mathrm{BC}(r))$, where $i(r)\colon C(r) \to W(r)$ is the inclusion.

The case when $r = 1$ is elementary: $C(1) = W(1) = \mathbb{Z}/p$, so $\mathrm{im}(i(1)^*) = H^*(B\mathbb{Z}/p)$ and $e(W(1)) = 0$ for all primes p.

To proceed by induction, we observe that the inclusions

$$C(r+1) \to C(r)^p \to W(r)^p \to W(r+1)$$

induce a factorization of $i(r+1)^*$ as

$$H^*(BW(r+1)) \twoheadrightarrow H^*(BW(r)^p)^{\mathbb{Z}/p} \xrightarrow{(i(r)^p)^*} H^*(\mathrm{BC}(r)^p)^{\mathbb{Z}/p} \to H^*(\mathrm{BC}(r+1)),$$

and the first map is epic as indicated.

https://doi.org/10.1017/S001309151200017X Published online by Cambridge University Press

Now let p be odd. Identifying $H^*(\mathrm{BC}(r))$ with $\Lambda(x) \otimes \mathbb{F}_p[y]$, we prove by induction that, for $r \geqslant 2$, $\mathrm{im}(i(r)^*) = \mathbb{F}_p[y^{p^{r-1}}]$ so that $e(W(r)) = 2p^{r-1} - 1$.

The case when $r = 2$ is slightly special: $\mathrm{im}(i(2)^*)$ will be the image of

$$(\Lambda(x_1, \dots, x_p) \otimes \mathbb{F}_p[y_1, \dots, y_p])^{\mathbb{Z}/p} \to \Lambda(x) \otimes \mathbb{F}_p[y]$$

under the map induced by sending each x_i to x and y_i to y. Recall also that this image will be a Hopf algebra. As y^p is the image of the invariant $y_1 \dots y_p$, while x and y are easily checked to not be in this image, we see that $\mathrm{im}(i(2)^*) = \mathbb{F}_p[y^p]$.

Assume by induction that $\mathrm{im}(i(r)^*) = \mathbb{F}_p[y^{p^{r-1}}]$. Then, reasoning as above,

$$\mathrm{im}(i(r+1)^*) = \mathrm{im}\{\mathbb{F}_p[y_1^{p^{r-1}}, \dots, y_p^{p^{r-1}}]^{\mathbb{Z}/p} \to \mathbb{F}_p[y]\} = \mathbb{F}_p[y^{p^r}].$$

The case when $p = 2$ is similar. Identifying $H^*(\mathrm{BC}(r))$ with $\mathbb{F}_2[x]$, one proves by induction that, for $r \geqslant 1$, $\mathrm{im}(i(r)^*) = \mathbb{F}_2[x^{2^{r-1}}]$ so that $e(W(r)) = 2^{r-1} - 1$. □

3.5. Reduction of Theorem 1.6 to invariant theory

We begin the proof of Theorem 1.6. Our goal is to show that, if Q is a subgroup of a p-group P, then $e(Q) \leqslant e(P)$. Thus, we need to somehow compare the image of the restriction

$$H^*(BP) \to H^*(\mathrm{BC}(P))$$

to the image of the restriction

$$H^*(BQ) \to H^*(\mathrm{BC}(Q)).$$

We make some initial reductions.

First of all, by induction of the index of Q in P, we can assume that Q has index p, and thus will be normal in P. Then $\mathbb{Z}/p \simeq P/Q$ will act on $H^*(BQ)$ and also on $C(Q)$, with $C(Q)^{\mathbb{Z}/p} = C(P) \cap Q$.

Next, suppose that $C(P)$ is not contained in Q. Then there would exist a central element $\sigma \in P$ of order p, not in Q. It follows easily that then $\langle\sigma\rangle \times Q = P$, and we conclude that $e(P) = e(Q)$.

Thus, we shall assume that $C(P)$ is contained in Q. Suppose P admits a direct product decomposition $P = \langle\sigma\rangle \times P_1$, with σ of order p. Then σ would be contained in $C(P)$ and thus $Q = \langle\sigma\rangle \times Q_1$ with $Q_1 = P_1 \cap Q$. Then $e(P) = e(P_1)$ and $e(Q) = e(Q_1)$.

We are reduced to needing to prove that $e(Q) \leqslant e(P)$ under the following assumptions:

- Q is normal of index p, so $\mathbb{Z}/p \simeq P/Q$ acts on both $H^*(BQ)$ and $C = C(Q)$;
- $C(P) = C^{\mathbb{Z}/p}$;
- P has no non-trivial elementary abelian direct summands.

https://doi.org/10.1017/S001309151200017X Published online by Cambridge University Press

In this situation, the restriction map $H^*(BP) \to H^*(C(P))$ factors

$$H^*(BP) \to H^*(BQ)^{\mathbb{Z}/p} \to H^*(BC)^{\mathbb{Z}/p} \hookrightarrow H^*(BC) \twoheadrightarrow H^*(BC^{\mathbb{Z}/p}),$$

and the last assumption tell us that the image lands in the part of $H^*(BC^{\mathbb{Z}/p})$ generated by $\beta(H^1(BC^{\mathbb{Z}/p}))$.

Let V denote $\beta(H^1(BC)) \subseteq H^2(BC)$. As V is naturally isomorphic to the dual of C, it can be viewed as a $\mathbb{Z}/p$-module. Let $V_{\mathbb{Z}/p}$ denote the $\mathbb{Z}/p$-coinvariants $V/\langle x - \sigma x \colon x \in V\rangle$, where σ generates $\mathbb{Z}/p$. The part of $H^*(BC^{\mathbb{Z}/p})$ generated by $\beta(H^1(BC^{\mathbb{Z}/p}))$ is identified with $S^*(V_{\mathbb{Z}/p})$.

As the image of $H^*(BQ) \to H^*(BC) \twoheadrightarrow S^*(V)$ is a Hopf algebra, it must be the Hopf algebra $\mathcal{H}(\mathcal{F})$ associated to a filtration $\mathcal{F}$ of V, and $e(Q) \leqslant e(\mathcal{F})$.

As the map $H^*(BQ) \to S^*(V)$ is $\mathbb{Z}/p$-equivariant, $\mathcal{H}(\mathcal{F})$ is a sub-$\mathbb{Z}/p$-module of $S^*(V)$. It follows that the filtration $\mathcal{F}$ will be preserved by the $\mathbb{Z}/p$ action on V.

From our observations above, the image of $H^*(BP) \to H^*(C(P))$ will be contained in the image of

$$\mathcal{H}(\mathcal{F})^{\mathbb{Z}/p} \hookrightarrow S^*(V)^{\mathbb{Z}/p} \hookrightarrow S^*(V) \twoheadrightarrow S^*(V_{\mathbb{Z}/p}).$$

As $e(Q) \leqslant e(\mathcal{F})$, we shall be able to deduce that $e(Q) \leqslant e(P)$ if we can solve the following problem in invariant theory.

Problem 3.13. *Given a filtration $\mathcal{F}$ of a $\mathbb{Z}/p$-module V, find a filtration $\mathcal{F}_{\mathbb{Z}/p}$ of $V_{\mathbb{Z}/p}$ such that*

- *the image of $\mathcal{H}(\mathcal{F})^{\mathbb{Z}/p} \to S^*(V_{\mathbb{Z}/p})$ is contained in $\mathcal{H}(\mathcal{F}_{\mathbb{Z}/p})$, and*
- *$e(\mathcal{F}) \leqslant e(\mathcal{F}_{\mathbb{Z}/p})$.*

In the next section we find such a filtration $\mathcal{F}_{\mathbb{Z}/p}$; see Theorem 4.6.

4. New results in invariant theory

In this section $\mathcal{F}$ is a filtration of an $\mathbb{F}_p[\mathbb{Z}/p]$-module V,

$$V(0) \subseteq V(1) \subseteq \cdots \subseteq V(n) = V,$$

and we wish to understand the image of the composite

$$\mathcal{H}(\mathcal{F})^{\mathbb{Z}/p} \hookrightarrow S^*(V)^{\mathbb{Z}/p} \hookrightarrow S^*(V) \twoheadrightarrow S^*(V_{\mathbb{Z}/p}),$$

with our goal being to solve Problem 3.13. Throughout we let σ be a generator for $\mathbb{Z}/p$.

4.1. $\mathbb{Z}/p$-modules

The modular representation theory of $\mathbb{Z}/p$ is quite tame. There are p indecomposable $\mathbb{F}_p[\mathbb{Z}/p]$-modules, $V_1, \ldots, V_p$, where V_i has dimension i. An explicit model for V_i is the vector space with basis $x_1, \ldots, x_i$ with

$$\sigma x_j = \begin{cases} x_j + x_{j-1} & \text{if } 1 < j \leqslant i, \\ x_1 & \text{if } j = 1. \end{cases}$$

https://doi.org/10.1017/S001309151200017X Published online by Cambridge University Press

A general $\mathbb{F}_p[\mathbb{Z}/p]$-module V decomposes as a direct sum

$$V \simeq m_1V_1 \oplus m_2V_2 \oplus \cdots \oplus m_pV_p.$$

We say that V is *trivial free* if $m_1 = 0$.

We let $\mathrm{rad}(V)$ and $\mathrm{soc}(V)$ be the radical and socle of a module V. Thus, $\mathrm{soc}(V) = V^{\mathbb{Z}/p}$ and $V/\mathrm{rad}(V) = V_{\mathbb{Z}/p}$. In the usual way, we define $\mathrm{soc}(V) \subset \mathrm{soc}^2(V) \subset \cdots$ and $\mathrm{rad}(V) \supset \mathrm{rad}^2(V) \supset \cdots$.

The submodule m_1V_1 in a decomposition of V can be regarded as the image of a section of the quotient map $\mathrm{soc}(V) \twoheadrightarrow (\mathrm{soc}(V)+\mathrm{rad}(V))/\mathrm{rad}(V)$. Thus, V is trivial free precisely when $\mathrm{soc}(V) \subset \mathrm{rad}(V)$, or, equivalently, when the composite $V^{\mathbb{Z}/p} \hookrightarrow V \twoheadrightarrow V_{\mathbb{Z}/p}$ is zero.

4.2. The case when the filtration is trivial

Given a $\mathbb{Z}/p$-module V, a special case of our general problem is to understand the image of

$$S^*(V)^{\mathbb{Z}/p} \hookrightarrow S^*(V) \twoheadrightarrow S^*(V_{\mathbb{Z}/p}).$$

We remark that, in spite of the simple classification of modules V, a complete calculation of $S^*(V)^{\mathbb{Z}/p}$ is not known in all cases, and is the subject of much research. Even so, we prove the following theorem.

Theorem 4.1. *If $V = W \oplus U$, where W is trivial and U is trivial free, the image of $S^*(V)^{\mathbb{Z}/p} \to S^*(V_{\mathbb{Z}/p})$ is $S^*(W \oplus U^{(1)}_{\mathbb{Z}/p})$.*

Here is a more invariant way of stating this. Given V, let $W_{\mathbb{Z}/p}$ be the image of the composite $V^{\mathbb{Z}/p} \hookrightarrow V \twoheadrightarrow V_{\mathbb{Z}/p}$. Then the image of

$$S^*(V)^{\mathbb{Z}/p} \hookrightarrow S^*(V) \twoheadrightarrow S^*(V_{\mathbb{Z}/p})$$

will be

$$S^*(W_{\mathbb{Z}/p} + V^{(1)}_{\mathbb{Z}/p}).$$

The next example both illustrates the theorem and will be used in its proof.

Example 4.2. Suppose that $V = mV_2$, where the ith copy of V_2 has basis $\{x_i, y_i\}$ with $\sigma y_i = y_i + x_i$ and $\sigma x_i = x_i$. The kernel of the quotient $V \twoheadrightarrow V_{\mathbb{Z}/p}$ is the span of the x_i, so we can view $V_{\mathbb{Z}/p}$ as having a basis given by the y_i. The theorem in this case asserts that the image of the composite

$$\mathbb{F}_p[x_1, \ldots, x_m, y_1, \ldots, y_m]^{\mathbb{Z}/p} \hookrightarrow \mathbb{F}_p[x_1, \ldots, x_m, y_1, \ldots, y_m] \twoheadrightarrow \mathbb{F}_p[y_1, \ldots, y_m]$$

is $\mathbb{F}_p[y_1^p, \ldots, y_m^p]$. The main theorem of [**7**] is a description of generators of $S^*(mV_2)^{\mathbb{Z}/p}$ as polynomials in the x_i and y_j; see also [**25**]. One sees that all of these are sent to 0 modulo the ideal $(x_1, \ldots, x_m)$ except for the 'norm' generators

$$\prod_{j=0}^{p-1} \sigma^j y_i = y_i^p - x_i^{p-1} y_i,$$

which map to y_i^p. So, the assertion of the theorem is true in this case.

https://doi.org/10.1017/S001309151200017X Published online by Cambridge University Press

Proof of Theorem 4.1. First we note that if $V = W \oplus U$ with W trivial, then $S^*(V)^{\mathbb{Z}/p} = S^*(W) \otimes S^*(U)^{\mathbb{Z}/p}$ and $S^*(W \oplus U^{(1)}_{\mathbb{Z}/p}) = S^*(W) \otimes S^*(U^{(1)}_{\mathbb{Z}/p})$.

Thus, it suffices to prove that, when V is trivial free, there is an equality

$$I(V) = S^*(V^{(1)}_{\mathbb{Z}/p}),$$

where $I(V) = \mathrm{im}\{S^*(V)^{\mathbb{Z}/p} \hookrightarrow S^*(V) \twoheadrightarrow S^*(V_{\mathbb{Z}/p})\}$.

The previous example showed that this holds when $V = mV_2$. We use this to show that the equality holds for a general trivial free V. Recall that $V_{\mathbb{Z}/p} = V/\mathrm{rad}(V)$. If we let $\bar{V} = V/\mathrm{rad}^2(V)$, and let $\tilde{V}$ be the projective cover of V, then $\bar{V} = mV_2$ and $\tilde{V} = mV_p$, if $V_{\mathbb{Z}/p} = mV_1$. The surjections $\tilde{V} \twoheadrightarrow V \twoheadrightarrow \bar{V}$ will induce isomorphisms $\tilde{V}_{\mathbb{Z}/p} = V_{\mathbb{Z}/p} = \bar{V}_{\mathbb{Z}/p}$, and then inclusions

$$I(\tilde{V}) \subseteq I(V) \subseteq I(\bar{V}) = S^*(V^{(1)}_{\mathbb{Z}/p}).$$

Finally, to see that all of these inclusions are, in fact, equalities, we note that $I(\tilde{V}_p)$ is easily seen to contain $S^*(V^{(1)}_{\mathbb{Z}/p})$: our proof of Proposition 3.12 showed that $I(V_p) = S^*(V_1^{(1)})$, and so $I(mV_p)$ certainly contains $S^*(mV_1^{(1)})$. □

4.3. The case when the filtration is non-trivial

Now suppose that there exists a decomposition of *filtered* $\mathbb{Z}/p$-modules $V = W \oplus U$, with W trivial and U trivial free. Define a filtration $\mathcal{F}_{\mathbb{Z}/p}$ of $V_{\mathbb{Z}/p}$ by letting

$$V_{\mathbb{Z}/p}(k) = (W(k) + U(k-1) + \mathrm{rad}(V))/\mathrm{rad}(V).$$

Proposition 4.3. *The image of* $\mathcal{H}(\mathcal{F})^{\mathbb{Z}/p} \to S^*(V_{\mathbb{Z}/p})$ *is contained in* $\mathcal{H}(\mathcal{F}_{\mathbb{Z}/p})$.

Proof. Just as in the proof of Theorem 4.1, it suffices to prove this when V is trivial free, and then $\mathcal{F}_{\mathbb{Z}/p}$ is defined by the simpler formula

$$V_{\mathbb{Z}/p}(k) = (V(k-1) + \mathrm{rad}(V))/\mathrm{rad}(V).$$

Also, similar to the proof of Theorem 4.1, we let $\bar{V} = V/\mathrm{rad}^2(V)$, with filtration $\bar{\mathcal{F}}$ defined by $\bar{V}(k) = (V(k) + \mathrm{rad}^2(V))/\mathrm{rad}^2(V)$. Then

$$\mathrm{im}\{\mathcal{H}(\mathcal{F})^{\mathbb{Z}/p} \to S^*(V_{\mathbb{Z}/p})\} \subseteq \mathrm{im}\{\mathcal{H}(\bar{\mathcal{F}})^{\mathbb{Z}/p} \to S^*(V_{\mathbb{Z}/p})\},$$

and the filtrations $\mathcal{F}_{\mathbb{Z}/p}$ and $\bar{\mathcal{F}}_{\mathbb{Z}/p}$ of $V_{\mathbb{Z}/p}$ agree. Thus, it suffices to also assume that V satisfies $\mathrm{rad}^2(V) = 0$, so that V is isomorphic to mV_2 for some m.

In this case, let elements $y_1, \ldots, y_m \in V$, of filtration $k_1, \ldots, k_m$, project to a filtered basis of $V_{\mathbb{Z}/p}$, and let $x_j = \sigma y_j - y_j$. Then

$$\mathcal{H}(\mathcal{F}) \subseteq \mathbb{F}_p[x_1, \ldots, x_m, y_1^{p^{k_1}}, \ldots, y_m^{p^{k_m}}]$$

as algebras with $\mathbb{Z}/p$ action, and so the image of $\mathcal{H}(\mathcal{F})^{\mathbb{Z}/p} \to S^*(V_{\mathbb{Z}/p})$ is contained in $\mathcal{H}(\mathcal{F}_{\mathbb{Z}/p}) = \mathbb{F}_p[y_1^{p^{k_1}+1}, \ldots, y_m^{p^{k_m}+1}]$, as this is the image of

$$\mathbb{F}_p[x_1, \ldots, x_m, y_1^{p^{k_1}}, \ldots, y_m^{p^{k_m}}]^{\mathbb{Z}/p} \to \mathbb{F}_p[y_1, \ldots, y_m].$$

□

https://doi.org/10.1017/S001309151200017X Published online by Cambridge University Press

4.4. The general case

Unfortunately, at least when $p \geqslant 3$, a general filtered $\mathbb{Z}/p$-module V need not admit a direct sum decomposition as *filtered* modules of the form $V = W \oplus U$, with W trivial and U trivial free.

Example 4.4. With $p \geqslant 3$, let $V(0) = V_2$, embedded 'diagonally' in $V_1 \oplus V_3 = V(1) = V$. Then the image of $\mathrm{soc}(V) \to V/\mathrm{rad}(V)$ is V_1, generated by an element of $V(0)$, but not of $\mathrm{soc}(V(0))$, and we see that there is no isomorphism $V \simeq V_1 \oplus V_3$ as filtered modules.*

This phenomenon goes away if we assume that $\mathrm{rad}(V) \subseteq V(0)$.

Lemma 4.5. *If $\mathrm{rad}(V) \subseteq V(0)$, then there exists a decomposition of filtered $\mathbb{Z}/p$-modules $V = W \oplus U$, with W trivial and U trivial free.*

We temporarily postpone the proof.

Now let $\mathcal{F}$ be an arbitrary filtration of a $\mathbb{Z}/p$-module V. Define a filtration $\mathcal{F}_{\mathbb{Z}/p}$ of $V_{\mathbb{Z}/p}$ by letting

$$V_{\mathbb{Z}/p}(k) = (\mathrm{soc}(V(k) + \mathrm{rad}(V)) + V(k-1) + \mathrm{rad}(V))/\mathrm{rad}(V).$$

Note that, if $V = W \oplus U$ with W trivial and U reduced, then the filtration $\mathcal{F}_{\mathbb{Z}/p}$ agrees with the filtration of the same name in the last subsection.

The next theorem says that this filtration solves Problem 3.13.

Theorem 4.6.

(a) *The image of $\mathcal{H}(\mathcal{F})^{\mathbb{Z}/p} \to S^*(V_{\mathbb{Z}/p})$ is contained in $\mathcal{H}(\mathcal{F}_{\mathbb{Z}/p})$.*

(b) $e(\mathcal{F}) \leqslant e(\mathcal{F}_{\mathbb{Z}/p})$.

Proof of Theorem 4.6 (a). Define a new $\mathbb{Z}/p$-equivariant filtration $\mathcal{F}'$ of V by letting

$$V'(k) = V(k) + \mathrm{rad}(V),$$

so that, for all k,

$$V(k) \subseteq V'(k).$$

Then $\mathcal{H}(\mathcal{F}) \subseteq \mathcal{H}(\mathcal{F}')$, so that

$$\mathrm{im}\{\mathcal{H}(\mathcal{F})^{\mathbb{Z}/p} \to S^*(V_{\mathbb{Z}/p})\} \subseteq \mathrm{im}\{\mathcal{H}(\mathcal{F}')^{\mathbb{Z}/p} \to S^*(V_{\mathbb{Z}/p})\}.$$

Moreover, $\mathcal{F}'_{\mathbb{Z}/p} = \mathcal{F}_{\mathbb{Z}/p}$.

By construction, $\mathrm{rad}(V) \subseteq V'(0)$, and so Lemma 4.5 applies. Thus, part (a) of the theorem follows from Proposition 4.3, which tells us that

$$\mathrm{im}\{\mathcal{H}(\mathcal{F}')^{\mathbb{Z}/p} \to S^*(V_{\mathbb{Z}/p})\} \subseteq \mathcal{H}(\mathcal{F}_{\mathbb{Z}/p}).$$

□

* We thank Dave Benson for showing us this example.

https://doi.org/10.1017/S001309151200017X Published online by Cambridge University Press

Proof of Theorem 4.6 (b). For $v \in V$, let $\bar{v}$ denote its image in $V_{\mathbb{Z}/p}$. We define $|v| = k$ if $v \in V(k) - V(k-1)$, and define $|\bar{v}|$ similarly. We say that a basis $\{v_\alpha\}$ for V is a filtered basis if, for all k, $\{v_\alpha \mid |v_\alpha| \leqslant k\}$ is a basis for $V(k)$.

One can choose a filtered basis for V which includes families of elements y_β, z_γ such that the $\bar{z}_\gamma$ form a basis for $(\mathrm{soc}(V) + \mathrm{rad}(V))/\mathrm{rad}(V)$, and the $\bar{y}_\beta, \bar{z}_\gamma$ form a basis for $V_{\mathbb{Z}/p} = V/\mathrm{rad}(V)$. Then $|\bar{y}_\beta| = |y_\beta| + 1$, while $|\bar{z}_\beta| \geqslant |z_\beta|$, with the possibility of $>$ due to the phenomenon illustrated in Example 4.4 (reprised below as Example 4.7).

Each y_β will generate a $\mathbb{Z}/p$-submodule $V_\beta \subset V(|y_\beta|)$ of dimension at most p, and such modules, together with the z_γ, span V.

Define a new filtration $\mathcal{F}''$ of V by letting $V''(k)$ be the linear span of all V_β and z_γ such that $|y_\beta| \leqslant k$ and $|z_\gamma| \leqslant k$. (This might not be a filtration by sub-$\mathbb{Z}/p$-modules.) Then, for all k,

$$V''(k) \subseteq V(k).$$

It follows that

$$\begin{aligned} e(\mathcal{F}) &\leqslant e(\mathcal{F}'') \\ &\leqslant \sum_\beta 2p^{|y_\beta|} \dim V_\beta + \sum_\gamma 2p^{|z_\gamma|} - r(V) \\ &\leqslant \sum_\beta 2p^{|y_\beta|+1} + \sum_\gamma 2p^{|z_\gamma|} - r(V) \\ &\leqslant \sum_\beta 2p^{|\bar{y}_\beta|} + \sum_\gamma 2p^{|\bar{z}_\gamma|} - r(V_{\mathbb{Z}/p}) \\ &= e(\mathcal{F}_{\mathbb{Z}/p}). \end{aligned}$$

□

Proof of Lemma 4.5. Filter $V_{\mathbb{Z}/p}$ by letting $F_k V_{\mathbb{Z}/p} = (V(k) + \mathrm{rad}(V))/\mathrm{rad}(V)$. Then let

$$W_{\mathbb{Z}/p} = (\mathrm{soc}(V) + \mathrm{rad}(V))/\mathrm{rad}(V) \subset V_{\mathbb{Z}/p}$$

be filtered by letting

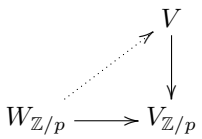
$$F_k W_{\mathbb{Z}/p} = W_{\mathbb{Z}/p} \cap F_k V_{\mathbb{Z}/p}.$$

It is easy to choose a filtered complement $U_{\mathbb{Z}/p}$ so that

$$F_k V_{\mathbb{Z}/p} = F_k W_{\mathbb{Z}/p} \oplus F_k U_{\mathbb{Z}/p}$$

as filtered $\mathbb{Z}/p$-vector spaces.

The point is now that, as $\mathrm{rad}(V) \subseteq V(0)$, one can choose a lifting



https://doi.org/10.1017/S001309151200017X Published online by Cambridge University Press

as filtered vector spaces so that the image is contained in $\mathrm{soc}(V)$, and thus can be viewed as a lifting of filtered $\mathbb{Z}/p$-modules, since if $x + \mathrm{rad}(V) = y + \mathrm{rad}(V)$ with $x \in V(k)$ and $y \in \mathrm{soc}(V)$, then $y \in V(k) \cap \mathrm{soc}(V) = \mathrm{soc}(V(k))$. The conclusion of the lemma follows if we let W be the image of such a lifting, and let U be equal to the filtered $\mathbb{Z}/p$-module generated by any lifting

$$\begin{array}{ccc} & & V \\ & \nearrow & \downarrow \\ U_{\mathbb{Z}/p} & \longrightarrow & V_{\mathbb{Z}/p}. \end{array}$$

□

Example 4.7. We illustrate how Theorem 4.6, and its proof, work when our filtered module V is as in Example 4.4. Thus, let $p \geqslant 3$, and let $\mathcal{F}$ be the filtration given by having $V(0) = V_2$ diagonally embedded in $V = V(1) = V_1 \oplus V_3$. Then $\mathcal{F}_{\mathbb{Z}/p}$ is the filtration having $V_{\mathbb{Z}/p}(0) = V_1$ embedded as the first factor of $V_{\mathbb{Z}/p} = V_{\mathbb{Z}/p}(1) = V_1 \oplus V_1$.

Corresponding to the elements chosen in the proof of part (b) of the theorem, V has a basis z, y, x_2, x_1 satisfying the following:

- y is a $\mathbb{Z}/p$-module generator of V_3;
- $x_2 = \sigma y - y$, $x_1 = \sigma x_2 - x_2$, and these span $\mathrm{rad}(V)$;
- $V(0) = \langle z, x_1 \rangle$, and $\sigma z - z = x_1$;
- the direct summand V_1 is spanned by $z - x_2$;
- $0 = V_{\mathbb{Z}/p}(0) \subset V_{\mathbb{Z}/p}(1) = \langle \bar{z} \rangle \subset \langle \bar{z}, \bar{y} \rangle = V_{\mathbb{Z}/p}(2) = V_{\mathbb{Z}/p}$.

Part (a) of the theorem then says that the image of $\mathbb{F}_p[z, x_1, y^p, x_2^p]^{\mathbb{Z}/p}$ in $\mathbb{F}_p[\bar{z}, \bar{y}]$ will be contained in $\mathbb{F}_p[\bar{z}^p, \bar{y}^{p^2}]$, and part (b) correctly predicts that

$$e(\mathcal{F}) = 4p \leqslant 2p^2 + 2p - 2 = e(\mathcal{F}_{\mathbb{Z}/p}).$$

The auxiliary filtrations $\mathcal{F}'$ and $\mathcal{F}''$ of V used in the theorem's proof satisfy

$$\langle z \rangle = V''(0) \subset V(0) \subset V'(0) = \langle z, x_2, x_1 \rangle.$$

Acknowledgements. The organization of § 2 follows the presentation I gave at the Conference on Algebraic Topology, Group Theory and Representation Theory held on the Isle of Skye, Scotland, in June 2009. I have tried to keep the audience I had there in mind. Conversations with Dave Benson, Peter Symonds and invariant theorists David Wehlau, Jim Shank and Eddy Campbell have been helpful. This research was partly supported by NSF Grants 0604206 and 0967649.

References

1. J. Aguadé and L. Smith, On the Mod p Torus Theorem of John Hubbuck, *Math. Z.* **191** (1986), 325–326.
2. D. Benson, Modules with injective cohomology, and local duality for a finite group, *New York J. Math.* **7** (2001), 201–215.
3. D. Benson, Dickson invariants, regularity and computation in group cohomology, *Illinois J. Math.* **48** (2004), 171–197.
4. D. Benson and J. P. C. Greenlees, Commutative algebra for cohomology rings of classifying spaces of compact Lie groups, *J. Pure Appl. Alg.* **122** (1997), 41–53.
5. M. P. Brodmann and R. Y. Sharp, *Local cohomology*, Cambridge Studies in Advanced Mathematics, Volume 60 (Cambridge University Press, 1998).
6. C. Broto and H.-W. Henn, Some remarks on central elementary abelian p-subgroups and cohomology of classifying spaces, *Q. J. Math.* **44** (1993), 155–163.
7. H. E. A. Campbell and I. P. Hughes, Vector invariants of $U_2(\mathbb{F}_p)$: a proof of a conjecture of Richman, *Adv. Math.* **126** (1997), 1–20.
8. J. F. Carlson, Depth and transfer maps in the cohomology of groups, *Math. Z.* **218** (1995), 461–468.
9. J. Carlson, Mod 2 cohomology of 2 groups: Magma computer computations (available at www.math.uga.edu/~lvalero/cohointro.html).
10. J. F. Carlson, L. Townsley, L. Valeri-Elizondo and M. Zhang, *Cohomology rings of finite groups* Algebras and Applications, Volume 3 (Kluwer, Dordrecht, 2003).
11. J. Duflot, Depth and equivariant cohomology, *Comment. Math. Helv.* **56** (1981), 627–637.
12. D. J. Green, On Carlson's depth conjecture in group cohomology, *Math. Z.* **244** (2003), 711–723.
13. D. J. Green and S. A. King, The cohomology of finite p groups: computer calculations (available at http://users.minet.uni-jena.de/cohomology).
14. H.-W. Henn, Finiteness properties of injective resolutions of certain unstable modules over the Steenrod algebra and applications, *Math. Annalen* **291** (1991), 191–203.
15. H.-W. Henn, J. Lannes and L. Schwartz, Localizations of unstable A-modules and equivariant mod p cohomology, *Math. Annalen* **301** (1995), 23–68.
16. N. J. Kuhn, On topologically realizing modules over the Steenrod algebra, *Annals Math.* **141** (1995), 321–347.
17. N. J. Kuhn, Primitives and central detection numbers in group cohomology, *Adv. Math.* **216** (2007), 387–442.
18. N. J. Kuhn, The nilpotent filtration and the action of automorphisms on the cohomology of finite p-groups, *Math. Proc. Camb. Phil. Soc.* **144** (2008), 575–602.
19. J. Lannes, Cohomology of groups and function spaces, Preprint (based on a talk given at the University of Chicago, 1986).
20. J. Lannes, Sur les espaces fonctionnels dont la source est le classifiant d'un p-groupe abélien élémentaire, *Publ. Math. IHES* **75** (1992), 135–244.
21. D. Quillen, The spectrum of an equivariant cohomology ring, I, *Annals Math.* **94** (1971), 549–572.
22. L. Schwartz, La filtration nilpotente de la catégorie $\mathcal{U}$ et la cohomologie des espaces de lacets, in *Algebraic topology: rational homotopy*, Springer Lecture Notes in Mathematics, Volume 1318, pp. 208–218 (Springer, 1988).
23. L. Schwartz, *Modules over the Steenrod algebra and Sullivan's fixed point conjecture*, Chicago Lectures in Mathematics (University of Chicago Press, 1994).
24. P. Symonds, On the Castelnuovo–Mumford regularity of the cohomology ring of a group, *J. Am. Math. Soc.* **23** (2010), 1159–1173.
25. D. L. Wehlau, Invariants for the modular cyclic group of prime order via classical invariant theory, Preprint (arXiv:0912.1107, 2009).