On the Depth of Cohomology Modules*

Peter Fleischmann, Gregor Kemper, and R. James Shank

April 3, 2003

Abstract

We study the cohomology modules $H^i(G,R)$ of a p-group G acting on a ring R of characteristic p, for $i > 0$. In particular, we are interested in the Cohen-Macaulay property and the depth of $H^i(G,R)$ regarded as an R^G-module. We first determine the support of $H^i(G,R)$, which turns out to be independent of i. Then we study the Cohen-Macaulay property for $H^1(G,R)$. Further results are restricted to the special case that G is cyclic and R is the symmetric algebra of a vector space on which G acts. We determine the depth of $H^i(G,R)$ for i odd and obtain results in certain cases for i even. Along the way, we determine the degrees in which the transfer map $\mathrm{Tr}^G : R \to R^G$ has non-zero image.

Introduction

Modular invariant theory is the study of invariant rings R^G, where G is a finite group acting on a ring R such that the order of G is not invertible in R. The standard situation is the special case where R is the ring of polynomials on a vector space V over a field K with a linear G-action. More precisely, $R = S(V^*)$ is the symmetric algebra of the dual of V. The situation becomes modular if the characteristic of K divides $|G|$. Since R^G coincides with the zeroth cohomology $H^0(G,R)$, it is only natural to consider higher cohomology modules, $H^i(G,R)$, as well. Each cohomology module is an R^G-module, since multiplication with an invariant gives a G-equivariant mapping $R \to R$ which induces an endomorphism of $H^i(G,R)$. Considering $H^i(G,R)$ as an R^G-module raises natural questions concerning the Cohen-Macaulay property, the support, and the depth (in the case where $R = S(V^*)$, so we have a grading). Apart from being interesting in themselves, the cohomology modules $H^i(G,R)$ have proven to be a sharp tool in the study of the Cohen-Macaulay property and depth of the invariant ring R^G. Various authors [6, 9, 12, 13, 14, 15], have used this approach.

Not much is known about the structure of $H^i(G,R)$ as an R^G-module. Ellingsrud and Skjelbred [6] showed that $H^i(G,S(V^*))$ is Cohen-Macaulay if G is cyclic of order p. This result was generalized by Kemper [14, Example 2.14] to all groups G such that $p^2 \nmid |G|$. So the first question to ask is: What happens if we consider the group $G = \mathbf{Z}/p^2$ or, more generally, any cyclic p-group of order greater than p? The answer is that the Cohen-Macaulay property very often fails in these cases (see Theorem 3.1). This observation was the starting point of our investigations, which subsequently included larger classes of groups and actions on non-polynomial rings.

In the first section of this paper we determine the support of $H^+(G,R)$, the positive part of the cohomology, where R is a ring of positive characteristic p. It turns out that this support coincides with the wild branch locus of $\mathrm{Spec}(R) \to \mathrm{Spec}(R^G)$ (see Theorem 1.4). This result was obtained by Kemper [14, Theorem 2.10] for a special case. In the second

*This research was supported by EPSRC grant GR/R32055/01.
2000 Mathematics Subject Classification: 20J06, 13A50, 13C14, 13C15.

section we restrict our attention to the case of a p-group acting on a commutative ring R of characteristic p. We use localization techniques to show that for $i > 0$ the support of $H^i(G,R)$ does not depend on i. Then we study the first cohomology $H^1(G,R)$ and obtain a rather restrictive necessary condition for this module to be Cohen-Macaulay. In the case where $R = S(V^*)$ with V a faithful KG-module, this condition implies that G is generated by elements of order p. In Section 3 we consider the case where $G = \mathbf{Z}/p^{k+1}$ is cyclic and $R = S(V^*)$ with V a KG-module. This assumption renders the cohomology modules much more tractable. As a first result we establish that for odd i the depth of $H^i(G,R)$ is equal to the dimension of the fixed space V^G. The situation turns out to be much more difficult for i even. We first consider the case where V is a free KG-module. In that context we prove a general result, Theorem 3.3, about the image of the transfer for a p-group acting by permutations, and as a corollary we determine the depth of $H^i(G,S(V^*))$ for i even and V free. For the further study of $H^i(G,R)$ for i even we have to consider the transfer in greater detail. In Section 3.3 we determine the degrees where the transfer $\mathrm{Tr}^G : R \to R^G$ has non-zero image (all in the situation $G = \mathbf{Z}/p^{k+1}$ and $R = S(V^*)$). Since the transfer map is of utmost importance in modular invariant theory, this should be of some interest in itself. Using the results from Section 3.3, we obtain information about the depth of $H^i(G,R)$ in some special cases.

It is clear that our results are far from complete. In fact, we consider this paper to be the beginning of an investigation, which we hope will lead to further developments.

Acknowledgement. Most of this research was done during a stay of the second author at the University of Kent at Canterbury as an EPSRC Visiting Fellow. We thank the EPSRC for funding this visit.

1 The support of cohomology

In this section R is a commutative ring (with unity) of characteristic a prime p, and G is an arbitrary finite group acting on R by ring automorphisms. We first determine the support of the positive cohomology $H^+(G,R) := \oplus_{i \geq 1} H^i(G,R)$.

We need two lemmas which are well-known, but we include proofs for completeness.

Lemma 1.1. *Let A and B be rings (with unity but not necessarily commutative), let U be a left A-module, V a left A, right B, bimodule and W a left B-module. If U is free of finite rank, then there is a natural isomorphism*

$$\mathrm{Hom}_A(U, V \otimes_B W) \cong \mathrm{Hom}_A(U,V) \otimes_B W.$$

Proof. If U is isomorphic to the left regular module ${}_AA$, then $\mathrm{Hom}_A(U,X) \cong X$ for every left A-module X, verifying the lemma immediately. The general case now follows from the additivity of the functors $\mathrm{Hom}_A(\cdot, V \otimes_B W)$ and $\mathrm{Hom}_A(\cdot, V) \otimes_B W$. □

Lemma 1.2. *Let A be a commutative ring, G a finite group and M a module over the group ring AG. Furthermore, let $S \subset A \setminus \{0\}$ be a multiplicative set. Then for every $i \geq 0$*

$$H^i(G, S^{-1}M) \cong S^{-1}H^i(G,M).$$

Proof. Choose a resolution $F^* \to \mathbf{Z}$ of $\mathbf{Z}$ as a $\mathbf{Z}G$-module by free $\mathbf{Z}G$-modules F^i of finite rank, e.g. the bar resolution. Let $\mathrm{Hom}_{\mathbf{Z}G}(F^*, M)$ denote the complex with $\mathrm{Hom}_{\mathbf{Z}G}(F^i, M)$ as i-th part. Hence $H^*(G,M) = H\left(\mathrm{Hom}_{\mathbf{Z}G}(F^*, M)\right)$, where the right hand side is the homology of the complex. By Lemma 1.1 we have

$$\mathrm{Hom}_{\mathbf{Z}G}(F^*, S^{-1}M) = \mathrm{Hom}_{\mathbf{Z}G}(F^*, M \otimes_A S^{-1}A) \cong \mathrm{Hom}_{\mathbf{Z}G}(F^*, M) \otimes_A S^{-1}A$$

and therefore

$$H^*(G, S^{-1}M) \cong H\left(\mathrm{Hom}_{\mathbf{Z}G}(F^*, M) \otimes_A S^{-1}A\right) \cong H\left(\mathrm{Hom}_{\mathbf{Z}G}(F^*, M)\right) \otimes_A S^{-1}A. \quad (1)$$

The second isomorphism results from the facts that $S^{-1}A$ is a flat A-module (see Eisenbud [5, Proposition 2.5]) and that application of an exact functor and forming homology commute. The claim follows from (1). □

For each subgroup $H \leq G$, the abelian group $H^i(H, R)$ is an R^H-module and hence an R^G-module. We define $H^{+ev}(G, R) = \oplus_{i \geq 1} H^{2i}(G, R)$. For a prime ideal $\mathfrak{P} \in \mathrm{Spec}(R)$ define the **inertia group** $G_{\mathfrak{P}}$ as

$$G_{\mathfrak{P}} := \{g \in G \mid g(f) - f \in \mathfrak{P} \text{ for all } f \in R\}.$$

Lemma 1.3. *(a)* $\mathrm{Supp}_{R^G}(\mathrm{Im}\ \mathrm{res}_{G \to H}\ (H^{+ev}(G, R))) \subseteq \mathrm{Supp}_{R^G}\ (H^{+ev}(G, R))$.

(b) For $\mathfrak{p} \in \mathrm{Spec}(R^G)$*, suppose* $\mathfrak{P} \in \mathrm{Spec}(R)$ *with* $\mathfrak{P} \cap R^G = \mathfrak{p}$*. Then*

$$\mathfrak{p} \in \mathrm{Supp}_{R^G}\ (\mathrm{Im}\ \mathrm{res}_{G \to \langle g \rangle}\ (H^{+ev}(G, R)))$$

for each $g \in G_{\mathfrak{P}}$ *with* $|g| = p$.

Proof. (a) Suppose $\mathfrak{p} \notin RHS$, then by exactness of localization:

$$\mathrm{Im}\ \mathrm{res}_{G \to H}\ (H^{+ev}(G, R))_{\mathfrak{p}} = \mathrm{Im}\ \mathrm{res}_{G \to H}\ (H^{+ev}(G, R)_{\mathfrak{p}}) = 0,$$

so $\mathfrak{p} \notin LHS$.
(b) Suppose $g \in G_{\mathfrak{P}}$ with $|g| = p$, $H := \langle g \rangle$, $\alpha \in H^{2i}(G, \mathbb{F}_p)$ with $i > 0$, such that $0 \neq \beta := \mathrm{res}_{G \to H}(\alpha)$ (which exists by Benson [2, Theorem 4.1.3 and its proof]) and let $\widetilde{\beta}$ denote the image of β under the map $H^*(H, \mathbb{F}_p) \to H^*(H, R)$, induced by the inclusion $\mathbb{F}_p \hookrightarrow R$. Then $\widetilde{\beta} \in \mathrm{Im}\ \mathrm{res}_{G \to H}\ (H^{+ev}(G, R))$. Let $f \in R^G$ with $f\widetilde{\beta} = 0$. We have $H^{2i}(H, R) \cong R^H/(g-1)^{p-1}R$. The induced map

$$H^2(H, \mathbb{F}_p) \cong \mathbb{F}_p = \mathbb{F}_p^H/(g-1)^{p-1}\mathbb{F}_p \to R^H/(g-1)^{p-1}R \cong H^{2i}(H, R)$$

takes $\beta = \lambda \in \mathbb{F}_p$ to $\widetilde{\beta} = \lambda + (g-1)^{p-1}R$. Since $\lambda \in \mathbb{F}_p \setminus \{0\}$ we have $\lambda \notin \mathfrak{P}$ (as $\mathfrak{P}$ is a proper ideal). Since $g \in G_{\mathfrak{P}}$, $(g-1)^{p-1}R \subseteq \mathfrak{P}$, hence $f\lambda \in \mathfrak{P}$. It follows that $f \in \mathfrak{P} \cap R^G = \mathfrak{p}$. We have shown that every element from R^G which sends $\widetilde{\beta}$ to zero lies in $\mathfrak{p}$. This means that $\widetilde{\beta}$ remains non-zero in the localization $H^+(G, R)_{\mathfrak{p}}$, so

$$\mathfrak{p} \in \mathrm{Supp}_{R^G}\ (\mathrm{Im}\ \mathrm{res}_{G \to H}\ (H^{+ev}(G, R))).$$

□

Theorem 1.4.

$$\begin{aligned} \mathrm{Supp}_{R^G}(H^{+ev}(G, R)) &= \mathrm{Supp}_{R^G}(H^+(G, R)) = \mathcal{V}(\mathrm{Ann}_{R^G}(H^+(G, R))) \\ &= \mathcal{V}(\mathrm{Tr}^G(R)) = \{\mathfrak{P} \cap R^G \mid \mathfrak{P} \in \mathrm{Spec}(R),\ |G_{\mathfrak{P}}| \equiv 0 \bmod p\}. \end{aligned}$$

Proof. The last equality is Lorenz and Pathak [15, Lemma 1.1]. To prove the remaining equalities, we first show $\mathcal{V}(\mathrm{Ann}_{R^G}(H^+(G, R))) \subseteq \mathcal{V}(\mathrm{Tr}^G(R))$: Let $\mathfrak{p} \notin \mathcal{V}(\mathrm{Tr}^G(R))$, then for some $r \in R$, $f := \mathrm{Tr}^G(r) \notin \mathfrak{p}$. By Lorenz and Pathak [15, Lemma 1.3], f annihilates $\ker \mathrm{res}_{G \to 1}(H^*(G, R)) = H^+(G, R)$. Hence $\mathfrak{p} \notin \mathcal{V}(\mathrm{Ann}_{R^G}(H^+(G, R)))$.

Now assume $\mathfrak{p} \notin \mathrm{Supp}_{R^G}(H^{+ev}(G, R))$; then $\mathfrak{p} \notin \mathrm{Supp}_{R^G}\ (\mathrm{Im}\ \mathrm{res}_{G \to H}\ (H^{+ev}(G, R)))$ for each $H \leq G$. From Lemma 1.3 (b), we see that $G_{\mathfrak{P}}$ has no elements of order p. Thus

$$\mathcal{V}(\mathrm{Ann}_{R^G}(H^+(G, R))) \subseteq \mathcal{V}(\mathrm{Tr}^G(R)) \subseteq \mathrm{Supp}_{R^G}(H^{+ev}(G, R)) \subseteq \mathrm{Supp}_{R^G}(H^+(G, R))$$

and the theorem follows from the standard inclusion

$$\operatorname{Supp}_{R^G}(H^+(G,R)) \subseteq \mathcal{V}(\operatorname{Ann}_{R^G}(H^+(G,R))).$$

$\square$

Corollary 1.5.

$$\sqrt{\operatorname{Ann}_{R^G}(H^+(G,R))} = \sqrt{\operatorname{Tr}^G(R)}.$$

2 Cohomology modules for p-groups

In this section R is again a commutative ring of characteristic p, but now G is a finite p-group acting on R by ring automorphisms. Using Corollary 1.5, we will first determine the support of the cohomology modules $H^i(G,R)$. This implies knowledge about the dimension of $H^i(G,R)$. Then we derive rather restrictive necessary conditions for $H^1(G,R)$ to be Cohen-Macaulay.

Lemma 2.1. *With the notation introduced at the beginning of Section 2 we have*

$$\operatorname{Supp}_{R^G}\left(H^i(G,R)\right) = \operatorname{Supp}_{R^G}\left(H^j(G,R)\right)$$

for all positive integers i and j.

Proof. Take $\mathfrak{p} \in \operatorname{Spec}(R^G)$. Using Lemma 1.2 we obtain

$$\mathfrak{p} \in \operatorname{Supp}_{R^G}\left(H^i(G,R)\right) \quad \Leftrightarrow \quad H^i(G,R_{\mathfrak{p}}) \neq 0.$$

Since G is a p-group, $H^i(G,R_{\mathfrak{p}}) \neq 0$ is equivalent to $H^j(G,R_{\mathfrak{p}}) \neq 0$ (see Brown [3, Theorem VI.8.5] or Benson [1, Proposition 3.14.4]). The result follows. $\square$

Now Corollary 1.5 and Lemma 2.1 determine the support of the cohomology for a p-group, in fact the following theorem tells us that the support of $H^i(G,R)$ is equal to the image of the branch locus under the categorical quotient, independent of i.

Theorem 2.2. *For every positive integer i we have*

$$\operatorname{Supp}_{R^G}\left(H^i(G,R)\right) = \operatorname{Supp}_{R^G}\left(H^+(G,R)\right) = \{R^G \cap \mathfrak{P} \mid \mathfrak{P} \in \operatorname{Spec}(R), G_{\mathfrak{P}} \neq \{1\}\}.$$

As a special case we obtain:

Corollary 2.3. *Let G be a finite p-group acting linearly on a finite-dimensional vector space V over a field K of characteristic p. Then*

$$\dim\left(H^i\left(G, S(V^*)\right)\right) = \max\left\{\dim_K(V^\sigma) \mid \sigma \in G \setminus \{1\}\right\}.$$

We obtain the following, somewhat technical, necessary condition for $H^1(G,R)$ to be Cohen-Macaulay.

Theorem 2.4. *Assume that R^G is Noetherian and R is finitely generated as a module over R^G. Define $H := \langle G_{\mathfrak{P}} \mid \mathfrak{P} \in \operatorname{Spec}(R)\rangle$ and*

$$H_{\min} := \langle G_{\mathfrak{P}} \mid \mathfrak{P} \in \operatorname{Spec}(R) \textit{ is minimal with } G_{\mathfrak{P}} \neq \{1\}\rangle.$$

If $H^1(G,R)$ is Cohen-Macaulay as an R^G-module, then $H \subseteq H_{\min} \cdot \Phi(G)$, where $\Phi(G)$ is the Frattini subgroup.

Proof. First observe that $H^1(G,R)$ is the first homology of a complex of finitely generated R^G-modules, and is therefore itself finitely generated over R^G.

Assume that $H \not\subseteq H_{\min} \cdot \Phi(G)$. This implies $H \cdot \Phi(G)/H_{\min} \cdot \Phi(G) \neq \{1\}$. But this factor group is a subgroup of $G/H_{\min} \cdot \Phi(G)$, which is elementary abelian since G is a p-group (see Huppert [11, Chapt. III, Satz 3.14(a)]). It follows that there exists a maximal subgroup of $G/H_{\min} \cdot \Phi(G)$ which does not contain $H \cdot \Phi(G)/H_{\min} \cdot \Phi(G)$. This means that we have a normal subgroup $N \trianglelefteq G$ of index p such that $H_{\min} \subseteq N$ but $H \not\subseteq N$. Thus there exists a $\mathfrak{Q} \in \operatorname{Spec}(R)$ such that $G_{\mathfrak{Q}} \not\subseteq N$. Choose $\sigma \in G_{\mathfrak{Q}} \setminus N$ and write $\bar{\sigma} := \sigma N \in G/N$. Then $G/N = \langle \bar{\sigma} \rangle$. Consider the class $\alpha \in H^1(G/N, R^N) = \ker(\operatorname{Tr}_N^G)/(\bar{\sigma}-1)R^N$ given by $\alpha = 1 + (\bar{\sigma}-1)R^N$. The fact that σ lies in $G_{\mathfrak{Q}}$ implies $(\bar{\sigma}-1)R^N \subseteq \mathfrak{Q}$ and therefore $\alpha \neq 0$.

Let $\beta := \inf(\alpha)$ be the image of α under the inflation map $\inf\colon H^1(G/N, R^N) \to H^1(G,R)$. Then $\beta \neq 0$ (see Evens [7, Corollary 7.2.3]). Consider the ideal $I := \operatorname{Tr}_N^G(R^N) \subseteq R^G$. We have $I = (\bar{\sigma}-1)^{p-1}R^N$ and therefore $I \subseteq \operatorname{Ann}_{R^G}(\alpha)$. It follows that $I \subseteq \operatorname{Ann}_{R^G}(\beta)$, which implies

$$\operatorname{grade}\left(I, H^1(G,R)\right) \in \{0, \infty\} \tag{2}$$

(using the convention of Bruns and Herzog [4, Definition 1.2.6] that $\operatorname{grade}(I,M) = \infty$ if $IM = M$). On the other hand, Bruns and Herzog [4, Proposition 1.2.10(a)] (which is applicable since R^G is Noetherian and $H^1(G,R)$ is finitely generated over R^G) yields

$$\operatorname{grade}\left(I, H^1(G,R)\right) = \min\left\{\operatorname{depth}\left(H^1(G,R)_{\mathfrak{p}}\right) \mid \mathfrak{p} \in \operatorname{Spec}(R^G), I \subseteq \mathfrak{p}\right\}. \tag{3}$$

The hypothesis that $H^1(G,R)$ is Cohen-Macaulay implies that

$$\operatorname{depth}\left(H^1(G,R)_{\mathfrak{p}}\right) = \dim\left(H^1(G,R)_{\mathfrak{p}}\right)$$

for every $\mathfrak{p} \in \operatorname{Spec}(R^G)$ (see Bruns and Herzog [4, Theorem 2.1.3(b)]), where we use the convention $\dim(0) = \infty$. Thus in the right hand side of (3) we can substitute the depth by the dimension. Now it follows from (2) that there exists $\mathfrak{p} \in \operatorname{Spec}(R^G)$ with $I \subseteq \mathfrak{p}$ and $H^1(G,R)_{\mathfrak{p}} = 0$ or $\dim\left(H^1(G,R)_{\mathfrak{p}}\right) = 0$. Choose a $\mathfrak{P} \in \operatorname{Spec}(R)$ with $R^G \cap \mathfrak{P} = \mathfrak{p}$. Then $I \subseteq \mathfrak{P}$, which by Lorenz and Pathak [15, Lemma 1.1] implies

$$N_{\mathfrak{P}} \subsetneqq G_{\mathfrak{P}}, \tag{4}$$

hence $G_{\mathfrak{P}} \neq \{1\}$. By Theorem 2.2 this implies $H^1(G,R)_{\mathfrak{p}} \neq 0$. Hence $\dim\left(H^1(G,R)_{\mathfrak{p}}\right) = 0$, which means that $\mathfrak{p}$ is a minimal element of $\operatorname{Supp}_{R^G}\left(H^1(G,R)\right)$. But then $\mathfrak{P}$ must also be minimal with $G_{\mathfrak{P}} \neq \{1\}$, since by Theorem 2.2, an ideal $\mathfrak{P}' \subsetneqq \mathfrak{P}$ with $G_{\mathfrak{P}'} \neq \{1\}$ would yield $\mathfrak{p}' \subsetneqq \mathfrak{p}$ with $\mathfrak{p}' \in \operatorname{Supp}_{R^G}\left(H^1(G,R)\right)$ (see Eisenbud [5, Corollary 4.18]). By the definition of $H_{\min}$, this means that $G_{\mathfrak{P}} \subseteq H_{\min}$, implying $G_{\mathfrak{P}} \subseteq N$ and contradicting (4). □

Remark. The hypotheses in Theorem 2.4 requiring R^G to be Noetherian and R to be finitely generated over R^G, may seem a bit awkward. In particular, the hypotheses imply that R is Noetherian, so one might wonder if it suffices to assume that R is Noetherian. However, there exist examples of a Noetherian ring R and a finite group $G \leq \operatorname{Aut}(R)$ such that R^G is not Noetherian and R is not finitely generated over R^G (see Montgomery [16, Example 5.5]). ◁

The following corollaries are less technical. We consider the special case where G (still a p-group) acts linearly on a finite-dimensional vector space V over a field K of characteristic p. Then G also acts on $R := S(V^*)$, the symmetric algebra of the dual of V.

Corollary 2.5. *In the above situation define $\mathcal{F} := \{V^\sigma \mid \sigma \in G \setminus \{1\}\}$. If $H^1(G,R)$ is Cohen-Macaulay (as a module over R^G), then*

$$G = \langle \sigma \in G \setminus \{1\} \mid V^\sigma \text{ is maximal in } \mathcal{F} \rangle.$$

The following elementary lemma is needed for the proof.

Lemma 2.6. *Let $\mathfrak{P} = \left((V^\sigma)^\perp\right)$ be the ideal in R generated by all linear forms in V^* vanishing on V^σ. Then*

(a) $\sigma \in G_{\mathfrak{P}}$;

(b) if $\sigma \in G_{\mathfrak{Q}}$ *for* $\mathfrak{Q} \in \operatorname{Spec}(R)$, *then* $\mathfrak{P} \subseteq \mathfrak{Q}$.

Proof. (a) Let $l \in V^*$ be a linear form. Then for $v \in V^\sigma$ we have

$$((\sigma - 1)l)(v) = l\left(\sigma^{-1}(v) - v\right) = l(0) = 0, \tag{5}$$

so $(\sigma - 1)l \in (V^\sigma)^\perp \subset \mathfrak{P}$. Assume that we have shown $(\sigma - 1)f \in \mathfrak{P}$ for an $f \in R$. Then

$$(\sigma - 1)(lf) = \sigma(l) \cdot (\sigma - 1)f + f \cdot (\sigma - 1)l \in \mathfrak{P}.$$

By induction, $(\sigma - 1)R \subseteq \mathfrak{P}$ now follows.
(b) Equation (5) shows that $(\sigma - 1)V^* \subseteq (V^\sigma)^\perp$. The rank of $\sigma - 1$ on V^* equals the rank on V, which in turn is equal to $\dim_K(V) - \dim_K(V^\sigma) = \dim_K\left((V^\sigma)^\perp\right)$. Thus $(\sigma - 1)V^* = (V^\sigma)^\perp$, so for $l \in (V^\sigma)^\perp$ there exists $h \in V^*$ with $(\sigma - 1)h = l$. Hence $l \in (\sigma - 1)R \subseteq \mathfrak{Q}$. Since $\mathfrak{P}$ is generated by $(V^\sigma)^\perp$, the result follows. □

Proof of Corollary 2.5. The hypotheses of Theorem 2.4 are satisfied, so we need to analyse the conclusion in the context of the corollary. For $\mathfrak{Q} := R^+$, the direct sum of all $S^i(V)$, $i > 0$, we have $\mathfrak{Q} \in \operatorname{Spec}(R)$ and $G_{\mathfrak{Q}} = G$. Therefore the subgroup H from Theorem 2.4 coincides with G. Hence Theorem 2.4 says that $H_{\min} = G$. In other words, G is generated by $\sigma \in G_{\mathfrak{P}} \setminus \{1\}$ with $\mathfrak{P} \in \operatorname{Spec}(R)$ minimal with the property that $G_{\mathfrak{P}} \neq \{1\}$.

Take such a σ and assume, by way of contradiction, that V^σ is not maximal in $\mathcal{F}$. Hence there exists a $\tau \in G \setminus \{1\}$ with $V^\sigma \subsetneqq V^\tau$. Let $\mathfrak{P}' := \left((V^\tau)^\perp\right)$ be the ideal in R generated by the linear forms vanishing on V^τ. Then $\tau \in G_{\mathfrak{P}'}$ by Lemma 2.6(a), hence $G_{\mathfrak{P}'} \neq \{1\}$. We claim that $\mathfrak{P}' \subsetneqq \mathfrak{P}$, which will contradict the minimality of $\mathfrak{P}$. Indeed, take $l \in (V^\tau)^\perp$. Then $V^\sigma \subseteq V^\tau$ implies $l \in (V^\sigma)^\perp$ and so, by Lemma 2.6(b), $l \in \mathfrak{P}$. This yields $\mathfrak{P}' \subseteq \mathfrak{P}$. Since V^σ is proper in V^τ there exists an $l \in (V^\sigma)^\perp \setminus (V^\tau)^\perp$. As above, it follows that $l \in \mathfrak{P}$, but $l \notin \mathfrak{P}'$ by the construction of $\mathfrak{P}'$. Therefore $\mathfrak{P}' \subsetneqq \mathfrak{P}$, which completes the proof. □

Corollary 2.7. *In the situation of Corollary 2.5, assume that the action of G on V is faithful and $H^1(G, R)$ is Cohen-Macaulay as an R^G-module. Then G is generated by elements of order p.*

Proof. By Corollary 2.5, G is generated by $\sigma \in G \setminus \{1\}$ such that V^σ is maximal among the V^τ, $\tau \in G \setminus \{1\}$. But it can be seen from the Jordan canonical form of σ that $V^\sigma \subsetneqq V^{\sigma^p}$. Hence $\sigma^p = 1$. □

Remark. Corollary 2.7 is in sharp contrast with Example 2.14 from Kemper [14], where it is shown that $H^i(G, R)$ is Cohen-Macaulay for all $i > 0$ if the order of G is not divisible by p^2. ◁

3 Cohomology modules for cyclic p-groups

In this section $G = \langle\sigma\rangle$ is a cyclic group of order p^{k+1} acting on a finite-dimensional vector space V over a field K of characteristic p. We write $R = S(V^*)$ for the symmetric algebra of the dual of V. We will analyse the R^G-modules $H^j(G, R)$. The depth of $H^0(G, R)$ is known by Ellingsrud and Skjelbred [6]. We are interested in the depth of $H^j(G,R)$ for $j>0$ as R^G-modules. By Kemper [14, Theorem 2.13(a)] we know that

$$\operatorname{depth}\left(H^j(G,R)\right) \geq \dim_K(V^G). \tag{6}$$

To obtain more information we use the special form of the group. In fact, we have

$$H^i(G,V) = \begin{cases} V^G/\operatorname{Tr}^G(V) & \text{if } i>0 \text{ is even,}\\ \ker(\operatorname{Tr}^G)/(\sigma-1)V & \text{if } i \text{ is odd}\end{cases} \tag{7}$$

for any KG-module V (see, for example, Evens [7, p. 6]). Hence it suffices to consider $j=1$ and $j=2$, where the case $j=1$ is fairly straightforward and will be discussed in the next subsection. After that we discuss the case $j=2$ with V being a free KG-module. The case $j=2$ and V not free is more subtle and requires detailed information on the transfer ideal $\operatorname{Tr}^G(R)$. These results, some of which are of independent interest, will be collected in the third subsection. Throughout this section we use V_m, for $m \leq |G|$, to denote the indecomposable KG-module of dimension m.

3.1 The depth of $H^1(G,R)$

In this section we determine the depth of $H^1(G,R)$ when G a cyclic p-group.

Theorem 3.1. *With the notation introduced at the beginning of Section 3 we have*

$$\operatorname{depth}\left(H^1(G,R)\right) = \dim_K(V^G). \tag{8}$$

In particular, $H^1(G,R)$ is Cohen-Macaulay if and only if $|G|=p$.

Proof. V^G is a submodule of V on which G acts trivially. Moreover, $H^1(G,R)$ is a module over $\operatorname{End}_{KG}(R)$. Thus Theorem 1.5 of Kemper [14] yields

$$\operatorname{depth}\left(H^1(G,R)\right) = \dim_K(V^G) + \operatorname{grade}\left(\mathfrak{i}, H^1(G,R)\right),$$

where $\mathfrak{i}$ is the intersection with R^G of the ideal in R generated by all linear forms vanishing on V^G. But $\mathfrak{i}$ coincides with the radical ideal of the image of the relative transfer $\operatorname{Tr}^G_N\colon R^N \to R^G$ for $N := \langle \sigma^p \rangle$ (see Fleischmann [8]). Thus

$$\operatorname{depth}\left(H^1(G,R)\right) = \dim_K(V^G) + \operatorname{grade}\left(\operatorname{Tr}^G_N(R^N), H^1(G,R)\right).$$

Take any $f \in \operatorname{Tr}^G_N(R^N)$. Then $f = \operatorname{Tr}^G_N(g) = (\sigma-1)^{p-1}(g)$ with $g \in R^N$. Let $\alpha := 1 + (\sigma-1)R$ be the class of 1 in $H^1(G,R)$. Then

$$f\alpha = (\sigma-1)^{p-1}(g) + (\sigma-1)R = 0.$$

Thus every element in $\operatorname{Tr}^G_N(R^N)$ is a zero-divisor on $H^1(G,R)$, and, therefore, we obtain $\operatorname{grade}\left(\operatorname{Tr}^G_N(R^N), H^1(G,R)\right) = 0$. This yields (8).

The additional statement follows from comparing (8) with Corollary 2.3. $\square$

3.2 The depth of $H^2(G,S(V^*))$ for V free

We now consider $H^2(G,R)$ when V is a free G-module, i.e., $V = mV_{p^{k+1}}$. In this case $V \cong V^*$ is a permutation module and, choosing a permutation basis for V^*, the group G permutes monomials in $R = S(V^*)$, i.e. R^G is what is called a ring of *permutation invariants*. We will now prove a general result on permutation invariants of p-groups that contains the required information on $H^2(G,R)$ in the special case where G is cyclic.

The following lemma, which will also be used later in the paper, tells how to recognize free summands using the transfer. Although it is well known in representation theory, we will provide a short proof:

Lemma 3.2. *Let P be a p-group and V a finitely generated KP-module. Then V contains a free direct summand if and only if $\mathrm{Tr}^P(V) \neq 0$ and V is free if and only if $\mathrm{Tr}^P(V) = V^P$.*

Proof. First assume that $w := \mathrm{Tr}^P(v) \neq 0$ for $v \in V$. The homomorphism

$$\vartheta : \ KP \to V, \ f \mapsto fv$$

maps the one-dimensional socle $\mathrm{soc}(KP) = K \cdot \mathrm{Tr}^P(1_P)$ onto the line $K \cdot w \subseteq V^P$. Hence ϑ is a monomorphism. Since KP is a finite-dimensional Frobenius-algebra, the notions of finitely generated projective, injective and free modules coincide. Hence ϑ splits, i.e. $V \cong KP \oplus W$. For the second claim we can assume that $V \neq 0$ is indecomposable. If V is not free, then by the previous argument $\mathrm{Tr}^P(V)$ must be zero, whereas V^P is nonzero. If V is free, then $V \cong KP$ and clearly $V^P = \mathrm{Tr}^P(V)$. □

Theorem 3.3. *Let P be a p-group acting on the finite set Ω and let K^Ω denote the corresponding KP-permutation module over the field K of characteristic p. Let $Z \triangleleft P$ be a normal subgroup of order p with quotient $\overline{P} := P/Z$; furthermore let Ω/Z denote the set of Z-orbits on Ω. Then one has for $R := S(K^\Omega)$:*

$$R^P / \mathrm{Tr}^P(R) \cong S(K^{\Omega/Z})^{\overline{P}} \oplus \left(\mathrm{Tr}^Z(R)\right)^{\overline{P}} / \mathrm{Tr}^P(R).$$

Moreover $\left(\mathrm{Tr}^Z(R)\right)^{\overline{P}} = \mathrm{Tr}^P(R)$ if and only if $\mathrm{Tr}^Z(R)$ is free as $K\overline{P}$-module. In particular, this is true if P is cyclic, i.e., in this case $R^P / \mathrm{Tr}^P(R) \cong S(K^{\Omega/Z})^{\overline{P}}$.

Proof. Note that the action of P on Ω induces an action of $\overline{P}$ on Ω/Z in a natural way. Let $V := K^\Omega$ with basis $\{X_\omega \mid \omega \in \Omega\}$. Then $R = \oplus_{\alpha:\ \Omega \to \mathbb{N}_0} K\underline{X}^\alpha$ with $\underline{X}^\alpha := \prod_{\omega \in \Omega} X_\omega^{\alpha_\omega}$ and P acts on R by $g(\underline{X}^\alpha) = \underline{X}^{\alpha \circ g^{-1}}$. For every subgroup $H \leq P$ the invariant ring R^H has a K-basis consisting of H-orbit sums, i.e. relative transfers $\mathrm{Tr}^H_{H_\alpha}(\underline{X}^\alpha)$, where $H_\alpha := \{h \in H \mid \alpha \circ h = \alpha\}$ is the stabiliser of $\underline{X}^\alpha$. For each Z-orbit $\mathcal{O} \in \Omega/Z$ let $N_{\mathcal{O}} = \prod_{\omega \in \mathcal{O}} X_\omega$ be the orbit product in R^Z. A monomial $\underline{X}^\alpha$ is stabilised by Z if and only if α is constant on the orbits in Ω/Z, and hence if and only if it is a monomial in the $N_{\mathcal{O}}$'s. These orbit products generate a polynomial subalgebra B of R^Z, which is isomorphic to $S(K^{\Omega/Z})$ as a $K\overline{P}$-module. All the other Z-orbit sums in R^Z are absolute transfers, because Z has no nontrivial proper subgroups. It is now easy to see that $R^Z = \mathrm{Tr}^Z(R) \oplus B$ as $K\overline{P}$-modules. Moreover

$$R^P = (R^Z)^{\overline{P}} = \mathrm{Tr}^Z(R)^{\overline{P}} \oplus B^{\overline{P}}$$

and $\mathrm{Tr}^P(R) = \mathrm{Tr}^P_Z(\mathrm{Tr}^Z(R)) = \mathrm{Tr}^{\overline{P}}(\mathrm{Tr}^Z(R)) \subseteq \mathrm{Tr}^Z(R)^{\overline{P}}$. This, together with Lemma 3.2, proves the first two statements.

Now assume that P is cyclic. Then $R = X \oplus Y$, where X is spanned by the $\underline{X}^\alpha$ with $P_\alpha = 1$ and Y is spanned by the $\underline{X}^\beta$ with $Z \leq P_\beta$. It follows that $\mathrm{Tr}^Z(R) = \mathrm{Tr}^Z(X)$. But X is a direct sum of regular KP-modules, hence it is free in each fixed degree. Let $Z^+ := \mathrm{Tr}^Z(1) \in KP$; then

$$\mathrm{Tr}^Z(KP) = Z^+ KP = Z^+ KZ \otimes_{KZ} K\overline{P} \cong KZ^+ \otimes_{KZ} K\overline{P} \cong K\overline{P}.$$

Hence in each degree $\mathrm{Tr}^Z(R)$ is free as $K\overline{P}$-module. □

Returning to the standard situation of this section, let G be cyclic of order p^{k+1} and $R = S(V^*)$. Assume that $V := mV_{p^{k+1}}$ is the direct sum of m copies of the regular module KG and let $Z \leq G$ be the unique minimal subgroup. The corresponding set Ω is the union of m copies of G and Ω/Z is the union of m copies of $\overline{G} = G/Z$. Hence $K^{\Omega/Z}$ is the sum of m copies of the regular module $\overline{G}$ and we get

$$H^2(G,R) \cong R^G / \operatorname{Tr}^G(R) \cong S(mK\overline{G})^{\overline{G}}.$$

Thus applying Ellingsrud and Skjelbred [6] gives:

Corollary 3.4. *In the above situation we have*

$$\operatorname{depth}\left(H^2(G,R)\right) = \min\{2+m, mp^k\}.$$

In particular, $H^2(G,R)$ is Cohen-Macaulay if and only if

$$m(p^k - 1) \leq 2.$$

Proof. We only need to prove the statement on the Cohen-Macaulay property. From Corollary 2.3 we see that $\dim\left(H^2(G,R)\right) = \dim_K(V^Z) = mp^k$. Thus $H^2(G,R)$ is Cohen-Macaulay if and only if $2 + m \geq mp^k$. □

Remark 3.5. Note that the isomorphism $B \cong S(K^{\Omega/Z})$ does not preserve degrees. In fact, for $\mathcal{O} \in \Omega/Z$ the 'variable' $N_{\mathcal{O}} \in B$ has degree $|\mathcal{O}|$ rather than degree one. Let P be cyclic of order p^2 and Z the subgroup of order p. Then Theorem 3.3 gives

$$S(V_{p^2}^*)^{\mathbf{Z}/p^2} / \operatorname{Tr}^{\mathbf{Z}/p^2}(S(V_{p^2}^*)) \cong S\left(V_p^*\right)^{\mathbf{Z}/p}.$$

From Shank and Wehlau [17, Theorem 6.2], $S\left(V_p^*\right)^{\mathbf{Z}/p}$ contains an indecomposable invariant of degree $2p-3$. Taking into account the 'blow-up' of degrees in the isomorphism $B \cong S(K^{\Omega/Z})$, we see that the quotient ring $S(V_{p^2}^*)^{\mathbf{Z}/p^2} / \operatorname{Tr}^{\mathbf{Z}/p^2}(S(V_{p^2}^*))$ contains an indecomposable element of degree $p(2p-3) = 2p^2 - 3p > p^2$ (for $p > 3$). It had been conjectured that all indecomposable homogeneous modular invariants of degree larger than $|P|$ lie in the transfer ideal. The above arguments show that this is not the case, if P is cyclic of order p^2.

3.3 The lowest degree in the image of the transfer for a cyclic p-group

Next we consider $H^2(G,R)$ in greater generality. For that purpose we study the image of the transfer in R^G. We are particularly interested in the smallest degree for which the transfer is non-zero. From Lemma 3.2, we know that $\operatorname{Tr}^G(R)_d \neq 0$ is equivalent to the condition that the KG-module R_d contains a free direct summand. Recall that $R = S(V^*)$ for some KG-module V. Hence $R_d \cong S^d(V^*)$ is a quotient of the d-fold tensor space $(V^*)^{\otimes d}$. Hence $\operatorname{Tr}^G(R)_d \neq 0$ also implies that $(V^*)^{\otimes d}$ contains a free summand. It is somewhat surprising that the reverse turns out to be true for a cyclic group G.

If V is not faithful, then the minimal subgroup $Z \leq G$ acts trivially on R and $\operatorname{Tr}^G(R) = \operatorname{Tr}^G_Z(\operatorname{Tr}^Z(R)) = 0$. Thus we can restrict attention to faithful modules. For any KG-module V we define $mt(V) := \min\{d \in \mathbb{N} \mid \operatorname{Tr}^G(S^d(V^*)) \neq 0\}$ with the convention $\min \emptyset = \infty$. Recall that the indecomposable modules for G (the cyclic group of order p^{k+1}) are given by V_n $(1 \leq n \leq p^{k+1})$, where $n = \dim(V_n)$, and a generator of G acts as a full Jordan block. The following is the main result of this subsection:

Theorem 3.6. *Let $G \cong \mathbf{Z}/p^{k+1}$ and V a KG-module.*

i) Let $0 \leq n = \sum_{i=0}^{k} n_i p^i < p^{k+1}$ with $0 \leq n_i < p$; if $n_k > 0$, let $p - 1 = dn_k + r$ with $0 \leq r < n_k$. Then

$$mt(V_{n+1}) = \begin{cases} \infty & \text{if } n_k = 0 \\ d & \text{if } r = 0 \text{ and } n \geq n_k(1 + p + \cdots + p^k) \\ d+1 & \text{otherwise.} \end{cases}$$

ii) Suppose that $V \cong V_{m_1} \oplus V_{m_2} \oplus \cdots \oplus V_{m_l}$ *with* $0 \le m_1 \le m_2 \le \cdots \le m_l \le p^{k+1}$. *Then* $mt(V) = mt(V_{m_l})$.

iii) For any non-negative integer d *the following are equivalent:*

(a) the free module $V_{p^{k+1}}$ *appears as a direct summand of* $V^{\otimes d}$;

(b) the free module $V_{p^{k+1}}$ *appears as a direct summand of* $S^d(V)$;

(c) $d \ge mt(V)$.

The proof will be given below, after a series of technical lemmas. We will make use of the *representation ring* (also called the Green ring) R_{KG}. As a $\mathbf{Z}$-module R_{KG} is a free module with the isomorphism classes of indecomposable KG-modules as basis elements, and the multiplication is given by the tensor product. We will consider the elements $\chi_i := V_{p^i+1} - V_{p^i-1} \in R_{KG}$ $(0 \le i \le k)$, where formally we set $V_0 := 0$. We will use the following formulas of Green [10, Theorem 3], which hold for $0 \le i \le k$.

$$\chi_i V_r = \begin{cases} V_{r+p^i} - V_{p^i-r} & \text{if } 1 \le r \le p^i, \\ V_{r+p^i} + V_{r-p^i} & \text{if } p^i < r \le (p-1)p^i, \\ V_{r-p^i} + 2V_{p^{i+1}} - V_{2p^{i+1}-p^i-r} & \text{if } (p-1)p^i < r \le p^{i+1}. \end{cases} \tag{9}$$

Lemma 3.7. *Let* n *be an integer with* $0 \le n < p^{k+1}$ *and write* $n = \sum_{i=0}^{k} n_i p^i$ *with* $0 \le n_i < p$. *There exists a unique polynomial* $f_n \in \mathbf{Z}[X_0, \ldots, X_k]$ *with* $\deg_{X_i}(f_n) < p$ *for all* i*, such that*

$$V_{n+1} = f_n(\chi_0, \ldots, \chi_k).$$

Moreover, using the lexicographical monomial ordering with $X_k > X_{k-1} > \cdots > X_0$, f_n *has the leading monomial* $X_k^{n_k} X_{k-1}^{n_{k-1}} \cdots X_0^{n_0}$ *with leading coefficient* 1.

Proof. We first remark that the existence of the f_n will imply uniqueness. In fact, if B is the set of all polynomials $f \in \mathbf{Z}[X_0, \ldots, X_k]$ with $\deg_{X_i}(f) < p$ for all i, then the existence will provide an epimorphism $B \to R_{KG}$ of $\mathbf{Z}$-modules. However B and R_{KG} are both free of rank p^{k+1}, therefore the epimorphism must in fact be an isomorphism.

We prove the existence of f_n and the statement on the leading monomial and coefficient by induction on n. For $n = 0$ we have $f_0 = 1$. So assume $n > 0$ and let j be maximal with $n_j \ne 0$. We have $1 \le n + 1 - p^j \le (p-1)p^j$. Hence Green's formulas (9) yield

$$\chi_j V_{n+1-p^j} = \begin{cases} V_{n+1} - V_{2p^j-n-1} & \text{if } n+1 \le 2p^j, \\ V_{n+1} + V_{n+1-2p^j} & \text{if } n+1 > 2p^j. \end{cases}$$

We have $2p^j - n - 1 < n + 1$, hence in each case we obtain $V_{n+1} = \chi_j V_{n+1-p^j} \pm V_{m+1}$ for some $m < n$. By induction, this yields

$$V_{n+1} = \chi_j f_{n-p^j}(\chi_0, \ldots, \chi_k) \pm f_m(\chi_0, \ldots, \chi_k),$$

so with $f_n := X_j f_{n-p^j} \pm f_m$ we have $V_{n+1} = f_n(\chi_0, \ldots, \chi_k)$. Also by induction, the leading monomial of f_m is less than $X_j^{n_j} X_{j-1}^{n_{j-1}} \cdots X_0^{n_0}$, and the leading term of f_{n-p^j} is $X_j^{n_j-1} X_{j-1}^{n_{j-1}} \cdots X_0^{n_0}$. This yields the statement on the leading monomial and coefficient of f_n. We also get from the induction hypothesis that $\deg_{X_i}(f_n) < p$ for $i \ne j$, and it follows from the description of the leading monomial of f_n that $\deg_{X_j}(f_n) = n_j < p$. □

By Lemma 3.7, we have an epimorphism $\mathbf{Z}[X_0, \ldots, X_k] \to R_{KG}$ by sending each X_i to χ_i. We denote the kernel of this epimorphism by I.

Lemma 3.8. *There exist polynomials $r_0, \dots, r_k \in I$ with the leading monomial* $\mathrm{LM}(r_i) = X_i^p$*. Moreover, the leading coefficient of r_i is* 1*.*

Proof. Take an integer i with $0 \le i \le k$. By (9) we have

$$\chi_i V_{(p-1)p^i+1} = V_{(p-2)p^i+1} + 2V_{p^{i+1}} - V_{p^{i+1}-1},$$

so $r_i := X_i f_{(p-1)p^i} - f_{(p-2)p^i} - 2f_{p^{i+1}-1} + f_{p^{i+1}-2}$ lies in I. By Lemma 3.7 this has leading monomial X_i^p with coefficient 1. □

Proposition 3.9. *Let $V = V_{m_1+1} \oplus \cdots \oplus V_{m_l+1}$ be a finitely generated KG-module and let d be a non-negative integer. Write $n := \max\{m_1, \dots, m_l\}$ as $n = \sum_{i=0}^k n_i p^i$ with $0 \le n_i < p$. If there exists a $j \in \{0, \dots, k\}$ such that $n_i = (p-1)/d$ for $j < i \le k$ but $n_j < (p-1)/d$, then* $\mathrm{Tr}^G\left(V^{\otimes d}\right) = 0$*.*

Proof. By Lemma 3.2 we have to show that under the assumption of the proposition, no $V_{p^{k+1}}$ occurs as an indecomposable summand in $V^{\otimes d}$. With $f := f_{m_1} + \cdots + f_{m_l}$, Lemma 3.7 tells us that $V = f(\chi_0, \dots, \chi_k)$, and $\mathrm{LM}(f) = X_k^{n_k} X_{k-1}^{n_{k-1}} \cdots X_0^{n_0}$. Hence $V^{\otimes d} = f^d(\chi_0, \dots, \chi_k)$, and

$$\mathrm{LM}(f^d) = X_k^{dn_k} X_{k-1}^{dn_{k-1}} \cdots X_0^{dn_0} = X_k^{p-1} \cdots X_{j+1}^{p-1} X_j^{dn_j} X_{j-1}^{dn_{j-1}} \cdots X_0^{dn_0} < (X_k \cdots X_0)^{p-1}.$$

Let $g \in \mathbf{Z}[X_0, \dots, X_k]$ be a normal form of f^d with respect to the set $\{r_0, \dots, r_k\}$ from Lemma 3.8. Then $\mathrm{LM}(g) \le \mathrm{LM}(f^d)$ and $g - f^d \in I$, so $V^{\otimes d} = g(\chi_0, \dots, \chi_k)$. But we have $\deg_{X_i}(g) < p$ for every i, since $\mathrm{LM}(r_i) = X_i^p$. Therefore g is the unique polynomial with $\deg_{X_i}(g) < p$ and $V^{\otimes d} = g(\chi_0, \dots, \chi_k)$. But if $V^{\otimes d}$ had $V_{p^{k+1}}$ as an indecomposable summand, this unique polynomial would have the leading monomial $(X_k \cdots X_0)^{p-1}$ by Lemma 3.7. However, the leading monomial of g is smaller than this. □

Corollary 3.10. *With the setting and assumptions of Proposition 3.9, there exists no non-zero element of degree d in* $\mathrm{Tr}^G(S(V))$*. In particular, the numbers given in Theorem 3.6(i) and (ii) are lower bounds for $mt(V)$.*

Proof. We have to show that $\mathrm{Tr}^G\left(S^d(V)\right) = 0$, where $S^d(V)$ is the d-th symmetric power. But there exists natural epimorphism $\varphi\colon V^{\otimes d} \to S^d(V)$ of KG-modules. Therefore

$$\mathrm{Tr}^G\left(S^d(V)\right) = \mathrm{Tr}^G\left(\varphi\left(V^{\otimes d}\right)\right) = \varphi\left(\mathrm{Tr}^G\left(V^{\otimes d}\right)\right) = 0$$

by Proposition 3.9. □

So far we have looked at conditions ensuring that $V^{\otimes d}$ and therefore $S^d(V)$ do **not** contain a free summand. We now look at the opposite, namely conditions such that $S^d(V)$ and therefore $V^{\otimes d}$ **do** contain such a summand. We will use Lemma 3.2 as our main tool and therefore we need some results on transfers.

3.3.1 Computing transfers

Lemma 3.11. *Let X be an arbitrary finite group, acting on a ring A. Suppose that H is a subgroup of X, $g \in A$ and $h \in A^H$. Further suppose $f := \mathrm{Tr}^H(g) \in A^X$. Then* $\mathrm{Tr}^X(gh) = f\,\mathrm{Tr}_H^X(h)$*.*

Proof. Using the factorisation $\mathrm{Tr}^X = \mathrm{Tr}^X_H \circ \mathrm{Tr}^H$ gives $\mathrm{Tr}^X(gh) = \mathrm{Tr}^X_H(\mathrm{Tr}^H(gh))$. Since $h \in A^H$, we have $\mathrm{Tr}^H(gh) = h\,\mathrm{Tr}^H(g)$. By hypothesis $\mathrm{Tr}^H(g) \in A^X$. Thus

$$\mathrm{Tr}^X_H(h\,\mathrm{Tr}^H(g)) = \mathrm{Tr}^X_H(h)\,\mathrm{Tr}^H(g) = f\,\mathrm{Tr}^X_H(h)$$

as required. □

Lemma 3.12. *For an integer $0 \le \ell < p$ we have*

$$\sum_{c \in \mathbf{F}_p} c^\ell = \begin{cases} 0 & \text{if } 0 \le \ell < p-1; \\ -1 & \text{if } \ell = p-1. \end{cases}$$

Defining $\Delta := \sigma - 1$ and applying the binomial theorem gives

$$\sigma^i = \sum_{j=0}^{i} \binom{i}{j} \Delta^j.$$

Over a field of characteristic p this gives $\sigma^{p^i} = 1 + \Delta^{p^i}$. Suppose $G = \langle \sigma \rangle \cong \mathbf{Z}/p^{k+1}$ and α is an element in a KG-module with $KG\alpha \cong V_{n+1}$. Then comparing binomial coefficients gives

$$\sigma^i \alpha = \sum_{j=0}^{n} \binom{i}{j} \Delta^j \alpha.$$

If $n = p^i m + r$ with $0 \le r < p^i$ and $H := \langle \sigma^{p^i} \rangle$ then $KH\alpha \cong V_{m+1}$ and the corresponding fixed point is $\Delta^{mp^i}\alpha$.

Theorem 3.13. *Let $H = \mathbf{Z}/p$ and suppose that V is a KH-module and $\alpha_1, \alpha_2, \ldots, \alpha_\ell$ is a sequence of not necessarily distinct elements of $S(V^*)$. Define m_i by $KH \cdot \alpha_i \cong V_{m_i+1}$ and define β_i by $\Delta^{m_i}\alpha_i = \beta_i$. If $\sum_{i=1}^{\ell} m_i = p-1$ then*

$$\mathrm{Tr}^H\left(\prod_{i=1}^{\ell} \alpha_i\right) = -\prod_{i=1}^{\ell} \frac{\beta_i}{m_i!}.$$

Proof. Observe that $\sigma^c(\alpha_i) = \sum_{j=0}^{m_i} \binom{c}{j} \Delta^j \alpha_i$. Thus

$$\begin{aligned}
\mathrm{Tr}^{\mathbf{Z}/p}\left(\prod_{i=1}^{\ell} \alpha_i\right) &= \sum_{c \in \mathbf{F}_p} \prod_{i=1}^{\ell} \sum_{j=0}^{m_i} \binom{c}{j} \Delta^j \alpha_i \\
&= \sum_{c \in \mathbf{F}_p} \prod_{i=1}^{\ell} \left(\alpha_i + \cdots + \binom{c}{m_i}\beta_i\right) \\
&= \sum_{c \in \mathbf{F}_p} \left(\prod_{i=1}^{\ell} \alpha_i + \cdots + \prod_{i=1}^{\ell} \binom{c}{m_i}\beta_i\right).
\end{aligned}$$

Note that the degree of $\binom{c}{j}$ as a polynomial in c is j. Thus $\prod_{i=1}^{\ell} \binom{c}{m_i}$ has degree $\sum_{i=1}^{\ell} m_i = p-1$. All other terms in the sum have coefficients which, as polynomials in c, have degree less than $p-1$. Therefore, using Lemma 3.12, these terms don't contribute. Thus

$$\begin{aligned}
\mathrm{Tr}^{\mathbf{Z}/p}\left(\prod_{i=1}^{\ell} \alpha_i\right) &= \sum_{c \in \mathbf{F}_p} \prod_{i=1}^{\ell} \binom{c}{m_i}\beta_i \\
&= \left(\prod_{i=1}^{\ell} \frac{\beta_i}{m_i!}\right) \sum_{c \in \mathbf{F}_p} \prod_{i=1}^{\ell} c(c-1)\cdots(c-m_i+1).
\end{aligned}$$

A further application of Lemma 3.12 gives

$$\sum_{c\in\mathbf{F}_p}\prod_{i=1}^{\ell} c(c-1)\cdots(c-m_i+1) = \sum_{c\in\mathbf{F}_p}(c^{p-1}+\cdots) = -1$$

as required. □

In the following we write x_{n+1} for a linear form in V^* which generates a KG-module of type V_{n+1}. Furthermore, for $r \le n$, we write $x_r := \Delta^{n+1-r}(x_{n+1})$.

Corollary 3.14. *Suppose $n+1 \le p$ and $nd = p-1$. Then*

$$\mathrm{Tr}^{\mathbf{Z}/p}(x_{n+1}^d) = -\left(\frac{x_1}{n!}\right)^d.$$

Proof. Apply Theorem 3.13 with $\alpha_i = x_{n+1}$, $\beta_i = x_1$, $m_i = n$ and $\sum m_i = dn = p-1$. □

Lemma 3.15. *Suppose t and d are positive integers with $td = p-1$ and let $n := t(1+p+p^2+\cdots+p^k) = (p^{k+1}-1)/d$. Then*

$$\mathrm{Tr}^G(x_{n+1}^d) = \frac{x_1^d}{(-(t!)^d)^{k+1}}.$$

Proof. The proof is by induction on k. For $k=0$, the result is given by Corollary 3.14. For $k>0$, let $N := \langle\sigma^p\rangle \cong \mathbf{Z}/p^k$. The N-module generated by x_{n+1} is isomorphic to $V_{n'+1}$ with $n' = (p^k-1)/d$ and the corresponding fixed point is x_{t+1}. Therefore, using the induction hypothesis, $\mathrm{Tr}^N(x_{n+1}^d) = (-(t!)^{-d})^k x_{t+1}^d$. However $\mathrm{Tr}^G = \mathrm{Tr}^G_N \circ \mathrm{Tr}^N = \mathrm{Tr}^{G/N}\circ\mathrm{Tr}^N$. Thus $\mathrm{Tr}^G(x_{n+1}^d) = (-(t!)^{-d})^k\,\mathrm{Tr}^{G/N}(x_{t+1}^d)$. The G/N-module generated by x_{t+1} is isomorphic to V_{t+1} and the corresponding fixed point is x_1. Therefore, applying Corollary 3.14 gives $\mathrm{Tr}^{G/N}(x_{t+1}^d) = -(t!)^{-d}x_1^d$ and the result follows. □

Lemma 3.16. *Suppose $t \le p-1$ is a positive integer. Divide t into $p-1$ to get $p-1 = td+r$ with $0 \le r < t$. Then*

$$\mathrm{Tr}^G\left(x_{tp^k+1}^d x_{(r+1)p^k}\right) = \frac{-x_1^{d+1}}{(t!)^d r!}.$$

Proof. Let $H := \langle\sigma^{p^k}\rangle \cong \mathbf{Z}/p$. The H-module generated by x_{tp^k+1} is isomorphic to V_{t+1} with corresponding fixed point x_1. Since $(r+1)p^k = rp^k + (p^k-1)+1$, the H-module generated by $x_{(r+1)p^k}$ is isomorphic to V_{r+1} with corresponding fixed point x_{p^k}. Thus applying Theorem 3.13 gives

$$\mathrm{Tr}^H\left(x_{tp^k+1}^d x_{(r+1)p^k}\right) = \frac{-x_1^d x_{p^k}}{(t!)^d r!}.$$

The result then follows from the factorisation $\mathrm{Tr}^G = \mathrm{Tr}^G_H \circ \mathrm{Tr}^H$ and the fact that $\mathrm{Tr}^G_H(x_{p^k}) = \mathrm{Tr}^{\mathbf{Z}/p^k}(x_{p^k}) = x_1$. □

3.3.2 Proof of Theorem 3.6

For brevity we write $I^G := \mathrm{Tr}^G(R)$. Assume $p^k \le n < p^{k+1}$ and $V = V_{n+1}$. Write $n = \sum_{i=0}^k n_i p^i$ with $0 \le n_i \le p-1$. Divide n_k into $p-1$ to get $p-1 = dn_k + r$ with $0 \le r < n_k$. Using Lemma 3.16, we see that $x_1^{d+1} \in I^G$. If $r>0$, applying Proposition 3.9 with $j=k$ shows that I^G is zero in degrees less than or equal to d. If $r=0$ and $n_k(p^j+\cdots+p^k) \le n < n_k(p^{j-1}+\cdots+p^k)$ then again Proposition 3.9 tells us that I^G is zero in degrees less than or equal to d. However if $n \geq n_k(1+p+\cdots+p^k)$, then from Lemma 3.15, $x_1^d \in I^G$. A further application of Proposition 3.9 shows that, in this case, I^G is zero in degrees less than or equal to $d-1$. Note that n necessarily falls into one of three cases: (i) $r > 0$, (ii) $r = 0$ and $n_k(p^j + \cdots + p^k) \leq n < n_k(p^{j-1} + \cdots + p^k)$, (iii) $r = 0$ and $n \geq n_k(1+p+\cdots+p^k)$. In the first two cases the minimal non-zero degree for I^G is $d+1$ while in the third case the minimal non-zero degree for I^G is d. In all three cases there is a power of x_1 in the first non-zero degree.

This proves part i) of Theorem 3.6 for *indecomposable* KG-modules. Suppose V is arbitrary KG-module. Since G is a p-group, there is an invariant $0 \neq v \in S(V^*)^G$ of degree one. Suppose $d > mt(V)$ and $X \cong V_{p^{k+1}}$ is a submodule of $S^{mt(V)}(V^*)$. Then $V_{p^{k+1}} \cong v^{d-mt(V)} \cdot X \leq S^d(V^*)$, which splits off, because X is projective and hence injective in the category of KG-modules. This shows that the implications $(c) \Leftrightarrow (b) \Rightarrow (a)$ hold for arbitrary V. Together with the proof so far we see that (a), (b) and (c) are equivalent if V is indecomposable.

Suppose V is decomposed as in part ii) of the theorem. Then $S^{mt(V_{m_l})}(V_{m_l})$ appears as a submodule of $\left(S^{mt(V_{m_l}}(V)\right)$, hence $mt(V) \leq mt(V_{m_l})$. Now assume that some summand $F \cong V_{p^{k+1}}$ appears in a submodule S of $S^d(V) \cong \left(\otimes_{i=1}^l S(V_{m_i})\right)_d$. We can choose S of the form $S^{s_1}(V_{m_1}) \otimes \cdots \otimes S^{s_l}(V_{m_l})$ with $s_1+s_2+\cdots+s_k = d = mt(V)$. Hence F also appears in $V_{m_1}^{\otimes s_1} \otimes \cdots \otimes V_{m_l}^{\otimes s_l}$. Since $m_1 \leq m_2 \leq \cdots \leq m_l$, we know that $V_{m_1}^{\otimes s_1} \otimes \cdots \otimes V_{m_l}^{\otimes s_l}$ is isomorphic to a submodule of $V_{m_l}^{\otimes s_1} \otimes \cdots \otimes V_{m_l}^{\otimes s_l} \cong V_{m_l}^{\otimes mt(V)}$. Hence F splits off $V_{m_l}^{\otimes mt(V)}$. Since V_{m_l} is indecomposable, we can use iii) (c) to conclude $mt(V) \geq mt(V_{m_l})$. This finishes the proof of Theorem 3.6.

3.4 On the depth of even cohomology

We keep the notation introduced at the beginning of Section 3, and we continue to write $I^G = \mathrm{Tr}^G(R)$. For a subgroup $H \leq G$ we write $I_H^G = \mathrm{Tr}_H^G(R^H)$ for the image of the relative transfer.

Theorem 3.17. *Suppose that H is a subgroup of G and $(I^H \setminus I^G) \cap R^G$ is non-empty. Then* $\mathrm{depth}(R^G/I^G) \leq \dim(R^G/I_H^G)$.

Proof. Choose $f \in (I^H \setminus I^G) \cap R^G$. By Lemma 3.11, $f + I^G$ is a nonzero element of $M := R^G/I^G$ which annihilates $I_H^G + I^G \subset R^G/I^G$. Thus every element of I_H^G acts as a zero divisor on M and therefore I_H^G is contained in some associated prime $\mathfrak{p}$ of M. Now the 'graded version' of Bruns and Herzog [4, Proposition 1.2.13] shows that the depth of M is less than or equal to $\dim(R^G/\mathfrak{p})$ which in turn is less than or equal to $\dim(R^G/I_H^G)$. □

Theorem 3.18. *Suppose $td = p-1$ and $t(p^i + p^{i+1} + \cdots + p^k) \leq n < t(p^{i-1} + p^i + \cdots p^k)$. Then* $\mathrm{depth}(H^2(G, S(V_{n+1}^*))) \leq p^{i-1}$ *and, if $i \leq k$, $H^2(G, S(V_{n+1}^*))$ is not Cohen-Macaulay.*

Proof. Let $H := \langle \sigma^{p^i} \rangle \cong \mathbf{Z}/p^{k+1-i}$, $m := t(p^i + p^{i+1} + \cdots + p^k)$ and let $m' := m/p^i$. The H-module generated by x_{m+1} is isomorphic to $V_{m'+1}$ with corresponding fixed point x_1. Thus applying Lemma 3.15 gives $\mathrm{Tr}^H(x_{m+1}^d) = (-1(t!)^{-d})^{k+1-i} x_1^d \in R^G$. By Corollary 3.10 we know that I^G is zero in degree d thus $x_1^d \notin I^G$. Therefore $x_1^d \in (I^H \setminus I^G) \cap R^G$. Applying Theorem 3.17 gives $\mathrm{depth}(H^2(G,R)) \leq \dim(R^G/I_H^G)$. However $\dim(R^G/I_H^G)$ is the dimension of the subspace of V_{n+1} fixed by $\sigma^{p^{i-1}}$. Thus $\mathrm{depth}(H^2(G,R)) \leq p^{i-1}$. Furthermore $\dim(H^2(G,R)) = p^k$. Therefore, as long as $k \geq i$, $H^2(G,R)$ is not Cohen-Macaulay. □

Theorem 3.19. *Suppose $td = p-1$ and $t(p + p^2 + \cdots + p^k) \leq n < t(1 + p + p^2 + \cdots p^k)$. Then* $\mathrm{depth}(H^2(G, S(V_{n+1}^*)) = 1$.

Proof. Applying Theorem 3.18 with $i = 1$ gives $\operatorname{depth}(H^2(G, R)) \leq 1$ and from 6, we have $\operatorname{depth}(H^2(G, S(V_{n+1}^*)) \geq 1$. $\square$

Theorem 3.20. *Let $V = V_{m_1+1} \oplus \cdots \oplus V_{m_\ell+1}$ be a finitely generated KG-module and define $n := \max\{m_1, \ldots, m_\ell\}$. Suppose that $td = p - 1$ and $t(p + p^2 + \cdots + p^k) \leq n < t(1 + p + p^2 + \cdots p^k)$. Then* $\operatorname{depth}(H^2(G, S(V^*)) = \ell$.

Proof. It follows from Corollary 3.10 that $x_1^d + I^G$ is a non-zero element of $H^2(G, S(V^*))$. We choose a homogeneous system of parameters for R^G consisting of the norms of the terminal variables and elements from the image of the relative transfer and then proceed as in the proof of Theorem 3.19. $\square$

The following gives an 'if and only if' - criterion for the hypothesis in Theorem 3.17, in the special case where H is the maximal subgroup of G.

Lemma 3.21. *If $N \triangleleft G$, the equation*

$$I^G = I^N \cap R^G$$

holds if and only if I^N is free as a $K(G/N)$-module.

Proof. Let $\bar{G} := G/N$ and note that $I^G = \operatorname{Tr}^{\bar{G}}(I^N)$, whereas $I^N \cap R^G = (I^N)^{\bar{G}}$. Now the statement follows immediately from Lemma 3.2 with $P = \bar{G}$. $\square$

Lemma 3.22. *Let $N < G$ be the maximal subgroup and $S := \oplus_{m=1}^{p^{k+1}} n_m V_m$. Then $\operatorname{Tr}^N(S)$ is free as $K\bar{G}$-module if and only if $n_m = 0$ for all m satisfying $p^{k+1} - p + 1 \leq m < p^{k+1}$.*

Proof. Note that V_m viewed as $K[\Delta]$-module satisfies: $V_m \cong K[\Delta]/(\Delta^m)$ and hence

$$\Delta^i(V_m) \cong \Delta^i \cdot K[\Delta]/(\Delta^m) \cong K[\Delta]/(\Delta^{m-i}) \cong V_{m-i},$$

with $V_j := 0$ for $j \leq 0$. Therefore one has

$$\begin{aligned} \operatorname{Tr}^N(S) &= (\sigma^p - 1)^{p^k - 1}(S) = \Delta^{p^{k+1}-p}(S) = \oplus_{\ell=0}^{p-1} n_{p^{k+1}-\ell}(\Delta^{p^{k+1}-p}(V_{p^{k+1}-\ell})) \\ &\cong \oplus_{\ell=0}^{p-1} n_{p^{k+1}-\ell}(V_{p-\ell}) \in K\bar{G} - \mathrm{mod}. \end{aligned}$$

Now the statement in the lemma follows from the fact that $V_{p-\ell}$ is a free $K\bar{G}$ - module if and only if $\ell = 0$. $\square$

Using (6), Kemper [14, Theorem 1.5] and the preceding lemmas, we obtain:

Proposition 3.23. *Let $N < G$ be the maximal subgroup. Then we have $I^G \subsetneqq I^N \cap R^G$ if and only if the KG-module R has a direct summand V_m with $p(p^k - 1) < m < p^{k+1}$. In this case*

$$\operatorname{grade}\left(\sqrt{\operatorname{Tr}_N^G(R^N)}\ ,\ H^2(G, R)\right) = 0$$

and

$$\operatorname{depth}(H^2(G, R)) = \dim(V^G).$$

We think that it is quite common to find a V_m with $p(p^k - 1) < m < p^{k+1}$ in the symmetric powers of V^*. Unfortunately we were not able to prove any concrete instances of this, apart from the ones found in Theorems 3.19 and 3.20.

References

[1] David J. Benson, *Representations and Cohomology I*, Cambridge Studies in Advanced Mathematics **30**, Cambridge Univ. Press, Cambridge 1991.

[2] David J. Benson, *Representations and Cohomology II*, Cambridge Studies in Advanced Mathematics **31**, Cambridge Univ. Press, Cambridge 1991.

[3] Kenneth S. Brown, *Cohomology of Groups*, Graduate Texts in Mathematics **87**, Springer-Verlag, New York, Heidelberg, Berlin 1982.

[4] Winfried Bruns, Jürgen Herzog, *Cohen-Macaulay Rings*, Cambridge University Press, Cambridge 1993.

[5] David Eisenbud, *Commutative Algebra with a View Toward Algebraic Geometry*, Springer-Verlag, New York 1995.

[6] Geir Ellingsrud, Tor Skjelbred, *Profondeur d'anneaux d'invariants en caractéristique p*, Compos. Math. **41** (1980), 233–244.

[7] Leonard Evens, *The Cohomology of Groups*, Oxford University Press, Oxford 1991.

[8] Peter Fleischmann, *Relative Trace Ideals and Cohen-Macaulay Quotients of Modular Invariant Rings*, in: P. Dräxler, G.O. Michler, C. M. Ringel, eds., *Computational Methods for Representations of Groups and Algebras, Euroconference in Essen, April 1-5 1997*, Progress in Mathematics **173**, Birkhäuser, Basel 1999.

[9] Nikolai Gordeev, Gregor Kemper, *On the Branch Locus of Quotients by Finite Groups and the Depth of the Algebra of Invariants*, J. Algebra (2003), to appear.

[10] J. A. Green, *The Modular Representation Algebra of a Finite Group*, Illinois J. Math. **6** (1962), 607–619.

[11] Bertram Huppert, *Endliche Gruppen I*, Springer-Verlag, Berlin, Heidelberg, New York 1967.

[12] Gregor Kemper, *On the Cohen-Macaulay Property of Modular Invariant Rings*, J. of Algebra **215** (1999), 330–351.

[13] Gregor Kemper, *A Characterization of Linearly Reductive Groups by their Invariants*, Transformation Groups **5** (2000), 85–92.

[14] Gregor Kemper, *The Depth of Invariant Rings and Cohomology,* with an appendix by Kay Magaard, J. of Algebra **245** (2001), 463–531.

[15] Martin Lorenz, Jay Pathak, *On Cohen-Macaulay Rings of Invariants*, J. of Algebra **245** (2001), 247–264.

[16] Susan Montgomery, *Fixed Rings of Finite Automorphism Groups of Associative Rings*, Lecture Notes in Mathematics **818**, Springer-Verlag, Berlin, Heidelberg, New York 1980.

[17] R. James Shank, David L. Wehlau, *Noether numbers for subrepresentations of cyclic groups of prime order*, Bull. London Math. Soc. **34** (2002), 438–450.

P. Fleischmann and R.J. Shank
Institute of Mathematics and Statistics
University of Kent
Canterbury, CT2 7NF
UK
`P.Fleischmann@ukc.ac.uk`
`R.J.Shank@ukc.ac.uk`

G. Kemper
Technische Universität München
Zentrum Mathematik - M11
Boltzmannstr. 3
85 748 Garching
Germany
`kemper@ma.tum.de`