On the Cohen-Macaulay Property of Modular Invariant Rings

Gregor Kemper*

IWR, Universität Heidelberg, Im Neuenheimer Feld 368

69 120 Heidelberg, Germany

email `Gregor.Kemper@iwr.uni-heidelberg.de`

August 11, 1998

Abstract

If V is a faithful module for a finite group G over a field of characteristic p, then the ring of invariants need not be Cohen-Macaulay if p divides the order of G. In this article the cohomology of G is used to study the question of Cohen-Macaulayness of the invariant ring.

One of the results is a classification of all groups for which the invariant ring with respect to the regular representation is Cohen-Macaulay. Moreover, it is proved that if p divides the order of G, then the ring of vector invariants of sufficiently many copies of V is not Cohen-Macaulay. A further result is that if G is a p-group and the invariant ring is Cohen-Macaulay, then G is a bireflection group, i.e., it is generated by elements which fix a subspace of V of codimension at most 2.

Introduction

Let $G \leq \mathrm{GL}(V)$ be a finite group acting on a vector space V of dimension n over a field K. Then G acts on the symmetric algebra $R = S(V^*)$ of the dual of V, which is a polynomial ring over K, and we consider the invariant ring R^G. By the Noether normalization lemma, there exist homogeneous $f_1, \ldots, f_n \in R^G$ such that R^G is finitely generated as a module over $A = K[f_1, \ldots, f_n]$. R^G is called **Cohen-Macaulay** if it is a *free* module over A. This is independent of the choice of the set $\{f_1, \ldots, f_n\}$. An equivalent condition is that $f_1, \ldots, f_n$ form an R^G-regular sequence (see the beginning of Section 1). R^G is always Cohen-Macaulay if the characteristic p of K does not divide the order of G. If, however, $|G|$ is a multiple of p (which we call the **modular** case), then R^G is in general not Cohen-Macaulay. At the moment, the knowledge about which linear

*The author thanks Ian Hughes, Eddy Campbell, Jim Shank, and David Wehlau for their hospitality during his visit to Queen's University in Kingston, Ontario, where most of this paper was prepared.

groups in the modular case have invariant rings which are Cohen-Macaulay and which ones do not is very sketchy, to say the least. The only classes of groups where we have a complete answer are the cyclic groups, which were treated by Ellingsrud and Skjelbred [10], and, more generally, the so-called shallow groups (Campbell et al. [7]). For further references relevant to this question, we refer the reader to the books by Smith [17] and Benson [4], which also provide introductory texts on invariant theory of finite groups.

In the first section of this paper we relate the regularity of sequences $f_1, \dots, f_n \in R^G$ to the cohomology $H^*(G, R)$ of G with values in the polynomial ring R. These cohomology groups are viewed as modules over R^G, and it is shown that, loosely speaking, large annihilators of elements of the cohomology destroy the Cohen-Macaulay property. As a first application, it is proved that if $H \leq G$ is a strongly p-embedded subgroup, then $\operatorname{depth}(R^H) = \operatorname{depth}(R^G)$. This is a partial converse to a result of Campbell et al. [6].

In Section 2, geometric arguments are used to prove that the annihilator mentioned above is large enough in many cases. This leads to the first main result (Theorem 2.3) and the corollary that in the modular case the ring of sufficiently large vector invariants is not Cohen-Macaulay. The latter statement confirms a conjecture made by the author in a talk given in April 1996. A further application of Theorem 2.3 is the classification of all groups G and fields K such that $K[V_{reg}]^G$ is Cohen-Macaulay for the regular representation V_{reg}. Moreover, we get the result that for certain representations of symmetric groups, the invariant ring is not Cohen-Macaulay. These representations include the irreducible reflection representation of degree $n-2$ of the symmetric group $G = S_n$ on n letters, where $p \geq 5$ divides n, and $n > 5$. It is also possible to use Theorem 2.3 to derive results on cohomology from the knowledge of invariant rings. For example, the fact that the symmetric and alternating groups S_n and A_n have no non-split central extension with kernel of order $p \geq 5$ becomes a consequence of the well-known fact that the invariant rings of S_n and A_n (with the usual permutation representation) are Cohen-Macaulay (see Example 2.10(a)).

In the third section we restrict our attention to the first cohomology group with values in K. This permits a more accurate analysis of the geometry of annihilators, which leads to the second main result (Theorem 3.6). The result that a p-group G is generated by bireflections if its invariant ring is Cohen-Macaulay arises as a corollary. This is remarkable since it yields a special case of a theorem by Kac and Watanabe [12], but under a much weaker hypothesis (see Remark 3.8). Refining the methods a little bit more, we recover one of the results in Nakajima [16], which consists of a further series of reflection groups whose invariant rings are not Cohen-Macaulay.

Apart from producing classes of groups whose invariant rings are not Cohen-Macaulay, the methods developed in this article provide a means to analyze the Cohen-Macaulay property of invariant rings. In fact, every example of a non-Cohen-Macaulay invariant ring known to the author can be understood in terms of these methods.

Smith [18] took an approach to the question of depth and Cohen-Macaulayness of modular invariant rings which uses cohomology of G with values in a certain Koszul complex. Although his paper makes heavy use of spectral sequences and this article does not, the methods used in the first section of this paper are quite similar to Smith's methods. However, the main results of both papers are almost disjoint.

The main parts of this paper were written during a visit of the author to Queen's University in Kingston, Ontario. I would like to express my thanks to Ian Hughes, Eddy Campbell, Jim Shank, and David Wehlau for many conversations which inspired this work, and for the stimulating atmosphere which they created. In particular, I am indebted to Jim Shank and Ian Hughes for sharing the ideas which lead to Proposition 3.4 and Example 3.10. I also thank David Benson, Kay Magaard, Jürgen Müller, Larry Smith, and Jacques Thévenaz for very fruitful conversations. Further thanks go to the referee for pointing out some typos and suggesting some better formulations.

1 Regular sequences and cohomology

In this section, let R be a Noetherian commutative ring with 1 and let $G \leq \mathrm{Aut}(R)$ be a group of automorphisms of R. We write R^G for the invariant ring. A sequence $a_1, \dots, a_m \in R$ is called **R-regular** if $(a_1, \dots, a_m) \neq R$ and a_i is not a zero divisor on $R/(a_1, \dots, a_{i-1})$, for $i = 1, \dots, m$. We have the corresponding definition of R^G-regularity, where the ideals have to be taken in R^G. The **depth** of R is the maximal length of an R-regular sequence, denoted by $\mathrm{depth}(R)$.

The following proposition gives a cohomological criterion to decide whether a sequence $a_1, \dots, a_m \in R^G$ which is R-regular is also R^G-regular. Before stating it, we recall the Koszul complex

$$0 \longrightarrow R \xrightarrow{\partial_{m-1}} R^m \xrightarrow{\partial_{m-2}} R^{\binom{m}{m-2}} \xrightarrow{\partial_{m-3}} \quad \cdots \quad \xrightarrow{\partial_3} R^{\binom{m}{3}} \xrightarrow{\partial_2} R^{\binom{m}{2}} \xrightarrow{\partial_1} R^m \xrightarrow{\partial_0} R \tag{1}$$

associated to $a_1, \dots, a_m$. If $e_1, \dots, e_m$ is a basis for R^m, then ∂_0 sends e_i to a_i, and if $e_{i,j}$ for $1 \leq i < j \leq m$ is a basis for $R^{\binom{m}{2}}$, then $\partial_1(e_{i,j}) = a_j e_i - a_i e_j$. Furthermore, $\partial_{m-1}(1) = \epsilon_1 a_1 e_1 + \cdots + \epsilon_m a_m e_m$ with $\epsilon_i \in \{1, -1\}$.

Proposition 1.1. *Let $a_1, \dots, a_m \in R^G$ be an R-regular sequence. For $k = 2, \dots, m$, let $M_k \subseteq R^{\binom{k}{2}}$ be the kernel of the map ∂_1 of the Koszul complex associated to $a_1, \dots, a_k$. Then $a_1, \dots, a_m$ is an R^G-regular sequence if and only if the maps*

$$H^1(G, M_k) \longrightarrow H^1(G, R^{\binom{k}{2}}) \tag{2}$$

induced by the embeddings $M_k \subseteq R^{\binom{k}{2}}$ are injective for $k = 2, \dots, m$.

Proof. Since $a_1, \dots, a_m$ is R-regular, the sequence (1) is exact (see, for example, Eisenbud [9, Corollary 17.5]). Applying this to R^G, we see that in particular the part

$$(R^G)^{\binom{k}{2}} \longrightarrow (R^G)^k \longrightarrow R^G \tag{3}$$

from the Koszul complex over R^G associated to $a_1, \dots, a_k$ is exact if $a_1, \dots, a_k$ is R^G-regular. Conversely, it is easily seen from the definitions of the maps ∂_0 and ∂_1 that the exactness of (3) implies that a_k is not a zero divisor on $R^G/(a_1, \dots, a_{k-1})$. Hence $a_1, \dots, a_m$ is R^G-regular if and only if (3) is exact for $k = 2, \dots, m$.

Write N_k for the image of the map $R^{\binom{k}{2}} \longrightarrow R^k$. Since N_k is also the kernel of $R^k \longrightarrow R$, we obtain an exact sequence $0 \longrightarrow N_k^G \longrightarrow (R^G)^k \longrightarrow R^G$ and a commutative diagram

$$\begin{tikzcd} & N_k^G \arrow[dr] & \\ (R^G)^{\binom{k}{2}} \arrow[ur] \arrow[r] & (R^G)^k \arrow[r] & R^G. \end{tikzcd}$$

Hence (3) is exact if and only if the map $(R^G)^{\binom{k}{2}} \longrightarrow N_k^G$ is surjective. Now the exact sequence $0 \longrightarrow M_k \longrightarrow R^{\binom{k}{2}} \longrightarrow N_k \longrightarrow 0$ gives rise to the long exact sequence

$$0 \longrightarrow M_k^G \longrightarrow (R^G)^{\binom{k}{2}} \longrightarrow N_k^G \longrightarrow H^1(G, M_k) \longrightarrow H^1(G, R^{\binom{k}{2}}),$$

hence the surjectivity of $(R^G)^{\binom{k}{2}} \longrightarrow N_k^G$ is equivalent to the injectivity of $H^1(G, M_k) \longrightarrow H^1(G, R^{\binom{k}{2}})$. This completes the proof. $\square$

At this point we embark on a short digression. Suppose that G is finite and $H \leq G$ is a subgroup whose index is invertible in R. It was proved in Kemper [13] that then $\operatorname{depth}(R^H) \leq \operatorname{depth}(R^G)$. In particular, if R^H is Cohen-Macaulay, then so is R^G, which was already proved in Campbell et al. [6]. Unfortunately, the converse of this fails in general, and it is an interesting question under which conditions the converse does hold. For example, it was proved by Campbell et al. [6] that if K is a field of characteristic p, $R = S(V^*)$ for a KG-module V and H is a normal Sylow p-subgroup of G such that G is generated by H and reflections, then R^G is Cohen-Macaulay if and only if R^H is Cohen-Macaulay. We will give a further condition where this is true. A subgroup $H \leq G$ is called **strongly R-embedded** (see, for example, Thévenaz [20, p. 440]) if the following two properties hold:

(a) The index $(G : H)$ is invertible in R, and

(b) for $\sigma \in G \setminus H$ the intersection ${}^{\sigma}H \cap H$ has an order which is invertible in R, where ${}^{\sigma}H = \sigma H \sigma^{-1}$.

If the characteristic of R is a prime number p, we also say that H is strongly p-embedded. As a typical example, the normalizer of a Sylow p-subgroup P of G is strongly p-embedded if for all $\sigma \in G$ the intersection ${}^{\sigma}P \cap P$ is either P or the trivial group. Suppose that $H \leq G$ is strongly R-embedded. Then for $i > 0$ and M a module over the group ring $R^G G$, the restriction map $H^i(G, M) \longrightarrow H^i(H, M)$ is an isomorphism. This is a well-known result, but for lack of a reference I present a proof here which I learned from Jacques Thévenaz. Indeed, consider the transfer map $\mathrm{Tr}_{H,G}$: $H^i(H, M) \longrightarrow H^i(G, M)$. We have

$$\mathrm{Tr}_{H,G} \circ \mathrm{res}_{G,H} = (G : H) \cdot \mathrm{id},$$

hence $\mathrm{res}_{G,H}$ is injective by the property (a) above. Now use the Mackey formula (see, for example, Benson [2, Lemma 3.6.16]) to get

$$\mathrm{res}_{G,H} \mathrm{Tr}_{H,G}(g) = \sum_{\sigma \in H \backslash G / H} \mathrm{Tr}_{{}^{\sigma}H \cap H, H} \mathrm{res}_{H, {}^{\sigma}H \cap H}(\sigma g) = g$$

for $g \in H^i(H, M)$, since $H^i({}^{\sigma}H \cap H, M) = 0$ for $\sigma \notin H$ by the property (b). Hence $\mathrm{res}_{G,H}$ is also surjective.

The following corollary now becomes an easy consequence of Proposition 1.1.

Corollary 1.2. *Suppose $H \leq G$ is a strongly R-embedded subgroup. Then*

$$\mathrm{depth}(R^G) = \mathrm{depth}(R^H).$$

Proof. The inequality $\mathrm{depth}(R^G) \geq \mathrm{depth}(R^H)$ is proved in Kemper [13]. For the reverse inequality, let $a_1, \ldots, a_m \in R^G$ be a maximal R^G-regular sequence. Using the notation of Proposition 1.1, we conclude from this proposition that $H^1(G, M_k) \longrightarrow H^1(G, R^{\binom{k}{2}})$ is injective for $k = 2, \ldots, m$. But by the assumption we have a commutative diagram

$$\begin{array}{ccc} H^1(G, M_k) & \longrightarrow & H^1(G, R^{\binom{k}{2}}) \\ \downarrow \wr & & \downarrow \wr \\ H^1(H, M_k) & \longrightarrow & H^1(H, R^{\binom{k}{2}}), \end{array}$$

which by Proposition 1.1 shows that $a_1, \ldots, a_m$ is R^H-regular as well, hence $\mathrm{depth}(R^H) \geq \mathrm{depth}(R^G)$. □

Example 1.3. Let p be a prime number and $G = S_p$ the symmetric group on p symbols. Pick a Sylow p-subgroup $P \cong Z_p$, then the normalizer $H = \mathcal{N}_G(P) \cong Z_p \rtimes Z_{p-1}$ is a strongly p-embedded subgroup of G. Consider the action of G on the polynomial ring $R = \mathbb{F}_p[x_1, \ldots, x_p]$ by permutations of the indeterminates, so R^G is a polynomial algebra and in particular Cohen-Macaulay. Hence by Corollary 1.2 also R^H is Cohen-Macaulay. This may be unexpected, since R^P is not Cohen-Macaulay if $p \geq 5$ by Ellingsrud and Skjelbred [10] (or also by also by Theorem 3.6 of this paper).

We resume the main stream of the paper again and use the Proposition 1.1 to prove

Theorem 1.4. *Suppose that $r \geq 0$ is an integer and assume that $H^i(G,R) = 0$ for $1 \leq i < r$. (This assumption is void if $r \leq 1$.) Then any sequence in R^G of length $\leq r+1$ which is R-regular is also R^G-regular. Furthermore, an R-regular sequence $a_1, \ldots, a_{r+2} \in R^G$ is R^G-regular if and only if the map*

$$H^r(G,R) \longrightarrow H^r(G,R^{r+2}) \tag{4}$$

induced by the multiplication with $a_1, \ldots, a_{r+2}$ is injective.

Proof. Let $a_1, \ldots, a_m \in R^G$ be R-regular, with $1 \leq m \leq r+2$. We first treat a few special cases. If $m = 1$, then the sequence is clearly also R^G-regular. If $m = 2$, then the module M_m from Proposition 1.1 is 0, hence the map (2) is injective and the sequence is R^G-regular. If also $r = 0$, then the map (4) is always injective, which establishes the claimed equivalence in that case. Furthermore, suppose $m = 3$ and $r = 1$. Then M_m is the image of R under the (injective) map $\partial_2 = \partial_{m-1}$ from (1), hence the map (4) is up to signs equal to the map (2). This reduces the theorem in this case to Proposition 1.1.

Now we assume that $r > 1$. Then by assumption $H^1(G,R) = 0$, so the injectivity conditions in Proposition 1.1 are satisfied if and only if $H^1(G,M_k) = 0$ for $k = 2, \ldots, m$. Hence we have to show that $H^1(G,M_m) = 0$ for $2 \leq m \leq r+1$ and that $H^1(G,M_{r+2}) = 0$ if and only if the map (4) is injective. We first prove by induction on k that for $1 \leq k \leq \min\{r-1, m-1\}$, $H^1(G,M_m)$ is isomorphic to $H^k(G,\ker(\partial_k))$, where the ∂_k are the maps from the Koszul complex (1). In fact, from (1) we get the short exact sequence

$$0 \longrightarrow \ker(\partial_k) \longrightarrow R^{\binom{m}{k+1}} \xrightarrow{\partial_k} \ker(\partial_{k-1}) \longrightarrow 0,$$

which gives rise to the exact sequence

$$0 = H^{k-1}(G,R^{\binom{m}{k+1}}) \longrightarrow H^{k-1}(G,\ker(\partial_{k-1})) \longrightarrow$$
$$H^k(G,\ker(\partial_k)) \longrightarrow H^k(G,R^{\binom{m}{k+1}}) = 0,$$

which proves the claim.

Now if $m \leq r$, then we have shown that $H^1(G,M_m) \cong H^{m-1}(G,\ker(\partial_{m-1}))$, but $\ker(\partial_{m-1}) = 0$. Hence $H^1(G,M_m) = 0$ in this case. If $m = r+1$, then $H^1(G,M_m) \cong H^{r-1}(G,\ker(\partial_{m-2})) \cong H^{r-1}(G,R) = 0$. Finally, if $m = r+2$, then $H^1(G,M_m) \cong H^{r-1}(G,\ker(\partial_{m-3}))$, and the short exact sequence

$$0 \longrightarrow R \xrightarrow{\partial_{m-1}} R^m \xrightarrow{\partial_{m-2}} \ker(\partial_{m-3}) \longrightarrow 0$$

gives rise to the exact sequence

$$0 = H^{r-1}(G,R^m) \longrightarrow H^{r-1}(G,\ker(\partial_{m-3})) \longrightarrow H^r(G,R) \xrightarrow{\varphi} H^r(G,R^m),$$

where φ is up to signs induced by multiplication with $a_1, \ldots, a_m$. Hence for $m = r+2$, $H^1(G,M_m) \cong H^{r-1}(G,\ker(\partial_{m-3}))$ is 0 if and only if the map (4) is injective, which was to be shown. $\square$

We now change our point of view by fixing an element from $H^r(G, R)$ and considering its annihilator, which is an ideal in R^G. We need some more terminology and a few facts from commutative algebra. For an ideal $I \lhd R$ the maximal length of an R-regular sequence whose elements lie in I is denoted by $\operatorname{depth}_I(R)$, and $\operatorname{ht}(I)$ denotes the height of the ideal, which is the minimal height of a prime ideal containing I. Furthermore, a sequence $a_1, \ldots, a_m \in R$ is said to be a **partial system of parameters** if $(a_1, \ldots, a_m) \neq R$ and $\operatorname{ht}(a_1, \ldots, a_k) = k$ for $k = 1, \ldots, m$.

Lemma 1.5. *Let $a_1, \ldots, a_m \in R$ such that $(a_1, \ldots, a_m) \neq R$. Then the following statements hold:*

(a) The sequence $a_1, \ldots, a_m$ is a partial system of parameters if and only if a_i lies in none of the associated prime ideals $\mathfrak{p} \lhd R$ of $(a_1, \ldots, a_{i-1})$ for which $\operatorname{ht}(\mathfrak{p}) = i - 1$, for $i = 1, \ldots, m$.

(b) The sequence $a_1, \ldots, a_m$ is R-regular if and only if a_i lies in none of the associated prime ideals of $(a_1, \ldots, a_{i-1})$, for $i = 1, \ldots, m$. In particular, if $a_1, \ldots, a_m$ is R-regular, then it is a partial system of parameters.

(c) If R is Cohen-Macaulay and $a_1, \ldots, a_m$ is a partial system of parameters, then it is R-regular.

(d) If $I \lhd R$ is an ideal of height m, then there exist $a_1, \ldots, a_m \in I$ which are a partial system of parameters.

(e) If $R \subseteq S$ is an integral extension of rings and $I \lhd R$, then $\operatorname{ht}(SI) = \operatorname{ht}(I)$, where SI denotes the ideal in S generated by I. In particular, if $a_1, \ldots, a_m$ is a partial system of parameters in R, it is also one in S.

Proof. Clearly if $a_i \in \mathfrak{p}$ for an associated prime ideal $\mathfrak{p}$ of $(a_1, \ldots, a_{i-1})$ of height $i - 1$, then $\operatorname{ht}(a_1, \ldots, a_i) \leq i - 1$. Conversely, if $\operatorname{ht}(a_1, \ldots, a_i) = \operatorname{ht}(a_1, \ldots, a_{i-1}) = i - 1$ for some i, then there exists a prime ideal of height $i - 1$ containing $(a_1, \ldots, a_i)$. This prime must then be a minimal prime containing $(a_1, \ldots, a_{i-1})$ and is hence an associated prime of $(a_1, \ldots, a_{i-1})$ (see Eisenbud [9, Theorem 3.1]). This proves (a). The same theorem in [loc. cit.] says that the set of zero divisors of $R/(a_1, \ldots, a_{i-1})$ is the union of the associated primes of $(a_1, \ldots, a_{i-1})$, from which (b) follows immediately. Now (c) follows from the unmixedness theorem (see [loc. cit., Corollary 18.14]). To prove (d), we assume that $a_1, \ldots, a_{i-1} \in I$ with $\operatorname{ht}(a_1, \ldots, a_{i-1})$ have already been found. Then there exists $a_i \in I$ which lies in none of the associated primes of $(a_1, \ldots, a_{i-1})$ of height $i - 1$, since otherwise I would be contained in one of these prime ideals by the prime avoidance lemma (see [loc. cit., Lemma 3.3]), and hence $\operatorname{ht}(I) \leq i - 1$. By (a), this leads to a partial system of parameters.

To prove (e), let $\mathfrak{p} \lhd R$ be a prime of minimal height m containing I, and let $\mathfrak{p}_0 \subsetneqq \ldots \subsetneqq \mathfrak{p}_m = \mathfrak{p}$ be an ascending chain of primes. By the going-up theorem (see [loc. cit, Proposition 4.15]), there exists a chain $\mathfrak{q}_0 \subseteq \ldots \subseteq \mathfrak{q}_m$ of primes $\mathfrak{q}_i \lhd S$ with $\mathfrak{q}_i \cap R = \mathfrak{p}_i$, and by [loc. cit., Corollary 4.18], this chain cannot be refined. Since $\mathfrak{q}_m$ contains SI, $\mathrm{ht}(SI) \leq m$. For the reverse inequality, let $\mathfrak{q}_0 \subsetneqq \dots \subsetneqq \mathfrak{q}_r$ be an ascending chain of primes in S with $SI \subseteq \mathfrak{q}_r$, $r = \mathrm{ht}(SI)$, and set $\mathfrak{p}_i = \mathfrak{q}_i \cap R$. Then by [loc. cit., Corollary 4.18], $\mathfrak{p}_0 \subsetneqq \dots \subsetneqq \mathfrak{p}_r$, and $I \subseteq SI \cap R \subseteq \mathfrak{p}_r$. This shows $\mathrm{ht}(I) \leq r$. □

With these facts, we can now deduce the following corollary from Theorem 1.4. Larry Smith pointed out to me that this corollary also follows from the spectral sequence he studied in [18].

Corollary 1.6. *Assume that R is Cohen-Macaulay and G is finite, and that $H^i(G,R) = 0$ for $1 \leq i < r$, where $r > 0$ is an integer. Let $g \in H^r(G,R)$ be nonzero. Then for*

$$I = \mathrm{Ann}_{R^G}(g) := \{a \in R^G \mid a \cdot g = 0\} \lhd R^G$$

we have

$$\mathrm{depth}_I(R^G) = \min\{r+1, \mathrm{ht}(I)\}.$$

In particular, R^G is not Cohen-Macaulay if $\mathrm{ht}(I) > r+1$.

Proof. Assume that there exist $a_1, \dots, a_{r+2} \in I$ which form an R^G-regular sequence. By Lemma 1.5(b), the a_i are a partial system of parameters in R^G. So by (e) and the finiteness of G, they are also a partial system of parameters in R, hence the a_i form an R-regular sequence by (c). But since the a_i lie in I, g lies in the kernel of the map (4) from Theorem 1.4. Since $g \neq 0$, it follows by Theorem 1.4 that $a_1, \dots, a_{r+2}$ is in fact not R^G-regular. This proves that $\mathrm{depth}_I(R^G) \leq r+1$. Also clearly $\mathrm{depth}_I(R^G) \leq \mathrm{ht}(I)$.

By Lemma 1.5(d), there exists a partial system of parameters $a_1, \dots, a_m$ of length $m := \mathrm{ht}(I)$ with $a_i \in I$. Let $m' = \min\{r+1, m\}$. Then $a_1, \dots, a_{m'}$ is R-regular, and by Theorem 1.4, it is also R^G-regular. Hence $\mathrm{depth}_I(R^G) \geq m'$. If $m > r+1$, then $a_1, \dots, a_{r+2}$ is a partial system of parameters which is not an R^G-regular sequence, hence R^G is not Cohen-Macaulay by Lemma 1.5(c). □

In the above corollary the cohomology group $H^r(G,R)$ is regarded as a module over R^G, and a non-vacuous statement can be made if $I \neq 0$, i.e., if the element $g \in H^r(G,R)$ under consideration is a torsion element. If R is an integral domain with field of fractions $\mathrm{Quot}(R)$, then the kernel of the map

$$H^r(G,R) \longrightarrow H^r(G,\mathrm{Quot}(R))$$

consists exactly of the torsion elements. But it is well known that $H^r(G,\mathrm{Quot}(R)) = 0$. In fact, by the normal basis theorem $\mathrm{Quot}(R)$ is isomorphic to the regular module over $\mathrm{Quot}(R^G)$. Hence $H^r(G,R)$ is a torsion module. We will make use of this in the next section. However, we will need more precise information on the annihilators than is provided by the above argument.

Lemma 1.7. *Suppose that U is a finitely generated KG-module and let $g \in H^r(G,U)$ with $r > 0$. Let $W = KG$ be the regular module and $a = \sum_{\sigma \in G} \sigma \in W^G$. Then $a \otimes g = 0$ as an element of $H^r(G, W \otimes U)$.*

Proof. We first observe that $H^r(G, W) = 0$. This can be seen by the Eckmann-Shapiro lemma (see Benson [2, Corollary 2.8.4]), for example. It follows that $H^r(G, P) = 0$ for any projective module P. But $W \otimes U$ is the tensor product of a projective module and another module, hence it is projective (see, for example, Benson [2, Proposition 3.1.5]). So $H^r(G, W \otimes U) = 0$. $\square$

2 Linear actions

In this section, we specialize the assumptions by looking at the standard situation of invariant theory of finite groups: K is a field, V is a finite dimensional vector space over K, and $R = S(V^*)$ is the symmetric algebra of the dual of V, which is isomorphic to a multivariate polynomial ring. Furthermore, $G \leq \mathrm{GL}(V)$ is a finite linear group on V, which has a natural action on R. As in Section 1, we write R^G for the invariant ring. Furthermore, let p be the characteristic of K, which may be 0.

In order to use Lemma 1.7 for finding elements $a \in R^G$ which annihilate a given $g \in H^r(G, R)$, we have to recover (copies of) the regular module in R. This is done in the next lemma, where we assume that K is algebraically closed, which allows us to view the elements of R as functions on V. We write $V^\sigma \leq V$ for the fixed space of a $\sigma \in G$, and $\mathrm{Stab}_G(v)$ for the stabilizer of a $v \in V$.

Lemma 2.1. *Assume that K is algebraically closed, let $m \in \{1, \dots, \dim(V)\}$ be an integer and suppose that every element $\sigma \in G$ of order p has $\mathrm{rank}(\sigma - 1) \geq m$. (This assumption is void if $p = \mathrm{char}(K) = 0$.) Then there exist m embeddings*

$$\varphi_i \colon KG \hookrightarrow R \quad (i = 1, \dots, m)$$

of the regular KG-module into R such that the polynomials

$$a_i = \varphi_i\left(\sum_{\sigma \in G} \sigma\right) \quad (i = 1, \dots, m)$$

form a partial system of parameters in R^G. Moreover, the a_i lie in the unique homogeneous maximal ideal R_+^G of R^G.

Proof. Suppose by induction that $\varphi_1, \dots, \varphi_{k-1}$ have already been constructed for a $k \in \{1, \dots, m\}$. By assumption, the set

$$X = \{v \in V \mid \mathrm{Stab}_G(v) \text{ has an order divisible by } p\} = \bigcup_{\substack{\sigma \in G,\\ \mathrm{ord}(\sigma) = p}} V^\sigma$$

has dimension $\leq n - m$, where $n = \dim_K(V)$. But every associated prime $\mathfrak{p} \lhd R$ of $(a_1, \dots, a_{k-1})$ has height $k - 1$ and Krull dimension $n - k + 1$, which is greater than $n - m$. Hence there exists a point $w_\mathfrak{p} \in \mathcal{V}_V(\mathfrak{p}) \setminus X \subseteq V$ for every such $\mathfrak{p}$, where $\mathcal{V}_V(\mathfrak{p})$ denotes the variety in V given by $\mathfrak{p}$, and the $w_\mathfrak{p}$ can be chosen such that $w_{\mathfrak{p}} \neq \sigma(w_{\mathfrak{p}'})$ for $\mathfrak{p} \neq \mathfrak{p}'$ and $\sigma \in G$. Furthermore, we can choose a point $v_0 \in V$ such that the set

$$\{\sigma(v_0) \mid \sigma \in G\} \cup \{w_{\mathfrak{p}} \mid \mathfrak{p} \in \operatorname{Ass}(a_1, \ldots, a_{k-1})\} \cup \{0\}$$

has exactly $|G| + |\operatorname{Ass}(a_1, \ldots, a_{k-1})| + 1$ (distinct) elements. In fact, v_0 has to avoid the points 0 and $\sigma(w_{\mathfrak{p}})$ for $\sigma \in G$, and the finite union $\cup_{\sigma \in G \setminus \{\mathrm{id}\}} V^\sigma$ of proper subspaces. Now there exists a polynomial $g \in R$ with the following properties (where δ is the Kronecker-delta):

(i) $g(\sigma(v_0)) = \delta_{\sigma,\mathrm{id}}$,

(ii) $g(\sigma(w_{\mathfrak{p}})) = \delta_{\sigma(w_{\mathfrak{p}}),w_{\mathfrak{p}}}$,

(iii) $g(0) = 0$.

We define φ_k: $KG \to R$ by setting $\varphi_k(\sigma) = \sigma(g)$. This is clearly a G-map. To prove that it is injective, suppose that

$$\sum_{\sigma \in G} \alpha_\sigma \cdot \sigma(g) = 0$$

with $\alpha_\sigma \in K$. For $\tau \in G$, evaluation at $\tau(v_0)$ yields

$$0 = \sum_{\sigma \in G} \alpha_\sigma \cdot \sigma(g)(\tau(v_0)) = \sum_{\sigma \in G} \alpha_\sigma \cdot g(\sigma^{-1}\tau v_0) = \alpha_\tau.$$

Hence the $\sigma(g)$ are linearly independent, and φ_k is injective.

The polynomial a_k defined in the statement of the lemma is clearly an invariant, and $1 \notin (a_1, \ldots, a_k)$ by the property (iii). Evaluating a_k at $w_{\mathfrak{p}}$ yields

$$a_k(w_{\mathfrak{p}}) = \sum_{\sigma \in G} \sigma(g)(w_{\mathfrak{p}}) = \sum_{\sigma \in G} g(\sigma^{-1}(w_{\mathfrak{p}})) = |\operatorname{Stab}_G(w_{\mathfrak{p}})| \neq 0,$$

since $w_{\mathfrak{p}} \notin X$. Because $w_{\mathfrak{p}} \in \mathcal{V}_V(\mathfrak{p})$, this means that a_k lies in none of the associated prime ideals of $(a_1, \ldots, a_{k-1})$, which by Lemma 1.5(a) shows that $a_1, \ldots, a_k$ is a partial system of parameters. The a_i lie in R_+^G since $a_i(0) = 0$ by the property (iii) above. This completes the proof. □

Remark 2.2. If $|G|$ is a multiple of p, then by Benson [3, Theorem 4.1.3] $H^r(G, K) \neq 0$ for some $r > 0$. In fact, we see from the proof in [3] that if $\sigma \in G$ is an element of order p and if the index of $\langle\sigma\rangle$ in its normalizer is $p^a h$ with $p \nmid h$, then r can be chosen as $2(p-1)p^a$. Since K occurs as the direct summand $S^0(V^*)$ in R, it follows that $H^r(G, R) \neq 0$.

Putting the various strands together, we obtain

Theorem 2.3. *Suppose that $H^r(G, R) \neq 0$ for an integer $r > 0$ and that every element $\sigma \in G$ of order p has $\operatorname{rank}(\sigma - 1) \geq r + 2$. Then R^G is not Cohen-Macaulay.*

Proof. We may assume that $r > 0$ is minimal with $H^r(G, R) \neq 0$. Furthermore, since $H^r(G, R) \neq 0$, p must divide the order of G, hence there exist elements $\sigma \in G$ of order p. By the assumption it follows that $n := \dim(V) \geq r + 2$. Assume that R^G is Cohen-Macaulay. Then R^G is a free module over the algebra $K[a_1, \ldots, a_n]$ generated by a homogeneous system of parameters. If $\bar{K}$ is the algebraic closure of K, then it follows that $\bar{K} \otimes_K R^G$ is free over $\bar{K}[a_1, \ldots, a_n]$, hence $\bar{K} \otimes_K R^G$ is also Cohen-Macaulay. So we can assume that K is algebraically closed. Then by Lemma 2.1 there are $m := r + 2$ embeddings $\varphi_1, \ldots, \varphi_m$ of the regular module KG into R, and the images contain invariants $a_i \in R^G$ which form a partial system of parameters of length m. Now take a nonzero $g \in H^r(G, R)$. Then by Lemma 1.7, $a_i \otimes g = 0$ as elements in $H^r(G, R \otimes R)$. Applying the map $H^r(G, R \otimes R) \longrightarrow H^r(G, R)$ induced by $R \otimes R \longrightarrow R$, $f \otimes g \mapsto fg$ yields that $a_i g = 0$ in $H^r(G, R)$, hence the a_i lie in the annihilator I of g. It follows that $\mathrm{ht}(I) \geq m > r + 1$, so R^G is not Cohen-Macaulay by Corollary 1.6. $\square$

We obtain the following result on vector invariants.

Corollary 2.4. *Suppose that $|G|$ is a multiple of p. Then there exists an $m \in \mathbb{N}$ such that $S((V^k)^*)^G$ is not Cohen-Macaulay for $k \geq m$. Here V^k denotes the direct sum of k copies of V, and $S((V^k)^*)$ is the symmetric algebra of its dual. In particular, there exists a KG-module W such that $S(W^*)^G$ is not Cohen-Macaulay.*

Proof. By Remark 2.2, there exists an $r > 0$, such that $H^r(G, K) \neq 0$. Then $H^r(G, S((V^k)^*)) \neq 0$ for all $k \in \mathbb{N}$. Now if $k \geq r + 2$, then and every $\sigma \in G$ with $\sigma \neq \mathrm{id}$ acts on V^k with $\mathrm{rank}_{V^k}(\sigma - 1) \geq r + 2$. So the assertion follows from Theorem 2.3. $\square$

Remark 2.5. As we see by the above proof, one can take $m = 3$ if G contains a normal subgroup of index p, since this implies the existence of a nonzero additive character $G \to K$, or, equivalently, a nonzero element in $H^1(G, K)$. This generalizes one of the results in Campbell et al. [8].

We now study regular representations of finite groups. If G is a finite group and K a field we shall write V_{reg} for the regular KG-module. The aim is to classify all pairs (G, K) such that $K[V_{reg}]^G$ is Cohen-Macaulay. I am thankful to Ian Hughes for raising this question.

Lemma 2.6. *If with the above notation $|G|$ is divisible by $\mathrm{char}(K)$, then $H^1(G, K[V_{reg}]) \neq 0$.*

Proof. $K[V_{reg}]$ is a polynomial ring with indeterminates x_σ indexed by elements of G. Choose a subgroup $H \leq G$ of order $p := \mathrm{char}(K)$ and form the monomial $t = \prod_{\sigma \in H} x_\sigma$, whose stabilizer is H. The module $M \leq K[V_{reg}]$ spanned by the G-orbit of t is the induced module from the trivial KH-module, hence by the Eckmann-Shapiro lemma $H^1(G, M) \cong H^1(H, K) \neq 0$. But M is a direct summand of $K[V_{reg}]$, so $H^1(G, M)$ is a direct summand of $H^1(G, K[V_{reg}])$. $\square$

Theorem 2.7. *Let G be a finite group and K a field. Then $K[V_{reg}]^G$ is Cohen-Macaulay if and only if $|G|$ is not a multiple of the characteristic of K or $G \in \{Z_2, Z_3, Z_2 \times Z_2\}$.*

Proof. Suppose that $K[V_{reg}]^G$ is Cohen-Macaulay and $p := \mathrm{char}(K)$ divides $|G|$. We have to show that then $G \in \{Z_2, Z_3, Z_2 \times Z_2\}$. Indeed, $H^1(G, K[V_{reg}]) \neq 0$ by Lemma 2.6 and an element $\sigma \in G$ of order p acts on V_{reg} with $\mathrm{rank}(\sigma - 1) = |G| \cdot (p-1)/p$. Hence by Theorem 2.3 we must have $|G| \cdot (p-1)/p < 3$, so $|G| \leq 4$. So we must only show that G cannot be Z_4. Indeed, $K[V_{reg}]^{Z_4}$ is not Cohen-Macaulay if $\mathrm{char}(K) = 2$ by Bertin [5], or by Theorem 3.6 of this paper.

Conversely, if $p \nmid |G|$ then $K[V_{reg}]^G$ is Cohen-Macaulay by Hochster and Eagon [11]. For $G \in \{Z_2, Z_3\}$ the Cohen-Macaulayness follows from Ellingsrud and Skjelbred [10] since G is a p-group and the dimension of the representation is ≤ 3. We are left with the case $G = Z_2 \times Z_2$, and here the invariant ring can be looked up in Adem and Milgram [1, Chapter 3, Corollary 1.8] or calculated with a computer (see Kemper and Steel [15]). The result is a Cohen-Macaulay ring. □

We note a few more applications of Theorem 2.3.

Corollary 2.8. *Suppose that $p = \mathrm{char}(K) \geq 5$ and that G acts as a transitive permutation group on a basis $e_1, \ldots, e_n$ of a vector space W over K, where n is a multiple of p.*

(a) Let V be the quotient module $W/K \cdot (e_1 + \cdots + e_n)$. Then $R^G = S(V^*)^G$ is not Cohen-Macaulay.

(b) Suppose that G contains a transitive cyclic subgroup, $n > 5$, and V_0 is the kernel of the trace map

$$\pi\colon V \to K,\ \sum_{i=1}^{n} \alpha_i e_i + K \cdot (e_1 + \cdots + e_n) \mapsto \sum_{i=1}^{n} \alpha_i.$$

Then $S(V_0^*)^G$ is not Cohen-Macaulay.

Proof. Consider the exact sequence

$$0 \longrightarrow K \longrightarrow W \longrightarrow V \longrightarrow 0.$$

By the transitivity of G, a G-map from W into K must assign the same value to all e_i. Composing this with the map $K \to W$ yields the zero-map $K \to K$. Hence the sequence is non-split. Dualizing gives a non-split extension of K by V^*, which shows that $H^1(G, V^*) \neq 0$, hence $H^1(G, R) \neq 0$. Now consider the exact sequence

$$0 \longrightarrow K \longrightarrow W_0 \longrightarrow V_0 \longrightarrow 0,$$

where W_0 is the kernel of the trace map, and assume there exists a $\sigma_0 \in G$ with $\sigma_0(e_i) = e_{i+1}$, where the indices are taken modulo n. Then a G-map $W_0 \to K$ must take the same value α on all $e_i - e_{i+1}$, hence the vector $e_1 + \cdots + e_n =$

$\sum_{i=1}^{n} i\cdot(e_i - e_{i+1})$ is mapped to $\binom{n+1}{2}\alpha = 0$. As above, the sequence is non-split, and we obtain $H^1(G, V_0^*) \neq 0$.

The proof is complete if we can show that $\mathrm{rank}_V(\sigma - 1)$ and $\mathrm{rank}_{V_0}(\sigma - 1)$ are at least 3 for every element $\sigma \in G$ of order p. We can assume that the disjoint cycle representation of σ contains the cycle $(1, 2, \ldots, p)$, and will show that $(\sigma-1)(e_1), (\sigma-1)(e_2), (\sigma-1)(e_3)$ are linearly independent in V. Indeed, a linear relation has the form

$$\alpha_1(e_2 - e_1) + \alpha_2(e_3 - e_2) + \alpha_3(e_4 - e_3) = \alpha(e_1 + \cdots + e_n)$$

with $\alpha, \alpha_1, \alpha_2, \alpha_3 \in K$. It follows that $\alpha = \alpha_3 = \alpha_2 = \alpha_1 = 0$. Next we show that $(\sigma-1)(e_2 - e_1), (\sigma-1)(e_3 - e_2), (\sigma-1)(e_4 - e_3)$ are linearly independent in V_0 if $n > 5$. Here we obtain

$$\alpha_1(e_3 - 2e_2 + e_1) + \alpha_2(e_4 - 2e_3 + e_2) + \alpha_3(e_5 - 2e_4 + e_3) = \alpha(e_1 + \cdots + e_n),$$

so again all α_i are zero. □

Example 2.9. If n is a multiple of p and $p \geq 5$, then the symmetric group S_n is an example of the type dealt with in Corollary 2.8. With the notation from the corollary, we get the result that $S(V^*)^{S_n}$ is not Cohen-Macaulay, and neither is $S(V_0^*)^{S_n}$ if $n > 5$. S_n acts on both V and V_0 as a reflection group. Thus we have found an infinite series of finite reflection groups whose invariant rings are not even Cohen-Macaulay. Another such series, which consists of abelian p-groups, was given by Nakajima [16] (see Example 3.10 below). In our example, the action of S_n on V_0 is irreducible for $n > 5$. It is quite surprising that by Kemper and Malle [14] the field of fractions $K(V_0)^{S_n}$ of $S(V_0^*)^{S_n}$ is a rational function field over K. What may be even more surprising is that although $S(V^*)^{S_n}$ is not Cohen-Macaulay, the invariant ring $S(V)^{S_n}$ of the dual representation is a polynomial ring. In fact it is easily seen that $S(V)^{S_n}$ is generated by the images of the elementary symmetric polynomials $s_2(e_1, \ldots, e_n), \ldots, s_n(e_1, \ldots, e_n) \in S(W)$ in $S(V)$.

It is sometimes possible to read Theorem 2.3 "backwards" to obtain lower bounds on $r > 0$ such that $H^r(G, R) \neq 0$. This leads to an example where easy facts from invariant theory can be used to obtain non-trivial statements of group theory.

Example 2.10. Suppose that $G = S_n$ or $G = A_n$ is the symmetric or alternating group on n letters. We look at several permutation representations of G.

(a) First, let V be the natural permutation module, and $p = \mathrm{char}(K) \geq 3$. (We do not assume that p divides n.) The invariant ring R^G is Cohen-Macaulay. In fact, it is isomorphic to a polynomial ring if $G = S_n$, and a hypersurface of $G = A_n$. For an element $\sigma \in G$ of order p we have $\mathrm{rank}(\sigma - 1) \geq p - 1$. It now follows by Theorem 2.3 that $H^r(G, R) = 0$ for $0 < r \leq p - 3$. In particular, $H^r(G, K) = 0$ for such r. Thus the fact that S_n and A_n have no non-split central extension with kernel of order $p \geq 5$ can easily be derived from Theorem 2.3.

(b) Now suppose that V is a direct sum of m copies of the natural permutation module of G ($m \in \mathbb{N}$). In order to calculate the cohomology of R, we look at a decomposition of R into a direct sum of KG-modules, which will yield a decomposition of $H^r(G,R)$. Such a decomposition is given by taking the submodules of R spanned by G-orbits of monomials in the variables $x_{i,j}$ $(1 \leq i \leq m,\ 1 \leq j \leq n)$, which are a basis of V^* on which G acts by $\sigma(x_{i,j}) = x_{i,\sigma(j)}$. Each of these modules is induced from the trivial module over KH, where H is the stabilizer of a monomial. So by the Eckmann-Shapiro lemma, the cohomology of G with values in the span of a monomial-orbit is equal to the cohomology of the stabilizer H of the monomial with values in K. But we see that such a stabilizer is either a direct product of symmetric groups (possibly on fewer letters) or the subgroup of even permutations contained in this product, so it has no normal subgroup of index p except for the case $G = A_3$, hence $H^1(H,K) = 0$ in all other cases. It follows that $H^1(G,R) = 0$ if $G \neq A_3$. In fact, one can combine the arguments from parts (a) and (b) of this example to show that $H^r(G,R) = 0$ for $0 < r \leq p-3$.

(c) Let V be as in (b) and assume that $G = S_p$ or A_p. Take an element $\sigma \in G$ of order p, then $\langle\sigma\rangle$ has an index divisible by $p-1$ in its normalizer. It follows by Remark 2.2 that the first $r > 0$ with $H^r(G,R) \neq 0$ is bounded from above by $2(p-1)$. On the other hand, $\operatorname{rank}(\sigma - 1) = m(p-1)$, so by Theorem 2.3, R^G is not Cohen-Macaulay if $m \geq 3$. In view of (b), this yields an example where the higher cohomology modules are indeed needed.

3 A closer look at the geometry

In this section we restrict our point of view drastically by only considering $H^1(G,R)$ and most of the time only cocycles with values in K. Using $H^1(G,R)$ means that we are looking for partial systems of parameters of length 3 which are not R^G-regular sequences. It is surprising how much can be said in spite of this narrowing of possibilities. The benefit of the restriction lies in a more accurate geometric description of the ideal $I = \operatorname{Ann}_{R^G}(g)$ occurring in Corollary 1.6.

We adopt the same notation as in the previous section, so V is a finite dimensional vector space over a field K of characteristic p, and $G \leq \mathrm{GL}(V)$ is a finite linear group on V with the natural action on the symmetric algebra $R = S(V^*)$ of the dual. Furthermore, if $X \subseteq V$ is a set of points, we write $I_R(X)$ and $I_{R^G}(X)$ for the ideals of all polynomials or invariants, respectively, which vanish on all points of X. If $I \subseteq R$ is a set of polynomials, we write $\mathcal{V}_V(I)$ for the set of points in V where all $f \in I$ vanish. It is convenient to use the bar resolution, so we view cocycles from $Z^1(G,M)$ as maps $G \to M$ which we denote by $(g_\sigma)_{\sigma \in G}$.

Proposition 3.1. *Let $g \in H^1(G,R)$ be nonzero, $(g_\sigma)_{\sigma\in G} \in Z^1(G,R)$ a cocycle representing g, and let*

$$X = \bigcup_{\sigma\in G} \left(V^\sigma \setminus \mathcal{V}_V(g_\sigma)\right) \subseteq V.$$

Then $\operatorname{Ann}_{R^G}(g) \subseteq I_{R^G}(X)$.

Proof. Take $f \in I := \operatorname{Ann}_{R^G}(g)$. Then there exists an $h \in R$ such that $f \cdot g_\sigma = (\sigma - 1)h$ for all $\sigma \in G$. Hence if a point $v \in V$ lies in $V^\sigma \setminus \mathcal{V}_V(g_\sigma)$ for some σ, we obtain $f(v) \cdot g_\sigma(v) = h(\sigma^{-1}(v)) - h(v) = 0$, hence $f(v) = 0$. This shows that $f \in I_{R^G}(X)$. □

We are going to prove the reverse inclusion for the special case that the cocycle (g_σ) takes values in K. Before doing so, we present the following cautionary example.

Example 3.2. Suppose that $G = \langle\sigma\rangle$ is a cyclic group and we are interested in computing the ideal $I \lhd R^G$ consisting of all $(\sigma - 1)h \in R^G$ with $h \in R$. If $v \in V^\sigma$, then $((\sigma-1)h)(v) = h(\sigma^{-1}(v)) - h(v) = 0$. If on the other hand v lies in $V \setminus V^\sigma$, then there exists an $h \in R$ which takes different values on v and on $\sigma^{-1}(v)$, hence $((\sigma - 1)h)(v) \neq 0$. So one might be tempted to conclude that the radical ideal of I is exactly $I_{R^G}(V^\sigma)$. But if K is of characteristic 0, then I must be the zero ideal, since $(\sigma - 1)h = g \in R^G$ implies $\sigma^i(h) = h + i \cdot g$, hence $g = 0$ or G would be infinite. So the conclusion $\sqrt{I} = I_{R^G}(V^\sigma)$ is in general quite wrong.

It is surprising that in the situation of Proposition 3.5 we will obtain exactly the result that turned out to be false in the above example. In order to move on safe ground, we prove

Lemma 3.3. *Suppose that K is algebraically closed and let A be a subalgebra of R such that R is finitely generated as a module over A. Then for an ideal $I \trianglelefteq A$ we have*

$$\sqrt{I} = I_A(\mathcal{V}_V(I)).$$

Proof. If $f \in \sqrt{I}$, then $f^k \in I$ for some $k \in \mathbb{N}$, so for $v \in \mathcal{V}_V(I)$ we have $f^k(v) = 0$, hence $f \in I_A(\mathcal{V}_V(I))$.

Conversely, suppose that $f \in I_A(\mathcal{V}_V(I))$. Then f lies in all maximal ideals $\mathfrak{m} \lhd R$ in R containing I, since K is algebraically closed. Let $\mathfrak{p} \lhd A$ be a prime ideal in A containing I. Then by the going-up theorem, there exists a prime ideal $\mathfrak{q} \lhd R$ such that $\mathfrak{q} \cap A = \mathfrak{p}$. By Hilbert's Nullstellensatz (Eisenbud [9, Theorem 4.19]), $\mathfrak{q}$ is equal to the intersection of all maximal ideals in R containing $\mathfrak{q}$. But f lies in each of these maximal ideals, hence $f \in \mathfrak{q}$ and then also $f \in \mathfrak{p}$, since f is an invariant. We have shown that f lies in every prime ideal in A containing I, and by Eisenbud [9, Corollary 2.12], the intersection of all these prime ideals is the radical of I. □

If $g \in H^1(G,K)$, then the cocycle (g_σ) representing g is uniquely determined and is in fact a homomorphism from G into the additive group of K. Hence we can look at its kernel.

Proposition 3.4. *Assume that K is algebraically closed and let $g \in H^1(G, K)$ be nonzero with kernel $N \lhd G$. Let $J \lhd R^G$ be the image of the relative transfer*

$$\mathrm{Tr}_N^G : R^N \to R^G, \; f \mapsto \sum_{i=1}^{r} \sigma_i(f),$$

where $\sigma_1, \ldots, \sigma_r$ is a system of coset representatives of N in G. Then

$$\sqrt{J} = I_{R^G}(X) \quad \textit{with} \quad X = \bigcup_{\sigma \in G \setminus N} V^\sigma.$$

Proof. In view of Lemma 3.3, we must show that $X = \mathcal{V}_V(J)$. So take a point $v \in V^\sigma$ for some $\sigma \in G \setminus N$. We have $\sigma^p \in N$, since $g_{\sigma^p} = p \cdot g_\sigma = 0$. Let $H \leq G$ be the subgroup generated by N and σ, then for $h \in R^N$ we have

$$\mathrm{Tr}_N^H(h)(v) = \sum_{i=0}^{p-1} h(\sigma^{-i}(v)) = \sum_{i=0}^{p-1} h(v) = 0,$$

hence $\mathrm{Tr}_N^G(h)(v) = 0$. This shows that $v \in \mathcal{V}_V(J)$.

Now suppose that $v \in V \setminus X$. An easy calculation shows that this implies that the N-orbits of $\sigma_i(v)$ for $i = 1, \ldots, r$ are pairwise disjoint. Hence there exists an $h \in R^N$ such that $h(\sigma_i^{-1}(v)) = \delta_{1,i}$. It follows that $\mathrm{Tr}_N^G(h)(v) = 1$, hence $v \notin \mathcal{V}_V(J)$. □

I owe the idea of the preceding proof to a conversation with Jim Shank. We now put Proposition 3.1 and Proposition 3.4 together.

Proposition 3.5. *Assume that K is algebraically closed and let $g \in H^1(G, K)$ be nonzero with kernel $N \lhd G$. Moreover, let $I = \mathrm{Ann}_{R^G}(g)$ be its annihilator. Then*

$$\sqrt{I} = I_{R^G}(X) \quad \textit{with} \quad X = \bigcup_{\sigma \in G \setminus N} V^\sigma.$$

Proof. The inclusion $\sqrt{I} \subseteq I_{R^G}(X)$ was already shown in Proposition 3.1. So suppose that $f \in I_{R^G}(X)$. Then by Proposition 3.4, $f^k = \mathrm{Tr}_N^G(h)$ with $h \in R^N$ and $k \in \mathbb{N}$. Now G/N is embedded in K, so it must be an elementary abelian p-group. Take $\sigma_1, \ldots, \sigma_m \in G$ to be generators for this group, then

$$f^k = \sum_{i_1, \ldots, i_m = 0}^{p-1} \sigma_1^{i_1} \cdots \sigma_m^{i_m}(h) = (\sigma_1 - 1)^{p-1} \cdots (\sigma_m - 1)^{p-1}(h),$$

where we used the polynomial identity $1 + X + \cdots + X^{p-1} = (X-1)^{p-1}$ over K. Write $\delta_j = \sigma_j - 1$ and form

$$\widetilde{h} = \sum_{i=1}^{m} g_{\sigma_i} \cdot \left(\delta_1^{p-1} \cdots \delta_{i-1}^{p-1} \delta_i^{p-2} \delta_{i+1}^{p-1} \cdots \delta_m^{p-1}(h) \right).$$

Since δ_i^p yields zero when applied to an invariant under N, it follows that $\delta_i \widetilde{h} = g_{\sigma_i} \cdot f^k$, and from that $(\sigma - 1)\widetilde{h} = g_\sigma \cdot f^k$ for any $\sigma \in G$. Hence f^k lies in $I = \mathrm{Ann}_{R^G}(g)$ and so $f \in \sqrt{I}$. $\square$

An automorphism $\sigma \neq \mathrm{id}$ of a vector space is called a **bireflection** if $\mathrm{rank}(\sigma - 1) \leq 2$. In the case $r = 1$ of Theorem 2.3, the hypothesis is that G contains no bireflection of order p. With the help of Proposition 3.5, we can now weaken this hypothesis.

Theorem 3.6. *Assume that G has a normal subgroup N of index p, which contains all bireflections in G. Then R^G is not Cohen-Macaulay.*

Proof. As in the proof of Theorem 2.3, we can assume that K is algebraically closed. There is an element $g \in H^1(G, K)$ with kernel N. Since all bireflections of G are contained in N, the codimension of all V^σ for $\sigma \in G \setminus N$ is at least 3. Hence for $X = \cup_{\sigma \in G \setminus N} V^\sigma$ we have $\mathrm{ht}(I_{R^G}(X)) \geq 3$. But by Proposition 3.5, $I_{R^G}(X)$ is the radical of $I = \mathrm{Ann}_{R^G}(g)$, hence $\mathrm{ht}(I) \geq 3$, and the theorem follows from Corollary 1.6. $\square$

If G is not generated by bireflections, then the bireflections in G generate a proper normal subgroup. If G is a p-group, then this can be extended to a normal subgroup of index p. So we obtain

Corollary 3.7. *If G is a p-group and R^G is Cohen-Macaulay, then G is generated by bireflections.*

Remark 3.8. Kac and Watanabe proved in [12] that if the invariant ring of a finite linear group G is a complete intersection, then G is generated by bireflections. Since the complete intersection property implies the Cohen-Macaulay property (see Stanley [19]), we have recovered their result for the special case of p-groups. The remarkable thing is that in this case the much weaker hypothesis of Cohen-Macaulayness of the invariant ring suffices.

We can do better than Theorem 3.6 if we widen our point of view just very slightly by multiplying a 1-cocycle with values in K, as considered in Theorem 3.6, by an invariant from R^G. This leads to the following improvement.

Theorem 3.9. *Suppose that G has a normal subgroup N with factor group an elementary abelian p-group, and suppose that there is a $\sigma_0 \in G \setminus N$, σ_0 not a bireflection, such that for all bireflections $\sigma \in G \setminus N$ we have*

$$V^{\sigma_0} \not\subseteq V^\sigma.$$

Then R^G is not Cohen-Macaulay.

Proof. As before, we can assume that K is algebraically closed. Write

$$X = \bigcup_{\sigma \in G \setminus N} V^\sigma \quad \text{and} \quad X' = \bigcup_{\substack{\sigma \in G \setminus N, \\ \sigma \text{ bireflection}}} V^\sigma.$$

Then the hypothesis says that $X' \subsetneqq X$. Since X and X' are closed and G-stable, there exists an invariant $h \in I_{R^G}(X') \setminus I_{R^G}(X)$. Let $I \lhd R$ be the ideal of the invariants which vanish on all fixed spaces V^σ for $\sigma \in G \setminus N$ not a bireflection. Then $\operatorname{ht}(I) \geq 3$, hence by Lemma 1.5(d) there exist $a_1, a_2, a_3 \in I$ which form a partial system of parameters. We have $h \cdot a_i \in I_{R^G}(X)$.

There exists a $g \in H^1(G, K)$ with kernel N. By Proposition 3.5, the $h \cdot a_i$ lie in the radical of the annihilator of g, hence $h^k \cdot a_i^k \in \operatorname{Ann}_{R^G}(g)$ for some $k \in \mathbb{N}$. It follows that $a_i^k \in \operatorname{Ann}_{R^G}(g')$ with $g' = h^k \cdot g$ $(i = 1, 2, 3)$. The proof is complete by Corollary 1.6 if we can show that g' is nonzero. But that is equivalent to $h^k \notin \operatorname{Ann}_{R^G}(g)$, which is true since $h \notin I_{R^G}(X) = \sqrt{\operatorname{Ann}_{R^G}(g)}$. □

Clearly Theorem 3.6 cannot be used to show the non-Cohen-Macaulayness of R^G in the case that G is generated by bireflections. However, in the following example G is even generated by reflections, and we are able to prove that R^G is not Cohen-Macaulay by using Theorem 3.9.

Example 3.10. In [16], Nakajima gave the following groups as an example of reflection groups whose invariant rings are not Cohen-Macaulay. Let K be a finite field, $m \geq 3$, $n = 2m + 1$, and consider the group G consisting of the $n \times n$-matrices

$$\left(\begin{array}{cccc|ccc}
1 & & & & & & \\
& \ddots & & & & 0 & \\
& & 1 & & & & \\
& & & 1 & & & \\
\hline
\alpha_0 & & & \alpha_m & 1 & & \\
& \ddots & & \vdots & & \ddots & \\
& & \alpha_{m-1} & \alpha_m & & & 1
\end{array}\right)$$

with $\alpha_0, \ldots, \alpha_m \in K$. Our goal is to recover Nakajima's result that R^G is not Cohen-Macaulay. Let $N \lhd G$ be the subgroup consisting of all matrices with $\alpha_m = 0$. For any bireflection $\sigma \in G \setminus N$, α_m must be nonzero, and at most one other α_i can be nonzero, since $m \geq 3$. Hence the $(m+1)$-st coordinate of a vector in V^σ must be zero. Now let σ_0 be the matrix with $\alpha_0 = \ldots = \alpha_m = 1$. Then $\sigma_0 \in G \setminus N$ is not a bireflection, and V^{σ_0} contains a vector whose $(m+1)$-st coordinate is nonzero. This means that $V^{\sigma_0} \nsubseteq V^\sigma$ for all bireflections $\sigma \in G \setminus N$. Hence the result follows by Theorem 3.9.

The argument in the above example is based on a more elementary proof which was shown to me by Ian Hughes.

References

[1] Alejandro Adem, R. James Milgram, *Cohomology of Finite Groups*, Springer-Verlag, Berlin, Heidelberg, New York 1994.

[2] David J. Benson, *Representations and Cohomology I*, Cambridge studies in advanced mathematics **30**, Cambridge Univ. Press, Cambridge 1991.

[3] David J. Benson, *Representations and Cohomology II*, Cambridge studies in advanced mathematics **31**, Cambridge Univ. Press, Cambridge 1991.

[4] David J. Benson, *Polynomial Invariants of Finite Groups*, Lond. Math. Soc. Lecture Note Ser. **190**, Cambridge Univ. Press, Cambridge 1993.

[5] Marie-José Bertin, *Anneaux d'invariants d'anneaux de polynomes, en caractéristique p*, Comptes Rendus Acad. Sci. Paris (Série A) **264** (1967), 653–656.

[6] H. E. A. Campbell, I. Hughes, R. D. Pollack, *Rings of Invariants and p-Sylow Subgroups*, Canad. Math. Bull. **34(1)** (1991), 42–47.

[7] H. E. A. Campbell, I. P. Hughes, G. Kemper, R. J. Shank, D. L. Wehlau, *Depth of Modular Invariant Rings*, preprint, Queen's University, Kingston, Ontario, 1997, submitted.

[8] H. E. A. Campbell, A. V. Geramita, I. P. Hughes, R. J. Shank, D. L. Wehlau, *Non-Cohen-Macaulay Vector Invariants and a Noether Bound for a Gorenstein Ring of Invariants*, Canad. Math. Bull. (to appear).

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

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

[11] M. Hochster, J. A. Eagon, *Cohen-Macaulay Rings, Invariant Theory, and the Generic Perfection of Determinantal Loci*, Amer. J. of Math. **93** (1971), 1020–1058.

[12] Victor Kac, Kei-Ichi Watanabe, *Finite Linear Groups whose Ring of Invariants is a Complete Intersection*, Bull. Amer. Math. Soc. **6** (1982), 221–223.

[13] Gregor Kemper, *Calculating Invariant Rings of Finite Groups over Arbitrary Fields*, J. Symbolic Computation **21** (1996), 351–366.

[14] Gregor Kemper, Gunter Malle, *Invariant Fields of Finite Irreducible Reflection Groups*, Preprint **97-26**, IWR, Heidelberg, 1997, submitted.

[15] Gregor Kemper, Allan Steel, *Some Algorithms in Invariant Theory of Finite Groups*, in: P. Dräxler, G.O. Michler, C. M. Ringel, eds., *Proceedings of the Euroconference on Computational Methods for Representations of Groups and Algebras*, Progress in Mathematics, Birkhäuser, Basel 1998 (to appear).

[16] Haruhisa Nakajima, *Invariants of Finite Abelian Groups Generated by Transvections*, Tokyo J. Math. **3** (1980), 201–214.

[17] Larry Smith, *Polynomial Invariants of Finite Groups*, A. K. Peters, Wellesley, Mass. 1995.

[18] Larry Smith, *Homological Codimension of Modular Rings of Invariants and the Koszul Complex*, Preprint, Toulouse, March 1997.

[19] Richard P. Stanley, *Invariants of Finite Groups and their Applications to Combinatorics*, Bull. Amer. Math. Soc. **1(3)** (1979), 475–511.

[20] Jacques Thévenaz, *G-Algebras and Modular Representation Theory*, Clarendon Press, Oxford 1995.