COHEN-MACAULAY MODULES OF COVARIANTS FOR CYCLIC-p-GROUPS

JONATHAN ELMER

Abstract. Let G be a a finite group, $\Bbbk$ a field of characteristic dividing $|G|$ and and V, W $\Bbbk G$-modules. Broer and Chuai [1] showed that if $\operatorname{codim}(V^G) \leq 2$ then the module of covariants $\Bbbk[V, W]^G = (\Bbbk[V] \otimes W)^G$ is a Cohen-Macaulay module, hence free over a homogeneous system of parameters for the invariant ring $\Bbbk[V]^G$.

In the present article we prove a general result which allows us to determine whether a set of elements of a free A-module M is a generating set, for any $\Bbbk$-algebra A. We use this result to find generating sets for all modules of covariants $\Bbbk[V, W]^G$ over a homogeneous system of parameters, where $\operatorname{codim}(V^G) \leq 2$ and G is a cyclic p-group.

1. Introduction

Let G be a finite group, $\Bbbk$ a field and let V, W be a pair of finite-dimensional $\Bbbk G$-modules. Then G-acts on the set $\Bbbk[V, W] = S(V^*) \otimes W$ of polynomial morphisms $V \to W$ via the formula

$$(g\phi)(v) = g\phi(g^{-1}v).$$

Morphisms fixed under the action of G are called *covariants*, and we denote the set of covariants by $\Bbbk[V, W]^G$. In the special case $W = \Bbbk$ we write $\Bbbk[V, \Bbbk] = \Bbbk[V]$ and the corresponding fixed points $\Bbbk[V]^G$ are called invariants. The set of invariants is a $\Bbbk$-algebra, and pointwise multiplication endows $\Bbbk[V, W]^G$ with the structure of a $\Bbbk[V]^G$-module.

Many theorems about invariant algebras have analogues for covariants which are less well-known. For example, suppose $\Bbbk$ has characteristic zero. Then it is well-known that $\Bbbk[V]^G$ is a polynomial ring if and only if G is generated by reflections (elements fixing a subspace of codimension 1 in V). It is less well-known that these conditions are equivalent to $\Bbbk[V, W]^G$ being a free module over $\Bbbk[V]^G$ for all W [3], [12]. Similarly, it is well-known that $\Bbbk[V]^G$ is always a Cohen-Macaulay algebra. It is less well-known that $\Bbbk[V, W]^G$ is always a Cohen-Macaulay module over $\Bbbk[V]^G$ [9].

In the modular case, much less is known about the structure of covariant modules. The following result is taken from [1]:

Proposition 1. *Let $\Bbbk$ be field whose characteristic divides $|G|$, where G is a finite group acting on vector spaces V, W.*

- *Suppose that $\operatorname{codim}(V^G) = 1$. Then $\Bbbk[V, W]^G$ is a free $\Bbbk[V]^G$-module.*
- *Suppose that $\operatorname{codim}(V^G) \leq 2$. Then $\Bbbk[V, W]^G$ is a Cohen-Macaulay $\Bbbk[V]^G$-module.*

In addition, Broer and Chuai give necessary and sufficient conditions for a set of covariants to generate $\Bbbk[V, W]^G$ freely over $\Bbbk[V]^G$.

Date: June 5, 2025.

2010 *Mathematics Subject Classification.* 13A50.

Key words and phrases. Invariant theory, module of covariants, free module, Cohen-Macaulay module.

Suppose $\Bbbk[V,W]^G$ is a Cohen-Macaulay $\Bbbk[V]^G$-module. This means that there exists a polynomial subalgebra $A \subseteq \Bbbk[V]^G$ (generated by a homogeneous system of parameters) over which $\Bbbk[V,W]^G$ is finitely generated and free.

The purpose of the present article is to give a method to test whether a set of covariants generates $\Bbbk[V,W]^G$ over A.. We obtain explicit sets of covariants generating $\Bbbk[V,W]^G$ freely over a homogeneous system of parameters when G is a cyclic p-group, $\operatorname{codim}(V^G) \leq 2$ and W is arbitrary. Note that in this case we have that $\Bbbk[V]^G$ itself is Cohen-Macaulay (apply Proposition 1 with W trivial). In fact, it follows from [6] and [8] that $\Bbbk[V]^G$ is Cohen-Macaulay *if and only if* $\operatorname{codim}(V^G) \leq 2$.

Suppose G is a cyclic group of order $q = p^k$. Recall the following concerning representation theory of G; there are exactly q isomorphism classes of indecomposable modules for G. The dimensions of these are $1, 2, 3, \ldots, q$, and we denote by V_r the unique indecomposable of dimension r. A generator σ of G acts on V_r by left-multiplication with a Jordan block of size r with eigenvalue 1. If $r \leq p^l$ for $l < k$ we have that σ^{p^l} acts trivially on V_r; thus, V_r is faithful only when $r > p^{k-1}$. The dimension of the fixed-point space V^G is one for any indecomposable V. As a consequence, we obtain:

Proposition 2. *Suppose V is a faithful representation of a cyclic group G of order p^k, and that $\operatorname{codim}(V^G) \leq 2$. Suppose in addition that V contains no trivial direct summands. Then one of the following hold:*

1. $|G| = p$ *and* $V \cong V_2$;
2. $|G| = p > 2$ *and* $V \cong V_3$;
3. $|G| = p$ *and* $V \cong V_2 \oplus V_2$.
4. $|G| = 4$ *and* $V \cong V_3$;

This paper is organised as follows: in the next section we will prove a very general result which allows us to test whether a set of elements of a free module is a basis (Proposition 4). In the third section we will show how modular covariants for cyclic groups can be viewed as the kernel of a certain homomorphism. This generalises [7, Proposition 4]. As an incidental result we show that the kernel of the relative transfer map $\operatorname{Tr}^G_H : \Bbbk[V]^H \to \Bbbk[V]^G$ can also be viewed as a module of covariants.

The last section gives explicit generating sets of covariants over a homogeneous system of parameters for the four cases explained above. In the first two cases, such generating sets were obtained in [7], but the proof here using Proposition 4 is shorter in the second case, as we can circumvent computation of the Hilbert series of $\Bbbk[V,W]^G$. The results in the third and fourth cases are new.

Acknowledgments. The author would like to thank an anonymous referee of [7] for the communication which inspired section 3 of this paper.

2. The s-invariant and freeness

Let $\Bbbk$ be a field and A a $\Bbbk$-algebra. Let M be a finitely-generated module over A. A set $g_1, g_2, \ldots, g_r$ of elements of M is called a *generating set* if $M = A(g_1, g_2, \ldots, g_r)$. It is said to be A-*independent* if we have

$$\sum_{i=1}^{r} a_i g_i = 0 \Rightarrow a_1 = a_2 = \ldots = a_r = 0 \text{ for all } a_1, a_2, \ldots, a_r \in A.$$

An A-independent, generating set for M is called a *basis* of M.

The most familiar setting is where $A = \Bbbk$. In that case M is a finite-dimensional vector space. It is then well known that M has a basis, and any maximal A-independent set, or minimal generating set for M is a basis. This may not be the case for modules over other algebras. A module which has a basis is called *free*, and one can show that every free module over A is isomorphic to A^r for some r.

Now suppose $A = \oplus_{i\geq 0} A_i$ is a graded $\Bbbk$-algebra with $A_0 = \Bbbk$. Let $M = \oplus_{i\geq 0} M_i$ be a graded A module. We have Hilbert series

$$H(A,t) = \sum_{i\geq 0} \dim(A_i) t^i,$$
$$H(M,t) = \sum_{i\geq 0} \dim(M_i) t^i.$$

Consider the quotient of these series, expanded about $t = 1$:

$$H(M,A;t) := \frac{H(M,t)}{H(A,t)} = a_0 + a_1(t-1) + \dots$$

If M is finitely generated, then by the Hilbert-Poincaré theorem we can write

$$H(M,t) = \frac{f(t)}{H(A,t)}$$

for some polynomial $f(t)$. In that case we have

$$a_0 = f(1) = r(M,A).$$

This is called the *rank* of M over A. If M has finite projective dimension (for example, if A is regular) it can be shown to equal the dimension of M as a vector space over $\mathrm{Quot}(A)$. We also have

$$a_1 = f'(1) = s(M,A).$$

This is called the *s-invariant* of M over A.

The following is an easy consequence of the definition of $H(M,A;t)$:

Proposition 3 ([1]). *Let A be a $\Bbbk$-algebra and $B \subset A$ a subalgebra of A over which A is finitely generated. Then we have*

(a)
$$r(M,B) = r(M,A)r(A,B);$$

(b)
$$s(M,B) = r(M,A)s(A,B) + r(A,B)s(M,A).$$

The next result is the main result of this section, and will be used frequently in the remainder of the article.

Proposition 4. *Let A be a regular, graded $\Bbbk$-module with $A_0 = \Bbbk$ and let M be a finite generated free graded module over A. Let $g_1, g_2, \dots, g_r$ be a A-independent set of elements of M, where $r = r(M,A)$. Then*

$$\sum_{i=1}^{r} \deg(g_i) \geq s(M,A)$$

with equality if and only if M is generated by $g_1, \dots, g_r$.

Proof. Let $f_1, f_2, \dots, f_r$ be a generating set of M. We may assume without loss of generality that

$$\deg(f_1) \leq \deg(f_2) \leq \dots \leq \deg(f_r)$$

and also

$$\deg(g_1) \leq \deg(g_2) \leq \dots \leq \deg(g_r).$$

As M is free, we have

$$\frac{H(M,t)}{H(A,t)} = \sum_{j=1}^{r} t^{\deg(f_j)}$$

and $s(M,A) = \sum_{j=1}^{r} \deg(f_j)$.

We claim that $\deg(g_j) \geq \deg(f_j)$ for all $j \leq r$. Suppose the contrary. Then for some $k \leq r-1$ we must have $\deg(g_{k+1}) < \deg(f_{k+1})$ and consequently

$$g_j \in A(f_1, \dots, f_k)$$

for all $j = 1, \dots, k+1$. Write $g_j = \sum_{i=1}^{k} a_{ij} f_i$. Let A be the $k \times (k+1)$ matrix with elements

$$(a_{ij} : i = 1, \dots, k, j = 1, \dots, k+1.)$$

We will prove by reverse induction on t that all $t \times t$ minors of A are zero. The initial case is $t = k$. Form the matrix A' by adding an extra row $\{g_1, \dots, g_{k+1}\}$. Now the matrix A' is

$$\begin{pmatrix} g_1 & g_2 & \cdots & g_{k+1} \\ a_{11} & a_{12} & \cdots & a_{1k+1} \\ \vdots & \vdots & & \vdots \\ a_{k1} & a_{k2} & \cdots & a_{kk+1} \end{pmatrix}$$

The determinant of this matrix is a A-linear combination of $f_1, \dots, f_k$, and the coefficent of f_i is

$$\det \begin{pmatrix} a_{i1} & a_{i2} & \cdots & a_{ik+1} \\ a_{11} & a_{12} & \cdots & a_{1k+1} \\ \vdots & \vdots & & \vdots \\ a_{k1} & a_{k2} & \cdots & a_{kk+1} \end{pmatrix}$$

which is zero because it has a repeated row. We thus obtain a relation

$$\sum_{j=1}^{k+1} (-1)^j g_j A_j = 0$$

where A_j is the $k \times k$ minor of A obtained by deleting the jth column. Since $g_1, g_2, \dots, g_{k+1}$ are linearly independent over A, we get that $A_j = 0$ as required.

Now suppose that all $(t+1) \times (t+1)$ minors of A are zero, where $t < k$. Consider a $t \times t$ submatrix

$$B := (a_{p_i q_j} : i, j = 1, \dots, t).$$

Pick any $q_{t+1} \in \{1, \dots, k+1\} \setminus \{q_1, q_2, \dots, q_t\}$ and consider the determinant of the matrix

$$B' := \begin{pmatrix} g_{q_1} & g_{q_2} & \cdots & g_{q_{t+1}} \\ a_{p_1 q_1} & a_{p_1 q_2} & \cdots & a_{p_1 q_{t+1}} \\ \vdots & \vdots & & \vdots \\ a_{p_t q_1} & a_{p_t q_2} & \cdots & a_{p_t q_{t+1}} \end{pmatrix}$$

This is again an A-linear combination of $f_1, \dots, f_k$, and the coefficient of f_i is

$$\det \begin{pmatrix} a_{i q_1} & a_{i q_2} & \cdots & a_{i q_{t+1}} \\ a_{p_1 q_1} & a_{p_1 q_2} & \cdots & a_{p_1 q_{t+1}} \\ \vdots & \vdots & & \vdots \\ a_{p_t q_1} & a_{p_t q_2} & \cdots & a_{p_t q_{t+1}}. \end{pmatrix}$$

If $i \not\in \{p_1, \dots, p_t\}$ then this is a $t+1 \times t+1$ minor of A, and zero by inductive hypothesis. Otherwise it is again zero, being the determinant of a matrix with a repeated row. We thus obtain

$$0 = \sum_{j=1}^{t+1} (-1)^j g_{q_j} B_j$$

where B_j is the $t \times t$ minor of B' obtained by removing the jth column. Since $g_{q_1}, \ldots, g_{q_t}$ are linearly independent we obtain $B_j = 0$ for all $j = 1, \ldots, t$, in particular,

$$\det(B) = B_t = 0.$$

This completes the induction. Taking $t = 1$, we see that $a_{ij} = 0$ for all $i = 1, \ldots, k$ and $j = 1, \ldots, k+1$. Therefore

$$g_1 = g_2 = \ldots g_{k+1} = 0$$

which contradicts linear independence.

This completes the proof of our claim, and we may conclude that $\sum_{j=1}^{r} \deg(g_j) \geq \sum_{j=1}^{r} \deg(f_j)$. Further, if $\sum_{j=1}^{r} \deg(g_j) = \sum_{j=1}^{r} \deg(f_j)$ then we must have $\deg(g_j) = \deg(f_j)$ for all $j = 1, \ldots, r$, and $A(g_1, g_2, \ldots, g_r)$ is a submodule of M with the same Hilbert series, and therefore $g_1, g_2, \ldots, g_r$ are free generators of M. On the other hand, if $\sum_{j=1}^{r} \deg(g_j) > \sum_{j=1}^{r} \deg(f_j)$ then $\deg(g_j) > \deg(f_j)$ for some j, and $A(g_1, g_2, \ldots, g_r)$ is a proper submodule of M. □

3. Characterising covariants

In this section we will show how modules of covariants can often be viewed as the kernel of a certain homomorphism. First, let G denote a finite group and $\Bbbk$ a field of arbitary characteristic. Let $H \leq G$. Suppose G acts on a $\Bbbk$-vector space V and let T be a left-transveral of H in G. We can assume $\iota \in T$ where ι is the identity element in G. Let $\{e_t : t \in T\}$ be a basis for the left permutation module $\Bbbk(G/H)$ on which H acts trivially. We define a map

$$\Theta : \Bbbk[V]^H \to \Bbbk[V] \otimes \Bbbk(G/H)$$
$$\Theta(f) = \sum_{t \in T} tf \otimes e_t.$$

where G acts diagonally on the tensor product.

Clearly Θ is an injective, degree-preserving homomorphsim of $\Bbbk[V]^G$ modules. Further we claim:

Proposition 5. *Θ induces an isomorphism of graded $\Bbbk[V]^G$-modules*

$$\Bbbk[V]^H \cong (\Bbbk[V] \otimes \Bbbk(G/H))^G.$$

Proof. We show first that if $f \in \Bbbk[V]^H$ then $\Theta(f) \in (\Bbbk[V] \otimes \Bbbk(G/H))^G$. Let $g \in G$, then we have

$$g \cdot \Theta(f) = \sum_{t \in T} gtf \otimes ge_t.$$

Write $gt = \sigma_g(t)h_g$, where $\sigma_g(t) \in T$ and $h_g \in H$, noting that σ_g is a permutation of T. Then since $f \in \Bbbk[V]^H$ and H acts trivially on $\Bbbk(G/H)$ we have

$$\sum_{t \in T} gtf \otimes ge_t = \sum_{t \in T} \sigma_g(t)h_g f \otimes h_g e_{\sigma_g(t)} = \sum_{t \in T} \sigma_g(t) f \otimes e_{\sigma_g(t)} = \Theta(f)$$

as required

Now we need only show that Θ is surjective. Let

$$f = \sum_{t \in T}^{r} f_t \otimes e_t \in (\Bbbk[V] \otimes \Bbbk(G/H))^G$$

where $f_t \in \Bbbk[V]$. Again for any $g \in G$ write $gt = \sigma_g(t)h_g$. Thus since $f = gf$ we have

$$f = \sum_{t \in T} gf_t \otimes e_{\sigma_g(t)} = \sum_{t \in T} f_t \otimes e_t.$$

Equating coefficients of e_t shows that

$$gf_t = f_{\sigma_g(t)}$$

for any $g \in G$ and $t \in T$. In particular, if $t \in T$ then the permutation σ_t satisfies $\sigma_t(\iota) = t$. Thus for any $t \in T$ we have

$$tf_\iota = f_t$$

and hence

$$f = \sum_{t \in T}^{r} f_t \otimes e_t = \sum_{t \in T} tf_\iota \otimes e_t = \Theta(f_\iota)$$

which shows that Θ is surjective as required. □

Now let M be a submodule of $\Bbbk(G/H)$. Tensor the short exact sequence

$$0 \to M \xrightarrow{i} \Bbbk(G/H) \xrightarrow{j} N \to 0,$$

where $N = \ker(i)$ with $\Bbbk[V]$ and take G-invariants. This induces a long exact sequence

$$0 \to (\Bbbk[V] \otimes M)^G \to (\Bbbk[V] \otimes \Bbbk(G/H))^G \to (\Bbbk[V] \otimes N)^G \to H^1(G, \Bbbk[V] \otimes M) \to \dots$$

By composing the isomorphism Θ with the second nontrivial map in this sequence, we obtain a graded $\Bbbk[V]^G$ homomorphism

$$\phi : \Bbbk[V]^H \to (\Bbbk[V] \otimes N)^G$$

whose kernel is isomorphic to the module of covariants $(\Bbbk[V] \otimes M)^G = \Bbbk[V, M]^G$.

We will consider two special cases of the above: first, suppose $M = M_{G/H} = \langle e_t - e_\iota : t \in T \rangle_\Bbbk$. Then N is a one-dimensional module on which G acts trivially and the map j sends each e_t to its basis element, which we will denote by e. The induced map in the long exact sequence sends an expression

$$\sum_{t \in T} f_t \otimes e_t$$

to

$$\sum_{t \in T} f_t \otimes e.$$

Thus, the composition with Θ sends an element $f \in \Bbbk[V]^H$ to $\sum_{t \in T} tf$ - in other words, this is the *relative transfer map* $\mathrm{Tr}^G_H : \Bbbk[V]^H \to \Bbbk[V]^G$. It follows that the kernel of the relative transfer map is isomorphic, as a graded $\Bbbk[V]^G$-module, to the module of covariants $\Bbbk[V, M_{G/H}]^G$. This is interesting, but we will not pursue it further in the present article. We note for future use that the (relative) transfer map is a useful way of producing invariants. Along similar lines, one has a *relative norm map* $N^G_H : \Bbbk[V]^H \to \Bbbk[V]^G$ defined by

$$N^G_H(f) = \prod_{t \in T} tf.$$

Now suppose G is cyclic of order $q = p^r$, $\Bbbk$ is a field of characteristic p and H is trivial. Let g be a generator of G and set $\Delta := g - \iota \in \Bbbk G$. For each $1 \leq n < q$ there is a submodule $\ker(\Delta^n)$ of $\Bbbk G$ isomorphic to V_n. The image of Δ^n is a submodule isomorphic to V_{q-n}.

Let M and N denote the kernel and image of Δ^n respectively. Then the canonical short exact sequence induces a long exact sequence

$$0 \to (\Bbbk[V] \otimes M)^G \to (\Bbbk[V] \otimes \Bbbk(G))^G \xrightarrow{\psi} (\Bbbk[V] \otimes N)^G \to H^1(G, \Bbbk[V] \otimes M) \to \dots$$

Consider the composition

$$\Bbbk[V] \xrightarrow{\Theta} (\Bbbk[V] \otimes \Bbbk G)^G \xrightarrow{\psi} (\Bbbk[V] \otimes N)^G \xrightarrow{k} (\Bbbk[V] \otimes \Bbbk G)^G \xrightarrow{\Theta^{-1}} \Bbbk[V]$$

Here k is the canonical inclusion. Choose a basis $\{e_i : i = 0, \dots q-1\}$ for $\Bbbk G$ with $ge_i = e_{i+1}$ for $i < q$ and $ge_{q-1} = e_0$. For $n = 1$, the composition $k\psi$ sends an element

$$\sum_{i=0}^{q-1} f_i \otimes e_i$$

to

$$\sum_{i=0}^{q-1} f_i \otimes (e_{i+1} - e_i) = \sum_{i=0}^{q-1} (f_{i-1} - f_i) \otimes e_i$$

with indices understood modulo q. Thus the composition $k\psi\Theta$ sends $f \in \Bbbk[V]$ to

$$\sum_{i=0}^{q-1} (g^{i-1} f - g^i f) \otimes e_i.$$

Composing this with Θ^{-1} then picks out the coefficient of e_0, which is

$$g^{-1} f - f.$$

Thus, the composition is action by $g^{-1} - \iota \in \Bbbk G$. An easy inductive argument shows that for arbitrary n, the composition is action by $(g^{-1} - \iota)^n \in \Bbbk G$. Since Θ is an isomorphism and k is injective, the kernel of this map (which is the same as the kernel of Δ^n) can be identified with the kernel of ψ, which in turn is isomorphic to $\Bbbk[V, M]^G$. Thus, we obtain a degree-preserving isomorphism of $\Bbbk[V]^G$ modules

$$\Xi : \ker(\Delta^n) \cong \Bbbk[V, V_n]^G.$$

Note that a version of this isomorphism was used in [7] for G a cyclic group of prime order. As noted there, if we choose a basis $\{w_1, w-2, \dots, w_n\}$ of V_n such that

$$\begin{aligned}
\sigma w_1 &= w_1 \\
\sigma w_2 &= w_2 - w_1 \\
\sigma w_3 &= w_2 - w_2 + w_1 \\
&\vdots \\
\sigma w_n &= w_n - w_{n-1} + w_{n-2} - \dots \pm w_1.
\end{aligned}$$

then Ξ is given by the particularly convenient formula

$$\Xi(f) = \sum_{i=0}^{n} \Delta^i(f) w_i.$$

4. Main results

From now on let $G = \langle \sigma \rangle$ be a cyclic group of order $q = p^k$, let $\Bbbk$ be a field of characteristic p and let V and W be finite-dimensional $\Bbbk G$-modules.

The operator $\Delta = \sigma - \iota \in \Bbbk G$ will play a major role in our exposition, so we begin with some general results, following [7] quite closely. Notice that, for $\phi \in \Bbbk[V, W]^G$ we have

$$\Delta(\phi) = 0 \Rightarrow \sigma \cdot \phi = \phi$$

and thus by induction $\sigma^k \phi = \phi$ for all k. So $\Delta(\phi) = 0$ if and only if $\phi \in \Bbbk[V, W]^G$. Similarly for $f \in \Bbbk[V]$ we have $\Delta(f) = 0$ if and only if $f \in \Bbbk[V]^G$.

Δ is a *σ-twisted derivation* on $\Bbbk[V]$; that is, it satisfies the formula

$$\Delta(fg) = f\Delta(g) + \Delta(f)\sigma(g) \tag{1}$$

for all $f, g \in \Bbbk[V]$.

Further, using induction and the fact that σ and Δ commute, one can show Δ satisfies a Leibniz-type rule

$$\Delta^k(fg) = \sum_{i=0}^{k} \binom{k}{i} \Delta^i(f)\sigma^{k-i}(\Delta^{k-i}(g)). \tag{2}$$

A further result, which can be deduced from the above and proved by induction is the rule for differentiating powers:

$$\Delta(f^k) = \Delta(f) \left(\sum_{i=0}^{k-1} f^i \sigma(f)^{k-1-i} \right) \tag{3}$$

for any $k \geq 1$.

For any $f \in \Bbbk[V]$ we define the **weight** of f:

$$\mathrm{wt}(f) = \min\{i > 0 : \Delta^i(f) = 0\}.$$

Notice that $\Delta^{\mathrm{wt}(f)-1}(f) \in \ker(\Delta) = \Bbbk[V]^G$ for all $f \in \Bbbk[V]$. Another consequence of (2) is the following: let $f, g \in \Bbbk[V]$ and set $d = \mathrm{wt}(f), e = \mathrm{wt}(g)$. Suppose that

$$d + e - 1 \leq p.$$

Then

$$\Delta^{d+e-1}(fg) = \sum_{i=0}^{d+e-1} \binom{d+e-1}{i} \Delta^i(f)\sigma^{d+e-1-i}(\Delta^{d+e-1-i}(g)) = 0$$

since if $i < e$ then $d + e - 1 - i > d - 1$. On the other hand

$$\begin{aligned} \Delta^{d+e-2}(fg) &= \sum_{i=0}^{d+e-2} \binom{d+e-2}{i} \Delta^i(f)\sigma^{d+e-2-i}(\Delta^{d+e-2-i}(g)) \\ &= \binom{d+e-2}{i} \Delta^{d-1}(f)\sigma^{e-1}(\Delta^{e-1}(g)) \neq 0 \end{aligned}$$

since $\binom{d+e-2}{i} \neq 0 \mod p$. We obtain the followng:

Proposition 6. *Let $f, g \in \Bbbk[V]$ with $\mathrm{wt}(f) + \mathrm{wt}(g) - 1 \leq p$. Then $\mathrm{wt}(fg) = \mathrm{wt}(f) + \mathrm{wt}(g) - 1$.*

Also note that

$$\Delta^q = \sigma^q - 1 = 0$$

which shows that $\mathrm{wt}(f) \leq q$ for all $f \in \Bbbk[V]^G$. Finally notice that

$$\Delta^{q-1} = \sum_{i=0}^{q-1} \sigma^i \tag{4}$$

which shows that $\Delta^{q-1}(f) = \mathrm{Tr}^G(f)$ for all $f \in \Bbbk[V]$.

Now we assume that $\mathrm{codim}(V^G) \leq 2$, so V is isomorphic to one of the modules listed in Proposition 2. Our goal is to find, for arbitrary indecomposable $W \cong V_n$, an explicit set of covariants generating $\Bbbk[V, W]^G$ freely over A, where A is a homogeneous system of parameters for $\Bbbk[V]^G$. Our strategy is to find in each case an A-independent set of $r(K_n, A)$ elements of $K_n := \ker(\Delta^n)$ whose degree sum equals $s(K_n, A)$. That such a set generates K_n freely over A follows from Proposition 4, and the results of Section 3 imply that applying Ξ to each element in the set yields a free generating set for $\Bbbk[V, W]^G$ over A.

Broer and Chuai studied the s-invariant for modules of covariants over $\Bbbk[V]^G$ for arbitrary G. In particular they proved:

Proposition 7. *Suppose G is a finite group and let H be the subgroup of G generated by all pseudo-reflections (i.e. elements stabilising a subspace of V with codimension 1). Then $s(\Bbbk[V, W]^G, \Bbbk[V]^G) = s(\Bbbk[V, W]^H, \Bbbk[V]^H)$. In particular if G contains no pseudo-reflections, then $s(\Bbbk[V, W]^G, \Bbbk[V]^G) = 0$.*

This makes computation of $(\Bbbk[V, W]^G, A)$ using Proposition 3 quite easy when G is a cyclic p-group containing no pseudo-reflections. This holds when $V = V_3$ and $p > 2$ or $V = V_2 \oplus V_2$. The only cases remaining in which the ring of invariants is Cohen-Macaulay are $V = V_2$ and $V = V_3, p = 2$. In the former case our methods do not yield any substantial improvement, so we will simply quote the results from [7] for the sake of completeness:

Proposition 8. *Let $p \geq n$, $V = V_2$ and $K_n = \ker(\Delta^n)$. K_n is a free $\Bbbk[V^G]$-module, generated by $\{x_1^k : k = 0, \dots, n-1\}$.*

Corollary 9. *Let $p \geq n$, $W = V_n$ and $V = V_2$. The module of covariants $\Bbbk[V, W]^G$ is generated freely over $\Bbbk[V]^G$ by*

$$\{\Xi(x_1^k) : k = 0, \dots, n-1\}.$$

The case $V = V_3$, $p = 2$ will be dealt with in the final subsection. If $V = V_3$ and $p > 2$ or $V = V_2 \oplus V_2$ then we have the following:

Lemma 10. *Let $p \geq n$ and let $W = V_n$. Let $A \subseteq \Bbbk[V]^G$ be a subalgebra generated by a homogeneous system of parameters. Then $\Bbbk[V, W]^G$ is a free A-module and*

$$r(\Bbbk[V, W]^G, A) = r(\Bbbk[V]^G, A)n;$$
$$s(\Bbbk[V, W]^G, A) = s(\Bbbk[V]^G, A)n.$$

Proof. The first result follows from Proposition 3; the second from the same, Proposition 7 and the fact that V contains no pseudo-reflections. □

Note that an application of Ξ now shows that

$$r(K_n, A) = r(\Bbbk[V]^G, A)n;$$
$$s(K_n, A) = s(\Bbbk[V]^G, A)n.$$

We now consider these cases separately in detail.

4.1. $V = V_3, p > 2$. In this subsection let $V = V_3$, $W = V_n$ and p an odd prime. Then G is cyclic of order p. Choose a basis v_1, v_2, v_3 of V so that

$$\sigma x_1 = x_1 + x_2$$
$$\sigma x_2 = x_2 + x_3$$
$$\sigma x_3 = x_3$$

where x_1, x_2, x_3 is the corresponding dual basis.

We begin by describing $\Bbbk[V]^G$. This has been done in several places before, for example [5] and [10, Theorem 5.8], but we will follow [7]. We use a graded lexicographic order on monomials $\Bbbk[V]$ with $x_1 > x_2 > x_3$. Here and in the next two subsections, if $f \in \Bbbk[V]$ then the *lead term* of f is the term with the largest monomial in our order and the *lead monomial* is the corresponding monomial.

It is easily shown that

$$\begin{aligned} a_1 &:= x_3, \\ a_2 &:= x_2^2 - 2x_1x_3 - x_2x_3, \\ a_3 &:= N^G(x_1) = \prod_{i=0}^{p-1} \sigma^i(x_1) \end{aligned}$$

are invariants, and looking at their lead terms tells us that they form a homogeneous system of parameters for $\Bbbk[V]^G$, with degrees $1, 2$ and p.

Proposition 11. *Let $f \in \Bbbk[V]^G$ be any invariant with lead term x_2^p. Let $A = \Bbbk[a_1, a_2, a_3]$. Then $\Bbbk[V]^G$ is a free A-module, whose generators are 1 and f.*

Proof. See [7, Proposition 12] □

The obvious choice of invariant with lead term x_2^p is $N^G(x_2)$. The following observations are consequences of the generating set above.

Lemma 12. *Let $f \in A$. Then the lead term of f is of the form $x_1^{pi}x_2^{2j}x_3^k$ for some positive integers i, j, k.*

Lemma 13. *We have $r(\Bbbk[V]^G, A) = 2$ and $s(\Bbbk[V]^G, A) = p$.*

Corollary 14. *We have $r(\Bbbk[V, W]^G, A) = 2n$ and $s(\Bbbk[V, W]^G, A) = np$.*

Proof. This follows immediately from Lemma 13 and Lemma 10. □

For the rest of this section, we set $l = \frac{1}{2}n$ if n is even, with $l = \frac{1}{2}(n-1)$ if n is odd. Next, we need some information about the lead monomials of certain polynomials. The following pair of lemmas were proved in [7]:

Lemma 15. *Let $j \le k < p$. Then $\Delta^j(x_1^k)$ has lead term*

$$\frac{k!}{(k-j)!}x_1^{k-j}x_2^j.$$

Lemma 16. *Let $j \le k < p$. Then $\Delta^j(x_1^k x_2)$ has lead term*

$$\frac{k!}{(k-j)!}x_1^{k-j}x_2^{j+1}.$$

We are now ready to state our main results. Let $V = V_3$ and $W = V_n$. For any $i = 0, 1, \ldots, n-1$ we define monomials

$$M_i = \begin{cases} x_1^{i/2} & \text{if } i \text{ is even,} \\ x_1^{(i-1)/2}x_2 & \text{if } i \text{ is odd.} \end{cases}$$

and polynomials

$$P_i = \begin{cases} \Delta(x_1^{p-i/2}) & \text{if } i \text{ is even, } i > 0, \\ x_1^{p-(i+1)/2} & \text{if } i \text{ is odd.} \end{cases}$$

with $P_0 = x_1^{p-1}x_2$.

Theorem 17. *Let $n \le p$. Then K_n is a free A-module, generated by*

$$S_n = \{M_0, M_1, \ldots, M_{n-1}, \Delta^{p-n}(P_0), \Delta^{p-n}(P_1), \ldots, \Delta^{p-n}(P_{n-1})\}.$$

Proof. By Lemma 6, the weight of M_i is $i+1$ for $i < p$, while the weight of P_i is

$$\begin{cases} p & i \text{ odd or zero} \\ p-1 & i \text{ even, } i > 0. \end{cases}$$

Therefore the given polynomials all lie in K_n. Further, the degree of M_i is $\lceil \frac{i}{2} \rceil$ and the degree of P_i is $p - \lceil \frac{i}{2} \rceil$, so the sum of the degrees of the elements of K_n

is $np = s(K_n, A)$. Therefore by Proposition 4 it is enough to prove that S_n is A-independent.

Applying Lemmas 15 and 16, the lead monomials of S_n are

$$\{1, x_2, x_1, x_1x_2, \ldots, x_1^{l-1}x_2, x_1^l,$$
$$x_1^{n-l-1}x_2^{p-n+1}, x_1^{n-l}x_2^{p-n}, \ldots, x_1^{n-2}x_2^{p-n+1}, x_1^{n-1}x_2^{p-n}, x_1^{n-1}x_2^{p-n+1}\}$$

if n is odd, and

$$\{1, x_2, x_1, x_1x_2, \ldots, x_1^{l-2}x_2, x_1^{l-1}, x_1^{l-1}x_2,$$
$$x_1^{n-l}x_2^{p-n}, x_1^{n-l}x_2^{p-n+1}, x_1^{n-l+1}x_2^{p-n} \ldots, x_1^{n-2}x_2^{p-n+1}, x_1^{n-1}x_2^{p-n}, x_1^{n-1}x_2^{p-n+1}\}$$

if n is even.

In either case, we note that none of the claimed generators have lead term divisible by x_3, that each has x_1-degree $< p$, that there are at most two elements in S_n with the same x_1-degree, and that when this happens these elements have x_2-degrees differing by 1. Combined with Lemma 12, we see that for every possible choice of $f \in A$ and $g \in S_n$, the lead monomial of fg is different. Therefore there cannot be any A-linear relations between the elements of S_n. □

4.2. $V_2 \oplus V_2$**.** In this subsection let $V \cong V_2 \oplus V_2$. Choose a basis v_1, v_2, v_3, v_4 of V so that the action on the corresponding dual basis x_1, x_2, x_3, x_4 is given by

$$\begin{aligned}\sigma x_1 &= x_1 + x_3;\\ \sigma x_2 &= x_2 + x_4;\\ \sigma x_3 &= x_3;\\ \sigma x_4 &= x_4.\end{aligned}$$

It is easy to see that $\{N^G(x_1) = x_1^p - x_1x_3^{p-1}, N^G(x_2) = x_2^p - x_2x_4^{p-1}, x_3, x_4\}$ is a homogeneous system of parameters. We also see easily that $u := x_1x_4 - x_2x_3$ is invariant, and does not belong to the algebra A spanned by the given system of parameters. Campbell and Hughes [2, Proposition 2.1] showed that $\{1, u, \ldots, u^{p-1}\}$ generate $\Bbbk[V]^G$ as a free A-module. Therefore

$$s(\Bbbk[V]^G, A) = \sum_{i=0}^{p-1} 2i = p(p-1). \tag{5}$$

Noting that G contains no pseudo-reflections, we obtain the following:

Lemma 18. *We have $r(K_n, A) = np$ and $s(K_n, A) = np(p-1)$.*

Proof. This follows from Equations (6) and (5) above and Proposition 3. □

We use a graded lexicographical order on monomials with $x_1 > x_2 > x_3 > x_4$. An easy inductive argument establishes the following:

Lemma 19. *The lead term of $\Delta^k(x_1^ix_2^j)$ is:*

$$\begin{cases} \frac{j!}{(j-k)!}x_1^ix_2^{j-k}x_4^k & k \le j \\ \frac{i!j!}{(i-j-k)!}x_1^{i-k}x_3^{k-j}x_4^j & j < k \le i+j. \end{cases}$$

Corollary 20. *Let $0 \le i, j < p$. The weight of $x_1^ix_2^jx_3^kx_4^k$ is $\min(i+j+1, p)$.*

We now define, for $k \ge 0$,

$$M_k := \{x_1^ix_2^j : i+j = k, i < p, j < p\}.$$

We use the notation

$$fM_k := \{fm : m \in M_k\}$$

for any $f \in \Bbbk[V]$ and

$$\Delta^r M_k := \{\Delta^r(m) : m \in M_k\}$$

for any $r \geq 0$.

We are now able to state the main result of this subsection:

Theorem 21. *Let $n \leq p$. The Kernel K_n of $\Delta^n : \Bbbk[V] \to \Bbbk[V]$ is a free A-module generated by the set $S := M \cup U \cup D$ where*

$$\begin{aligned} M &= \bigcup_{k=0}^{n-1} M_k; \\ U &= \bigcup_{k=1}^{p-n} u^k M_{n-1}; \\ D &= \bigcup_{k=2p-n}^{2p-2} \Delta^{p-n} M_k. \end{aligned}$$

Proof. The A-isomorphism $K_n \cong \Bbbk[V,W]^G$ shows that K_n is free, and $r(K_n, A) = np$, and $s(K_n, A) = np(p-1)$. The elements of M_k for $k \leq n-1$ have weight $k+1$, so the weight of each element of M is at most n. Since $u \in \Bbbk[V]^G$, the weight of each element of U is n. If $k \geq 2p-n$ then $k \geq p$, so in that case the weight of each element of M_k is p. It follows that the weight of each element of D is n. The shows that the proposed generators all lie in K_n. Now by Proposition 4 it is enough to show that the given set is A-independent, has np elements, and degree sum $np(p-1)$.

Viewed as a polynomial in x_1, x_2 with coefficients in $\Bbbk[x_3, x_4]$, the monomials in M_k each have total degree k. Therefore the elements of M have total degree at most $n-1$. Further, each monomial in M_k has a distinct x_1, x_2 bidegree. So the elements of M have distinct bidegrees.

Meanwhile, the elements of $u^k M_{n-1}$ have total degree (in x_1, x_2) $k+n-1$. Therefore the total degrees of the elements of U lie between n and $p-1$ inclusive. Further, each element of $u^k M_{n-1}$ has distinct bidegree. So the bidegrees of the elements of U are distinct from each other and also from all elements of M.

Let $m := x_1^i x_2^j \in M_k$ with $k \geq 2p-n$. Then $p-n \leq k-p = i+j-p < j$, so by Lemma 19, the lead term of $\Delta^{p-n}(m)$ is

$$\frac{j!}{(j-p+n)!} x_1^i x_2^{j-p+n} x_4^{p-n}.$$

In particular, its total degree in x_1, x_2 is $i+j-p+n = k-p+n \geq p$. So the elements of D have bidegree $\geq p$. Further, the bidegrees of the elements of $\Delta^{p-n} M_k$ are distinct from one another. We have shown that the bidegrees of the elements of S are all distinct from one another.

Multiplying an element of $\Bbbk[V]$ by an element of A preserves its x_1- and x_2-degree modulo p. Since each element of S has x_1- and x_2- degree $< p$, and distinct x_1, x_2-bidegree, it follows that there is no A-linear relation between the elements of S. So S is A-independent as required.

It remains to check the size and degree sum of S. The number of elements in M_k is $k+1$ if $k<p$, and $2p-k-1$ otherwise. Thus

$$\begin{aligned}
|S| &= |M| + |U| + |D| \\
&= \sum_{k=0}^{n-1}(k+1) + n(p-n) + \sum_{k=2p-n}^{2p-2}(2p-1-k) \\
&= \frac{1}{2}n(n+1) + n(p-n) + (2p-1)(n-1) - \frac{1}{2}(n-1)(4p-n-2) \\
&= \frac{1}{2}n(n+1) + n(p-n) + \frac{1}{2}n(n-1) \\
&= \frac{1}{2}n\cdot(2n) + np - n^2 \\
&= np
\end{aligned}$$

as required.

Finally, the degree of each element of M_k is k, the degree of each element of $u^k M_{n-1}$ is $2k+n-1$ and the degree of each element of $\Delta^{p-n}M_k$ is also k. We note the identity

$$\sum_{k=0}^{n} k(k+1) = \frac{1}{3}n(n+1)(n+2).$$

Therefore the degree sum of M is

$$\begin{aligned}
\sum_{k=0}^{n-1} k(k+1) &= \frac{1}{3}(n-1)n(n+1) \\
&= \frac{1}{3}(n^3-n).
\end{aligned}$$

The degree sum of U is

$$\begin{aligned}
\sum_{k=1}^{p-n}(2k+n-1)n &= 2n\sum_{k=1}^{p-n} k + (p-n)(n-1)n \\
&= n(p-n)(p-n+1) + n(p-n)(n-1) \\
&= np^2 - n^2 p.
\end{aligned}$$

And the degree sum of D is

$$\begin{aligned}
&\sum_{k=2p-n}^{2p-2} k(2p-1-k)\\
&= 2p\sum_{k=2p-n}^{2p-2} k - \sum_{k=2p-n}^{2p-2} k(k+1)\\
&= p(4p-2-n)(n-1) - \frac{1}{3}(2p-2)(2p-1)(2p) + \frac{1}{3}(2p-n-1)(2p-n)(2p-n+1)\\
&= p(4p-2-n)(n-1) - \frac{1}{3}(2p-2)(2p-1)(2p)\\
&\qquad + \frac{1}{3}(2p-2-(n-1))(2p-1-(n-1))(2p-(n-1))\\
&= p(4p-2-n)(n-1) - \frac{1}{3}\left((6p-3)(n-1)^2 - (12p^2-12p+2)(n-1) - (n-1)^3\right)\\
&= (n-1)\left(p(4p-2-n + \frac{1}{3}(6p-3(n-1) - 12p^2 + 12p - 2 - (n-1)^2))\right)\\
&= (n-1)(pn - \frac{1}{3}n - \frac{1}{3}n^2)\\
&= n^2p - np - \frac{1}{3}(n^3-n).
\end{aligned}$$

So the degree sum of S is

$$\begin{aligned}
\frac{1}{3}(n^3-n) + np^2 - n^2p = n^2p - np - \frac{1}{3}(n^3-n)\\
= np(p-1)
\end{aligned}$$

as required. This completes the proof. □

4.3. $V_3, p = 2$. . In this section we consider the representation $V = V_3$ of $C_4 = \langle\sigma\rangle$ over a field of characteristic two. Shank and Wehlau [11] studied the modular invariant rings $\Bbbk[V_{p+1}]^G$ where $G = C_{p^2}$, of which this is particularly simple example. They showed that the invariants were generated by the norms of the variables, and relative transfers from the unique proper subgroup of G. For our purposes we need not a fundamental generating set, but rather primary and secondary invariants. We proceed as follows: Let v_1, v_2, v_3 be a basis of V such that the action of σ on the dual basis $\{x_1, x_2, x_3\}$is given by

$$\begin{aligned}
\sigma x_1 &= x_1 + x_2\\
\sigma x_2 &= x_2 + x_3\\
\sigma x_3 &= x_3.
\end{aligned}$$

Once more we use a graded lexicographic order with $x_1 > x_2 > x_3$. We set $H = \langle\sigma^2\rangle$. Note that the action of H is given by

$$\begin{aligned}
\sigma^2 x_1 &= x_1 + x_3\\
\sigma^2 x_2 &= x_2\\
\sigma^2 x_3 &= x_3.
\end{aligned}$$

It is easy to see that $\{N^G(x_1), N^G_H(x_2), x_3\}$ form a homogeneous system of parameters. Since $\dim(V^G) = 1$, $\Bbbk[V]^G$ is a Cohen-Macaulay ring, hence a free module over the subalgebra $A = \Bbbk[N^G(x_1), N_H^G(x_2), x_3]$. Now by [4, Theorem 3.71] we have

$$r(\Bbbk[V]^G, A) = \frac{8}{|G|} = 2 \tag{6}$$

as the degree product of the generators of A is 8.

A direct computation establishes that $N_H^G(x_2)$ and x_3^2 are the only invariants of degree two. Further it is easily shown that

$$u := x_1^2 x_3 + x_1 x_3^2 + x_2^3 + x_2^2 x_3 \in \Bbbk[V]^G,$$

and a lead term argument shows that $u \notin A$. It must follow therefore that $\{1, u\}$ generates $\Bbbk[V]^G$ freely over A. In particular $s(\Bbbk[V]^G, A) = 3$.

Now by Proposition 3, we get

$$r(K_n, A) = 2n,$$

and

$$s(K_n, A) = 3n + 2s(\Bbbk[V, V_n]^H, \Bbbk[V]^H),$$

the latter because H is the subgroup of G generated by pseudo-reflections.

We consider each value of $n = 2, 3, 4$ separately. We note that $\Delta^2 = \sigma^2 - \iota$, so $K_2 = \Bbbk[V]^H = \Bbbk[N^H(x_1), x_2, x_3]$. However, we seek generators of K_2 as an A-module. Our first result is:

Proposition 22. *The set $S = \{1, x_2, N^H(x_1), x_2 N^H(x_1)\}$ generates K_2 over A.*

Proof. We will need to compute $s(\Bbbk[V, V_2]^H, \Bbbk[V]^H)$. Observe that, since H acts trivially on V_2, we may write

$$\Bbbk[V, V_2]^H = \Bbbk[V]^H \otimes V_2.$$

If $\{w_1, w_2\}$ is a basis of V_2, then $\Bbbk[V, V_2]^H$ is generated over $\Bbbk[V]^H$ by w_1 and w_2, both having degree zero. So $s(\Bbbk[V, V_2]^H, \Bbbk[V]^H) = 0$ and therefore $s(K_2, A) = 6$.

Now it is clear that every element of S lies in $K_2 = \Bbbk[V]^H$. Further, $|S| = 4$ and the degree sum of S is 6. It remains to show that S is A-independent. This is easy to see: the lead terms of S are $1, x_2, x_1^2$ and $x_1^2 x_2$ and every element of A has lead term $x_1^{4a} x_2^{2b} x_3$, so the lead terms of any different pair of elements of the form fg where $f \in A$, $g \in S$ are distinct. ☐

Proposition 23. *The set $S = \{1, x_1, x_2, x_1^2, \Delta(x_1^3), \Delta(x_1^3 x_2).\}$ generates K_3 over A.*

Proof. We will need to compute $s(\Bbbk[V, V_3]^H, \Bbbk[V]^H)$. Choose a basis $\{w_1, w_2, w_3\}$ of (the second copy of) V_3 such that

$$\sigma^2 w_1 = w_1 + w_3$$
$$\sigma^2 w_2 = w_2$$
$$\sigma^2 w_3 = w_3.$$

Then we may write

$$\Bbbk[V, V_3]^H = (S(V^*) \otimes V_3)^H = w_2 \otimes \Bbbk[V]^H \oplus (S(V^*) \otimes W)^H$$

where $W = \langle w_1, w_3 \rangle$. The first direct summand is generated by w_2 over $\Bbbk[V]^H$, with degree zero. The second is isomorphic to $\ker((\sigma^2 - 1)^2) = \Bbbk[V]$, which is generated over $\Bbbk[V]^H = \Bbbk[N^H(x_1), x_2, x_3]$ by x_1. Therefore

$$s(\Bbbk[V, V_3]^H, \Bbbk[V]^H) = 1.$$

Consequently we get that $s(\Bbbk[V, V_3]^G, \Bbbk[V]^G) = 11$.

Now an easy direct calculation shows that every element of S lies in K_3 (for the last two simply note that $\Delta^4 = 0$). We have $|S| = 6$ and the degree sum of S is 11. Further, the lead terms of S are

$$\{1, x_1, x_2, x_1^2, x_1^2 x_2, x_1^2, x_1^3 x_3\}$$

and so once more every for different pair of elements of the form fg where $f \in A$ and $g \in S$, the lead terms are distinct. $\square$

Proposition 24. *The set* $S = \{1, x_1, x_2, x_1^2, x_1 x_2, x_1^3, x_1^2 x_2, x_1^3 x_2\}$ *generates* K_4 *over* A.

Proof. We have $K_4 = \Bbbk[V]$ so obviously each element of S lies in K_4, and the proof of A-independence is similar to the previous result. To prove S is a generating set we could proceed as before, where we would find that $s(\Bbbk[V, V_4]^H, \Bbbk[V]^H) = 2$ and hence $s(\Bbbk[V, V_4]^G, \Bbbk[V]^G) = 16$. However it is probably simpler to argue as follows: let $f \in \Bbbk[V]$ and assume $f \notin SA$ with minimal degree in x_1. By long division with $N^G(x_1)$ we may assume the x_1-degree of f is at most three. Thus we may write

$$f = g_0 + g_1 x_1 + g_2 x_1^2 + g_3 x_1^3,$$

with $g_i \in \Bbbk[x_2, x_3]$. Now assume that among all such examples, g_3 has minimal x_2-degree; by long division with $N_H^G(x_2)$ we may assume this x_2-degree is at most one. Treating each $g_i = 2, 1, 0$ in turn in the same manner, we see that $f \in SA$ after all, a contradiction. $\square$

References

[1] Abraham Broer and Jianjun Chuai. Modules of covariants in modular invariant theory. *Proc. Lond. Math. Soc. (3)*, 100(3):705–735, 2010.

[2] H. E. A. Campbell and I. P. Hughes. 2-dimensional vector invariants of parabolic subgroups of $\mathrm{Gl}_2(\mathbf{F}_p)$ over the field $\mathbf{F}_p$. *J. Pure Appl. Algebra*, 112(1):1–12, 1996.

[3] Claude Chevalley. Invariants of finite groups generated by reflections. *Amer. J. Math.*, 77:778–782, 1955.

[4] Harm Derksen and Gregor Kemper. *Computational invariant theory*. Invariant Theory and Algebraic Transformation Groups, I. Springer-Verlag, Berlin, 2002. Encyclopaedia of Mathematical Sciences, 130.

[5] Leonard Eugene Dickson. *On invariants and the theory of numbers*. Dover Publications, Inc., New York, 1966.

[6] Geir Ellingsrud and Tor Skjelbred. Profondeur d'anneaux d'invariants en caractéristique p. *Compositio Math.*, 41(2):233–244, 1980.

[7] Jonathan Elmer. Modular covariants of cyclic groups of order p. *J. Algebra*, 598:134–155, 2022.

[8] Peter Fleischmann, Gregor Kemper, and R. James Shank. Depth and cohomological connectivity in modular invariant theory. *Trans. Amer. Math. Soc.*, 357(9):3605–3621 (electronic), 2005.

[9] M. Hochster and John A. Eagon. Cohen-Macaulay rings, invariant theory, and the generic perfection of determinantal loci. *Amer. J. Math.*, 93:1020–1058, 1971.

[10] Barbara R. Peskin. Quotient-singularities and wild p-cyclic actions. *J. Algebra*, 81(1):72–99, 1983.

[11] R. James Shank and David L. Wehlau. Decomposing symmetric powers of certain modular representations of cyclic groups. In *Symmetry and spaces*, volume 278 of *Progr. Math.*, pages 169–196. Birkhäuser Boston, Boston, MA, 2010.

[12] G. C. Shephard and J. A. Todd. Finite unitary reflection groups. *Canadian J. Math.*, 6:274–304, 1954.

Middlesex University, The Burroughs, Hendon, London, NW4 4BT UK
Email address: j.elmer@mdx.ac.uk