



ELSEVIER

Contents lists available at ScienceDirect

Journal of Algebra

www.elsevier.com/locate/jalgebra



# Modular covariants of cyclic groups of order $p$



Jonathan Elmer

Middlesex University, The Burroughs, London, NW4 4BT, United Kingdom

## ARTICLE INFO

### Article history:

Received 14 November 2019

Available online 3 February 2022

Communicated by Bernd Ulrich

### MSC:

13A50

### Keywords:

Modular invariant theory

Covariants

Free module

Cohen-Macaulay

Hilbert series

## ABSTRACT

Let  $G$  be a cyclic group of order  $p$  and let  $V, W$  be  $\mathbb{k}G$ -modules. We study the modules of covariants  $\mathbb{k}[V, W]^G = (S(V^*) \otimes W)^G$ . Recall that  $G$  has exactly  $p$  inequivalent indecomposable  $\mathbb{k}G$ -modules, denoted  $V_n$  ( $n = 1, \dots, p$ ) and  $V_n$  has dimension  $n$ . For any  $n$ , we show that  $\mathbb{k}[V_2, V_n]^G$  is a free  $\mathbb{k}[V_2]^G$ -module (recovering a result of Broer and Chuai [1]) and we give an explicit set of covariants generating  $\mathbb{k}[V_2, V_n]^G$  freely over  $\mathbb{k}[V_2]^G$ . For any  $n$ , we show that  $\mathbb{k}[V_3, V_n]^G$  is a Cohen-Macaulay  $\mathbb{k}[V_3]^G$ -module (again recovering a result of Broer and Chuai) and we give an explicit set of covariants which generate  $\mathbb{k}[V_3, V_n]^G$  freely over a homogeneous system of parameters for  $\mathbb{k}[V_3]^G$ . We also use our results to compute a minimal generating set for the transfer ideal of  $\mathbb{k}[V_3]^G$  over a homogeneous system of parameters.

© 2022 The Author. Published by Elsevier Inc. This is an open access article under the CC BY-NC-ND license (<http://creativecommons.org/licenses/by-nc-nd/4.0/>).

## 1. Introduction

Let  $G$  be a finite group,  $\mathbb{k}$  a field, and  $V$  and  $W$  finite-dimensional  $\mathbb{k}G$ -modules on which  $G$  acts linearly. Then  $G$  acts on the set of functions  $V \rightarrow W$  according to the formula

*E-mail address:* [j.elmer@mdx.ac.uk](mailto:j.elmer@mdx.ac.uk).

<https://doi.org/10.1016/j.jalgebra.2022.01.015>

0021-8693/© 2022 The Author. Published by Elsevier Inc. This is an open access article under the CC BY-NC-ND license (<http://creativecommons.org/licenses/by-nc-nd/4.0/>).

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

for all  $g \in G$  and  $v \in V$ .

We denote the set of polynomial functions  $V \rightarrow W$  by  $\mathbb{k}[V, W]$ . With the above action, the  $G$ -fixed points  $\mathbb{k}[V, W]^G$  are precisely the  $G$ -equivariant polynomial maps. We call such maps *covariants*. In the special case  $W = \mathbb{k}$  with trivial  $G$ -action we write  $\mathbb{k}[V]$  instead of  $\mathbb{k}[V, \mathbb{k}]$ , and the fixed points  $\mathbb{k}[V]^G$  are called *invariants*.

For  $f \in \mathbb{k}[V]$  and  $\phi \in \mathbb{k}[V, W]$  we denote by  $f\phi$  the pointwise product. Then one sees that, for all  $g \in G$  and  $v \in V$  we have

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

Therefore  $\mathbb{k}[V]^G$  is a  $\mathbb{k}$ -algebra and  $\mathbb{k}[V, W]^G$  is a  $\mathbb{k}[V]^G$ -module. We are interested in the structure of this module. Note that if the field  $\mathbb{k}$  is infinite, then  $\mathbb{k}[V, W]$  can be identified with  $S(V^*) \otimes W$ , where the action on the tensor product is diagonal and the action on  $S(V^*)$  is the natural extension of the action on  $V^*$  by algebra automorphisms.

If  $G$  is finite and the characteristic of  $\mathbb{k}$  does not divide  $|G|$ , then Schur’s lemma implies that every covariant restricts to an isomorphism of some direct summand of  $S(V^*)$  onto  $W$ . Thus, covariants can be viewed as “copies” of  $W$  inside  $S(V^*)$ . Otherwise, the situation is more complicated.

This question has been considered by a number of authors over the years. For example, Chevalley and Sheppard-Todd [2], [12] showed that if the characteristic of  $\mathbb{k}$  does not divide  $|G|$  and  $G$  acts as a reflection group on  $V$ , then  $\mathbb{k}[V]^G$  is a polynomial algebra and  $\mathbb{k}[V, W]^G$  is free. More generally, Eagon and Hochster [8] showed that if the characteristic of  $\mathbb{k}$  does not divide  $|G|$  then  $\mathbb{k}[V, W]^G$  is a Cohen-Macaulay module (and  $\mathbb{k}[V]^G$  a Cohen-Macaulay ring in particular). In the modular case, Hartmann [6] and Hartmann-Shepler [7] gave necessary and sufficient conditions for a set of covariants to generate  $\mathbb{k}[V, W]^G$  as a free  $\mathbb{k}[V]^G$ -module, provided that  $\mathbb{k}[V]^G$  is polynomial and  $W \cong V^*$ . Broer and Chuai [1] remove the restrictions on both  $W$  and  $\mathbb{k}[V]^G$ .

The present article is inspired by two particular results from [1], which we state here for convenience:

**Proposition 1** ([1], Proposition 6). *Let  $G$  be a finite group of order divisible by  $p = \text{char}(\mathbb{k})$  and let  $V, W$  be  $\mathbb{k}G$ -modules.*

- (i) *Suppose  $\text{codim}(V^G) = 1$ . Then  $\mathbb{k}[V]^G$  is a polynomial algebra and  $\mathbb{k}[V, W]^G$  is free as a graded module over  $\mathbb{k}[V]^G$ .*
- (ii) *Suppose  $\text{codim}(V^G) = 2$ . Then  $\mathbb{k}[V, W]^G$  is a Cohen-Macaulay graded module over  $\mathbb{k}[V]^G$ .*

In the situation of (i) above, there is a method for checking a set of covariants generates  $\mathbb{k}[V, W]^G$  over  $\mathbb{k}[V]^G$ , but no method of constructing generators. Meanwhile, in the

situation of (ii), there exists a polynomial subalgebra  $A$  of  $\mathbb{k}[V]^G$  over which  $\mathbb{k}[V, W]^G$  is a free module. It is not clear how to find module generators, or to check that they generate  $\mathbb{k}[V, W]^G$ .

The purpose of this article is to work towards making these results constructive. We investigate certain modules of covariants for  $V$  satisfying (i) or (ii) above and  $G$  a cyclic group of order  $p$ . Let  $V_n$  denote the unique indecomposable  $\mathbb{k}G$ -module of dimension  $n$  (the action of  $G$  on  $V_n$  will be described in the next section). In Section 5, for any  $n$ , we show that  $\mathbb{k}[V_2, V_n]^G$  is a free  $\mathbb{k}[V_2]^G$ -module (recovering a result of Broer and Chuai) and we give an explicit set of covariants generating  $\mathbb{k}[V_2, V_n]^G$  freely over  $\mathbb{k}[V_2]^G$ . For any  $n$ , we show in Section 6 that  $\mathbb{k}[V_3, V_n]^G$  is a Cohen-Macaulay  $\mathbb{k}[V_3]^G$ -module (again recovering a result of Broer and Chuai) and we give an explicit set of covariants which generate  $\mathbb{k}[V_3, V_n]^G$  freely over a homogeneous system of parameters for  $\mathbb{k}[V_3]^G$ . We also use our results to compute a minimal generating set for the transfer ideal of  $\mathbb{k}[V_3]^G$  over a homogeneous system of parameters.

## 2. Preliminaries

From this point onwards we let  $G$  be a cyclic group of order  $p$  and  $\mathbb{k}$  a field of characteristic  $p$ . Let  $V$  and  $W$  be  $\mathbb{k}G$ -modules. We fix a generator  $\sigma$  of  $G$ . Recall that, up to isomorphism, there are exactly  $p$  indecomposable  $\mathbb{k}G$ -modules  $V_1, V_2, \dots, V_p$ , where the dimension of  $V_i$  is  $i$  and each has fixed-point space of dimension 1. The isomorphism class of  $V_i$  is usually represented by a module of column vectors on which  $\sigma$  acts as left-multiplication by a single Jordan block of size  $i$ .

Suppose  $W \cong V_n$ . It is convenient to choose a basis  $w_1, w_2, \dots, w_n$  of  $W$  for which the action of  $G$  is given by

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

(thus, the action of  $\sigma^{-1}$  is given by left-multiplication by an upper-triangular Jordan block). We do not (yet) choose a particular action on a basis for  $V$ , nor do we assume  $V$  is indecomposable; we let  $v_1, v_2, \dots, v_m$  be a basis of  $V$  and let  $x_1, \dots, x_m$  be the dual of this basis.

Note that  $\mathbb{k}[V] = \mathbb{k}[x_1, x_2, \dots, x_m]$ , and a general element of  $\mathbb{k}[V, W]$  is given by

$$\phi = f_1 w_1 + f_2 w_2 + \dots + f_n w_n$$

where each  $f_i \in \mathbb{k}[V]$ . We define the **support** of  $\phi$  by

$$\text{Supp}(\phi) = \{i : f_i \neq 0\}.$$

The operator  $\Delta = \sigma - 1 \in \mathbb{k}G$  will play a major role in our exposition. Notice that, for  $\phi \in \mathbb{k}[V, W]^G$  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  $\phi \in \mathbb{k}[V, W]^G$ . Similarly for  $f \in \mathbb{k}[V]$  we have  $\Delta(f) = 0$  if and only if  $f \in \mathbb{k}[V]^G$ .

$\Delta$  is a  $\sigma$ -twisted derivation on  $\mathbb{k}[V]$ ; that is, it satisfies the formula

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

for all  $f, g \in \mathbb{k}[V]$ .

Further, using induction and the fact that  $\sigma$  and  $\Delta$  commute, one can show  $\Delta$  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  $f \in \mathbb{k}[V]$  we define the **weight** of  $f$ :

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

Notice that  $\Delta^{\text{wt}(f)-1}(f) \in \ker(\Delta) = \mathbb{k}[V]^G$  for all  $f \in \mathbb{k}[V]$ . Another consequence of (2) is the following: let  $f, g \in \mathbb{k}[V]$  and set  $d = \text{wt}(f), e = \text{wt}(g)$ . 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  $\binom{d+e-2}{i} \neq 0 \pmod p$ . We obtain the following:

**Proposition 2.** *Let  $f, g \in \mathbb{k}[V]$  with  $\text{wt}(f) + \text{wt}(g) - 1 \leq p$ . Then  $\text{wt}(fg) = \text{wt}(f) + \text{wt}(g) - 1$ .*

Also note that

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

which shows that  $\text{wt}(f) \leq p$  for all  $f \in \mathbb{k}[V]^G$ . Finally notice that

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

This is the *Transfer map*, a  $\mathbb{k}[V]^G$ -homomorphism  $\text{Tr}^G : \mathbb{k}[V] \rightarrow \mathbb{k}[V]^G$  which is well-known to invariant theorists.

Now we have a crucial observation concerning the action of  $\sigma$  on  $W$ : for all  $i = 1, \dots, n - 1$  we have

$$\Delta(w_{i+1}) + \sigma(w_i) = 0 \tag{5}$$

and  $\Delta(w_1) = 0$ .

From this we obtain a simple characterisation of covariants:

**Proposition 3.** *Let*

$$\phi = f_1w_1 + f_2w_2 + \dots + f_nw_n.$$

*Then  $\phi \in \mathbb{k}[V, W]^G$  if and only if there exists  $f \in \mathbb{k}[V]$  with weight  $\leq n$  such that  $f_i = \Delta^{i-1}(f)$  for all  $i = 1, \dots, n$ .*

**Proof.** Assume  $\phi \in \mathbb{k}[V, W]^G$ . Then we have

$$\begin{aligned} 0 &= \Delta \left( \sum_{i=1}^n f_i w_i \right) \\ &= \sum_{i=1}^n (f_i \Delta(w_i) + \Delta(f_i) \sigma(w_i)) \end{aligned}$$

$$= \sum_{i=1}^{n-1} (\Delta(f_i) - f_{i+1})\sigma(w_i) + \Delta(f_n)\sigma(w_n)$$

where we used (5) in the final step. Now note that

$$\sigma(w_i) = w_i + (\text{terms in } w_{i-1}, w_{i-2}, \dots, w_1)$$

for all  $i = 1, \dots, n$ . Thus, equating coefficients of  $w_i$ , for  $i = n, \dots, 1$  gives

$$\Delta(f_n) = 0, \Delta(f_{n-1}) = f_n, \dots, \Delta(f_2) = f_3, \Delta(f_1) = f_2.$$

Putting  $f = f_1$  gives  $f_i = \Delta^{i-1}(f)$  for all  $i = 1, \dots, n$  and  $0 = \Delta^n(f)$  as required.

Conversely, suppose that

$$\phi = \sum_{i=1}^n \Delta^{i-1}(f)w_i$$

for some  $f \in \mathbb{k}[V]$  with  $\Delta^n(f) = 0$ . Then we have

$$\begin{aligned} \Delta(\phi) &= \sum_{i=1}^n \Delta^{i-1}(f)\Delta(w_i) + \Delta^i(f)\sigma(w_i) \\ &= \sum_{i=2}^n (-\Delta^{i-1}(f)\sigma(w_{i-1}) + \Delta^i(f)\sigma(w_i)) + \Delta(f)\sigma(w_1) \quad \text{by (5)} \\ &= \Delta^n(f)\sigma(w_n) \\ &= 0 \end{aligned}$$

as required.  $\square$

Note that the support of any covariant is therefore of the form  $\{1, 2, \dots, i\}$  for some  $i \leq n$ . We will write

$$\text{Supp}(\phi) = i$$

if  $\phi$  is a covariant and  $\text{Supp}(\phi) = \{1, 2, \dots, i\}$ .

Introduce notation

$$K_n := \ker(\Delta^n)$$

and

$$I_n := \text{im}(\Delta^n).$$

These are  $\mathbb{k}[V]^G$ -modules lying inside  $\mathbb{k}[V]$ .

Now we can define a map

$$\begin{aligned} \Theta : K_n &\rightarrow \mathbb{k}[V, W]^G \\ \Theta(f) &= \sum_{i=1}^n \Delta^{i-1}(f)w_i. \end{aligned} \tag{6}$$

Clearly  $\Theta$  is an injective, degree-preserving map of  $\mathbb{k}[V]^G$ -modules, and Proposition 3 implies it is also surjective. We conclude that

**Proposition 4.**  *$K_n$  and  $\mathbb{k}[V, W]^G$  are isomorphic as graded  $\mathbb{k}[V]^G$ -modules.*

From this point onwards we set  $V = V_m$  and  $W = V_n$ , with the basis of  $V$  chosen so that

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

**Lemma 5.** *Let  $z = x_1^{e_1}x_2^{e_2} \dots x_m^{e_m}$ . Let  $d = \sum_{i=1}^m e_i(m - i)$ ,  $e = \sum_{i=1}^m e_i = \deg(z)$  and assume  $d < p$ . Then*

$$\text{wt}(z) = d + 1.$$

**Proof.** Applying Proposition 2 repeatedly and noting that  $\text{wt}(x_i) = m - i + 1$ , we find

$$\begin{aligned} \text{wt}(z) &= \sum_{i=1}^m (e_i(m - i + 1) - e_i + 1) - (n - 1) \\ &= \sum_{i=1}^m (e_i(m - i)) + 1 = d + 1. \quad \square \end{aligned}$$

### 3. Hilbert series

Let  $\mathbb{k}$  be a field and let  $S = \bigoplus_{i \geq 0} S_i$  be a positively graded  $\mathbb{k}$ -vector space. The dimension of each graded component of  $S$  is encoded in its Hilbert Series

$$H(S, t) = \sum_{i \geq 0} \dim(S_i)t^i.$$

Proposition 4 implies that  $H(\mathbb{k}[V, W]^G, t) = H(K_n, t)$ . In this section we will outline a method for computing  $H(K_n, t)$ .

Each homogeneous component  $\mathbb{k}[V]_i$  of  $\mathbb{k}[V]$  is a  $\mathbb{k}G$ -module. As such, each one decomposes as a direct sum of modules isomorphic to  $V_k$  for some values of  $k$ . Write  $\mu_k(\mathbb{k}[V]_i)$  for the multiplicity of  $V_k$  in  $\mathbb{k}[V]_i$  and define the series

$$H_k(\mathbb{k}[V]) = \sum_{i \geq 0} \mu_k(\mathbb{k}[V]_i) t^i.$$

The series  $H_k(\mathbb{k}[V_m])$  were studied by Hughes and Kemper in [9]. They can also be used to compute the Hilbert series of  $\mathbb{k}[V_m]^G$ ; since  $\dim(V_k^G) = 1$  for all  $k = 1, \dots, p$  we have

$$H(\mathbb{k}[V_m]^G, t) = \sum_{k=1}^p H_k(\mathbb{k}[V_m], t). \tag{7}$$

Now observe that

$$\dim(\ker(\Delta^n|_{V_k})) = \begin{cases} n & k \geq n \\ k & \text{otherwise.} \end{cases}$$

Therefore

$$H(K_n, t) = \sum_{k=1}^{n-1} k H_k(\mathbb{k}[V], t) + \sum_{k=n}^p n H_k(\mathbb{k}[V], t).$$

We can write this as a series not depending on  $p$ :

$$H(K_n, t) = n H(\mathbb{k}[V]^G, t) - \left( \sum_{k=1}^{n-1} (n - k) H_k(\mathbb{k}[V], t) \right), \tag{8}$$

using equation (7).

We will need the Hilbert Series of  $I_n^G = \mathbb{k}[V]^G \cap I_n$  in the final section. For all  $k = 1, \dots, p$  we have

$$\dim(\Delta^n(V_k))^G = \begin{cases} 1 & k > n \\ 0 & \text{otherwise.} \end{cases}$$

Therefore

$$H(I_n^G, t) = \sum_{k=n+1}^p H_k(\mathbb{k}[V], t),$$

which we can write independently of  $p$  as



$$H(I_n^G, t) = H(\mathbb{k}[V]^G, t) - \left(\sum_{k=1}^n H_k(\mathbb{k}[V], t)\right). \tag{9}$$

**4. Decomposition theorems**

In this section we will compute the series  $H_k(\mathbb{k}[V_2], t)$  and  $H_k(\mathbb{k}[V_3], t)$  for all  $k = 1, \dots, p - 1$ .

Hughes and Kemper [9, Theorem 3.4] give the formula

$$H_k(\mathbb{k}[V_m], t) = \sum_{\gamma \in M_{2p}} \frac{\gamma - \gamma^{-1}}{2p} \gamma^{-k} \frac{1 - \gamma^{p(m-1)}t^p}{1 - t^p} \prod_{j=0}^{m-1} (1 - \gamma^{m-1-2j}t)^{-1}, \tag{10}$$

where  $M_{2p}$  represents the set of  $2p$ th roots of unity in  $\mathbb{C}$ . A similar formula is given for  $H_p(\mathbb{k}[V], t)$  but we will not need this. The following result can be derived from the formula above, but follows more easily from [4, Proposition 3.4]:

**Lemma 6.**  $H_k(\mathbb{k}[V_2], t) = \frac{t^{k-1}}{1-t^p}$ .

For  $V_3$  we will have to use Equation (10). This becomes

$$H_k(\mathbb{k}[V_3], t) = \frac{1}{2p(1-t)} \sum_{\gamma \in M_{2p}} \frac{(\gamma - \gamma^{-1})\gamma^{-k+2}}{(1 - \gamma^2t)(\gamma^2 - t)}.$$

**Lemma 7.**

$$H_k(\mathbb{k}[V_3], t) = \begin{cases} \frac{t^{p-l} - t^{p-l-1} + t^{l+1} - t^l}{(1-t)(1-t^2)(1-t^p)} & \text{if } k = 2l + 1 \text{ is odd} \\ 0 & \text{if } k \text{ is even.} \end{cases}$$

**Proof.** We evaluate

$$\frac{(\gamma - \gamma^{-1})\gamma^{-k+2}}{(1 - \gamma^2t)(\gamma^2 - t)} = \frac{A}{\gamma - t^{\frac{1}{2}}} + \frac{B}{\gamma + t^{\frac{1}{2}}} + \frac{C}{1 - \gamma t^{\frac{1}{2}}} + \frac{D}{1 + \gamma t^{\frac{1}{2}}}$$

using partial fractions, finding

$$\begin{aligned} A &= \frac{t^{-l+1} - t^{-l}}{(2t^{\frac{1}{2}})(1 - t^2)}, \\ B &= (-1)^{-k+3} \frac{t^{-l+1} - t^{-l}}{(-2t^{\frac{1}{2}})(1 - t^2)}, \\ C &= \frac{t^{l-1} - t^l}{2(t^{-1} - t)}, \\ D &= (-1)^{-k+3} \frac{t^{l-1} - t^l}{2(t^{-1} - t)}. \end{aligned}$$

Now we compute:

$$\begin{aligned}
 \sum_{\gamma \in M_{2p}} \frac{1}{\gamma - t^{\frac{1}{2}}} &= \sum_{\gamma \in M_{2p}} \frac{-t^{-\frac{1}{2}}}{1 - \gamma t^{-\frac{1}{2}}} \\
 &= -t^{-\frac{1}{2}} \sum_{i=0}^{\infty} \sum_{\gamma \in M_{2p}} (\gamma t^{-\frac{1}{2}})^i \\
 &= -t^{-\frac{1}{2}} 2p \sum_{i=0}^{\infty} (t^{-\frac{1}{2}})^{2pi} \\
 &= -t^{-\frac{1}{2}} 2p \frac{1}{1 - (t^{-\frac{1}{2}})^{2p}} \\
 &= -t^{\frac{1}{2}} 2p \frac{1}{1 - t^{-p}} \\
 &= 2p \frac{t^{p-\frac{1}{2}}}{1 - t^p}
 \end{aligned}$$

Similarly we have

$$\sum_{\gamma \in M_{2p}} \frac{1}{\gamma + t^{\frac{1}{2}}} = -2p \frac{t^{p-\frac{1}{2}}}{1 - t^p}$$

while

$$\begin{aligned}
 \sum_{\gamma \in M_{2p}} \frac{1}{1 - \gamma t^{\frac{1}{2}}} &= \sum_{i=0}^{\infty} \sum_{\gamma \in M_{2p}} (\gamma t^{\frac{1}{2}})^i \\
 &= 2p \sum_{i=0}^{\infty} (t^{\frac{1}{2}})^{2pi} \\
 &= 2p \sum_{i=0}^{\infty} (t^{pi}) \\
 &= 2p \frac{1}{1 - t^p}
 \end{aligned}$$

and similarly

$$\sum_{\gamma \in M_{2p}} \frac{1}{1 + \gamma t^{\frac{1}{2}}} = 2p \frac{1}{1 - t^p}$$

as  $\{-\gamma : \gamma \in M_{2p}\} = M_{2p}$ .

It follows that

$$\begin{aligned}
 H_k(\mathbb{k}[V_3], t) &= \frac{1}{2p(1-t)} \left( \frac{(A-B)2pt^{p-\frac{1}{2}}}{1-t^p} + \frac{2p(C+D)}{1-t^p} \right) \\
 &= \frac{1}{(1-t)(1-t^p)} \left( \frac{(1+(-1)^{-k+3})(t^{p-l} - t^{p-l-1})}{2(1-t^2)} \right. \\
 &\quad \left. + \frac{(1+(-1)^{-k+3})(t^{l-1} - t^l)}{2(t^{-1} - t)} \right) \\
 &= \begin{cases} \frac{t^{p-l} - t^{p-l-1} + t^{l+1} - t^l}{(1-t)(1-t^2)(1-t^p)} & \text{if } k \text{ is odd} \\ 0 & \text{if } k \text{ is even} \end{cases}
 \end{aligned}$$

as required.  $\square$

**5. Main results:  $V_2$**

We are now in a position to state our main results. First, suppose  $V = V_2$  and  $W = V_n$  where  $n \leq p$ . Then it's well known that  $\mathbb{k}[V]^G$  is a polynomial ring, generated by  $x_2$  and

$$N = \prod_{i=0}^{p-1} \sigma^i(x_1) = x_1^p - x_1 x_2^{p-1}.$$

Therefore we have

$$H(\mathbb{k}[V]^G, t) = \frac{1}{(1-t)(1-t^p)}. \tag{11}$$

**Proposition 8.** *We have*

$$H(K_n, t) = H(\mathbb{k}[V, W]^G, t) = \frac{1+t+t^2+\dots+t^{n-1}}{(1-t)(1-t^p)}.$$

**Proof.** Using equations (8) and (11) and Lemma 6 we have

$$H(K_n, t) = \frac{n}{(1-t)(1-t^p)} - \sum_{k=1}^{n-1} \frac{(n-k)t^{k-1}}{1-t^p} = \frac{1+t+t^2+\dots+t^{n-1}}{(1-t)(1-t^p)}.$$

The result now follows from Proposition 4.  $\square$

**Theorem 9.** *The module of covariants  $\mathbb{k}[V, W]^G$  is generated freely over  $\mathbb{k}[V]^G$  by*

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

where  $\Theta(x_1^0) = \Theta(1) = w_1$ .

Note that, by Proposition 1(i),  $\mathbb{k}[V, W]^G$  is free over  $\mathbb{k}[V]^G$  and we could use [1, Theorem 3] to check our proposed module generators. However, we prefer a more direct approach.

**Proof.** It follows from Lemma 5 that  $\text{wt}(x_1^k) = k + 1$ . Therefore  $\text{Supp}(\Theta(x_1^k)) = k + 1$ , and so it's clear that the  $\mathbb{k}[V]^G$ -submodule  $M$  of  $\mathbb{k}[V, W]^G$  generated by the proposed generating set is free. Moreover, as  $\text{deg}(\Theta(x_1^k)) = k$ ,  $M$  has Hilbert series

$$\frac{1 + t + t^2 + \dots + t^{n-1}}{(1 - t)(1 - t^p)}.$$

But by Proposition 8, this is the Hilbert series of  $\mathbb{k}[V, W]^G$ . Therefore  $M = \mathbb{k}[V, W]^G$  as required.  $\square$

**Corollary 10.**  $K_n$  is a free  $\mathbb{k}[V^G]$ -module, generated by  $\{x_1^k : k = 0, \dots, n - 1\}$ .

**Proof.** Follows from Theorem 9 above and the proof of Proposition 4.  $\square$

**Remark 11.** The above was also obtained, in the special case  $n = p - 1$ , by Erkuş and Madran [5].

### 6. Main results: $V_3$

In this section let  $p$  be an odd prime and  $V = V_3$ . We begin by describing  $\mathbb{k}[V]^G$ . This has been done in several places before, for example [3] and [10, Theorem 5.8], but we include this for completeness.

We use a graded reverse lexicographic order on monomials  $\mathbb{k}[V]$  with  $x_1 > x_2 > x_3$ . If  $f \in \mathbb{k}[V]$  then the *lead term* of  $f$  is the term with the largest monomial in our order and the *lead monomial* is the corresponding monomial. If  $f, g \in \mathbb{k}[V]$  we will write

$$f > g$$

if the lead monomial of  $f$  is greater than the lead monomial of  $g$ .

The results of section 3 can be used to show

$$H(\mathbb{k}[V]^G, t) = \frac{1 + t^p}{(1 - t)(1 - t^2)(1 - t^p)}. \tag{12}$$

Note that using the given order, we have

$$f > \Delta(f)$$

for all  $f \in \mathbb{k}[V]$ .

We recall two popular means of constructing invariants. Let  $f \in \mathbb{k}[V]$ . As mentioned in section 2, the transfer

$$\Delta^{p-1}(f) = \text{Tr}^G(f) = \sum_{i=0}^{p-1} (\sigma^i f)$$

and also the norm

$$N(f) = \prod_{i=0}^{p-1} (\sigma^i f)$$

of  $f$  both lie in  $\mathbb{k}[V]^G$ . It is easily shown that

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

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

**Proposition 12.** *Let  $f \in \mathbb{k}[V]^G$  be any invariant with lead term  $x_2^p$ . Let  $A = \mathbb{k}[a_1, a_2, a_3]$ . Then  $f \notin A$ . Consequently  $\mathbb{k}[V]^G$  is a free  $A$ -module, whose generators are 1 and  $f$ .*

**Proof.** It is clear that  $f \notin A$ , as its lead term is not in the subalgebra of  $\mathbb{k}[V]$  generated by the lead terms of  $a_1, a_2$  and  $a_3$ . Therefore the  $A$ -submodule of  $\mathbb{k}[V]^G$  generated by 1 and  $f$  has Hilbert series

$$\frac{1 + t^p}{(1 - t)(1 - t^2)(1 - t^p)}$$

which is the Hilbert series of  $\mathbb{k}[V]^G$  as required.  $\square$

The obvious choice of invariant with lead term  $x_2^p$  is  $N(x_2)$ . However, we will use  $\text{Tr}^G(x_1^{p-1}x_2)$  instead. For the calculation of the lead term of this invariant see [11, Lemma 3.1] or Lemma 16 to come.

The following observation is a consequence of the generating set above.

**Lemma 13.** *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  $i, j, k$ .*

Now let  $W = V_n$  for some  $n \leq p$ . 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. Our first task is to compute the Hilbert Series of

$\mathbb{k}[V, W]^G$ . Once more we use equation (8) and the bijection  $\Theta$  to do this. We omit the details.

**Proposition 14.**

$$H(\mathbb{k}[V, W]^G, t) = \frac{1 + 2t + 2t^2 + \dots + 2t^l + 2t^{p-l} + 2t^{p-l+1} + \dots + t^p}{(1-t)(1-t^2)(1-t^p)}$$

if  $n$  is odd, while

$$H(\mathbb{k}[V, W]^G, t) = \frac{1 + 2t + 2t^2 + \dots + 2t^{l-1} + t^l + t^{p-l} + 2t^{p-l+1} + \dots + 2t^{p-1} + t^p}{(1-t)(1-t^2)(1-t^p)}$$

if  $n$  is even.

Next, we need some information about the lead monomials of certain polynomials:

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

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

**Proof.** The proof is by induction on  $j$ , the case  $j = 0$  being clear. Suppose  $1 \leq j < k$  and

$$\Delta^j(x_1^k) = \frac{k!}{(k-j)!} x_1^{k-j} x_2^j + g$$

where  $g \in \mathbb{k}[V]$  has lead monomial  $\leq x_1^{k-j-1} x_2^{j+1}$ . Then

$$\begin{aligned} \Delta^{j+1}(x_1^k) &= \frac{k!}{(k-j)!} \Delta(x_1^{k-j} x_2^j) + \Delta(g) \\ &= \frac{k!}{(k-j)!} \Delta(x_1^{k-j}) \sigma(x_2^j) + x_1^{k-j} \Delta(x_2^j) + \Delta(g). \end{aligned}$$

Note that the lead monomial of  $\Delta(g)$  is  $< x_1^{k-j-1} x_2^{j+1}$ . Now applying (3) shows that  $\Delta(x_2^j)$  is divisible by  $x_3$  and

$$\begin{aligned} \Delta(x_1^{k-j}) &= x_2(x_1^{k-j-1} + x_1^{k-j-2} \sigma(x_1) + \dots + \sigma(x_1)^{k-j-1}) \\ &= (k-j)x_1^{k-j-1} x_2 + \text{smaller terms.} \end{aligned}$$

In addition,

$$\sigma(x_2^j) = (x_2 + x_3)^j = x_2^j + \text{smaller terms.}$$

Therefore the lead term of  $\Delta^{j+1}(x_1^k)$  is

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

as required.  $\square$

Similarly we have

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

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

**Proof.** We have by (2)

$$\Delta^j(x_1^k x_2) = \sum_{i=0}^j \binom{j}{i} \Delta^{j-i}(x_1^k) \sigma^i(\Delta^i(x_2)).$$

Only the first two terms are nonzero, hence

$$\begin{aligned} \Delta^j(x_1^k x_2) &= \Delta^j(x_1^k) x_2 + j \Delta^{j-1}(x_1^k) x_3 \\ &= \frac{k!}{(k - j)!} x_1^{k-j} x_2^{j+1} + \text{smaller terms} \end{aligned}$$

where we used Lemma 15 is the last step.  $\square$

We are now ready to state our main results. Let  $V = V_3$  and  $W = V_n$ . For any  $i = 0, 1, \dots, n - 1$  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  $n \leq p$ . Then  $K_n$  is a free  $A$ -module, generated by*

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

**Proof.** By Lemma 2, 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  $p - \lceil \frac{i}{2} \rceil$  which shows that the  $A$ -module generated by  $S_n$  has Hilbert series bounded above by the Hilbert series of  $K_n$  given in Proposition 14, with equality if and only if it is free. Therefore it is enough to prove that  $S_n$  is linearly independent over  $A$ .

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

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

if  $n$  is odd, and

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

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 13, 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  $S_n$ .  $\square$

**Remark 18.** A generating set for  $K_{p-1}$  over a different system of parameters can be found in [5].

**Corollary 19.** *Let  $n \leq p$ . Then  $\mathbb{k}[V, W]^G$  is a Cohen-Macaulay module, generated over  $A$  by*

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

**Proof.** Follows from Theorem 17 and the proof of Proposition 4.  $\square$

### 7. Application to transfers

The transfer ideal  $\text{Tr}^G(\mathbb{k}[V])$  is widely studied in invariant theory. In the notation of this article, we have  $\text{Tr}^G(\mathbb{k}[V]) = I_{p-1}^G = I_{p-1}$ . In this section, we use our work on covariants to give minimal  $\mathbb{k}[V]^G$ -generating sets of the ideals  $I_{n-1}^G$  for each  $n = 1, 2, \dots, p$



when  $V = V_2$ , and minimal  $A$ -generating sets of the ideals  $I_{n-1}^G$  for each  $n = 1, 2, \dots, p$  when  $V = V_3$ . We retain the notation of sections 5 and 6.

**Theorem 20.** *Let  $V = V_2$  and  $1 \leq n \leq p$ . Then  $I_{n-1}^G$  is a free  $\mathbb{k}[V]^G$ -module, generated by  $x_2^{n-1}$ .*

**Proof.** The same argument as in Lemma 15 implies that  $\Delta^{n-1}(x_1^{n-1}) = \lambda x_2^{n-1}$  for some nonzero constant  $\lambda$ , so  $x_2^{n-1} \in I_{n-1}^G$ . Using (9) we see that

$$H(I_{n-1}^G, t) = \frac{t^{n-1}}{(1-t)(1-t^n)}.$$

As this is the Hilbert series of the ideal  $x_2^{n-1}\mathbb{k}[V]^G$ , the result follows.  $\square$

For  $V = V_3$  we need to do a bit more work. We define a set of invariants

$$T_{n-1} = \{\Delta^{n-1}(M_{n-1})\} \cup \{\Delta^{p-1}(P_i) : i \text{ odd or zero, } i < n\}.$$

Bearing in mind the weight of  $M_{n-1}$  is  $n$ , and the weight of each  $P_i$  above is  $p$ , it's clear that  $T_{n-1} \subset I_{n-1}^G$ . We claim that

**Proposition 21.**  *$T_{n-1}$  generates  $I_{n-1}^G$  as an  $A$ -module.*

**Proof.** Let  $h \in I_{n-1}^G$ . Then we can write  $h = \Delta^{n-1}(f)$  for some  $f \in \mathbb{k}[V]^G$  with weight  $n$ , and by Proposition 3 we have  $\Theta(f) \in \mathbb{k}[V, V_n]^G$ . By Corollary 19 we can find elements  $\alpha_0, \alpha_1, \dots, \alpha_{n-1}, \beta_0, \beta_1, \dots, \beta_{n-1} \in A$  such that

$$\Theta(f) = \sum_{i=0}^{n-1} \alpha_i \Theta(M_i) + \sum_{i=0}^{n-1} \beta_i \Theta(\Delta^{p-n}(P_i)).$$

Equating coefficients of  $w_n$  in the above we obtain

$$h = \sum_{i=0}^{n-1} \alpha_i \Delta^{n-1}(M_i) + \sum_{i=0}^{n-1} \beta_i \Delta^{p-1}(P_i)$$

but since  $\Delta^{n-1}(M_i) = 0$  for  $i < n - 1$  and  $\Delta^{p-1}(P_i) = 0$  when  $i$  is even and  $i > 0$ , we get  $h \in AT_n$  as desired.  $\square$

$T_{n-1}$  does not generate  $I_{n-1}^G$  freely over  $A$ . To see this, note that if  $T_{n-1}$  were free over  $A$ , the resulting module would have Hilbert series

$$\frac{t^l + t^{p-l} + t^{p-l+1} + \dots + t^p}{(1-t)(1-t^2)(1-t^p)}.$$

But using (9) to calculate the Hilbert series of  $I_n^G$  yields

$$H(I_{n-1}^G, t) = \frac{t^l + t^{p-l}}{(1-t)(1-t^2)(1-t^p)} \tag{13}$$

which is strictly smaller. We claim, however, that  $T_n$  is a minimal generating set. The first step in our argument requires more knowledge of certain lead monomials:

**Lemma 22.** *Let  $j \leq k$  with  $j + k < p$ . Then  $\Delta^{k+j}(x_1^k)$  can be expressed as*

$$2^{-j}(j+k)! \binom{k}{j} x_2^{k-j} x_3^j + \mu_{j,k} x_1 x_2^{k-j-2} x_3^{j+1} + \text{smaller terms}$$

for some constant  $\mu_{j,k} \in \mathbb{k}$ , where  $\mu_{j,k} = 0$  if  $j - k < 2$ . In particular, the lead monomial of  $\Delta^{k+j}(x_1^k)$  is  $x_2^{k-j} x_3^j$ .

**Proof.** For shorthand we write

$$\lambda_{j,k} = 2^{-j}(j+k)! \binom{k}{j}.$$

We begin by showing, for all  $0 < j \leq k$ , that

$$\lambda_{j,k+1} = (j+k+1)\lambda_{j,k} + \binom{j+k+1}{2} \lambda_{j-1,k}. \tag{14}$$

The author wishes to thank Fedor Petrov for pointing out this fact. To prove it, note that

$$\begin{aligned} & \binom{j+k+1}{2} \lambda_{j-1,k} + (j+k+1)\lambda_{j,k} \\ &= \frac{(j+k+1)(j+k)}{2} 2^{-j+1}(j+k-1)! \binom{k}{j-1} + (j+k+1)2^{-j}(j+k)! \binom{k}{j} \\ &= 2^{-j}(j+k+1)! \left( \binom{k}{j-1} + \binom{k}{j} \right) \\ &= 2^{-j}(j+k+1)! \binom{k+1}{j} \\ &= \lambda_{j,k+1} \end{aligned}$$

as required.

The proof is by induction on  $j$ . First suppose  $j = 0$ . We must show that

$$\Delta^k(x_1^k) = k!x_2^k + \mu_{0,k}x_1x_2^{k-2}x_3 + \text{smaller terms}. \tag{15}$$

We prove this by induction on  $k$ . The case  $k = 1$  is clear (with  $\mu_{0,1} = 0$ ), so let  $k \geq 1$ . Then we have

$$\begin{aligned} \Delta^{k+1}(x_1^{k+1}) &= \Delta^{k+1}(x_1^k \cdot x_1) \\ &= \sum_{i=0}^{k+1} \binom{k+1}{i} \Delta^{k+1-i}(x_1^k) \sigma^i(\Delta^i(x_1)) \\ &= x_1 \Delta^{k+1}(x_1^k) + (k+1)(x_2 + x_3) \Delta^k(x_1^k) + \binom{k+1}{2} x_3 \Delta^{k-1}(x_1^k). \end{aligned}$$

Now by Lemma 15 we have

$$\Delta^{k-1}(x_1^k) = k!x_1x_2^{k-1} + f$$

for some  $f \in \mathbb{k}[V]$  with lead monomial  $\leq x_2^k$ . By induction we have

$$\Delta^k(x_1^k) = k!x_2^k + \mu_{0,k}x_1x_2^{k-2}x_3 + \text{smaller terms}$$

and

$$\begin{aligned} \Delta^{k+1}x_1^k &= k! \Delta(x_2^k) + \mu_{0,k}x_3 \Delta(x_1x_2^{k-2}) + \text{smaller terms} \\ &= k!x_3(x_2^{k-1} + x_2^{k-2}\sigma(x_2) + \dots + \sigma(x_2)^{k-1}) \\ &\quad + \mu_{0,k}x_3(x_2\sigma(x_2^{k-2}) + x_1\Delta(x^{k-2})) + \text{smaller terms} \\ &= (k \cdot k! + \mu_{0,k})x_2^{k-1}x_3 + \text{smaller terms.} \end{aligned}$$

So, ignoring terms smaller than  $x_1x_2^{k-1}x_3$  we have

$$\begin{aligned} \Delta^{k+1}(x_1^{k+1}) &= (k \cdot k! + \mu_{0,k})x_1x_2^{k-1}x_3 + (k+1)!x_2^{k+1} + (k+1)\mu_{0,k}x_1x_2^{k-1}x_3 \\ &\quad + k! \binom{k+1}{2} x_1x_2^{k-1}x_3 \\ &= (k+1)!x_2^{k+1} + (k!(k + \binom{k+1}{2})) + (k+2)\mu_{0,k}x_1x_2^{k-1}x_3 \end{aligned}$$

from which the claim (15) follows.

Now suppose  $j > 0$ . We proceed by induction on  $k$ . The initial case is  $k = j$ , so we must first show that

$$\Delta^{2k}(x_1^k) = 2^{-k}(2k)!x_3^k.$$

We prove this by induction on  $k$ . The result is clear when  $k = 1$ . Suppose that  $k \geq 1$ , then we have by (2)

$$\Delta^{2k+2}(x_1^{k+1}) = x_1\Delta^{2k+2}(x_1^k) + (2k+2)(x_2+x_3)\Delta^{2k+1}(x_1^k) + \frac{(2k+2)(2k+1)}{2}x_3\Delta^{2k}(x_1^k).$$

But by Lemma 5, the weight of  $x_1^k$  is  $2k+1$ , so the first two terms vanish. By induction we are left with

$$\Delta^{2k+2}(x_1^{k+1}) = \frac{(2k+2)(2k+1)}{2}x_3\frac{(2k)!}{2^k}x_3^k = \frac{(2k+2)!}{2^{k+1}}x_3^{k+1}$$

as required.

Now suppose  $k \geq j$ , then we have

$$\begin{aligned} \Delta^{j+k+1}(x_1^{k+1}) &= \Delta^{j+k+1}(x_1^k \cdot x_1) \\ &= \sum_{i=0}^{j+k+1} \binom{j+k+1}{i} \Delta^{j+k+1-i}(x_1^k)\sigma^i(\Delta^i(x_1)) \\ &= x_1\Delta^{j+k+1}(x_1^k) + (j+k+1)(x_2+x_3)\Delta^{j+k}(x_1^k) \\ &\quad + \binom{j+k+1}{2}x_3\Delta^{j-1+k}(x_1^k). \end{aligned}$$

Now by induction on  $k$  we have

$$\Delta^{j+k}(x_1^k) = \lambda_{j,k}x_2^{k-j}x_3^j + \mu_{j,k}x_1x_2^{k-j-2}x_3^{j+1} + \text{smaller terms.}$$

So

$$\begin{aligned} \Delta^{j+k+1}(x_1^k) &= \lambda_{j,k}x_3^j\Delta(x_2^{k-j}) + \mu_{j,k}x_3^{j+1}\Delta(x_1x_2^{k-j-2}) + \text{smaller terms} \\ &= \lambda_{j,k}x_3^j(x_3)(x_2^{k-j-1} + x_2^{k-j-2}\sigma(x_2) + \dots + \sigma(x_2)^{k-j-1}) \\ &\quad + \mu_{j,k}x_3^{j+1}(x_2\sigma(x_2^{k-j-2}) + x_1\Delta(x_2^{k-j-2})) + \text{smaller terms} \\ &= (\lambda_{j,k}(k-j) + \mu_{j,k})x_3^{j+1}x_2^{k-j-2} + \text{smaller terms.} \end{aligned}$$

Also by induction on  $j$  we have

$$\Delta^{j-1+k}(x_1^k) = \lambda_{j-1,k}x_2^{k-j+1}x_3^{j-1} + \mu_{j-1,k}x_1x_2^{k-j-1}x_3^j + \text{smaller terms.}$$

So, ignoring terms smaller than  $x_1x_2^{k-j-1}x_3^{j+1}$  we have

$$\begin{aligned} \Delta^{j+k+1}(x_1^{k+1}) &= (\lambda_{j,k}(k-j) + \mu_{j,k})x_1x_3^{j+1}x_2^{k-j-2} \\ &\quad + (j+k+1)(\lambda_{j,k}x_2^{k+1-j}x_3^j + \mu_{j,k}x_1x_2^{k-j-1}x_3^{j+1}) \\ &\quad + \binom{j+k+1}{2}(\lambda_{j-1,k}x_2^{k-j+1}x_3^j + \mu_{j-1,k}x_1x_2^{k-j-1}x_3^{j+1}) \\ &= \left( (j+k+1)\lambda_{j,k} + \binom{j+k+1}{2}\lambda_{j-1,k} \right) x_2^{k+1-j}x_3^j \end{aligned}$$

$$\begin{aligned}
 & + (\lambda_{j,k}(k - j) + (j + k + 2)\mu_{j,k} \\
 & + \binom{j + k + 1}{2} \mu_{j-1,k}) x_1 x_2^{k-j-1} x_3^{j+1} \\
 = & \lambda_{j,k+1} x_2^{k+1-j} x_3^j \\
 & + (\lambda_{j,k}(k - j) + (j + k + 2)\mu_{j,k} + \binom{j + k + 1}{2} \mu_{j-1,k}) x_1 x_2^{k-j-1} x_3^{j+1}
 \end{aligned}$$

where we used the observation at the beginning of the proof in the final step.

This completes the proof of the formula for  $\Delta^{j+k}(x_1^k)$ . Finally, note that  $\lambda_{j,k} \neq 0$  modulo  $p$  if  $j + k < p$ .  $\square$

We can use this result, along with Lemma 16 to determine the lead monomial of each element of  $T_{n-1}$ : we have

- $LM(\Delta^{n-1}M_{n-1}) = x_3^l$ ;
- $LM(\Delta^{p-1}(P_0)) = x_2^p$ ;
- $LM(\Delta^{p-1}(P_i)) = x_2^{p-i} x_3^{(i-1)/2}$  when  $i$  is odd.

In particular for each  $i < n$  odd or  $i = 0$  we have that

$$\Delta^{p-1}(P_i) \notin A(\Delta^{n-1}(M_{n-1}), \Delta^{p-1}(P_j) : j > i, j \text{ odd}),$$

which is the ideal generated by the elements of  $T_{n-1}$  with degree smaller than the degree of  $\Delta^{p-1}(P_i)$ , since each of these had lead monomial divisible by a larger power of  $x_3$  than  $(i - 1)/2$ . This shows that  $T_{n-1}$  is indeed a minimal generating set.

**References**

[1] Abraham Broer, Jianjun Chuai, Modules of covariants in modular invariant theory, Proc. Lond. Math. Soc. (3) 100 (3) (2010) 705–735.  
 [2] Claude Chevalley, Invariants of finite groups generated by reflections, Am. J. Math. 77 (1955) 778–782.  
 [3] Leonard Eugene Dickson, On Invariants and the Theory of Numbers, Dover Publications, Inc., New York, 1966.  
 [4] Jonathan Elmer, Symmetric powers and modular invariants of elementary abelian  $p$ -groups, J. Algebra 492 (2017) 157–184.  
 [5] Deniz Erdemirci Erkuş, Uğur Madran, On generalized invariants of cyclic groups, J. Pure Appl. Algebra 219 (6) (2015) 2463–2470.  
 [6] J. Hartmann, Transvection free groups and invariants of polynomial tensor exterior algebras, Transform. Groups 6 (2) (2001) 157–164.  
 [7] Julia Hartmann, Anne V. Shepler, Reflection groups and differential forms, Math. Res. Lett. 14 (6) (2007) 955–971.  
 [8] M. Hochster, John A. Eagon, Cohen-Macaulay rings, invariant theory, and the generic perfection of determinantal loci, Am. J. Math. 93 (1971) 1020–1058.  
 [9] Ian Hughes, Gregor Kemper, Symmetric powers of modular representations, Hilbert series and degree bounds, Commun. Algebra 28 (4) (2000) 2059–2088.  
 [10] Barbara R. Peskin, Quotient-singularities and wild  $p$ -cyclic actions, J. Algebra 81 (1) (1983) 72–99.

- [11] R. James Shank, S.A.G.B.I. bases for rings of formal modular seminvariants [semi-invariants], *Comment. Math. Helv.* 73 (4) (1998) 548–565.
- [12] G.C. Shephard, J.A. Todd, Finite unitary reflection groups, *Can. J. Math.* 6 (1954) 274–304.