



# The transfer in modular invariant theory<sup>1</sup>

R. James Shank<sup>a,\*</sup>, David L. Wehlau<sup>a,b</sup>

<sup>a</sup>*Department of Mathematics and Statistics, Queen's University, Kingston, Ont., Canada K7L 3N6*

<sup>b</sup>*Department of Mathematics and Computer Science, Royal Military College, Kingston, Ont., Canada K7K 7B4*

Communicated by A.V. Geramita; received 8 July 1997; received in revised form 29 November 1997

---

## Abstract

We study the transfer homomorphism in modular invariant theory paying particular attention to the image of the transfer which is a proper non-zero ideal in the ring of invariants. We prove that, for a  $p$ -group over  $\mathbf{F}_p$  whose ring of invariants is a polynomial algebra, the image of the transfer is a principal ideal. We compute the image of the transfer for  $SL_n(\mathbf{F}_q)$  and  $GL_n(\mathbf{F}_q)$  showing that both ideals are principal. We prove that, for a permutation group, the image of the transfer is a radical ideal and for a cyclic permutation group the image of the transfer is a prime ideal. © 1999 Elsevier Science B.V. All rights reserved.

MSC: 13A50

---

## 1. Introduction

We let  $V$  be a vector space of dimension  $n$  over a field  $\mathbf{k}$  and we choose a basis,  $\{x_1, \dots, x_n\}$ , for the dual,  $V^*$ , of  $V$ . Consider a finite subgroup  $G$  of  $GL(V)$ . The action of  $G$  on  $V$  induces an action on  $V^*$  which extends to an action by algebra automorphisms on the symmetric algebra of  $V^*$ ,  $\mathbf{k}[V] = \mathbf{k}[x_1, \dots, x_n]$ . Specifically, for  $g \in G$ ,  $f \in \mathbf{k}[V]$  and  $v \in V$ ,  $(g \cdot f)(v) = f(g^{-1} \cdot v)$ . The ring of invariants of  $G$  is the subring of  $\mathbf{k}[V]$  given by

$$\mathbf{k}[V]^G := \{f \in \mathbf{k}[V] \mid g \cdot f = f \text{ for all } g \in G\}.$$

---

\* Corresponding author. E-mail: shank@mast.queensu.ca.

<sup>1</sup> Research partially supported by grants from ARP and NSERC.

The transfer homomorphism is defined by

$$Tr^G : \mathbf{k}[V] \rightarrow \mathbf{k}[V]^G$$

$$f \mapsto \sum_{g \in G} g \cdot f$$

and is a homomorphism of  $\mathbf{k}[V]^G$ -modules. If the order of  $G$  is invertible in  $\mathbf{k}$ , then the Reynolds operator,  $(1/|G|)Tr^G$ , is a projection onto  $\mathbf{k}[V]^G$ . When the characteristic of  $\mathbf{k}$  divides the order of  $G$ , the image of the transfer is a proper, non-zero ideal in  $\mathbf{k}[V]^G$  – see Theorem 2.2 and Remark 5.6.

For each subgroup,  $H$ , of  $G$  there are two factorizations of  $Tr^G$ . Define the relative transfer:

$$Tr_H^G : \mathbf{k}[V]^H \rightarrow \mathbf{k}[V]^G$$

$$f \mapsto \sum_{g \in G/H} g \cdot f$$

Clearly,  $Tr^G = Tr_H^G \circ Tr^H$ . For the second factorization choose a set of right coset representatives for  $H$ , say  $\mathcal{R}$ . Define  $\widehat{Tr}_H^G : \mathbf{k}[V] \rightarrow \mathbf{k}[V]$  by  $\widehat{Tr}_H^G(f) = \sum_{g \in \mathcal{R}} g \cdot f$ . Although  $\widehat{Tr}_H^G$  does depend on the choice of  $\mathcal{R}$ , it is easy to see that, regardless of the choice,  $Tr^H \circ \widehat{Tr}_H^G = Tr^G$ .

Throughout this paper we assume that the characteristic of  $\mathbf{k}$  is  $p$  and that  $p$  divides the order of  $G$ . In other words, this is a paper on modular invariant theory. We use  $I^G$  to denote the image of  $Tr^G$  and  $\mathbf{F}_q$  to denote the field with  $q$  elements. In Section 2 we collect some consequences of the work of Feshbach [8]. In particular we produce a formula for the radical of the image of the transfer. We use this formula in Section 6 to prove that the image of the transfer for a cyclic permutation group is a prime ideal after showing that  $I^G$  is radical for any permutation representation.

One way to construct generators for the image of the transfer is to evaluate the transfer on a set of module generators for  $\mathbf{k}[V]$  as a  $\mathbf{k}[V]^G$ -module. In Section 3 we give sufficient conditions for the existence of a block basis for  $\mathbf{k}[V]$  over certain subalgebras. We use this result to describe module generators for  $\mathbf{k}[V]$  as a  $\mathbf{k}[V]^P$ -module for any  $p$ -group  $P$ . This generating set is used in Section 4 to prove that, for a  $p$ -subgroup of  $GL_n(\mathbf{F}_p)$  whose ring of invariants is a polynomial algebra, the image of the transfer is a principal ideal. We also show that  $I^P$  is a principal ideal for certain examples of  $p$ -subgroups of  $GL_n(\mathbf{F}_q)$ , with  $q = p^s$  and  $s > 1$ , having a polynomial ring of invariants and we give an example of a representation of a  $p$ -group where the ring of invariants is a hypersurface and the image of the transfer is not principal. These results lend support to the following conjecture.

**Conjecture 1.1.** *Suppose that  $P$  is a  $p$ -subgroup of  $GL(V)$ . Then  $\mathbf{k}[V]^P$  is a polynomial algebra if and only if  $I^P$  is a principal ideal.*

For the usual permutation representation of the symmetric group  $\Sigma_p$  over  $\mathbb{F}_p$ , if  $p > 2$  then the image of the transfer is not a principal ideal (see [5, Theorem 9.18]) even though the ring of invariants is a polynomial algebra. (If  $p = 2$  then the image of the transfer is the principal ideal generated by the discriminant (see [5, Theorem 9.17]).) Therefore this conjecture does not extend to arbitrary modular representations.

In Section 5 we relate the image of the transfer for  $G$  with the image of the transfer for its  $p$ -Sylow subgroup. Using this result we show that, for both  $SL_n(\mathbb{F}_q)$  and  $GL_n(\mathbb{F}_q)$ , the image of the transfer is a principal ideal.

We thank Mara Neusel for suggesting the use of the additivity of the  $p$ th power operation to simplify the proof of Theorem 6.1. We also thank Eddy Campbell and Ian Hughes for their assistance and encouragement.

## 2. The radical of the image of the transfer

Suppose  $a$  is an element of some set on which  $G$  acts. The isotropy subgroup of  $a$  is  $G_a := \{g \in G \mid g \cdot a = a\}$  and the orbit of  $a$  is the set  $Ga := \{g \cdot a \mid g \in G\} = \{g \cdot a \mid g \in G/G_a\}$ . Using the action of  $G$  on  $V$  we define the orbit space of  $V$  as  $V/G := \{Gv \mid v \in V\}$ . For  $f \in \mathbf{k}[V]$ , the norm of  $f$ ,  $N(f)$ , is the product of the elements in the orbit of  $f$ . Clearly  $N(f) \in \mathbf{k}[V]^G$ .

When  $\mathbf{k}$  is algebraically closed, the finitely generated Noetherian algebra  $\mathbf{k}[V]^G$  is the ring of regular functions on the affine variety  $V/G$  (see [11, Ch. III Section 12]). When  $\mathbf{k}$  is finite, the elements of  $\mathbf{k}[V]^G$  still represent regular functions on  $V/G$  but distinct polynomials may represent the same function. For example, if  $\mathbf{k} = \mathbb{F}_p$  then  $f$  and  $f^p$  represent the same function.

Let  $\bar{\mathbf{k}}$  denote the algebraic closure of  $\mathbf{k}$  and, for any vector space,  $U$ , over  $\mathbf{k}$ , define  $\bar{U} := U \otimes_{\mathbf{k}} \bar{\mathbf{k}}$ . Extend the action of  $G$  on  $V$  to a linear action of  $G$  on  $\bar{V}$  by defining  $g(v \otimes c) := (g \cdot v) \otimes c$  for  $g \in G$ ,  $v \in V$  and  $c \in \bar{\mathbf{k}}$ . Similarly extend the action of  $G$  on  $\mathbf{k}[V]$  to an action on  $\bar{\mathbf{k}}[\bar{V}]$ . It is not hard to prove that  $\bar{\mathbf{k}}[\bar{V}]^G = (\bar{\mathbf{k}}[\bar{V}])^G = (\bar{\mathbf{k}}[\bar{V}])^G$ . In other words, taking the invariants of a linear representation commutes with extending the field. We will identify  $\mathbf{k}[V]^G$  with the subring  $\mathbf{k}[V]^G \otimes_{\mathbf{k}} \bar{\mathbf{k}} \subseteq \bar{\mathbf{k}}[\bar{V}]^G$ . Using this identification, elements of  $\mathbf{k}[V]^G$  represent regular functions on the  $\bar{V}/G$  and distinct polynomials do represent distinct functions (see [15, Ch. VII Section 3]).

For any subset  $X$  of  $\bar{\mathbf{k}}[\bar{V}]^G$ , let

$$\mathcal{V}(X) := \{Gv \in \bar{V}/G \mid f(v) = 0 \text{ for all } f \in X\}.$$

If  $I$  is an ideal in  $\mathbf{k}[V]^G$  then identifying  $I$  with  $I \otimes_{\mathbf{k}} \bar{\mathbf{k}} \subseteq \bar{\mathbf{k}}[\bar{V}]^G$  allows us to define  $\mathcal{V}(I) \subseteq \bar{V}/G$ . Of course  $\mathcal{V}(\sqrt{I}) = \mathcal{V}(I)$ . By definition  $\bar{I}$  is a vector space over  $\bar{\mathbf{k}}$ . Using the fact that  $I$  is an ideal in  $\mathbf{k}[V]^G$ , it is easy to show that  $\bar{I}$  is an ideal in  $\bar{\mathbf{k}}[\bar{V}]^G$ . Furthermore  $\mathcal{V}(I) = \mathcal{V}(\bar{I})$ . Thus  $\mathcal{V}(I)$  is a subvariety of  $\bar{V}/G$ .

The following result is reasonably well known. We include a proof for completeness.

**Theorem 2.1.**  $\mathcal{V}(I^G) = \{Gv \in \bar{V}/G \mid p \text{ divides } |G_v|\}$ .

**Proof.** Since the transfer is a linear map, the image of  $Tr^G$  applied to  $\overline{\mathbf{k}[V]}$  is  $\overline{I^G}$ . Therefore, since  $\mathcal{V}(I^G) = \mathcal{V}(\overline{I^G})$ , we may assume that  $\mathbf{k} = \overline{\mathbf{k}}$  and  $V = \overline{V}$ .

A point  $G \cdot v \in V/G$  belongs to  $\mathcal{V}(I^G)$  if and only if  $f(v) = 0$  for all  $f \in I^G$ . Therefore we need to show that  $f(v) = 0$  for all  $f \in I^G$  if and only if  $p$  divides  $|G_v|$ . Observe that, for any  $h \in \mathbf{k}[V]$ ,

$$(Tr^{G_v}(h))(v) = \left( \sum_{g \in G_v} g \cdot h \right) (v) = \sum_{g \in G_v} h(g^{-1} \cdot v) = \sum_{g \in G_v} h(v) = |G_v| h(v).$$

Therefore

$$\begin{aligned} (Tr^G(h))(v) &= (Tr^{G_v} \circ \widehat{Tr}_{G_v}^G(h))(v) = Tr^{G_v}(\widehat{Tr}_{G_v}^G(h))(v) \\ &= |G_v| \left( \sum_{g \in G/G_v} g \cdot h \right) (v) = |G_v| \sum_{g \in G/G_v} h(g^{-1} \cdot v). \end{aligned}$$

Thus if  $p$  divides  $|G_v|$ , then  $(Tr^G(h))(v) = 0$ . However, since the orbit  $Gv$  is finite, there exist  $h \in \mathbf{k}[V]$  such that  $h(v)$  is non-zero and  $h(g^{-1} \cdot v) = 0$  for all  $g \notin G_v$ . One such function is given by

$$h = \prod_{\substack{w \in Gv \\ w \neq v}} x_{i(w)} - x_{i(w)}(w),$$

where  $i(w)$  is the least  $i$  such that  $x_i(v) \neq x_i(w)$ . Note that  $h$  is not homogeneous and

$$(Tr^G(h))(v) = |G_v| \sum_{g \in G/G_v} h(g^{-1} \cdot v) = |G_v| h(v).$$

Therefore, if  $p$  does not divide  $|G_v|$ , we conclude that  $(Tr^G(h))(v) \neq 0$ .  $\square$

We remind the reader that the augmentation ideal of  $\mathbf{k}[V]^G$  is the ideal generated by the homogeneous elements of positive degree.

**Theorem 2.2.** *If  $p$  divides the order of  $G$ , then  $I^G$  is a non-zero ideal which is properly contained in the augmentation ideal of  $\mathbf{k}[V]^G$ .*

**Proof.** We first show that  $I^G$  is properly contained in the augmentation ideal. Since  $p$  divides the order of  $G$ , the restriction of the transfer to elements of degree zero is the zero map. Therefore  $I^G$  is a subset of the augmentation ideal. The variety associated to the augmentation ideal is the orbit of the zero vector. On the other hand  $G$  has a non-trivial  $p$ -Sylow subgroup and every representation of a  $p$ -group has a non-zero fixed point  $v \in \overline{V}$ . By Theorem 2.1, the orbit  $Gv$  lies in  $\mathcal{V}(I^G)$ . Therefore the variety of the augmentation ideal is properly contained in  $\mathcal{V}(I^G)$  and, consequently,  $I^G$  is properly contained in the augmentation ideal.

To see that  $I^G$  is non-zero, start by extending the action of  $G$  to the field of fractions  $\mathbf{k}(V)$ . The group acts on  $\mathbf{k}(V)$  by field automorphisms. Since  $G$  is a subgroup

of  $GL(V)$ , the representation of  $G$  is faithful and distinct group elements give distinct field automorphisms. Any set of field automorphisms is linearly independent. Therefore  $Tr^G$  is non-zero on  $\mathbf{k}(V)$ . Thus there are polynomials  $f$  and  $h$  in  $\mathbf{k}[V]$  such that  $Tr^G(f/h)$  is non-zero. However  $N(h)f/h \in \mathbf{k}[V]$  and  $N(h) \in \mathbf{k}[V]^G$ . Therefore  $Tr^G(N(h)f/h) = N(h)Tr^G(f/h)$  is nonzero.  $\square$

We note that, for a non-faithful representation, if the order of the kernel of the representation is divisible by  $p$  then the image of the transfer is the zero ideal.

Following Feshbach in [8], for every  $g \in G$  of order  $p$ , define  $\mathcal{P}_g$  to be the ideal in  $\mathbf{k}[V]$  generated by  $(g - 1)V^*$ . Observe that, since it is generated by homogeneous elements of degree one,  $\mathcal{P}_g$  is a prime ideal. Therefore  $\mathcal{P}_g \cap \mathbf{k}[V]^G$  is also a prime ideal. If  $f$  and  $h$  are in  $\mathbf{k}[V]$ , then  $(g - 1)(f)h = h(g - 1)(f) + (g \cdot f)(g - 1)(h)$ . Hence  $(g - 1)\mathbf{k}[V] \subseteq \mathcal{P}_g$ . We also define  $\mathcal{P}_G = \cap \mathcal{P}_g$  where the intersection runs over all group elements,  $g$ , of order  $p$  in  $G$ .

**Lemma 2.3.** *If  $1 \leq r < p$ , then  $\mathcal{P}_g = \mathcal{P}_{g^r}$ .*

**Proof.** Factoring  $g^r - 1$  as  $(g - 1)(1 + g + \dots + g^{r-1})$  shows that  $(g^r - 1)V^* \subseteq (g - 1)V^*$ . Therefore, since  $\mathcal{P}_{g^r}$  is generated by  $(g^r - 1)V^*$  and  $\mathcal{P}_g$  is generated by  $(g - 1)V^*$ , we have  $\mathcal{P}_{g^r} \subseteq \mathcal{P}_g$ . However,  $g$  generates a subgroup of order  $p$  so, as long as  $g^r$  is not the identity,  $g^r$  is another generator of the same subgroup. Therefore, if  $1 \leq r < p$  then, for some  $m$ ,  $(g^r)^m = g$  and  $\mathcal{P}_g = \mathcal{P}_{(g^r)^m} \subseteq \mathcal{P}_{g^r}$  as required.  $\square$

It follows from Lemma 2.3 that  $\mathcal{P}_g$  depends only on the subgroup generated by  $g$  and  $\mathcal{P}_G$  can be constructed by taking the intersection over subgroups of order  $p$ .

**Theorem 2.4.**  $\sqrt{I^G} = \mathcal{P}_G \cap \mathbf{k}[V]^G$ .

**Proof.** In [8, Theorem 2.4] Feshbach proves that  $I^G \subseteq \mathcal{P}_G \cap \mathbf{k}[V]^G \subseteq \sqrt{I^G}$ . Since  $\mathcal{P}_G \cap \mathbf{k}[V]^G$  is a finite intersection of prime ideals, it is a radical ideal. Therefore  $\sqrt{I^G} = \mathcal{P}_G \cap \mathbf{k}[V]^G$ .  $\square$

**Remark 2.5.** Suppose  $G \cong \mathbf{Z}/p$  and let  $g$  be a generator for  $G$ . Using Lemma 2.3, we see that  $\mathcal{P}_g = \mathcal{P}_G$ . By Theorem 2.4,  $\sqrt{I^G} = \mathcal{P}_G \cap \mathbf{k}[V]^G$ . Therefore  $\sqrt{I^G} = \mathcal{P}_g \cap \mathbf{k}[V]^G$  is a prime ideal. If the representation of  $G$  on  $V$  is indecomposable then the set of fixed points in  $V$ ,  $V^g$ , is a one dimensional subspace and  $\mathcal{P}_g$  is generated by the elements of  $V^*$  which are zero on  $V^g$ . If we choose our basis so that  $V^g$  is the span of the dual of  $x_n$ , then  $\mathcal{P}_g = (x_1, \dots, x_{n-1})$  and  $\sqrt{I^G} = (x_1, \dots, x_{n-1}) \cap \mathbf{k}[V]^G$ .

### 3. Block bases

A homogeneous system of parameters for a graded  $\mathbf{k}$ -algebra  $\mathcal{A}$  is a collection of homogeneous elements,  $\{a_1, \dots, a_n\}$ , such that  $\{a_1, \dots, a_n\}$  is algebraically independent

and  $\mathcal{A}$  is a finitely generated  $\mathbf{k}[a_1, \dots, a_n]$ -module. When  $\mathcal{A} = \mathbf{k}[V]$ , elements of  $\mathcal{A}$  represent regular functions on  $\bar{V} = V \otimes_{\mathbf{k}} \bar{\mathbf{k}}$  and a homogeneous set  $\{a_1, \dots, a_n\}$  is a homogeneous system of parameters if and only if the only common zero of the  $a_i$  is the origin. Also, since  $\mathbf{k}[V]$  is Cohen–Macaulay, if  $\{a_1, \dots, a_n\}$  is a homogeneous system of parameters then  $\mathbf{k}[V]$  is a free  $\mathbf{k}[a_1, \dots, a_n]$ -module and  $a_1, \dots, a_n$  is a regular sequence. For details we refer the reader to [12, Chs. 5 & 6].

Recall that  $\mathbf{k}[V]$  is a finitely generated  $\mathbf{k}[V]^G$ -module and suppose that  $\mathcal{B}$  is a set of module generators for  $\mathbf{k}[V]$  as a  $\mathbf{k}[V]^G$ -module. Since  $Tr^G$  is a map of  $\mathbf{k}[V]^G$ -modules, we can construct a generating set for  $I^G$  by evaluating  $Tr^G$  on  $\mathcal{B}$ . Suppose that  $\{a_1, \dots, a_n\} \subseteq \mathbf{k}[V]^G$  is a homogeneous system of parameters for  $\mathbf{k}[V]$ . Since  $\mathbf{k}[V]$  is Cohen–Macaulay, it is a free  $\mathbf{k}[a_1, \dots, a_n]$ -module. Any basis for  $\mathbf{k}[V]$  over  $\mathbf{k}[a_1, \dots, a_n]$  is a generating set for  $\mathbf{k}[V]$  as a  $\mathbf{k}[V]^G$ -module and can be used to construct a generating set for  $I^G$ . The purpose of this section is to describe certain families of bases, called block bases, which will be used in the later sections to compute the image of the transfer for various examples. A *block basis* is a basis consisting of the monomial factors of a single monomial. The single monomial is called the generator of the block basis. We refer the reader to [5] for a more extensive discussion of block bases.

In the following we make use of the theory of monomial orders. We refer the reader to [6, Ch. 2] for the appropriate definitions and a detailed discussion of monomial orders. We use the convention that a monomial is a product of variables and a term is a monomial with a coefficient.

**Theorem 3.1.** *Suppose that  $\dim_{\mathbf{k}}(V) = n$  and that  $a_1, \dots, a_n$  is a sequence of homogeneous elements in  $\mathbf{k}[V]$ . Further suppose that there exist integers  $d_1, \dots, d_n$  such that, with respect to some monomial order, the lead term of  $a_i$  is  $x_i^{d_i}$  for all  $i$ . Then  $a_1, \dots, a_n$  is a regular sequence in  $\mathbf{k}[V]$  and  $\prod_{i=1}^n x_i^{d_i-1}$  generates a block bases for  $\mathbf{k}[V]$  over  $\mathbf{k}[a_1, \dots, a_n]$ .*

**Proof.** We begin by proving that  $a_1, \dots, a_n$  is a regular sequence. Since  $\mathbf{k}[V]$  is Cohen–Macaulay, it is sufficient to prove that  $a_1, \dots, a_n$  is a homogeneous system of parameters. We prove this by showing that the only common zero of  $a_1, \dots, a_n$  is the origin. We remind the reader that elements of  $\mathbf{k}[V]$  represent functions on  $\bar{V}$ . Without loss of generality we may assume that  $x_1 < x_2 < \dots < x_n$  in the given monomial order. Observe that the multiplicative property of the order implies that for each monomial  $\beta$  appearing in  $a_i$ , other than  $x_i^{d_i}$ , there exists  $j < i$  such that  $x_j$  divides  $\beta$ . In particular,  $a_1$  must equal  $x_1^{d_1}$ . Thus the zero set of  $a_1$  is the hyperplane cut out by  $x_1 = 0$ . The restriction of  $a_2$  to this hyperplane is just  $x_2^{d_2}$ . Therefore the set of common zeros of  $a_1$  and  $a_2$  is the subspace defined by  $x_1 = x_2 = 0$ . Continuing in this fashion we see that the only common zero of  $a_1, \dots, a_n$  is the origin.

We remind the reader that if  $M$  is a graded subspace of  $\mathbf{k}[V]$  and  $M_d$  is the homogeneous component of degree  $d$ , then the *Poincaré series* of  $M$  is

$$P(M, t) = \sum_{i=0}^{\infty} \dim_{\mathbf{k}}(M_d) t^d.$$

Since  $a_1, \dots, a_n$  is a regular sequence,  $\mathbf{k}[a_1, \dots, a_n]$  is a polynomial algebra with Poincaré series  $\prod_{i=1}^n (1 - t^{d_i})^{-1}$ . Therefore the Poincaré series of  $\mathbf{k}[V]/(a_1, \dots, a_n)$  is

$$\prod_{i=1}^n \frac{1 - t^{d_i}}{1 - t}.$$

In particular, the rank of  $\mathbf{k}[V]$  as a free  $\mathbf{k}[a_1, \dots, a_n]$ -module is  $\prod_{i=1}^n d_i$ . This is equal to the number of monomial factors of  $\prod_{i=1}^n x_i^{d_i-1}$ . Thus it suffices to prove that these monomial factors span  $\mathbf{k}[V]$  as a  $\mathbf{k}[a_1, \dots, a_n]$ -module.

Let  $\mathcal{S}$  denote the  $\mathbf{k}[a_1, \dots, a_n]$ -module spanned by the factors of  $\prod_{i=1}^n x_i^{d_i-1}$ . Suppose, by way of contradiction, that  $\mathcal{S}$  is a proper subset of  $\mathbf{k}[V]$ . Choose an element  $f \in \mathbf{k}[V] - \mathcal{S}$  with smallest possible lead monomial. Let  $\beta = x_1^{e_1} \cdots x_n^{e_n}$  be the lead monomial of  $f$  and let  $c\beta$  be the lead term of  $f$ . Note that  $c \neq 0$ . For each  $i$ , write  $e_i = q_i d_i + r_i$  where  $0 \leq r_i < d_i$ . Define

$$f' = f - c \left( \prod_{j=1}^n a_j^{q_j} \right) \left( \prod_{i=1}^n x_i^{r_i} \right).$$

Clearly  $f' \in \mathbf{k}[V] - \mathcal{S}$  and the lead monomial of  $f'$  is less than  $\beta$ , contradicting the choice of  $f$ .  $\square$

**Remark 3.2.** Suppose that the sequence  $a_1, \dots, a_n$  satisfies the hypotheses of Theorem 3.1. Let  $I$  denote the ideal in  $\mathbf{k}[V]$  generated by the sequence and let  $J$  be the ideal generated by  $x_1^{d_1}, \dots, x_n^{d_n}$ . Clearly  $J$  is contained in the lead term ideal of  $I$ . Furthermore, the Poincaré series of  $\mathbf{k}[V]/I$  equals the Poincaré series of  $\mathbf{k}[V]/J$ . Therefore  $J$  is the lead term ideal of  $I$  and  $a_1, \dots, a_n$  is a Gröbner basis for  $I$  (for more on Gröbner bases, see [6]). Also, the block basis generated by  $\prod_{i=1}^n x_i^{d_i-1}$  projects to a  $\mathbf{k}$ -basis for  $\mathbf{k}[V]/I$ . It is not hard to show that  $\mathbf{k}[V]/I$  is a Hodge algebra governed by the ideal of monomials generated by the projections of  $x_1^{d_1}, \dots, x_n^{d_n}$  (for more on Hodge algebras, see [7]).

**Corollary 3.3.** *Suppose that  $P$  is a  $p$ -subgroup of  $GL_n(\mathbf{F}_q)$ . Choose a basis in which  $P$  is an upper-triangular group and let  $p^{m_i}$  be the size of the  $P$ -orbit of  $x_i$ . Then  $N(x_1), \dots, N(x_n)$  is a regular sequence in  $\mathbf{F}_q[V]$  and  $\prod_{i=1}^n x_i^{p^{m_i}-1}$  generates a block basis for  $\mathbf{F}_q[V]$  over  $\mathbf{F}_q[N(x_1), \dots, N(x_n)]$ .*

**Proof.** Using the graded reverse lexicographic order with  $x_1 < x_2 < \dots < x_n$ , we see that the lead monomial of  $N(x_i)$  is  $x_i^{p^{m_i}}$ . Now apply Theorem 3.1.  $\square$

#### 4. Nakajima groups

In [9] Nakajima characterized the representations of  $p$ -groups over  $\mathbf{F}_p$  with polynomial invariants. Nakajima’s characterization prompts us to make the following

definitions. Suppose  $P$  is a  $p$ -subgroup of  $GL_n(\mathbb{F}_q)$  and, for  $1 \leq i \leq n$ , let

$$P_i = \{g \in P \mid g \cdot x_j = x_j \text{ if } j \neq i\}.$$

Clearly the subgroups  $P_i$  depend on the choice of basis.

**Definition 4.1.**  $P$  is a Nakajima group if, for some choice of basis,

- (i)  $P$  is an upper triangular group and
- (ii)  $P = P_n P_{n-1} \cdots P_1$ .

For any Nakajima group  $|P| = \prod_{i=1}^n |P_i|$ . Furthermore, for any  $i$ , the orbit of  $x_i$  under  $P$  is the same as the orbit of  $x_i$  under  $P_i$ . Note that  $P_i$  is an elementary abelian  $p$ -group and the orbit of  $x_i$  is  $\{x_i + u \mid u \in W_i\}$  where  $W_i$  is closed under addition and is a subset of the span of  $\{x_1, \dots, x_{i-1}\}$ . Thus  $W_i$  is vector space over  $\mathbb{F}_p$ . However  $W_i$  not necessarily a vector space over  $\mathbb{F}_q$ . Let  $m_i = \dim_{\mathbb{F}_p}(W_i)$  and observe that the degree of  $N(x_i)$  is  $p^{m_i}$ . Since  $\{N(x_1), \dots, N(x_n)\}$  is a homogeneous system of parameters for both  $\mathbb{F}_q[V]$  and  $\mathbb{F}_q[V]^P$  and the product of the degrees is equal to the order of the group,  $\mathbb{F}_q[V]^P = \mathbb{F}_q[N(x_1), \dots, N(x_n)]$ . Therefore, from Corollary 3.3,  $\prod_{i=1}^n x_i^{p^{m_i}-1}$  generates a block basis for  $\mathbb{F}_q[V]$  as a free  $\mathbb{F}_q[V]^P$ -module.

Nakajima’s characterization is expressed by the following proposition.

**Proposition 4.2** (Nakajima [9, Proposition 4.1]). *Suppose  $P$  is a  $p$ -subgroup of  $GL_n(\mathbb{F}_p)$ . Then  $\mathbb{F}_p[V]^P$  is a polynomial algebra if and only if  $P$  is a Nakajima group.*

Suppose that  $r$  is a non-negative integer. We denote by  $\alpha_p(r)$  the sum of the digits in the  $p$ -adic expansion of  $r$ . Also, if  $W$  is a finite dimensional vector space over a finite field then define  $d(W) := \prod_{u \in W - \{0\}} u$ . We warn the reader that, in the following proposition,  $W$  is a vector space over  $\mathbb{F}_p$  but not necessarily a vector space over  $\mathbb{F}_q$ .

**Proposition 4.3.** *Suppose that  $V$  is a vector space over  $\mathbb{F}_q$  and that  $W$  is a subset of  $V$  which is closed under addition so that  $W$  is a vector space over  $\mathbb{F}_p$ . Let  $m = \dim_{\mathbb{F}_p}(W)$ . Then  $\sum_{u \in W} u^i = 0$  unless  $p - 1$  divides  $i$  and  $\alpha_p(i) \geq m(p - 1)$ . Furthermore,*

$$\sum_{u \in W} u^{p^m-1} = \prod_{u \in W - \{0\}} u = d(W).$$

**Proof.** The proof is a simple generalization of the proof of [5, Proposition 9.5].  $\square$

**Theorem 4.4.** *If  $P$  is a Nakajima group then  $I^P$  is the principal ideal generated by*

$$\prod_{i=1}^n d(W_i).$$

**Proof.** Using Corollary 3.3, we see that the monomial factors of  $\beta = \prod_{i=1}^n x_i^{p^{m_i}-1}$  are a block basis for  $\mathbb{F}_q[V]$  over  $\mathbb{F}_q[V]^P$ . Since  $Tr^P$  is an homomorphism of  $\mathbb{F}_q[V]^P$ -modules,

applying the transfer to the elements of a basis gives a generating set for the image. Consider

$$Tr^P \left( \prod_{i=1}^n x_i^{r_i} \right) = \prod_{i=1}^n \left( \sum_{u \in W_i} (x_i + u)^{r_i} \right),$$

where  $r_i < p^{m_i}$  for each  $i$ . Expanding gives

$$\sum_{u \in W_i} (x_i + u)^{r_i} = \sum_{u \in W_i} \sum_{j=0}^{r_i} \binom{r_i}{j} x_i^{r_i-j} u^j = \sum_{j=0}^{r_i} \binom{r_i}{j} x_i^{r_i-j} \sum_{u \in W_i} u^j.$$

By Proposition 4.3,  $\sum_{u \in W_i} u^j = 0$  unless  $p - 1$  divides  $j$  and  $\alpha_p(j) \geq m_i(p - 1)$ . Since  $j \leq r_i \leq p^{m_i} - 1$ , this expression is zero unless  $j = r_i = p^{m_i} - 1$ . Therefore  $Tr^P(\prod_{i=1}^n x_i^{r_i}) = 0$  unless  $r_i = m_i$  for all  $i$ . Again by Proposition 4.3,

$$Tr^P \left( \prod_{i=1}^n x_i^{m_i} \right) = \prod_{i=1}^n \sum_{u \in W_i} u^{p^{m_i}-1} = \prod_{i=1}^n d(W_i). \quad \square$$

Nakajima’s characterization does not extend to representations of  $p$ -groups over  $\mathbb{F}_q$  for  $q = p^s$  with  $s > 1$ . One of the reasons Nakajima’s characterization does not extend is the fact that  $W_i$  is not necessarily a vector space over  $\mathbb{F}_q$ . Although all Nakajima groups have polynomial invariants, there are  $p$ -groups with polynomial invariants which are not Nakajima groups. One example of such a group is due to Stong (see [13]). We continue our investigation of the relationship between  $G$  and  $I^G$  by computing  $I^G$  for this example. We will use our basis to identify elements of  $G$  with the corresponding matrices and we identify  $V^*$  with the space of column vectors.

**Example 4.5.** Let  $\{1, \omega, v\}$  be a basis for  $\mathbb{F}_{p^3}$  over  $\mathbb{F}_p$ ,

$$T_1 = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad T_2 = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \text{and} \quad T_3 = \begin{pmatrix} 1 & \omega & v \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Let  $G$  be the group generated by  $T_1, T_2$  and  $T_3$ . Then  $G$  is isomorphic to  $(\mathbb{Z}/p)^3$ . Define  $\Gamma := (v^p - v)(x_2^p - x_2x_1^{p-1}) - (\omega^p - \omega)(x_3^p - x_3x_1^{p-1})$  and  $\Lambda := (x_2^p - x_2x_1^{p-1})^p - (\omega^p - \omega)^{p-1}(x_2^p - x_2x_1^{p-1})x_1^{p(p-1)}$ . Note that  $\Gamma$  and  $\Lambda$  are both elements of  $\mathbb{F}_{p^3}[V]^G$ . In the graded reverse lexicographic order, with  $x_1 < x_2 < x_3$ , the lead monomial of  $\Gamma$  is  $x_3^p$  and the lead monomial of  $\Lambda$  is  $x_2^{p^2}$ . Applying Theorem 3.1, we see that  $x_1, \Lambda, \Gamma$  is a regular sequence in  $\mathbb{F}_{p^3}[V]$  and the monomial factors of  $x_2^{p^2-1}x_3^{p-1}$  form a basis for  $\mathbb{F}_{p^3}[V]$  over  $\mathbb{F}_{p^3}[x_1, \Lambda, \Gamma]$ . Thus  $\{x_1, \Lambda, \Gamma\}$  is a homogeneous system of parameters for  $\mathbb{F}_{p^3}[V]^G$  and, since the product of the degrees equals the order of the group, we conclude that  $\mathbb{F}_{p^3}[V]^G = \mathbb{F}_{p^3}[x_1, \Gamma, \Lambda]$  (or see [13]). We will construct a generating set for  $I^G$  by evaluating  $Tr^G$  on the monomial factors of  $x_2^{p^2-1}x_3^{p-1}$ . Let  $H$  be the subgroup generated by  $T_1$  and  $T_2$ . Then  $Tr^G = Tr_H^G \circ Tr^H$ .

$$\begin{aligned} \text{Tr}^H(x_2^i x_3^j) &= \sum_{a,b \in \mathbb{F}_p} (x_2 + ax_1)^i (x_3 + bx_1)^j \\ &= \sum_{m=0}^i \sum_{k=0}^j \binom{i}{m} \binom{j}{k} x_1^{m+k} x_2^{i-m} x_3^{j-k} \sum_{a,b \in \mathbb{F}_p} a^m b^k. \end{aligned}$$

Recall that  $\sum_{c \in \mathbb{F}_p} c^r$  is  $-1$  if  $p - 1$  divides  $r$  and  $r > 0$ ; otherwise this sum zero. Since  $j \leq p - 1$ ,  $\text{Tr}^H(x_2^i x_3^j) = 0$  unless  $j = p - 1$ . Furthermore, when  $j = p - 1$  only the terms with  $k = p - 1$  and  $m$  divisible by  $p - 1$  and  $m > 0$  contribute. Writing  $m = m'(p - 1)$  we have

$$\text{Tr}^H(x_2^i x_3^{p-1}) = \sum_{m'=1}^{p+1} \binom{i}{m'(p-1)} x_1^{(m'+1)(p-1)} x_2^{i-m'(p-1)}.$$

Thus

$$\begin{aligned} \text{Tr}^G(x_2^i x_3^{p-1}) &= \text{Tr}_H^G \circ \text{Tr}^H(x_2^i x_3^{p-1}) \\ &= \sum_{m'=1}^{p+1} \binom{i}{m'(p-1)} x_1^{(m'+1)(p-1)} \sum_{c \in \mathbb{F}_p} (x_2 + c\omega x_1)^{i-m'(p-1)} \\ &= \sum_{m'=1}^{p+1} \binom{i}{m} x_1^{(m'+1)(p-1)} \sum_{c \in \mathbb{F}_p} \sum_{t=0}^{i-m} \binom{i-m}{t} x_2^{i-m-t} c^t \omega^t x_1^t \\ &= \sum_{m'=1}^{p+1} \binom{i}{m} x_1^{(m'+1)(p-1)} \sum_{t=0}^{i-m} \binom{i-m}{t} x_2^{i-m-t} \omega^t x_1^t \sum_{c \in \mathbb{F}_p} c^t. \end{aligned}$$

As above, this simplifies to

$$\begin{aligned} \text{Tr}^G(x_2^i x_3^{p-1}) &= - \sum_{m'=1}^{p+1} \sum_{t'=1}^p \binom{i}{m} \binom{i-m}{t'(p-1)} \\ &\quad \times x_1^{(m'+t'+1)(p-1)} x_2^{i-(m'+t')(p-1)} \omega^{t'(p-1)} \\ &= - \sum_{m'=1}^{p+1} \sum_{t'=1}^p \binom{i}{m'(p-1)} \binom{i-m'(p-1)}{t'(p-1)} \\ &\quad \times x_1^{(m'+t'+1)(p-1)} x_2^{i-(m+t)} \omega^t. \end{aligned}$$

**Lemma 4.6.** *Suppose  $i < p^2 - 1$ ,  $t' > 0$  and  $m' > 0$ . Then*

$$\binom{i}{m'(p-1)} \binom{i-m'(p-1)}{t'(p-1)} \equiv 0 \pmod{p}.$$

**Proof.** We consider the three  $p$ -adic expansions:  $m'(p-1) = (m' - 1)p + (p - m')$ ,  $t'(p-1) = (t' - 1)p + (p - t')$  and  $i = i_1 p + i_0$ . Now if  $\binom{i}{m'(p-1)} \not\equiv 0 \pmod p$  then the  $p$ -adic expansion of  $i - m'(p-1)$  is  $(i_1 - (m' - 1))p + (i_0 - (p - m'))$ . Similarly if  $\binom{i - m'(p-1)}{t'(p-1)} \not\equiv 0 \pmod p$  then the  $p$ -adic expansion of  $i - (m' + t')(p-1)$  is  $(i_1 - (m' - 1) - (t' - 1))p + (i_0 - (p - m') - (p - t'))$ . In particular  $i_1 - (m' - 1) - (t' - 1) \geq 0$  and  $i_0 - (p - m') - (p - t') \geq 0$ . Therefore  $i_1 + i_0 \geq 2(p-1)$ . However, since  $i < p^2 - 1$ ,  $i_1 + i_0 < 2(p-1)$ .  $\square$

Therefore, if  $Tr^G(x_2^i x_3^j)$  is non-zero, then  $i = p^2 - 1$ ,  $j = p - 1$  and

$$Tr^G(x_2^{p^2-1} x_3^{p-1}) = - \sum_{m'=1}^{p+1} \sum_{t'=1}^p \binom{p^2-1}{m'} \binom{p^2-1-m}{t'} x_1^{(m'+t'+1)(p-1)} x_2^{p^2-1-(m+t)} \omega^t.$$

However, if  $m = p^2 - 1$  then, since  $t > 0$ ,  $\binom{p^2-1-m}{t} = 0$ . Thus we may assume that  $m < p^2 - 1$ . If  $\binom{p^2-1-m}{t} = \binom{p^2-1-m'(p-1)}{t'(p-1)}$  is non-zero then the  $p$ -adic expansion of  $p^2 - 1 - m'(p-1) - t'(p-1)$  is  $(p - m' - t' + 1)p + (m' - 1 - p + t')$ . Therefore  $p - m' - t' + 1 \geq 0$  and  $m' - 1 - p + t' \geq 0$ . Thus  $m' + t' = p + 1$  and  $\binom{p^2-1-m'(p-1)}{t'(p-1)} = 1$ . Furthermore,

$$\begin{aligned} \binom{p^2-1}{m} &= \binom{p^2-1}{m'(p-1)} = \binom{p-1}{m'-1} \binom{p-1}{p-m'} \\ &= (-1)^{m'-1} (-1)^{p-m'} = (-1)^{p-1} = 1. \end{aligned}$$

Therefore,

$$\begin{aligned} Tr^G(x_2^{p^2-1} x_3^{p-1}) &= (-1) x_1^{(p+2)(p-1)} \sum_{t'=1}^p \omega^{t'(p-1)} \\ &= (-1) x_1^{(p+2)(p-1)} \frac{\omega^{p-1} (\omega^{p^2-p} - 1)}{\omega^{p-1} - 1}. \end{aligned}$$

Observe that  $\omega$  is not in  $\mathbf{F}_p$  and therefore  $\omega^{p-1} \neq 1$ . Furthermore, since  $\mathbf{F}_{p^3}$  has no non-trivial  $p$ th roots of unity,  $(\omega^{p-1})^p \neq 1$  and the coefficient in the above expression is non-zero. Note that this also follows from the fact that  $Tr^G$  is never the zero map.

In conclusion,  $I^G$  is the principal ideal generated by  $x_1^{p^2+p-2}$

We include the following example to illustrate the fact that, for a  $p$ -group whose ring of invariants is a hypersurface, the image of the transfer is not always a principal ideal.

**Example 4.7.** For simplicity we restrict our attention to  $p = 2$  but similar examples exist for all primes. Let

$$\sigma = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad \text{and} \quad \tau = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Let  $G = \langle \sigma, \tau \rangle$  and  $H = \langle \sigma\tau \rangle$ . Clearly  $G \cong \mathbf{Z}/2 \times \mathbf{Z}/2$  and  $H \cong \mathbf{Z}/2$ . Furthermore  $G$  is a Nakajima group and  $\mathbf{F}_2[V]^G = \mathbf{F}_2[x_1, N(x_2), x_3, N(x_4)]$ . From Theorem 4.4,  $I^G$  is the principal ideal generated by  $x_1x_3$ .  $H$  is a subgroup of index 2 in the Nakajima group  $G$ . Applying [4, Theorem 4.4] we see that  $\mathbf{F}_2[V]^H$  is a free  $\mathbf{F}_2[V]^G$ -module with basis  $\{1, a\}$  where  $a = x_1x_4 + x_2x_3$ . In other words  $\mathbf{F}_2[V]^H$  is a hypersurface. We wish to describe  $I^H$ . Note that  $Tr^H$  is a homomorphism of  $\mathbf{F}_2[V]^G$ -modules and that  $\mathbf{F}_2[V]$  is a free  $\mathbf{F}_2[V]^G$ -module with a block basis generated by  $x_2x_4$ . Therefore  $I^H$  is generated by  $Tr^H(x_2) = x_1$ ,  $Tr^H(x_4) = x_3$  and  $Tr^H(x_2x_4) = x_1x_4 + x_2x_3 = a$ . In particular  $I^H$  is not a principal ideal.

### 5. The $p$ -Sylow transfer

In this section we consider the relationship between the image of the transfer for  $G$  and the image of the transfer for a  $p$ -Sylow subgroup of  $G$ . Our starting point is the following theorem.

**Theorem 5.1.** *If  $p$  does not divide  $[G : H]$ , then  $I^G = I^H \cap \mathbf{k}[V]^G$ .*

**Proof.** We first show that  $I^H \cap \mathbf{k}[V]^G \subseteq I^G$ . Suppose that  $f \in I^H \cap \mathbf{k}[V]^G$  and  $Tr^H(k) = f$ . Then  $Tr_H^G(f) = [G : H]f$  and therefore  $Tr^G(k/[G : H]) = f$ .

In order to show that  $I^G \subseteq I^H \cap \mathbf{k}[V]^G$ , we use the factorization  $Tr^G = Tr^H \circ \widehat{Tr}_H^G$ . Suppose that  $f \in I^G \subset \mathbf{k}[V]^G$ . Therefore  $f = Tr^G(k)$  for some  $k \in \mathbf{k}[V]$  and thus  $f = Tr^H(\widehat{Tr}_H^G(k)) \in I^H$ .  $\square$

The height of a prime ideal  $\mathcal{P}$  is the length of a maximal chain, with respect to inclusion, of prime ideals contained in  $\mathcal{P}$ . The height of an arbitrary ideal  $I$  is the minimal height of a prime ideal containing  $I$ . We denote the height of  $I$  by  $ht(I)$  and we refer the reader to [3, Appendix] for details.

**Corollary 5.2.** *If  $P$  is the the  $p$ -Sylow subgroup of  $G$ , then  $ht(I^G) = ht(I^P)$ .*

**Proof.** Since  $\mathbf{k}[V]^P$  is integral over  $\mathbf{k}[V]^G$ , we have both “going up” and “going down” (see, e.g., [2, Theorem 1.4.4]). From Theorem 5.1,  $I^P$  lies over  $I^G$  and thus they have the same height.  $\square$

We now use Theorem 5.1 to compute the image of the transfer for  $SL_n(\mathbb{F}_q)$ . A  $p$ -Sylow subgroup for both  $SL_n(\mathbb{F}_q)$  and  $GL_n(\mathbb{F}_q)$  is given by  $U_n(\mathbb{F}_q)$ , the group of upper triangular matrices with 1's along the diagonal. Clearly  $U_n(\mathbb{F}_q)$  is a Nakajima group (see Section 4) and  $\mathbb{F}_q[V]^{U_n(\mathbb{F}_q)}$  is the polynomial algebra  $\mathbb{F}_q[h_1, \dots, h_n]$  where  $h_i = N_{U_n(\mathbb{F}_q)}(x_i)$  has degree  $q^{i-1}$ . The ring of invariants for  $GL_n(\mathbb{F}_q)$ , known as the Dickson algebra, is the polynomial algebra  $\mathbb{F}_q[d_{1,n}, d_{2,n}, \dots, d_{n,n}]$  where  $d_{i,n}$  has degree  $q^n - q^{n-i}$ . We refer the reader to [12, Section 8.1] for a detailed discussion of the Dickson algebra. Finally, choose a non-zero representative from each line in  $V^*$  and take the product to form  $L \in \mathbb{F}_q[V]$ . It is well known that  $L^{q-1} = d_{n,n}$  and  $\mathbb{F}_q[V]^{SL_n(\mathbb{F}_q)} = \mathbb{F}_q[d_{1,n}, \dots, d_{n-1,n}, L]$  (again, see [12, Section 8.1]).

**Theorem 5.3.** *The image of  $Tr^{SL_n(\mathbb{F}_q)}$  is the the principal ideal generated by  $L^{(q-1)(n-1)}$ .*

**Proof.** From Theorem 5.1,  $I^{SL_n(\mathbb{F}_q)} = I^{U_n(\mathbb{F}_q)} \cap \mathbb{F}_q[V]^{SL_n(\mathbb{F}_q)}$ . By [5, Corollary 9.7] or Theorem 4.4,  $I^{U_n(\mathbb{F}_q)}$  is the principal ideal generated by  $(h_1^{n-1}h_2^{n-2} \dots h_{n-1})^{q-1}$ . Suppose that  $f \in I^{SL_n(\mathbb{F}_q)} = I^{U_n(\mathbb{F}_q)} \cap \mathbb{F}_q[V]^{SL_n(\mathbb{F}_q)}$ . Therefore  $f = h \cdot (h_1^{n-1}h_2^{n-2} \dots h_{n-1})^{q-1}$  for some  $h \in \mathbb{F}_q[V]^{U_n(\mathbb{F}_q)}$ . Since  $h_1 = x_1$ , we see that  $x_1^{(q-1)(n-1)}$  divides  $f$ . Suppose that  $\ell$  is a non-zero linear functional. Clearly  $\ell$  is in the  $SL_n(\mathbb{F}_q)$ -orbit of  $x_1$ . Because  $f$  is an  $SL_n(\mathbb{F}_q)$ -invariant and  $x_1^{(q-1)(n-1)}$  divides  $f$ , it follows that  $\ell^{(q-1)(n-1)}$  divides  $f$ . Since  $x_1^{q-1} = -\prod_{c \in \mathbb{F}_q - \{0\}} cx_1$  and  $d_{n,n}$  is the product of all non-zero linear functionals, we conclude that  $d_{n,n}^{n-1}$  divides  $f$ . In  $\mathbb{F}_q[V]^{SL_n(\mathbb{F}_q)}$ ,  $d_{n,n} = L^{q-1}$ . Thus  $f = L^{(q-1)(n-1)}k$  for some  $k \in \mathbb{F}_q[V]$ . Clearly  $k \in \mathbb{F}_q[V]^{SL_n(\mathbb{F}_q)}$ . Finally, since  $d_{n,n} = (-1)^n(h_1 \dots h_n)^{q-1}$  and  $L^{(q-1)(n-1)} = d_{n,n}^{n-1}$  we see that  $L^{(q-1)(n-1)} \in I^{U_n(\mathbb{F}_q)} \cap \mathbb{F}_q[V]^{SL_n(\mathbb{F}_q)} = I^{SL_n(\mathbb{F}_q)}$ .  $\square$

**Remark 5.4.** Suppose  $G$  is a subgroup of  $GL_n(\mathbb{F}_q)$  and  $G$  contains  $SL_n(\mathbb{F}_q)$ . Then there exists an  $m$  dividing  $q - 1$  such that  $G = \{g \in GL_n(\mathbb{F}_q) \mid (\det g)^m = 1\}$ . It is easy to see that  $L^m$  is  $G$ -invariant and that  $\mathbb{F}_p[V]^G$  is a polynomial algebra. Furthermore the proof of Theorem 5.3 shows that  $I^G$  is the principal ideal generated by  $(L^m)^{(n-1)(q-1)/m}$ .

In particular this gives us a simpler proof of [5, Corollary 9.14].

**Theorem 5.5.** *The image of  $Tr^{GL_n(\mathbb{F}_q)}$  is the the principal ideal generated by  $d_{n,n}^{n-1}$ .*

**Remark 5.6.** For any modular representation of a finite group  $G$  over  $\mathbf{k} \subseteq \overline{\mathbb{F}_p}$ , there exists a  $q$  such that  $G \leq GL_n(\mathbb{F}_q)$ . Since,  $Tr^{GL_n(\mathbb{F}_q)} = Tr_G^{GL_n(\mathbb{F}_q)} \circ Tr^G$ , the kernel of  $Tr^G$  is a subset of the kernel of  $Tr^{GL_n(\mathbb{F}_q)}$ . Using the other factorization,  $Tr^{GL_n(\mathbb{F}_q)} = Tr^G \circ \widehat{Tr}_G^{GL_n(\mathbb{F}_q)}$ , we see that  $I^{GL_n(\mathbb{F}_q)} \subseteq I^G$ . In particular  $d_{n,n}^{n-1} \in I^G$  and  $Tr^G$  is non-zero.

### 6. Permutation groups

In this section we consider groups which act by permuting a fixed basis of  $V$ . We will call such groups permutation groups. For a monomial  $\beta$  we denote the orbit sum of  $\beta$  by  $\vartheta s(\beta) = \sum_{g \in G/G_\beta} g \cdot \beta$ . It is well known that, for a permutation group, the

orbit sums of monomials form a vector space basis for the ring of invariants. Since  $Tr^G(\beta) = |G_\beta| \vartheta s(\beta)$ , the set  $\{\vartheta s(\beta) \mid p \text{ does not divide } |G_\beta|\}$  forms a vector space basis for  $I^G$ . In particular  $\vartheta s(\beta) \in I^G$  if and only if  $p$  does not divide  $|G_\beta|$ . Therefore if  $f \in I^G$  then  $f$  is a linear combination of orbit sums each of which is contained in  $I^G$ .

**Theorem 6.1.** *Suppose that  $G$  is a permutation group. Then  $I^G$  is a radical ideal and  $I^G = \mathcal{P}_G \cap \mathbf{k}[V]^G$ .*

**Proof.** Suppose  $f^r \in I^G$ . Write  $f = \sum_{i=1}^t c_i \vartheta s(\beta_i)$  where  $c_i \in \mathbf{k}$  and each  $\beta_i$  is a monomial. Choose  $m$  so that  $p^m \geq r$ . Then  $f^{p^m} \in I^G$ . However,

$$f^{p^m} = \left( \sum_{i=1}^t c_i \vartheta s(\beta_i) \right)^{p^m} = \sum_{i=1}^t c_i^{p^m} \vartheta s(\beta_i^{p^m}).$$

Therefore for each  $i$ ,  $\vartheta s(\beta_i^{p^m}) \in I^G$ . Thus  $p$  does not divide the order of  $G_{\beta_i^{p^m}}$ . However  $G_{\beta_i} = G_{\beta_i^{p^m}}$ . Hence, for each  $i$ ,  $\vartheta s(\beta_i) \in I^G$  and therefore  $f \in I^G$ . Thus  $I^G$  is radical and, by Theorem 2.4,  $I^G = \mathcal{P}_G \cap \mathbf{k}[V]^G$ .  $\square$

As a corollary we obtain the following generalization of recent results of Neusel [10] and Smith [14].

**Corollary 6.2.** *If  $G$  is a cyclic permutation group, then  $I^G$  is a prime ideal.*

**Proof.** If  $G$  is non-modular then the transfer is surjective and  $I^G$  is prime. If  $p$  divides the order of  $G$  then there is a unique subgroup of  $G$  with order  $p$ . Let  $g$  be a generator for this subgroup. Using Lemma 2.3, we see that  $\mathcal{P}_g = \mathcal{P}_G$ . By Theorem 2.4,  $\sqrt{I^G} = \mathcal{P}_G \cap \mathbf{k}[V]^G$ . By Theorem 6.1,  $I^G = \sqrt{I^G}$ . Therefore  $I^G = \mathcal{P}_g \cap \mathbf{k}[V]^G$  is a prime ideal.  $\square$

We return briefly to Example 4.7. In this example, after a change of basis, both  $G$  and  $H$  are permutation groups.  $H$  is a cyclic permutation group and  $I^H$  is the prime ideal generated by  $x_1, x_3$  and  $x_1x_4 + x_2x_3$ .  $G$  is isomorphic to  $\mathbf{Z}/2 \times \mathbf{Z}/2$  and  $I^G$  is generated by  $x_1x_3$ . In particular  $I^G$  is radical but not prime.

## References

- [1] A. Adem, R.J. Milgram, Cohomology of Finite Groups, Springer, New York, 1994.
- [2] D.J. Benson, Polynomial Invariants of Finite Groups, Lecture Note Series, vol. 190, Cambridge University Press, London, 1993.
- [3] W. Bruns, J. Herzog, Cohen–Macaulay Rings, Cambridge Studies in Adv. Math., vol. 39, Cambridge University Press, Cambridge, 1993.
- [4] H.E.A. Campbell, I.P. Hughes, Rings of invariants of certain  $p$ -groups over the field  $\mathbf{F}_p$ , J. Alg., to appear.
- [5] H.E.A. Campbell, I.P. Hughes, R.J. Shank, D.L. Wehlau, Bases for rings of coinvariants, Transformation Groups 1 (4) (1996) 307–336.

- [6] D. Cox, J. Little, D. O’Shea, *Ideals, Varieties, and Algorithms*, Springer, New York, 1992.
- [7] C. DeConcini, D. Eisenbud, C. Procesi, *Hodge Algebras*, *Astérisque* 91, Société Mathématique de France, 1982.
- [8] M. Feshbach,  $p$ -Subgroups of compact Lie groups and torsion of infinite height in  $H^*(BG)$ , II, *Mich. Math. J.* 29 (1982) 299–306.
- [9] H. Nakajima, Regular rings of invariants of unipotent groups, *J. Algebra* 85 (1983) 253–286.
- [10] M. Neusel, The transfer in the invariant theory of modular permutation representations, preprint, 1997.
- [11] J.P. Serre, *Algebraic Groups and Class Fields*, Springer, New York, 1988.
- [12] L. Smith, *Polynomial Invariants of Finite Groups*, A.K. Peters, Wellesley, MA, 1995.
- [13] L. Smith, Modular representations of  $q$ -groups with regular rings of invariants, preprint, 1996.
- [14] L. Smith, Modular vector invariants of cyclic permutation representations, preprint, 1997.
- [15] O. Zariski, P. Samuel, *Commutative Algebra*, vol. II, Springer, New York, 1960.