J. Symbolic Computation (2002) **34**, 307–327
doi:10.1006/jsco.2002.0558
Available online at http://www.idealibrary.com on IDEAL®

Computing Modular Invariants of *p*-groups

R. JAMES SHANK[†§] AND DAVID L. WEHLAU[‡¶]

[†] *Institute of Mathematics & Statistics, University of Kent at Canterbury, CT2 7NF, U.K.*
[‡] *Department of Mathematics & Computer Science, Royal Military College, Kingston, Ontario, Canada K7K 7B4*

Let V be a finite dimensional representation of a p-group, G, over a field, $\mathbf{k}$, of characteristic p. We show that there exists a choice of basis and monomial order for which the ring of invariants, $\mathbf{k}[V]^G$, has a finite SAGBI basis. We describe two algorithms for constructing a generating set for $\mathbf{k}[V]^G$. We use these methods to analyse $\mathbf{k}[2V_3]^{U_3}$ where U_3 is the p-Sylow subgroup of $\mathrm{GL}_3(\mathbf{F}_p)$ and $2V_3$ is the sum of two copies of the canonical representation. We give a generating set for $\mathbf{k}[2V_3]^{U_3}$ for $p = 3$ and prove that the invariants fail to be Cohen–Macaulay for $p > 2$. We also give a minimal generating set for $\mathbf{k}[mV_2]^{\mathbf{Z}/p}$ were V_2 is the two-dimensional indecomposable representation of the cyclic group $\mathbf{Z}/p$.

1. Introduction

Let V be a finite dimensional vector space over a field $\mathbf{k}$. We choose a basis, $\{x_1, \ldots, x_n\}$, for the dual, V^*, of V. Consider a 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^*, $S = \mathbf{k}[x_1, \ldots, x_n]$. Specifically, for $g \in G$, $f \in S$ and $v \in V$, $(g \cdot f)(v) = f(g^{-1} \cdot v)$. The ring of invariants of G is the subring of S given by

$$S^G := \{f \in S \mid g \cdot f = f \text{ for all } g \in G\}.$$

For an introduction to the invariant theory of finite groups see Benson (1993) or Smith (1995).

If G is a finite group and $|G|$ is not invertible in $\mathbf{k}$ then we say the representation of G on V is *modular*. If $|G|$ is invertible in $\mathbf{k}$ then V is called a *non-modular* representation. Noether (1916, 1926) proved that S^G is always a finitely generated algebra. In Noether (1916) she showed that if the characteristic of $\mathbf{k}$ is zero then S^G is always generated by the invariant polynomials in S of degree less than or equal to $|G|$. Recently this result has been extended independently by Fleischmann (2000) and Fogarty (2001) to the general case of a non-modular representation. The result does not hold for modular representations. In fact, as illustrated by the vector invariants of the regular representation of $\mathbf{Z}/2$ over a field of characteristic 2 (see Richman, 1990 or Campbell and Hughes, 1997), no function

[§] E-mail: R.J.Shank@ukc.ac.uk
[¶] E-mail: wehlau@rmc.ca

0747–7171/02/050307 + 21 $35.00/0

depending solely on the order of the group can serve as an upper bound on the degrees of the generators.

The central problem of invariant theory is to find generators for the algebra S^G. In practice, this problem is much harder in the modular setting. In this paper we describe various methods for computing generators of S^G for modular representations. We especially consider the case where G is a p-group and $\mathbf{k}$ is a field of characteristic p.

A SAGBI basis for a subalgebra of S is the analog of a Gröbner basis and as such is a particularly nice generating set. SAGBI bases were introduced independently by Robbiano and Sweedler (1990) and Kapur and Madlener (1989). Unfortunately, even a finitely generated subalgebra does not necessarily have a finite SAGBI basis. In fact even the ring of invariants of a finite group may fail to have a SAGBI basis (see Göbel, 1995, Lemma 2.1; Göbel, 1998 or Sturmfels, 1996, Example 11.2). The characterization of subalgebras which admit a finite SAGBI basis is an important open problem. In Section 3 we show that for any representation of a p-group over a field of characteristics p, there is a choice of basis and monomial order for which the ring of invariants has a finite SAGBI basis. In fact our result applies to any triangular representation.

In Section 5 we give a number of criteria for determining whether an algebra consisting of invariants is in fact the entire ring of invariants S^G. We also give an algorithm for constructing a generating set for the ring of invariants of a p-group or, more generally, a triangular representation. The algorithm makes use of the theory of SAGBI bases, in particular the computation of syzygy modules for subalgebras, and exploits the fact that S^G is integrally closed.

Suppose that $N \lhd G$ is a normal subgroup of G. Then G acts on $\mathbf{k}[V]^N$ and $\mathbf{k}[V]^G = (\mathbf{k}[V]^N)^G = (\mathbf{k}[V]^N)^{G/N}$. Thus we may reduce the problem of computing S^G to two smaller problems: computing invariants first under the subgroup N and then under the quotient group G/N. However computing the G/N-invariants is considerably complicated by the fact that the algebra, $\mathbf{k}[V]^N$, on which G/N is acting is not, in general, a polynomial ring. One solution to this difficulty is to construct a G/N-module W together with a G/N-equivariant surjection $\rho : \mathbf{k}[W] \to S^N$. In the non-modular case the restriction of this homomorphism is a surjection $\rho^G : \mathbf{k}[W]^{G/N} \to S^G$. For non-modular representations this technique, called a ladder, is one of the most effective for computing rings of invariants (see, for example, Wehlau, 1993). However, in the modular setting the induced map ρ^G is not, in general, surjective. In Section 7 we describe how group cohomology may be used to overcome this difficulty. If G is a p-group this provides a method to compute S^G by computing the $\mathbf{Z}/p$-invariants of a number of $\mathbf{Z}/p$-representations together with a number of group cohomology computations. In particular, one must be able to compute rings of invariants for modular $\mathbf{Z}/p$-representations.

Attempts to apply the ladder technique to modular representations of p-groups emphasize the importance of being able to construct manageable generating sets for rings of invariants for representations of $\mathbf{Z}/p$. However, for most such representations, this is quite difficult. Hughes and Kemper (2002) have given an upper bound on the degrees of the generators for any representation of $\mathbf{Z}/p$. Therefore by taking all homogeneous invariants with degree less than or equal to the upper bound we do get a finite generating set. However such generating sets are far from manageable. Throughout the paper we use V_n, for $n \leq p$, to denote the unique indecomposable modular representation of $\mathbf{Z}/p$ with dimension n. Minimal generating sets for $\mathbf{k}[V_2]^{\mathbf{Z}/p}$ and $\mathbf{k}[V_3]^{\mathbf{Z}/p}$ can be found in Dickson's Madison Colloquium (Dickson, 1966). Finite SAGBI bases for $\mathbf{k}[V_4]^{\mathbf{Z}/p}$ and $\mathbf{k}[V_5]^{\mathbf{Z}/p}$ can be found in Shank (1998). The problem of finding a nice generating set for

$\mathbf{k}[V_n]^{\mathbf{Z}/p}$ for $n > 5$ remains open. Even when the invariants of the indecomposable summands are understood, it can be difficult to construct generating sets for decomposable representations. Campbell and Hughes (1997) manage to describe a generating set for $\mathbf{k}[mV_2]^{\mathbf{Z}/p}$. In Section 4 we refine their solution giving a minimal generating set for this ring. This result is used in Section 8. For the special case of $p = 2$, every representation is of the form $mV_2 \oplus \ell V_1$. Since $\mathbf{k}[mV_2 \oplus \ell V_1]^{\mathbf{Z}/p} = \mathbf{k}[mV_2]^{\mathbf{Z}/p} \otimes \mathbf{k}[\ell V_1]$, we therefore obtain a minimal generating set for the ring of invariants of every finite dimensional modular representation of $\mathbf{Z}/2$.

Suppose that R is a graded subalgebra of S and M is an R-module. Let R_+ denote the augmentation ideal of R, i.e. the ideal generated by the homogeneous elements of positive degree. A sequence of homogeneous elements $h_1, \ldots, h_k$ in R_+ is *regular* on M if, for each $i \leq k$, h_i is not a zero-divisor on $M/(h_1, \ldots, h_{i-1})M$. The *depth* of M is the length of the longest regular sequence on M. The depth of a ring is bounded above by its Krull dimension. A ring is *Cohen–Macaulay* if the depth equals the dimension. For a detailed discussion of depth and dimension see Eisenbud (1996). For a non-modular representation, the ring of invariants is always Cohen–Macaulay. However, when the characteristic of $\mathbf{k}$ divides the order of the group, the invariants often fail to be Cohen–Macaulay. Characterizing the modular representations which have a Cohen–Macaulay ring of invariants is an interesting and important problem. Kemper (1999) proved that if G is a p-group and S^G is Cohen–Macaulay then G is generated by a set of bi-reflections, i.e. by elements which fix pointwise a subspace of codimension 1 or 2. In particular, this means that if $\mathbf{k}[V \oplus V]^G$ is Cohen–Macaulay then the action of G on V must be generated by reflections, i.e. by elements which fix pointwise a subspace of codimension 1. In Section 8 we analyze the invariants of U_3, the p-Sylow subgroup of $\mathrm{GL}_3(\mathbf{F}_p)$, acting on $V_3 \oplus V_3$. The action of U_3 on V_3 is generated by reflections and the ring of invariants is a polynomial algebra, i.e. there are no relations among the generators. Therefore $\mathbf{k}[2V_3]^{U_3}$ passes Kemper's criteria and could be Cohen–Macaulay. In fact, for $p = 2$, the invariant ring is Cohen–Macaulay. However, using the ladder technique, we are able to show that for $p > 2$ the invariants fail to be Cohen–Macaulay.

2. Preliminaries

The *transfer* is defined by:

$$\begin{array}{rccc} Tr^G: & \mathbf{k}[V] & \longrightarrow & \mathbf{k}[V]^G \\ & f & \longmapsto & \displaystyle\sum_{g \in G} g \cdot f \end{array}$$

and is a homomorphism of $\mathbf{k}[V]^G$-modules. For non-modular representations, Tr^G is surjective. For modular representations, the image of the transfer, $\mathrm{Im}\,\mathrm{Tr}^G$, is a proper non-zero ideal of $\mathbf{k}[V]^G$. For proofs of this fact and other general properties of the modular transfer see Shank and Wehlau (1999).

If a is an element of a set on which the finite group G acts, we write $G \cdot a = \{g \cdot a \mid g \in G\}$ for the G orbit of a. For $f \in \mathbf{k}[V]$, we define the *norm* of f by $N_G(f) = N(f) = \prod_{h \in G \cdot f} h$.

We will consider representations of $\mathbf{Z}/p$, the cyclic group of order p, in some detail. Let σ denote a fixed generator of $\mathbf{Z}/p$. Define $\Delta := \sigma - 1$ and $\mathrm{Tr} := \sum_{i=1}^{p} \sigma^i$ in the group ring of $\mathbf{Z}/p$. There are exactly p distinct inequivalent indecomposable representations of $\mathbf{Z}/p$, one of each dimension $1, 2, \ldots, p$. We will denote the indecomposable representation

of $\mathbf{Z}/p$ of dimension n by V_n. There exists a basis, $\{e_1, \ldots, e_p\}$, of V_p, with $\Delta e_1 = 0$ and, for $i > 1$, $\Delta e_i = e_{i-1}$. The vector space spanned by $\{e_1, \ldots, e_n\}$ is a $\mathbf{Z}/p$-submodule isomorphic to V_n. There are $\mathbf{Z}/p$-equivariant inclusions: $V_1 \subset V_2 \subset \cdots \subset V_p$, and $V_n^{\mathbf{Z}/p}$ is isomorphic to V_1.

Consider the vector space of linear functionals V_n^*. Since V_n^* is an indecomposable $\mathbf{Z}/p$-module, V_n^* and V_n are isomorphic. We will call an element, z, of V_n^* a *distinguished variable* for V_n if z is a generator of the cyclic $\mathbf{Z}/p$-module V_n^*. Equivalently z is a distinguished variable if z restricted to ${V_n}^{\mathbf{Z}/p}$ is not identically zero. For any distinguished variable z there is a *triangular basis*, $\{z, \Delta z, \Delta^2 z, \ldots, \Delta^{n-1} z\}$, of V_n^*. For any $f \in \mathbf{k}[V_n]$, let $\deg_z(f)$ denote the degree of f as a polynomial in z with coefficients in $\mathbf{k}[\Delta z, \Delta^2 z, \ldots, \Delta^{n-1} z]$. The special property of the distinguished variable z, and the corresponding triangular basis, which we will exploit, is the fact that $\deg_z(\sigma(f)) = \deg_z(f)$.

Consider a $\mathbf{Z}/p$-module W. Decompose W into a direct sum of indecomposable $\mathbf{Z}/p$-summands:

$$W = \bigoplus_{i=1}^{t} W_i$$

where $W_i \cong V_{\dim(W_i)}$ for all i. For each i choose a distinguished variable $z_i \in W_i^*$ and use the corresponding triangular basis for W_i^*. Let N_i denote the norm of z_i. Thus $N_i = z_i$ if $W_i \cong V_1$ and $N_i := \prod_{j=1}^{p} \sigma^j(z_i)$, otherwise.

Let $f \in \mathbf{k}[W]^{\mathbf{Z}/p}$. Since N_1, considered as a polynomial in z_1, is monic we may divide N_1 into f to obtain the unique decomposition $f = f_1 N_1 + r_1$ where the remainder r_1 has degree at most $p-1$ in the variable z_1. Next we divide r_1 by N_2 to obtain a decomposition: $f = f_1 N_1 + f_2 N_2 + r_2$ where $\deg_{z_1}(f_2) < p$, $\deg_{z_1}(r_2) < p$ and $\deg_{z_2}(r_2) < p$. Continuing in this manner we obtain a decomposition

$$f = f_1 N_1 + f_2 N_2 + \cdots + f_t N_t + r$$

where $\deg_{z_i}(f_j) < p$ for all $i < j$ and $\deg_{z_i}(r) < p$ for all i. Note that r is the normal form of f with respect to the Gröbner basis $\{N_1, N_2, \ldots, N_t\}$ of the ideal $(N_1, N_2, \ldots, N_t)\mathbf{k}[W]$. Furthermore the decomposition $f = f_1 N_1 + f_2 N_2 + \cdots + f_t N_t + r$ is a normal decomposition of f with respect to this Gröbner basis. We will call this the *norm decomposition* of f. Note that the norm decomposition depends upon the choice of the z_i but is otherwise unique.

Let $\mathbf{k}[W]^\flat := \{r \in \mathbf{k}[W] \mid \deg_{z_i}(r) < p \text{ for all } i = 1, 2, \ldots, t\}$. Thus $\mathbf{k}[W]^\flat$ is the set of functions f having all coefficients $f_i = 0$ in its norm decomposition. Note that $\mathbf{k}[W]^\flat$ is $\mathbf{Z}/p$-stable.

The ring $\mathbf{k}[W]$ has a multi-grading given by the degrees in each W_i, that is, induced by $\mathbf{k}[W] \cong \mathbf{k}[W_1] \otimes \mathbf{k}[W_2] \otimes \cdots \otimes \mathbf{k}[W_t]$. The action of $\mathbf{Z}/p$ preserves this grading and thus $\mathbf{k}[W]^{\mathbf{Z}/p}$ and $\mathbf{k}[W]^\flat$ inherit this grading.

3. SAGBI Bases

We use the convention that a monomial is a product of variables and that a term is a monomial with a non-zero coefficient. We direct the reader to Cox *et al.* (1992, Chapter 2) for a detailed discussion of monomial orders. For $f \in S$ we use $\mathrm{LT}(f)$ to denote the lead term of f and $\mathrm{LM}(f)$ to denote the lead monomial of f.

Suppose that R is a subalgebra of S. Let $\mathrm{LT}(R)$ denote the vector space spanned by the lead terms of elements of R. Then $\mathrm{LT}(R)$ is a subalgebra of S. If C is a subset of R

then let $\mathrm{LM}(C)$ denote the set of lead monomials of elements of C. If C is a subset of R such that $\mathrm{LM}(C)$ generates the algebra $\mathrm{LT}(R)$ then C generates R and C is called a *SAGBI basis* for R. For a detailed discussion of SAGBI bases see Robbiano and Sweedler (1990), Kapur and Madlener (1989) or Sturmfels (1996, Chapter 11).

Taking $C = R$ gives a SAGBI basis for R. Thus every subalgebra has a SAGBI basis. However, subalgebras of S are not necessarily finitely generated. If $\mathrm{LT}(R)$ is not finitely generated then R does not have a finite SAGBI basis (at least using the given monomial order). Even if R is finitely generated, $\mathrm{LT}(R)$ may fail to be finitely generated. In fact, as shown by Göbel (1995, Lemma 2.1), the ring of invariants of the permutation representation of the alternating group on three letters does not have a finite SAGBI basis using the lexicographic order. Although the characterization of subalgebras which admit a finite SAGBI basis remains an important open problem, there are some circumstances which guarantee the existence of a finite SAGBI basis.

LEMMA 3.1. *Suppose* $\{h_1, \ldots, h_n\}$ *is a homogeneous system of parameters for* $\mathbf{k}[V]$ *with* $\mathrm{LM}(h_i) = x_i^{d_i}$. *If* $A \subseteq \mathbf{k}[V]$ *is a subalgebra with* $\{h_1, \ldots, h_n\} \subseteq A$, *then* A *has a finite SAGBI basis.*

PROOF. Since $\{h_1, \ldots, h_n\} \subseteq A$ and $\mathrm{LM}(h_i) = x_i^{d_i}$, $\{x_1^{d_1}, \ldots, x_n^{d_n}\} \subseteq \mathrm{LT}(A)$. Therefore $\mathbf{k}[x_1^{d_1}, \ldots, x_n^{d_n}]$ is contained in $\mathrm{LT}(A)$. Furthermore the set $\{x_1^{d_1}, \ldots, x_n^{d_n}\}$ is a homogeneous system of parameters for $\mathbf{k}[V]$. Thus $\mathrm{LT}(A)$ is a submodule of the finitely generated module $\mathbf{k}[V]$ over the Noetherian algebra $\mathbf{k}[x_1^{d_1}, \ldots, x_n^{d_n}]$. Hence $\mathrm{LT}(A)$ is a finite module over $\mathbf{k}[x_1^{d_1}, \ldots, x_n^{d_n}]$. Since $\mathrm{LT}(A)$ is generated by monomials, we may choose the module generators to be monomials. For each module generator $\alpha \in \mathrm{LT}(A)$ choose an element $f \in A$ with $\mathrm{LT}(f) = \alpha$. These elements along with $h_1, \ldots, h_n$ form a SAGBI basis for A. □

Choose an order with $x_1 < x_2 < \cdots < x_n$. We call the representation of G *triangular* if $\mathrm{LM}(g(x_i)) = x_i$ for every $g \in G$. If we view the variables as column vectors then the elements of G are upper-triangular matrices.

THEOREM 3.2. *If the representation of* G *is triangular then* $\mathbf{k}[V]^G$ *has a finite SAGBI basis.*

PROOF. Since $\mathrm{LM}(g(x_i)) = x_i$, we see that $\mathrm{LM}(N(x_i)) = x_i^{d_i}$ where d_i is the index of the isotropy subgroup G_{x_i}. Thus $\{N(x_1), \ldots, N(x_n)\} \subset \mathbf{k}[V]^G$ is a homogeneous system of parameters for $\mathbf{k}[V]$ satisfying the hypotheses of Lemma 3.1. Therefore $\mathbf{k}[V]^G$ has a finite SAGBI basis. □

COROLLARY 3.3. *Suppose* G *is a* p*-group and* $\mathbf{k}$ *has characteristic* p. *Then there is a choice of basis and monomial order with respect to which* $\mathbf{k}[V]^G$ *has a finite SAGBI basis.*

PROOF. Under these conditions G is conjugate to a subgroup of the upper-triangular matrices. If $\mathbf{k}$ is finite then the set of upper-triangular matrices with 1's along the diagonal form a p-Sylow subgroup of $\mathrm{GL}(n, \mathbf{k})$. In this case G is clearly conjugate to a subgroup of this p-Sylow group. For more general fields, first observe that G has

a composition series, $\{e\} = G_0 \leq G_1 \leq \cdots \leq G_m = G$, whose factors are all isomorphic to $\mathbf{Z}/p$. As a simple consequence of the Jordan canonical form of a generator, every representation of $\mathbf{Z}/p$ over a field of characteristic p has a fixed line. Thus, for any representation of G over a field of characteristic p, say W, using the fact that $(W^{G_i})^{G_{i+1}/G_i} = W^{G_{i+1}}$, we conclude that $\dim(W^G) \geq 1$. The proof now proceeds by induction on $\dim(W) - \dim(W^G)$. Clearly if $\dim(W) - \dim(W^G) = 0$, any basis is triangular. Suppose $\dim(W) - \dim(W^G) > 0$ and consider the G-module W/W^G. Since $\dim(W/W^G) - \dim((W/W^G)^G) \leq \dim(W) - \dim(W^G) - 1$, the induction hypothesis gives a triangular basis for W/W^G. Lifting the elements of this basis to W and adjoining elements which form a basis for W^G gives a triangular basis for W. □

4. The Vector Invariants of V_2

Let $\mathbf{k}$ be field of characteristic p and let V_n denote the n-dimensional indecomposable representation of $\mathbf{Z}/p$. The ladder technique for computing rings of invariants of p-groups described in Section 7 relies heavily upon computing $\mathbf{Z}/p$-invariants. One step in this method requires the construction of a surjection from a polynomial ring, $A := \mathbf{k}[a_1, \ldots, a_t]$, onto a ring of invariants, $\mathbf{k}[V]^{\mathbf{Z}/p}$. In order to minimize the complexity of the ladder computation it is desirable to minimize the Krull dimension of A and this usually means having a minimal set of generators for $\mathbf{k}[V]^{\mathbf{Z}/p}$.

As discussed in Section 1, the problem of constructing a manageable generating set for $\mathbf{k}[V]^{\mathbf{Z}/p}$ is, in general, quite difficult. If $V = mV_2 \oplus \ell V_1$ then, since $\mathbf{k}[mV_2 \oplus \ell V_1]^{\mathbf{Z}/p} \cong \mathbf{k}[mV_2]^{\mathbf{Z}/p} \otimes \mathbf{k}[\ell V_1]$, the problem reduces to constructing a generating set for $\mathbf{k}[mV_2]^{\mathbf{Z}/p}$. This was done by Campbell and Hughes (1997). However the generating set given in Campbell and Hughes (1997) is usually not a minimal set. The current section is devoted to identifying a minimal generating set for $\mathbf{k}[mV_2]^{\mathbf{Z}/p}$. The results for $m = 3$ will play a role in Section 8.

Choose a basis $\{x_i, y_i \mid i = 1, \ldots, m\}$ for mV_2^* with $\Delta(y_i) = x_i$. Define $N_i := N(y_i)$ and, for $i < j$, define $u_{ij} := x_j y_i - x_i y_j$. For $m = 2$, $\mathbf{k}[mV_2]^{\mathbf{Z}/p}$ is generated by x_1, x_2 N_1, N_2 and u_{12}. This is clearly a minimal generating set. For $m > 2$ the generating set must include some elements from the image of the transfer, $\operatorname{Im}\operatorname{Tr}^{\mathbf{Z}/p}$. In particular $\operatorname{Tr}^{\mathbf{Z}/p}(y_1^{p-1} \cdots y_m^{p-1})$ is not contained in the subalgebra generated by invariants of lower degree (see Richman, 1990 or Campbell and Hughes, 1997) and $m(p-1)$ is the least upper bound on the degrees of a generating set. Using the homogeneous system of parameters consisting of x_i, N_i, we see that the factors of $(y_1 y_2 \cdots y_m)^{p-1}$ generate $\mathbf{k}[mV_2]$ as a $\mathbf{k}[mV_2]^{\mathbf{Z}/p}$-module and, therefore, the ideal $\operatorname{Im}\operatorname{Tr}^{\mathbf{Z}/p}$ is generated by

$$\{\operatorname{Tr}^{\mathbf{Z}/p}(y_1^{e_1} \cdots y_m^{e_m}) \mid e_1 \leq p-1, e_2 \leq p-1, \ldots, e_m \leq p-1\}.$$

Campbell and Hughes showed that this set of transfers together with the x_i, N_i and u_{ij} generate the ring of invariants, $\mathbf{k}[mV_2]^{\mathbf{Z}/p}$.

Suppose $E = (e_1, \ldots, e_m)$ is a sequence of non-negative integers. Let $x^E := x_1^{e_1} \cdots x_m^{e_m}$, $y^E := y_1^{e_1} \cdots y_m^{e_m}$, and $|E| := e_1 + \cdots + e_m$. If $J = (j_1, \ldots, j_m)$ is a second sequence of non-negative integers then we say that $J \leq E$ if $j_i \leq e_i$ for $i = 1, \ldots, m$ and we denote $\binom{E}{J} := \prod_{i=1}^m \binom{e_i}{j_i}$. Thus

$$\operatorname{Tr}^{\mathbf{Z}/p}(y^E) = \sum_{c \in \mathbf{F}_p} \prod_{i=1}^m (y_i + c x_i)^{e_i}$$

$$= \sum_{c\in\mathbf{F}_p} \prod_{i=1}^{m} \sum_{j_i=0}^{e_i} c^{j_i} \binom{e_i}{j_i} x_i^{j_i} y_i^{e_i-j_i}$$

$$= \sum_{J\le E} \left(\sum_{c\in\mathbf{F}_p} c^{|J|} \right) \binom{E}{J} x^J y^{E-J}. \tag{1}$$

Recall that

$$\sum_{c\in\mathbf{F}_p} c^{|J|} = \begin{cases} -1 & \text{if } |J| = k(p-1) \text{ for some } k>0; \\ 0 & \text{otherwise.} \end{cases}$$

Thus $\mathrm{Tr}^{\mathbf{Z}/p}(y^E) = 0$ if $|E| < p-1$. Introduce a bidegree on $\mathbf{k}[mV_2]$ by taking x_i to have bidegree $(1,0)$ and y_i to have bidegree $(0,1)$. If $|E| < 2(p-1)$, then $\mathrm{Tr}^{\mathbf{Z}/p}(y^E)$ is homogeneous with bidegree $(p-1, |E|-p+1)$. If $|E| = 2(p-1)$ then $\mathrm{Tr}^{\mathbf{Z}/p}(y^E) + x^E$ is homogeneous with bidegree $(p-1, p-1)$.

Let R denote the subalgebra of $\mathbf{k}[mV_2]$ generated by x_i, N_i and u_{ij}. If we use a graded reverse lexicographic order with $x_i < y_i$ and $x_i < x_{i+1}$ then the only non-trivial tête-a-têtes[†] are of the form $u_{ij}^p - x_j^p N_i$. These tête-a-têtes subduct to zero using the relation $u_{ij}^p - x_j^p N_i + x_i^p N_j - (x_i x_j)^{p-1} u_{ij}$. Thus $\{x_i, N_i, u_{ij} \mid i = 1, \ldots, m \text{ and } i < j \le m\}$ is a SAGBI basis for R.

LEMMA 4.1. *If $f \in R$ is homogeneous of bidegree (i,j) with $j < p$, then f is in the subalgebra generated by $\{x_i, u_{ij} \mid i = 1, \ldots, m \text{ and } i < j \le m\}$.*

PROOF. Suppose f is a minimal counter-example where minimal is defined using the partial order induced on R by the monomial order. Using the SAGBI basis for R, the lead monomial of f is of the form $\mathrm{LM}(x^I u^J N^K)$. However $\mathrm{LM}(f)$ has bidegree (i,j) with $j < p$. Thus $K = 0$. Furthermore, x_i and u_{ij} are homogeneous with respect to the bidegree. Thus $f - x^I u^J$ is still a homogeneous element of R with bidegree (i,j). Clearly $f > f - x^I u^J$, contradicting the minimality hypothesis. □

The following lemma shows that the transfers of the form $\mathrm{Tr}^{\mathbf{Z}/p}(y^E)$ with $|E| \le 2(p-1)$ are not required as generators of $\mathbf{k}[mV_2]^{\mathbf{Z}/p}$.

LEMMA 4.2. *The algebras $\mathbf{k}[mV_2]^{\mathbf{Z}/p}$ and R agree in degrees less than or equal to $2(p-1)$, i.e. $(\mathbf{k}[mV_2]^{\mathbf{Z}/p})_i = R_i$ for $i = 0, 1, \ldots, 2(p-1)$.*

PROOF. The proof is by induction on degree. Clearly the two algebras agree in degree zero. If $|E| < p-1$, then $\mathrm{Tr}^{\mathbf{Z}/p}(y^E) = 0$. If $|E| = p-1$, then $\mathrm{Tr}^{\mathbf{Z}/p}(y^E) = -x^E \in R$. Therefore the algebras agree in degrees less than or equal to $p-1$. Consider $\mathrm{Tr}^{\mathbf{Z}/p}(y^E) = \mathrm{Tr}^{\mathbf{Z}/p}(y_1^{e_1} \cdots y_\ell^{e_\ell})$ with $e_\ell \neq 0$ and $p-1 < |E| \le 2(p-1)$. Work modulo the ideal $(x_\ell)\mathbf{k}[mV_2]$. Using the definition of $\mathrm{Tr}^{\mathbf{Z}/p}$,

$$\mathrm{Tr}^{\mathbf{Z}/p}(y_1^{e_1} \cdots y_\ell^{e_\ell}) \equiv y_\ell^{e_\ell}\ \mathrm{Tr}^{\mathbf{Z}/p}(y_1^{e_1} \cdots y_{\ell-1}^{e_{\ell-1}}) \pmod{(x_\ell)\mathbf{k}[mV_2]}.$$

[†]Given a set of algebra generators, say $\mathcal{C}$, and a pair of polynomials, f and h, each given by a product of an element of $\mathbf{k}$ with elements of $\mathcal{C}$, then if $\mathrm{LT}(f) = \mathrm{LT}(h)$ the polynomial $f - h$ is called a tête-a-tête. If no element of $\mathcal{C}$ divides both f and h, then the tête-a-tête is said to be non-trivial. See Robbiano and Sweedler (1990, p. 71).

By the induction hypothesis, $\mathrm{Tr}^{\mathbf{Z}/p}(y_1^{e_1}\cdots y_{\ell-1}^{e_{\ell-1}})$ lies in R. Furthermore, since $e_1+\cdots+e_{\ell-1}<2(p-1)$, $\mathrm{Tr}^{\mathbf{Z}/p}(y_1^{e_1}\cdots y_{\ell-1}^{e_{\ell-1}})$ is homogeneous of bidegree $(p-1,|E|-(p-1)-e_\ell)$. Thus by Lemma 4.1 $\mathrm{Tr}^{\mathbf{Z}/p}(y_1^{e_1}\cdots y_{\ell-1}^{e_{\ell-1}})$ lies in the subalgebra generated by x_i and u_{ij}. Since $2(p-1)\geq|E|$, we have $p-1-e_\ell\geq|E|-(p-1)-e_\ell$ and each monomial in $\mathrm{Tr}^{\mathbf{Z}/p}(y_1^{e_1}\cdots y_{\ell-1}^{e_{\ell-1}})$ has at least e_ℓ more x's than y's. Thus

$$\mathrm{Tr}^{\mathbf{Z}/p}(y_1^{e_1}\cdots y_{\ell-1}^{e_{\ell-1}})=\sum_{|I|=e_\ell}x^If_I$$

with $I=(i_1,\ldots,i_{\ell-l})$ and f_I in the subalgebra generated by x_i and u_{ij}. Let $u_\ell^I:=\prod_{j=1}^{\ell-1}u_{j\ell}^{i_j}$. Then $u_\ell^I\equiv y_\ell^{e_\ell}x^I\pmod{(x_\ell)\mathbf{k}[mV_2]}$ and

$$\mathrm{Tr}^{\mathbf{Z}/p}(y^E)\equiv\sum_I u_\ell^If_I\pmod{(x_\ell)\mathbf{k}[mV_2]}.$$

Thus

$$\mathrm{Tr}^{\mathbf{Z}/p}(y^E)=\sum_I u_\ell^If_I+x_\ell h$$

for some $h\in\mathbf{k}[mV_2]$. However $x_\ell h=\mathrm{Tr}^{\mathbf{Z}/p}(y^E)-\sum_I u_\ell^If_I\in\mathbf{k}[mV_2]^{\mathbf{Z}/p}$. Hence $h\in\mathbf{k}[mV_2]^{\mathbf{Z}/p}$. Furthermore the degree of h is $|E|-1$. Thus by the induction hypothesis, $h\in R$. Therefore $\mathrm{Tr}^{\mathbf{Z}/p}(y^E)\in R$. □

The next lemma shows that each of the transfers $\mathrm{Tr}^{\mathbf{Z}/p}(y^E)$ with $e_i\leq p-1$ and $|E|>2(p-1)$ where $E=(e_1,\ldots,e_m)$ is required in our minimal generating set.

LEMMA 4.3. *If $E=(e_1,\ldots,e_m)$, $e_i\leq p-1$ and $|E|>2(p-1)$ then $\mathrm{Tr}^{\mathbf{Z}/p}(y^E)$ is indecomposable.*

PROOF. We use the graded reverse lexicographic order with $x_1<x_2<\cdots<x_m<y_1<\cdots<y_m$. Suppose, by way of contradiction, that $\mathrm{Tr}^{\mathbf{Z}/p}(y^E)=c_1m_1+c_2m_2+\cdots+c_rm_r$ where each m_i is a non-trivial product of generators, each $c_i\in\mathbf{k}$ and $\mathrm{LM}(m_i)\geq\mathrm{LM}(m_{i+1})$. Either $\mathrm{LM}(m_1)=\mathrm{LM}(\mathrm{Tr}^{\mathbf{Z}/p}(y^E))$ or $\mathrm{LM}(m_1)=\mathrm{LM}(m_2)>\mathrm{LM}(\mathrm{Tr}^{\mathbf{Z}/p}(y^E))$. From equation (1) we see that $\mathrm{LM}(\mathrm{Tr}^{\mathbf{Z}/p}(y^E))=x^Iy^{E-I}$ where $x^I=\max\{x^J\mid|J|=p-1\text{ and }J\leq E\}$.

We first show that $\mathrm{LM}(m_1)\neq\mathrm{LM}(\mathrm{Tr}^{\mathbf{Z}/p}(y^E))$. Since $e_i\leq p-1$, $\mathrm{LM}(N_i)=y_i^p$ does not divide x^Iy^{E-I}. Note that x^Iy^{E-I} has bidegree $(p-1,|E|-(p+1))$ and $|E|-(p-1)>p-1$. Therefore x^Iy^{E-I} does not factor using only elements from $\{x_i,\mathrm{LM}(u_{ij})\mid i=1,\ldots,m\text{ and }i<j\leq m\}$. If we try to factor x^Iy^{E-I} using $\mathrm{LM}(\mathrm{Tr}^{\mathbf{Z}/p}(y^F))$ with $F=(f_1,\ldots,f_m)$, $f_i\leq p-1$ and $|F|\geq p-1$, then the complement is y^{F-E}. However, since $f_i-e_i\leq p-1$, this is not the lead term of a product of generators. Thus $\mathrm{LM}(m_1)\neq\mathrm{LM}(\mathrm{Tr}^{\mathbf{Z}/p}(y^E))$.

Now suppose $\mathrm{LM}(m_1)=\mathrm{LM}(m_2)>\mathrm{LM}(\mathrm{Tr}^{\mathbf{Z}/p}(y^E))$. This means that m_1 and m_2 form a tête-a-tête. However, for every non-trivial tête-a-tête formed from the generators, the leading monomial has bidegree (d_1,d_2) with $d_1>p-1$. Thus $\mathrm{LM}(m_1)<x^Iy^{E-I}$ giving the required contradiction. □

Putting together Lemmas 4.2 and 4.3 we obtain the following corollary.

COROLLARY 4.4. *The set*

$$\{x_i, N_i, u_{ij} \mid i = 1, \dots m \text{ and } i < j \leq m\}$$
$$\bigcup \{\mathrm{Tr}^{\mathbf{Z}/p}(y_1^{e_1} \cdots y_m^{e_m}) \mid e_i \leq p-1 \text{ and } e_1 + \cdots + e_m > 2(p-1)\}$$

is a minimal generating set for $\mathbf{k}[mV_2]^{\mathbf{Z}/p}$.

5. Localization and Normalization

Let R be a finitely generated algebra. Throughout this section we will further suppose that R contains no zero-divisors. We denote by R_f the localization of R with respect to the multiplicative set generated by f.

The following theorem is essentially Schwarz (1980, 15.11). See also Wehlau (1993, Lemma 4.6.10).

THEOREM 5.1. *Suppose that A is a subalgebra of R and that f_1, f_2 is a regular sequence in A such that $A_{f_1} = R_{f_1}$ and $A_{f_2} = R_{f_2}$. Then $A = R$.*

PROOF. Take $h \in R$. Since $R \subseteq R_{f_i} = A_{f_i}$ we may write $h = a_1/f_1^n$ and $h = a_2/f_2^m$ for some $a_1, a_2 \in A$ and $n, m \in \mathbf{Z}$. Thus $a_1 f_2^m = a_2 f_1^n$. Since f_1, f_2 is a regular sequence in A so also is f_1^n, f_2^m. This implies that $a_2 = a f_2^m$ for some $a \in A$. Therefore $h = a f_2^m / f_2^m = a$ lies in A. □

LEMMA 5.2. *Suppose that A is a subalgebra of R and I is an ideal of R. If $I \subseteq A$ and $f \in \sqrt{I} \cap A$ then $A_f = R_f$.*

PROOF. There exists $m \in \mathbf{Z}$ such that $f^m \in I$. Take $h \in R_f$ and write $h = r/f^k$ with $r \in R$. Then $rf^m = hf^{k+m} \in I \subseteq A$ and $h = rf^m/f^{k+m} \in A_f$. □

COROLLARY 5.3. *Suppose A is a subalgebra of $\mathbf{k}[V]^G$ and that A contains the image of the transfer, $\mathrm{Im}\,\mathrm{Tr}^G$. If there exist $f_1, f_2 \in \sqrt{\mathrm{Im}\,\mathrm{Tr}^G} \cap A$ such that f_1, f_2 is a regular sequence on A, then $A = \mathbf{k}[V]^G$.*

REMARK 5.4. Suppose that A is a subalgebra of $\mathbf{k}[V]^G$ containing the image of the transfer. Further suppose that f_1 and f_2 are non-associate primes of A lying in $\sqrt{\mathrm{Im}\,\mathrm{Tr}^G}$. A relatively routine calculation shows that f_1, f_2 is a regular sequence in A and so $A = \mathbf{k}[V]^G$.

REMARK 5.5. Let $\overline{\mathbf{k}}$ denote the algebraic closure of $\mathbf{k}$ and define $\overline{V} := \overline{\mathbf{k}} \otimes V$. By Shank and Wehlau (1999, Theorem 2.1), we have that $\sqrt{\mathrm{Im}\,\mathrm{Tr}^G}$ consists of those invariant polynomials in $\mathbf{k}[V]$ which vanish on the subvariety $\mathcal{V}$ of $\overline{V}$ defined by $\mathcal{V} = \cup_{\sigma \in \Sigma} \overline{V}^\sigma$ where Σ consists of all the elements σ of G of order p. Thus given an element $f \in \mathbf{k}[V]^G$ we may check that $f \in \sqrt{\mathrm{Im}\,\mathrm{Tr}^G}$ by verifying that f vanishes on $\overline{V}^\sigma$ for every element $\sigma \in G$ of order p.

Suppose that f_1 and f_2 are elements of an algebra A. The *syzygy module*, $\mathrm{syz}_A(f_1, -f_2)$, is the kernel of the map from A^2 to A which takes (c_1, c_2) to $c_1 f_1 - c_2 f_2$.

LEMMA 5.6. *Suppose that A is a subalgebra of $\mathbf{k}[V]$, $\{f_1, f_2\} \subset A$, and f_1, f_2 is a regular sequence in $\mathbf{k}[V]$. Then f_1, f_2 is regular on A if and only if $\mathrm{syz}_A(f_1, -f_2)$ is a principal A-module.*

PROOF. Suppose that f_1, f_2 is regular on A. For an arbitrary $(a, b) \in \mathrm{syz}_A(f_1, -f_2)$, we have $af_1 - bf_2 = 0$. Thus $bf_2 = af_1$. Since f_1, f_2 is regular on A, there exists $c \in A$ such that $b = cf_1$. Thus $f_1(a - cf_2) = af_1 - cf_1f_2 = 0$. Since f_1 is not a zero divisor, we conclude $a = cf_2$. Therefore $(a, b) = c(f_2, f_1)$ and $\mathrm{syz}_A(f_1, -f_2)$ is the principal A-module generated by (f_2, f_1).

Suppose that $\mathrm{syz}_A(f_1, -f_2)$ is a principal A-module. Clearly $(f_2, f_1) \in \mathrm{syz}_A(f_1, -f_2)$. Furthermore, since f_1, f_2 is a regular sequence in $\mathbf{k}[V]$, f_1 and f_2 have no positive degree common factors. Thus $\mathrm{syz}_A(f_1, -f_2)$ is the principal A-module generated by (f_2, f_1). By hypothesis, f_1 is not a zero divisor in A. Thus to show that f_1, f_2 is regular on A, it is sufficient to show that f_2 is not a zero divisor on $A/(f_1)A$. For an arbitrary $a, b \in A$ with $bf_2 = af_1$, we have $(a, b) \in \mathrm{syz}_A(f_1, -f_2)$. Thus $(a, b) = c(f_2, f_1)$ for some element $c \in A$. Therefore $b = cf_1$ as required. □

ALGORITHM 5.7. *Suppose that V is a triangular representation of G and the height of the image of the transfer is at least 2. Then a generating set for $\mathbf{k}[V]^G$ can be constructed as follows.*

Step 1: *Use the homogeneous system of parameters $\{x_1, N(x_2), N(x_3), \ldots, N(x_n)\}$. Note that $\mathrm{LM}(N(x_i)) = x_i^{d_i}$ where d_i is the index of the isotropy subgroup, G_{x_i}, in G. Thus the monomials dividing $x_2^{d_2-1}x_3^{d_3-1}\cdots x_n^{d_n-1}$ are a basis for $\mathbf{k}[V]$ over $\mathbf{k}[x_1, N(x_2), \ldots, N(x_n)]$ and*

$$\mathcal{T} := \{\mathrm{Tr}^G(\beta) \mid \beta \text{ divides } x_2^{d_2-1}\cdots x_n^{d_n-1}\}$$

is a generating set for $\mathrm{Im}\,\mathrm{Tr}^G$ as a module over $R := \mathbf{k}[x_1, N(x_2), \ldots, N(x_n)]$.

Step 2: *Choose f_1, f_2, a partial homogeneous system of parameters for S with $\{f_1, f_2\} \subset \sqrt{\mathrm{Im}\,\mathrm{Tr}^G}$ and take $\mathcal{C} := \{f_1, f_2, x_1, N(x_2), \ldots, N(x_n)\} \cup \mathcal{T}$.*

Step 3: *Take A to be the subalgebra of $\mathbf{k}[V]^G$ generated by $\mathcal{C}$.*

Step 4 (*optional*): *If one of the generators for A divides another, perform the division and add the quotient to $\mathcal{C}$. Remove redundant generators from $\mathcal{C}$.*

Step 5: *Compute a generating set for the syzygy module $\mathrm{syz}_A(f_1, -f_2)$. This module is the kernel of the map from A^2 to A which takes (c_1, c_2) to $c_1f_1 - c_2f_2$. The syzygy module computation involves the construction of a SAGBI basis for A. It follows from Lemma* 3.1 *that A has a finite SAGBI basis. The details of the syzygy module computation, for algebras with a finite SAGBI basis, can be found in Miller* (1996, *Section* 5).

Step 6: *If $\mathrm{syz}_A(f_1, -f_2)$ is a principal A-module, stop. From Lemma* 5.6, *the sequence f_1, f_2 is regular on A if and only if $\mathrm{syz}_A(f_1, -f_2)$ is a principal module. Therefore, using Corollary* 5.3, *if $\mathrm{syz}_A(f_1, -f_2)$ is principal then $A = \mathbf{k}[V]^G$.*

Step 7: *By construction, f_1, f_2 is a regular sequence in $\mathbf{k}[V]^G$ and therefore $\mathrm{syz}_{\mathbf{k}[V]^G}(f_1, -f_2)$ is a principal $\mathbf{k}[V]^G$-module with generator (f_2, f_1). Hence for each generator, $(h_1, h_2) \in \mathrm{syz}_A(f_1, -f_2) \subseteq \mathrm{syz}_{\mathbf{k}[V]^G}(f_1, -f_2)$, we have $(h_1, h_2) = c(f_2, f_1)$ for $c = h_1/f_2 \in \mathbf{k}[V]^G$. For each generator, add the corresponding c to $\mathcal{C}$. Go to Step* 3.

PROOF. The algorithm generates an increasing sequence of R-submodules of the Noetherian R-module $\mathbf{k}[V]^G$. Therefore the algorithm terminates. □

REMARK 5.8. In practice, it is probably best to combine Algorithm 5.7 with a certain amount of "preprocessing". We can start Step 5 with any subalgebra of $\mathbf{k}[V]^G$ containing the set $\mathcal{C}$. One might as well include any known invariants before computing the generators of the syzygy module.

REMARK 5.9. In Algorithm 5.7, we need the hypothesis that the height of the image of the transfer is at least 2 in order to guarantee the existence of a suitable f_1 and f_2. We can rephrase this restriction. The reduced variety corresponding to the image of the transfer is the set $\mathcal{V}$ described in Remark 5.5. The height of the ideal $\operatorname{Im}\operatorname{Tr}^G$ is the codimension of the variety, $\mathcal{V}$. The codimension of a union of subspaces is the minimum of the codimensions of the subspaces. We wish to exclude height 1. This means that $\overline{V}^\sigma$, or equivalently V^σ, must have codimension at least 2 for every $\sigma \in G$ of order p. The subspace V^σ is a codimension 1 subspace of V if and only if σ is a (pseudo) reflection of order p (i.e. a transvection). Thus Algorithm 5.7 applies as long as the representation V is triangular and G contains no transvections.

REMARK 5.10. There is a variation on Algorithm 5.7 in which the finitely generated algebra A is identified with a quotient $\mathbf{k}[W]/I$. The syzygy module calculation can then be performed in $\mathbf{k}[W]$. This means that SAGBI basis is not required and the representation need not be triangular. However, when using this approach it is necessary to construct a generating set for the ideal I. This can be quite difficult.

EXAMPLE 5.11. Suppose $\mathbf{k}$ has characteristic $p > 2$ and consider $\mathbf{k}[V_2 \oplus V_3]^{\mathbf{Z}/p}$. Let $\{y_1, x_1\}$ be a triangular basis of V_2^* where y_1 is a distinguished variable. Let $\{z_2, y_2, x_2\}$ be a triangular basis of V_3^* where z_2 is a distinguished variable. A relatively simple calculation gives $\operatorname{Tr}^{\mathbf{Z}/p}(y_i^{p-1}) = -x_i^{p-1}$. Thus x_1 and x_2 lie in the radical of the image of the transfer and we may apply Algorithm 5.7 with $f_1 := x_1$ and $f_2 := x_2$. For the initial iteration, A is generated by the homogeneous system of parameters and the image of the transfer. However, using (Shank and Wehlau, 2002, Section 5), we know that $\mathbf{k}[V_2 \oplus V_3]^{\mathbf{Z}/p}$ contains three "rational invariants", $u := y_1x_2 - y_2x_1$, $d := y_2^2 - 2x_2z_2 - x_2y_2$ and $w := y_1^2x_2 + x_1y_1x_2 - 2x_1y_1y_2 + x_1^2z_2$, which, at least for general p, are not in A (this can be easily verified for small p using MAGMA (Bosma *et al.*, 1997)). Therefore x_1, x_2 is not regular in A, $\operatorname{syz}_A(x_1, -x_2)$ is not a principal A-module and, referring to Remark 5.4, x_1, x_2 are not non-associate primes in A. To see this last fact directly note that $\operatorname{Tr}^{\mathbf{Z}/p}(uy_1^{p-1}) = -ux_1^{p-1}$, $\operatorname{Tr}^{\mathbf{Z}/p}(wy_2^{p-1}) = -wx_2^{p-1}$ and $\operatorname{Tr}^{\mathbf{Z}/p}(uwy_2^{p-1}) = -uwx_2^{p-1}$ are all in A. Thus $(ux_1^{p-1})(wx_2^{p-1}) = (uwx_2^{p-1})(x_1^{p-2})x_1 \in (x_1)A$. However neither ux_1^{p-1} nor wx_2^{p-1} lie in $(x_1)A$. Therefore $(x_1)A$ is not a prime ideal. To see the algorithm in action, start with the fact that $\operatorname{Tr}^{\mathbf{Z}/p}(uy_1^iy_2^{p-1-i}) = -ux_1^ix_2^{p-1-i} \in A$. Thus $(ux_1^{p-2}x_2, ux_1^{p-1})$ lies in $\operatorname{syz}_A(x_1, -x_2)$ and the first iteration of Step 7 would add ux_1^{p-2} to A. However, judicious use of Step 4 would have produced a generating set and Step 5 would then have produced a principal module. A finite SAGBI basis for $\mathbf{k}[V_2 \oplus V_3]^{\mathbf{Z}/p}$ is given in Shank and Wehlau (2002, Section 5).

See Remark 8.1 for a second example.

REMARK 5.12. At the beginning of this section we assumed that R contains no zero-divisors. This was done to (slightly) simplify the discussion and because it is true for all our applications. However, this assumption is not really necessary; all that is required is that the elements f_1 and f_2 with respect to which we localized must not be zero-divisors.

6. Cohomology

To apply the method of ladders described in Section 7 to a modular representation will require group cohomology computations for the cyclic group $\mathbf{Z}/p$. In this section we develop the group cohomology results we will need.

For a $\mathbf{Z}/p$-module M, the first cohomology group of Z/p with coefficients in M is given by

$$H^1(\mathbf{Z}/p, M) = \frac{\text{kernel}(\text{Tr}\,|_M)}{\text{image}(\Delta|_M)}.$$

A $\mathbf{Z}/p$-module decomposition of M gives a vector space decomposition of $H^1(\mathbf{Z}/p, M)$. Using the fact that $\text{Tr} = \Delta^{p-1}$, we see that $H^1(\mathbf{Z}/p, V_p) = 0$ and, for $n < p$, any element v with $\Delta^{n-1}v \neq 0$ represents a non-zero class in the one-dimensional vector space $H^1(\mathbf{Z}/p, V_n)$. One way to identify such an element is to chose a non-zero element $u \in V_n^{\mathbf{Z}/p}$ and then to find v such that $\Delta^{n-1}v = u$. A detailed discussion of group cohomology may be found in Evens (1991).

Consider a $\mathbf{Z}/p$-module W and decompose W into a direct sum of indecomposable $\mathbf{Z}/p$-summands: $W = \bigoplus_{i=1}^{t} W_i$ where $W_i \cong V_{\dim(W_i)}$ for all i. As usual we choose a distinguished variable $z_i \in W_i^*$ for each i and use the corresponding triangular basis for W_i^*. Also as usual we let N_i denote the norm of z_i. Let $B := \mathbf{k}[N_1, \ldots, N_t]$.

Suppose $f \in \mathbf{k}[W]$ and consider the norm decomposition $f = f_1N_1 + f_2N_2 + \cdots + f_tN_t + r$. Since $N_i \in \mathbf{k}[W]^{\mathbf{Z}/p}$, $\text{Tr}(f) = \text{Tr}(f_1)N_1 + \cdots + \text{Tr}(f_t)N_t + \text{Tr}(r)$ and $\Delta(f) = \Delta(f_1)N_1 + \cdots + \Delta(f_t)N_t + \Delta(r)$. Thus f represents an element of $H^1(\mathbf{Z}/p, \mathbf{k}[W])$ if and only if f_i for $i = 1, \ldots, t$ and r represent elements of $H^1(\mathbf{Z}/p, \mathbf{k}[W])$. Similarly, $[f] = 0$ if and only if $[f_i] = 0$ for $i = 1, \ldots, t$ and $[r] = 0$.

LEMMA 6.1. *N_i acts injectively on $H^1(\mathbf{Z}/p, \mathbf{k}[W])$.*

PROOF. Suppose f represents an element of $H^1(\mathbf{Z}/p, \mathbf{k}[W])$ and $N_i[f] = 0$. Then $fN_i = \Delta h$ for some $h \in \mathbf{k}[W]$. Divide h by N_i to get $h = qN_i + r$ with $\deg_{z_i}(r) < p$. Thus $\Delta(h) = \Delta(q)N_i + \Delta(r)$ and, since Δ does not increase the z_i-degree, we have $\deg_{z_i}(\Delta(r)) < p$. However, we also have $\Delta(h) = fN_i$. Therefore, using the uniqueness of the division algorithm, $\Delta(r) = 0$ and $\Delta(q) = f$. Thus $[f] = 0$. □

Note that if U is a vector space over $\mathbf{k}$, then $B \otimes_{\mathbf{k}} U$ is a free B-module of rank $\dim(U)$.

PROPOSITION 6.2. *$H^1(\mathbf{Z}/p, \mathbf{k}[W])$ is isomorphic to the free B-module $B \otimes_{\mathbf{k}} H^1(\mathbf{Z}/p, \mathbf{k}[W]^\flat)$.*

PROOF. Note that $\mathbf{k}[W]$ is isomorphic to the free B-module $B \otimes_{\mathbf{k}} \mathbf{k}[W]^\flat$. Also $\mathbf{k}[W]^\flat$ is a $\mathbf{Z}/p$-submodule of $\mathbf{k}[W]$ and $B \subseteq \mathbf{k}[W]^{\mathbf{Z}/p}$. Thus

$$H^1(\mathbf{Z}/p, \mathbf{k}[W]) \cong H^1(\mathbf{Z}/p, B \otimes_{\mathbf{k}} \mathbf{k}[W]^\flat) \cong B \otimes_{\mathbf{k}} H^1(\mathbf{Z}/p, \mathbf{k}[W]^\flat)$$

as required. □

The multi-grading of $\mathbf{k}[W]$ described near the end of Section 2 is inherited by $H^1(\mathbf{Z}/p, \mathbf{k}[W])$.

COROLLARY 6.3. *The free B-module $H^1(\mathbf{Z}/p, \mathbf{k}[W])$ is generated in multi-degrees $(d_1, \ldots, d_t)$ with $d_i \leq p - \dim(W_i)$.*

PROOF. It follows from Proposition 6.2 that a vector space basis for $H^1(\mathbf{Z}/p, \mathbf{k}[W]^\flat)$ gives a generating set for the free B-module $H^1(\mathbf{Z}/p, \mathbf{k}[W])$. Furthermore one can choose a basis for $H^1(\mathbf{Z}/p, \mathbf{k}[W]^\flat)$ with one basis element for each non-free $\mathbf{Z}/p$-module summand of $\mathbf{k}[W]^\flat$. In fact the basis element can be represented by an element of the summand and has the same multi-degree as the summand. It is easy to see that

$$\mathbf{k}[W]^\flat_{(d_1,\ldots,d_t)} \cong \mathbf{k}[W_1]^\flat_{d_1} \otimes \mathbf{k}[W_2]^\flat_{d_2} \otimes \cdots \otimes \mathbf{k}[W_t]^\flat_{d_t}.$$

From Almkvist and Fossum (1978) (see also Hughes and Kemper, 2002, Lemma 2.10), $\mathbf{k}[V_n]^\flat_d$ is a free $\mathbf{Z}/p$-module for all $d \geq p - n + 1$. Since the tensor product of any finite dimensional $\mathbf{Z}/p$-module with a free $\mathbf{Z}/p$-module is free (see, for example, Alperin, 1986, II Section 7 Lemma 4), we see that $\mathbf{k}[W]^\flat_{(d_1,\ldots,d_t)}$ is free if any $d_i \geq p - \dim(W_i) + 1$. Therefore the B-module generators lie in multi-degrees with $d_i < p - \dim(W_i) + 1$. □

In Section 8 we will need to understand $H^1(\mathbf{Z}/p, \mathbf{k}[3V_2])$ as a module over $\mathbf{k}[3V_2]^{\mathbf{Z}/p}$. We use the notation introduced in Section 4. Using Proposition 6.2 and Corollary 6.3, it is sufficient to consider $\mathbf{k}[3V_2]$ in multi-degrees (d_1, d_2, d_3) with $d_i \leq p - 2$. If $p = 2$, we are left with a single generator in degree zero and $H^1(\mathbf{Z}/2, \mathbf{k}[3V_2])$ is isomorphic to $\mathbf{k}[N(y_1), N(y_2), N(y_3)]$.

Assume $p > 2$. Let M denote the subspace of $\mathbf{k}[V_2]$ given by $M = \sum_{d=0}^{p-2} \mathbf{k}[V_2]_d$. As a graded $\mathbf{Z}/p$-module, M is isomorphic to $V_1 \oplus V_2 \oplus \cdots \oplus V_{p-1}$. Furthermore $H^1(\mathbf{Z}/p, \mathbf{k}[3V_2]^\flat) \cong H^1(\mathbf{Z}/p, M^{\otimes 3})$. Thus it is sufficient to consider $(V_1 \oplus V_2 \oplus \cdots \oplus V_{p-1})^{\otimes 3}$. In degree 1 this gives $3V_2$. A basis for the invariants is given by $\{x_1, x_2, x_3\}$ and a basis for the cohomology is given by $\{[y_1], [y_2], [y_3]\}$. In multi-degree $(1, 1, 0)$ we have $V_2 \otimes V_2 \cong V_3 \oplus V_1$ (see Alperin, 1986, p. 50). Since $\Delta^2(y_1 y_2) = 2x_1 x_2$ we can choose $y_1 y_2$ as a generator for V_3 and $u_{12} = y_1 x_2 - x_1 y_2$ as a generator for V_1. The analogous results hold for the multi-degrees $(1, 0, 1)$ and $(0, 1, 1)$. In multi-degree $(\ell, 0, 0)$ with $\ell < p - 1$ we have $V_{\ell+1}$ generated by y_1^ℓ.

In the next lemma we consider how the invariants x_i and x_i^2 act on the cohomology classes represented by certain simple monomials.

LEMMA 6.4. *Suppose $\ell < p - 1$ and $i \neq j$. Then $x_i[y_i^\ell] = 0$ and, if $\ell > 0$, $x_i^2[y_j y_i^{\ell-1}] = 0$, but $x_i[y_j^\ell] \neq 0$.*

PROOF. We first show that $x_i[y_i^\ell] = 0$. The proof is by induction on ℓ. For $\ell = 0$ we have $\Delta(y_i) = x_i$ and thus $x_i[1] = 0$. Suppose $0 < \ell < p - 1$. Using the definition of Δ we have

$$\Delta(y_i^{\ell+1}) = (\ell + 1) x_i y_i^{\ell+1} + \sum_{t=2}^{\ell} \binom{\ell + 1}{t} x_i^t y_i^{\ell+1-t}.$$

By induction, if $t > 1$ then $x_i[y_i^{\ell+1-t}] = 0$. Since $\ell < p - 1$, $\ell + 1$ is a unit in $\mathbf{k}$ and $x_i[y_i^\ell] = 0$.

Next we show that $x_i^2[y_j y_i^{\ell-1}] = 0$ if $\ell > 0$. First suppose $i < j$. Using our first result we have $[u_{ij} x_i y_i^{\ell-1}] = u_{ij} x_i [y_i^{\ell-1}] = 0$. Using the definition of u_{ij} gives $x_j x_i [y_i^\ell] - x_i^2 [y_j y_i^{\ell-1}] = 0$. Thus $x_i^2 [y_j y_i^{\ell-1}] = x_j x_i [y_i^\ell] = 0$. For $i > j$, repeat the argument using u_{ji}.

Finally we show $x_i[y_j^\ell] \neq 0$. Suppose first that $j = 1$ and $i = 2$. The multi-degree component $(\ell, 1, 0)$ of $M^{\otimes 3}$ is isomorphic to $V_{\ell+1} \otimes V_2 \cong V_{\ell+2} \oplus V_\ell$. Note that for any $f \in \mathbf{k}[V]$, either $\Delta(f) = 0$ or $\deg_x(\Delta(f)) > \deg_x(f)$. Therefore $y_1^\ell y_2$ generates $V_{\ell+2}$ and the corresponding invariant, $\Delta^{\ell+1} y_1^\ell y_2$ is a non-zero multiple of $x_1^\ell x_2$. The second invariant in this bidegree is $x_1^{\ell-1} u_{12}$. Thus the generator, h, of the summand isomorphic to V_ℓ lying in multi-degree $(\ell, 1, 0)$ must satisfy $\deg_y(h) \geq \ell$. Therefore we may take this generator to be a linear combination of $x_1 y_1^{\ell-1} y_2$ and $y_1^\ell x_2$. Using the fact that Δ is a twisted derivation, $\Delta(y_1^\ell y_2 - y_1^\ell x_2) = y_2 \Delta(y_1^\ell) + x_2 y_1^\ell$ and $x_2[y_1^\ell] = -[y_2 \Delta(y_1^\ell)]$. However

$$\begin{aligned} y_2 \Delta(y_1^\ell) &= y_2 \sum_{t=1}^{\ell} \binom{\ell}{t} x_1^t y_1^{\ell-t} \\ &= \ell y_2 x_1 y_1^{\ell-1} + x_1^2 \sum_{t=2}^{\ell} \binom{\ell}{t} x_1^{t-2} y_2 y_1^{\ell-t}. \end{aligned}$$

Thus using the fact that $x_1^2[y_2 y_1^{\ell-t}] = 0$ we have $[y_2 \Delta(y_1^\ell)] = \ell x_1 [y_2 y_1^{\ell-1}]$. Combining this with our earlier calculation gives $x_2[y_1^\ell] = -\ell x_1 [y_2 y_1^\ell]$. Thus $x_2[y_1^\ell] + \ell x_1 [y_2 y_1^\ell] = 0$ but any other non-zero linear combination may be chosen to generate $V_{\ell-1}$. Hence $x_2[y_1^\ell] \neq 0$. The analogous argument works for all choices of i and j. □

In multi-degree $(1, 1, 1)$ we have $V_2 \otimes V_2 \otimes V_2 \cong (V_3 \oplus V_1) \otimes V_2$. For $p = 3$ this is isomorphic to $2V_3 \oplus V_2$ and $\{[u_{12} y_3]\}$ is a basis for the cohomology. For $p > 3$ we have $V_3 \otimes V_2 \cong V_4 \oplus V_2$ and so the module is isomorphic to $V_4 \oplus 2V_2$. A simple computation gives $\Delta^3(y_1 y_2 y_3) = 6 x_1 x_2 x_3$. Also, note that $y_1 u_{23} - y_2 u_{13} + y_3 u_{12} = 0$ and $x_1 u_{23} - x_2 u_{13} + x_3 u_{12} = 0$. In this multi-degree a basis for the invariants is given by $\{x_1 x_2 x_3, x_1 u_{23}, x_3 u_{12}\}$ and $\{[y_1 y_2 y_3], [y_1 u_{23}], [u_{12} y_3]\}$ is a basis for the cohomology.

THEOREM 6.5. *Take $p = 3$. Then $H^1(\mathbf{Z}/3, \mathbf{k}[3V_2])$ is the free $\mathbf{k}[N(y_1), N(y_2), N(y_3)]$-module generated by $\{[1], [y_1], [y_2], [y_3], [u_{12}], [u_{13}], [u_{23}], [u_{12} y_3]\}$. As a module over $\mathbf{k}[3V_2]^{\mathbf{Z}/3}$, $H^1(\mathbf{Z}/3, \mathbf{k}[3V_2])$ is generated by $\{[1], [y_1], [y_2], [y_3]\}$ The action of $\mathbf{k}[3V_2]^{\mathbf{Z}/3}$ is determined by $x_i[y_i] = 0$, $x_1[y_2] = -x_2[y_1] = u_{12}[1]$, $x_1[y_3] = -x_3[y_1] = u_{13}[1]$, $x_2[y_3] = -x_3[y_2] = u_{23}[1]$, and $u_{23}[y_1] = -u_{13}[y_2] = u_{12}[y_3]$.*

PROOF. For $p = 3$, $M = V_1 \oplus V_2$ and each non-zero multi-degree was discussed in the paragraph preceding the statement of the theorem. It remains to show that the action of $H^1(\mathbf{Z}/3, \mathbf{k}[V])$ is as described. Note that $\Delta(y_i y_j - x_i y_j) = x_i y_j + x_j y_i$. Thus, if $i = j$ we have $[x_i y_i] = 0$ and if $i < j$ we have $[u_{ij}] = [x_j y_i - x_i y_j] = 2[x_j y_i] = -2[x_i y_j]$ and $x_i[y_j] = -x_j[y_i] = u_{ij}[1]$. A straightforward computation gives $\Delta(y_1 y_2 y_3 - u_{12} y_3 + u_{23} y_1 - x_1 x_3 y_2) = y_1 u_{23} - y_3 u_{12}$. Thus $u_{23}[y_1] = u_{12}[y_3]$. Since $y_1 u_{23} - y_2 u_{13} + y_3 u_{12} = 0$, we have $u_{13}[y_2] = u_{23}[y_1] + u_{12}[y_3] = -u_{12}[y_3]$. □

7. Ladders

Suppose that p is the characteristic of $\mathbf{k}$ and G is a p-group. Then there exists a normal subgroup, N, with G/N isomorphic to the cyclic group of order p, $\mathbf{Z}/p$. The ring

of invariants is given by

$$\mathbf{k}[V]^G = (\mathbf{k}[V]^N)^{G/N} = (\mathbf{k}[V]^N)^{\mathbf{Z}/p}.$$

Suppose we have computed $\mathbf{k}[V]^N$. More precisely, suppose we have a short exact sequence of $\mathbf{Z}/p$-modules $0 \to J \xrightarrow{i} A := \mathbf{k}[a_1, \ldots, a_k] \xrightarrow{\rho} \mathbf{k}[V]^N \to 0$. This gives rise to a long exact sequence in group cohomology

$$0 \to J^{\mathbf{Z}/p} \to A^{\mathbf{Z}/p} \to \mathbf{k}[V]^G \to H^1(\mathbf{Z}/p, J) \xrightarrow{i^1} H^1(\mathbf{Z}/p, A) \to \cdots.$$

All of the maps in this long exact sequence are $A^{\mathbf{Z}/p}$-module maps. Furthermore $\mathbf{k}[V]^G$ is generated by $\rho(A^{\mathbf{Z}/p})$ and the preimage of the $A^{\mathbf{Z}/p}$-module generators of the kernel of i^1.

We may choose the ring A so that $A \cong \mathbf{k}[W]$ for some graded $\mathbf{Z}/p$-module W. One way to do this is to take W to be $\oplus_{j=1}^m \mathbf{k}[V]_j^N$ for a sufficiently large m. In practice one should choose W so as to minimize $\dim(W)$.

As in Section 6 we can decompose W, choose distinguished variables, and construct norms. Let $B = \mathbf{k}[N_1, \ldots, N_t]$. From Proposition 6.2, $H^1(\mathbf{Z}/p, A)$ is a finitely generated, free B-module.

PROPOSITION 7.1. $\operatorname{Im} \operatorname{Tr}^G \subseteq \rho(A^{\mathbf{Z}/p})$.

PROOF. The action of $G/N \cong \mathbf{Z}/p$ on A induces an action of the group ring of $\mathbf{Z}/p$ on A. Thus Tr acts on A and $\operatorname{Tr}(A) \subseteq A^{\mathbf{Z}/p}$. Since ρ is a map of $\mathbf{Z}/p$-modules, we have $\rho \circ \operatorname{Tr} = \operatorname{Tr} \circ \rho$. Furthermore, $\rho(A) = \mathbf{k}[V]^N$ implies $\operatorname{Im} \operatorname{Tr}^N \subseteq \rho(A)$. Either by interpreting Tr as the relative transfer, Tr_N^G (see Shank and Wehlau, 1999 for details), or by direct observation, we see that $\operatorname{Tr}^G = \operatorname{Tr} \circ \operatorname{Tr}^N$. Thus $\operatorname{Im} \operatorname{Tr}^G = \operatorname{Tr}(\operatorname{Im} \operatorname{Tr}^N) \subseteq \operatorname{Tr}(\rho(A)) = \rho(\operatorname{Tr}(A)) \subseteq \rho(A^{\mathbf{Z}/p})$. □

REMARK 7.2. As a consequence of the proposition, as long as G/N, in its action on W, is not generated by a transvection, we can use $\rho(A^{\mathbf{Z}/p})$ as input to Step 5 of Algorithm 5.7 (see Remark 5.8) to compute $\mathbf{k}[V]^G$. Thus replacing the cohomology calculation with a syzygy module calculation.

For a p-group G there is a composition series $\{e\} = G_0 \lhd G_1 \lhd G_2 \lhd \cdots \lhd G_{m+1} = G$ with $G_{i+1}/G_i \cong \mathbf{Z}/p$. Using the above method we may first compute $\mathbf{k}[V]^{G_2} = (\mathbf{k}[V]^{G_1})^{G_2/G_1}$. Then having computed $\mathbf{k}[V]^{G_2}$ we may again use the method to compute $\mathbf{k}[V]^{G_3} = (\mathbf{k}[V]^{G_2})^{G_3/G_2}$. Continuing in this manner we may finally compute $\mathbf{k}[V]^G = (\mathbf{k}[V]^{G_m})^{G/G_m}$. This iterated process is the *ladder algorithm* for computing $\mathbf{k}[V]^G$. The strength of the ladder algorithm is that at each rung we are computing the invariants and group cohomology with respect to the relatively simple group $G_{i+1}/G_i \cong \mathbf{Z}/p$.

8. An Example: $\mathbf{k}[2V_3]^{U_3}$

Here we illustrate the ladder algorithm by using it to compute the invariants of an interesting representation of a non-Abelian group of order p^3.

Let $\mathbf{k}$ be a field of characteristic p and let V_3 be a three-dimensional vector space over $\mathbf{k}$. Choose a basis, $\{x, y, z\}$ for V_3^* and define

$$G = U_3 := \left\{ \left. \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} \right| a, b, c \in \mathbf{F}_p \right\},$$

with the action on V_3^* given by

$$x \leftrightarrow \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}, \qquad y \leftrightarrow \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}, \qquad z \leftrightarrow \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}.$$

Let β denote the element of U_3 formed by taking $a = 0$, $b = 1$, and $c = 0$. Let α denote the element formed by taking $a = 1$, $b = 0$, and $c = 0$. Let γ denote the element formed by taking $a = 0$, $b = 0$, and $c = 1$. The (pseudo) reflections α, β and γ generate U_3. The invariants x, $N(y)$ and $N(z)$ form a homogeneous system of parameters for $\mathbf{k}[V_3]^{U_3}$ such that the product of the degrees equals the order of the group. Therefore $\mathbf{k}[V_3]^{U_3} = \mathbf{k}[x, N(y), N(z)]$ (see, for example, Smith, 1995, Proposition 5.5.5).

Consider the representation of U_3 afforded by $W = V_3 \oplus V_3 = 2V_3$. Since U_3 is generated by elements that act on W as bi-reflections, the representation satisfies Kemper's criteria (Kemper, 1999, Corollary 3.7) and the invariants could be Cohen–Macaulay. In fact a simple MAGMA (Bosma *et al.*, 1997) calculation shows that for $p = 2$ the invariants are Cohen–Macaulay. Using Kemper (2002, Theorem A) we know that the depth of the invariants of the isotropy subgroups give an upper bound on the depth of the invariants. However, for the representation W, all proper isotropy subgroups have Cohen–Macaulay rings of invariants so this result imposes no restriction on $\operatorname{depth}(\mathbf{k}[W]^{U_3})$. Thus there appears to be no simple method for deciding whether or not $\mathbf{k}[W]^{U_3}$ is Cohen–Macaulay for $p > 2$.

Using the ladder algorithm we will compute a complete list of generators for $\mathbf{k}[W]^{U_3}$ for the prime 3. The limitations of our computing resources prevent us from obtaining a complete list of generators for $\mathbf{k}[W]^{U_3}$ for primes greater than 3. However, the method does provide enough information for us to prove that $\mathbf{k}[W]^{U_3}$ is not Cohen–Macaulay for all primes $p \geq 3$.

Remark 8.1. Using Remark 5.5 one sees that $xN(y)$ lies in the radical of the image of the transfer in $\mathbf{k}[V_3]^G$. Therefore, in principle, one can construct a generating set for $\mathbf{k}[2V_3]^{U_3}$ using Algorithm 5.7 with $f_1 := x_1 N(y_1)$ and $f_2 := x_2 N(y_2)$. We were able to do this calculation, using MAGMA (Bosma *et al.*, 1997), for $p = 3$. However the $p = 5$ calculation was beyond the capabilities of the computers and algorithms at our disposal.

Take G_1 to be the subgroup generated by β and let G_2 be the subgroup generated by α and β. We have a two rung ladder $G_1 \lhd G_2 \lhd G$.

The action of β on W is the action of $\mathbf{Z}/p$ on $2V_1 \oplus 2V_2$. Using Campbell and Hughes (1997), we see that $\mathbf{k}[W]^\beta$ is generated by x_i, y_i, $N_\beta(z_i) := z_i^p - z_i x_i^{p-1}$ and $u_\beta := z_1 x_2 - z_2 x_1$. Take $A_1 := \mathbf{k}[x_1, y_1, N_1, x_2, y_2, N_2, U_\beta]$ with $\alpha(N_i) = N_i$ and $\alpha(U_\beta) = U_\beta$. Define $\rho_1 : A_1 \to \mathbf{k}[W]^\beta$ by $\rho_1(N_i) = N_\beta(z_i)$ and $\rho_1(U_\beta) = u_\beta$. Then ρ_1 is an α-equivariant algebra epimorphism and the kernel of ρ_1, J_1, is the principal ideal generated by $r := U_\beta^p - x_2^p N_1 + x_1^p N_2 - (x_1 x_2)^{p-1} U_\beta$.

Lemma 8.2. *The inclusion of J_1 into A_1 induces a monomorphism from $H^1(\langle\alpha\rangle, J_1)$ to $H^1(\langle\alpha\rangle, A_1)$ where $\langle\alpha\rangle \cong \mathbf{Z}/p$.*

Proof. An element in $H^1(\langle\alpha\rangle, J_1)$ which maps to zero in $H^1(\langle\alpha\rangle, A_1)$ is represented by rf with $f \in A_1$ and $rf = \Delta h$ for some $h \in A_1$. View h and r as polynomials in U. Since r is monic in U we can divide h by r to get $h = qr + \ell$ with $\deg_U(\ell) < \deg_U(r) = p$. Apply Δ

and use the fact that r is α-invariant to get $rf = \Delta h = (\Delta q)r + \Delta\ell$. Thus $\Delta\ell = (f - \Delta q)r$. The operator Δ does not increase the U-degree of a polynomial. Therefore $\deg_U(\Delta\ell) < p$. However $\deg_U(r) = p$. Thus $f - \Delta q = 0$. Therefore $\Delta(rq) = rf$ and rf represents zero in $H^1(\langle\alpha\rangle, J_1)$. □

As a consequence of the lemma, ρ_1 induces an epimorphism from A_1^α to $(\mathbf{k}[W]^\beta)^\alpha = \mathbf{k}[W]^{G_2}$. The action of α on the generators of A_1 is the action of $\mathbf{Z}/p$ on $3V_1 \oplus 2V_2$. Again using Campbell and Hughes (1997), we see that $\mathbf{k}[W]^{G_2}$ is generated by x_i, $N(y_i) = y_i^p - y_i x_i^{p-1}$, $u_\alpha := y_1x_2 - y_2x_1$, $N_\beta(z_i)$ and u_β. Take $A_2 := \mathbf{k}[x_1, H_1, N_1, x_2, H_2, N_2, U_\alpha, U_\beta]$ with $\gamma(N_i) = N_i + H_i$, $\gamma(U_\beta) = U_\beta + U_\alpha$ and the other generators invariant. Define $\rho_2 : A_2 \to \mathbf{k}[W]^{G_2}$ by $\rho_2(H_i) = N(y_i)$, $\rho_2(N_i) = N_\beta(z_i)$, $\rho_2(U_\alpha) = u_\alpha$ and $\rho_2(U_\beta) = u_\beta$. Then ρ_2 is a γ-equivariant algebra epimorphism. Let J_2 denote the kernel of ρ_2. A straightforward Gröbner basis calculation can be used to show that the kernel of the map from A_2 to $\mathbf{k}[W]$, given by ρ_2 followed by inclusion, is generated by $r := U_\beta^p - x_2^pN_1 + x_1^pN_2 - (x_1x_2)^{p-1}U_\beta$ and $s := \Delta r = U_\alpha^p - x_2^pH_1 + x_1^pH_2 - (x_1x_2)^{p-1}U_\alpha$. Thus we conclude that J_2 is generated by r and s.

The action of γ on A_2 is the action of $\mathbf{Z}/p$ on $2V_1 \oplus 3V_2$. Again using Campbell and Hughes (1997), we see that A_2^γ is generated by x_i, H_i, $N_\gamma(N_i)$, U_α, $N_\gamma(U_\beta)$, $U_{12} := N_1H_2 - N_2H_1$, $U_{13} := N_1U_\alpha - H_1U_\beta$, $U_{23} := N_2U_\alpha - H_2U_\beta$ and $\mathrm{Tr}(N_1^{e_1}N_2^{e_2}U_\beta^{e_3})$ for $e_j \le p-1$. Using Corollary 4.4, we need only include transfers with $e_1+e_2+e_3 > 2(p-1)$. Applying ρ_2 to this set gives

$$\begin{aligned}\mathcal{A} := {} & \{x_i, N(y_i), N(z_i) \mid i = 1, 2\} \cup \{u_\alpha, N_\gamma(u_\beta), u_{12}, u_{13}, u_{23}\} \\ & \cup \{\mathrm{Tr}_{G_2}^G(N_\beta(z_1)^{e_1}N_\beta(z_2)^{e_2}u_\beta^{e_3}) \mid e_j \le p-1 \text{ and } e_1+e_2+e_3 > 2(p-1)\},\end{aligned}$$

where $u_{12} := \rho_2(U_{12}) = N_\beta(z_1)N(y_2) - N_\beta(z_2)N(y_1)$, $u_{13} := \rho_2(U_{13}) = N_\beta(z_1)u_\alpha - u_\beta N(y_1)$ and $u_{23} := \rho_2(U_{23}) = N_\beta(z_2)u_\alpha - u_\beta N(y_2)$.

The ring $\mathbf{k}[W]^G$ is generated by the union of $\mathcal{A}$ and the preimage of a set of A_2^γ-module generators for the kernel of the map from $H^1(\langle\gamma\rangle, J_2)$ to $H^1(\langle\gamma\rangle, A_2)$.

We now turn our attention to the kernel of $i^1 : H^1(\langle\gamma\rangle, J_2) \to H^1(\langle\gamma\rangle, A_2)$. Define $s' := s - U_\alpha^p = x_1^pH_2 - x_2^pH_1 - (x_1x_2)^{p-1}U_\alpha$ and let K denote the A_2^γ-submodule of $H^1(\langle\gamma\rangle, A_2)$ consisting of the classes annihilated by s'.

LEMMA 8.3. *There is an epimorphism, say Φ, of A_2^γ-modules from K to* kernel(i^1) *which takes a class represented by $h \in A_2$ to an element represented by sh in* kernel(i^1). *If $\ell \in A_2$ with $\Delta\ell = sh$ then the connecting homomorphism takes $\rho_2(\ell)$ to $[sh]$.*

PROOF. Since $s \in A_2^\gamma$, if $h = h' + \Delta m$ then $sh = sh' + \Delta(sm)$ and, thus, sh and sh' represent the same class in $H^1(\mathbf{Z}/p, J_2)$. Therefore multiplication by s gives a well defined map from $H^1(\mathbf{Z}/p, A_2)$ to $H^1(\mathbf{Z}/p, J_2)$.

Elements in A_2^γ contained in the image of the transfer annihilate all elements of $H^1(\mathbf{Z}/p, A_2)$ (see, for example, Kemper, 2001, Corollary 2.4). Furthermore, $\mathrm{Tr}(U_\beta^{p-1}U_\alpha) = U_\alpha^p$. Thus s and $s' = s - U_\alpha^p$ annihilate the same submodule of $H^1(\mathbf{Z}/p, A_2)$. Hence if we restrict to K then $[sh] \in$ kernel(i^1) and we have a well defined map from K to kernel(i^1). Since A_2^γ is a commutative ring, this is a map of A_2^γ-modules.

Suppose $\mu \in$ kernel(i^1). Then $\mu = [\Delta f]$ for some $f \in A_2$. View f and r as polynomials in $U = U_\beta$ and divide f by r to get $f = qr + \ell$ with $\deg_U(\ell) < p$. Thus $\ell = f - qr$ and $\Delta\ell = \Delta f - \Delta(qr)$. Since $qr \in J_2$, $\Delta(qr)$ represents zero in $H^1(\mathbf{Z}/p, J_2)$. Thus $\Delta\ell$

and Δf represent the same element in $H^1(\mathbf{Z}/p, J_2)$ and $\mu = [\Delta\ell]$. Furthermore, Δ does not increase the U-degree. Therefore $\deg_U(\Delta\ell) < p$ and, since $\deg_U(r) = p$, $\Delta\ell$ lies in the principal ideal generated by s. Thus $\mu = [\Delta\ell] = [sh]$ for some $h \in A_2$. However $\mu \in \text{kernel}(i^1)$ implies $[h] \in K$. Hence the map is surjective.

Suppose that $\ell \in A_2$ with $\Delta\ell = sh$. Note that Δ gives the first differential in the cochain complex used to compute $H^*(\mathbf{Z}/p, A_2)$. As a consequence, using basic homological algebra, the connecting homomorphism takes $\rho_2(\ell)$ to $[sh]$. □

Suppose that $h \in A_2^\gamma$. Then $\Delta(hr) = h\Delta(r) = hs$ and, if $\text{Tr}(h) = 0$, $[h] \in K$ and $\Phi([h]) = 0$. Thus Φ determines an epimorphism of A_2^γ-modules from K_γ to kernel(i^1) where K_γ is the quotient of K by the submodule of cohomology classes represented by elements of A_2^γ.

THEOREM 8.4. *The A_2^γ-module* kernel(i^1) *is generated in degrees greater than* $3p$.

PROOF. Since Φ increases degree by $2p$, it is sufficient to show that K_γ is zero in degrees less than or equal to p. From Proposition 6.2, $H^1(\mathbf{Z}/p, A_2)$ is a free module over $\mathbf{k}[x_1, x_2, N_\gamma(N_1), N_\gamma(N_2)]$. Furthermore, any basis for $H^1(\mathbf{Z}/p, A_2^\flat)$ gives a set of module generators. Recall that $\deg(N_i) = \deg(H_i) = p$ and $\deg(U_\beta) = \deg(U_\alpha) = 2$. Therefore, if we restrict to degrees less than or equal to p we can take $U_\alpha^i[1]$, $[N_1]$, $[N_2]$, and $U_\alpha^j[U_\beta^\ell]$ with $i < (p-1)/2$ and $j + \ell < (p-1)/2$ as the generating set. Since we are interested in K_γ we may omit $U_\alpha^i[1]$. Using Lemma 6.4, $U_\alpha[U_\beta^\ell] = 0$ and so we can take $j = 0$. Let $f := c_1N_1 + c_2N_2 + c_3U_\beta^\ell$ where $c_1, c_2 \in \mathbf{k}$ and $c_3 \in \mathbf{k}[x_1, x_2]$ with $\deg(c_3) \leq p - 2\ell$. Suppose $s'[f] = 0$. Using Lemma 6.4, $[H_1N_1] = [H_2N_2] = [U_\alpha U_\beta^\ell] = 0$. Thus $s'[f] = x_1^p c_1[N_1H_2] + x_1^p c_3[H_2U_\beta^\ell] - x_2^p c_2[H_1N_2] - x_2^p c_3[H_1U_\beta^\ell] - (x_1x_2)^{p-1}[U_\alpha(c_1N_1 + c_2N_2)]$. We may assume that f is homogeneous. If $\deg(f) < p$ then $c_1 = c_2 = 0$ and $s'[f] = c_3(x_1^p[H_2U_\beta^\ell] - x_2^p[H_1U_\beta^\ell])$. From Lemma 6.4 and Proposition 6.2, $(x_1^p[H_2U_\beta^\ell] - x_2^p[H_1U_\beta^\ell]) \neq 0$. Thus $c_3 = 0$ and $f = 0$. If $\deg(f) = p$ then $\deg(c_3) = p - 2\ell > 0$ and $\{x_1^p, x_2^p, c_3x_1^p, c_3x_2^p, (x_1x_2)^{p-1}\}$ is a linearly independent subset of $\mathbf{k}[x_1, x_2]$. Therefore $c_1[H_1N_2] = c_2[H_2N_1] = c_3[H_1U_\beta^\ell] = 0$. Again using Lemma 6.4, $[H_1N_2] \neq 0$, $[H_2N_1] \neq 0$ and $[H_1U_\beta^\ell] \neq 0$. Thus $c_1 = c_2 = c_3 = 0$ and $f = 0$. □

THEOREM 8.5. *For $p = 3$, $\mathbf{k}[2V_3]^{U_3}$ is generated by $\mathcal{A}$ and one additional generator:*

$$\begin{aligned}\kappa := {} & (u_\alpha^{p-1} - (x_1x_2)^{p-1})u_{12}(u_\beta^2 - u_\beta u_\alpha) \\ & - x_2^p u_{23}(N_\beta(z_1^2) - N(y_1)N_\beta(z_1)) - x_1^p u_{13}(N_\beta(z_2^2) - N(y_2)N_\beta(z_2)) \\ & - (x_1^p N(y_2) + x_2^p N(y_1))(N_\beta(z_1z_2)u_\beta - u_{12}u_\beta + u_{23}N_\beta(z_1) - N(y_1)u_\alpha N_\beta(z_2)).\end{aligned}$$

PROOF. We use the description of $H^1(\mathbf{Z}/3, 3V_2)$ given in Theorem 6.5. Since we are interested in identifying K_γ we may omit cohomology classes represented by invariants. Thus it is sufficient to consider the module generated by $[N_1]$, $[N_2]$, $[U_\beta]$, and $U_{12}[U_\beta]$. Since $U_\alpha U_{12}[U_\beta] = 0$, $H_1U_{12}[U_\beta] = 0$ and $H_2U_{12}[U_\beta] = 0$, we see that $U_{12}[U_\beta]$ is in K_γ. To describe the corresponding invariant we need to find $f \in A_2$ such that $\Delta(f) = sU_{12}U_\beta$. Let $h := N_1N_2U_\beta - U_{12}U_\beta + U_{23}N_1 - H_1U_\alpha N_2$. Referring to the proof of Theorem 6.5, we see that

$$U_{12}\Delta(U_\beta^2 - U_\alpha U_\beta) = 2U_\alpha U_{12}U_\beta$$

$$H_1\Delta(h) + U_{23}\Delta(N_1^2 - N_1H_1) = 2H_1U_{12}U_\beta$$
$$H_2\Delta(h) + U_{13}\Delta(N_2^2 - N_2H_2) = H_2U_{12}U_\beta.$$

Let $f_1 := U_{12}(U_\beta^2 - U_\alpha U_\beta)$, $f_2 := H_1h + U_{23}(N_1^2 - N_1H_1)$, $f_3 := H_2h + U_{13}(N_2^2 - N_2H_2)$ and $f := f_1(U_\alpha^{p-1} - (x_1x_2)^{p-1}) - f_2x_2^p - f_3x_1^p$. Then $\Delta(f) = s(2U_{12}U_\beta)$ and $\rho_2(f) = \kappa$ is the corresponding invariant.

We still need to examine the contribution to K_γ from the module generated by $[N_1]$, $[N_2]$ and $[U_\beta]$. Multiplication by s' induces a map from this module to the module generated by $[U_{12}]$, $[U_{13}]$ and $[U_{23}]$. Using Theorem 6.5 we see that the matrix representing s' is

$$\begin{pmatrix} -x_1^3 & -x_2^3 & 0 \\ (x_1x_2)^2 & 0 & -x_2^p \\ 0 & (x_1x_2)^2 & x_1^3 \end{pmatrix}.$$

A generator for the kernel is given by $(x_2^3, -x_1^3, (x_1x_2)^2)$. In other words we get one more generator for K_γ, $x_2^3N_1 - x_1^3N_2 + (x_1x_2)^2U_\beta = U_\beta^3 - r$. However

$$\Delta(r(r - s + N_\gamma(U_\beta)) + sU_\beta U_\alpha(U_\alpha - U_\beta)) = s(U_\beta^3 - r).$$

Thus the corresponding invariant is zero. □

REMARK 8.6. For $p = 2$, $\mathbf{k}[2V_3]^{U_3}$ can be computed rather quickly using the invariant theory packages in MAGMA (Bosma *et al.*, 1997). When we first considered the problem, the $p = 3$ computation was beyond the capabilities of our computing facilities. Our original calculation for $p = 3$ was based, essentially, on Algorithm 5.7. The ladder calculations evolved out of an attempt to better understand the result and a so far unsuccessful attempt to extend the calculation to $p = 5$. Recently, Gregor Kemper, using a computer with 4 GB of RAM, has been able to construct a generating set for $p = 3$ using the invariant theory packages in MAGMA. His calculations agree with ours. As far as we know, no one has been able to construct a generating set for $p = 5$. The most effective approach to the $p = 5$ problem may well be the hybrid of Algorithm 5.7 and the ladder technique consisting of using the algebra generated by $\mathcal{A}$ as the input to Step 5 of Algorithm 5.7. For $p = 2$, $\mathbf{k}[2V_3]^{U_3}$ is Cohen–Macaulay. As we prove below, for $p > 2$, the invariants are not Cohen–Macaulay. This at least partly explains the dramatic increase in computational complexity in passing from $p = 2$ to 3.

THEOREM 8.7. *If $p > 2$, then $\mathbf{k}[2V_3]^{U_3}$ is not Cohen–Macaulay.*

PROOF. We will show that the partial homogeneous system of parameters $\{x_1, N(y_1), N(y_2)\}$ is not a regular sequence in $\mathbf{k}[2V_3]^{U_3}$. Clearly $\{x_1, N(y_1)\}$ is regular. Thus it is sufficient to show that $N(y_2)$ is a zero divisor in $\mathbf{k}[2V_3]^{U_3}/(x_1, N(y_1))\mathbf{k}[2V_3]^{U_3}$. We break the argument into two steps.

Step 1: Show that $u_{13}^2u_\alpha^{p-2}N(y_2) - (u_{12}N_\gamma(u_\beta) + u_{13}u_{23}u_\alpha^{p-2})N(y_1) \in (x_1)\mathbf{k}[2V_3]^{U_3}$.

Step 2: Show that $u_{13}^2u_\alpha^{p-2} \notin (x_1, N(y_1))\mathbf{k}[2V_3]^{U_3}$.

PROOF OF STEP 1. Observe that $u_{12}u_\alpha - u_{13}N(y_2) + u_{23}N(y_1) = 0$. Thus

$$\begin{aligned} u_{13}^2u_\alpha^{p-2}N(y_2) - u_{13}u_{23}u_\alpha^{p-2}N(y_1) &= u_{13}u_\alpha^{p-2}(u_{13}N(y_2) - u_{23}N(y_1)) \\ &= u_{13}u_\alpha^{p-2}u_{12}u_\alpha \end{aligned}$$

and $u_{13}^2 u_\alpha^{p-2} N(y_2) - (u_{12} N_\gamma(u_\beta) + u_{13} u_{23} u_\alpha^{p-2}) N(y_1) = u_{12}(u_{13} u_\alpha^{p-1} - N_\gamma(u_\beta) N(y_1))$. A simple calculation using the definitions of the appropriate invariants gives $u_{13} u_\alpha^{p-1} - N_\gamma(u_\beta) N(y_1) \equiv 0 \pmod{(x_1)\mathbf{k}[2V_3]}$. Therefore there exists $f \in \mathbf{k}[2V_3]$ such that $u_{13} u_\alpha^{p-1} - N_\gamma(u_\beta) N(y_1) = x_1 f$. Since $x_1 f$ and x_1 are both elements of $\mathbf{k}[2V_3]^{U_3}$ we have $f \in \mathbf{k}[2V_3]^{U_3}$ concluding the proof of Step 1.

Proof of Step 2. We use the graded reverse lexicographic order with $x_1 < y_1 < z_1 < x_2 < y_2 < z_2$. Suppose $u_{13}^2 u_\alpha^{p-2} = f N(y_1) + h x_1$ for $f, h \in \mathbf{k}[2V_3]^{U_3}$. Since $\mathrm{LM}(u_{13}^2 u_\alpha^{p-2}) = x_2^p y_1^p z_1^{2p} > \mathrm{LM}(h x_1)$ we have $\mathrm{LM}(u_{13}^2 u_\alpha^{p-2}) = \mathrm{LM}(f N(y_1))$. Therefore $\mathrm{LM}(f) = x_2^p z_1^{2p}$. We will show that there is no element of $\mathbf{k}[2V_3]^{U_3}$ with this lead monomial. Using Theorem 8.4 we see that we need only consider elements in the algebra generated by $\mathcal{A}$. Elements from $\mathcal{A}$ of the form $\mathrm{Tr}^G_{G_2}(N_\beta(z_1)^{e_1} N_\beta(z_2)^{e_2} u_\beta^{e_3})$ have degree $p(e_1+e_2)+2e_3$ and must satisfy $e_i \le p-1$ and $e_1+e_2+e_3 > 2(p-1)$. The smallest possible degree for such an element is $2(p-1)+p^2$ and comes from taking $e_3 = p-1$ and $e_1+e_2 = p$. As long as $p > 2$, $p^2 + 2(p-1) > 3p$ and so we can restrict to the subalgebra generated by

$$\{x_i, N(y_i), N(z_i) \mid i = 1, 2\} \cup \{u_\alpha, N_\gamma(u_\beta), u_{12}, u_{13}, u_{23}\}.$$

The corresponding lead monomials are

$$\{x_i, y_i^p, z_i^{p^2} \mid i = 1, 2\} \cup \{y_1 x_2, (z_1 x_2)^p, (z_1 y_2)^p, z_1^p y_1 x_2, z_2^p y_1 x_2\}.$$

Clearly $x_2^p z_1^{2p}$ is not a product of monomials from this list. Therefore f comes from a tête-a-tête. All of our generators are homogeneous with respect to the bidegree so the tête-a-tête must occur in bidegree $(2p, p)$. The monomials of bidegree $(2p, p)$ which are greater than $x_2^p z_1^{2p}$ are of the form $z_1^{2p} m$ where m has bidegree $(0, p)$ and $m > x_2^p$. Since there are no tête-a-têtes generated by monomials of this form, there is no suitable f. □

Acknowledgements

We thank Gregor Kemper for reading an earlier draft of this paper and suggesting some improvements and corrections. DLW's research was partially supported by grants from ARP and NSERC.

References

Almkvist, G., Fossum, R. (1978). *Decompositions of Exterior and Symmetric Powers of Indecomposable* $\mathbf{Z}/p$*-modules in Characteristic p*, LNM **641**, pp. 1–114. Springer.

Alperin, J. L. (1986). *Local Representation Theory*, Cambridge University Press.

Benson, D. J. (1993). *Polynomial Invariants of Finite Groups*, Cambridge University Press.

Bosma, W., Cannon, J. J., Playoust, C. (1997). The Magma algebra system I: the user language. *J. Symb. Comput.*, **24**, 235–265.

Campbell, H. E. A., Hughes, I. P. (1997). Vector invariants of $U_2(\mathbf{F}_p)$: a proof of a conjecture of Richman. *Adv. Math.*, **126**, 1–20.

Cox, D., Little, J., O'Shea, D. (1992). *Ideals, Varieties, and Algorithms*, Springer.

Dickson, L. E. (1966). On invariants and the theory of numbers. In *The Madison Colloquium (1913)*, Am. Math. Soc., reprinted by Dover.

Eisenbud, D. (1996). *Commutative Algebra with a View Toward Algebraic Geometry*, Springer.

Evens, L. (1991). *The Cohomology of Groups, Oxford Math. Monographs*, Clarendon Press.

Fleischmann, P. (2000). The Noether bound in invariant theory of finite groups. *Adv. Math.*, **152**, 23–32.

Fogarty, J. (2001). On Noether's bound for polynomial invariants of a finite group. *Electron. Res. Announc. Am. Math. Soc.*, **7**, 5–7.

Göbel, M. (1995). Computing bases for rings of permutation-invariant polynomials. *J. Symb. Comput.*, **19**, 285–291.
Göbel, M. (1998). A constructive description of SAGBI bases for polynomial invariants of permutation groups. *J. Symb. Comput.*, **26**, 261–272.
Hughes, I., Kemper, G. (2002). Symmetric powers of modular representations, Hilbert series and degree bounds. *Comm. Alg.*, **28**, 2059–2088.
Kapur, D., Madlener, K. (1989). A completion procedure for computing a canonical basis of a k-subalgebra. In Kaltofen, E., Watt, S. eds, *Proceedings of Computers and Mathematics* 89, pp. 1–11. MIT.
Kemper, G. (1999). On the Cohen–Macaulay property of modular invariant rings. *J. Algebra*, **215**, 330–351.
Kemper, G. (2001). The depth of invariant rings and cohomology, (with an appendix by K. Magaard). *J. Algebra*, **245**, 463–531.
Kemper, G. (2002). Loci in quotients by finite groups, pointwise stabilizers and the buchsbaum property. *J. Reine Angew. Math.*, **547**, 69–96.
Miller, J. L. (1996). Analogs of Gröbner bases in polynomial rings over a ring. *J. Symb. Comput.*, **21**, 139–153.
Noether, E. (1916). Der endlichkeitssatz der invarianten endlicher Gruppen. *Math. Ann.*, **77**, 89–92.
Noether, E. (1926). Der endlichkeitssatz der invarianten endlicher linearer Gruppen der characteristik p. *Nachr. v.d.Ges. d. Wiss. zu Göttingen*, 28–35.
Richman, D. R. (1990). On vector invariants over finite fields. *Adv. Math.*, **81**, 30–65.
Robbiano, L., Sweedler, M. (1990). *Subalgebra Bases*, LNM **1430**, pp. 61–87. Springer.
Schwarz, G. W. (1980). Lifting smooth homotopies of orbit spaces. *Inst. Hautes Études Sci. Publ. Math.*, **51**, 37–135.
Shank, R. J. (1998). S.A.G.B.I. bases for rings of formal modular semiinvariants. *Commentarii Mathematici Helvetici*, **73**, 548–565.
Shank, R. J., Wehlau, D. L. (1999). The transfer in modular invariant theory. *J. Pure Appl. Algebra*, **142**, 63–77.
Shank, R. J., Wehlau, D. L. (2002). Noether numbers for subrepresentations of cyclic groups of prime order. *Bull. London Math. Soc.*, **34**, 438–450.
Smith, L. (1995). *Polynomial Invariants of Finite Groups*, Wellesley, MA, A. K. Peters.
Sturmfels, B. (1996). *Gröbner Bases and Convex Polytopes*, ULS **8**, American Mathematical Society.
Wehlau, D. L. (1993). Equidimensional representations of 2-simple groups. *J. Algebra*, **154**, 437–489.