Bull. London Math. Soc. 34 (2002) 438–450
DOI: 10.1112/S0024609302001054

NOETHER NUMBERS FOR SUBREPRESENTATIONS OF CYCLIC GROUPS OF PRIME ORDER

R. JAMES SHANK AND DAVID L. WEHLAU

ABSTRACT

Let W be a finite-dimensional $\mathbb{Z}/p$-module over a field, $\mathbf{k}$, of characteristic p. The maximum degree of an indecomposable element of the algebra of invariants, $\mathbf{k}[W]^{\mathbb{Z}/p}$, is called the Noether number of the representation, and is denoted by $\beta(W)$. A lower bound for $\beta(W)$ is derived, and it is shown that if U is a $\mathbb{Z}/p$ submodule of W, then $\beta(U) \leqslant \beta(W)$. A set of generators, in fact a SAGBI basis, is constructed for $\mathbf{k}[V_2 \oplus V_3]^{\mathbb{Z}/p}$, where V_n is the indecomposable $\mathbb{Z}/p$-module of dimension n.

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 finite subgroup G of $\mathrm{GL}(V)$. 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^*, $\mathbf{k}[V] = \mathbf{k}[x_1, \ldots, x_n]$. The *ring of invariants* of G is the subring of $\mathbf{k}[V]$ given by

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

We say that the representation of G on V is *modular* if the characteristic of $\mathbf{k}$ divides the order of G. We say the representation is *non-modular* if $|G|$ is invertible in $\mathbf{k}$. For an introduction to the invariant theory of finite groups, we recommend [**3**] or [**22**].

Suppose that $R = \oplus_{i=0}^{\infty} R_i$ is a finitely generated graded algebra. Let R_+ denote the augmentation ideal of R, that is, the ideal generated by the homogeneous elements of positive degree. We call an element of R *decomposable* if it lies in the ideal $(R_+)^2$. Otherwise we say the element is *indecomposable in* R. The *Noether number* of R, $\beta(R)$, is the least integer d such that the set $\oplus_{i=0}^{d} R_i$ generates R as an algebra. In other words, $\beta(R)$ is the largest degree of a homogeneous indecomposable element of R. If $R = \mathbf{k}[V]^G$, we shall often write $\beta(V)$ in place of $\beta(R)$ if the group G is clear from the context.

Emmy Noether [**18**] proved that if the characteristic of $\mathbf{k}$ is zero, or if it exceeds $|G|$, then $\beta(V) \leqslant |G|$. Fleischmann [**14**] and Fogarty [**12**] recently proved that the same bound holds for the general non-modular case. Much less is known about $\beta(V)$ in the modular case. Göbel [**15**] proved that, for any characteristic, if G acts by permuting a basis of V, then $\beta(V) \leqslant \binom{\dim V}{2}$. Recently, Hughes and Kemper [**16**] found bounds for $\beta(V)$ for any modular representation of $\mathbb{Z}/p$. Here, we shall show that if W is a representation of $\mathbb{Z}/p$ in characteristic p and U is a subrepresentation, then $\beta(U) \leqslant \beta(W)$. We shall also give a lower bound for $\beta(V)$ for any modular representation of $\mathbb{Z}/p$, and we compute a SAGBI basis for $\mathbf{k}[V_2 \oplus V_3]^{\mathbb{Z}/p}$, where $\mathbf{k}$ is

Received 17 August 2000; revised 13 May 2001.

2000 *Mathematics Subject Classification* 13A50, 20J06.

The research of the second author is supported by grants from ARP and NSERC. This work was done during a visit of the second author to the University of Kent at Canterbury.

a field of characteristic p and V_n is the indecomposable $\mathbb{Z}/p$-module of dimension n. The term 'SAGBI' is an acronym for **S**ubalgebra **A**nalog to **G**röbner **B**ases for **I**deals, and was introduced by Robbiano and Sweedler [**20**]. The concept was introduced independently by Kapur and Madlener [**17**]. In the final section of the paper, we discuss a conjectured value for the Noether number of the regular modular representation of $\mathbb{Z}/p$.

Let R be a finitely generated graded algebra. We shall denote by $\mathscr{P}(R, \lambda)$ the *Hilbert series* of R: $\mathscr{P}(R, \lambda) := \sum_{d=0}^{\infty} (\dim_{\mathbf{k}} R_d)\lambda^d$. A sequence of homogeneous elements $h_1, h_2, \ldots, h_n$ in R_+ is a *homogeneous system of parameters* if R is a finitely generated module over the subalgebra generated by $h_1, h_2, \ldots, h_n$. The *Krull dimension* of R is the length, n, of a homogeneous system of parameters for R. A sequence of homogeneous elements $h_1, h_2, \ldots, h_k$ in R_+ is *regular* if, for each $i \leqslant k$, h_i is not a zero-divisor on $R/(h_1, \ldots, h_{i-1})R$. 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 [**9**].

2. *Preliminaries*

In this paper we consider the invariant theory of $\mathbb{Z}/p$, the cyclic group of order p, over a field $\mathbf{k}$ of characteristic p. We denote by σ a fixed generator of $\mathbb{Z}/p$. In the group ring, $\mathbf{k}(\mathbb{Z}/p)$, define $\Delta := \sigma - 1$ and $\mathrm{Tr} := \sum_{i=1}^{p} \sigma^i$. Note that $\mathrm{Tr} = \Delta^{p-1}$. Further, note that Tr gives a homomorphism, called the *transfer*, of $\mathbf{k}[V]^{\mathbb{Z}/p}$-modules: $\mathrm{Tr}^{\mathbb{Z}/p} : \mathbf{k}[V] \to \mathbf{k}[V]^{\mathbb{Z}/p}$.

There are exactly p distinct inequivalent indecomposable representations of $\mathbb{Z}/p$, one of each dimension $1, 2, \ldots, p$. We shall denote the indecomposable representation of $\mathbb{Z}/p$ of dimension n by V_n. Note that V_p is the unique indecomposable projective $\mathbb{Z}/p$-module, and V_1 is the unique simple $\mathbb{Z}/p$-module. We choose a basis, $\{e_1, \ldots, e_p\}$, for 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 $\mathbb{Z}/p$-submodule isomorphic to V_n, and we have $\mathbb{Z}/p$-equivariant inclusions: $V_1 \subset V_2 \subset \ldots \subset V_p$. Note that $V_n^{\mathbb{Z}/p}$ is isomorphic to V_1.

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

$$H^0(\mathbb{Z}/p, M) = \mathrm{kernel}(\Delta|_M) = M^{\mathbb{Z}/p},$$

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

$$H^2(\mathbb{Z}/p, M) = \frac{\mathrm{kernel}(\,\Delta|_M\,)}{\mathrm{image}(\mathrm{Tr}\,|_M)},$$

and, for $i > 0$, $H^{2i+1}(\mathbb{Z}/p, M) = H^1(\mathbb{Z}/p, M)$ and $H^{2i}(\mathbb{Z}/p, M) = H^2(\mathbb{Z}/p, M)$. A $\mathbb{Z}/p$-module decomposition of M gives a vector space decomposition of $H^*(\mathbb{Z}/p, M)$. Thus it is important to understand $H^*(\mathbb{Z}/p, V_n)$. Using the fact that $\mathrm{Tr} = \Delta^{p-1}$, we see that $H^1(\mathbb{Z}/p, V_p) = H^2(\mathbb{Z}/p, V_p) = 0$ and, for $n < p$, the element e_n represents a non-zero class in the one-dimensional vector space $H^1(\mathbb{Z}/p, V_n)$, whereas e_1 represents a non-zero class in the one-dimensional vector space $H^2(\mathbb{Z}/p, V_n)$. We are particularly interested in $H^1(\mathbb{Z}/p, \mathbf{k}[V])$. Since the action of $\mathbf{k}[V]^{\mathbb{Z}/p}$ on $\mathbf{k}[V]$ commutes with both Δ and Tr, $H^1(\mathbb{Z}/p, \mathbf{k}[V])$ is a $\mathbf{k}[V]^{\mathbb{Z}/p}$-module. Furthermore, $\mathbf{k}[V]^{\mathbb{Z}/p}$ is a Noetherian ring, and $H^1(\mathbb{Z}/p, \mathbf{k}[V])$ is a quotient of a submodule of the finitely generated module $\mathbf{k}[V]$. Therefore $H^1(\mathbb{Z}/p, \mathbf{k}[V])$ is a finitely generated $\mathbf{k}[V]^{\mathbb{Z}/p}$-module. We direct the reader to [**11**] for a detailed discussion of group cohomology.

Every $\mathbb{Z}/p$-module may be written as a direct sum of copies of indecomposable modules. Note that $\mathbf{k}[W \oplus V_1]^{\mathbb{Z}/p} \cong \mathbf{k}[W]^{\mathbb{Z}/p} \otimes \mathbf{k}[V_1]$. Thus, to study the ring of invariants of a module V, it suffices to consider modules having no summand isomorphic to V_1. We shall say that a $\mathbb{Z}/p$-module W is *reduced* if W contains no summands isomorphic to V_1.

Consider the vector space of linear functionals V_n^*. Since V_n^* is an indecomposable $\mathbb{Z}/p$-module, V_n^* and V_n are isomorphic. We shall call an element, z, of V_n^* a *distinguished variable* for V_n if z is a generator of the cyclic $\mathbb{Z}/p$-module V_n^*. Equivalently, z is a distinguished variable if z restricted to ${V_n}^{\mathbb{Z}/p}$ 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 shall exploit, is the fact that $\deg_z(\sigma(f)) = \deg_z(f)$. Dual to the inclusion of V_n into V_{n+1} we have a $\mathbb{Z}/p$-equivariant surjection $V_{n+1}^* \to V_n^*$. Note that this surjection carries a distinguished variable of V_{n+1} to a distinguished variable of V_n.

Consider a $\mathbb{Z}/p$-module W. Decompose W into a direct sum of indecomposable $\mathbb{Z}/p$-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 $f \in \mathbf{k}[W]^{\mathbb{Z}/p}$. 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

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

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 $f = f_1 N_1 + f_2 N_2 + \ldots + f_t N_t + r$ is a normal decomposition of f with respect to this Gröbner basis. We shall call this the *norm decomposition* of f. Note that the norm decomposition depends upon the choice of the z_i, but is otherwise unique.

PROPOSITION 2.1. *Suppose that $f \in \mathbf{k}[W]^{\mathbb{Z}/p}$, and consider its norm decomposition: $f = f_1 N_1 + f_2 N_2 + \ldots + f_t N_t + r$. Then $f_1, f_2, \ldots, f_t, r \in \mathbf{k}[W]^{\mathbb{Z}/p}$*

Proof. Applying σ, we have $f = \sigma(f_1) \cdot N_1 + \sigma(f_2) \cdot N_2 + \ldots + \sigma(f_t) \cdot N_t + \sigma(r)$. Since $\deg_{z_i}(\sigma(r)) = \deg_{z_i}(r)$ and $\deg_{z_i}(\sigma(f_j)) = \deg_{z_i}(f_j)$ for all i and j, the uniqueness of the norm decomposition shows that $\sigma(r) = r$ and $\sigma(f_j) = f_j$ for all j. □

Denote by $\mathbf{k}[W]^{\sharp}$ the ideal of $\mathbf{k}[W]$ generated by $N_1, N_2, \ldots, N_t$. 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 $\mathbf{k}[W]^{\flat}$ and $\mathbf{k}[W]^{\sharp}$ are both $\mathbb{Z}/p$-stable, and we have the decomposition

$$\mathbf{k}[W] = \mathbf{k}[W]^{\sharp} \oplus \mathbf{k}[W]^{\flat}.$$

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

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

Furthermore, $\mathbf{k}[V_n]^{\flat}_d$ is a free $\mathbb{Z}/p$-module for all $d \geqslant p - n + 1$ (see [**1**] or [**16**, Lemma 2.10]). Thus $\mathbf{k}[W]^{\flat}_{(d_1,\ldots,d_t)}$ is free if any $d_i \geqslant p - \dim(W_i) + 1$.

3. *Lower bounds*

It is well known (see, for example, [**5**] or [**19**]) that $\mathbf{k}[2\,V_2]^{\mathbb{Z}/p} = \mathbf{k}[x_1, N_1, x_2, N_2, u]$, where $N_1 = y_1^p - y_1 x_1^{p-1}$, $N_2 = y_2^p - y_2 x_2^{p-1}$, $u = x_2 y_1 - x_1 y_2$, and $\{x_1, y_1, x_2, y_2\}$ is a basis for $(2\,V_2)^*$ with $\Delta y_1 = x_1$, $\Delta x_1 = 0$, $\Delta y_2 = x_2$, and $\Delta x_2 = 0$. In particular, $\beta(2\,V_2) = p$. The next proposition shows that this is the only reduced decomposable representation of $\mathbb{Z}/p$ with such a low value of β.

PROPOSITION 3.1. *Suppose that W is a non-zero reduced $\mathbb{Z}/p$-module with $W \ncong 2\,V_2$. Then*

$$\beta(W) \geqslant \max\left\{p, (p-1)\dim W^{\mathbb{Z}/p}\right\}.$$

Proof. Let t denote $\dim W^{\mathbb{Z}/p}$. Note that $p \leqslant t(p-1)$ unless $t = 1$. Decompose W into a direct sum of indecomposable $\mathbb{Z}/p$-modules:

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

Denote by z_i a distinguished variable for W_i. Suppose first that $t = 1$. By hypothesis, $W_1 = V_n$ for some $n > 1$. Thus there is an inclusion of $\mathbb{Z}/p$-modules $V_2 \hookrightarrow V_n = W_1$ giving rise to a surjection of $\mathbb{Z}/p$-modules, $W_1^* \to V_2^*$. The surjection takes the distinguished variable z_1 to a distinguished variable, say y. The induced map $\mathbf{k}[V_n]^{\mathbb{Z}/p} \to \mathbf{k}[V_2]^{\mathbb{Z}/p}$ takes N_1, the norm of z_1, to $N = y^p - (\Delta y)^{p-1} y$, the norm of y. A decomposition of N_1 would give a decomposition of N. However, it is well known that $\mathbf{k}[V_2]^{\mathbb{Z}/p} = \mathbf{k}[\Delta(y), N]$ (see, for example, [**5**], [**19**] or [**22**, Chapter 5, Section 6, Example 3]) and thus N is indecomposable. Therefore N_1 is an indecomposable invariant of degree p, and the proposition follows for the case $t = 1$.

For the remainder of the proof, we suppose that $t \geqslant 2$. Define

$$f := \mathrm{Tr}^{\mathbb{Z}/p}\left(z_1^{p-1} z_2^{p-1} \ldots z_t^{p-1}\right).$$

We shall show that f is an indecomposable invariant, and therefore that $\beta(W) \geqslant \deg(f) = t(p-1)$.

There is a $\mathbb{Z}/p$-module injection of $t\,V_2$ into W. This induces a surjection $\rho : \mathbf{k}[W] \to \mathbf{k}[t\,V_2]$. If $t \geqslant 3$, then $\rho(f)$ is an indecomposable invariant in $\mathbf{k}[t\,V_2]^{\mathbb{Z}/p}$ (see [**19**, Proposition 0.6, p. 31] or [**5**, Corollary, p. 4]). Since ρ induces an algebra map of the rings of invariants, f is indecomposable in $\mathbf{k}[W]^{\mathbb{Z}/p}$.

The only remaining case is $t = 2$. Since $W \ncong 2\,V_2$, there is a $\mathbb{Z}/p$-module injection of $V_2 \oplus V_3$ into W. This induces a surjection $\tau : \mathbf{k}[W] \to \mathbf{k}[V_2 \oplus V_3]$. By Corollary 5.2 below, $\tau(f)$ is indecomposable in $\mathbf{k}[V_2 \oplus V_3]^{\mathbb{Z}/p}$, and thus f is an indecomposable invariant. □

4. *The main theorem*

Suppose that U is a $\mathbb{Z}/p$-submodule of W. Decomposing U and W into indecomposable $\mathbb{Z}/p$-modules gives

$$W = \bigoplus_{i=1}^{t} W_i \qquad \text{and} \qquad U = \bigoplus_{i=1}^{s} U_i,$$

where we label the summands so that $\dim(W_i) \geqslant \dim(W_{i+1})$ and $\dim(U_i) \geqslant \dim(U_{i+1})$.

LEMMA 4.1. *There exists a $\mathbb{Z}/p$-module monomorphism, $\phi : U \to W$, satisfying $\phi(U_i) \subseteq W_i$ for $i = 1, 2, \ldots, s$.*

Proof. Decomposing U and W gives

$$W \cong \bigoplus_{j=1}^{p} n_j V_j \qquad \text{and} \qquad U \cong \bigoplus_{j=1}^{p} m_j V_j,$$

where n_j and m_j are non-negative integers. Clearly, if $\sum_{j=\ell}^{p} n_j \geqslant \sum_{j=\ell}^{p} m_j$ for all ℓ, then ϕ can be constructed by starting with the largest indecomposable summands of U and working down.

Let k be the largest integer such that $n_k \neq 0$. We prove that $\sum_{j=\ell}^{p} n_j \geqslant \sum_{j=\ell}^{p} m_j$ for all ℓ by induction on k. If $k = 1$, then $W = W^{\mathbb{Z}/p}$, and the result follows. Suppose that $k > 1$. Observe that $U^{\mathbb{Z}/p} = U \cap W^{\mathbb{Z}/p}$, and therefore inclusion induces a monomorphism from $U/U^{\mathbb{Z}/p}$ to $W/W^{\mathbb{Z}/p}$. Taking a quotient by the fixed points will map V_j to V_{j-1} for $j > 1$, and V_1 to the zero space. Thus

$$W/W^{\mathbb{Z}/p} \cong \bigoplus_{j=2}^{p} n_j V_{j-1} \qquad \text{and} \qquad U/U^{\mathbb{Z}/p} \cong \bigoplus_{j=2}^{p} m_j V_{j-1}.$$

Therefore the induction hypothesis gives $\sum_{j=\ell}^{p} n_j \geqslant \sum_{j=\ell}^{p} m_j$ for $\ell > 1$. For $\ell = 1$, $\sum_{j=1}^{p} n_j = \dim(W^{\mathbb{Z}/p}) \geqslant \dim(U^{\mathbb{Z}/p}) = \sum_{j=1}^{p} m_j$. □

THEOREM 4.2. *Suppose that U is a $\mathbb{Z}/p$-submodule of W. Then $\beta(W) \geqslant \beta(U)$.*

Proof. Decompose W into a direct sum of indecomposable $\mathbb{Z}/p$-modules,

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

Since β is preserved by a $\mathbb{Z}/p$-module isomorphism, we may replace U with the image of U under the monomorphism ϕ given by Lemma 4.1. Having made this replacement, we have

$$U = \bigoplus_{i=1}^{s} U_i,$$

where $U_i = U \cap W_i$.

Note that if U is a summand of W, the result is clear. As a consequence, we may assume that U is not contained in any proper summand of W; that is, we may assume that $s = t$. Clearly, we may assume that both U and W are reduced $\mathbb{Z}/p$-modules. If $U \cong 2\,V_2$, then $\beta(U) = p$ (see the discussion preceding Proposition 3.1),

and thus by Proposition 3.1, we find that $\beta(U) \leqslant \beta(W)$. Hence we also suppose that $U \ncong 2V_2$.

The inclusion of U into W induces a surjection of algebras $\rho : \mathbf{k}[W] \to \mathbf{k}[U]$. Let J denote the kernel of ρ. The short exact sequence of $\mathbb{Z}/p$-modules

$$0 \to J \xrightarrow{\gamma} \mathbf{k}[W] \xrightarrow{\rho} \mathbf{k}[U] \to 0$$

gives rise to a long exact sequence in group cohomology

$$0 \to J^{\mathbb{Z}/p} \to \mathbf{k}[W]^{\mathbb{Z}/p} \xrightarrow{\rho} \mathbf{k}[U]^{\mathbb{Z}/p} \to H^1(\mathbb{Z}/p, J) \xrightarrow{\gamma^1} H^1(\mathbb{Z}/p, \mathbf{k}[W]) \to \dots .$$

The maps in the above sequence are all $\mathbf{k}[W]^{\mathbb{Z}/p}$-module homomorphisms.

The ring of invariants $\mathbf{k}[U]^{\mathbb{Z}/p}$ is generated as an algebra by $\rho(\mathbf{k}[W]^{\mathbb{Z}/p})$ together with the preimage of kernel(γ^1). The assumptions that we made above, together with Proposition 3.1, imply that $\beta(U) \geqslant t(p-1)$. Therefore, to prove the theorem it suffices to show that the kernel of γ^1 is generated, as a $\mathbf{k}[W]^{\mathbb{Z}/p}$-module, in degrees less than $t(p-1)$.

For each summand W_i, choose a distinguished variable, z_i, and let N_i denote its norm. Define $\widetilde{z_i} := \rho(z_i)$ and $\widetilde{N_i} := \rho(N_i)$. Note that $\widetilde{z_i}$ is a distinguished variable for U_i, and the norm of $\widetilde{z_i}$ is $\widetilde{N_i}$. Therefore, the map ρ respects the decompositions $\mathbf{k}[U] = \mathbf{k}[U]^\sharp \oplus \mathbf{k}[U]^\flat$ and $\mathbf{k}[W] = \mathbf{k}[W]^\sharp \oplus \mathbf{k}[W]^\flat$.

Define $J^\sharp := J \cdot \mathbf{k}[W]^\sharp$. Clearly, $J^\sharp \subseteq J \cap \mathbf{k}[W]^\sharp$. We shall now prove that these ideals are in fact equal.

Choose $f \in J \cap \mathbf{k}[W]^\sharp$, and let $f = f_1 N_1 + f_2 N_2 + \dots + f_t N_t$ be its norm decomposition. Then $0 = \rho(f) = \rho(f_1)(\widetilde{N_1}) + \rho(f_2)(\widetilde{N_2}) + \dots + \rho(f_t)(\widetilde{N_t})$. For $i < j$, we have $\deg_{z_i}(f_j) < p$, and thus also $\deg_{\widetilde{z_i}}(\rho(f_j)) < p$. By the uniqueness of the norm decomposition of 0 in $\mathbf{k}[U]$, this implies that $\rho(f_1) = \rho(f_2) = \dots = \rho(f_t) = 0$; that is, $f_1, f_2, \dots, f_t \in J$. Therefore $f \in J \cdot \mathbf{k}[W]^\sharp$, and this shows that $J \cap \mathbf{k}[W]^\sharp = J \cdot \mathbf{k}[W]^\sharp$.

We define $J^\flat = J \cap \mathbf{k}[W]^\flat$, and obtain $J = J^\sharp \oplus J^\flat$.

Thus our short exact sequence separates into two short exact sequences:

$$0 \to J^\sharp \xrightarrow{\gamma^\sharp} \mathbf{k}[W]^\sharp \xrightarrow{\rho^\sharp} \mathbf{k}[U]^\sharp \to 0$$

and

$$0 \to J^\flat \xrightarrow{\gamma^\flat} \mathbf{k}[W]^\flat \xrightarrow{\rho^\flat} \mathbf{k}[U]^\flat \to 0.$$

Furthermore, γ^1 separates into the two graded vector space homomorphisms:

$$(\gamma^1)^\sharp : H^1(\mathbb{Z}/p, J^\sharp) \to H^1(\mathbb{Z}/p, \mathbf{k}[W]^\sharp)$$

and

$$(\gamma^1)^\flat : H^1(\mathbb{Z}/p, J^\flat) \to H^1(\mathbb{Z}/p, \mathbf{k}[W]^\flat).$$

Consider the latter homomorphism first. We know that $\mathbf{k}[W]^\flat_{(d_1,d_2,\dots,d_t)}$ is free if some $d_i \geqslant p - \dim W_i + 1$. Similarly, $\mathbf{k}[U]^\flat_{(d_1,d_2,\dots,d_t)}$ is free if some $d_i \geqslant p - \dim U_i + 1$. Thus both $\mathbf{k}[W]^\flat_{(d_1,d_2,\dots,d_t)}$ and $\mathbf{k}[U]^\flat_{(d_1,d_2,\dots,d_t)}$ are free if some $d_i \geqslant p-1$. In particular, both $\mathbf{k}[W]^\flat_d$ and $\mathbf{k}[U]^\flat_d$ are free if $d \geqslant t(p-1)$. Therefore, for $d \geqslant t(p-1)$, $\rho^\flat_d$ is a surjection between free modules. Thus the map splits and the kernel, $J^\flat_d$, is also free. Therefore $H^1(\mathbb{Z}/p, J^\flat)_d = 0$ for all $d \geqslant t(p-1)$. In particular, kernel$(\gamma^1) \cap H^1(\mathbb{Z}/p, J^\flat)_d = \{0\}$ for all $d \geqslant t(p-1)$.

Thus we have reduced the problem to considering the kernel of $(\gamma^1)^\sharp$. Consider a cohomology class $[f] \in$ kernel$((\gamma^1)^\sharp)$. We shall show that $[f]$ is not a $\mathbf{k}[W]^{\mathbb{Z}/p}$-module

generator of kernel(γ^1). We have $f \in J \cap \mathbf{k}[W]^\sharp$. Let $f = f_1N_1 + f_2N_2 + \ldots + f_tN_t$ be the norm decomposition of f. By the proof that $J \cap \mathbf{k}[W]^\sharp = J \cdot \mathbf{k}[W]^\sharp$, we know that $f_1, f_2, \ldots, f_t \in J$. Since f represents a cohomology class, $\mathrm{Tr}(f) = 0$. Thus $\mathrm{Tr}(f_1)N_1 + \mathrm{Tr}(f_2)N_2 + \ldots + \mathrm{Tr}(f_t)N_t = 0$. Since $\deg_{z_i}(\mathrm{Tr}(f_j)) \leqslant \deg_{z_i}(f_j) < p$ for all $i < j$, this must be the norm decomposition of 0; that is, $\mathrm{Tr}(f_1) = \mathrm{Tr}(f_2) = \ldots = \mathrm{Tr}(f_t) = 0$. Therefore, each function $f_1, f_2, \ldots, f_t$ itself represents a cohomology class in $H^1(\mathbb{Z}/p, J)$.

Now $(\gamma^1)^\sharp([f]) = 0$ means that there exists some $h \in \mathbf{k}[W]^\sharp$ such that $\Delta(h) = f$. Let $h = h_1N_1 + h_2N_2 + \ldots + h_tN_t$ be the norm decomposition of h. Then $\Delta(h) = \Delta(h_1)N_1 + \Delta(h_2)N_2 + \ldots + \Delta(h_t)N_t$, where $\deg_{z_i}(\Delta(h_j)) \leqslant \deg_{z_i}(h_j) < p$ for all $i < j$. Therefore, by the uniqueness of the norm decomposition of f, we have $\Delta(h_j) = f_j$ and $\gamma^1([f_j]) = 0$. Thus $[f] = [f_1]N_1 + [f_2]N_2 + \ldots + [f_t]N_t$ with $[f_j] \in \mathrm{kernel}(\gamma^1)$ for all $j = 1, \ldots, t$, and therefore $[f]$ is not a generator of the $\mathbf{k}[W]^{\mathbb{Z}/p}$-module, kernel($\gamma^1$). □

5. $V_2 \oplus V_3$

Choose distinguished variables $y_1 \in V_2^*$ and $z_2 \in V_3^*$. Define $x_1 := \Delta(y_1)$, $y_2 := \Delta(z_2)$ and $x_2 := \Delta(y_2)$. Then $\{x_1, y_1, x_2, y_2, z_2\}$ is a basis for $(V_2 \oplus V_3)^*$, and elements of $\mathbf{k}[V_2 \oplus V_3]$ are polynomials in these five variables. In $\mathbf{k}[V_2 \oplus V_3]^{\mathbb{Z}/p}$ there are five so-called 'rational' invariants: x_1, x_2, $u := y_1x_2 - x_1y_2$, $d := y_2^2 - 2x_2z_2 - x_2y_2$ and $w := y_1^2x_2 + x_1y_1x_2 - 2x_1y_1y_2 + 2x_1^2z_2$. (These invariants are called *rational* invariants because they admit prime independent descriptions which represent invariants under a lifting of the $\mathbb{Z}/p$-action to a $\mathbb{Z}$-action on $\mathbb{Z}[x_1, y_1, x_2, y_2, z_2]$.) We also have the norms of the distinguished variables: $N_1 := \prod_{i=1}^p \sigma^i(y_1) = y_1^p - x_1^{p-1}y_1$ and $N_2 := \prod_{i=1}^p \sigma^i(z_2)$.

This section is devoted to proving the following theorem and corollary.

THEOREM 5.1. *The ring of invariants $\mathbf{k}[V_2 \oplus V_3]^{\mathbb{Z}/p}$ is generated by x_1, x_2, d, N_1, N_2, u, w and the following two families of transfers:*

(i) $\{\mathrm{Tr}^{\mathbb{Z}/p}(y_1^i y_2 z_2^{p-1}) \mid 0 \leqslant i \leqslant p-1\}$, *and*

(ii) $\{\mathrm{Tr}^{\mathbb{Z}/p}(y_1^i z_2^\ell) \mid 1 \leqslant i \leqslant p-1, p-1 \geqslant \ell \geqslant p - \lceil i/2 \rceil\}$.

Furthermore, this generating set is a SAGBI basis for $\mathbf{k}[V_2 \oplus V_3]^{\mathbb{Z}/p}$ using the graded reverse lexicographic monomial order with $x_1 < y_1 < x_2 < y_2 < z_2$.

COROLLARY 5.2. *The invariants $\mathrm{Tr}^{\mathbb{Z}/p}(y_1^{p-1}y_2z_2^{p-1})$ and $\mathrm{Tr}^{\mathbb{Z}/p}(y_1^{p-1}z_2^{p-1})$ are indecomposable elements of $\mathbf{k}[V_2 \oplus V_3]^{\mathbb{Z}/p}$. In particular, $\beta(V_2 \oplus V_3) \geqslant 2p-1$.*

To prove Theorem 5.1, we shall use the method which the first author used in [**21**] to compute $\mathbf{k}[V_4]^{\mathbb{Z}/p}$ and $\mathbf{k}[V_5]^{\mathbb{Z}/p}$. The method involves constructing a subalgebra Q of $\mathbf{k}[V_2 \oplus V_3]^{\mathbb{Z}/p}$, and then showing that $Q = \mathbf{k}[V_2 \oplus V_3]^{\mathbb{Z}/p}$, by showing that the two algebras have the same Hilbert series.

Our Hilbert series computations make use of the theory of SAGBI bases, a generalization to subalgebras of the theory of Gröbner bases. We direct the reader to [**8**, Chapter 2] for a detailed discussion of monomial orders. We use the convention that a monomial is a product of variables, and that a term is a monomial with a non-zero coefficient. For $f \in \mathbf{k}[V]$, 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 Q is a subalgebra of $\mathbf{k}[V]$. Let $\mathrm{LT}(Q)$ denote the vector space

spanned by the lead terms of elements of Q. Note that $\mathrm{LT}(Q)$ is a subalgebra of $\mathbf{k}[V]$. If $\mathscr{C}$ is a subset of $\mathbf{k}[V]$, then let $\mathrm{LM}(\mathscr{C})$ denote the set of lead monomials of elements of $\mathscr{C}$. If $\mathscr{C}$ is a subset of Q such that $\mathrm{LM}(\mathscr{C})$ generates the algebra $\mathrm{LT}(Q)$, then $\mathscr{C}$ generates Q, and $\mathscr{C}$ is called a *SAGBI basis* for Q. For more on SAGBI bases, see [**17**], [**20**] or [**23**, Chapter 11].

Before proving Theorem 5.1, we prove a lemma and its corollary, which we need in the proof of Theorem 5.1.

LEMMA 5.3. *Let $H := \mathbf{k}[x, y]$, and let $I \subset H$ be an ideal generated by monomials. Let $\gamma_1, \gamma_2, \ldots, \gamma_s$ be monomials that minimally generate I, where $\gamma_1 < \gamma_2 < \ldots < \gamma_s$ with respect to lexicographic order with $x < y$. Then the Hilbert series of the module I is*

$$\mathscr{P}(I, \lambda) = \frac{\sum_{i=1}^{s} \lambda^{\deg(\gamma_i)} - \sum_{i=1}^{s-1} \lambda^{\deg(\mathrm{LCM}(\gamma_i, \gamma_{i+1}))}}{(1-\lambda)^2},$$

where $\mathrm{LCM}(\gamma_i, \gamma_{i+1})$ denotes the least common multiple of $\{\gamma_i, \gamma_{i+1}\}$.

Proof. Let $\Gamma_1, \Gamma_2, \ldots, \Gamma_s$ and $R_{1,2}, R_{2,3}, \ldots, R_{s-1,s}$ be formal symbols. Define

$$r_{i,j} := \frac{\mathrm{LCM}(\gamma_i, \gamma_j)}{\gamma_i}\Gamma_i - \frac{\mathrm{LCM}(\gamma_i, \gamma_j)}{\gamma_j}\Gamma_j.$$

We claim that the following is a resolution of I by free H-modules:

$$0 \longrightarrow \bigoplus_{i=1}^{s-1} H R_{i,i+1} \xrightarrow{\Psi_1} \bigoplus_{i=1}^{s} H\Gamma_i \xrightarrow{\Psi_0} I \longrightarrow 0,$$

with $\Psi_0(\Gamma_i) = \gamma_i$ and $\Psi_1(R_{i,i+1}) = r_{i,i+1}$.

The kernel of Ψ_0 is generated as an H-module by $\{r_{i,j} \mid 1 \leqslant i < j \leqslant s\}$. For a proof of this fact, see [**2**, Proposition 6.1] or [**8**, Chapter 2, Section 9, Proposition 8]. If we write $\gamma_i = x^{e_i} y^{f_i}$, then the ordering on the γ_i implies that $f_i \leqslant f_{i+1}$ for all i. But then the hypothesis that the γ_i minimally generate I implies that $f_1 < f_2 < \ldots < f_s$ and $e_1 > e_2 > \ldots > e_s$. Therefore, if $i < j$, then $\mathrm{LCM}(\gamma_i, \gamma_j) = x^{e_i} y^{f_j}$.

Now consider $r_{i,j}$, where $j \geqslant i + 2$. Then

$$r_{i,j} = \frac{\mathrm{LCM}(\gamma_i, \gamma_j)}{\mathrm{LCM}(\gamma_i, \gamma_{j-1})} r_{i,j-1} + \frac{\mathrm{LCM}(\gamma_i, \gamma_j)}{\mathrm{LCM}(\gamma_{j-1}, \gamma_j)} r_{j-1,j}$$

where $\mathrm{LCM}(\gamma_i, \gamma_j)/\mathrm{LCM}(\gamma_i, \gamma_{j-1})$, $\mathrm{LCM}(\gamma_i, \gamma_j)/\mathrm{LCM}(\gamma_{j-1}, \gamma_j) \in H$. Thus $\{r_{1,2}, r_{2,3}, \ldots, r_{s-1,s}\}$ generates the kernel of Ψ_0.

Next consider Ψ_1. We have

$$\begin{aligned}
\Psi_1\left(\sum_{i=1}^{s-1} f_i R_{i,i+1}\right) = &\left(f_1 \frac{\mathrm{LCM}(\gamma_1, \gamma_2)}{\gamma_1}\right)\Gamma_1 \\
&+ \left(f_2 \frac{\mathrm{LCM}(\gamma_2, \gamma_3)}{\gamma_2} - f_1 \frac{\mathrm{LCM}(\gamma_1, \gamma_2)}{\gamma_2}\right)\Gamma_2 \\
&\vdots \\
&+ \left(f_{s-1} \frac{\mathrm{LCM}(\gamma_{s-1}, \gamma_s)}{\gamma_{s-1}} - f_{s-2} \frac{\mathrm{LCM}(\gamma_{s-2}, \gamma_{s-1})}{\gamma_{s-1}}\right)\Gamma_{s-1} \\
&- \left(f_{s-1} \frac{\mathrm{LCM}(\gamma_{s-1}, \gamma_s)}{\gamma_s}\right)\Gamma_s.
\end{aligned}$$

Thus if $\Psi_1(\sum_{i=1}^{s-1} f_i R_{i,i+1}) = 0$, then we must have $f_1 = f_2 = \ldots = f_{s-1} = 0$, and so Ψ_1 is injective.

Therefore

$$\begin{aligned}\mathscr{P}(I,\lambda) &= \mathscr{P}(\oplus_{i=1}^{s} H\Gamma_i, \lambda) - \mathscr{P}(\oplus_{i=1}^{s-1} HR_{i,i+1}, \lambda)\\ &= \mathscr{P}(H,\lambda)\sum_{i=1}^{s}\lambda^{\deg(\gamma_i)} - \mathscr{P}(H,\lambda)\sum_{i=1}^{s-1}\lambda^{\deg(\mathrm{LCM}(\gamma_i,\gamma_{i+1}))}\\ &= \left(\sum_{i=1}^{s}\lambda^{\deg(\gamma_i)} - \sum_{i=1}^{s-1}\lambda^{\deg(\mathrm{LCM}(\gamma_i,\gamma_{i+1}))}\right)/(1-\lambda)^2. \qquad \square\end{aligned}$$

The following corollary is a consequence of the lemma and the fact that submodules of rank 1 free modules correspond to ideals.

COROLLARY 5.4. *Let $R := \mathbf{k}[x, y, a_1, a_2, \ldots, a_n]$. Suppose that α generates a free R-module, and that I is an ideal in $\mathbf{k}[x, y]$ minimally generated by monomials $\gamma_1 < \ldots < \gamma_s$. Let M be the R-module generated by $\{\alpha\gamma_1, \alpha\gamma_2, \ldots, \alpha\gamma_s\}$. Then*

$$\mathscr{P}(M,\lambda) = \lambda^{deg(\alpha)}\left(\sum_{i=1}^{s}\lambda^{\deg(\gamma_i)} - \sum_{i=1}^{s-1}\lambda^{\deg(\mathrm{LCM}(\gamma_i,\gamma_{i+1}))}\right)\mathscr{P}(R,\lambda).$$

Now we proceed with the proof of Theorem 5.1 We shall use the graded reverse lexicographic monomial order with $x_1 < y_1 < x_2 < y_2 < z_2$. Let $\mathscr{C}$ denote the collection of invariants given in the statement of Theorem 5.1, and let Q denote the subalgebra of $\mathbf{k}[V]^{\mathbb{Z}/p}$ generated by $\mathscr{C}$. We shall show that $\mathscr{C}$ is a SAGBI basis for Q, and that $Q = \mathbf{k}[V]^{\mathbb{Z}/p}$.

Let $\mathscr{A}$ denote the algebra generated by $\mathrm{LM}(\mathscr{C})$. Note that $\{x_1, N_1, x_2, d, N_2\}$ is a homogeneous system of parameters for $\mathbf{k}[V]$, as is $\mathrm{LM}(\{x_1, N_1, x_2, d, N_2\}) = \{x_1, y_1^p, x_2, y_2^2, z_2^p\}$. Let $R := \mathbf{k}[x_1, y_1^p, x_2, y_2^2, z_2^p]$. Then $\mathscr{A}$ is a finite R-module, and we shall exploit the structure of $\mathscr{A}$ as an R-module in order to compute its Hilbert series.

Note that $\mathrm{LT}(u) = x_2y_1$ and $\mathrm{LT}(w) = x_2y_1^2$. By [**21**, Theorem 3.3], we have $\mathrm{LM}(\mathrm{Tr}^{\mathbb{Z}/p}(y_2z_2^{p-1})) = y_2^p$; also, $\mathrm{LM}(\mathrm{Tr}^{\mathbb{Z}/p}(z_2^\ell)) = y_2^{2\ell-p+1}x_2^{p-\ell-1}$, by [**21**, Theorem 3.2]. From these two facts, using a simple generalization of [**21**, Theorem 3.6], we obtain $\mathrm{LM}(\mathrm{Tr}^{\mathbb{Z}/p}(y_1^iy_2z_2^{p-1})) = y_1^iy_2^p$ and $\mathrm{LM}(\mathrm{Tr}^{\mathbb{Z}/p}(y_1^iz_2^\ell)) = y_1^iy_2^{2\ell-p+1}x_2^{p-\ell-1}$.

We define a $(\mathbb{Z}/p \times \mathbb{Z}/2)$-grading on $\mathbf{k}[V_2 \oplus V_3]$ by declaring that a monomial $x_1^{i_1}y_1^{i_2}x_1^{j_1}y_2^{j_2}z_2^{j_3}$ has bi-degree $(i_2, j_2) \in (\mathbb{Z}/p \times \mathbb{Z}/2)$. Let $\mathscr{A}_{(i,j)}$ denote the elements of $\mathscr{A}$ whose bi-degree is (i, j). Note that the action of R preserves bi-degree, and thus since $\mathscr{A}$ is generated by monomials, $\mathscr{A}$ is a $(\mathbb{Z}/p \times \mathbb{Z}/2)$-graded R-module. Furthermore, this means that the $\mathscr{A}_{(i,j)}$ are themselves R-submodules of $\mathscr{A}$, and thus $\mathscr{A}$ decomposes as an R-module: $\mathscr{A} = \oplus_{i=0}^{p-1}\oplus_{j=0}^{1}\mathscr{A}_{(i,j)}$. Therefore, we may compute the Hilbert series of the R-module $\mathscr{A}$ by summing the Hilbert series of the individual R-modules, $\mathscr{A}_{(i,j)}$. We shall consider each bi-degree (i, j) in turn.

Since $\mathscr{A}_{(0,0)}$ is the free R-module generated by the unit, 1, its Hilbert series is $\mathscr{P}(R,\lambda)$.

Similarly, for each $i \in \mathbb{Z}/p$ we see that $\mathscr{A}_{(i,1)}$ is the free R-module generated by $y_1^iy_2^p = \mathrm{LM}(\mathrm{Tr}^{\mathbb{Z}/p}(y_1^iy_2z_2^{p-1}))$. Therefore the Hilbert series of $\mathscr{A}_{(i,1)}$ is $\lambda^{p+i}\mathscr{P}(R,\lambda)$.

For $i = 2t$ with $1 \leqslant t \leqslant (p-1)/2$, the R-module $\mathscr{A}_{(2t,0)}$ is generated by the $t+1$ elements: $y_1^iy_2^{p-1}, y_1^ix_2y_2^{p-3}, y_1^ix_2^2y_2^{p-5}, \ldots, y_1^ix_2^{t-1}y_2^{p-2t+1}$ and $y_1^ix_2^t$. These are the

lead monomials of $\mathrm{Tr}^{\mathbb{Z}/p}(y_1^i z_2^{p-1}), \mathrm{Tr}^{\mathbb{Z}/p}(y_1^i z_2^{p-2}), \mathrm{Tr}^{\mathbb{Z}/p}(y_1^i z_2^{p-3}), \ldots, \mathrm{Tr}^{\mathbb{Z}/p}(y_1^i z_2^{p-t})$ and w^t respectively. Applying Corollary 5.4 with $\alpha = y_1^i$, $x = x_2$ and $y = y_2^2$, we see that the Hilbert series of $\mathscr{A}_{(2t,0)}$ is

$$\begin{aligned}\mathscr{P}(\mathscr{A}_{(2t,0)}, \lambda) &= \lambda^i\big((\lambda^{p-1} + \lambda^{p-2} + \ldots + \lambda^{p-t} + \lambda^t)\\ &\qquad -(\lambda^p + \lambda^{p-1} + \ldots + \lambda^{p-t+2} + \lambda^{p-t+1})\big)\mathscr{P}(R, \lambda)\\ &= \lambda^i(\lambda^{p-t} + \lambda^t - \lambda^p)\mathscr{P}(R, \lambda).\end{aligned}$$

Similarly, for $i = 2t-1$ with $1 \leqslant t \leqslant (p-1)/2$, the R-module $\mathscr{A}_{(2t-1,0)}$ is generated by the $t+1$ elements: $y_1^i y_2^{p-1}, y_1^i x_2 y_2^{p-3}, y_1^i x_2^2 y_2^{p-5}, \ldots, y_1^i x_2^{t-1} y_2^{p-2t+1}$ and $y_1^i x_2^t$. These are the lead monomials of $\mathrm{Tr}^{\mathbb{Z}/p}(y_1^i z_2^{p-1})$, $\mathrm{Tr}^{\mathbb{Z}/p}(y_1^i z_2^{p-2})$, $\mathrm{Tr}^{\mathbb{Z}/p}(y_1^i z_2^{p-3}), \ldots, \mathrm{Tr}^{\mathbb{Z}/p}(y_1^i z_2^{p-t})$ and $w^{t-1}u$ respectively. Again by Corollary 5.4, we see that the Hilbert series of $\mathscr{A}_{(2t-1,0)}$ is

$$\mathscr{P}(\mathscr{A}_{(2t-1,0)}, \lambda) = \lambda^i(\lambda^{p-t} + \lambda^t - \lambda^p)\mathscr{P}(R, \lambda).$$

Summing the Hilbert series of all $2p$ homogeneous components, $\mathscr{A}_{(i,j)}$, we obtain

$$\begin{aligned}\mathscr{P}(\mathscr{A}, \lambda) &= \sum_{i=0}^{p-1}\sum_{j=0}^{1}\mathscr{P}(\mathscr{A}_{(i,j)}, \lambda)\\ &= \frac{-\lambda^{(3p-1)/2}\left(\lambda^3 + 3\lambda^2 + 3\lambda + 1\right) + 2\lambda^p\left(\lambda^2 + \lambda + 1\right) + \lambda^2 + 1}{\left(\lambda^3 - 1\right)(\lambda - 1)^2\left(\lambda^2 - 1\right)(\lambda^p - 1)^2}.\end{aligned}$$

Using the method of Hughes and Kemper [**16**], one can compute $\mathscr{P}(\mathbf{k}[V_2 \oplus V_3]^{\mathbb{Z}/p}, \lambda)$. Gregor Kemper has written a MAGMA script implementing this algorithm, and using the output of this script we observe that $\mathscr{P}(\mathbf{k}[V_2 \oplus V_3]^{\mathbb{Z}/p}, \lambda) = \mathscr{P}(\mathscr{A}, \lambda)$. Since $\mathscr{A}$ is a subalgebra of $\mathrm{LT}(Q)$, $\mathscr{P}(\mathscr{A}, \lambda) \leqslant \mathscr{P}(\mathrm{LT}(Q), \lambda)$. By [**21**, Proposition 1.2], $\mathscr{P}(\mathrm{LT}(Q), \lambda) = \mathscr{P}(Q, \lambda)$. Furthermore, $Q \subseteq \mathbf{k}[V_2 \oplus V_3]^{\mathbb{Z}/p}$ implies that $\mathscr{P}(Q, \lambda) \leqslant \mathscr{P}(\mathbf{k}[V_2 \oplus V_3]^{\mathbb{Z}/p}, \lambda)$. The fact that $\mathscr{P}(\mathbf{k}[V_2 \oplus V_3]^{\mathbb{Z}/p}, \lambda) = \mathscr{P}(\mathscr{A}, \lambda)$ means that all of these Hilbert series are equal. Thus $\mathscr{A} = \mathrm{LT}(Q)$, $Q = \mathbf{k}[V_2 \oplus V_3]^{\mathbb{Z}/p}$ and $\mathscr{C}$ is a SAGBI basis for $\mathbf{k}[V_2 \oplus V_3]^{\mathbb{Z}/p}$. This completes the proof of Theorem 5.1.

Now we show how Corollary 5.2 follows from Theorem 5.1.

Proof of Corollary 5.2. Suppose, by way of contradiction, that $\mathrm{Tr}^{\mathbb{Z}/p}(y_1^{p-1} y_2 z_2^{p-1})$ is equal to $f_1 h_1 + f_2 h_2 + \ldots + f_m h_m$, with $f_\ell, h_\ell \in \mathbf{k}[V_2 \oplus V_3]_+^{\mathbb{Z}/p}$ for $\ell = 1, 2, \ldots, m$. We may assume that $\mathrm{LM}(f_\ell h_\ell) \geqslant \mathrm{LM}(f_{\ell+1} h_{\ell+1})$. Clearly, either $\mathrm{LM}(f_1 h_1) = \mathrm{LM}(\mathrm{Tr}^{\mathbb{Z}/p}(y_1^{p-1} y_2 z_2^{p-1})) = y_1^{p-1} y_2^p$, or $\mathrm{LM}(f_1 h_1) = \mathrm{LM}(f_2 h_2) > y_1^{p-1} y_2^p$. The elements in $\mathrm{LM}(\mathscr{C})$ of the form $y_1^i y_2^j$ are $\{y_2^2, y_1^p, y_2^p\} \cup \{y_1^i y_2^{p-1}, y_1^i y_2^p \mid 1 \leqslant i \leqslant p-1\}$. Thus $y_1^{p-1} y_2^p$ is an indecomposable element of $\mathscr{A} = \mathrm{LT}(\mathbf{k}[V_2 \oplus V_3]^{\mathbb{Z}/p})$. Therefore $\mathrm{LM}(f_1 h_1) = \mathrm{LM}(f_2 h_2) > y_1^{p-1} y_2^p$. Note that $\mathbf{k}[V_2 \oplus V_3] \cong \mathbf{k}[V_2] \otimes \mathbf{k}[V_3]$ is bi-graded, the action of $\mathbb{Z}/p$ respects this grading, and all of our generators are homogeneous with respect to this grading. However, there are no monomials with bi-degree $(p-1, p)$ which are greater than $y_1^{p-1} y_2^p$ and are contained in $\mathscr{A}$. Thus $\mathrm{Tr}^{\mathbb{Z}/p}(y_1^{p-1} y_2 z_2^{p-1})$ is indecomposable.

Similarly, since $\mathrm{LM}(\mathrm{Tr}^{\mathbb{Z}/p}(y_1^{p-1} z_2^{p-1})) = y_1^{p-1} y_2^{p-1}$, we see that $\mathrm{Tr}^{\mathbb{Z}/p}(y_1^{p-1} z_2^{p-1})$ is also indecomposable. □

By [**10**] or [**6**], we know that $\mathbf{k}[V_2 \oplus V_3]^{\mathbb{Z}/p}$ is not Cohen–Macaulay. Here we shall show explicitly that the partial homogeneous system of parameters x_1, x_2, d in $\mathbf{k}[V_2 \oplus V_3]^{\mathbb{Z}/p}$ is not a regular sequence.

Since $\mathrm{LT}(\mathrm{Tr}^{\mathbb{Z}/p}(z_2^{p-1})) = -y_2^{p-1} = \mathrm{LT}(-d^{(p-1)/2})$, there exists $f \in \mathbf{k}[V_3]^{\mathbb{Z}/p}$ such that

$$d^{(p-1)/2} = -\mathrm{Tr}^{\mathbb{Z}/p}(z_2^{p-1}) + x_2 f.$$

Thus

$$\begin{aligned} ud^{(p-1)/2} + (\mathrm{Tr}^{\mathbb{Z}/p}(y_1 z_2^{p-1}) - fu)x_2 &= u\big(x_2 f - \mathrm{Tr}^{\mathbb{Z}/p}(z_2^{p-1})\big) + \big(\mathrm{Tr}^{\mathbb{Z}/p}(y_1 z_2^{p-1}) - fu\big)x_2 \\ &= \mathrm{Tr}^{\mathbb{Z}/p}\left(-uz_2^{p-1} + y_1 z_2^{p-1} x_2\right) \\ &= \mathrm{Tr}^{\mathbb{Z}/p}\left((x_2 y_1 - u)z_2^{p-1}\right) \\ &= \mathrm{Tr}^{\mathbb{Z}/p}\left(x_1 y_2 z_2^{p-1}\right) \\ &= x_1 \,\mathrm{Tr}^{\mathbb{Z}/p}\left(y_2 z_2^{p-1}\right) \in (x_1)\mathbf{k}[V_2 \oplus V_3]^{\mathbb{Z}/p}. \end{aligned}$$

Note that $\{x_1, x_2\}$ is a Gröbner basis for $(x_1, x_2)\mathbf{k}[V_2 \oplus V_3]^{\mathbb{Z}/p}$, and $\mathrm{LM}(ud^{(p-3)/2}) = x_2 y_1 y_2^{p-3}$. Therefore, using the SAGBI basis $\mathscr{C}$, $ud^{(p-3)/2} \notin (x_1, x_2)\mathbf{k}[V_2 \oplus V_3]^{\mathbb{Z}/p}$. Thus x_1, x_2, d is not a regular sequence in $\mathbf{k}[V_2 \oplus V_3]^{\mathbb{Z}/p}$.

6. *The* $2p-3$ *conjecture*

As a consequence of Theorem 4.2, $\beta(V_p)$ is an upper bound for the Noether number of every indecomposable representation of $\mathbb{Z}/p$. Since V_p is a permutation representation, Göbel [**15**] gives us $\beta(V_p) \leqslant \max\{2, \binom{p}{2}\}$. For $p > 3$, this has been improved to $\binom{p-1}{2}+1$ by Fleischmann [**13**, Proposition 12.3], and to $(p+3)(p-1)/4+1$ by Hughes and Kemper [**16**, Corollary 2.15].

CONJECTURE 6.1. $\beta(V_p) = 2p-3$.

Direct calculation of $\mathbf{F}_p[V_p]^{\mathbb{Z}/p}$ using MAGMA [**4**] confirms the conjecture for $p \leqslant 7$. A less direct method, outlined below, confirms the conjecture for the primes 11 and 13.

Let z be a distinguished variable for V_p, and let N be the norm of z. Let $I^{\mathbb{Z}/p}$ denote the image of $\mathrm{Tr}^{\mathbb{Z}/p} : \mathbf{k}[V] \to \mathbf{k}[V]^{\mathbb{Z}/p}$. Thus $I^{\mathbb{Z}/p}$ is an ideal in $\mathbf{k}[V]^{\mathbb{Z}/p}$. It is well known that $\mathbf{k}[V_p]^{\mathbb{Z}/p}/I^{\mathbb{Z}/p} = \mathbf{k}[N]$, which has Noether number p (see, for example, [**13**, Example 12.1] or [**16**, Lemma 2.12]). Therefore, to prove the conjecture, it is sufficient to study indecomposable invariants in $I^{\mathbb{Z}/p}$.

THEOREM 6.2. $\beta(V_p) \geqslant 2p-3$.

Proof. Let $y := \Delta(z)$. We shall show that $f := \mathrm{Tr}^{\mathbb{Z}/p}(z^{p-1}y^{p-2})$ is indecomposable. We use the graded reverse lexicographic monomial order with $\Delta^i(z) > \Delta^{i+1}(z)$. Suppose, by way of contradiction, that $f = f_1h_1 + f_2h_2 + \ldots + f_mh_m$ with $f_i, h_i \in \mathbf{k}[V_p]_+^{\mathbb{Z}/p}$ and $\mathrm{LM}(f_ih_i) \geqslant \mathrm{LM}(f_{i+1}h_{i+1})$. From [**21**, Theorem 3.3], $\mathrm{LM}(f) = y^{2p-3}$. Thus either $\mathrm{LM}(f_1h_1) = y^{2p-3}$, or $\mathrm{LM}(f_1h_1) = \mathrm{LM}(f_2h_2) > y^{2p-3}$. In either case, $\mathrm{LM}(f_1h_1)$ is a monomial in z and y, with degree $2p-3$. Thus $\mathrm{LM}(f_1) = z^jy^k$ and $\mathrm{LM}(h_1) = z^ry^s$, with $j+k+r+s = 2p-3$.

Since we are using a triangular basis, $\deg_z(f) \leqslant \deg_z(z^{p-1}y^{p-2}) = p-1$. Thus $f \in \mathbf{k}[V_p]^\flat$ and, by the uniqueness of the norm decomposition, we may take f_1 and h_1 to be elements of $\mathbf{k}[V_p]^\flat$. Therefore f_1 and h_1 lie in $I^{\mathbb{Z}/p}$. Consider the $\mathbb{Z}/p$-equivariant surjection $\rho : \mathbf{k}[V_p] \to \mathbf{k}[V_2] = \mathbf{k}[\widetilde{z}, \widetilde{y}]$, given by $\rho(z) = \widetilde{z}$. The map ρ commutes with the transfer. Thus $\widetilde{f_1} := \rho(f_1)$ and $\widetilde{h_1} := \rho(h_1)$ are in the image of the

transfer. Furthermore, it is clear that $\mathrm{LM}(\widetilde{f_1}) = \widetilde{z}^j\widetilde{y}^k$ and $\mathrm{LM}(\widetilde{h_1}) = \widetilde{z}^r\widetilde{y}^s$. However, the image of the transfer in $\mathbf{k}[V_2]^{\mathbb{Z}/p}$ is the principal ideal generated by $\widetilde{y}^{p-1}$ (see [**7**, Corollary 9.7]). Thus $k \geqslant p-1$ and $s \geqslant p-1$. Therefore $j+k+r+s \geqslant 2p-2 > 2p-3$, giving the required contradiction. □

For a finite-dimensional representation V of a finite group G, $\mathbf{k}[V]$ is a finite module over $\mathbf{k}[V]^G$. Define a homomorphism of $\mathbf{k}[V]^G$-modules, $\mathrm{Tr}^G : \mathbf{k}[V] \to \mathbf{k}[V]^G$, by $\mathrm{Tr}^G(f) := \sum_{g\in G} g(f)$. Applying Tr^G to a set of module generators gives a generating set for the image of Tr^G, the ideal I^G. Let $\mathscr{H} := \mathbf{k}[V]^G_+\mathbf{k}[V]$ denote the Hilbert ideal of $\mathbf{k}[V]$. A homogeneous basis for the finite-dimensional algebra $\mathbf{k}[V]/\mathscr{H}$ lifts to a set of $\mathbf{k}[V]^G$-modules generators for $\mathbf{k}[V]$. Thus a basis element of largest degree in $\mathbf{k}[V]/\mathscr{H}$ lifts to a module generator of largest degree in $\mathbf{k}[V]$. For a homogeneous ideal $J \subset \mathbf{k}[V]$ of height $\dim(V)$, the quotient, $\mathbf{k}[V]/J$, is a finite-dimensional graded algebra. Let $\mathrm{td}(\mathbf{k}[V]/J)$ denote the *top degree* of $\mathbf{k}[V]/J$, that is, the largest degree in which $\mathbf{k}[V]/J$ is non-zero.

PROPOSITION 6.3. *Suppose that $J \subset \mathbf{k}[V_n]$ is an ideal of height n. If J is contained in the Hilbert ideal, $\mathscr{H} = \mathbf{k}[V_n]^G_+\mathbf{k}[V_n]$, then $\max\{p, \mathrm{td}(\mathbf{k}[V_n]/J)\}$ is an upper bound for $\beta(V_n)$.*

Proof. Using the notation of Section 2, recall that $\mathbf{k}[V_n] = (N)\mathbf{k}[V_n] \oplus \mathbf{k}[V_n]^{\flat}$, and that $\mathbf{k}[V_n]^{\flat}_d$ is a free $\mathbb{Z}/p$-module if $d \geqslant p-n+1$. Since invariants associated to free $\mathbb{Z}/p$-modules are in the image of the transfer, we conclude that all indecomposable invariants in degrees greater than p are in the image of the transfer. The proposition follows from the fact that $\mathrm{td}(\mathbf{k}[V_n]/J)$ is an upper bound for $\mathrm{td}(\mathbf{k}[V_n]/\mathscr{H})$, which is in turn an upper bound for the degree of an indecomposable in $I^{\mathbb{Z}/p}$. □

Proposition 6.3 has been used to verify Conjecture 6.1 for the primes 11 and 13. In each case, it was possible to construct an ideal J, satisfying the hypotheses of the proposition, with $\mathrm{td}(\mathbf{k}[V_p]/J) = 2p-3$. The calculations were performed using MAGMA [**4**].

Acknowledgements. We would like to thank Gregor Kemper for providing us with a closed form for the Hilbert series, $\mathscr{P}(\mathbf{k}[V_2 \oplus V_3]^{\mathbb{Z}/p}, \lambda)$, which we required for our proof of Theorem 5.1. We would also like to thank the referee for several helpful suggestions.

References

1. G. ALMKVIST and R. FOSSUM, *Decompositions of exterior and symmetric powers of indecomposable $\mathbb{Z}/p$-modules in characteristic p*, Lecture Notes in Math. 641 (Springer, 1978) 1–114.
2. T. BECKER and V. WEISPFENNING, *Gröbner bases: a computational approach to commutative algebra* (Springer, 1993).
3. D. J. BENSON, *Polynomial invariants of finite groups*, London Math. Soc. Lecture Note Ser. 190 (Cambridge University Press, 1993).
4. W. BOSMA, J. J. CANNON and C. PLAYOUST, 'The Magma algebra system I: the user language', *J. Symbolic Comput.* 24 (1997) 235–265.
5. H. E. A. CAMPBELL and I. P. HUGHES, 'Vector invariants of $U_2(\mathbf{F}_p)$: a proof of a conjecture of Richman', *Adv. in Math.* 126 (1997) 1–20.
6. H. E. A. CAMPBELL, I. P. HUGHES, G. KEMPER, R. J. SHANK and D. L. WEHLAU, 'Depth of modular invariant rings', *Transform. Groups* 5 (2000) 21–34.

7. H. E. A. Campbell, I. P. Hughes, R. J. Shank and D. L. Wehlau, 'Bases for rings of coinvariants', *Transform. Groups* 1 (1996) 307–336.
8. D. Cox, J. Little and D. O'Shea, *Ideals, varieties, and algorithms* (Springer, 1992).
9. D. Eisenbud, *Commutative algebra with a view toward algebraic geometry*, Graduate Texts in Math. 150 (Springer, 1996).
10. G. Ellingsrud and T. Skjelbred, 'Profonder d'anneaux d'invariants en caractéristique p', *Compositio Math.* 41 (1980) 233–244.
11. L. Evens, *The cohomology of groups*, Oxford Math. Monogr. (Clarendon Press, 1991).
12. J. Fogarty, 'On Noether's bound for polynomial invariants of a finite group', *Electron. Res. Announc. Amer. Math. Soc.* 7 (2001) 5–7.
13. P. Fleischmann, 'Relative trace ideals and Cohen–Macaulay quotients of modular invariant rings', *Computational methods for representations of groups and algebras* (ed. P. Dräxler, G. Michler and C. M. Ringel, Birkhäuser, 1999) 211–233.
14. P. Fleischmann, 'The Noether bound in invariant theory of finite groups', *Adv. in Math.* 152 (2000) 23–32.
15. M. Göbel, 'Computing bases for rings of permutation invariant polynomials', *J. Symbolic Comput.* 19 (1995) 285–291.
16. I. Hughes and G. Kemper, 'Symmetric powers of modular representations, Hilbert series and degree bounds', *Comm. Algebra* 28 (2000) 2059–2088.
17. D. Kapur and K. Madlener, 'A completion procedure for computing a canonical basis of a k-subalgebra', *Proceedings of Computers and Mathematics* 89 (ed. E. Kaltofen and S. Watt, MIT, 1989) 1–11.
18. E. Noether, 'Der Endlichkeitssatz der Invarianten endlicher Gruppen', *Math. Ann.* 77 (1916) 28–35.
19. D. Richman, 'On vector invariants over finite fields', *Adv. in Math.* 81 (1990) 30–65.
20. L. Robbiano and M. Sweedler, *Subalgebra bases*, Lecture Notes in Math. 1430 (Springer, 1990) 61–87.
21. R. J. Shank, 'S.A.G.B.I. bases for rings of formal modular seminvariants', *Comment. Math. Helv.* 73 (1998) 548–565.
22. L. Smith, *Polynomial invariants of finite groups* (A. K. Peters, 1995).
23. B. Sturmfels, *Gröbner bases and convex polytopes*, Univ. Lecture Ser. 8 (Amer. Math. Soc., Providence, RI, 1996).

Institute of Mathematics and Statistics
University of Kent at Canterbury
Canterbury CT2 7NF

R.J.Shank@ukc.ac.uk

Department of Mathematics and Computer Science
Royal Military College
Kingston
Ontario
Canada K7K 7B4

wehlau@rmc.ca