ON THE COINVARIANTS OF MODULAR REPRESENTATIONS OF CYCLIC GROUPS OF PRIME ORDER

MÜFIT SEZER AND R. JAMES SHANK

Abstract. We consider the ring of coinvariants for modular representations of cyclic groups of prime order. For all cases for which explicit generators for the ring of invariants are known, we give a reduced Gröbner basis for the Hilbert ideal and the corresponding monomial basis for the coinvariants. We also describe the decomposition of the coinvariants as a module over the group ring. For one family of representations, we are able to describe the coinvariants despite the fact that an explicit generating set for the invariants is not known. In all cases our results confirm the conjecture of Harm Derksen and Gregor Kemper on degree bounds for generators of the Hilbert ideal. As an incidental result, we identify the coefficients of the monomials appearing in the orbit product of a terminal variable for the three dimensional indecomposable representation.

1. Introduction

Let V denote a finite dimensional representation of a finite group G over a field $\mathbf{F}$. If the characteristic of $\mathbf{F}$ divides the order of G, then V is called a *modular* representation. Choose a basis $\{X_1, \ldots, X_n\}$ for the dual vector space V^*. The action of G on V induces an action on V^* which extends to an action by algebra automorphisms on the symmetric algebra $\mathbf{F}[V] := S(V^*) = \mathbf{F}[X_1, \ldots, X_n]$. The ring of *invariants*,

$$\mathbf{F}[V]^G := \{f \in \mathbf{F}[V] \mid g(f) = f,\ \forall g \in G\},$$

is a finitely generated subring of $\mathbf{F}[V]$. The *Noether number*, $\beta(V)$, is defined to be the least integer d such that $\mathbf{F}[V]^G$ is generated by homogeneous elements of degree less than or equal to d. The *Hilbert ideal*, which we denote by $\mathcal{H}$, is the ideal in $\mathbf{F}[V]$ generated by the homogeneous invariants of positive degree and the ring of *coinvariants* is the quotient

$$\mathbf{F}[V]_G := \mathbf{F}[V]/\mathcal{H}.$$

Since the Hilbert ideal is closed under the group action, the coinvariants are a module over the group ring $\mathbf{F}G$. Furthermore, since G is finite, $\mathbf{F}[V]$ is integral over $\mathbf{F}[V]^G$. Therefore $\mathbf{F}[V]_G$ is a finite dimensional graded $\mathbf{F}$-algebra. Let $\mathrm{td}(\mathbf{F}[V]_G)$ denote the *top degree* of $\mathbf{F}[V]_G$, i.e., the largest degree in which $\mathbf{F}[V]_G$ is non-zero. The ring of coinvariants has been studied extensively for $\mathbf{F}$ a field of characteristic zero, particularly for V a reflection representation. For reflection

Date: May 10, 2005.

1991 *Mathematics Subject Classification.* 13A50.

Research supported by a grant from EPSRC.

representations in characteristic zero, the coinvariants are isomorphic, as a module over the group ring, to the regular representation (see, for example, [8], [4, Ch. V, §5.2] or [15, Ch. VII, §24-1]). Coinvariants in characteristic zero continue to attract attention (see, for example, [11], [12] and [13]). Relatively little is known about coinvariants for modular representations. The coinvariants for the natural modular representations of $\mathrm{GL}_n(\mathbf{F}_q)$ and its p-Sylow subgroup were considered by Campbell et al. in [7]. Larry Smith has investigated modular coinvariants for two and three dimensional representations [25] and in the case that the invariants are a polynomial algebra ([26], [24]). In this paper we consider the coinvariants for the simplest modular representations, the modular representations of cyclic groups of prime order.

For the remainder of the paper, let p denote a prime number, let $\mathbf{Z}/p$ denote the cyclic group of order p and let $\mathbf{F}$ denote a field of characteristic p. A representation of a cyclic group is determined by the Jordan canonical form of the image of the generator. If $n \leq p$ then the $n \times n$ matrix over $\mathbf{F}$ consisting of a single Jordan block with eigenvalue 1, has order p and determines an indecomposable representation of $\mathbf{Z}/p$ which we denote by V_n (For $n > p$, the order of the matrix is greater than p.). Note that there are no non-trivial p^{th} roots of unity in $\mathbf{F}$. Thus 1 is the only eigenvalue for the image of a generator of $\mathbf{Z}/p$ under a representation over $\mathbf{F}$. Therefore, up to isomorphism, the only indecomposable $\mathbf{F}\mathbf{Z}/p$ – modules are $V_1, V_2, \ldots, V_p$. We will denote the direct sum of m copies of V_n by mV_n.

Despite the simplicity of the representation theory, computing explicit generators for $\mathbf{F}[V]^{\mathbf{Z}/p}$ is a relatively difficult problem. Minimal generating sets for $\mathbf{F}[V_2]^{\mathbf{Z}/p}$ and $\mathbf{F}[V_3]^{\mathbf{Z}/p}$ can be found in Dickson's Madison Colloquium [10]. Finite SAGBI bases[1] for $\mathbf{F}[V_4]^{\mathbf{Z}/p}$ and $\mathbf{F}[V_5]^{\mathbf{Z}/p}$ can be found in [20]. The problem of finding an explicit generating set for $\mathbf{F}[V_n]^{\mathbf{Z}/p}$ 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 & Hughes, in [6], describe a generating set for $\mathbf{F}[mV_2]^{\mathbf{Z}/p}$ which is refined to a minimal generating set in [22]. SAGBI bases are given for $\mathbf{F}[V_2 \oplus V_3]^{\mathbf{Z}/p}$ in [21] and $\mathbf{F}[2V_3]^{\mathbf{Z}/p}$ in [5]. We refer to an $\mathbf{F}\mathbf{Z}/p$ – module as *reduced* if it is a direct sum of non-trivial modules. In summary, the only reduced representations for which explicit generating sets for the ring of invariants are known are: mV_2, $V_2 \oplus V_3$, V_3, $2V_3$, V_4, V_5. For each of these representations we will give a reduced Gröbner basis for the Hilbert ideal and describe the corresponding monomial basis for the coinvariants. We will also use the monomial basis to describe the $\mathbf{F}\mathbf{Z}/p$ – module structure of the coinvariants. By relating $mV_2 \oplus \ell V_3$ to $(m+\ell)V_2$, we are able describe $\mathbf{F}[mV_2 \oplus \ell V_3]_{\mathbf{Z}/p}$ despite the fact that an explicit generating set is not known for $\mathbf{F}[mV_2 \oplus \ell V_3]^{\mathbf{Z}/p}$. Our results give $(m+\ell)(p-1)+1$ as an upper bound on the degrees of a minimal generating set for $\mathbf{F}[mV_2 \oplus \ell V_3]^{\mathbf{Z}/p}$. Harm Derksen and Gregor Kemper have conjectured that the order of the group is an upper bound on the degrees of a minimal homogeneous generating set for the Hilbert ideal [9, 3.8.6 (b)]. For all of the examples considered here, our calculations confirm this conjecture. We note that $\mathbf{F}[2V_2]_{\mathbf{Z}/2}$ was considered in [25].

[1] A SAGBI basis is a particularly nice generating set.

Let σ denote a generator of $\mathbf{Z}/p$. In the group ring $\mathbf{F}\mathbf{Z}/p$, define $\Delta := \sigma - 1$ and $\mathrm{Tr} := \sum_{i=1}^{p} \sigma^i$. The kernel of Δ acting on a module gives the invariant elements in the module and Tr gives a homomorphism of $\mathbf{F}[V]^{\mathbf{Z}/p}$ – modules from $\mathbf{F}[V]$ to $\mathbf{F}[V]^{\mathbf{Z}/p}$ known as the *transfer*. The image of the transfer is an ideal in the ring of invariants. Observe that a basis for the coinvariants lifts to a set of generators for $\mathbf{F}[V]$ as a module over $\mathbf{F}[V]^{\mathbf{Z}/p}$. Applying the transfer to a set of module generators gives a generating set for the image of the transfer as an ideal. Thus a basis for the coinvariants gives a generating set for the image of the transfer and the largest degree of a basis element gives an upper bound on the degrees of a generating set for the image of the transfer. It is a consequence of [21, 4.2 & 6.3] and [20, 4.1] that for $n > 3$, $\mathrm{td}(\mathbf{F}[V_n]_{\mathbf{Z}/p}) \geq \beta(V_n) \geq 2p - 3$. The results in this paper support the following strengthening of [21, Conjecture 6.1].

Conjecture 1.1. *For $n > 3$, $\mathrm{td}(\mathbf{F}[V_n]_{\mathbf{Z}/p}) = 2p - 3$.*

For an element $\varphi \in V^*$, define the *norm* of φ to be the product over the orbit of φ. Thus, if $\varphi \in V^* \setminus (V^*)^{\mathbf{Z}/p}$, $N(\varphi) := \prod_{i=1}^{p} \sigma^i(\varphi)$. If we choose a basis $\{X, Y, Z\}$ for V_3^* so that $\Delta(Z) = Y$, $\Delta(Y) = X$ and $\Delta(X) = 0$, then $\mathbf{F}[V_3]^{\mathbf{Z}/p}$ is the hypersurface generated by X, $Y^2 - X(Y + 2Z)$, $N(Y)$ and $N(Z)$. It is well known that $N(Y) = Y^p - YX^{p-1}$. However, the expansion of $N(Z)$ is far more complicated and, to our knowledge, does not appear in the literature. Knowledge of certain coefficients in the expansion was necessary for some of our calculations. In Section 6, we have worked out a complete description of the expansion.

We adopt the convention of using upper case letters to denote variables in $\mathbf{F}[V]$ and the corresponding lower case letters to denote the images of the variables in $\mathbf{F}[V]_G$. We use the term *monomial* to mean a product of variables. For an ideal I, we write $f \equiv_I h$ if $f - h \in I$. As a general reference for the invariant theory of finite groups see Benson [2], Derksen & Kemper [9], Neusel & Smith [16] or Smith [23]. As a reference for Gröbner bases we recommend Adams & Loustaunau [1] or Sturmfels [27].

At the suggestion of the referee, some of the more computational aspects of the proofs given in an earlier draft of this paper [19] have been removed. The detailed proofs can still be found on the arXiv preprint server.

2. The coinvariants of $mV_2 \oplus \ell V_3$

We start by describing the coinvariants of mV_2. Choose a basis $\{X_i, Y_i \mid i = 1, \ldots, m\}$ for $(mV_2)^*$ with $\Delta(Y_i) = X_i$ and $\Delta(X_i) = 0$. For $i = 1, \ldots, m$ and $i < j$, define $u_{ij} := X_jY_i - X_iY_j$. Campbell and Hughes [6] have shown that

$$\{X_i, N(Y_i), u_{ij} \mid i = 1, \ldots, m;\ i < j\} \cup \{\mathrm{Tr}(\beta) \mid \beta \text{ divides } (Y_1 \cdots Y_m)^{p-1}\}$$

is a generating set for $\mathbf{F}[mV_2]^{\mathbf{Z}/p}$. It is well known that $N(Y_i) = Y_i^p - Y_iX_i^{p-1}$. Furthermore, if β divides $(Y_1 \cdots Y_m)^{p-1}$, then $\Delta(\beta) \in (X_1, \ldots, X_m)\mathbf{F}[mV_2]$. Thus $\mathrm{Tr}(\beta) = \Delta^{p-1}(\beta) \in (X_1, \ldots, X_m)\mathbf{F}[mV_2]$. As a consequence, we have the following.

Theorem 2.1. *A reduced universal Gröbner basis for the Hilbert ideal of mV_2 is given by $\{X_i, Y_i^p \mid i = 1, \ldots, m\}$, the corresponding monomial basis for $\mathbf{F}[mV_2]_{\mathbf{Z}/p}$*

is given by the monomial factors of $(y_1 \cdots y_m)^{p-1}$*, and* $\mathbf{F}[mV_2]_{\mathbf{Z}/p}$ *is a trivial* $\mathbf{F}\mathbf{Z}/p$ *– module.*

For the rest of this section, we assume $p > 2$. The natural inclusion of $(m+\ell)V_2$ into $mV_2 \oplus \ell V_3$ induces an algebra epimorphism $\rho : \mathbf{F}[mV_2 \oplus \ell V_3] \to \mathbf{F}[(m+\ell)V_2]$. We will use this map in conjunction with Theorem 2.1 to describe the coinvariants of $mV_2 \oplus \ell V_3$. Choose a basis

$$\{X_i, Y_i \mid i = 1, \ldots, m\} \cup \{X_i, Y_i, Z_i \mid i = m+1, \ldots, m+\ell\}$$

for $(mV_2 \oplus \ell V_3)^*$ with $\Delta(Z_i) = Y_i$, $\Delta(Y_i) = X_i$ and $\Delta(X_i) = 0$. For $i = 1, \ldots, m+\ell$ and $i < j$, define $u_{ij} := X_jY_i - X_iY_j$ and, for $i = m+1, \ldots, m+\ell$ and $i < j$, define $d_i := Y_i^2 - X_i(Y_i + 2Z_i)$ and $w_{ij} := Z_iX_j - Y_iY_j + X_iZ_j + X_iY_j$. A straightforward calculation verifies that u_{ij}, d_i and w_{ij} are all elements of $\mathbf{F}[mV_2 \oplus \ell V_3]^{\mathbf{Z}/p}$. Let I be the ideal in $\mathbf{F}[mV_2 \oplus \ell V_3]$ generated by

$$\{X_i, N(Y_i) \mid i = 1, \ldots m\} \cup \{X_i, d_i, w_{ij}, N(Z_i) \mid i = m+1, \ldots, m+l;\ i < j\}.$$

and define

$$\Lambda := \{X_i, Y_i^p \mid i = 1, \ldots, m\} \cup \{X_i, Y_iY_j, Z_i^p \mid i = m+1, \ldots, m+\ell;\ i \le j\}.$$

Lemma 2.2. *The set* Λ *is a reduced universal Gröbner basis for* I*.*

Proof. It follows from Section 6 that $N(Z_i) \equiv_{(X_i)} Z_i^p - Z_iY_i^{p-1}$. Using this, along with the expansion of $N(Y_i)$ given above and the definition of d_i and w_{ij}, it is clear that Λ generates I. Since Λ is a set of monomials and a minimal generating set for I, it is a reduced universal Gröbner basis for I. □

Lemma 2.3. *If* β *divides* $(Y_1 \cdots Y_m Z_{m+1} \cdots Z_{m+\ell})^{p-1}$*, then* $\mathrm{Tr}(\beta) \in I$*.*

Proof. Write $\beta = Y^F Z^E$ where $Y^F := \prod_{i=1}^m Y_i^{f_i}$ with $F := (f_1, \ldots, f_m) \in \mathbf{Z}^m$ and $Z^E := \prod_{i=m+1}^{m+\ell} Z_i^{e_i}$ with $E := (e_{m+1}, \ldots, e_{m+\ell}) \in \mathbf{Z}^\ell$. Clearly $\Delta(Y_i) \equiv_I 0$. Therefore $\Delta(\beta) = Y^F\Delta(Z^E)$ and $\mathrm{Tr}(\beta) = \Delta^{p-1}(\beta) = Y^F\,\mathrm{Tr}(Z^E)$. Thus it is sufficient to show that $\mathrm{Tr}(Z^E) \in I$. Recall that $\sigma^c(Z_i) = Z_i + cY_i + \binom{c}{2}X_i \equiv_I Z_i + cY_i$. Thus

$$\begin{aligned} \mathrm{Tr}(Z^E) &= \sum_{c \in \mathbf{F}_p} \sigma^c(Z^E) \\ &\equiv_I \sum_{c \in \mathbf{F}_p} \prod_{i=m+1}^{m+\ell} (Z_i + cY_i)^{e_i}. \end{aligned}$$

Using the fact that, for $i = m+1, \ldots, m+\ell$, we have $Y_i^2 \in I$, gives

$$\mathrm{Tr}(Z^E) \equiv_I \sum_{c \in \mathbf{F}_p} \prod_{i=m+1}^{m+\ell} \left(Z_i^{e_i} + e_icY_iZ_i^{e_i-1}\right).$$

Furthermore, for $i = m+1, \ldots, m+\ell$ and $i < j$, we have $Y_iY_j \in I$. Thus

$$\begin{aligned}\mathrm{Tr}(Z^E) &\equiv_I \sum_{c\in\mathbf{F}_p}\left(Z^E + c\sum_{i=m+1}^{m+\ell} e_iY_i\frac{Z^E}{Z_i}\right)\\ &\equiv_I Z^E\left(\sum_{c\in\mathbf{F}_p}1\right) + \left(\sum_{c\in\mathbf{F}_p}c\right)\left(\sum_{i=m+1}^{m+\ell} e_iY_i\frac{Z^E}{Z_i}\right).\end{aligned}$$

Therefore, using using the fact that $\sum_{c\in\mathbf{F}_p} c^t = 0$ unless $p-1$ divides t (see, for example,[7, 9.4]), $\mathrm{Tr}(Z^E) \equiv_I 0$, as required. □

The algebra epimorphism $\rho : \mathbf{F}[mV_2 \oplus \ell V_3] \to \mathbf{F}[(m+\ell)V_2]$, introduced above, is a morphism of $\mathbf{FZ}/p$ – modules and is determined by $\rho(Z_i) = Y_i$, $\rho(Y_i) = X_i$ and $\rho(X_i) = 0$ for $i > m$ and by $\rho(Y_i) = Y_i$ and $\rho(X_i) = X_i$ for $i \le m$. The kernel of ρ is generated by $\{X_i \mid i = m+1, \ldots, m+\ell\}$ and is contained in I. Since ρ is surjective, the image of I under ρ is an ideal in $\mathbf{F}[(m+\ell)V_2]$. Intersecting this ideal with the ring of invariants gives the ideal $J := \rho(I) \cap \mathbf{F}[(m+\ell)V_2]^{\mathbf{Z}/p}$.

Lemma 2.4. *The natural projection from* $\mathbf{F}[(m+\ell)V_2]^{\mathbf{Z}/p}$ *to* $\mathbf{F}[(m+\ell)V_2]^{\mathbf{Z}/p}/J$ *induces an epimorphism of vector spaces from*

$$\mathrm{Span}\left(\{X_i \mid i = m+1, \ldots, m+\ell\} \cup \{u_{ij} \mid i = 1, \ldots, m+\ell;\ i < j \text{ and } m < j\}\right)$$

to $\mathbf{F}[(m+\ell)V_2]^{\mathbf{Z}/p}/J$.

Proof. Recall that $\mathbf{F}[(m+\ell)V_2]^{\mathbf{Z}/p}$ is generated by

$$\{X_i, N(Y_i), u_{ij} \mid i = 1, \ldots, m+\ell;\ i < j\} \cup \{\mathrm{Tr}(\alpha) \mid \alpha \text{ divides } (Y_1\cdots Y_{m+\ell})^{p-1}\}.$$

For each monomial α dividing $(Y_1\cdots Y_{m+\ell})^{p-1}$, there exists a monomial β dividing $(Y_1\cdots Y_mZ_{m+1}\cdots Z_{m+\ell})^{p-1}$ with $\rho(\beta) = \alpha$. By Lemma 2.3, $\mathrm{Tr}(\beta) \in I$. Therefore $\mathrm{Tr}(\alpha) = \rho(\mathrm{Tr}(\beta)) \in J$. For $i \le m$, $\rho(Y_i) = Y_i$. Thus $N(Y_i) = \rho\left(N\left(Y_i\right)\right) \in J$. For $i > m$, $\rho(Z_i) = Y_i$ giving $N(Y_i) = \rho(N(Z_i)) \in J$. For $i \le m$, $X_i = \rho(X_i) \in J$. For $i > m$, $X_i^2 = \rho(d_i) \in J$ and $X_iX_j = -\rho(w_{ij}) \in J$. For $i < j \le m$, $u_{ij} = \rho(u_{ij}) \in J$. We have shown that, for all i and j, X_i^2 and X_iX_j lie in $\rho(I)$. Therefore $u_{ij}u_{rs} = X_jX_sY_iY_r - X_iX_sY_jY_r - X_jX_rY_iY_s + X_iX_rY_jY_s$ and $X_iu_{rs} = X_iX_sY_r - X_iX_rY_s$ lie in $\rho(I)$. Since these elements are invariant, they lie in J. □

Theorem 2.5. *The ideal I coincides with the Hilbert ideal of $mV_2 \oplus \ell V_3$.*

Proof. By definition, $I \subseteq \mathcal{H}$. Thus it is sufficient to show that every invariant lies in I. Suppose that f is a homogeneous element of $\mathbf{F}[mV_2 \oplus \ell V_3]^{\mathbf{Z}/p}$ with $\deg(f) > 2$. Then using Lemma 2.4, $\rho(f) \in J \subseteq \rho(I)$. Thus there exist $\widetilde{f} \in I$ with $\rho(\widetilde{f}) = \rho(f)$. Therefore $\widetilde{f} - f \in \ker(\rho) \subseteq I$. Thus $f \in I$ as required.

Every homogeneous invariant of degree 1 is a linear combination of the X_i and hence lies in I. Therefore we need only verify that all homogeneous invariants of degree 2 lie in I. To do this we grade $\mathbf{F}[mV_2 \oplus \ell V_3]$ over $\mathbf{Z}^{m+\ell} = \oplus_{i=1}^{m+\ell} b_i\mathbf{Z}$ by defining the multidegree of X_i, Y_i and Z_i to be b_i. The group action preserves multidegree. Therefore we may restrict to invariants which are homogeneous with respect to multidegree. Since the total degree is 2, the possible multidegrees are

$2b_i$ and $b_i + b_j$. For multidegree $2b_i$, we use the descriptions of $\mathbf{F}[V_2]^{\mathbf{Z}/p}$ and $\mathbf{F}[V_3]^{\mathbf{Z}/p}$ from [10]. For multidegree $b_i + b_j$, we use the description of $\mathbf{F}[2V_2]^{\mathbf{Z}/p}$ from [6], the description of $\mathbf{F}[2V_3]^{\mathbf{Z}/p}$ from [5] and the description of $\mathbf{F}[V_2 \oplus V_3]^{\mathbf{Z}/p}$ from [21]. In all cases, the only generators in degrees less than or equal to 2 are X_i, d_i, u_{ij} and w_{ij}. All of these invariants appear in I. □

Corollary 2.6. *A reduced universal Gröbner basis for the Hilbert ideal of $mV_2 \oplus \ell V_3$ is given by*

$$\{X_i, Y_i^p \mid i = 1, \dots, m\} \cup \{X_i, Y_iY_j, Z_i^p \mid i = m+1, \dots, m+\ell;\ i \leq j\},$$

the corresponding monomial basis for $\mathbf{F}[mV_2 \oplus \ell V_3]_{\mathbf{Z}/p}$ is given by the monomial factors of $y_j(y_1 \cdots y_m z_{m+1} \cdots z_{m+\ell})^{p-1}$ for $j = m+1, \dots, m+\ell$, and the Hilbert series of $\mathbf{F}[mV_2 \oplus \ell V_3]_{\mathbf{Z}/p}$ is $(\ell t + 1)\left(1 + t + \cdots + t^{p-1}\right)^{m+\ell}$. Furthermore, both as $\mathbf{F}$-algebras and $\mathbf{F}\mathbf{Z}/p$ – modules, $\mathbf{F}[mV_2 \oplus \ell V_3]_{\mathbf{Z}/p} \cong \mathbf{F}[mV_2]_{\mathbf{Z}/p} \otimes \mathbf{F}[\ell V_3]_{\mathbf{Z}/p}$.

Remark 2.7. *We have shown that the Hilbert ideal of $mV_2 \oplus \ell V_3$ is generated by homogeneous elements of degree less than or equal to p, the order of the group, confirming the conjecture of Derksen & Kemper* [9, 3.8.6(b)] *in this case. Theorem 3.2 and Theorem 4.1 confirm the conjecture for V_4 and V_5 respectively.*

Corollary 2.8. *If $m + \ell > 2$, then*

$$(m+\ell)(p-1) \leq \beta(mV_2 \oplus \ell V_3) \leq (m+\ell)(p-1) + 1.$$

Proof. From [21, 4.2], we know that the Noether number of a representation is greater than or equal to the Noether number of a subrepresentation. Thus $\beta\left((m+\ell)\,V_2\right) \leq \beta\left(mV_2 \oplus \ell V_3\right)$. From [6] or [17], for $m + \ell > 2$, the Noether number of $(m+\ell)V_2$ is $(m+\ell)(p-1)$. This gives the first inequality. To see the second inequality, first recall that using [14, 2.12], $\mathbf{F}[mV_2 \oplus \ell V_3]^{\mathbf{Z}/p}$ is generated by elements in degree p, elements from the image of the transfer, and elements in degree less than or equal to $(m+\ell)(p-2)-\ell$. The top degree of the coinvariants gives an upper bound on the degrees of generators coming form the image of the transfer. Thus $\mathrm{td}\left(\mathbf{F}[mV_2 \oplus \ell V_3]_{\mathbf{Z}/p}\right) = (m+\ell)(p-1)+1$ is an upper bound on the degrees of the generators of $\mathbf{F}[mV_2 \oplus \ell V_3]^{\mathbf{Z}/p}$. □

Remark 2.9. *The generating sets for $\mathbf{F}[V_2 \oplus V_3]^{\mathbf{Z}/p}$ and $\mathbf{F}[2V_3]^{\mathbf{Z}/p}$ in* [21] *and* [5] *respectively, include elements of degree $2(p-1)+1$. However, these generating sets are not proven to be minimal. MAGMA* [3] *calculations for the primes* 3, 5 *and* 7 *do give $2(p-1)+1$ as the Noether number for these representations. Further MAGMA calculations show that $2V_2 \oplus V_3$, $V_2 \oplus 2V_3$ and $3V_3$ at $p = 3$, all have Noether number* 7.

In order to describe the $\mathbf{F}\mathbf{Z}/p$ – module structure of $\mathbf{F}[mV_2 \oplus \ell V_3]_{\mathbf{Z}/p}$, we use the grading introduced in the proof of Theorem 2.5. Since $\mathcal{H}$ is generated by elements which are homogeneous with respect to multidegree, the grading on $\mathbf{F}[mV_2 \oplus \ell V_3]$ induces a grading on $\mathbf{F}[mV_2 \oplus \ell V_3]_{\mathbf{Z}/p}$. The group action preserves the multidegree. Therefore the homogeneous components give an $\mathbf{F}\mathbf{Z}/p$ – module decomposition. Furthermore, since $\mathbf{F}[mV_2 \oplus \ell V_3]_{\mathbf{Z}/p} \cong \mathbf{F}[mV_2]_{\mathbf{Z}/p} \otimes \mathbf{F}[\ell V_3]_{\mathbf{Z}/p}$ and $\mathbf{F}[mV_2]_{\mathbf{Z}/p}$ is a trivial $\mathbf{F}\mathbf{Z}/p$ – module, it is sufficient to describe the module structure of $\mathbf{F}[\ell V_3]_{\mathbf{Z}/p}$. Using the notation from the proof of Lemma 2.3 we can

describe the basis elements for $\mathbf{F}[\ell V_3]_{\mathbf{Z}/p}$ as $y_j^{\varepsilon} z^E$ where $j > m$, $\varepsilon \in \{0,1\}$ and $E = (e_1, \ldots, e_\ell) \in \mathbf{Z}^\ell$ with $0 \leq e_i \leq p-1$. It is clear that $\Delta(y_j z^E) = 0$ and

$$\Delta(z^E) = \sum_{j \in \{m+i | e_i \neq 0\}} y_j \frac{z^E}{z_j}.$$

Sorting the basis elements into their multidegree components gives the following.

Theorem 2.10. *In top degree, $\ell(p-1)+1$, the ℓ multidegree components of $\mathbf{F}[\ell V_3]_{\mathbf{Z}/p}$ are one dimensional with each component given by $y_j z^{(p-1,p-1,\ldots,p-1)}\mathbf{F}$. For total degree greater than zero and less than $\ell(p-1)+1$, each multidegree component is given by the span of $\{z^E, y_j z^E/z_j \mid e_{j-m} \neq 0\}$ and is isomorphic to $V_2 \oplus (k-1)V_1$ where k is the number of non-zero entries in E.*

3. The coinvariants of V_4

In this section we use the generating set for $\mathbf{F}[V_4]^{\mathbf{Z}/p}$ given in [20] to construct a reduced universal Gröbner basis for the Hilbert ideal. Choose a basis $\{X_1, X_2, X_3, X_4\}$ for V_4^* with $\Delta(X_i) = X_{i-1}$ for $i > 1$ and $\Delta(X_1) = 0$. We use the graded reverse lexicographic order with $X_1 < X_2 < X_3 < X_4$. We start with a useful lemma.

Lemma 3.1. *Suppose $\beta = X_2^i X_3^j$. Further suppose that α is a monomial with $\alpha < \beta$ and $\deg(\alpha) = \deg(\beta)$. Then α lies in the ideal generated by $\{X_1, X_2^{i+1}\}$.*

Proof. When comparing α and β using the graded reverse lexicographic order, we first compare the exponents of X_1 and then, if necessary, the exponents of X_2. □

Theorem 3.2. *A reduced universal Gröbner basis for the Hilbert ideal of V_4 is given by $\{X_1, X_2^2, X_2X_3^{p-3}, X_3^{p-1}, X_4^p\}$, the corresponding monomial basis for $\mathbf{F}[V_4]_{\mathbf{Z}/p}$ is given by the monomial factors of $x_3^{p-2}x_4^{p-1}$ and $x_2x_3^{p-4}x_4^{p-1}$, and the Hilbert series of $\mathbf{F}[V_4]_{\mathbf{Z}/p}$ is given by $(1+2(t+t^2+\cdots+t^{p-3})+t^{p-2})(1+t+\cdots+t^{p-1})$.*

Proof. By [20, 4.1], the ring of invariants is generated by X_1, $X_2^2 - X_1(X_2+2X_3)$, $X_2^3 + X_1^2(3X_4 - X_2) - 3X_1X_2X_3$, $g = X_2^2X_3^2 + \cdots$, $N(X_4)$ and the following families:
(i) $\mathrm{Tr}(X_3^i X_4^{p-1})$ for $0 \leq i \leq p-2$,
(ii) $\mathrm{Tr}(X_3^i X_4^{p-2})$ for $3 \leq i \leq p-2$,
(iii) $\mathrm{Tr}(X_4^j)$ for $q \leq j \leq p-2$,
(iv) $\mathrm{Tr}(X_3^2 X_4^j)$ for $2l-1 \leq j \leq p-2$.

where $l = \frac{p-1}{3}$, $q = 2l+1$ if $p \equiv 1$ modulo 3 and $l = \frac{p+1}{3}$, $q = 2l-1$ if $p \equiv -1$ modulo 3. In the following, we will determine the contribution of each generator to the reduced Gröbner basis. We first note that the ideal generated by X_1, $X_2^2 - X_1(X_2+2X_3)$, $X_2^3 + X_1^2(3X_4 - X_2) - 3X_1X_2X_3$ has reduced Gröbner basis $\{X_1, X_2^2\}$. Furthermore, by Lemma 3.1, all of the monomials appearing in g lie in the ideal (X_1, X_2^2).

The leading monomials of the elements in the transfer families above were computed in [20]. Using these results, we compute the contributions to the Gröbner basis of the second, third and fourth families.

For the third family, using [20, 3.2], the leading monomials are $\mathrm{LM}(\mathrm{Tr}(X_4^j)) = X_2^{p-1-j}X_3^{2j-p+1}$ for $q \leq j \leq p-2$. For $j < p-2$, the leading monomial is divisible by X_2^2. For $j = p-2$, the leading monomial is $X_2X_3^{p-3}$. Using Lemma 3.1 all "non-leading" monomials are in the ideal (X_1, X_2^2). Therefore the third family contributes $X_2X_3^{p-3}$ to the Gröbner basis.

For the second family of transfers, by [20, 3.4] we have $\mathrm{LM}(\mathrm{Tr}(X_3^iX_4^{p-2})) = X_2X_3^{i+p-3}$ for $3 \leq i \leq p-2$. Thus each leading monomial is divisible by $X_2X_3^{p-3}$ and, using Lemma 3.1, the non-leading monomials lie in (X_1, X_2^2). Thus the second family does not contribute to the Gröbner basis.

For the fourth family, by [20, 3.5], we have $\mathrm{LM}(\mathrm{Tr}(X_3^2X_4^j)) = X_2^{p-1-j}X_3^{2j-p+3}$ for $2l-1 \leq j \leq p-2$. For $j < p-2$, the leading monomial is divisible by X_2^2. For $j = p-2$ the leading monomial is divisible by $X_2X_3^{p-3}$. Again using Lemma 3.1, all of the non-leading monomials lie in (X_1, X_2^2). Therefore the fourth family does not contribute to the Gröbner basis.

For the first family, by [20, 3.3] and [20, 3.2], we have $\mathrm{LM}(\mathrm{Tr}(X_3^iX_4^{p-1}) = X_3^{i+p-1}$ for $0 \leq i \leq p-2$. Thus the leading monomials are all divisible by X_3^{p-1}. We claim that the non-leading monomials appearing in $\mathrm{Tr}(X_3^iX_4^{p-1})$ all lie in $(X_1, X_2^2, X_2X_3^{p-3})$. Therefore, proving the claim will show that the first family contributes X_3^{p-1} to the Gröbner basis. To prove the claim, we first observe that

$$\sigma^j(X_3^iX_4^{p-1}) = \left(X_3 + jX_2 + \binom{j}{2}X_1\right)^i \left(X_4 + jX_3 + \binom{j}{2}X_2 + \binom{j}{3}X_1\right)^{p-1}.$$

Using the fact that $\sum_{j\in\mathbf{F}_p} j^t = 0$ unless $p-1$ divides t, the only term not divisible by X_1 or X_2 which "survives" the summation is $j^{p-1}X_3^{p+i-1}$. Clearly terms divisible by X_1 or X_2^2 lie in the ideal $(X_1, X_2^2, X_2X_3^{p-3})$. Thus we may restrict our attention to monomials of the form $X_2X_3^{p-2+i-a}X_4^a$. If $p-2+i-a \geq p-3$, this monomial lies in $(X_1, X_2^2, X_2X_3^{p-3})$. Therefore, it is sufficient to show that if $a > i+1$, the term with monomial $X_2X_3^{p-2+i-a}X_4^a$ does not survive the summation. The coefficient of $X_2X_3^{p-2+i-a}X_4^a$ in $\sigma^j(X_4^{p-1})$ is $(p-1)j^{p-2-a}\binom{j}{2}\binom{p-2}{a} + ij^{p-a}\binom{p-1}{a}$. This coefficient has degree $p-a$ as a polynomial in j. Since $i+1 < a$, we have $p-a < p-(i+1) = (p-1)-i$. Therefore $p-a < p-1$ and the term does not survive the summation, proving the claim.

The only remaining invariant is $N(X_4)$. Working modulo (X_1), the variable X_4 generates an $\mathbf{FZ}/p$ – module isomorphic to V_3. Thus we may use the results of Section 6. Write $N(X_4) \equiv_{(X_1,X_2^2)} A_0 + A_1X_2$ for $A_0, A_1 \in \mathbf{F}[X_3, X_4]$. By Theorem 6.1, we may take $A_0 = X_4^p - X_4X_3^{p-1}$ and $A_1 = \xi_{11}X_4X_3^{p-2} + \xi_{12}X_4^2X_3^{p-3}$. Thus $X_2A_1 \in (X_2X_3^{p-3})$ and $N(X_4) - X_4^p \in (X_1, X_2^2, X_2X_3^{p-3}, X_3^{p-1})$. Therefore $N(X_4)$ contributes X_4^p to the Gröbner basis.

We have shown that $\{X_1, X_2^2, X_2X_3^{p-3}, X_3^{p-1}, X_4^p\}$ generates the Hilbert ideal. Furthermore, it is clear that this is a minimal generating set of monomials and is, therefore, a reduced universal Gröbner basis. The corresponding monomial basis consists of all monomials not divisible by any of the generators and the description of the Hilbert series comes from the monomial basis. □

Remark 3.3. *We observe that the top degree of* $\mathbf{F}[V_4]_{\mathbf{Z}/p}$ *is* $2p-3$. *It is clear that* $2p-3$ *is an upper bound for the Noether number of* V_4. *Using the theory of SAGBI bases it is possible to prove that that* $\mathrm{Tr}(X_3^{p-2}X_4^{p-1})$ *is indecomposable and, therefore,* $\beta(V_4) = 2p-3$. *We give a sketch of the proof. For the required background see* [18] *or* [27, Ch. 11].

Let $\mathcal{C}$ *denote the generating set given above and define* $\mathcal{D} = \mathcal{C}\setminus\{\mathrm{Tr}(X_3^{p-2}X_4^{p-1})\}$. *Note that the elements of* $\mathcal{D}$ *all have degree less than* $2p-3$. *Recall that* $\mathcal{C}$ *is a SAGBI basis for* $\mathbf{F}[V_4]^{\mathbf{Z}/p}$. *Therefore* $\mathcal{D}$ *is "SAGBI to degree* $2p-4$*". The leading monomial of* $\mathrm{Tr}(X_3^{p-2}X_4^{p-1})$ *is* X_3^{2p-3}. *The powers of* X_3 *appearing in* $\mathrm{LM}(\mathcal{D})$ *are* $X_3^{p-1}, X_3^p, \ldots, X_3^{2p-4}$. *Therefore the leading monomial of* $\mathrm{Tr}(X_3^{p-2}X_4^{p-1})$ *does not factor over* $\mathrm{LM}(\mathcal{D})$ *and* $\mathcal{D}$ *is not a SAGBI basis for* $\mathbf{F}[V_4]^{\mathbf{Z}/p}$. *Thus either* $\mathrm{Tr}(X_3^{p-2}X_4^{p-1})$ *is indecomposable or a non-trivial tête-a-tête from* $\mathcal{D}$ *subducts to an invariant with leading monomial* X_3^{2p-3}. *However, the only monomials in degree* $2p-3$ *which are greater than* X_3^{2p-3} *are of the form* $X_3^{2p-3-a}X_4^a$ *and the only element of* $\mathcal{D}$ *whose lead monomial is divisible by* X_4 *is* $N(X_4)$. *Therefore the only tête-a-têtes from* $\mathcal{D}$ *which could subduct to an invariant with leading monomial* X_3^{2p-3} *are of the form* $f_1N(X_4) - f_2N(X_4)$. *However,* $\mathcal{D}$ *is "SAGBI to degree* $2p-4$*". Therefore the tête-a-tête* $f_1 - f_2$ *subducts to zero. Thus* $f_1N(X_4) - f_2N(X_4)$ *subducts to zero. Since no tête-a-tête from* $\mathcal{D}$ *can subduct to an invariant with leading monomial* X_3^{2p-3}, $\mathrm{Tr}(X_3^{p-2}X_4^{p-1})$ *is indecomposable.*

4. The coinvariants of V_5

The generating set for $\mathbf{F}[V_5]^{\mathbf{Z}/p}$ given in [20] can be used to construct a reduced Gröbner basis for the Hilbert ideal. Choose a basis $\{X_1, X_2, X_3, X_4, X_5\}$ for V_5^* with $\Delta(X_i) = X_{i-1}$ for $i > 1$ and $\Delta(X_1) = 0$. We use the graded reverse lexicographic order with $X_1 < X_2 < X_3 < X_4 < X_5$.

Theorem 4.1. *For* $p > 5$, *a reduced Gröbner basis for the Hilbert ideal of* V_5 *is given by*

$$\{X_1, X_2^2, X_3^2 - 2X_4X_2 - X_3X_2, X_4X_3X_2, X_4^{p-4}X_2, X_4^{p-3}X_3, X_4^{p-1}, X_5^p\},$$

the corresponding monomial basis for $\mathbf{F}[V_5]_{\mathbf{Z}/p}$ *is given by the monomial factors of* $x_4^{p-2}x_5^{p-1}$, $x_3x_4^{p-4}x_5^{p-1}$, $x_2x_4^{p-5}x_5^{p-1}$, *and* $x_2x_3x_5^{p-1}$, *and the Hilbert series of* $\mathbf{F}[V_4]_{\mathbf{Z}/p}$ *is given by* $(1+3t+4t^2+3(t^3+\cdots+t^{p-4})+2t^{p-3}+t^{p-2})(1+t+\cdots+t^{p-1})$.

Remark 4.2. *For* $p = 5$, *a MAGMA* [3] *calculation shows that a reduced Gröbner basis for the Hilbert ideal of* V_5 *is given by*

$$\{X_1, X_2^2, X_3^2 - 2X_4X_2 - X_3X_2, X_2X_3X_4, X_4^2X_3 + 2X_4^2X_2, X_4^3X_2, X_4^4, X_5^5\},$$

the corresponding monomial basis for $\mathbf{F}[V_5]_{\mathbf{Z}/5}$ *is given by the monomial factors of* $x_4^3x_5^4$, $x_3x_4x_5^4$, $x_2x_4^2x_5^4$, *and* $x_2x_3x_5^4$ *and the Hilbert series of* $\mathbf{F}[V_5]_{\mathbf{Z}/p}$ *is given by* $(1+3t+4t^2+2t^3)(1+t+t^2+t^3+t^4)$.

We give an outline of the proof of Theorem 4.1 and refer the reader to Section 5 of [19] for the details. The generating set given in [20, 5.1] consists of a list of prime independent *rational* invariants, a list of transfers, and $N(X_5)$. The first four rational invariants are X_1, $X_2^2 - X_1(X_2+2X_3)$, $X_3^2 - X_2(X_3+2X_4) + X_1(X_3+3X_4+2X_5)$ and $X_2^3 + X_1^2(3X_4 - X_2) - 3X_1X_2X_3$. These invariants contribute X_1, X_2^2

and $X_3^2 - X_2(X_3+2X_4)$ to the reduced Gröbner basis. The fifth rational invariant, denoted by $\overline{\mathrm{inv}}(X_3^3)$ in [20], can be computed using the algorithm given in the proof of [20, 2.3]. Working modulo the ideal generated by X_1, this computation gives $\overline{\mathrm{inv}}(X_3^3) \equiv_{(X_1)} 2X_3^3 - 6X_2X_3X_4 + 6X_2^2X_5 - 2X_2^2X_3 - 3X_2X_3^2 - 6X_2^2X_4$. This invariant contributes $X_2X_3X_4$ to the reduced Gröbner basis. The sixth rational invariant is in fact decomposable and was required in [20, 5.1] in order for the generating set to be a SAGBI basis. Therefore, denoting the ideal generated by the rational invariants by $\mathfrak{R}$, we have

$$\mathfrak{R} = (X_1, X_2^2, X_3^2 - X_2(X_3 + 2X_4), X_2X_3X_4)\mathbf{F}[V].$$

We next consider the contribution of the transfers to the Hilbert ideal. The generating set in [20, 5.1] includes one exceptional transfer, $\mathrm{Tr}(X_2X_3X_5^{(p-1)/2})$, and the following five families:
(i) $\mathrm{Tr}(X_4^iX_5^{p-1})$ and $\mathrm{Tr}(X_2X_4^iX_5^{p-1})$ for $0 \le i \le p-2$,
(ii) $\mathrm{Tr}(X_4^iX_5^{p-2})$ and $\mathrm{Tr}(X_2X_4^iX_5^{p-2})$ for $3 \le i \le p-2$,
(iii) $\mathrm{Tr}(X_4^2X_5^i)$ and $\mathrm{Tr}(X_2X_4^2X_5^i)$ for $(p-1)/2 \le i \le p-2$,
(iv) $\mathrm{Tr}(X_5^i)$ for $(p+1)/2 \le i \le p-1$,
(v) $\mathrm{Tr}(X_2X_5^i)$ for $(p-1)/2 \le i \le p-2$.

The only contribution to the Hilbert ideal comes from the fourth family. Define $I := \mathfrak{R} + (\mathrm{Tr}(X_5^i) \mid i = (p-3)/2, \ldots, p-1)$. Careful term analysis can be used to show that $\{X_1, X_2^2, X_3^2 - 2X_4X_2 - X_3X_2, X_4X_3X_2, X_4^{p-4}X_2, X_4^{p-3}X_3, X_4^{p-1}\}$ is a generating set for I (see pages 14–16 of [19]).

The final element remaining in the generating set is $N(X_5)$. The leading monomial of $N(X_5)$ is clearly X_5^p. Choose polynomials B_0 and B_1 in $\mathbf{F}[X_3, X_4, X_5]$ such that $N(X_5) \equiv_{(X_1, X_2^2)} B_0 + X_2B_1$. Working modulo (X_1, X_2), the variable X_5 generates an $\mathbf{FZ}/p$ – module isomorphic to V_3. Thus the results of Section 6 may be applied to compute B_0 giving $B_0 \equiv_I X_5^p$. A careful expansion and simplification gives $X_2B_1 \in I$, completing the proof of Theorem 4.1 (see pages 17 and 18 of [19]).

Remark 4.3. *We observe that the top degree of* $\mathbf{F}[V_5]_{\mathbf{Z}/p}$ *is* $2p-3$. *It is clear that* $2p-3$ *is an upper bound for the Noether number of* V_4. *It follows from Remark 3.3 and* [21, 4.2]*, that the Noether number of* V_5 *is* $2p-3$.

5. The module structure for the coinvariants of V_4 and V_5

The bases constructed in Sections 3 and 4 can be used to determine the $\mathbf{FZ}/p$ – module structure of the coinvariants of V_4 and V_5. Note that, since the Hilbert ideal is homogeneous, the coinvariants are a graded ring. Furthermore, the group action preserves degrees. Thus the homogeneous components are $\mathbf{FZ}/p$ – module summands. We will refine this decomposition by describing each homogeneous component as a direct sum of indecomposable modules.

Recall that the socle of a module is the sum of its irreducible submodules. For an $\mathbf{FZ}/p$ – module, this is the span of the fixed points. A non-zero cyclic $\mathbf{FZ}/p$ – module has a one dimensional socle and, since all indecomposable $\mathbf{FZ}/p$ – modules are cyclic, the dimension of the socle is the number of summands.

Lemma 5.1. *Suppose that $W_1, W_2, \dots W_m$ are cyclic submodules of W and that ω_i spans the socle of W_i. If $\{\omega_1, \omega_2, \dots, \omega_m\}$ is linearly independent and $\dim(W) = \dim(W_1) + \dim(W_2) + \cdots + \dim(W_m)$, then $W = W_1 \oplus W_2 \oplus \cdots \oplus W_m$.*

Proof. For a homomorphism of modules, the socle of the kernel is the kernel of the restriction of the homomorphism to the socle. Thus a homomorphism which is injective on its socle is injective. Apply this to the homomorphism from the external direct sum of the W_i to their internal sum. Since $\{\omega_1, \omega_2, \dots, \omega_m\}$ is linearly independent, this map is injective on its socle and hence injective. Therefore the internal sum of the W_i is direct and $W_1 \oplus W_2 \oplus \cdots \oplus W_m$ is a subspace of W. However, since $\dim(W) = \dim(W_1) + \dim(W_2) + \cdots \dim(W_m)$, the subspace coincides with W. □

We define the *weight* of a monomial in $\mathbf{F}[V_n]$ by $\mathrm{wt}(X_1^{e_1} \cdots X_n^{e_n}) = e_1 + 2e_2 + \cdots + ne_n$. If f is a linear combination of monomials of the same weight, we will refer to f as *isobaric* and we will take the weight of f to be the common weight of the monomials appearing in f. Note that if β is a monomial appearing in $\Delta(f)$ with f isobaric, then $\mathrm{wt}(\beta) < \mathrm{wt}(f)$. Thus, for a fixed positive integer m, the span of the monomials of weight less than m forms an $\mathbf{FZ}/p$ – submodule. Allowing m to vary over the positive integers gives a weight filtration of the polynomial ring. For V_4 and V_5 we fix a basis for the coinvariants given by images of monomials. For V_4, the basis is given in Theorem 3.2 and for V_5 the basis is given by Theorem 4.1. We define the weight of the basis elements to be the weight of the corresponding monomial and, as in the polynomial ring, a linear combination of basis elements of a common weight is isobaric with a well defined weight.

Lemma 5.2. *If f is an isobaric coinvariant of weight m, then $\Delta(f)$ is in the span of the basis elements of weight less than m.*

Proof. Since Δ is linear it is sufficient to consider $\Delta(\beta)$ for a basis element β of weight m. To compute $\Delta(\beta)$, we lift to the corresponding monomial in the polynomial ring, say $\overline{\beta}$, compute $\Delta(\overline{\beta})$, and then project back to coinvariants. The terms appearing in $\Delta(\overline{\beta})$ all have weight less than m. For V_4, the reduced Gröbner basis is a set of monomials. Thus each term appearing in $\Delta(\overline{\beta})$ either projects to zero or projects to a term of weight less than m. For V_5, there are seven monomial relations and one non-isobaric relation given by $X_3^2 - 2X_2X_4 - X_2X_3$. This last relation is used to give a rewriting rule which replaces the product $x_3 \cdot x_3$ with $2x_2x_4 + x_2x_3$. Thus an element of weight 6 in the polynomial ring is identified with a sum of two terms, one of weight 6 and one of weight 5, in the coinvariants. Thus each term appearing in $\Delta(\overline{\beta})$ either projects to zero or projects to a linear combination of terms with weight less than m. □

As a consequence of Lemma 5.2, for each positive integer m, the span of the basis elements of weight less than m form an $\mathbf{FZ}/p$ – submodule. Collectively these submodules give a weight filtration of the coinvariants. Suppose β is a basis element of weight m. Define $\delta(\beta)$ to be the sum of terms of weight $m-1$ appearing in $\Delta(\beta)$ and extend δ to a linear map on the coinvariants. We can think of δ as the linear map induced by Δ on the associated graded module of

the weight filtration. In the following we use $\mathbf{F}[V]^d_{\mathbf{Z}/p}$ to denote the homogeneous component of degree d.

Lemma 5.3. *Suppose n is 4 or 5, and m is the minimum weight occurring in $\mathbf{F}[V_n]^d_{\mathbf{Z}/p}$. For an isobaric coinvariant f of weight ℓ and a positive integer k, any term appearing in $\delta^k(f) - \Delta^k(f)$ has weight less than $\ell - k$. In particular, if $\ell = m + k$, then $\delta^k(f) = \Delta^k(f)$. Furthermore, if $\ell = m$, then f is invariant.*

Proof. The proof is by induction on k. For $k = 1$, the result is essentially the definition of δ. Suppose the result is true for $k > 1$. Then $\delta^k(f) = \Delta^k(f)+h$ where h is a sum of terms of weight less than $\ell-k$. Thus $\delta(\delta^k(f))$ consists of the sum of the terms of weight $\ell-k-1$ in $\Delta(\Delta^k(f))+\Delta(h)$. However, from Lemma 5.2, all of terms appearing in $\Delta(h)$ have weight less than $\ell-k-1$. Therefore $\delta^{k+1}(f)$ consists of the sum of the terms of weight $\ell - (k + 1)$ appearing in $\Delta^{k+1}(f)$, as required. If $\ell - k = m$, there are no terms of weight less than $\ell - k$ so $\delta^k(f) = \Delta^k(f)$. If $\ell = m$, the fact that f is invariant follows from Lemma 5.2. □

Theorem 5.4. $\mathbf{F}[V_4]^0_{\mathbf{Z}/p} \cong V_1$ *and* $\mathbf{F}[V_4]^1_{\mathbf{Z}/p} \cong V_3$.

For $d = 2, \dots, p-3$,

$$\mathbf{F}[V_4]^d_{\mathbf{Z}/p} = x_4^d\mathbf{F}\mathbf{Z}/p \oplus \left(x_3^2x_4^{d-2} - \frac{d+2}{2}x_2x_4^{d-1}\right)\mathbf{F}\mathbf{Z}/p \cong V_{d+2} \oplus V_{d-1}$$

with $\left(\mathbf{F}[V_4]^d_{\mathbf{Z}/p}\right)^{\mathbf{Z}/p} = \mathrm{Span}\{x_3^d - dx_2x_3^{d-2}x_4, x_2x_3^{d-1}\}$.

For $d = p-2, p-1$,

$$\mathbf{F}[V_4]^d_{\mathbf{Z}/p} = x_4^d\mathbf{F}\mathbf{Z}/p \oplus \ x_2x_4^{d-1}\mathbf{F}\mathbf{Z}/p \cong V_{p-1} \oplus V_{p-3}$$

with $\left(\mathbf{F}[V_4]^d_{\mathbf{Z}/p}\right)^{\mathbf{Z}/p} = \mathrm{Span}\{x_3^{p-2}x_4^{d-(p-2)}, x_2x_3^{p-4}x_4^{d-(p-3)}\}$.

For $d = p, \dots, 2p-4$,

$$\mathbf{F}[V_4]^d_{\mathbf{Z}/p} = x_3^{d-(p-1)}x_4^{p-1}\mathbf{F}\mathbf{Z}/p \oplus \ x_2x_3^{d-p}x_4^{p-1}\mathbf{F}\mathbf{Z}/p \cong V_{2p-2-d} \oplus V_{2p-3-d}$$

with $\left(\mathbf{F}[V_4]^d_{\mathbf{Z}/p}\right)^{\mathbf{Z}/p} = \mathrm{Span}\{x_3^{p-2}x_4^{d-(p-2)}, x_2x_3^{p-4}x_4^{d-(p-3)}\}$.

$\mathbf{F}[V_4]^{2p-3}_{\mathbf{Z}/p} = \mathrm{Span}(x_3^{p-2}x_4^{p-1}) \cong V_1$.

Theorem 5.5. *Suppose $p > 5$.*

$\mathbf{F}[V_5]^0_{\mathbf{Z}/p} \cong V_1$, $\mathbf{F}[V_5]^1_{\mathbf{Z}/p} \cong V_4$ *and* $\mathbf{F}[V_5]^2_{\mathbf{Z}/p} \cong V_6 \oplus V_2$.

For $p > 11$: $\mathbf{F}[V_5]^3_{\mathbf{Z}/p} \cong V_6 \oplus V_4 \oplus V_1$ *and* $\mathbf{F}[V_5]^4_{\mathbf{Z}/p} \cong V_7 \oplus V_4 \oplus V_3$.

For $d = 5, \dots, p-4$*: if* $3d-1 \not\equiv_{(p)} 0$ *and* $3d-2 \not\equiv_{(p)} 0$ *then*

$$\mathbf{F}[V_5]^d_{\mathbf{Z}/p} \cong V_{d+3} \oplus V_d \oplus V_{d-2} \oplus V_1;$$

if $3d-1 \not\equiv_{(p)} 0$ *and* $3d-2 \equiv_{(p)} 0$ *then*

$$\mathbf{F}[V_5]^d_{\mathbf{Z}/p} \cong V_{d+3} \oplus 2V_{d-1} \oplus V_1;$$

if $3d-1 \equiv_{(p)} 0$ *then* $\mathbf{F}[V_5]^d_{\mathbf{Z}/p} \cong V_{d+2} \oplus V_{d+1} \oplus V_{d-2} \oplus V_1$.

For $d = p-3$ *and* $p > 11$*:* $\mathbf{F}[V_5]^d_{\mathbf{Z}/p} \cong V_{p-1} \oplus V_{p-3} \oplus V_{p-5} \oplus V_1$.

For $d = p-2,\ p-1$*:* $\mathbf{F}[V_5]^d_{\mathbf{Z}/p} \cong V_{p-1} \oplus V_{p-3} \oplus V_{p-4} \oplus V_1$.

For $d = p,\ p+1$*:* $\mathbf{F}[V_5]^d_{\mathbf{Z}/p} \cong V_{2p-d-2} \oplus V_{2p-d-3} \oplus V_{2p-d-4} \oplus V_1$.

For $d = p+2, \ldots, 2p-5$*:* $\mathbf{F}[V_5]^d_{\mathbf{Z}/p} \cong V_{2p-d-2} \oplus V_{2p-d-3} \oplus V_{2p-d-4}$.

$\mathbf{F}[V_5]^{2p-4}_{\mathbf{Z}/p} \cong V_2 \oplus V_1$ *and* $\mathbf{F}[V_5]^{2p-3}_{\mathbf{Z}/p} \cong V_1$.

Remark 5.6. *MAGMA* [3] *calculations give the following:*

For $p = 5$*, the homogeneous component of* $\mathbf{F}[V_5]_{\mathbf{Z}/5}$*, in increasing degree, are isomorphic to* V_1*,* V_4*,* $2V_4$*,* $2V_4 \oplus 2V_1$*,* $2V_4 \oplus 2V_1$*,* $V_3 \oplus V_4 \oplus 2V_1$*,* $V_4 \oplus 2V_1$*,* $2V_1$*;*

For $p = 7$*:* $\mathbf{F}[V_5]^3_{\mathbf{Z}/7} \cong V_6 \oplus V_3 \oplus V_2$ *and* $\mathbf{F}[V_5]^4_{\mathbf{Z}/7} \cong V_6 \oplus V_4 \oplus V_3$*;*

For $p = 11$*:* $\mathbf{F}[V_5]^3_{\mathbf{Z}/11} \cong V_6 \oplus V_4 \oplus V_1$*,* $\mathbf{F}[V_5]^4_{\mathbf{Z}/11} \cong V_6 \oplus V_5 \oplus V_3$ *and* $\mathbf{F}[V_5]^8_{\mathbf{Z}/11} \cong V_{10} \oplus 2V_7 \oplus V_1$.

The proofs of Theorems 5.4 and 5.5 involve calculating $\delta^k(\beta)$ for various coinvariants β, and using the results to determine the socles and dimensions of the corresponding cyclic modules. Lemma 5.1 is then used to identity the decomposition. The details can be found in Section 6 of [19].

6. The expansion of $N(Z)$

In this section we describe the expansion of the norm of an $\mathbf{F}\mathbf{Z}/p$ – module generator of V_3^*. This expansion is used in the proofs of Theorems 3.2 and 4.1. Furthermore, although the result is somewhat technical, we believe it may be of independent interest.

Choose a basis $\{X, Y, Z\}$ for V_3^* with $\Delta(Z) = Y$, $\Delta(Y) = X$ and $\Delta(X) = 0$. Write $N(Z) = A_0 + A_1X + \cdots + A_pX^p$ with each $A_i \in \mathbf{F}[Y, Z]$.

Lemma 6.1. $A_0 = Z^p - ZY^{p-1}$*,* $A_p = A_{p-1} = 0$ *and*

$$A_i = \begin{cases} \sum_{k=1}^{i+1} \xi_{ik} Z^k Y^{p-i-k} & \text{for } 1 \le i \le \frac{p-1}{2}, \\ \sum_{k=1}^{p-i} \xi_{ik} Z^k Y^{p-i-k} & \text{for } \frac{p+1}{2} \le i \le p-2, \end{cases}$$

where $\xi_{ik} = \frac{(-1)^i}{2^i(p-k)} \binom{p-2k+1}{i-k+1} \binom{p-k}{k-1}$.

Proof. Let S_i denote the set of subsets of $\mathbf{F}_p$ of size i and, for $j \in \mathbf{F}_p$, let $S_{i,j}$ denote the set of subsets of $\mathbf{F}_p$ of size i not containing j. For a set $\gamma \subseteq \mathbf{F}_p$, let $S_{b,\gamma}$ denote the set of subsets of $\mathbf{F}_p$ of size b that do not contain any element from the set γ and for $\alpha \subseteq \mathbf{F}_p$, let $\sigma_k(\alpha)$ denote the k^{th} elementary symmetric polynomial in the elements of α. For convenience, we set $\sigma_0(\alpha) = 1$ and to simplify notation we will denote $\sigma_i(\alpha)$ by $\pi(\alpha)$ for $\alpha \in S_i$. For $j \le k$, define functions $b_{k,j} : \mathbf{F}_p \to \mathbf{F}_p$ by

$$b_{k,j}(t) := \sum_{\alpha \in S_{k-1,t}} t\pi(\alpha)\sigma_j(\alpha \cup \{t\})$$

and set $d_{k,j} := \sum_{\alpha \in S_k} \pi(\alpha)\sigma_j(\alpha)$. Note that $d_{0,0} = 1$.

Let $A_{b,c}$ denote the coefficient of $X^cY^bZ^{p-c-b}$ in $N(Z)$. Recall that $\sigma^m(Z) = Z + mY + \binom{m}{2}X$. By identifying the terms in $\prod_{m\in\mathbf{F}_p}\sigma^m(Z)$ which contribute to the coefficient of $X^cY^bZ^{p-c-b}$ we see that

$$\begin{aligned} A_{b,c} &= \sum_{\{i_1,\dots,i_c\}\in S_c}\ \sum_{\{j_1,\dots j_b\}\in S_{b,\{i_1,\dots,i_c\}}} \binom{i_1}{2}\binom{i_2}{2}\cdots\binom{i_c}{2} j_1\cdots j_b \\ &= \frac{1}{2^c}\sum_{\gamma\in S_c,\ \alpha\in S_{b,\gamma}} \pi(\alpha)\prod_{i\in\gamma}(i^2-i). \end{aligned}$$

Expanding gives

$$\prod_{i\in\gamma}(i^2-i) = \sum_{\beta\subseteq\gamma}(-1)^{|\gamma\setminus\beta|}\pi(\beta)\pi(\gamma) = \pi(\gamma)\sum_{\ell=0}^{c}(-1)^{c-l}\sigma_\ell(\gamma).$$

Substituting this into the previous expression gives

$$\begin{aligned} A_{b,c} &= \frac{1}{2^c}\sum_{\gamma\in S_c,\ \alpha\in S_{b,\gamma}} \pi(\alpha)\pi(\gamma)\sum_{\ell=0}^{c}(-1)^{c-l}\sigma_\ell(\gamma) \\ &= \frac{1}{2^c}\sum_{\ell=0}^{c}(-1)^{c-\ell}\left(\sum_{\gamma\in S_c,\ \alpha\in S_{b,\gamma}}\sigma_\ell(\gamma)\pi(\alpha)\pi(\gamma)\right). \end{aligned}$$

Using Lemma 2.7 of [19] gives

$$A_{b,c} = \frac{1}{2^c}\sum_{\ell=0}^{c}(-1)^{c-\ell}\binom{b+c-\ell}{b} d_{b+c,\ell}.$$

From [19, Lemma 2.5], $d_{k,j} = \frac{(-1)^k}{k}\binom{k}{j}$ if $k+j = p-1$. From [19, Lemmas 2.5–2.7], $d_{k,j} = 0$ if $1 \le k+j < 2p-2$ and $k+j \ne p-1$. The polynomial A_i is clearly determined by the coefficients $A_{b,i}$, completing the proof of the lemma. □

References

[1] W.W. Adams, P. Loustaunau, *An Introduction to Gröbner Bases*, Graduate Studies in Math. **3**, Amer. Math. Soc., 1994.

[2] D. Benson, *Polynomial Invariants of Finite Groups*, Cambridge Univ. Press, 1993.

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

[4] N. Bourbaki, *Éléments de mathématique: Groupes et algèbras de Lie. Chapitres 4, 5 et 6*, Masson, 1981.

[5] H.E.A. Campbell, B. Fodden, D.L. Wehlau, *Invariants of the diagonal C_p-action on V_3,* J. Algebra, to appear.

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

[7] H.E.A. Campbell, I.P. Hughes, R.J. Shank, D.L. Wehlau, *Bases for rings of coinvariants,* Transformation Groups **1** (4) (1996), 307-336.

[8] C. Chevalley, *Invariants of finite groups generated by reflections*, Amer. J. Math. **77** (1955), 778–782.

[9] H. Derksen, G. Kemper, *Computational Invariant Theory*, Springer-Verlag, 2002.

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

[11] I.G. Gordan, *On the quotient ring by diagonal invariants*, Invent. Math. **153** (2003), 503–518.
[12] J. Haglund, M. Haiman, N. Loehr, J. B. Remmel, A. Ulyanov, *A Combinatorial Formula for the Character of the Diagonal Coinvariants*, Duke Math. J. **126** (2005) no. 2, 195–232.
[13] M.D. Haiman, *Conjectures on the quotient ring by diagonal invariants*, J. Algebraic Combin. **3** (1994) no. 1, 17-76.
[14] I.P. Hughes, G. Kemper, *Symmetric Powers of Modular Representations, Hilbert Series and Degree Bounds*, Comm. Algebra **28** (2000) no. 4, 2059–2088.
[15] R. Kane, *Reflection Groups and Invariant Theory*, Springer-Verlag, 2001.
[16] M.D. Neusel, L. Smith, *Invariant Theory of Finite Groups*, Math. Surveys and Monographs **94**, Amer. Math. Soc., 2002.
[17] D. Richman, *On vector invariants over finite fields*, Adv. in Math. **81** (1990) 30–65.
[18] L. Robbiano, M. Sweedler, *Subalgebra bases*, Lecture Notes in Math. **1430**, pp. 61–87, Springer–Verlag, 1990.
[19] M. Sezer, R.J. Shank, *Coinvariants for modular representations of cyclic groups of prime order,* arXiv:math.AC/0409107 (2004) 29 pages.
[20] R.J. Shank, *S.A.G.B.I. bases for rings of formal modular semiinvariants,* Comm. Math. Helv. **73** (1998), 548-565.
[21] R.J. Shank, D.L. Wehlau, *Noether numbers for subrepresentations of cyclic groups of prime order* , Bull. London Math. Soc. **34** (2002), 438-450.
[22] R.J. Shank, D.L. Wehlau, *Computing modular invariants of p-groups*, J. Symbolic Comput. **34** (2002) no. 5, 307-327.
[23] L. Smith, *Polynomial Invariants of Finite Groups*, A.K. Peters Ltd., (1995).
[24] L. Smith, *Invariants and coinvariants of finite pseudoreflection groups, Jacobian determinants and Steenrod operation*, Proc. Edinb. Math. Soc., II. Ser. **44**(2001) no.3, 597–611.
[25] L. Smith, *On a theorem of R. Steinberg on rings of coinvariants*, Proc. Amer. Math. Soc. **131** (2003), 1043–1048.
[26] L. Smith, *A modular analog of a theorem of R. Steinberg on coinvariants of complex pseudoreflection groups*, Glasg. Math. J. **45** (2003) no.1, 69–71.
[27] B. Sturmfels, *Gröbner bases and convex polytopes*, Univ. Lect. Series **8**, Amer. Math. Soc., 1996.

Department of Mathematics, Boğaziçi University,
TR-34342 Bebek, Istanbul, Turkey

E-mail address: mufit.sezer@boun.edu.tr

Institute of Mathematics, Statistics & Actuarial Science,
University of Kent at Canterbury, CT2 7NF, UK

E-mail address: R.J.Shank@kent.ac.uk