Math. Ann. (2008) 341:575–587
DOI 10.1007/s00208-007-0203-2

Mathematische Annalen

The invariants of modular indecomposable representations of $\mathbb{Z}_{p^2}$

Mara D. Neusel · Müfit Sezer

Received: 15 August 2007 / Revised: 23 November 2007 / Published online: 9 January 2008

Abstract We consider the invariant ring for an indecomposable representation of a cyclic group of order p^2 over a field $\mathbb{F}$ of characteristic p. We describe a set of $\mathbb{F}$-algebra generators of this ring of invariants, and thus derive an upper bound for the largest degree of an element in a minimal generating set for the ring of invariants. This bound, as a polynomial in p, is of degree two.

0 Introduction

Let $\rho : G \hookrightarrow \mathsf{GL}(n, \mathbb{F})$ be a faithful representation of a finite group G. Denote by $V = \mathbb{F}^n$ the n-dimensional vector space over $\mathbb{F}$. Then G acts via ρ on V, which in turn induces an action on the dual space V^*. This extends to the symmetric algebra $S(V^*) = \mathbb{F}[V]$. The algebra of invariant polynomials

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

is a graded connected commutative Noetherian subalgebra of $\mathbb{F}[V]$, see [11] for a general treatment of the subject. Let

$$\beta(\mathbb{F}[V]^G)$$

M. D. Neusel (✉)
Department of Mathematics and Statistics, Texas Tech University,
MS 1042, Lubbock, TX 79409, USA
e-mail: Mara.D.Neusel@ttu.edu

M. Sezer
Department of Mathematics, Bilkent University, Ankara 06800, Turkey
e-mail: mufit.sezer@fen.bilkent.edu.tr

denote the smallest integer d such that $\mathbb{F}[V]^G$ is generated as an $\mathbb{F}$-algebra by homogeneous polynomials of degree at most d. In the nonmodular case, i.e., $|G| \in \mathbb{F}^\times$, we have that

$$\beta(\mathbb{F}[V]^G) \leq |G|,$$

see [11, Theorem 2.3.3] and the references there. This bound does not remain valid in the modular case, i.e., when $|G| \equiv 0 \in \mathbb{F}$. Indeed, Richmann constructed modular representations V with arbitrarily large $\beta(\mathbb{F}[V]^G)$, see [12]. In other words, there cannot be a degree bound for $\beta(\mathbb{F}[V]^G)$ that depends only on the group, see [10] for an overview in these matters.

In this paper we want to study rings of invariants of cyclic p-groups $\mathbb{Z}_{p^r}$ of order p^r over a field $\mathbb{F}$ of finite characteristic p. There are exactly p^r indecomposable $\mathbb{Z}_{p^r}$-modules, which we denote by $V_1, V_2, \ldots, V_{p^r}$, see [1, Chap. II], where V_n has dimension n as a vector space over $\mathbb{F}$.

We note that Göbel's bound gives, of course, a bound on the degrees of a generating set of $\mathbb{F}[V_{p^r}]^{\mathbb{Z}_{p^r}}$ for any p and r, see [11, Corollary 3.4.4]. In this case we have

$$\beta\left(\mathbb{F}[V_{p^r}]^{\mathbb{Z}_{p^r}}\right) \leq \max\left\{p^r, \binom{p^r}{2}\right\}.$$

This bound depends on the dimension of the representation which coincides in this case with the order of the group.

If $r = 1$ and $G = \mathbb{Z}_p$ is the cyclic group of prime order, then a general degree bound for a minimal generating set of the ring of invariants for any $\mathbb{Z}_p$-module V was given in [5]. This bound is sharp, as the case of the regular representation of $\mathbb{Z}_3$ shows.

For the case $r = 2$ much less is known: In [9] we find an explicit description of the ring of invariants $\mathbb{F}[V_3]^{\mathbb{Z}_4}$. This was generalized to $\mathbb{F}[V_{p+1}]^{\mathbb{Z}_{p^2}}$ in [13]. Furthermore, in [8] we find an explicit description of the ring of invariants of the regular representation of $\mathbb{Z}_4$.

We want to extend this study and find an upper bound for $\beta\left(\mathbb{F}[V_n]^{\mathbb{Z}_{p^2}}\right)$ for any indecomposable $\mathbb{Z}_{p^2}$-module V_n. In Sect. 1 we derive an upper bound for the top degree of the coinvariant ring. In Sect. 2 we describe a set of $\mathbb{F}$-algebra generators for $\mathbb{F}[V_n]^{\mathbb{Z}_{p^2}}$. This description yields an upper bound for $\beta\left(\mathbb{F}[V_n]^{\mathbb{Z}_{p^2}}\right)$. This bound transpires to be quadratic in p. We postpone some technical calculations to Sect. 3.

For the remainder of the paper, we assume that $G \cong \mathbb{Z}_{p^2}$ and that $H \cong \mathbb{Z}_p$ is the non-trivial subgroup.

We choose a basis $x_1, \ldots, x_n$ for the dual space V_n^* and write

$$\mathbb{F}[V_n] \cong \mathbb{F}[x_1, \ldots, x_n].$$

Next, we choose a generator σ for the group G. Then

$$\sigma x_i = \begin{cases} x_1 & \text{for } i = 1, \text{ and} \\ x_i + x_{i-1} & \text{for } 2 \leq i \leq n. \end{cases}$$

Set $\Delta = \sigma - 1$. Then we have

$$\Delta(x_i) = \begin{cases} 0 & \text{for } i = 1, \text{ and} \\ x_{i-1} & \text{for } 2 \leq i \leq n. \end{cases}$$

The various transfer maps involved are given by the following formulae

$$\mathrm{Tr}^G = \sum_{i=0}^{p^2-1} \sigma^i, \quad \mathrm{Tr}^H = \sum_{i=0}^{p-1} \sigma^{ip}, \quad \text{and} \quad \mathrm{Tr}^G_H = \sum_{i=0}^{p-1} \sigma^i.$$

We use the graded reverse lexicographic order with $x_i > x_{i-1}$ for $i = 2, \ldots, n$.

1 An upper bound for $\beta(\mathbb{F}[V]_G)$

Since G is a finite group, the extension $\mathbb{F}[V]^G \hookrightarrow \mathbb{F}[V]$ is finite. Denote by $(\overline{\mathbb{F}[V]^G}) \subseteq \mathbb{F}[V]$ the Hilbert ideal, i.e., the ideal generated by the invariants of positive degree. Then the coinvariants

$$\mathbb{F}[V]_G = \mathbb{F}[V]/(\overline{\mathbb{F}[V]^G})$$

form a finite-dimensional vector space over $\mathbb{F}$. Thus its Hilbert series is a polynomial. In this section we want to derive an upper bound on its degree.

Note that the Hilbert series of the Hilbert ideal $(\overline{\mathbb{F}[V]^G}) \subseteq \mathbb{F}[V]$ coincides with the Hilbert series of the ideal I of leading terms of $(\overline{\mathbb{F}[V]^G})$, see [2, Theorem 15.26]. Thus it suffices to find an upper degree bound for $\mathbb{F}[V]/I$.

If $n \leq p$ then V_n is an indecomposable $G/H \cong \mathbb{Z}_p$-module and thus $\mathbb{F}[V_n]^G \cong \mathbb{F}[V_n]^{G/H}$. Therefore we restrict our attention to the case $n > p$ in what follows.

We need two somewhat technical constructions:

Let r be a positive integer with $\max\{n-2p, 1\} \leq r \leq n-p$. Set $d = \max\{1, r-p+1\}$. Then choose a monomial $\mathbf{m} \in \mathbb{F}[d_d, \ldots, x_r]$ of degree $2p-2$. We write

$$\mathbf{m} = u_1 u_2 \cdots u_{2p-2}$$

for suitable $u_i \in \{x_d, \ldots, x_r\}$. Without loss of generality we assume that the u_i's are numbered such that

$$u_1 \leq u_2 \leq \cdots \leq u_{2p-2}.$$

Thus $x_d \leq u_1 \leq \cdots \leq u_{2p-2} \leq x_r \leq x_{n-p}$. Therefore, for $u_i = x_j$, there exist x_{j+1} and x_{j+p} which satisfy

$$\Delta(x_{j+1}) = x_j = u_i \quad \text{and} \quad \Delta^p(x_{j+p}) = x_j = u_i.$$

Hence we can define $w_{i,0} \in \{x_{d+1}, \ldots, x_n\}$ by

$$u_i = \begin{cases} \Delta(w_{i,0}) & \text{if } 1 \le i \le p-1, \text{ and} \\ \Delta^p(w_{i,0}) & \text{if } p \le i \le 2p-2, \end{cases}$$

and set

$$w_{i,j} = \Delta^j(w_{i,0}) \quad 1 \le i \le 2p-2, \; j \in \mathbb{N}_0.$$

For a $2p-2$-tuple $\alpha = [\alpha(1), \alpha(2), \ldots, \alpha(2p-2)] \in \mathbb{N}^{2p-2}$ of natural numbers we define

$$w_\alpha = \prod_{i=1}^{2p-2} w_{i,\alpha(i)}.$$

Thus we can write

$$\mathbf{m} = u_1 u_2 \cdots u_{2p-2} = \prod_{i=1}^{p-1} w_{i,1} \prod_{i=p}^{2p-2} w_{i,p} = w_{\alpha'},$$

where $\alpha'(i) = 1$ if $1 \le i \le p-1$ and $\alpha'(i) = p$ if $p \le i \le 2p-2$.

Let $S \subseteq \{1, 2, \ldots, 2p-2\}$ be a subset and set

$$X_S = \prod_{i \in S} w_{i,0}.$$

We consider the following polynomial

$$\mathsf{T}_1(\mathbf{m}) = \sum_{S \subseteq \{1,\ldots,2p-2\}} (-1)^{|S|} X_{S'} \mathrm{Tr}^G(X_S),$$

where S' denotes the complement of S in $\{1, 2, \ldots, 2p-2\}$.

Proposition 1 *The leading term of* $\mathsf{T}_1(\mathbf{m})$ *is* $\mathbf{m}$.

Proof The proof of this result is postponed to Sect. 3. □

The polynomials $\mathsf{T}_1(\mathbf{m})$ are by construction in the Hilbert ideal $(\overline{\mathbb{F}[V]^G}) \subseteq \mathbb{F}[V]$. Thus the preceding result tells us that any monomial divisible by some $\mathbf{m}$ is in the ideal I of leading terms of the Hilbert ideal.

We need another, similar, construction. Since $n > p$, the G-module V_n^* decomposes into a direct sum of p indecomposable H-modules:

$$V_n^* = V_{n,1}^* \oplus \cdots \oplus V_{n,p}^*.$$

Moreover, $V_{n,i}^*$ is generated as a H-module by x_i for $i = n-p+1, \ldots, n$.

For each $i = n - p + 1, \dots, n$, we define the H-norms

$$\mathsf{N}_i^H = \prod_{\sigma \in H} \sigma x_i .$$

Note that every N_i^H has degree p and coincides with the respective top orbit Chern classes if $i \geq p$.

Choose a monomial

$$\mathbf{M} = \prod_{1 \leq j \leq p-1} \mathsf{N}_{i_j}^H \in \mathbb{F}[\mathsf{N}_d^H, \dots, \mathsf{N}_{n-1}^H]$$

of degree $p-1$ as a polynomial in these norms. For $1 \leq j \leq p-1$ define $W_j = \mathsf{N}_{i_j+1}^H$. Let $S \subseteq \{1, \dots, p-1\}$ be a subset and S' its complement. Then similarly to the contruction of $\mathsf{T}_1(\mathbf{m})$ we set $X_S = \prod_{j \in S} W_j$, and obtain a polynomial $\mathsf{T}_2(\mathbf{M})$ as follows

$$\mathsf{T}_2(\mathbf{M}) = \sum_{S \subseteq \{1, \dots, p-1\}} (-1)^{|S|} X_{S'} \mathrm{Tr}_H^G(X_S).$$

Proposition 2 *The leading monomial of* $\mathsf{T}_2(\mathbf{M})$ *is the leading monomial of* $\mathbf{M}$.

Proof The proof of this result is postponed to Sect. 3. □

As for $\mathsf{T}_1(\mathbf{m})$ the polynomials $\mathsf{T}_2(\mathbf{M})$ lie in the Hilbert ideal associated to $\mathbb{F}[V]^G$. Thus the preceding result shows that any monomial divisible by the leading term of some $\mathbf{M}$ is contained in the ideal I of leading terms of the Hilbert ideal.

This enables us to prove the desired result:

Theorem 3 *Let* $n = tp + r > p$, *where* $1 \leq t \leq p$ *and* $0 \leq r < p$ *are integers. Then the top degree of* $\mathbb{F}[V_n]_G$ *is bounded above by* $3p^2 + (2t - 4)p - 3t$.

Proof The Hilbert series of the Hilbert ideal $(\overline{\mathbb{F}[V]^G}) \subseteq \mathbb{F}[V]$ coincides with the Hilbert series of the ideal, I, of leading terms of $(\overline{\mathbb{F}[V]^G})$. Thus in order to find a bound on the degrees of the coinvariants it suffices to find a degree bound for $\mathbb{F}[V]/I$.

To that end, let $m_1 m_2 x_n^l$ be a monomial that is not in the lead term ideal of the Hilbert ideal. Without loss of generality we assume that $m_1 \in \mathbb{F}[x_1, \dots, x_{n-p}]$ and $m_2 \in \mathbb{F}[x_{n-p+1}, \dots, x_{n-1}]$.

Let $\max\{n - 2p, 1\} \leq r \leq n - p$ and $\mathbf{m}$ a monomial of degree $2p - 2$ in $\mathbb{F}[x_d, \dots, x_r]$, where $d = \max\{1, r - p + 1\}$. Then Proposition 1 shows that $\mathbf{m}$ appears as leading term of some $\mathsf{T}_1(\mathbf{m})$. Since $\mathsf{T}_1(\mathbf{m})$ is contained in the Hilbert ideal it follows that the degree of m_1 is at most $t(2p - 3)$.

Similary, the polynomials $\mathsf{T}_2(\mathbf{M})$ are in the Hilbert ideal and thus by Proposition 2, m_2 is not divisible by the lead term of a product of $p - 1$ norms N_i^H, where $d \leq i \leq n - 1$. Therefore the degree of m_2 is at most $(p - 2)p + (p - 1)^2$.

Finally $x_n^{p^2}$ is the leading term of the norm $\mathsf{N}_n^G = \prod_{\sigma \in G} \sigma x_n$. Therefore $l \leq p^2 - 1$. Hence

$$\deg \left(m_1 m_2 x_n^l\right) \leq t(2p-3) + (p-2)p + (p-1)^2 + p^2 - 1 = 3p^2 + (2t-4)p - 3t$$

as claimed. □

Corollary 4 *Let $n > p$. Then the image of the transfer $\mathrm{Im}(\mathrm{Tr}^G) \subseteq \mathbb{F}[V]^G$ is generated by forms of degree at most $3p^2 + (2t-4)p - 3t$.*

Proof We write the ring of polynomials as a module over the ring of invariants as follows

$$\mathbb{F}[V] = \sum_{\text{finite}} \mathbb{F}[V]^G h_i.$$

We note that by construction the h_i's form a basis of $\mathbb{F}[V]_G$. Since $|G| = p^2 \equiv 0 \mod p$, we have that $\mathrm{Tr}^G(\mathbb{F}[V]^G) = 0$. Thus the image of the transfer is generated by the $\mathrm{Tr}^G(h_i)$'s, and the result follows from Theorem 3. □

2 Generators for rings of invariants

We apply the results found in the previous section to rings of invariants. We start with an explicit calculation for the regular representation.

Example 5 Consider the regular representation of $\mathbb{Z}_{p^2}$. Its ring of invariants is generated by forms of degree at most $5p^2 - 7p$. This can be seen as follows:

By Theorem 3.3 in [4], $\mathbb{F}[V_{p^2}]^G / \mathrm{Im}\mathrm{Tr}^G \simeq \mathbb{F}[V_p]^H$, where the isomorphism scales the degrees by $\frac{1}{p}$. It is shown in [5] that $\mathbb{F}[V_p]^H$ is generated by invariants of degree $2p-3$. Hence $\mathbb{F}[V_{p^2}]^G / \mathrm{Im}\mathrm{Tr}^G$ is generated by classes of degree at most $(2p-3)p$. On the other hand, Corollary 4 tells us that $\mathrm{Im}(\mathrm{Tr}^G)$ is generated by invariants of degree at most $5p^2 - 7p$. Hence

$$\beta(\mathbb{F}[V_{p^2}]^G) \leq \max\{(2p-3)p, 5p^2 - 7p\} = 5p^2 - 7p$$

as claimed.

We proceed to the general case. As in Sect. 1, let $n > p$ and

$$V_n^* = V_{n_{n-p+1}}^* \oplus \cdots \oplus V_{n_n}^*$$

be an H-module decomposition. For $i \in \{n-p+1, \ldots, n\}$ we have that x_i generates $V_{n_i}^*$ as H-module.

Lemma 6 *The image of the relative transfer, $\mathrm{Im}\mathrm{Tr}_H^G$, is generated by $\mathrm{Im}\mathrm{Tr}^G$ and G-invariants of degree at most $3p^2 - 3p$.*

Proof Let $f \in \mathbb{F}[V_n]^H$. By Lemma 2.12 in [7] the ring $\mathbb{F}[V_n]^H$ is generated as a module over $\mathbb{F}\left[\mathsf{N}_d^H, \ldots, \mathsf{N}_n^H\right]$ by invariants of degree at most $p^2 - n$ and the image of the transfer Tr^H. Thus f can be written as

$$f = \sum p_i \left(\mathsf{N}_d^H, \ldots, \mathsf{N}_n^H\right) b_i + \sum q_j \left(\mathsf{N}_d^H, \ldots, \mathsf{N}_n^H\right) \mathrm{Tr}^H(g_j)$$

for some polynomials $p_i,\ q_j \in \mathbb{F}\left[\mathsf{N}_d^H, \ldots, \mathsf{N}_n^H\right]$, H-invariants b_i of degree at most $p^2 - n$ and suitable $g_j \in \mathbb{F}[V_n]$. Since

$$\sum q_j \left(\mathsf{N}_d^H, \ldots, \mathsf{N}_n^H\right) \mathrm{Tr}^H(g_j) = \mathrm{Tr}^H \left(\sum q_j \left(\mathsf{N}_d^H, \ldots, \mathsf{N}_n^H\right) g_j\right)$$

we find that

$$\mathrm{Tr}_H^G \left(\sum q_j \left(\mathsf{N}_d^H, \ldots, \mathsf{N}_n^H\right) \mathrm{Tr}^H(g_j)\right) = \mathrm{Tr}^G \left(\sum q_j \left(\mathsf{N}_d^H, \ldots, \mathsf{N}_n^H\right) g_j\right)$$

is in the image of the transfer Tr^G. Thus we need to take care of the first summand and assume without lost of generality that

$$f = \sum p_i \left(\mathsf{N}_d^H, \ldots, \mathsf{N}_n^H\right) b_i. \qquad (\circ)$$

We sort $(\circ)$ by monomials in the norms and obtain

$$f = \sum_J b_J \mathsf{N}_J^H,$$

where b_J is a sum of suitable b_i's and thus is still an H-invariant of degree at most $p^2 - n$.

We claim that the degree of N_J^H as a polynomial in N_n^H is at most $p - 1$. Otherwise set $U = \left(\mathsf{N}_n^H\right)^p$. Then

$$\mathrm{Tr}_H^G \left(\frac{b_J \mathsf{N}_J^H}{U} \mathsf{N}_n^G\right) = \mathsf{N}_n^G \mathrm{Tr}_H^G \left(\frac{b_J \mathsf{N}_J^H}{U}\right)$$

can be written in terms of G-invariants of strictly smaller degree. On the other hand $\mathrm{LM}\left(b_J \mathsf{N}_J^H - \frac{b_J \mathsf{N}_J^H}{U} \mathsf{N}_n^G\right) < \mathrm{LM}\left(b_J \mathsf{N}_J^H\right)$. Therefore

$$\mathrm{Tr}_H^G\left(b_J \mathsf{N}_J^H\right) = \mathrm{Tr}_H^G \left(b_J \mathsf{N}_J^H - \frac{b_J \mathsf{N}_J^H}{U} \mathsf{N}_n^G\right) + \mathrm{Tr}_H^G \left(\frac{b_J \mathsf{N}_J^H}{U} \mathsf{N}_n^G\right)$$

yields that $\mathrm{Tr}_H^G\left(b_J \mathsf{N}_J^H\right)$ can be eliminated from a generating set for $\mathrm{Im}\mathrm{Tr}_H^G$.

Similarly, we claim that the degree of the $b_J \mathsf{N}_J^H$'s as a monomial in $\{\mathsf{N}_i^H | i = d, \ldots, n-1\}$ is strictly less than $p-1$. Assume the contrary and let $U_j \in \{\mathsf{N}_i^H | i = d, \ldots, n-1\}$ for $1 \le j \le p-1$. Set $U = \prod_{1 \le j \le p-1} U_j$. Then we have

$$\mathrm{Tr}_H^G\left(\frac{b_J \mathsf{N}_J^H}{U} \mathsf{T}_2(U_1 \cdots U_{p-1})\right) = \mathrm{Tr}_H^G\left(\frac{b_J \mathsf{N}_J^H}{U} \sum_{S \subseteq \{1,\ldots,p-1\}} (-1)^{|S|} X_{S'} \mathrm{Tr}_H^G(X_S)\right)$$
$$= \sum_{S \subseteq \{1,\ldots,p-1\}} \mathrm{Tr}_H^G(X_S) \mathrm{Tr}_H^G\left(\frac{b_J \mathsf{N}_J^H}{U} (-1)^{|S|} X_{S'}\right).$$

Hence, $\mathrm{Tr}_H^G\big(\frac{b_J \mathsf{N}_J^H}{U} \mathsf{T}_2\big(U_1 \cdots U_{p-1}\big)\big)$ can be written in terms of G-invariants of smaller degree. By Proposition 2 we have that $\mathrm{LM}\left(b_J \mathsf{N}_J^H - \frac{b_J \mathsf{N}_J^H}{U} \mathsf{T}_2\big(U_1 \cdots U_{p-1}\big)\right) < \mathrm{LM}\left(b_J \mathsf{N}_J^H\right)$. Therefore the equation

$$\mathrm{Tr}_H^G\big(b_J \mathsf{N}_J^H\big) = \mathrm{Tr}_H^G\left(b_J \mathsf{N}_J^H - \frac{b_J \mathsf{N}_J^H}{U} \mathsf{T}_2\left(U_1 \cdots U_{p-1}\right)\right)$$
$$+ \mathrm{Tr}_H^G\left(\frac{b_J \mathsf{N}_J^H}{U} \mathsf{T}_2\left(U_1 \cdots U_{p-1}\right)\right)$$

yields that $\mathrm{Tr}_H^G\big(b_J \mathsf{N}_J^H\big)$ can be eliminated from a generating set for $\mathrm{Im}\mathrm{Tr}_H^G$.

Thus, for any multi-index J, the degree (in the x's) of $b_J \mathsf{N}_J^H$ is bunded above by

$$p^2 - n + (p-2)p + p(p-1) = 3p^2 - 3p - n < 3p^2 - 3p$$

as claimed. □

Theorem 7 *Let V_n be an indecomposable G-module. Let $n = tp + r > p$, where $1 \le t \le p$ and $0 \le r < p$ are integers. Then*

$$\beta(V_n) \le \max\{3p^2 + (2t-4)p - 3t, 3p^2 - 3p\}.$$

Proof By the periodicity result of Theorem 1.2 in [14], $\mathbb{F}[V_n]$ is modulo the $\mathbb{F}H$-projective submodules generated by $\mathsf{N}_n^G = \prod_{\sigma \in G} \sigma x_n$ and invariants of degree less than p^2. Thus $\mathbb{F}[V_n]^G$ is generated by the G-norm N_n^G, invariants of degree less than p^2 and image $\mathrm{Im}\mathrm{Tr}_H^G$ of the relative transfer, since the fixed pointed of projective modules are in the image of the relative transfer.

By the previous lemma $\mathrm{Im}\mathrm{Tr}_H^G$ is generated by invariants of degree at most $3p^2 - 3p$ together with $\mathrm{Im}\mathrm{Tr}^G$. Therefore it follows from Corollary 4 that

$$\beta(V_n) \le \max\{3p^2 + (2t-4)p - 3t, 3p^2 - 3p\},$$

as desired. □

Remark 8 We note that for $n \leq p$ the representation

$$\rho : G \longrightarrow \mathsf{GL}(n, \mathbb{F})$$

has kernel $\mathbb{Z}_p$. Thus $\mathbb{F}[V]^G \cong \mathbb{F}[V]^H$. Hence this ring of invariants is generated by forms of degree at most $2p - 3$ by [5].

Remark 9 Furthermore, if $n = p + 1$ we find in [13] an explicit generating set of the ring of invariants and we read off

$$\beta(\mathbb{F}[V_{p+1}]^G) \leq 2p^2 - 2p - 1.$$

For $p = 3$ the authors of [13] refer to a Magma calculation and for $\beta(\mathbb{F}[V_4]^G) = 9$. For $p = 2$ we find $\beta(\mathbb{F}[V_3]^G) = 4$ by [9]. We note that

$$p^2 \leq 2p^2 - 2p - 1 \leq 3p^2 - 3p \leq \max\{3p^2 + (2t - 4)p - 3t, 3p^2 - 3p\}.$$

Note carefully that the degree bound given above is polynomial in p of degree 2. We thus state the following problem.

Conjecture 10 Let V be an indecomposable $\mathbb{Z}_{p^r}$-module. Then $\beta\big(\mathbb{F}[V]^{\mathbb{Z}_{p^r}}\big)$ is bounded above by a polynomial in p of degree r.

3 The leading terms of $\mathsf{T}_1(\mathbf{m})$ and $\mathsf{T}_2(\mathbf{M})$

In this section we want to identify the leading terms of the polynomials $\mathsf{T}_1(\mathbf{m})$ and $\mathsf{T}_2(\mathbf{M})$ as described in Propositions 1 and 2. We start by identifying the coefficients of monomials that appear in $\mathsf{T}_1(\mathbf{m})$.

Lemma 11 *The coefficients of* $\mathsf{T}_1(\mathbf{m}) = \sum_{\alpha \in \mathbb{N}^{2p-2}} c_\alpha w_\alpha$ *are given by*

$$c_\alpha = \sum_{0 \leq l \leq p^2 - 1} \prod_{i=1}^{2p-2} \binom{l}{\alpha(i)}.$$

Proof Since σ^l is an algebra automorphism we have that

$$\prod_{i=1}^{2p-2} (w_{i,0} - \sigma^l(w_{i,0})) = \sum_{S \subseteq \{1,\ldots,2p-2\}} (-1)^{|S|} X_{S'} \sigma^l(X_S). \qquad (✠)$$

Thus summing over $0 \leq l \leq p^2 - 1$ yields

$$\mathsf{T}_1(\mathbf{m}) = \sum_{0 \leq l \leq p^2 - 1} \prod_{i=1}^{2p-2} (w_{i,0} - \sigma^l(w_{i,0})).$$

Since we have[1]

$$(w_{i,0} - \sigma^l(w_{i,0})) = -lw_{i,1} - \binom{l}{2}w_{i,2} - \binom{l}{3}w_{i,3} - \cdots - \binom{l}{l}w_{i,l},$$

the desired equality follows. □

Lemma 12 *Let $\alpha \in \mathbb{N}^{2p-2}$. If $\alpha(i) > 1$ for some $1 \leq i \leq p-1$, then $w_\alpha < w_{\alpha'} = \mathbf{m}$.*

Proof Since $u_1 \leq u_2 \leq \cdots \leq u_{2p-2}$, it suffices to show that

$$\prod_{i=1}^{k} w_{i,\alpha(i)} < u_1 u_2 \ldots u_k$$

for some $1 \leq k \leq 2p-2$. Let j denote the smallest integer such that $\alpha(j) > 1$. Since $j \leq p-1$, it follows that $u_i = w_{i,1}$ for $i < j$ and $w_{j,\alpha(j)} < u_j$. Therefore $\prod_{i=1}^{j} w_{i,\alpha(i)} < u_1 u_2 \ldots u_j$ and the result follows. □

Lemma 13 *Let $\alpha \in \mathbb{N}^{2p-2}$. If $\alpha(i) \geq 2p$ for some $1 \leq i \leq 2p-2$, then $w_\alpha < w_{\alpha'} = \mathbf{m}$.*

Proof By Lemma 12 it is enough to show the result for $i \geq p$. Since $u_i = w_{i,p} \in \mathbb{F}[x_{r-p+1}, \ldots, x_r]$, it follows that $w_{i,\alpha(i)} \in \mathbb{F}[x_1, \ldots, x_{r-p}]$. Therefore w_α contains a variable that is smaller than all variables that appear in $\mathbf{m}$. □

Lemma 14 *Let α, β be two elements in $\mathbb{N}^{2p-2}$ such that $\alpha(i) \geq \beta(i)$ for $1 \leq i \leq 2p-2$. Then*

(1) *$w_\alpha \leq w_\beta$, and*
(2) *$w_\alpha = w_\beta$ if and only if $\alpha = \beta$.*

Proof Since $w_{i,\alpha(i)} \leq w_{i,\beta(i)}$ for $1 \leq i \leq 2p-2$, we have

$$w_\alpha = \prod_{i=1}^{2p-2} w_{i,\alpha(i)} \leq \prod_{i=1}^{2p-2} w_{i,\beta(i)} = w_\beta.$$

[1] This equation can be easily verified by induction on $l \geq 0$. If $l = 0$ the equation is trivial. For $l = 1$ we have

$$w_{i,0} - \sigma w_{i,0} = \Delta w_{i,0} = w_{i,1}.$$

Assume that $l > 1$. Then by induction we obtain

$$\begin{aligned} w_{i,0} - \sigma^l w_{i,0} &= (w_{i,0} - \sigma^{l-1} w_{i,0}) - \sigma^{l-1}\Delta w_{i,0} \\ &= -(l-1)w_{i,1} - \binom{l-1}{2}w_{i,2} - \cdots - \binom{l-1}{l-1}w_{i,l-1} - \sigma^{l-1}w_{i,1} \\ &= -(l-1)w_{i,1} - \binom{l-1}{2}w_{i,2} - \cdots - \binom{l-1}{l-1}w_{i,l-1} - w_{i,1} - \binom{l-1}{1}w_{i,2} - \cdots - \binom{l-1}{l-1}w_{i,l} \\ &= -lw_{i,1} - \binom{l}{2}w_{i,2} - \binom{l}{3}w_{i,3} - \cdots - \binom{l}{l}w_{i,l} \end{aligned}$$

as desired.

For the second assertion observe that if $\alpha(i) < \beta(i)$ for some $1 \leq i \leq 2p-2$, then $w_{i,\alpha(i)} < w_{i,\beta(i)}$. Hence

$$w_\alpha = \prod_{i=1}^{2p-2} w_{i,\alpha(i)} < \prod_{i=1}^{2p-2} w_{i,\beta(i)} = w_\beta$$

as desired. □

Lemma 15 *The coefficient of $c_{\alpha'}$ of the monomial $w_{\alpha'}$ in $\mathsf{T}_1(\mathbf{m})$ is* 1.

Proof By Lemma 11, we have $c_{\alpha'} = \sum_{0\leq l\leq p^2-1} l^{p-1}\binom{l}{p}^{p-1}$. For $0 \leq l \leq p^2-1$, write $l = l_1 p + l_2$, where $0 \leq l_1, l_2 < p$. Then we find

$$\begin{aligned}\sum_{0\leq l\leq p^2-1} l^{p-1}\binom{l}{p}^{p-1} &= \sum_{0\leq l_1,l_2\leq p-1} (l_1 p + l_2)^{p-1}\binom{l_1 p + l_2}{p}^{p-1}\\ &\overset{(1)}{\equiv} \sum_{0\leq l_1,l_2\leq p-1} l_2^{p-1} l_1^{p-1} \mod p\\ &\overset{(2)}{\equiv} 1 \mod p,\end{aligned}$$

where (1) follows from

$$\binom{s}{t} \equiv \binom{a_1}{a_2}\binom{b_1}{b_2} \mod p \qquad (\star)$$

(for any two integers $0 \leq s, t < p^2$ with $s = a_1 p + b_1$ and $t = a_2 p + b_2$, where $0 \leq a_i, b_i < p$), see [3], and (2) from

$$\sum_{0\leq l\leq p-1} l^c \equiv \begin{cases} -1 \mod p & \text{if } p-1 \mid c;\\ 0 \mod p & \text{otherwise,}\end{cases} \qquad (\bullet)$$

(for any natural number c), see [6, Theorem 119]. □

We are now able to prove Proposition 1:

Proposition 16 *The leading term of $\mathsf{T}_1(\mathbf{m})$ is $w_{\alpha'}$, and thus $\mathrm{LM}(\mathsf{T}_1(\mathbf{m})) = \mathbf{m} = w_{\alpha'}$.*

Proof The second statement follows from the first because $c_{\alpha'} = 1$ by Lemma 15. We proceed by showing that $w_{\alpha'} \leq w_\alpha$ and $c_\alpha \neq 0$ implies $\alpha = \alpha'$.

By Lemmas 12 and 13 we may assume $\alpha(i) = 1$ for $1 \leq i \leq p-1$ and $\alpha(i) < 2p$ for $p \leq i \leq 2p-2$. From Lemma 11 we have

$$c_\alpha = \sum_{0\leq l\leq p^2-1} \prod_{i=1}^{2p-2} \binom{l}{\alpha(i)} = \sum_{0\leq l\leq p^2-1} l^{p-1} \prod_{i=p}^{2p-2} \binom{l}{\alpha(i)}.$$

For $p \le i \le 2p-2$ write $\alpha(i) = a_i p + b_i$ with $0 \le b_i < p$ and $0 \le a_i \le 1$. Set $l = l_1 p + l_2$ with $0 \le l_1, l_2 < p$.

$$
\begin{aligned}
c_\alpha &= \sum_{0 \le l_1, l_2 \le p-1} (l_1 p + l_2)^{p-1} \prod_{i=p}^{2p-2} \binom{l_1 p + l_2}{a_i p + b_i} \\
&\equiv \sum_{0 \le l_1, l_2 \le p-1} l_2^{p-1} \prod_{i=p}^{2p-2} \binom{l_1}{a_i}\binom{l_2}{b_i} \\
&\equiv \begin{cases} \sum_{0 \le l_1, l_2 \le p-1} l_2^{p-1} l_1^{p-2} \prod_{i=p}^{2p-2} \binom{l_2}{b_i} & \text{if } a_i = 1 \text{ for all } i, \\ \sum_{0 \le l_2 \le p-1} \left(l_2^{p-1} \prod_{i=p}^{2p-2} \binom{l_2}{b_i} \left(\sum_{0 \le l_1 \le p-1} l_1^k \right)\right) \equiv 0 & \text{otherwise,} \end{cases}
\end{aligned}
$$

where the last equation follows since k an integer not divisible by $p-1$. Thus we may assume that $a_i = 1$ for $p \le i \le 2p-2$. It follows that $\alpha(i) = p + b_i \ge p = \alpha'(i)$ for $p \le i \le 2p-2$. Moreover $\alpha(i) = \alpha'(i) = 1$ for $1 \le i \le p-1$. Now $\alpha = \alpha'$ follows from Lemma 14. □

From this Proposition 2 can be easily derived, cf. [5, Lemmas 3.2, 3.3].

Proposition 17 *The leading monomial of* $\mathsf{T}_2(\mathbf{M})$ *is the leading monomial of* $\mathbf{M}$.

Proof Let $\mathbf{M} = U_1 \cdots U_{p-1}$ for $U_j \in \{\mathsf{N}_d^H, \ldots, \mathsf{N}_{n-1}^H\}$. Recall from Eq. (✠) that

$$
\prod_{j=1}^{p-1} (W_j - \sigma^l(W_j)) = \sum_{S \subseteq \{1,\ldots,p-1\}} (-1)^{|S|} X_{S'} \sigma^l(X_S).
$$

Summing over $0 \le l \le p-1$ yields

$$
\sum_{0 \le l \le p-1} \prod_{j=1}^{p-1} (W_j - \sigma^l(W_j)) = \sum_{S \subseteq \{1,\ldots,p-1\}} (-1)^{|S|} X_{S'} \mathrm{Tr}_H^G(X_S).
$$

The leading term of $(W_j - \sigma^l(W_j))$ is $-l \cdot \mathrm{LM}(U_j)$. Thus the leading term of $\prod_{j=1}^{p-1}(W_j - \sigma^l(W_j))$ is $(-l)^{p-1} \cdot \mathrm{LM}(U_1 \cdots U_{p-1})$. Hence the result follows from Eq. (•). □

Acknowledgment Müfit Sezer wishes to thank Jim Shank for bringing [4, Theorem 3.3] to his attention.

References

1. Alperin, J.L.: Local Representation Theory, Cambridge Studies in Advanced Mathmatics 11. Cambridge University Press, Cambridge (1986)
2. Eisenbud, D.: Commutative Algebra with a View Toward Algebraic Geometry. Graduate Texts in Mathematics 150. Springer, New York (1995)
3. Fine, N.J.: Binomial coefficients modulo a prime. Am. Math. Monthly **54**, 589–592 (1947)

4. Fleischmann, P., Kemper, G., Shank, R.J.: On the depth of cohomology modules. Q. J. Math. **55**(2), 167–184 (2004)
5. Fleischmann, P., Sezer, M., Shank, R.J., Woodcock, C.F.: The Noether numbers for cyclic groups of prime order. Adv. Math. **207**, 149–155 (2006)
6. Hardy, G.H., Wright, E.M.: An Introduction to the Theory of Numbers, 5th edn. Oxford Science Publications, Oxford University Press, Oxford (1979)
7. Hughes, I., Kemper, G.: Symmetric power of modular representations, Hilbert series and degree bounds. Commun. Algebra **28**, 2059–2089 (2000)
8. Neusel, M.D.: The transfer in the invariant theory of modular permutation representations. Pac. J. Math. **199**, 121–136 (2001)
9. Neusel, M.D.: Invariants of some Abelian p-groups in characteristic p. Proc. AMS **125**, 1921–1931 (1997)
10. Neusel, M.D.: Degree bounds. An invitation to postmodern invariant theory. Topol. Appl. **154**, 792–814 (2007)
11. Neusel, M.D., Smith, L.: Invariant theory of finite groups, Math. Surv. Monogr., vol. 94, Am. Math. Soc., Providence, RI (2002)
12. Richman, D.: Invariants of finite groups over fields of characteristic p. Adv. Math. **124**, 25–48 (1996)
13. Shank, R.J., Wehlau, D.L.: Decomposing symmetric powers of certain modular representations of cyclic groups. IMS Technical Report UKC/IMS/05/13. http://www.kent.ac.uk/IMS/personal/rjs/
14. Symonds, P.: Cyclic group actions on polynomial rings. Bull. Lond. Math. Soc. **39**, 181–188 (2007)