EXPLICIT SEPARATING INVARIANTS FOR CYCLIC P-GROUPS

MÜFİT SEZER

Abstract. We consider a finite dimensional indecomposable modular representation of a cyclic p-group and we give a recursive description of an associated separating set: We show that a separating set for a representation can be obtained by adding to a separating set for any subrepresentation some explicitly defined invariant polynomials. Meanwhile, an explicit generating set for the invariant ring is known only in a handful of cases for these representations.

INTRODUCTION

Let V denote a finite dimensional representation of a group G over a field F. The induced action on the dual space V^* extends to the symmetric algebra $S(V^*)$. This is a polynomial algebra in a basis of V^* and we denote it by $F[V]$. The action of $\sigma \in G$ on $f \in F[V]$ is given by $(\sigma f)(v) = f(\sigma^{-1}v)$ for $v \in V$. The subalgebra in $F[V]$ of polynomials that are left fixed under the action of the group is denoted by $F[V]^G$. A classical problem is to determine the invariant ring $F[V]^G$ for a given representation. This is, in general a difficult problem because the invariant ring becomes messier if one moves away from the groups generated by reflections and the degrees of the generators often get very big. A subset $A \subseteq F[V]^G$ is said to be separating for V if for any pair of vectors $u, w \in V$, we have: If $f(u) = f(w)$ for all $f \in A$, then $f(u) = f(w)$ for all $f \in F[V]^G$. Separating invariants have been a recent trend in invariant theory as a better behaved weakening of generating invariants. Although distinguishing between the orbits with invariants has been an object of study since the beginning of invariant theory, there has been a recent resurgence of interest in them which is initiated by Derksen and Kemper [6]. Since then, there have been several papers with the theme that one can get separating subalgebras with better constructive properties which make them easier to obtain than the full invariant ring. For instance there is always a finite separating set [6, 2.3.15.] and Noether's bound holds for separating invariants independently of the characteristic of the field [6, 3.9.14.]. Separating invariants also satisfy important efficiency properties in decomposable representations, see [8], [9] and [10]. Obtaining a generating set for the invariant ring is particularly difficult in the modular case, i.e., when the order of the group is divisible by the characteristic of the field. Even in the simplest situation of a representation of a cyclic group of prime order p over a field of characteristic p, an explicit generating set is known only in very limited cases. On the other hand a separating set is constructed for every such representation in [22]. We will tell more about modular representations shortly.

Date: December 7, 2009, 13 h 13 min.
2000 *Mathematics Subject Classification.* 13A50, 14L24.
Research supported by a grant from Tübitak: 109T384 .

There has been also some interest in the question whether one can have better ring theoretical properties by passing to a separating subalgebra. In [12] it is shown that there may exist a regular (resp. complete intersection) separating subalgebra where the invariant ring is not regular (resp. complete intersection). But some recent results [11] and [14] suggest that, in general, separating subalgebras do not provide substantial improvements in terms of the Cohen-Macaulay defect.

We recommend [6, 2.3.2, 3.9.4] and [17] for more background and motivation on separating invariants. The textbooks [1], [6] and [20] are good sources as general references in invariant theory.

In this paper we study separating invariants for representations of a cyclic p-group $\boldsymbol{Z}_{p^r}$ over a field of characteristic p. Although these representations are easy to describe the corresponding invariant ring is difficult to obtain. A major difficulty is that, as shown by Richman [21], the degrees of the generators increase unboundedly as the dimension of the representation increases. Actually for $r = 1$, the maximal degree of a polynomial in a minimal generating set for the invariant ring of any representation is known, see [16]. Nevertheless explicit generating sets are available only for handful of cases. The invariants of the two and the three dimensional indecomposable representations of $\boldsymbol{Z}_p$ were computed by Dickson [7] at the beginning of the twentieth century. After a long period without progress Shank [23] obtained the invariants of the four and the five dimensional indecomposable representations using difficult computations that involved S.A.G.B.I. bases. Finding generating invariants for higher dimensional indecomposable representations remain open. As for decomposable representations, the invariants for copies of the two dimensional indecomposable representation were computed by Campbell and Hughes [3], see also [5]. The adoption of S.A.G.B.I. bases method that was introduced by Shank also helped to resolve a couple of special cases where each indecomposable summand has dimension at most three, see [2], [13] and [25]. For $r = 2$ much less is known: Shank and Wehlau gave a generating set for the invariants of the $p + 1$ dimensional indecomposable representation [24]. Also in [19], a bound for the degrees of generators that apply to all indecomposable representations of $\boldsymbol{Z}_{p^2}$ was obtained. As a polynomial in p, this bound is of degree two and together with the bounds for $\boldsymbol{Z}_p$ it gives support for a general conjecture on the degrees of the generators of modular invariants of $\boldsymbol{Z}_{p^r}$, see [19]. Meanwhile, for $r > 2$, to the best of our information, no explicit description of a generating set exists for the invariants of any faithful representation.

Despite these complications concerning the modular generating invariants, separating invariants have been revealed to be remarkably better behaved. In [18] a separating set is constructed using only transfers and norms for any modular representation of any p-group. These are invariant polynomials that are obtained by taking orbit sums and orbit products. They are easy to obtain and it is known that they do not suffice to generate the invariant ring even when the group is cyclic. Unfortunately the size of the set in [18] is infinite. In [22] the focus is restricted to representations of $\boldsymbol{Z}_p$ and more explicit results are obtained. More precisely, it is shown that a separating set for a representation can be obtained by adding, to a separating set of a certain subrepresentation, some explicitly described invariant polynomials. This result is special to separating invariants and express their distinction from generating invariants in several directions. First of all, knowing the invariants of subrepresentations is not critically useful in building up a generating

set for higher dimensional representations. Practically, it is equally difficult to get a generating set for the invariants of a representation even when one is supplied with the invariants of its subrepresentations. Also the construction in [22] yields a separating set for any representation that consists of polynomials of degree one or p and the size of this set depends only on the dimension of the representation. On the other hand, the size of a generating set depends also on the order of the group and the degrees of the generators are somewhat randomly distributed. Moreover, each polynomial in this separating set depends on variables from at most two indecomposable summands in the representation, whereas a minimal generating set must contain a polynomial that involves a variable from every non-trivial indecomposable summand, see [16].

The purpose of this paper is to generalize the construction in [22] to all modular indecomposable representations of an arbitrary cyclic p-group. Since the dual of a subrepresentation still sits in the duals of higher dimensional representations for cyclic p-groups (we will be more precise about this in the next section), the strategy of building on separating sets for subresentations carry over to this generality. This allows us to reduce to the case of separating two vectors whose coordinates are all the same except the coordinate corresponding to the fixed point space. In the upper triangular basis this is the first coordinate. Then we split the pairs according to the length of the tails of zeros in their coordinates. It turns out that, for an integer $j \geq 1$, all pairs of vectors (in different orbits) whose j-th coordinates are non-zero and higher coordinates are zero can be separated by the same polynomial. While this polynomial is simply a transfer of a single monomial of degree p in the $\boldsymbol{Z}_p$ case for $j > 2$, one needs to take a large relative transfer of a certain product of norms with respect the right subgroup in the general treatment. The choice of the subgroup depends on the modulo p expansion of j. Since we are using this polynomial to separate vectors that have a tail of zeros of the same length , we compute this polynomial modulo the vanishing ideal of the vector space corresponding to the tail. This is the most difficult part of the proof. If the third and higher coordinates are all zero in this pair, then the norm of the linear form corresponding to the first coordinate separates the pair. Hence we obtain a set of invariants that connect separating sets of two indecomposable representations of consecutive dimensions. By induction this yields an explicit (finite) separating set for all indecomposable representations. This set has nice constructive features as in the case of $\boldsymbol{Z}_p$. From the construction it can be read off that the size of the separating set depends only on the dimension of the representation. Moreover, the maximal degree of a polynomial in this set is the group order p^r and there are $p^{r-1} + 1$ possibilities for the degree of a polynomial in this set.

Constructing separating invariants

Let $p > 0$ be a prime number and F be a field of characteristic p. Let G denote the cyclic group of order p^r, where r is a non-negative integer. We fix a generator σ of G. It is well known that there are exactly p^r indecomposable representations $V_1, V_2, \ldots, V_{p^r}$ of G up to isomorphism where σ acts on V_n for $1 \leq n \leq p^r$ by a Jordan block of dimension n with ones on the diagonal. Let $e_1, e_2, \ldots, e_n$ be the Jordan block basis for V_n with $\sigma(e_i) = e_i + e_{i-1}$ for $2 \leq i \leq n$ and $\sigma(e_1) = e_1$. We identify each e_i with the column vector with 1 on the i-th coordinate and zero elsewhere. Let $x_1, x_2, \ldots, x_n$ denote the corresponding elements in the dual space

V_n^*. Since V_n^* is indecomposable it is isomorphic to V_n. In fact, $x_1, x_2, \dots, x_n$ forms a Jordan block basis for V_n^* in the reverse order: We have $\sigma^{-1}(x_i) = x_i + x_{i+1}$ for $1 \leq i \leq n-1$ and $\sigma^{-1}(x_n) = x_n$. Since σ^{-1} generates G as well, we write σ for σ^{-1} for the rest of the paper. Note also that $F[V_n] = F[x_1, x_2, \dots, x_n]$. Pick a column vector $(c_1, c_2, \dots, c_n)^t$ in V_n, where $c_i \in F$ for $1 \leq i \leq n$. There is a G-equivariant surjection $V_n \to V_{n-1}$ given by $(c_1, c_2, \dots, c_n)^t \to (c_2, c_3 \dots, c_n)^t$. We use the convention that V_0 is the zero representation. Dual to this surjection, the subspace in V_n^* generated by $x_2, x_3, \dots, x_n$ is closed under the G-action and is isomorphic to V_{n-1}^*. Hence $F[V_{n-1}] = F[x_2, x_3, \dots, x_n]$ is a subalgebra in $F[V_n]$. For $0 \leq m \leq r$, let G_m denote the subgroup of G of order p^m which is generated by $\sigma^{p^{r-m}}$. For $f \in F[V_n]$, define $N_{G_m}(f) = \prod_{0 \leq l \leq p^m - 1} \sigma^{lp^{r-m}}(f)$ and for simplicity we write $N_G(f)$ for $N_{G_r}(f)$. Also for $f \in F[V_n]^{G_m}$, define the relative transfer $\mathrm{Tr}^G_{G_m}(f) = \sum_{0 \leq l \leq p^{r-m}-1} \sigma^l(f)$. Notice that $N_{G_m}(f) \in F[V_n]^{G_m}$ and $\mathrm{Tr}^G_{G_m}(f) \in F[V_n]^G$. For a positive integer i, Let I_i denote the ideal in $F[V_n]$ generated by $x_i, x_{i+1}, \dots, x_n$ if $1 \leq i \leq n$ and let I_i denote the zero ideal if $i > n$. Since the vector space generated by $x_i, x_{i+1}, \dots, x_n$ is closed under the G-action, I_i is also closed under the G-action.

Let $3 \leq j \leq n$ be an integer with $p^{k-1} + 1 < j \leq p^k + 1$, where k is a positive integer. We define the polynomial

$$H(j) = \mathrm{Tr}^G_{G_{r-k}} \left((N_{G_{r-k}}(x_1)) \prod_{0 \leq i \leq k-1} (N_{G_{r-k}}(x_{j-p^i}))^{p-1} \right).$$

It turns out that this polynomial is the right generalization of the polynomial in [22, Lemma 2] for our purposes. Our main task before the proof of the main theorem is to compute this polynomial modulo the ideal I_{j+1}. We start with a couple of well known results.

Lemma 1. *i) Let a be a positive integer. Then $\sum_{0 \leq l \leq p-1} l^a \equiv -1 \mod p$ if $p-1$ divides a and $\sum_{0 \leq l \leq p-1} l^a \equiv 0 \mod p$, otherwise.*

ii) Let s, t be integers with modulo p expansions $t = a_m p^m + a_{m-1} p^{m-1} + \cdots + a_0$ and $s = b_m p^m + b_{m-1} p^{m-1} + \cdots + b_0$, where $0 \leq a_i, b_i \leq p-1$ for $1 \leq i \leq m$. Then $\binom{t}{s} \equiv \prod_{0 \leq i \leq m} \binom{a_i}{b_i} \mod p$.

Proof. We direct the reader to [4, 9.4] for a proof of the first statement and to [15] for a proof of the second statement. □

From now on all equivalences are modulo I_{j+1} unless otherwise stated.

Lemma 2. *We have the following equivalences.*

i) $N_{G_{r-k}}(x_{j-p^i}) \equiv x_{j-p^i}^{p^{r-k}}$ *for* $0 \leq i \leq k-1$.

ii) $N_{G_{r-k}}(x_1) \equiv \begin{cases} x_1^{p^{r-k}} \text{ if } j \neq p^k + 1 \\ x_1^{p^{r-k}} - x_1^{p^{r-k-1}} x_{1+p^k}^{(p-1)p^{r-k-1}} \text{ if } j = p^k + 1. \end{cases}$

Proof. Let $1 \leq m \leq n$ be an integer. We first claim that $N_{G_{r-k}}(x_m) \equiv x_m^{p^{r-k}} \mod I_{m+p^k}$. Since $\sigma^{p^k}(x_m) = x_m + p^k x_{m+1} + \binom{p^k}{2} x_{m+2} \cdots$, by the previous lemma we have $\sigma^{p^k}(x_m) = x_m + x_{m+p^k}$. Therefore for $0 \leq l \leq p^{r-k} - 1$, we get $\sigma^{lp^k}(x_m) = x_m + l x_{m+p^k} + \binom{l}{2} x_{m+2p^k} + \cdots \equiv x_m \mod I_{m+p^k}$. Since $N_{G_{r-k}}(x_m) = \prod_{0 \leq l \leq p^{r-k}-1} \sigma^{lp^k}(x_m)$, we obtain the claim.

From the claim we have $N_{G_{r-k}}(x_{j-p^i}) \equiv x_{j-p^i}^{p^{r-k}} \mod I_{j-p^i+p^k}$. But since $I_{j-p^i+p^k}$ is contained in I_{j+1}, the first statement of the lemma follows. Similarly, if $j \neq p^k+1$, then $N_{G_{r-k}}(x_1) \equiv x_1^{p^{r-k}}$ because I_{p^k+1} is contained in I_{j+1}. On the other hand, if $j = p^k+1$, then $\sigma^{lp^k}(x_1) = x_1 + lx_{1+p^k} + \binom{l}{2}x_{1+2p^k} + \cdots \equiv x_1 + lx_{1+p^k}$ and therefore $N_{G_{r-k}}(x_1) \equiv \prod_{0\leq l\leq p^{r-k}-1}(x_1+lx_{1+p^k})$. Furthermore, $\prod_{0\leq l\leq p^{r-k}-1}(x_1+lx_{1+p^k}) \equiv (\prod_{0\leq l\leq p-1}(x_1+lx_{1+p^k}))^{p^{r-k-1}}$. But it is well known that $\prod_{0\leq l\leq p-1}(x_1+lx_{1+p^k}) = x_1^p - x_1x_{1+p^k}^{p-1}$, see for instance [7]. It follows that $N_{G_{r-k}}(x_1) \equiv x_1^{p^{r-k}} - x_1^{p^{r-k-1}}x_{1+p^k}^{(p-1)p^{r-k-1}}$. □

For simplicity we put $X = (\prod_{0\leq i\leq k-1}(N_{G_{r-k}}(x_{j-p^i}))^{p-1})$.

Lemma 3. *There exists $f \in F[x_2, x_3, \ldots, x_n]$ such that*

$$H(j) \equiv N_{G_{r-k}}(x_1)\,\mathrm{Tr}^G_{G_{r-k}}(X) + f.$$

Proof. We claim that for $0 \leq l \leq p^k-1$ there exists $g_l \in F[x_2, x_3, \ldots, x_n]$ such that $\sigma^l(N_{G_{r-k}}(x_1)) \equiv N_{G_{r-k}}(x_1) + g_l$. First assume that $j \neq p^k+1$. Then by the previous lemma we have $N_{G_{r-k}}(x_1) \equiv x_1^{p^{r-k}}$. Since this equivalence is preserved under the action of the group we get

$$\begin{aligned}\sigma^l(N_{G_{r-k}}(x_1)) &\equiv x_1^{p^{r-k}} + (lx_2)^{p^{r-k}} + \Big(\binom{l}{2}x_3\Big)^{p^{r-k}} + \cdots \\ &= x_1^{p^{r-k}} + lx_2^{p^{r-k}} + \binom{l}{2}x_3^{p^{r-k}} + \cdots.\end{aligned}$$

Hence we can choose $g_l = lx_2^{p^{r-k}} + \binom{l}{2}x_3^{p^{r-k}} + \cdots$. Next assume that $j = p^k+1$. By the previous lemma again, we have $N_{G_{r-k}}(x_1) \equiv x_1^{p^{r-k}} - x_1^{p^{r-k-1}}x_{1+p^k}^{(p-1)p^{r-k-1}}$. Similarly we get

$$\sigma^l(N_{G_{r-k}}(x_1)) \equiv (x_1^{p^{r-k}} + lx_2^{p^{r-k}} + \cdots) - (x_1^{p^{r-k-1}} + lx_2^{p^{r-k-1}} + \cdots)x_{1+p^k}^{(p-1)p^{r-k-1}},$$

where we used $\sigma^l(x_{1+p^k}^{(p-1)p^{r-k-1}}) \equiv x_{1+p^k}^{(p-1)p^{r-k-1}}$. Therefore we can choose $g_l = (lx_2^{p^{r-k}} + \binom{l}{2}x_3^{p^{r-k}} + \cdots) - (lx_2^{p^{r-k-1}} + \binom{l}{2}x_3^{p^{r-k-1}} + \cdots)(x_{1+p^k}^{(p-1)p^{r-k-1}})$. This establishes the claim. It follows that

$$\begin{aligned}H(j) &= \sum_{0\leq l\leq p^k-1}\sigma^l(N_{G_{r-k}}(x_1)X) = \sum_{0\leq l\leq p^k-1}\sigma^l(N_{G_{r-k}}(x_1))\sigma^l(X) \\ &\equiv \sum_{0\leq l\leq p^k-1}(N_{G_{r-k}}(x_1))\sigma^l(X) + \sum_{0\leq l\leq p^k-1}g_l\sigma^l(X) \\ &= N_{G_{r-k}}(x_1)\,\mathrm{Tr}^G_{G_{r-k}}(X) + \sum_{0\leq l\leq p^k-1}g_l\sigma^l(X).\end{aligned}$$

Notice that the smallest index of a variable in X is $j-p^{k-1}$ which is strictly bigger than one. So X lies in $F[x_2, x_3, \ldots, x_n]$ as well. Hence the result follows. □

We turn our attention to the polynomial $\mathrm{Tr}^G_{G_{r-k}}(X)$. By Lemma 2 we have

$$\mathrm{Tr}^G_{G_{r-k}}(X) \equiv \sum_{0\leq l\leq p^k-1}\sigma^l\Big(\prod_{0\leq i\leq k-1}(x_{j-p^i})^{p^{r-k}(p-1)}\Big).$$

We set

$$T = \sum_{0\leq l\leq p^k-1} \sigma^l\Big(\prod_{0\leq i\leq k-1} (x_{j-p^i})^{p^{r-k}(p-1)}\Big).$$

For $0 \leq m \leq k(p-1)-1$, write $m = a_m(p-1)+b_m$, where a_m, b_m are non-negative integers with $0 \leq b_m < p-1$. Define $w_{m,0} = (x_{j-p^{a_m}})^{p^{r-k}}$ and for an integer $t \geq 0$, set $w_{m,t} = (x_{j-p^{a_m}+t})^{p^{r-k}}$. Note that we have

$$\prod_{0\leq i\leq k-1} (x_{j-p^i})^{p^{r-k}(p-1)} = \prod_{0\leq m\leq k(p-1)-1} w_{m,0}.$$

For a $k(p-1)$-tuple $\alpha = [\alpha(0), \alpha(1), \ldots, \alpha(k(p-1)-1)] \in \mathbb{N}^{k(p-1)}$, define

$$w_\alpha = \prod_{0\leq m\leq k(p-1)-1} w_{m,\alpha(m)}.$$

Next lemma shows that T can be written as a linear combination of w_α's.

Lemma 4. *We have* $T = \sum_{w_\alpha \in \mathbb{N}^{k(p-1)}} c_\alpha w_\alpha$, *where*

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

Proof. We have

$$\begin{aligned}
T &= \sum_{0\leq l\leq p^k-1} \sigma^l\Big(\prod_{0\leq i\leq k-1} (x_{j-p^i})^{p^{r-k}(p-1)}\Big)\\
&= \sum_{0\leq l\leq p^k-1} \Big(\prod_{0\leq i\leq k-1} (\sigma^l(x_{j-p^i}))^{p^{r-k}(p-1)}\Big)\\
&= \sum_{0\leq l\leq p^k-1} \Big(\prod_{0\leq i\leq k-1} (x_{j-p^i} + lx_{j-p^i+1} + \binom{l}{2} x_{j-p^i+2} + \ldots)^{p^{r-k}(p-1)}\Big)\\
&= \sum_{0\leq l\leq p^k-1} \Big(\prod_{0\leq i\leq k-1} (x_{j-p^i}^{p^{r-k}} + lx_{j-p^i+1}^{p^{r-k}} + \binom{l}{2} x_{j-p^i+2}^{p^{r-k}} + \ldots)^{p-1}\Big)\\
&= \sum_{0\leq l\leq p^k-1} \Big(\prod_{0\leq m\leq k(p-1)-1} (w_{m,0} + lw_{m,1} + \binom{l}{2} w_{m,2} + \ldots)\Big).
\end{aligned}$$

Hence we get the result. □

Let α' denote the $k(p-1)$-tuple such that $\alpha'(m) = p^{a_m}$ for $0 \leq m \leq k(p-1)-1$. Notice that $w_{\alpha'} = x_j^{p^{r-k}k(p-1)}$. We show that T is in fact equivalent to a scalar multiple of this monomial modulo I_{j+1}.

Lemma 5. *We have* $c_{\alpha'} \neq 0$. *Moreover,* $T \equiv c_{\alpha'} w_{\alpha'}$.

Proof. Let $\alpha \in \mathbb{N}^{k(p-1)}$ with $w_\alpha \notin I_{j+1}$. We have $\alpha(m) - p^{a_m} \leq 0$ for all $0 \leq m \leq k(p-1)-1$, because otherwise $w_{m,\alpha(m)} = (x_{j-p^{a_m}+\alpha(m)})^{p^{r-k}} \in I_{j+1}$. But since $m \leq k(p-1)-1$, we have $a_m \leq k-1$ and therefore $\alpha(m) \leq p^{k-1}$ for all $0 \leq m \leq k(p-1)-1$. In particular it follows that the modulo p expansion of $\alpha(m)$ contains at most k digits. For $0 \leq m \leq k(p-1)-1$ and $0 \leq l \leq p^k-1$, let $\alpha(m) = \alpha(m)_{k-1}p^{k-1} + \alpha(m)_{k-2}p^{k-2} + \cdots + \alpha(m)_0$ and $l = l_{k-1}p^{k-1} + l_{k-2}p^{k-2} + \cdots l_0$

denote the modulo p-expansions of $\alpha(m)$ and l, respectively. From Lemma 1 and Lemma 4 we have

$$\begin{aligned} c_\alpha &= \sum_{0\le l\le p^k-1} \Big(\prod_{0\le m\le k(p-1)-1} \binom{l}{\alpha(m)} \Big) \\ &= \sum_{0\le l_t\le p-1,\ 0\le t\le k-1} \Big(\prod_{0\le m\le k(p-1)-1} \binom{l_{k-1}p^{k-1}+l_{k-2}p^{k-2}+\cdots}{\alpha(m)_{k-1}p^{k-1}+\alpha(m)_{k-2}p^{k-2}+\cdots} \Big) \\ &= \sum_{0\le l_t\le p-1,\ 0\le t\le k-1} \Big(\prod_{0\le m\le k(p-1)-1} \binom{l_{k-1}}{\alpha(m)_{k-1}}\binom{l_{k-2}}{\alpha(m)_{k-2}}\cdots\binom{l_0}{\alpha(m)_0} \Big). \end{aligned}$$

We compute $c_{\alpha'}$ from this identity as follows. Note that as m varies from 0 to $k(p-1)-1$, $\alpha'(m)$ takes on values $1, p, \ldots, p^{k-1}$ and that each value is taken precisely $p-1$ times. Therefore we get

$$\prod_{0\le m\le k(p-1)-1} \binom{l_{k-1}}{\alpha'(m)_{k-1}}\binom{l_{k-2}}{\alpha'(m)_{k-2}}\cdots\binom{l_0}{\alpha'(m)_0} = l_{k-1}^{p-1}l_{k-2}^{p-1}\cdots l_0^{p-1}.$$

Therefore $c_{\alpha'} = \sum_{0\le l_t\le p-1,\ 0\le t\le k-1} l_{k-1}^{p-1}l_{k-2}^{p-1}\cdots l_0^{p-1} = (-1)^k \neq 0$ by Lemma 1.

To prove the second statement assume that $c_\alpha \neq 0$ (and $w_\alpha \notin I_{j+1}$). We have already observed that $\alpha(m) \le p^{k-1}$ for all $0 \le m \le k(p-1)-1$. In fact, the inequality $\alpha(m) - p^{a_m} \le 0$ for $0 \le m \le k(p-1)-1$ tells us more: For $m \le (k-1)(p-1)-1$ we have $a_m \le k-2$ and therefore $\alpha(m) \le p^{k-2}$. Putting all this information together, we see that $\alpha(m)_{k-1} \le 1$ for $0 \le m \le k(p-1)-1$ and $\alpha(m)_{k-1} = 0$ for $0 \le m \le (k-1)(p-1)-1$. Now we arrange the terms in c_α to get

$$c_\alpha = A \cdot \sum_{0\le l_{k-1}\le p-1} \Big(\prod_{0\le m\le k(p-1)-1} \binom{l_{k-1}}{\alpha(m)_{k-1}} \Big),$$

where

$$A = \sum_{0\le l_t\le p-1,\ 0\le t\le k-2} \Big(\prod_{0\le m\le k(p-1)-1} \binom{l_{k-2}}{\alpha(m)_{k-2}}\cdots\binom{l_0}{\alpha(m)_0} \Big).$$

Since $\alpha(m)_{k-1} = 0$ for $0 \le m \le (k-1)(p-1)-1$, we have

$$c_\alpha = A \cdot \sum_{0\le l_{k-1}\le p-1} \Big(\prod_{(k-1)(p-1)\le m\le k(p-1)-1} \binom{l_{k-1}}{\alpha(m)_{k-1}} \Big).$$

On the other hand, since $\alpha(m)_{k-1}$ is at most one for $(k-1)(p-1) \le m \le k(p-1)-1$ we get

$$\prod_{(k-1)(p-1)\le m\le k(p-1)-1} \binom{l_{k-1}}{\alpha(m)_{k-1}} = \begin{cases} l_k^{p-1} \text{ if } \alpha(m)_{k-1} = 1 \text{ for } (k-1)(p-1) \le m \\ g \text{ otherwise,} \end{cases}$$

where g is a polynomial of degree strictly less than $p-1$ (as a polynomial in l_{k-1}). Since $c_\alpha \neq 0$, it follows from Lemma 1 that $\alpha(m)_{k-1} = 1$ for $(k-1)(p-1) \le m$. So $\alpha(m) = p^{a_m}$ for $(k-1)(p-1) \le m$ or equivalently $\alpha(m) = p^{k-1}$ for $(k-1)(p-1) \le m$. We determine the rest of the coordinates of α along the same way. From $c_\alpha \neq 0$ we have $A \neq 0$. Since $\alpha(m) = p^{k-1}$ for $(k-1)(p-1) \le m$ it follows that

$\alpha(m)_{k-2} = \alpha(m)_{k-3} = \cdots = \alpha(m)_0 = 0$ for $(k-1)(p-1) \leq m$, and therefore we get

$$A = \sum_{0 \leq l_t \leq p-1,\ 0 \leq t \leq k-2} \Big(\prod_{0 \leq m \leq (k-1)(p-1)-1} \binom{l_{k-2}}{\alpha(m)_{k-2}} \cdots \binom{l_0}{\alpha(m)_0} \Big).$$

The argument that was used to compute $\alpha(m)$ for $(k-1)(p-1) \leq m$ applies to $\alpha(m)$ for $(k-2)(p-1) \leq m \leq (k-1)(p-1)-1$ as well because from the condition $\alpha(m) - p^{a_m} \leq 0$ we get $\alpha(m) \leq p^{k-2}$ for $m \leq (k-1)(p-1)-1$ and $\alpha(m) \leq p^{k-3}$ for $m \leq (k-2)(p-1)-1$. Repeating this argument and losing l_t at each step for $0 \leq t \leq k-2$, one gets that $\alpha(m) = p^{a_m}$ for $0 \leq m \leq k(p-1)-1$. Hence $\alpha = \alpha'$ as desired. □

Lemma 6. *Let $v_1 = (a, b, 0, \ldots, 0)^t$ and $v_2 = (c, b, 0, \ldots, 0)^t$ be two vectors in V_n in different G-orbits. Then $N_G(x_1)$ separates v_1 and v_2.*

Proof. Note that $N_G(x_1)(v_1) = (\prod_{0 \leq l \leq p^r-1} \sigma^l(x_1))(v_1) = \prod_{0 \leq l \leq p^r-1} x_1(\sigma^l(v_1)) = \prod_{0 \leq l \leq p^r-1}(a + lb) = (\prod_{0 \leq l \leq p-1} a + lb)^{p^{r-1}}$. Similarly, we have $N_G(x_1)(v_2) = (\prod_{0 \leq l \leq p-1} c + lb)^{p^{r-1}}$. Since taking p-th powers is one to one in F, it suffices to show that $\prod_{0 \leq l \leq p-1}(a + lb) \neq \prod_{0 \leq l \leq p-1}(c + lb)$. Note that $a \neq c$ because $v_1 \neq v_2$. Therefore we may assume that $b \neq 0$, because otherwise $\prod_{0 \leq l \leq p-1}(a + lb) = a^p \neq c^p = \prod_{0 \leq l \leq p-1}(c + lb)$. We define a polynomial $Q(x) = \prod_{0 \leq l \leq p-1}(x + lb) \in F[x]$. we have $Q(a) = \prod_{0 \leq l \leq p-1}(a + lb)$ and $Q(c) = \prod_{0 \leq l \leq p-1}(c + lb)$. Notice also that $Q(a) = Q(a+b) = Q(a+2b) = \cdots = Q(a+(p-1)b)$. Hence $a, a+b, \cdots, a+(p-1)b$ is a set of distinct roots to the equation $Q(x) = Q(a)$. It follows that these are the only roots because $Q(x)$ is a polynomial of degree p. Therefore if $Q(a) = Q(c)$, then we have $c = a + tb$ for some $0 \leq t \leq p-1$, or equivalently $\sigma^t(v_1) = v_2$. This is a contradiction because v_1 and v_2 are in different orbits. □

Theorem 7. *Let $1 < n \leq p^r$ be an integer and $S \subseteq F[V_{n-1}]^G$ be a separating set for V_{n-1}, then S together with $N_G(x_1)$ and $H(j)$ for $3 \leq j \leq n$ is a separating set for V_n.*

Proof. Let $v_1 = (c_1, c_2, \ldots, c_n)^t$ and $v_2 = (d_1, d_2, \ldots, d_n)^t$ be two vectors in V_n in different G-orbits. If $(c_2, c_3, \ldots, c_n)^t$ and $(d_2, d_3, \ldots, d_n)^t$ are in different G-orbits in V_{n-1}, then there exists a polynomial in S that separates these vectors by assumption. Hence this polynomial separates v_1 and v_2 as well. Therefore we may assume that $c_i = d_i$ for $2 \leq i \leq n$ by replacing $(d_2, d_3, \ldots, d_n)^t$ with a suitable element in its orbit. So we have $c_1 \neq d_1$. First assume that there exists an integer $3 \leq j \leq n$ such that $c_j = d_j \neq 0$. We may also assume that j is the largest such integer. We show that $H(j)$ separates v_1 and v_2 as follows. Assume the notation of Lemma 3. Since $c_i = d_i = 0$ for $i \geq j+1$, by Lemma 3 it is enough to show that $N_{G_{r-k}}(x_1)\,\mathrm{Tr}^G_{G_{r-k}}(X) + f$ separates v_1 and v_2. But since $f \in F[x_2, \ldots, x_n]$, we have $f(v_1) = f(v_2)$. Moreover, by Lemma 4 and Lemma 5 we get $\mathrm{Tr}^G_{G_{r-k}}(X)(v_1) = \mathrm{Tr}^G_{G_{r-k}}(X)(v_2) = c_{\alpha'} c_j^{p^{r-k}k(p-1)} \neq 0$. It follows that we just need to show that $N_{G_{r-k}}(x_1)$ separates v_1 and v_2. If $j \neq p^k + 1$, then by Lemma 2 we have $N_{G_{r-k}}(x_1) \equiv x_1^{p^{r-k}}$ and this polynomial separates v_1 and v_2 because the first coordinates of v_1 and v_2 are different. If $j = p^k + 1$, then we have $\sigma^{p^k}(e_j) = e_j + e_1$. So the basis vectors e_1, e_j span a two dimensional representation

of G_{r-k} . Moreover, since v_1, v_2 are in different G-orbits, $c_1e_1+c_je_j$ and $d_1e_1+c_je_j$ are also in different G_{r-k}-orbits. The reason for this is that the basis elements $e_1, e_2, \ldots, e_{j-1} = e_{p^k}$ are fixed by σ^{p^k} and therefore $\sigma^{p^k l}(d_1e_1 + c_je_j) = c_1e_1 + c_je_j$ for some l implies that $\sigma^{p^k l}(v_2) = \sigma^{p^k l}(d_1e_1 + c_2e_2 + \cdots + c_je_j) = c_1e_1 + c_2e_2 + \cdots + c_je_j = v_1$ which contradicts that v_1 and v_2 are in different G-orbits. Hence by the previous lemma (applied to the group G_{r-k}) we see that $N_{G_{r-k}}(x_1)$ separates $c_1e_1+c_je_j$ and $d_1e_1+c_je_j$. But no variable in $\{x_2, \ldots, x_{j-1}\}$ appears in $N_{G_{r-k}}(x_1)$. It follows that $N_{G_{r-k}}(x_1)$ separates v_1 and v_2 as well. Finally, if $c_i = d_i = 0$ for $3 \leq i \leq n$, then $N_G(x_1)$ separates v_1 and v_2 by the previous lemma. □

References

[1] D. J. Benson. *Polynomial invariants of finite groups*, volume 190 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 1993.

[2] H. E. A. Campbell, B. Fodden, and David L. Wehlau. Invariants of the diagonal C_p-action on V_3. *J. Algebra*, 303(2):501–513, 2006.

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

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

[5] H. E. A. Campbell, R. J. Shank, and David L. Wehlau. Vector invariants for the two dimensional modular representation of a cyclic group of prime order p. *Preprint, arXiv:0901.2811v1*, 2009.

[6] Harm Derksen and Gregor Kemper. *Computational invariant theory*. Invariant Theory and Algebraic Transformation Groups, I. Springer-Verlag, Berlin, 2002. Encyclopaedia of Mathematical Sciences, 130.

[7] Leonard Eugene Dickson. *On invariants and the theory of numbers*. Reprinted by Dover Publications Inc., New York, 1966.

[8] M. Domokos. Typical separating invariants. *Transform. Groups*, 12(1):49–63, 2007.

[9] M. Domokos and E. Szabó. Helly dimension of algebraic groups. *Preprint, arXiv:0911.0404v2*, 2009.

[10] Jan Draisma, Gregor Kemper, and David Wehlau. Polarization of separating invariants. *Canad. J. Math.*, 60(3):556–571, 2008.

[11] E. Dufresne, J. Elmer, and M. Kohls. The Cohen-Macaulay property of separating invariants of finite groups. *To appear in Transform. Groups, arXiv:0904.1069*, 2009.

[12] Emilie Dufresne. Separating invariants and finite reflection groups. *Adv. Math.*, 221(6):1979–1989, 2009.

[13] Alexander Duncan, Michael LeBlanc, and David L. Wehlau. A SAGBI basis for $\mathbb{F}[V_2 \oplus V_2 \oplus V_3]^{C_p}$. *Canad. Math. Bull.*, 52(1):72–83, 2009.

[14] Jonathan Elmer. On the depth of separating algebras for finite groups. *Preprint, available at http://www.maths.qmul.ac.uk/ jelmer/*.

[15] N. J. Fine. Binomial coefficients modulo a prime. *Amer. Math. Monthly*, 54:589–592, 1947.

[16] P. Fleischmann, M. Sezer, R. J. Shank, and C. F. Woodcock. The Noether numbers for cyclic groups of prime order. *Adv. Math.*, 207(1):149–155, 2006.

[17] G. Kemper. Separating invariants. *J. Symbolic Comput.*, 44:1212–1222, 2009.

[18] M. D. Neusel and M. Sezer. Separating invariants for modular p-groups and groups acting diagonally. *To appear in Math. Res. Lett., available at http://www.fen.bilkent.edu.tr/∼sezer/*, 2008.

[19] Mara D. Neusel and Müfit Sezer. The invariants of modular indecomposable representations of Z_{p^2}. *Math. Ann.*, 341(3):575–587, 2008.

[20] Mara D. Neusel and Larry Smith. *Invariant theory of finite groups*, volume 94 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI, 2002.

[21] David R. Richman. Invariants of finite groups over fields of characteristic p. *Adv. Math.*, 124(1):25–48, 1996.

[22] Müfit Sezer. Constructing modular separating invariants. *J. Algebra*, 322(11):4099–4104, 2009.

[23] R. James Shank. S.A.G.B.I. bases for rings of formal modular seminvariants [semi-invariants]. *Comment. Math. Helv.*, 73(4):548–565, 1998.
[24] R. James Shank and David L. Wehlau. Decomposing symmetric powers of certain modular representations of cyclic groups. *Preprint, arXiv:math/0509044.*
[25] R. James Shank and David L. Wehlau. Noether numbers for subrepresentations of cyclic groups of prime order. *Bull. London Math. Soc.*, 34(4):438–450, 2002.

Department of Mathematics, Bilkent University, Ankara 06800 Turkey
E-mail address: sezer@fen.bilkent.edu.tr