Journal of Algebra 322 (2009) 4099–4104

Contents lists available at ScienceDirect

Journal of Algebra

www.elsevier.com/locate/jalgebra

Constructing modular separating invariants ☆

Müfit Sezer

Department of Mathematics, Bilkent University, Ankara 06800, Turkey

ARTICLE INFO

Article history:
Received 2 December 2008
Available online 25 July 2009
Communicated by Harm Derksen

Keywords:
Separating invariants
Modular groups

ABSTRACT

We consider a finite dimensional modular representation V of a cyclic group of prime order p. We show that two points in V that are in different orbits can be separated by a homogeneous invariant polynomial that has degree one or p and that involves variables from at most two summands in the dual representation. Simultaneously, we describe an explicit construction for a separating set consisting of polynomials with these properties.

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 $F[V] := S(V^*)$ of polynomial functions on V. More precisely, 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 $F[V]^G$. Any invariant polynomial $f \in F[V]^G$ is constant on the G-orbits in V. A subset $A \subseteq F[V]^G$ is said to be separating (for V) if for any pairs of vectors $v, w \in V$, we have: If $f(v) = f(w)$ for all $f \in A$, then $f(v) = f(w)$ for all $f \in F[V]^G$. If G is finite, this is equivalent to saying that whenever $v, w \in V$ are in different G-orbits, there exists $f \in A$ such that $f(v) \neq f(w)$. Although the concept of separating invariants dates back to the origins of the invariant theory there has been a recent interest in the topic initiated by Derksen and Kemper [2] who pointed out that one can get nice separating subalgebras as opposed to the full invariant ring which is often complicated in terms of constructive and ring theoretical considerations. For instance, there always exists a finite separating set [2, 2.3.15] and the Noether bound (for finite groups) holds with no restriction on the characteristic of the field [2, 3.9.14]. Since then, separating invariants have been studied by several people and further evidence for their well behavior has been revealed, see [3,5–7,9,13,14]. We direct the reader to [2, 2.3.2, 3.9.4] and [12] for more background and motivation on the subject.

☆ Research supported by a grant from Tübitak: 109T384.
E-mail address: sezer@fen.bilkent.edu.tr.

0021-8693/$ – see front matter
doi:10.1016/j.jalgebra.2009.07.011

In this paper we study separating invariants for representations of a cyclic group $\boldsymbol{Z}/p$ of prime order p, over a field F of characteristic p. Invariants of cyclic p-groups over characteristic p are difficult to describe. Although exact degree bounds for the algebra generators for the invariant rings of all representations of $\boldsymbol{Z}/p$ are known [10], explicit generating sets are available only for handful of cases. Actually, generating sets for the two and the three dimensional indecomposable representations of $\boldsymbol{Z}/p$ were given by Dickson [4] as early as the beginning of the twentieth century. It turns out that these invariant rings are generated by two and four elements respectively. But things get complicated very quickly. The only other indecomposable representations where a generating set for the corresponding ring of invariants are known are the four and the five dimensional representations which were computed by Shank through difficult computations, see [15]. His methods were later used to work out some decomposable cases. A generating set that applies to all representations of $\boldsymbol{Z}/p$ is described by Hughes and Kemper [11]. Their set consists of norms (orbit products) of some variables, transfers (orbit sums) and invariants up to a certain quite optimal degree. The reason to include invariants up to some degree is that norms and transfers can be employed to decompose invariants only after some degree and there are invariants in small degrees that are not expressible using norms and transfers. In [13] it is shown that this uncertainty in small degrees is not an issue for separating purposes: The sum of relative transfers with respect to maximal subgroups together with the norms of certain variables is separating for any representation of any p-group. But unfortunately this separating set is infinite dimensional as a vector space. In this paper we restrict ourselves to $\boldsymbol{Z}/p$ and show that a separating set for an indecomposable representation V_n of dimension n can be obtained by adding to any separating set for the indecomposable subrepresentation V_{n-1} some explicitly described transfers and the norm of the terminal variable of V_n^*, see Theorem 3. The set which we add to a separating set for V_{n-1} consists of polynomials of degree p. Inductively this yields a separating set of polynomials of degree one or p for an indecomposable representation V_n, see Remark 4. But the size of the separating set for V_n obtained from Theorem 3 is not optimal, see again the discussion in Remark 4.

Next we consider decomposable representations. A major result concerning decomposable representations is that the polarization of separating invariants yields a separating set over any characteristic, see Draisma et al. [6] which does not hold for generating invariants. A result by Domokos [5] states that for the direct sum of any number copies of a representation V there exists a separating set of polynomials each of which involve variables from at most $2n$ summands in V^*, where n is the dimension of V. If the group is reductive $2n$ can be replaced by $n+1$. We obtain a sharpening of this result for $\boldsymbol{Z}/p$ as follows. Let W be a $\boldsymbol{Z}/p$ representation over characteristic p. We show that the separating invariants for a particular proper subrepresentation of W union separating invariants for the indecomposable summands in W together with an explicitly constructed set of transfers form a separating set for W, see Theorem 6. These transfers involve variables from two summands only and are of degree p. Hence we obtain by induction that for any representation W of $\boldsymbol{Z}/p$ there is a separating set consisting of degree one and degree p polynomials that involve variables from at most two summands in W^*.

Modular separating invariants

Let $p>0$ be a prime number. For the rest of the paper G denotes the cyclic group of order p, and F denotes a field of characteristic p. We fix a generator σ of G. It is well known that there are exactly p indecomposable representations $V_1, V_2, \dots, V_p$ of G up to isomorphism where σ acts on V_n for $1 \leqslant n \leqslant p$ by a Jordan block of dimension n with ones on the diagonal. Let $e_1, e_2, \dots, e_n$ be the Jordan block basis for V_n with $\sigma(e_i) = e_i + e_{i-1}$ for $2 \leqslant i \leqslant n$ 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 $x_1, x_2, \dots, x_n$ 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 may assume that $\sigma(x_i) = x_i + x_{i+1}$ for $1 \leqslant i \leqslant n-1$ and $\sigma(x_n) = x_n$. We have $F[V_n] = F[x_1, x_2, \dots, x_n]$. Pick a column vector $(c_1, c_2, \dots, c_n)^t$ in V_n, where $c_i \in F$ for $1 \leqslant i \leqslant n$. 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 $F[V_{n-1}] = F[x_2, x_3, \ldots, x_n]$ sits as a subalgebra in $F[V_n]$. For $f \in F[V_n]$, the norm of f, denoted by $N(f)$, is defined by $\prod_{0 \leqslant l \leqslant p-1} \sigma^l(f)$. Moreover define $\mathrm{Tr} = \sum_{0 \leqslant l \leqslant p-1} \sigma^l$, which we call the transfer map. Note that both $N(f)$ and $\mathrm{Tr}(f)$ are invariant polynomials. For a positive integer k, let J_k denote the ideal in $F[V_n]$ generated by $x_k, x_{k+1}, \ldots, x_n$ if $1 \leqslant k \leqslant n$ and let J_k denote the zero ideal if $k > n$. We need the following well-known fact.

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

Proof. We direct the reader to [1, 9.4] for a proof. □

Lemma 2. *Let* $2 \leqslant i \leqslant n-1$ *be an integer. Then there exist* $f_1, f_2 \in F[x_2, x_3, \ldots, x_n]$ *such that* $\mathrm{Tr}(x_1 x_i^{p-1}) = f_1 x_1 + f_2$. *Moreover,* $f_1 \equiv -x_{i+1}^{p-1} \bmod J_{i+2}$.

Proof. Since the vector space generated by $x_2, x_3, \ldots, x_n$ is closed under the G-action and $\sigma(x_1) = x_1 + x_2$, it follows that $\mathrm{Tr}(x_1 x_i^{p-1})$ as a polynomial in x_1 (with coefficients in $F[V_{n-1}]$) is of degree at most one. Therefore the first assertion of the lemma follows.

For $0 \leqslant l \leqslant p-1$ we have

$$\sigma^l\big(x_1 x_i^{p-1}\big) = \left(x_1 + l x_2 + \binom{l}{2} x_3 + \cdots\right)\left(x_i + l x_{i+1} + \binom{l}{2} x_{i+2} + \cdots\right)^{p-1}.$$

Let a, b be non-negative integers with $a + b = p-1$. Then the coefficient of $x_1 x_i^a x_{i+1}^b$ in $\sigma^l(x_1 x_i^{p-1})$ is $\binom{p-1}{b} l^b$. Therefore the coefficient of $x_1 x_i^a x_{i+1}^b$ in $\mathrm{Tr}(x_1 x_i^{p-1})$ is $\sum_{0 \leqslant l \leqslant p-1} \binom{p-1}{b} l^b$. By the previous lemma this number is zero unless $b = p-1$ and is -1 if $b = p-1$. This completes the proof. □

Let $S \subseteq F[V_{n-1}]^G$ be a separating set of invariants for V_{n-1}. Our next result describes a finite set of invariant polynomials in $F[V_n]^G$ such that, when added to S, one gets a separating set for V_n.

Theorem 3. *Let* $S \subseteq F[V_{n-1}]^G$ *be a separating set for* V_{n-1}. *Then S together with* $N(x_1)$, $\mathrm{Tr}(x_1 x_i^{p-1})$ *for* $2 \leqslant i \leqslant n-1$ *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 column vectors in V_n in different G-orbits, where $c_i, d_i \in F$ for $1 \leqslant i \leqslant n$. If $(c_2, c_3, \ldots, c_n)^t$ and $(d_2, d_3, \ldots, d_n)^t$ are in different orbits in V_{n-1}, then there exists a polynomial in S that separates these points because $S \subseteq F[V_{n-1}]^G$ is separating. Therefore this polynomial separates v_1 and v_2 as well. Hence by replacing v_2 with a suitable element in its orbit we may assume that $c_i = d_i$ for $2 \leqslant i \leqslant n$. Note that with this assumption we must have $c_1 \neq d_1$. First assume that there exists index $3 \leqslant i \leqslant n$ such that $c_i = d_i \neq 0$. Let j denote the largest integer $\leqslant n$ such that $c_j \neq 0$. We show that $\mathrm{Tr}(x_1 x_{j-1}^{p-1})$ separates v_1 and v_2 as follows. By the previous lemma we can write $\mathrm{Tr}(x_1 x_{j-1}^{p-1}) = f_1 x_1 + f_2$ such that $f_1, f_2 \in F[x_2, x_3, \ldots, x_n]$ with $f_1 \equiv -x_j^{p-1} \bmod J_{j+1}$. Since $c_i = d_i$ for $2 \leqslant i \leqslant n$, we have $f_2(v_1) = f_2(v_2)$ and $f_1(v_1) = f_1(v_2)$. Moreover $f_1(v_1) = -c_j^{p-1}$ because $c_i = 0$ for $j < i$, so $f_1(v_1)$ (and hence $f_1(v_2)$) is non-zero. It follows that $f_1 x_1 + f_2$ separates v_1 and v_2 because the first coordinates of these vectors are different. We now assume that $c_i = d_i = 0$ for $3 \leqslant i \leqslant n$. We show that in this case $N(x_1)$ separates v_1 and v_2. Note that $N(x_1)(v_1) = \prod_{0 \leqslant l \leqslant p-1}(c_1 + l c_2)$. We define a polynomial $Q(x) = \prod_{0 \leqslant l \leqslant p-1}(x + l c_2) \in F[x]$. Notice that $N(x_1)(v_1) = Q(c_1)$ and that $Q(c_1) = Q(c_1 + c_2) = Q(c_1 + 2c_2) = \cdots = Q(c_1 + (p-1)c_2)$. Since $Q(x)$ is a polynomial of degree p, it follows that $c_1, c_1 + c_2, c_1 + 2c_2, \ldots, c_1 + (p-1)c_2$ are the only solutions to $Q(x) = Q(c_1)$. Therefore if $N(x_1)(v_2) = \prod_{0 \leqslant l \leqslant p-1}(d_1 + l d_2) = \prod_{0 \leqslant l \leqslant p-1}(d_1 + l c_2) = Q(d_1)$ is equal to $N(x_1)(v_1) = Q(c_1)$, then d_1 must be equal to $c_1 + l c_2$ for some $0 \leqslant l \leqslant p-1$. Equivalently we must have $\sigma^l(v_1) = v_2$. This is a contradiction because then v_1 and v_2 are in the same G-orbit. □

Remark 4. The invariants of the two dimensional indecomposable representation V_2 is a regular ring generated by the fixed variable of V_2^* and the norm of the terminal variable of V_2^*, see [4]. The set in Theorem 3 which we add to a separating set for V_{n-1} consists of $n-1$ polynomials of degree p. Hence, inductively this yields a separating set of $n(n-1)/2+1$ polynomials of degree one or p for an indecomposable representation V_n. We note that there is always a separating set of size $2n+2$ for any representation of dimension n of any group. This fact was forwarded to us with a sketch of a proof during the refereeing process of [13] and it also appears in [8]. However, the proof is not constructive as opposed to Theorem 3. We will see that it is possible to obtain separating sets consisting of polynomials of degree one or p for decomposable representations as well, see Corollary 7.

We have mentioned in the introduction that the computations [15] for the invariants of V_4 and V_5 are difficult and the generating sets are more complicated compared to the two and the three dimensional representations. On the other hand our result yields a much more simpler separating subalgebra. Consider $F[x_2,x_3,x_4]=F[V_3]\subseteq F[x_1,x_2,x_3,x_4]=F[V_4]$. Then $F[x_2,x_3,x_4]^G$ is generated by x_4, $x_3^2-2x_2x_4-x_3x_4$, $\mathrm{Tr}(x_3x_4^{p-1})$, $N(x_2)$, see [4]. Since these four polynomials form a separating set in $F[x_2,x_3,x_4]^G$, by the previous theorem, this set together with $N(x_1)$, $\mathrm{Tr}(x_1x_2^{p-1})$, $\mathrm{Tr}(x_1x_3^{p-1})$ is a separating set in $F[x_1,x_2,x_3,x_4]^G$. It is instructive to compare this separating set with the generating set given in [15].

We now consider decomposable representations of G. Let $W=\bigoplus_{i=1}^m W_i$, where W_i is an indecomposable G representation of dimension $q_i\leqslant p$, i.e., $W_i=V_{q_i}$. Let $e_{i,1},e_{i,2},\dots,e_{i,q_i}$ denote the standard basis vectors for W_i, where $e_{i,j}$ is the column vector of dimension q_i with one at the j-th coordinate and zero elsewhere. As before, we assume that these vectors form a Jordan block basis for W_i with $\sigma(e_{i,j})=e_{i,j-1}$ for $2\leqslant j\leqslant q_i$ and $\sigma(e_{i,1})=e_{i,1}$. Let $x_{i,1},x_{i,2},\dots,x_{i,q_i}$ denote the corresponding elements in the dual W_i^*. Define $T_i=V_{q_i-1}$ and recall that there is a G-equivariant surjection $\pi_i: W_i\to T_i$, given by $(c_{i,1},c_{i,2},\dots,c_{i,q_i})^t\to(c_{i,2},c_{i,3},\dots,c_{i,q_i})^t$, where $c_{i,j}\in F$ for $1\leqslant j\leqslant q_i$. Define $T=\bigoplus_{i=1}^m T_i$. We identify W as the vector space of m-tuples $(w_1,w_2,\dots,w_m)$ with $w_i\in W_i$ and T as the vector space of m-tuples $(t_1,t_2,\dots,t_m)$ with $t_i\in T_i$. Then we have a G-equivariant surjection $\pi: W\to T$ given by $(w_1,w_2,\dots,w_m)\to(\pi_1(w_1),\pi_2(w_2),\dots,\pi_m(w_m))$. Dual to this surjection, the subspace in W^* generated by $x_{i,j}$ for $1\leqslant i\leqslant m$, $2\leqslant j\leqslant q_i$ is isomorphic to T^*. Therefore we get the inclusion

$$F[T]=F[x_{i,j}\mid 1\leqslant i\leqslant m,\ 2\leqslant j\leqslant q_i]\subseteq F[W]=F[x_{i,j}\mid 1\leqslant i\leqslant m,\ 1\leqslant j\leqslant q_i].$$

We prove a result along the same lines of Lemma 2. Let k be a positive integer and for $1\leqslant j\leqslant m$, let $J_{j,k}$ denote the ideal in $F[W_j]$ generated by $x_{j,k},x_{j,k+1},\dots,x_{j,q_j}$. Set $J_{j,k}=0$ if $k>q_j$.

Lemma 5. *Let i,j,k be integers satisfying $1\leqslant i,j\leqslant m$, $i\neq j$ and $1\leqslant k\leqslant q_j-1$. Then there exist $f_1\in F[W_j]$ and $f_2\in F[T_i]\otimes F[W_j]$ such that $\mathrm{Tr}(x_{i,1}x_{j,k}^{p-1})=f_1x_{i,1}+f_2$. Moreover, $f_1\equiv -x_{j,k+1}^{p-1} \bmod J_{j,k+2}$.*

Proof. The proof essentially carries over from Lemma 2. For $0\leqslant l\leqslant p-1$, we have

$$\sigma^l\big(x_{i,1}x_{j,k}^{p-1}\big)=\left(x_{i,1}+lx_{i,2}+\binom{l}{2}x_{i,3}+\cdots\right)\left(x_{j,k}+lx_{j,k+1}+\binom{l}{2}x_{j,k+2}+\cdots\right)^{p-1}.$$

Note that no monomial in the above expansion is divisible by $x_{i,1}^2$. Therefore as a polynomial in $x_{i,1}$, the transfer $\mathrm{Tr}(x_{i,1}x_{j,k}^{p-1})$ is of degree at most one and moreover if a monomial m that appears in $\mathrm{Tr}(x_{i,1}x_{j,k}^{p-1})$ is divisible by $x_{i,1}$, then $m/x_{i,1}$ is in $F[W_j]$. Finally, for non-negative integers a and b with $a+b=p-1$ the coefficient of $x_{i,1}x_{j,k}^a x_{j,k+1}^b$ in $\sigma^l(x_1x_i^{p-1})$ is $\binom{p-1}{b}l^b$. Therefore the coefficient of $x_{i,1}x_{j,k}^a x_{j,k+1}^b$ in $\mathrm{Tr}(x_{i,1}x_{j,k}^{p-1})$ is $\sum_{0\leqslant l\leqslant p-1}\binom{p-1}{b}l^b$. Hence the final statement follows as in Lemma 2. □

For $1 \leqslant i, j \leqslant m$ with $i \neq j$ and $1 \leqslant k \leqslant q_j - 1$ define $H^k_{i,j} = \mathrm{Tr}(x_{i,1}x^{p-1}_{j,k})$. Set

$$H = \left\{H^k_{i,j} \;\middle|\; 1 \leqslant i, j \leqslant m,\ i \neq j,\ 1 \leqslant k \leqslant q_j - 1\right\}.$$

We show that the union polynomials in H and the separating sets for T, W_i for $1 \leqslant i \leqslant m$ gives a separating set for W.

Theorem 6. *Assume the notation and the convention of the previous paragraphs. For $1 \leqslant 1 \leqslant m$, let $S_i \subseteq F[W_i]^G$ denote a separating set for W_i and $S \subseteq F[T]^G$ denote a separating set for T. Then the union of the polynomials in $S, S_1, S_2, \dots, S_m, H$ is a separating set for W.*

Proof. Let $v_1 = (c_1, \dots, c_m)$ and $v_2 = (d_1, \dots, d_m)$ be two vectors in W in different G-orbits, where $c_i, d_i \in W_i$ for $1 \leqslant i \leqslant m$. Say $c_i = (c_{i,1}, c_{i,2}, \dots, c_{i,q_i})^t$ and $d_i = (d_{i,1}, d_{i,2}, \dots, d_{i,q_i})^t$, where $c_{i,j}, d_{i,j} \in F$ for $1 \leqslant i \leqslant m$ and $1 \leqslant j \leqslant q_i$. If $\pi(v_1)$ and $\pi(v_2)$ in T were in different G-orbits, then there exists a polynomial in S that separates $\pi(v_1)$ and $\pi(v_2)$ because S is a separating set for T. This polynomial separates v_1 and v_2 as well. Therefore we may assume that $\pi(v_1)$ and $\pi(v_2)$ are in the same G-orbit. Hence by replacing v_2 with a suitable vector in its orbit we may assume that $\pi(v_1) = \pi(v_2)$, that is $c_{i,j} = d_{i,j}$ for $1 \leqslant i \leqslant m$ and $2 \leqslant j \leqslant q_i$. Also if c_i and d_i are in different G-orbits for some $1 \leqslant i \leqslant m$, then there exists a polynomial in S_i that separates c_i and d_i because S_i is a separating set for W_i. Then v_1 and v_2 is separated by this polynomial as well. Therefore we may assume that c_i and d_i are in the same G-orbit for $1 \leqslant i \leqslant m$.

First assume that there exists $1 \leqslant r \leqslant m$ and $3 \leqslant k \leqslant q_r$ such that $c_{r,k} = d_{r,k} \neq 0$. By replacing k with a larger integer if necessary, we may assume that $c_{r,k'} = d_{r,k'} = 0$ for $k < k' \leqslant q_r$. Since $c_r, d_r \in W_r$ are in the same G-orbit, there exists an integer $0 \leqslant l \leqslant p - 1$ such that $\sigma^l(c_r) = d_r$. Since $c_{r,k'} = 0$ for $k' > k$, the $(k - 1)$-st coordinate of $\sigma^l(c_r)$ is equal to $c_{r,k-1} + lc_{r,k}$. Therefore the equality of the vectors $\sigma^l(c_r)$ and d_r gives $c_{r,k-1} + lc_{r,k} = d_{r,k-1}$. But since we have $c_{r,k-1} = d_{r,k-1}$, it follows that $l = 0$, that is $c_r = d_r$. On the other hand since $v_1 \neq v_2$, there exists $1 \leqslant b \leqslant m$, $b \neq r$ such that $c_b \neq d_b$. Equivalently $c_{b,1} \neq d_{b,1}$. We show that $H^{k-1}_{b,r} = \mathrm{Tr}(x_{b,1}x^{p-1}_{r,k-1})$ separates v_1 and v_2. By the previous lemma we can write $\mathrm{Tr}(x_{b,1}x^{p-1}_{r,k-1}) = f_1 x_{b,1} + f_2$ with $f_2 \in F[T_b] \otimes F[W_r]$, $f_1 \in F[W_r]$ with $f_1 \equiv -x^{p-1}_{r,k} \bmod J_{r,k+1}$. Since $c_{b,k'} = d_{b,k'}$ for $k' > 1$, $c_r = d_r$ and $f_2 \in F[T_b] \otimes F[W_r]$, it follows that $f_2(v_1) = f_2(v_2)$. We also have $f_1(v_1) = -c^{p-1}_{r,k}$ because $c_{r,k'} = 0$ for $k' > k$. Similarly $f_1(v_2) = -d^{p-1}_{r,k}$. Since $c_{r,k} = d_{r,k} \neq 0$, it follows that $f_1(v_1) = f_1(v_2) \neq 0$. Hence $H^{k-1}_{b,r}$ separates v_1 and v_2 because $c_{b,1} \neq d_{b,1}$.

Next we consider the case $c_{i,j} = d_{i,j} = 0$ for all $1 \leqslant i \leqslant m$ and $3 \leqslant j \leqslant q_i$. We look into two subcases. First assume that there exists $1 \leqslant r \leqslant m$ such that $c_{r,2} = d_{r,2} \neq 0$. Since c_r and d_r are in the same G-orbit there exists an integer $0 \leqslant l \leqslant p - 1$ such that $\sigma^l(c_r) = d_r$. Moreover, since $c_{i,j} = 0$ for $1 \leqslant i \leqslant m$ and $3 \leqslant j \leqslant q_i$, all coordinates of $\sigma^l(c_i)$ and c_i are the same except the first one for $1 \leqslant i \leqslant m$. That is $\pi(v_1) = \pi(\sigma^l(v_1))$. Therefore by replacing v_1 with $\sigma^l(v_1)$, we may assume that $c_{r,1} = d_{r,1}$ as well. On the other hand since $v_1 \neq v_2$, there exists $1 \leqslant b \leqslant m$, $b \neq r$ such that $c_b \neq d_b$. Now we have reduced to the situation considered in the previous paragraph: There exists $1 \leqslant r \leqslant m$ such that $c_r = d_r$ and $1 \leqslant b \leqslant m$ such that $c_{b,1} \neq d_{b,1}$. Since $c_{r,k'} = d_{r,k'} = 0$ for $2 < k' \leqslant q_r$, the argument in the previous paragraph shows that $H^1_{b,r} = \mathrm{Tr}(x_{b,1}x^{p-1}_{r,1})$ separates v_1 and v_2. Finally if $c_{i,j} = d_{i,j} = 0$ for all $1 \leqslant i \leqslant m$ and $2 \leqslant j \leqslant q_i$, then each c_i and d_i is a fixed point in W_i. Hence if c_i and d_i are in the same G-orbit, then $c_i = d_i$. Since this is true for all $1 \leqslant i \leqslant m$, it follows that $v_1 = v_2$. $\square$

Note that the dimensions of indecomposable summands in T are one less than the dimensions of the indecomposable summands in W. Meanwhile, the polynomials in S_i may be chosen to be of degree one and p for all $1 \leqslant i \leqslant m$ by Remark 4 and the polynomials in H are of degree p and involve variables from two summands. Therefore by induction on the maximum dimension of an indecomposable summand in a representation one easily gets the following.

Corollary 7. *Let W be a $\boldsymbol{Z}/p$ representation over characteristic p. Then there exists a separating set for W consisting of polynomials each of which has degree one or p and involves variables from at most two summands in W^*.*

References

[1] H.E.A. Campbell, I.P. Hughes, R.J. Shank, D.L. Wehlau, Bases for rings of coinvariants, Transform. Groups 1 (4) (1996) 307–336.
[2] Harm Derksen, Gregor Kemper, Computational invariant theory, in: Invariant Theory and Algebraic Transformation Groups, I, in: Encyclopaedia Math. Sci., vol. 130, Springer-Verlag, Berlin, 2002.
[3] Harm Derksen, Gregor Kemper, Computing invariants of algebraic groups in arbitrary characteristic, Adv. Math. 217 (5) (2008) 2089–2129.
[4] Leonard Eugene Dickson, On Invariants and the Theory of Numbers, Reprinted by Dover Publications Inc., New York, 1966.
[5] M. Domokos, Typical separating invariants, Transform. Groups 12 (1) (2007) 49–63.
[6] Jan Draisma, Gregor Kemper, David Wehlau, Polarization of separating invariants, Canad. J. Math. 60 (3) (2008) 556–571.
[7] E. Dufresne, J. Elmer, M. Kohls, The Cohen–Macaulay property of separating invariants of finite groups, preprint, arXiv:0904.1069, 2009.
[8] Emilie Dufresne, Separating invariants, PhD thesis, Queen's University, Kingston, Ontario, 2008.
[9] Emilie Dufresne, Separating invariants and finite reflection groups, Adv. Math. 221 (6) (2009) 1979–1989.
[10] P. Fleischmann, M. Sezer, R.J. Shank, C.F. Woodcock, The Noether numbers for cyclic groups of prime order, Adv. Math. 207 (1) (2006) 149–155.
[11] Ian Hughes, Gregor Kemper, Symmetric powers of modular representations, Hilbert series and degree bounds, Comm. Algebra 28 (4) (2000) 2059–2088.
[12] G. Kemper, Separating invariants, J. Symbolic Comput. 44 (2009) 1212–1222.
[13] M.D. Neusel, M. Sezer, Separating invariants for modular p-groups and groups acting diagonally, preprint, available at http://www.fen.bilkent.edu.tr/~sezer/, 2008.
[14] Mufit Sezer, Lexsegment and Gotzmann ideals associated with the diagonal action of $\boldsymbol{Z}/p$, preprint, available at http://www.fen.bilkent.edu.tr/~sezer/, 2008.
[15] R. James Shank, S.A.G.B.I. bases for rings of formal modular seminvariants [semi-invariants]., Comment. Math. Helv. 73 (4) (1998) 548–565.