Math. Res. Lett. **16** (2009), *no.* 6, 1029–1036

SEPARATING INVARIANTS FOR MODULAR P-GROUPS AND GROUPS ACTING DIAGONALLY

Mara D. Neusel and Müfit Sezer

Abstract. We study separating algebras for rings of invariants of finite groups. We describe a separating subalgebra for invariants of p-groups in characteristic p using only transfers and norms. Also we give an explicit construction of a finite separating set for invariants of groups acting diagonally.

Let $\mathbb{F}$ be an algebraically closed field and let G be a finite group. Consider a faithful representation

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

of degree n. It induces an action of the group G on the symmetric algebra on the dual space V^*, which we denote by $\mathbb{F}[V]$. The subring of G-invariants is denoted by $\mathbb{F}[V]^G$. We note that the vector space V decomposes into disjoint G-orbits. We denote the orbit space by

$$V/G = \{[\mathbf{v}] = \{g\mathbf{v} | g \in G\} | \mathbf{v} \in V\}.$$

Any invariant $f \in \mathbb{F}[V]^G$ is constant on the G-orbits $[\mathbf{v}]$. Indeed, $\mathbb{F}[V]^G \subseteq \mathbb{F}[V]$ is the largest subalgebra with this property. A finitely generated graded subalgebra $A \subseteq \mathbb{F}[V]^G$ (or more generally a subset in $\mathbb{F}[V]^G$) is called separating if for any two distinct G-orbits $[\mathbf{v}] \neq [\mathbf{w}]$ there exists a function $f \in A$ separating the two, i.e.,

$$f(\mathbf{v}) \neq f(\mathbf{w}),$$

see Definition 2.3.8 in [1]. Denote by $\overline{A}$ the integral closure of the algebra A (in its field of fractions) and by $\sqrt{A}$ its purely inseparable closure in $\mathbb{F}[V]$, where $p > 0$ is the characteristic of $\mathbb{F}$. If $\mathbb{F}$ has characteristic zero set $\sqrt{A} = A$. For the case of positive characteristic, a finitely generated separating graded subalgebra A is separating if and only if $\sqrt{\overline{A}} = \mathbb{F}[V]^G$, see Theorem 2.3.12 in [1] and Remark 1.3 in [2]. If $\mathbb{F}$ has characteristic zero, then $\overline{A} = \mathbb{F}[V]^G$ provided that A is finitely generated separating graded subalgebra, again by Theorem 2.3.12 ibid. The converse is not valid, see Example 2.3.14 in [1].

Remark 1. We note that for fields that are not algebraically closed, the notion "separating" does not give the desired results. For example, consider the finite field $\mathbb{F}_2$ with two elements. The general linear group $\mathsf{GL}(2, \mathbb{F}_2)$ is a finite group of order 6. Its ring of invariants $\mathbb{F}_2[x, y]^{\mathsf{GL}(2,\mathbb{F}_2)}$ is a polynomial ring generated by $\mathsf{d}_{2,0} = x^2y + xy^2$ and $\mathsf{d}_{2,1} = x^2 + xy + y^2$, see, e.g., Theorem 6.1.4 in [12]. The vector space

Received by the editors March 16, 2009.

2000 *Mathematics Subject Classification.* 13A50.

The second author is supported by a grant from Tübitak: 109T384.

$V = \mathrm{span}_{\mathbb{F}_2}\{\mathbf{e}_1, \mathbf{e}_2\}$ decomposes into the two orbits $V \setminus 0$ and $\{0\}$. Note that the subalgebra

$$\mathbb{F}_2[\mathsf{d}_{2,1}] \subseteq \mathbb{F}_2[x, y]^{\mathsf{GL}(2,\mathbb{F}_2)}$$

is separating, but the extension is neither finite nor integral. Even worse, the subgroup $\mathbb{Z}/3$ generated by $\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$ has the same orbits on V. In other words, the separating subalgebra $\mathbb{F}_2[\mathsf{d}_{2,1}]$ does not characterize the ring of invariants of $\mathsf{GL}(2, \mathbb{F}_2)$. However, we could consider the invariants over the algebraic closure of $\mathbb{F}_2$. We obtain

$$\overline{\mathbb{F}}[x, y]^{\mathsf{GL}(2,\mathbb{F}_2)} = \overline{\mathbb{F}} \otimes_{\mathbb{F}_2} \mathbb{F}_2[x, y]^{\mathsf{GL}(2,\mathbb{F}_2)}.$$

Taking into account the orbits of the group action on $\overline{V} = \mathrm{span}_{\overline{\mathbb{F}}}\{\mathbf{e}_1, \mathbf{e}_2\}$ we see that the subalgebra generated by the degree two invariant is, as expected, no longer separating: $\mathsf{d}_{2,1}$ vanishes on the orbit $[(1, \omega)]$ for a primitive 3rd root of unity ω.

Separating invariants have been studied by several people, see, e.g., [1], [3], [4], [5], [7], [11], [17], [18] and the references there. All of these studies show that separating invariants are often better behaved than the ring of invariants itself, e.g., there are always separating algebras that satisfy Noether's bound, see Corollary 3.9.14 in [1], or, separating invariants of vector invariants can be obtained by polarizations, see [5]. In this paper we continue the study of separating invariants.

In Section 1 we will describe a separating subalgebra for the ring of invariants of a finite p-group P over a field of characteristic p. We note that *generating* invariants of p-groups are usually difficult to describe. Indeed, apart from individual cases, the only large families of modular representations of finite p-groups for which complete (but maybe not minimal) generating sets with good degree bounds for the invariants are known are the (all of them) representations of cyclic groups of order p, see [9, 10], and the indecomposable representations of cyclic groups of order p^2, see [14]. In both cases, the rings of invariants are generated by norms, transfers, and invariants up to a certain degree. The reason for including all invariants up to some degree is that norms and transfers can be employed to decompose invariants usually only after some degree and not all invariants at small degrees are norms or (relative) transfers. We show that in contrast norms and transfers suffice to *separate* orbits for *all* representations of *any* p-group.

In Section 2 we turn to the other extreme: We consider groups that act by diagonal matrices. For these groups we describe a separating set of size $2^n - 1$. Moreover, if the group is cyclic of prime order we improve upon this by giving a separating set of size $\frac{n^2+n}{2}$. We remark that there always exists a separating set of size $2n + 2$ for any group. This fact was forwarded to us with a sketch of a proof by the anonymous referee and it also appears in [6]. However, the proof is not constructive. Meanwhile, our description of separating sets for these diagonal groups is constructive and use only combinatorial methods. Moreover the separating sets we produce consist of monomials.

We close the introduction with an example.

Example. Let $\rho : G \hookrightarrow \mathsf{GL}(n, \mathbb{F})$ be a representation of a finite group G. Denote by $\mathbb{F}G$ the group algebra and let

$$V(G) = \mathbb{F}G \otimes V$$

be the induced module. The group G acts on $V(G)$ by left multiplication on the first component. Hence $V(G)$ is just the direct sum of n copies of $\mathbb{F}G$. We obtain a surjective G-equivariant map between the rings of polynomial functions

$$\eta_G : \mathbb{F}[V(G)] \longrightarrow \mathbb{F}[V].$$

By restriction to the induced ring of invariants, we obtain the classical Noether map, see Section 4.2 in [12],

$$\eta_G^G : \mathbb{F}[V(G)]^G \longrightarrow \mathbb{F}[V]^G.$$

We note that $V(G)$ is the n-fold regular representation of G. Thus $\mathbb{F}[V(G)]^G$ are the n-fold vector invariants of the regular representation of G. In the classical nonmodular case the map η_G^G is surjective, see Proposition 4.2.2 in [12]. This does not remain true in the modular case. However, as shown in Proposition 2.2 of [15] the p-root closure of the image of the Noether map is equal to $\mathbb{F}[V]^G$. Thus, by Remark 1.3 in [2], the image of the Noether map is separating.

1. Separating subalgebras for modular P-Groups

In this section we want to present a new construction for separating subalgebras of rings of invariants of finite p-groups over an algebraically closed field $\mathbb{F}$ of characteristic p. All groups in this section are finite p-groups. We start with a recollection of two methods to construct invariants. For $f \in \mathbb{F}[V]$, we define the norm of f, denoted $\mathsf{N}(f)$, by

$$\prod_{g \in G} g(f) \in \mathbb{F}[V]^G.$$

Furthermore, the transfer is defined by

$$\mathsf{Tr}^G : \mathbb{F}[V] \longrightarrow \mathbb{F}[V]^G,\ f \mapsto \sum_{g \in G} g(f).$$

One obtains a relative version in the following way: Let H be a subgroup of G. Then the relative transfer (from H to G) is given by

$$\mathsf{Tr}_H^G : \mathbb{F}[V]^H \to \mathbb{F}[V]^G,\ \mathsf{Tr}_H^G(f) = \sum_{\bar{g} \in G/H} \bar{g}(f),$$

where the sum runs over a set of coset representatives of H in G. We set

$$I = \sum_{H < G,\ \max} \mathrm{Im}(\mathsf{Tr}_H^G) \subseteq \mathbb{F}[V]^G,$$

i.e., I is the ideal in $\mathbb{F}[V]^G$ generated by the image of the relative transfers for all maximal subgroups $H < G$.

As mentioned in the introduction, norms and transfers usually[1] do not suffice to generate the entire ring of invariants $\mathbb{F}[V]^G$, but play a crucial role for invariants of p-groups as they appear in every known list of generating invariants. We proceed by showing that, in contrast, norms and transfers suffice to *separate* orbits for any representation of a p-group.

[1] An exception would be vector invariants of the regular representation of the cyclic group of order p. Indeed, a very special case. See [13]

For a subset $X \in \mathbb{F}[V]^G$ we define its zero set in V/G by

$$\mathcal{V}(X) = \{[\mathbf{v}] \in V/G | f(\mathbf{v}) = 0 \ \ \forall f \in X\}.$$

For $\mathbf{v} \in V$, let $G_{\mathbf{v}}$ denote the stabilizer of $\mathbf{v}$ in G. The following is a part of Theorem 12.4 in [8] generalizing Feshbach's Transfer Theorem.

Lemma 2. *Let G be a finite p-group. The zero set of I in V/G is equal to the fixed point space of G. That is*

$$\mathcal{V}(I) = \{[\mathbf{v}] \in V/G \mid G_{\mathbf{v}} = G\} = V^G.$$

Proof. Let $\mathbf{v} \in V$ such that $G_{\mathbf{v}} = G$. Let $H < G$ be a maximal subgroup and $f \in \mathbb{F}[V]^H$. Then

$$\mathsf{Tr}^G_H(f)(\mathbf{v}) = (\sum_{\overline{g} \in G/H} g(f))(\mathbf{v}) = \sum_{\overline{g} \in G/H} f(g^{-1}\mathbf{v}) = |G : H| f(\mathbf{v}) = 0.$$

Conversely pick $\mathbf{v} \in V$ such that $G_{\mathbf{v}} \neq G$. Since G is finite, there exists $f \in \mathbb{F}[V]$ such that $f(\mathbf{v}) \neq 0$ and $f(g\mathbf{v}) = 0$ for all $g \notin G_{\mathbf{v}}$. Let

$$\mathsf{N} = \prod_{h \in G_{\mathbf{v}}} h(f) \in \mathbb{F}[V]^{G_{\mathbf{v}}}.$$

Note that $\mathsf{N}(\mathbf{v}) \neq 0$ and $\mathsf{N}(g\mathbf{v}) = 0$ for all $g \notin G_{\mathbf{v}}$. Moreover

$$\mathsf{Tr}^G_{G_{\mathbf{v}}}(\mathsf{N})(\mathbf{v}) = \sum_{\overline{g} \in G/G_{\mathbf{v}}} \overline{g}\mathsf{N}(\mathbf{v}) = \sum_{\overline{g} \in G/G_{\mathbf{v}}} \mathsf{N}(\overline{g}^{-1}\mathbf{v}) = \mathsf{N}(\mathbf{v}) \neq 0.$$

Let H be a maximal subgroup of G containing $G_{\mathbf{v}}$. Since $G_{\mathbf{v}} \subseteq H$, we have $\mathrm{Im}(\mathsf{Tr}^G_{G_{\mathbf{v}}}) \subseteq \mathrm{Im}(\mathsf{Tr}^G_H)$. It follows that $\mathbf{v} \notin \mathcal{V}(\mathrm{Im}(\mathsf{Tr}^G_H))$ and accordingly, $\mathbf{v} \notin \mathcal{V}(I)$ as desired. □

Let $\mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_k$ be a basis for V^G, and let $x_1, x_2, \ldots, x_k$ denote the corresponding basis elements in the dual space.

Theorem 3. *Let $\rho : P \hookrightarrow \mathsf{GL}(n, \mathbb{F})$ be a faithful representation of a finite p-group P over a field $\mathbb{F}$ of characteristic p. Then the subalgebra in $\mathbb{F}[V]^P$ generated by I and $\mathsf{N}(x_i)$, $i = 1, \ldots, k$ is separating.*

Proof. Assume that $\mathbf{v}, \mathbf{w} \in V$ are in different P-orbits. Then there exists an invariant $f \in \mathbb{F}[V]^P$ such that $f(\mathbf{v}) \neq f(\mathbf{w})$.

If one of them, say $\mathbf{v}$, lies outside of $\mathcal{V}(I)$, then there exists a maximal subgroup Q in P and an invariant $h \in \mathbb{F}[V]^Q$ such that $\mathsf{Tr}^P_Q(h)(\mathbf{v}) \neq 0$.

If $\mathsf{Tr}^P_Q(h)(\mathbf{v}) \neq \mathsf{Tr}^P_Q(h)(\mathbf{w})$ we are done. Otherwise, we find that

$$f \cdot \mathsf{Tr}^P_Q(h) = \mathsf{Tr}^P_Q(f \cdot h) \in \mathrm{Im}(\mathsf{Tr}^P_Q)$$

separates $\mathbf{v}$ and $\mathbf{w}$.

Thus, we may assume that both, $\mathbf{v}$ as well as $\mathbf{w}$, lie in $\mathcal{V}(I)$. From the previous lemma we have $\mathbf{v}, \mathbf{w} \in V^P$. Since the fixed point space V^P is spanned by $\{\mathbf{e}_1, \ldots, \mathbf{e}_k\}$ we can write $\mathbf{v} = \sum_{i=1}^k \alpha_i \mathbf{e}_i$ and $\mathbf{w} = \sum_{i=1}^k \beta_i \mathbf{e}_i$ for suitable $\alpha_i, \beta_i \in \mathbb{F}$, $1 \leq i \leq k$. Since $\mathbf{v} \neq \mathbf{w}$ there is a $i_0 \in \{1, \ldots, k\}$ such that $\alpha_{i_0} \neq \beta_{i_0}$. Thus

$$\mathsf{N}(x_{i_0})(\mathbf{v}) = \alpha_{i_0}^{p^r} \quad \text{and} \quad \mathsf{N}(x_{i_0})(\mathbf{w}) = \beta_{i_0}^{p^r}.$$

Since $\mathbb{F}$ has characteristic p, it also follows that $\mathsf{N}(x_{i_0})(\mathbf{v}) \neq \mathsf{N}(x_{i_0})(\mathbf{w})$. Thus $\mathsf{N}(x_{i_0})$ separates $\mathbf{v}$ and $\mathbf{w}$ as desired. □

We finish this section by describing the radical $\sqrt{I}$ of the ideal I, see Corollary 12.3 [8] for the special case of cyclic p-groups. We denote by $\mathcal{J}(V^P) \subseteq \mathbb{F}[V]$ the vanishing ideal of the fixed point set of P.

Proposition 4. *Let $\rho : P \hookrightarrow \mathsf{GL}(n, \mathbb{F})$ be a faithful representation of a finite p-group P over a field $\mathbb{F}$ of characteristic p. Then*

$$\sqrt{I} = \mathcal{J}(V^P) \cap \mathbb{F}[V]^P.$$

Proof. By Lemma 2, we have $\mathcal{V}(I) = V^P$. On the other hand, it is clear that $\mathcal{V}\big(\mathcal{J}(V^P)\big) = V^P$. Since $\mathcal{J}(V^P)$ is generated by the linear forms x_i such that $i \notin \{1, \ldots, k\}$, it is a prime ideal. The Nullstellensatz yields

$$\sqrt{I\mathbb{F}[V]} = \mathcal{J}(V^P),$$

where $I\mathbb{F}[V] \subseteq \mathbb{F}[V]$ denotes the extension of I in $\mathbb{F}[V]$. Thus we obtain

$$\sqrt{I} \subseteq \sqrt{I\mathbb{F}[V]} \cap \mathbb{F}[V]^P = \mathcal{J}(V^P) \cap \mathbb{F}[V]^P.$$

Since finite p-groups are reductive we also have

$$\sqrt{I\mathbb{F}[V]} \cap \mathbb{F}[V]^P \subseteq \sqrt{I}$$

by Lemma 3.4.2 in [16]. This completes the proof. □

2. Separating subsets for groups acting diagonally

In this section we consider an abelian group G that acts by a diagonal matrix on $\mathbb{F}[V] = \mathbb{F}[x_1, \ldots, x_n]$. As it turns out, in this case we can describe a separating subset (and thus separating subalgebra) that consists solely of monomials.

Let $\kappa(G)$ denote the character group of G over $\mathbb{F}$. For each $1 \leq i \leq n$, let χ_i be the element in $\kappa(G)$ such that $g(x_i) = \chi_i(g)x_i$.

The corresponding ring of invariants $\mathbb{F}[V]^G$ is generated by monomials, see, e.g., Lemma 7.3.5 in [12]. Furthermore, a monomial $\mathbf{m} = x_1^{e_1} x_2^{e_2} \cdots x_n^{e_n}$ is invariant if and only if $e_1\chi_1 + e_2\chi_2 + \cdots + e_n\chi_n = 0$ in $\kappa(G)$.

To each subset $\mathcal{S} \subseteq \{1, 2, \ldots, n\}$ we associate an invariant monomial in the following way. Set

$$M(\mathcal{S}) = \{x_1^{e_1} x_2^{e_2} \cdots x_n^{e_n} \in \mathbb{F}[V]^G |\, e_j = 0 \text{ for } j \notin \mathcal{S}\} \subseteq \mathbb{F}[V]^G.$$

Denote by $i = i(\mathcal{S})$ the smallest integer in $\mathcal{S}$. Define $\mathcal{A} = \mathcal{A}(\mathcal{S}) \subseteq \mathbb{N}$ to be the set of positive integers a such that there exists a monomial $x_i^{e_i} \cdots x_n^{e_n}$ in $M(\mathcal{S})$ such that $e_i = a$.

We note that $\mathcal{A}$ is not empty since it contains o_i, the order of χ_i in $\kappa(G)$.

For $a, b \in \mathcal{A}$ with $a > b$, we have that $a - b \in \mathcal{A}$ as can be seen as follows. By construction there are two invariants

$$x_i^{e_i} \cdots x_n^{e_n} \quad \text{and} \quad x_i^{f_i} \cdots x_n^{f_n} \in M(\mathcal{S})$$

and thus we obtain two equations

$$e_i\chi_i + \cdots + e_n\chi_n = 0 \quad \text{and} \quad f_i\chi_i + \cdots + f_n\chi_n = 0$$

such that $e_i = a$, $f_i = b$, and $e_j = f_j = 0$ for $j \notin \mathcal{S}$. Taking the difference of these equations yields

$$(e_i - f_i)\chi_i + \cdots + (e_n - f_n)\chi_n = 0,$$

with $e_i - f_i = a - b$. The coefficients of this equation are not necessarily non-negative. However, since G is finite, we can choose for each $1 \leq j \leq n$, a positive integer (namely, the order of χ_j) o_j such that $o_j \chi_j = 0$. Therefore by adding enough positive multiples of $o_j \chi_j$ for $j \in \mathcal{S} \setminus \{i\}$, we get an equation

$$h_i \chi_i + \cdots + h_n \chi_n = 0$$

with $h_i = a - b$, $h_j \geq 0$ for $j \in \mathcal{S}$ and $h_j = 0$ for $j \notin \mathcal{S}$. It follows that $\mathcal{A} \cup \{0\}$ is a lattice in $\mathbb{N}_0$ and hence generated by its smallest positive member, say $a_{\min}$. Let

$$\mathbf{m}_{\mathcal{S}} = x_i^{e_i} \cdots x_n^{e_n} \in M(\mathcal{S})$$

be the smallest monomial in $M(\mathcal{S})$ with respect to lexicographic order with $x_1 > x_2 > \cdots > x_n$ such that $e_i = a_{\min}$. Note that our definition does not place a monomial in a unique $M(\mathcal{S})$ but $\mathbf{m}_{\mathcal{S}}$ is well defined. We show that the collection of these monomials $\mathbf{m}_{\mathcal{S}}$, for every $\emptyset \neq \mathcal{S} \subseteq \{1, \ldots, n\}$ is separating. We remark that both Propositions 5 and 6 are motivated by Example 1.5 in [11] and the argument there.

Proposition 5. *The set $\mathcal{T} = \{\mathbf{m}_{\mathcal{S}} \mid \emptyset \neq \mathcal{S} \subseteq \{1, 2, \ldots, n\}\}$ is separating. Note that the size of $\mathcal{T}$ is $2^n - 1$.*

Proof. We assume to the contrary that the monomials in $\mathcal{T}$ do not separate the distinct orbits $[\mathbf{v}], [\mathbf{w}] \in V/G$. We will show that this implies that $\mathbf{m}(\mathbf{v}) = \mathbf{m}(\mathbf{w})$ for any invariant monomial $\mathbf{m}$, and hence for any invariant, which is the desired contradiction. Let

$$\mathbf{m} = x_1^{e_1} x_2^{e_2} \cdots x_n^{e_n} \in \mathbb{F}[V]^G.$$

Denote by $\mathcal{S}$ the complement in $\{1, 2, \ldots, n\}$ of $\{j \mid \ e_j = 0\}$. Thus $\mathbf{m} \in M(\mathcal{S})$. We proceed by induction on the order of $\mathcal{S}$.

If $|\mathcal{S}| = 1$, say $\mathcal{S} = \{j\}$, then $\mathbf{m} = x_j^{t \cdot o_j}$ for some positive integer t, since $\mathbf{m}$ is invariant. Furthermore, $\mathbf{m}_{\mathcal{S}} = x_j^{o_j} \in \mathcal{T}$. Since we are assuming the monomials in $\mathcal{T}$ do not separate $\mathbf{v} = (v_1, \ldots, v_n)$ and $\mathbf{w} = (w_1, \ldots, w_n)$ we find that

$$\mathbf{m}(\mathbf{v}) = v_j^{t \cdot o_j} = w_j^{t \cdot o_j} = \mathbf{m}(\mathbf{w}).$$

Since this is true for any choice of j we are done.

Next, we assume that $|\mathcal{S}| > 1$, and the result has been proven for sets of smaller size.

Let i denote the smallest integer in $\mathcal{S}$. By construction there exists a positive integer r such that the monomial

$$\mathbf{m}_{\mathcal{S}}^r = x_i^{f_i} \cdots x_n^{f_n}$$

satisfies $e_i = f_i$. Hence,

$$\frac{\mathbf{m}}{\mathbf{m}_{\mathcal{S}}^r} = \frac{x_{i+1}^{e_{i+1}} \cdots x_n^{e_n}}{x_{i+1}^{f_{i+1}} \cdots x_n^{f_n}} \in \mathbb{F}(V)^G.$$

is a rational invariant.

Let $\mathcal{J}$ denote the set of indices j such that x_j appears in the denominator of $\frac{\mathbf{m}}{\mathbf{m}_{\mathcal{S}}^r}$. Since $x_j^{o_j}$ is an invariant for all $j \in \mathcal{J}$, it follows that for some suitably large $t \in \mathbb{N}$

$$\mathbf{m}' := \frac{\mathbf{m}}{\mathbf{m}_{\mathcal{S}}^r} \prod_{j \in \mathcal{J}} x_j^{t o_j} \in \mathbb{F}[V]^G$$

is an invariant monomial. Moreover, since x_i does not appear in $\mathbf{m}'$ and all the indices of the variables that appear in $\mathbf{m}'$ come from $\mathcal{S}$, we have $\mathbf{m}' \in M(\mathcal{S}')$ for some $\mathcal{S}' \subsetneq \mathcal{S}$. Consider

$$\mathbf{m} = \frac{\mathbf{m}' \cdot \mathbf{m}_{\mathcal{S}}^{r}}{\prod_{j \in \mathcal{J}} x_j^{o_j}}.$$

Since $\mathbf{m}_{\mathcal{S}} \in \mathcal{T}$, the monomial $\mathbf{m}_{\mathcal{S}}^{r}$ does not separate $\mathbf{v}$ and $\mathbf{w}$. Moreover, by our induction hypothesis $\mathbf{m}' \in M(\mathcal{S}')$ and $\prod_{j \in \mathcal{T}} x_j^{o_j} \in M(\mathcal{J})$ do not separate $\mathbf{v}$ and $\mathbf{w}$ either, because $\mathcal{S}', J \subsetneq \mathcal{S}$. But the value of $\mathbf{m}$ at a point is uniquely determined by $\mathbf{m}'$, $\mathbf{m}_{\mathcal{S}}$ and $\prod_{j \in \mathcal{J}} x_j^{o_j}$ if $\prod_{j \in \mathcal{J}} x_j^{o_j}$ is non-zero at that point. Therefore $\mathbf{m}$ does separate $\mathbf{v}$ and $\mathbf{w}$ if $\prod_{j \in \mathcal{J}} x_j^{o_j}$ is non-zero at one (hence both) of $\mathbf{v}$ and $\mathbf{w}$.

On the other hand if $\prod_{j \in \mathcal{J}} x_j^{o_j}$ vanishes at a point, then $\mathbf{m}$ also vanishes at that point because $\mathcal{J} \subseteq \mathcal{S}$, namely if a variable appears in $\prod_{j \in \mathcal{J}} x_j^{o_j}$, it also appears in $\mathbf{m}$.

Finally, the monomial $\mathbf{m}_{\emptyset}$ corresponding to empty set is just 1, hence it is not needed in a separating set. This completes the proof. □

Meanwhile the separating set in Proposition 5 can be improved substantially for cyclic groups of prime order as we show in the next proposition. However note that the respective sizes of the separating sets of these propositions coincide for $n = 2$.

Proposition 6. *Let G be a cyclic group of prime order. Furthermore assume that $n \geq 2$ and $\chi_j \neq 0$ for $1 \leq j \leq n$. Then*

$$\mathcal{T} = \{\mathbf{m}_{\mathcal{S}} \mid \mathcal{S} \subseteq \{1, 2, \ldots, n\} \text{ and } |\mathcal{S}| = 1, 2\}$$

is separating. Note that the size of $\mathcal{T}$ is $\frac{n^2+n}{2}$.

Proof. Since we are assuming non-trivial characters exist, we have $\kappa(G) \cong G$.

Let $|\mathcal{S}| = 1$, say $\mathcal{S} = \{j\}$, then $\mathbf{m}_{\mathcal{S}} = x_j^{o_j}$. Assume next that $|\mathcal{S}| = 2$ with $\mathcal{S} = \{i, j\}$ and $i < j$. Since $\kappa(G)$ is cyclic of prime order and $\chi_i, \chi_j \neq 0$ there exists a unique positive integer $a_{i,j} < o_j$ such that

$$\chi_i + a_{i,j}\chi_j = 0 \in \kappa(G).$$

Hence $x_i x_j^{a_{i,j}}$ is an invariant monomial. Since $a_{i,j}$ is the smallest among the positive integers k such that $x_i x_j^k$ is invariant it follows that $\mathbf{m}_{\mathcal{S}} = x_i x_j^{a_{i,j}}$. Thus we have obtained

$$\mathcal{T} = \{x_j^{o_j}\}_{1 \leq j \leq n} \cup \{x_i x_j^{a_{i,j}}\}_{1 \leq i < j \leq n}.$$

From this point on, the proof of the previous proposition carries over: We assume that the monomials in $\mathcal{T}$ do not separate the vectors $\mathbf{v}, \mathbf{w} \in V$ with distinct G-orbits. Let $\mathbf{m} = x_1^{e_1} x_2^{e_2} \cdots x_n^{e_n}$ be an arbitrary invariant monomial and let $\mathcal{S}$ denote the complement in $\{1, 2, \ldots, n\}$ of $\{j \mid \ e_j = 0\}$. Then $\mathbf{m} \in M(\mathcal{S})$. Let i be the smallest integer in $\mathcal{S}$. We proceed by induction on $|\mathcal{S}|$.

If $|\mathcal{S}| = 1$, then $\mathbf{m} = x_i^{t \cdot o_i}$ for some positive integer o_i. But, being in $\mathcal{T}$, $x_i^{o_i}$ does not separate $\mathbf{v}$ and $\mathbf{w}$. Therefore $\mathbf{m} = x_i^{t \cdot o_i}$ does not either.

Assume next $|\mathcal{S}| \geq 2$. Pick $j \in \mathcal{S}$ with $j > i$. Then x_i does not appear in

$$\frac{\mathbf{m}}{(x_i x_j^{a_{i,j}})^{e_i}} = \frac{x_{i+1}^{e_{i+1}} \cdots x_n^{e_n}}{x_j^{a_{i,j} e_i}}.$$

It follows that for sufficiently large $t \in \mathbb{N}$

$$\mathbf{m} = \frac{\mathbf{m}'(x_i x_j^{a_{i,j}})^{e_i}}{x_j^{to_j}},$$

for some $\mathbf{m}'$ that lies in $M(\mathcal{S}')$ for some proper subset $\mathcal{S}'$ in $\mathcal{S}$. The value of $\mathbf{m}$ at a point is uniquely determined by $\mathbf{m}'$, $(x_i x_j^{a_{i,j}})^{e_i}$ and $x_j^{o_j}$, if j-th coordinate of that point is non-zero. In this case $\mathbf{m}$ does not separate $\mathbf{v}$ and $\mathbf{w}$ by induction since $\mathbf{m}' \in M(\mathcal{S}')$ and $x_j^{o_j}, x_i x_j^{a_{i,j}} \in \mathcal{T}$. On the other hand if $x_j^{o_j}(\mathbf{v}) = 0$ (hence $x_j^{o_j}(\mathbf{w}) = 0$), then $\mathbf{m}(\mathbf{v}) = \mathbf{m}(\mathbf{w}) = 0$ as well since $j \in S$, i.e., x_j appears in $\mathbf{m}$. □

References

[1] H. Derksen and G. Kemper, Computational invariant theory, Invariant Theory and Algebraic Transformation Groups, I, Springer-Verlag, Berlin (2002), ISBN 3-540-43476-3. Encyclopaedia of Mathematical Sciences, 130.

[2] ———, *Computing invariants of algebraic groups in arbitrary characteristic*, Adv. Math. **217** (2008), no. 5, 2089–2129.

[3] M. Domokos, *Typical separating invariants*, Transform. Groups **12** (2007), no. 1, 49–63.

[4] M. Domokos and E. Szabó, *Helly dimension of algebraic groups*, preprint, arXiv:0911.0404v2 (2009)

[5] J. Draisma, G. Kemper, and D. Wehlau, *Polarization of separating invariants*, Canad. J. of Math. **60** (2008) 556–571.

[6] E. Dufresne, *Separating invariants*, Ph.D. Thesis, Queen's University, Kingston, Ontario (2008)

[7] ———, *Separating invariants and finite reflection groups*, Adv. Math. **221** (2009), no. 6, 1979–1989.

[8] P. Fleischmann, *Relative trace ideals and Cohen-Macaulay quotients of modular invariant rings*, in Computational methods for representations of groups and algebras (Essen, 1997), Vol. 173 of *Progr. Math.*, 211–233, Birkhäuser, Basel (1999).

[9] P. Fleischmann, M. Sezer, R. J. Shank, and C. F. Woodcock, *The Noether numbers for cyclic groups of prime order*, Adv. Math. **207** (2006), no. 1, 149–155.

[10] I. Hughes and G. Kemper, *Symmetric powers of modular representations, Hilbert series and degree bounds*, Comm. Algebra **28** (2000), no. 4, 2059–2088.

[11] G. Kemper, *Separating invariants*, J. Symbolic Comput. **44** (2009) 1212–1222.

[12] M. Neusel and L. Smith, Invariant theory of finite groups, Vol. 94 of *Mathematical Surveys and Monographs*, American Mathematical Society, Providence, RI (2002), ISBN 0-8218-2916-5.

[13] M. D. Neusel, *The Transfer in the Invariant Theory of Modular Permutation Representations*, Pacific J. of Math. **199** (2001), no. 1, 121–135.

[14] M. D. Neusel and M. Sezer, *The invariants of modular indecomposable representations of* $\mathbb{Z}_{p^2}$, Math. Ann. **341** (2008), no. 3, 575–587.

[15] ———, *The Noether map. I*, Forum Math. **21** (2009), no. 4, 567–578.

[16] P. E. Newstead, Introduction to moduli problems and orbit spaces, Vol. 51 of *Tata Institute of Fundamental Research Lectures on Mathematics and Physics*, Tata Institute of Fundamental Research, Bombay (1978), ISBN 0-387-08851-2.

[17] M. Sezer, *Constructing modular separating invariants*, J. Algebra **322** (2009), no. 11, 4099–4104.

[18] L. Smith and R. E. Stong, *Invariants of binary bilinear forms modulo two*, Proc. Amer. Math. Soc. **138** (2010) 17–26.

Department of Math. and Stats., Texas Tech University, MS 1042 Lubbock, TX 79409, USA

E-mail address: `Mara.D.Neusel@ttu.edu`

Department of Mathematics, Bilkent University, Ankara 06800, Turkey

E-mail address: `sezer@fen.bilkent.edu.tr`