CHARACTERIZING SEPARATING INVARIANTS

DEDICATED TO LUCHO AVRAMOV ON THE OCCASION OF HIS 60TH BIRTHDAY

MARA D. NEUSEL AND MÜFİT SEZER

ABSTRACT. We study separating algebras for rings of invariants of finite groups. We give an algebraic characterization for these. Furthermore, we describe a particularly nice separating subalgebra for rings of invariants of p-groups in characteristic p. This leads to a characterization of subalgebras such that their p-root and integral closure is equal to the ring of invariants (see Property ($\star$) below). Finally, we present separating sets for invariants rings of nonmodular representations of abelian groups whose size depends only on the degree of the representation.

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.,

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

This notion was introducted in Definition 2.3.8 in [2]. Denote by $\overline{A}$ the integral closure of the algebra A (in its field of fractions) and by $\sqrt{A}$ its p-root closure in $\mathbb{F}[V]$, where p is the characteristic of $\mathbb{F}$. In Theorem 2.3.12 ibid. it is shown that

$$\sqrt{\overline{A}} = \mathbb{F}[V]^G, \tag{$\star$}$$

provided that $A \subseteq \mathbb{F}[V]^G$ is a finitely generated separating graded subalgebra. The converse is not valid, see Example 2.3.14 ibid.

Remark 1. We note that for fields that are not algebraically closed, the notion "separating" does not make sense. 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 [11]. The vector space

Date: April 10, 2008, 14 h 29 min.

$V = \operatorname{span}_{\mathbb{F}_2}\{\mathbf{e}_1, \mathbf{e}_2\}$ 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. 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 $\overline{V} = \operatorname{span}_{\overline{\mathbb{F}}}\{\mathbf{e}_1, \mathbf{e}_2\}$ 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., [7], [3], [4], [2] 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 [2], or, separating invariants of vector invariants can be obtained by polarizations, see [4]. 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 for the invariants are known are the (all of them) representations of cyclic groups of order p, see [6], and the indecomposable representations of cyclic groups of order p^2, see [10]. 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 want to show that in contrast norms and transfers suffice to *separate* orbits for *all* representations of *any* p-group. This study, moreover, will enable us to characterize subalgebras $A \subseteq \mathbb{F}[V]^P$ satisfying Property $(\star)$.

In Section 2 we turn to the other extreme: We will consider nonmodular representations of abelian groups. With Noether's bound, generating sets of the ring of invariants can be easily described leading to an upper estimate on the *number* of generators depending on the group order and the degree of the representation. However, again separating invariants have yet a simpler structure: We will describe separating sets whose size depends only on the degree of the representation.

We close the introduction with a characterization of separating subalgebras in algebraic terms.

Theorem 2. *Let $\rho : G \hookrightarrow \mathsf{GL}(n,\ \mathbb{F})$ be a faithful representation of a finite group G over some algebraically closed field $\mathbb{F}$. Then a finitely generated subalgebra $A \subseteq \mathbb{F}[V]^G$ is separating if and only if the following two conditions are satisfied:*

(1) The extension $\phi : A \hookrightarrow \mathbb{F}[V]^G$ is integral.

(2) The induced map

$$\phi^* : \operatorname{Max}(\mathbb{F}[V]^G) \longrightarrow \operatorname{Max}(A)$$

between the spectra of maximal ideals is bijective.

Proof. Choose coordinates for V^* and write $\mathbb{F}[V] = \mathbb{F}[x_1, \ldots, x_n]$. For any point $\mathbf{v} = (v_1, \ldots, v_n) \in V$ we obtain a maximal ideal

$$\mathfrak{m}_{\mathbf{v}} = (x_1 - v_1, \ldots, x_n - v_n) \subsetneq \mathbb{F}[V].$$

Two maximal ideals $\mathfrak{m}_{\mathbf{v}}$ and $\mathfrak{m}_{\mathbf{w}}$ coincide upon contraction to $\mathbb{F}[V]^G$,

$$\mathfrak{m}_{\mathbf{v}} \cap \mathbb{F}[V]^G = \mathfrak{m}_{\mathbf{w}} \cap \mathbb{F}[V]^G$$

if and only if $\mathbf{v}$ and $\mathbf{w}$ lie in the same G-orbit. Thus the spectrum of maximal ideal in $\mathbb{F}[V]^G$ is given by

$$\operatorname{Max}(\mathbb{F}[V]^G) = \{\mathfrak{m}_{\mathbf{v}} \cap \mathbb{F}[V]^G | [\mathbf{v}] \in V/G\}.$$

If A is separating, then the extension $A \hookrightarrow \mathbb{F}[V]^G$ is integral by Theorem 2.3.12 in [2]. Thus, the induced map on the spectra of maximal ideals is surjective. Furthermore, for any two points $\mathbf{v}, \mathbf{w} \in V$ lying in different G-orbits, there is a function $f \in A$ such that

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

The function $f - f(\mathbf{w})$ separates the two points as well and moreover vanishes at $\mathbf{w}$. Thus we may assume that $f \in \mathcal{J}(\mathbf{w}) = \mathfrak{m}_{\mathbf{w}} \subseteq \mathbb{F}[V]$ is contained in the vanishing ideal of the point $\mathbf{w}$, but $f \notin \mathcal{J}(\mathbf{v}) = \mathfrak{m}_{\mathbf{v}}$. Thus

$$f \in \mathfrak{m}_{\mathbf{w}} \cap A \quad \text{but} \quad f \notin \mathfrak{m}_{\mathbf{v}} \cap A.$$

Therefore, the induced map on the spectra of maximal ideals is also injective.

Conversely, if A satisfies the two conditions mentioned above, then for any two distinct G-orbits $[\mathbf{v}]$ and $[\mathbf{w}]$ we find

$$\mathfrak{m}_{\mathbf{v}} \cap A \neq \mathfrak{m}_{\mathbf{w}} \cap A.$$

Therefore, there is a function $f \in A$ vanishing on $\mathbf{v}$ but not on $\mathbf{w}$ (and vice versa). Thus A is separating. □

Since p-root extensions form a relatively nice subset of integral extensions we have the following characterization.

Proposition 3. *Let $\rho : G \hookrightarrow \mathsf{GL}(n, \mathbb{F})$ be a faithful representation of a finite group G over some algebraically closed field $\mathbb{F}$. Then a finitely generated integrally closed graded subalgebra $A \subseteq \mathbb{F}[V]^G$ is separating if and only if $\sqrt{\overline{A}} = \mathbb{F}[V]^G$. Furthermore, in that case the induced map on the prime ideal spectra*

$$\operatorname{Spec}(\mathbb{F}[V]^G) \longrightarrow \operatorname{Spec}(\overline{A})$$

is bijective.

Proof. If $\mathbb{F}$ has characteristic zero, then an integrally closed separating subalgebra A is equal to the ring of invariants, since there are no nontrivial purely inseparable extensions.

Thus let $\mathbb{F}$ have finite characteristic. If A is separating, then

$$\sqrt{\overline{A}} = \sqrt{A} = \mathbb{F}[V]^G$$

by Theorem 2.3.12 in [2]. Conversely, if $\sqrt{A} = \mathbb{F}[V]^G$, then there exists an integer $s \in \mathbb{N}_0$ such that

$$\sqrt{A}^{p^s} \subseteq A \subseteq \sqrt{A} = \mathbb{F}[V]^G.$$

Since with $\sqrt{A}$ also $\sqrt{A}^{p^s}$ is separating, so is A.

The last statement follows by Exercise 15 in Chapter 5 of [1]. □

Corollary 4. *Let $\rho : G \hookrightarrow \mathsf{GL}(n,\ \mathbb{F})$ be a faithful representation of a finite group G over some algebraically closed field $\mathbb{F}$. Let $A \subseteq \mathbb{F}[V]^G$ be a finitely generated graded subalgebra. If $\sqrt{A} = \mathbb{F}[V]^G$ then A is separating.*

Proof. Immediate from the preceding result. □

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. 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 [11],

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

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 [11]. This does not remain true in the modular case. However, as shown in Proposition 2.2 of [9] the p-root closure of the image of the Noether map is equal to $\mathbb{F}[V]^G$. Thus, by the preceding result, 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. This result is particularly interesting because it gives rise to a characterization of subalgebras satisfying Property $(\star)$.

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

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

We obtain 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.

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 [5] generalizing Feshbach's Transfer Theorem.

Lemma 5. *The zero set of I in V/G is equal to the fixed point space of G*

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

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

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

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

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

Let H be a maximal subgroup of G containing $G_{\mathbf{v}}$. Since $G_{\mathbf{v}} \subseteq H$, we have $\mathrm{Im}(\mathsf{Tr}_{G_{\mathbf{v}}}^G) \subseteq \mathrm{Im}(\mathsf{Tr}_H^G)$. It follows that $\mathbf{v} \notin \mathcal{V}(\mathrm{Im}(\mathsf{Tr}_H^G))$ 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 6. *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 $\mathsf{Tr}_Q^P(h)(\mathbf{v}) \neq 0$.

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

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

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

[1] An exception would be vector invariants of the regular representation of the cyclic group of order p. Indeed, a very special case. See [8]

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 $\{\mathbf{e}_1, \dots, \mathbf{e}_k\}$ 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 $i_0 \in \{1, \dots, k\}$ 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, $\mathsf{N}(x_{i_0})(\mathbf{v}) \neq \mathsf{N}(x_{i_0})(\mathbf{w})$. Thus $\mathsf{N}(x_{i_0})$ separates $\mathbf{v}$ and $\mathbf{w}$ as desired. □

The preceding result enables us to describe the radical of the ideal I, see Corollary 12.3 [5] 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 7. *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 we obtain the prime ideal*

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

Proof. By Lemma 5, 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 $i \notin \{1, \dots, k\}$, it is a prime ideal. Therefore, 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 it follows that

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

by Lemma 3.4.2 in [12]. □

Theorem 6 also enables us to characterize the set of algebras A with Property $(\star)$ in the case of p-groups. We need a preliminary lemma.

Lemma 8. *Let $A \subseteq \mathbb{F}[V]$ be a finitely generated $\mathbb{F}$-algebra. Then $\sqrt{\overline{A}}$ is integrally closed (in its field of fractions).*

Proof. Denote by $\mathsf{FF}(-)$ the field of fraction functor.

If $\mathsf{FF}(A) = \mathsf{FF}(\sqrt{\overline{A}})$, then $\overline{A} = \sqrt{\overline{A}}$, and thus the latter is integrally closed.

In general though

$$\mathsf{FF}(A) = \mathsf{FF}(\overline{A}) \hookrightarrow \mathsf{FF}(\sqrt{\overline{A}})$$

is a nontrivial purely inseparable extension. We note that by definition the extension

$$A \hookrightarrow \overline{A} \hookrightarrow \sqrt{\overline{A}}$$

is integral. Now, let $a \in \mathsf{FF}(\sqrt{\overline{A}})$ be integral over $\sqrt{\overline{A}}$. Let

$$a^m + \alpha_{m-1} a^{m-1} + \cdots + \alpha_1 a + \alpha_0 = 0$$

be a relation of integral dependence, where $\alpha_i \in \sqrt{\overline{A}}$ for all i. Thus, $\alpha_i^{p^s} \in \overline{A}$ and $a^{p^s} \in \mathsf{FF}(A)$ for some large $s \in \mathbb{N}$. In orther words, $a^{p^s} \in \mathsf{FF}(A)$ is integral over $\overline{A}$ and hence in $\overline{A}$. Thus $a \in \sqrt{\overline{A}}$ by definition. □

Theorem 9. *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. Let $A \subseteq \mathbb{F}[V]^P$ be a subalgebra. Then $\sqrt{\overline{A}} = \mathbb{F}[V]^P$ if and only if the following two conditions are satisfied:*

(1) The extension $A \hookrightarrow \mathbb{F}[V]^P$ is integral.

(2) There exists a $t \in \mathbb{N}_0$ such that $I^{p^t} \subseteq \overline{A}$.

Proof. If $A \subseteq \mathbb{F}[V]^P$ has Property $(\star)$ then the extension

$$A \hookrightarrow \mathbb{F}[V]^G$$

is integral. Furthermore, $\sqrt{\overline{A}} = \mathbb{F}[V]^P$ contains the image of the relative transfers Tr_Q^P for every maximal subgroup $Q \leq P$. Since rings of invariants are Noetherian, the image of any (relative) transfer is finitely generated. Thus there exist $s = s(Q) \in \mathbb{N}_0$ such that

$$(\mathrm{Im}(\mathsf{Tr}_Q^P))^{p^s} \subseteq \overline{A}$$

for all maximal subgroups $Q \leq P$. Furthermore, a finite group has only finitely many maximal subgroups. Thus setting

$$t = \max\{s(Q) | Q < P \text{ maximal}\}$$

yields a universal power such that

$$I^{p^t} \subseteq \overline{A}.$$

To prove the converse we assume that the two properties listed above are satisfied. Thus the image of the relative transfers Tr_Q^P is contained in $\sqrt{\overline{A}} \hookrightarrow \mathbb{F}[V]^P$. We obtain an algebraic extension of the associated fields of fractions as follows

$$\mathsf{ff}(\mathbb{F}[\mathrm{Im}(\sum_Q \mathsf{Tr}_Q^P)]) \subseteq \mathsf{ff}(\sqrt{\overline{A}}) \subseteq \mathbb{F}(V)^P.$$

Since the transfer is surjective at the level of fields of fractions, see Proposition 1.1 in [9], we have

$$\mathbb{F}(V)^P = \mathsf{ff}(\mathbb{F}[\mathrm{Im}(\sum_Q \mathsf{Tr}_Q^P)]).$$

Thus $\mathsf{ff}(\sqrt{\overline{A}}) = \mathbb{F}(V)^P$. Since $\sqrt{\overline{A}}$ is integrally closed by Lemma 8 it follows that $\sqrt{\overline{A}} = \mathbb{F}[V]^P$. □

2. Separating subsets for non-modular abelian groups

In this section we consider finite abelian groups G and nonmodular representations thereof, i.e., $|G| \in \mathbb{F}^\times$. The field $\mathbb{F}$ continues to be algebraically closed, thus $\mathbb{F}$ contains all $|G|$-th roots of unity. As it turns out, in this case we can not only describe a separating subset (and thus separating subalgebra), but also give a sharp upper bound on its order.

Let $\kappa(G)$ denote the character group of G over $\mathbb{F}$. Since every representation of G over $\mathbb{F}$ is diagonalizable, there exists a basis $\{x_1, x_2, \ldots, x_n\}$ of V^* such that $g(x_i) = \chi_i(g)x_i$, with $\chi_i \in \kappa(G)$ for $1 \leq i \leq n$.

The corresponding ring of invariants $\mathbb{F}[V]^G$ is generated by monomials, see, e.g., Lemma 7.3.5 in [11]. 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 $\mathcal{S} \subseteq \{1, 2, \dots, n\}$ 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 $M(\mathcal{S})$ w.r.t. lexicographic order with $x_1 > x_2 > \cdots > x_n$ such that $e_i = a_{\min}$. We show that the collection of these monomials $\mathbf{m}_{\mathcal{S}}$, for every $\mathcal{S} \subseteq \{1, \dots, n\}$ is separating.

Proposition 10. *The set $\mathcal{T} = \{\mathbf{m}_{\mathcal{S}} | \mathcal{S} \subseteq \{1, 2, \dots, n\}\}$ is separating. In particular, the minimal size of a separating set is at most $2^n - 1$.*

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 $\{1, 2, \dots, n\}$ 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 $\mathbf{v} = (v_1, \dots, v_n)$ and $\mathbf{w} = (w_1, \dots, w_n)$ 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 $t \in \mathbb{N}$

$$\mathbf{m}' := \frac{\mathbf{m}}{\mathbf{m}_{\mathcal{S}}^r} \prod_{j \in \mathcal{J}} x_j^{to_j} \in \mathbb{F}[V]^G$$

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. □

We demonstrate in the following example that the bound of the previous proposition is sharp.

Example. Let $G = \mathbb{Z}_3$ be the cyclic group of order 3 acting diagonally on the polynomial ring $\mathbb{C}[x_1, x_2]$ with complex coefficients by $\sigma(x_i) = \lambda x_i$ for $1 \leq i \leq 1$, where λ is a primitive 3rd root of unity and σ is a generator of G. The invariant ring is minimally generated by $\{x_1^3, x_1^2 x_2, x_1 x_2^2, x_2^3\}$. As the previous proposition predicts, the set $\{x_1^3, x_1 x_2^2, x_2^3\}$ is separating. If there were a separating set consisting of two elements, say f_1, f_2, then $\mathbb{C}[f_1, f_2] \subseteq \mathbb{C}[x_1, x_2]^G$ is a finite extension and moreover $\mathbb{C}[x_1, x_2]^G$ is the normalization of $\mathbb{C}[f_1, f_2]$, because there are no nontrivial purely inseparable extensions in characteristic zero. But this is impossible because $\mathbb{C}[f_1, f_2]$ is a regular ring and hence is integrally closed.

Meanwhile the separating set in Proposition 10 can be refined substantially for cyclic groups of prime order as we show next.

Proposition 11. *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*

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

is separating. Note that the order of $\mathcal{T}$ does not exceed $\frac{n^2+n}{2}$.

Proof. 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 invariants 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] M.F. Atiyah and I.G. Macdonald. *Introduction to Commutative Algebra*. Addison-Wesley Publishing Company, Reading, MA, 1969.

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

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

[4] J. Draisma, G. Kemper, and D. Wehlau. Polarization of separating invariants. *to appear in Canad. J. Math.*, 2006.

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

[6] 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.

[7] G. Kemper. Separating invariants. *preprint available at http://www-m11.ma.tum.de/ kemper/publications.html*, 2007.

[8] M. D. Neusel. The transfer in the invariant theory of modular permutation representations. *Pacific J. of Math.*, 199(1):121–135, 2001.

[9] M. D. Neusel and M. Sezer. The Noether map I. *to appear in Forum Math.*, 2007.

[10] M. D. Neusel and M. Sezer. Invariants of modular indecomposable representations of $\mathbb{Z}_{p^2}$. *to appear in Math. Ann.*, 2008.
[11] M.D. Neusel and L. Smith. *Invariant theory of finite groups*, volume 94 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI, 2002.
[12] P. E. Newstead. *Introduction to moduli problems and orbit spaces*, volume 51 of *Tata Institute of Fundamental Research Lectures on Mathematics and Physics*. Tata Institute of Fundamental Research, Bombay, 1978.

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