



Full Length Article

Separating polynomial invariants over non-closed fields of finite abelian groups

Mátyás Domokos 

HUN-REN Alfréd Rényi Institute of Mathematics, Reáltanoda utca 13-15., Budapest, 1053, Hungary

ARTICLE INFO

Communicated by Radu Balan

2000 MSC:

13A50

13P15

20C15

94A12

Keywords:

Polynomial invariants

Separating sets

Degree bounds

Finite abelian groups

Multireference alignment

Regular representation

ABSTRACT

It is proved that for any finite dimensional representation of a prime order group over the field of rational numbers, polynomial invariants of degree at most 3 separate the orbits. A result providing an upper degree bound for separating invariants for representations of finite abelian groups over algebraically closed base fields of non-modular characteristic is generalized for the case of base fields that are not algebraically closed (like the fields of real or rational numbers).

1. Introduction

This work is largely motivated by [1], where the authors develop an approach to multireference alignment using invariant theory. Multireference alignment is a basic problem in applied mathematics, which arose in connection with structural biology, image recognition, and signal processing (see e.g. the introduction of [2]). It was shown in [3] that the sample complexity of multireference alignment (an orbit recovery problem for the cyclic group C_n acting by cyclic shifts on the space $\mathbb{R}^n$) depends on the degree of invariants necessary to separate generic orbits. In particular, in [1, Theorem 4.1] a Galois theoretic proof is given for the fact that for the regular representation over $\mathbb{R}$ of a finite abelian group, the field of rational invariants is generated by polynomial invariants of degree at most 3 (and hence generic orbits can be separated by polynomial invariants of degree at most 3). This is in fact a special case of a theorem on the regular representation of an arbitrary finite group (see [1, 4, Remark 4.3]; a generalization is given in [5]), but here first we shall focus on the special case of cyclic groups of prime order p . It is proved in [6, Proposition 3.13] that for a faithful finite dimensional real representation of C_p , polynomial invariants of degree smaller than p are not sufficient to separate all the orbits. In sharp contrast with that result, our Theorem 1 says that different orbits in $\mathbb{Q}^p$ under the regular representation of C_p can always be separated by invariants of degree at most 3. As a consequence, the same conclusion holds for any finite dimensional representation of C_p over the field $\mathbb{Q}$ of rational numbers. As far as we know, this is the first example in the literature of a finite group whose separating Noether number over an infinite field $\mathbb{F}$ is not equal to its separating Noether number over the algebraic closure

E-mail address: domokos.matyas@renyi.hu<https://doi.org/10.1016/j.acha.2026.101877>

Received 14 July 2025; Received in revised form 2 March 2026; Accepted 6 March 2026

Available online 11 March 2026

1063-5203/© 2026 The Author(s). Published by Elsevier Inc. This is an open access article under the CC BY-NC-ND license (<http://creativecommons.org/licenses/by-nc-nd/4.0/>).

of $\mathbb{F}$ (see Section 2 for the definition of the separating Noether number). Also our Theorem 1 gives the first example of a field $\mathbb{F}$ and an infinite set of pairwise non-isomorphic groups such that the separating Noether numbers over $\mathbb{F}$ of the groups in the given set stay below a uniform upper bound. Note that a similar scenario does not occur for the ordinary Noether number (defined in terms of generating invariants, as opposed to separating invariants), because [7, Theorem 2.1] (and [8] in the modular case) imply that for any field $\mathbb{F}$, any infinite set of pairwise non-isomorphic finite groups contains an element with arbitrarily large Noether number. The study of separating invariants over the field of rational numbers may have interest from the point of view of applications, because the numerical data in applications are rational (have finite decimal representation), so the orbit recovery problem over $\mathbb{Q}$ has relevance.

We provide a theoretical explanation for the phenomenon revealed by Theorem 1 by placing it into a more general context. In fact a second motivation for this paper is that while degree bounds for separating invariants of finite abelian groups over the complex field are relatively well understood (see [9–12]), only sporadic information is available about the exact degree bounds for real representations of these groups. It is desirable to fill in this gap in the literature, because several applications require to work over the real field (see for example the problems mentioned in the introduction of [13], or see [14]). Recall that every representation of a finite abelian group over an algebraically closed base field of non-modular characteristic decomposes as a direct sum of 1-dimensional representations, and therefore the corresponding algebra of polynomial invariants is generated by monomials. Separating sets of monomials were characterized in [9] (see [15] and [16] for similar results on not necessarily finite diagonalizable group actions). Here in Theorem 2 we work out the generalization of this result appropriate for representations of finite abelian groups over non-algebraically closed base fields, where we can not diagonalize a representation. Theorem 2 clarifies the reason why the degree bound for separating invariants is smaller in general, than the corresponding degree bound when we replace the base field by its algebraic closure.

We begin in Section 2 by recalling some basic concepts and notation of invariant theory. In Section 3 we deduce from an observation on the block monoid Proposition 1, which is a variant of [1, Theorem 4.1] about generically separating invariants on the complex regular representation of a finite abelian group. This is then used to prove Theorem 1 on the regular representation of C_p over the field $\mathbb{Q}$ of rational numbers. We conclude Section 4 by Proposition 2 and Proposition 3, showing that Theorem 1 does not generalize for cyclic groups of composite order, or for non-abelian groups. In Section 5 we first recall in Proposition 4 the classification of irreducible representations of a finite abelian group G over a not necessarily algebraically closed base field of non-modular characteristic. We state and prove Theorem 2 giving a sufficient condition for a set of monomials (defined over the algebraic closure of the base field $\mathbb{F}$) to separate the orbits in the regular representation of G over $\mathbb{F}$, and deduce in Corollary 2 an improved bound on the separating Noether number of G over $\mathbb{F}$. This improvement is illustrated by a concrete example in Proposition 5 and Section 6.

2. Preliminaries in invariant theory

Let us recall some standard notation of invariant theory. Throughout this paper G will be a finite group, and $\mathbb{F}$ a field whose characteristic does not divide the order of G . Let V be a finite dimensional vector space over $\mathbb{F}$, endowed with a representation of G on V ; that is, we are given a homomorphism ρ from G into the group $\text{GL}(V)$ of invertible linear transformations of V . Sometimes we shall refer to a representation as the pair (V, ρ) , or we say that V is an $\mathbb{F}G$ -module. Write $\mathbb{F}[V]$ for the coordinate ring of V . This is a polynomial algebra in $\dim_{\mathbb{F}}(V)$ commuting variables endowed with the standard grading (where the variables have degree 1). The variables are thought of as the coordinate functions on V with respect to a chosen basis, and the elements of $\mathbb{F}[V]$ represent $\mathbb{F}$ -valued polynomial functions on V (when $\mathbb{F}$ is infinite, $\mathbb{F}[V]$ can be identified with the algebra of $\mathbb{F}$ -valued polynomial functions on V). We write $\deg(f)$ for the degree of a non-zero element f of $\mathbb{F}[V]$. The action of G on V induces an action of G on $\mathbb{F}[V]$ via graded $\mathbb{F}$ -algebra automorphisms (for $f \in \mathbb{F}[V]$, $g \in G$, $v \in V$ we have $(g \cdot f)(v) = f(g^{-1}v)$), and we denote by $\mathbb{F}[V]^G$ the subalgebra of polynomial G -invariants on V (the polynomials fixed by each group element). This is a graded subalgebra of $\mathbb{F}[V]$. For $v \in V$ we write $G \cdot v \subset V$ for the G -orbit of v . It is immediate from the definition that $G \cdot v = G \cdot w$ implies $f(v) = f(w)$ for all $f \in \mathbb{F}[V]^G$. The converse also holds (see [17, Theorem 3.12.1], [18, Theorem 16] or [19, Lemma 3.1]):

$$G \cdot v \neq G \cdot w \iff \exists f \in \mathbb{F}[V]^G : f(v) \neq f(w). \quad (1)$$

The algebra $\mathbb{F}[V]^G$ is generated by invariants of degree at most $|G|$ (see [20–22]). We shall denote by $\beta_{\text{sep}}(G, V)$ the minimal positive integer d such that for any $v, w \in V$ with $G \cdot v \neq G \cdot w$, there exists an $f \in \mathbb{F}[V]^G$ of degree at most d with $f(v) \neq f(w)$. Furthermore, we write $\beta_{\text{sep}}^{\mathbb{F}}(G)$ for the maximum of $\beta_{\text{sep}}(G, V)$, where V ranges over the finite dimensional $\mathbb{F}G$ -modules. We call $\beta_{\text{sep}}^{\mathbb{F}}(G)$ the *separating Noether number of G over $\mathbb{F}$* ; its study was initiated in [18, 23]. By the facts mentioned above, we have

$$\beta_{\text{sep}}^{\mathbb{F}}(G) \leq \beta^{\mathbb{F}}(G) \leq |G|, \quad (2)$$

where $\beta^{\mathbb{F}}(G)$ is the maximum of $\beta(G, V)$, as V ranges over the finite dimensional $\mathbb{F}G$ -modules, and $\beta(G, V)$ is the maximal degree of an element in a minimal homogeneous generating system of $\mathbb{F}[V]^G$. The study of the *Noether number* $\beta^{\mathbb{F}}(G)$ began in [24], and much of the presently known results on its exact value are summarized in [25].

3. An observation on the block monoid of a finite abelian group

Let G be a finite abelian group, written multiplicatively. Denote by $\mathcal{F}(G, \mathbb{N}_0)$ the set of non-negative integer valued functions on G . This is a commutative monoid, with pointwise addition of functions. It is a submonoid of the abelian group $\mathcal{F}(G, \mathbb{Z})$ of integer valued functions on G , with pointwise addition of functions. Clearly $\mathcal{F}(G, \mathbb{Z})$ is a free abelian group of rank $|G|$. For an element $s \in \mathcal{F}(G, \mathbb{Z})$

we call

$$|s| := \sum_{g \in G} |s(g)|$$

the *length* of s . The element s of $F(G, \mathbb{N}_0)$ can be thought of as a sequence over G of length $|s|$, where the order of the elements in the sequence is disregarded, and $s(g)$ is the number of occurrences of g in the sequence s . The submonoid

$$B(G) := \{s \in F(G, \mathbb{N}_0) \mid \prod_{g \in G} g^{s(g)} = 1_G\} \subseteq F(G, \mathbb{N}_0)$$

is called the *monoid of product-one sequences over G* (it is also called the *block monoid of G* , influenced by the terminology of [26]). The abelian group $F(G, \mathbb{Z})$ is freely generated by $\delta_g, g \in G$, where

$$\delta_g(x) = \begin{cases} 1 & \text{if } x = g; \\ 0 & \text{if } x \neq g. \end{cases} \quad (3)$$

Lemma 1. *The block monoid $B(G)$ is contained in the $\mathbb{Z}$ -submodule of $F(G, \mathbb{Z})$ generated by*

$$S := \{\delta_{1_G}, \delta_g + \delta_{g^{-1}}, \delta_g + \delta_h + \delta_{(gh)^{-1}} \mid g, h, gh \in G \setminus \{1_G\}\}. \quad (4)$$

Proof. Denote by A the $\mathbb{Z}$ -submodule in $F(G, \mathbb{Z})$ given as $A := \{s \in F(G, \mathbb{Z}) \mid \prod_{g \in G} g^{s(g)} = 1_G\}$. Clearly A contains $B(G)$, therefore it is sufficient to show that A is contained in $\langle S \rangle_{\mathbb{Z}}$, the $\mathbb{Z}$ -submodule of $F(G, \mathbb{Z})$ generated by S . Take any $s \in A$. We prove by induction on $|s|$ that s belongs to $\langle S \rangle_{\mathbb{Z}}$. If $|s| = 0$, then s is the zero element of $F(G, \mathbb{Z})$, so it belongs to all $\mathbb{Z}$ -submodules of $F(G, \mathbb{Z})$. Assume next that $|s| > 0$, and all $s' \in A$ with $|s'| < |s|$ belong to $\langle S \rangle_{\mathbb{Z}}$. If $|s| = 1$ then necessarily $s = \delta_{1_G}$ or $-\delta_{1_G}$, so s belongs to $\langle \delta_{1_G} \rangle_{\mathbb{Z}} \subseteq \langle S \rangle_{\mathbb{Z}}$. Moreover, if $s(1_G) \neq 0$, then replacing s by $-s$ if necessary, we may assume that $s(1_G) > 0$, hence for $s' := s - \delta_{1_G} \in A$ we have $|s'| = |s| - 1$. By the induction hypothesis $s' \in \langle S \rangle_{\mathbb{Z}}$, implying in turn that $s = s' + \delta_{1_G} \in \langle S \rangle_{\mathbb{Z}}$. From now on we assume that $s(1_G) = 0$. If $|s| = 2$, then $s \in A$ implies $s = \pm(\delta_g + \delta_{g^{-1}})$, hence $s \in \langle S \rangle_{\mathbb{Z}}$ by definition of S . Assume finally that $|s| \geq 3$. Then $\sum_{s(g) > 0} s(g) \geq 2$ or $\sum_{s(g) < 0} s(g) \leq -2$. Replacing s by $-s$ if necessary we may assume that the first option holds, so there exist elements $g, h \in G \setminus \{1_G\}$ such that for $s' := s - (\delta_g + \delta_h)$ we have $|s'| = |s| - 2$. Set $s'' := s - (\delta_g + \delta_h + \delta_{(gh)^{-1}})$ if $gh \neq 1$ and $s'' := s - (\delta_g + \delta_h)$ if $gh = 1$. Then $s'' \in A$ and $|s''| \leq |s'| + 1 = |s| - 1$, hence $s'' \in \langle S \rangle_{\mathbb{Z}}$ by the induction hypothesis, implying in turn that $s = s'' + (\delta_g + \delta_h + \delta_{(gh)^{-1}}) \in \langle S \rangle_{\mathbb{Z}}$. $\square$

Let K be an extension of $\mathbb{F}$ containing an element of multiplicative order $\exp(G)$, where $\exp(G)$ is the exponent of G (the least common multiple of the orders of the elements of G). For example, we may take for K the algebraic closure of $\mathbb{F}$. Denote by $\hat{G}$ the group of characters of G . That is, $\hat{G}$ is the set of group homomorphisms from G into the multiplicative group of K , endowed with pointwise multiplication. Then $\hat{G}$ is isomorphic to G .

Take a polynomial algebra $K[x_\chi \mid \chi \in \hat{G}]$ whose variables are labeled by the elements of $\hat{G}$. The group G acts on $K[x_\chi \mid \chi \in \hat{G}]$ via K -algebra automorphisms, such that for each $\chi \in \hat{G}$ and $g \in G$ we have

$$g \cdot x_\chi = \chi(g)^{-1} x_\chi.$$

It follows that each monomial spans a G -invariant subspace in the polynomial ring, and for $b \in F(\hat{G}, \mathbb{N}_0)$, the monomial $x^b := \prod_{\chi \in \hat{G}} x_\chi^{b(\chi)}$ is G -invariant if and only if $b \in B(\hat{G})$. Consequently, we have the well known equality

$$K[x_\chi \mid \chi \in \hat{G}]^G = \text{Span}_K \{x^b \mid b \in B(\hat{G})\}. \quad (5)$$

Consider the monomials associated to S (defined in 4):

$$T := \{x^s \mid s \in S\} = \{x_{1_{\hat{G}}}, x_\chi x_{\chi^{-1}}, x_\chi x_\rho x_{(\chi\rho)^{-1}} \mid \chi, \rho, \chi\rho \in \hat{G} \setminus \{1_{\hat{G}}\}\}. \quad (6)$$

Obviously, the elements of T are G -invariant.

The elements of $K[x_\chi \mid \chi \in \hat{G}]$ represent K -valued polynomial functions on the $|\hat{G}|$ -dimensional K -vector space V with basis $\{e_\chi \mid \chi \in \hat{G}\}$, namely for $v = \sum_{\chi \in \hat{G}} v_\chi e_\chi$ and x_ρ we have $x_\rho(v) = v_\rho$. The action of G on $K[x_\chi \mid \chi \in \hat{G}]$ is in fact induced by the following representation of G on V :

$$\text{for } g \in G, \quad v = \sum_{\chi \in \hat{G}} v_\chi e_\chi \in V \quad \text{we have } g \cdot v = \sum_{\chi \in \hat{G}} \chi(g) v_\chi e_\chi.$$

Proposition 1. *Let v, w be vectors in V such that $v_\chi \neq 0$ and $w_\chi \neq 0$ for all $\chi \in \hat{G} \setminus \{1_{\hat{G}}\}$. Then the G -orbit of v coincides with the G -orbit of w if and only if $f(v) = f(w)$ for all $f \in T$ (defined in 6).*

Proof. By Lemma 1, for any $b \in B(\hat{G})$, there exist $t_1, \dots, t_k \in T$, $u_1, \dots, u_m \in T \setminus \{x_{1_{\hat{G}}}\}$ such that $x^b = t_1 \cdots t_k u_1^{-1} \cdots u_m^{-1}$ (this equality takes place in the Laurent polynomial ring $K[x_\chi^{\pm 1} \mid \chi \in \hat{G}]$). The variable $x_{1_{\hat{G}}}$ does not appear in the elements of $T \setminus \{x_{1_{\hat{G}}}\}$, therefore none of $u_1, \dots, u_m$ involves the variable $x_{1_{\hat{G}}}$, so $u_j(z) \neq 0$ for $z \in \{v, w\}$ and $j = 1, \dots, m$. Consequently, for $z \in \{v, w\}$ we have $x^b(z) = t_1(z) \cdots t_k(z) u_1(z)^{-1} \cdots u_m(z)^{-1}$. It follows that $f(v) = f(w)$ for all $f \in T$ if and only if $x^b(v) = x^b(w)$ for all $b \in B(\hat{G})$. Thus by 5, $f(v) = f(w)$ for all $f \in T$ if and only if $h(v) = h(w)$ for all $h \in K[x_\chi \mid \chi \in \hat{G}]^G$. Since different orbits of a finite group can be separated by polynomial invariants (see 1), we conclude that $f(v) = f(w)$ for all $f \in T$ if and only if $G \cdot v = G \cdot w$. $\square$

Remark 1. As we mentioned in Section 1, it is known that the invariants of degree at most 3 separate the generic orbits (also for the regular representation of finite non-abelian groups), see [1] for the case of complex or real base field, and [4] for the case of an arbitrary infinite base field. Moreover, in the special case when G is cyclic and $\mathbb{F} = \mathbb{R}$ or $\mathbb{C}$ is the real or complex field, Proposition 1 is known, see [27].

4. Prime order cyclic groups over the rationals

Any finite group G acts on itself via left multiplication. This induces a linear action on the $\mathbb{F}$ -vector space $\mathcal{F}(G, \mathbb{F})$ of $\mathbb{F}$ -valued functions on G : for $f \in \mathcal{F}(G, \mathbb{F})$, $g, h \in G$ we have $(g \cdot f)(h) = f(g^{-1}h)$. This representation is called the *regular representation of G over $\mathbb{F}$* . More concretely, the elements δ_g ($g \in G$) defined in 3 form a $\mathbb{F}$ -vector space basis in $\mathcal{F}(G, \mathbb{F})$, and for $h \in G$ we have $h \cdot \delta_g = \delta_{hg}$.

When the characteristic of $\mathbb{F}$ does not divide $|G|$, all irreducible representations of G over $\mathbb{F}$ occur as a direct summand in $\mathcal{F}(G, \mathbb{F})$. Moreover, when $\mathbb{F}$ is also algebraically closed, the multiplicity of each irreducible representation of G over $\mathbb{F}$ equals the dimension of the representation.

Theorem 1. Consider the regular representation on $V := \mathcal{F}(G, \mathbb{Q})$ of the cyclic group $G := C_p$ of prime order p over the field $\mathbb{Q}$ of rational numbers. Then for any $v, w \in V$ with $G \cdot v \neq G \cdot w$ there exists an $f \in \mathbb{Q}[V]^G$ with $\deg(f) \leq 3$ and $f(v) \neq f(w)$.

Proof. Let ω be a primitive p th root of 1, and $K := \mathbb{Q}(\omega)$ the p th cyclotomic extension of $\mathbb{Q}$. For a character $\chi \in \hat{G}$ set

$$e_\chi := \frac{1}{p} \sum_{g \in G} \chi(g)^{-1} \delta_g,$$

where $\{\delta_g \mid g \in G\}$ is the basis of $\mathcal{F}(G, \mathbb{Q})$ defined in 3. Then $\{e_\chi \mid \chi \in \hat{G}\}$ is a K -vector space basis of $V_K := K \otimes_{\mathbb{Q}} V$, satisfying

$$g \cdot e_\chi = \chi(g) e_\chi \quad \text{for all } g \in G, \quad \chi \in \hat{G}.$$

Note that $\chi(g)^{-1}$ is the complex conjugate of $\chi(g)$, and therefore the second orthogonality relation of characters (cf. [28, Chapter 2, Proposition 7]) implies that

$$\delta_g = \sum_{\chi \in \hat{G}} \chi(g) e_\chi \quad \text{for } g \in G. \quad (7)$$

Now assume that for $v, w \in V$, $f(v) = f(w)$ for all $f \in \mathbb{Q}[V]^G$ with $\deg(f) \leq 3$. We claim that $G \cdot v = G \cdot w$. Since the G -action on $K \otimes_{\mathbb{Q}} V$ was obtained from the representation of G on V by extending scalars, each homogeneous component of $K[K \otimes_{\mathbb{Q}} V]^G$ is spanned as a K -vector space by the corresponding homogeneous component of $\mathbb{Q}[V]^G$. Therefore we have that $h(v) = h(w)$ for all $h \in K[K \otimes_{\mathbb{Q}} V]^G$ with $\deg(h) \leq 3$. In particular,

$$h(v) = h(w) \quad \text{for all } h \in T, \quad (8)$$

where T is defined in 6, and $K[K \otimes_{\mathbb{Q}} V] = K[x_\chi \mid \chi \in \hat{G}]$, and $\{x_\chi \mid \chi \in \hat{G}\}$ is the basis dual to the basis $\{e_\chi \mid \chi \in \hat{G}\}$ in $K \otimes_{\mathbb{Q}} V$.

By 7, the $\mathbb{Q}$ -vector subspace $V = \{\sum_{g \in G} v_g \delta_g \mid v_g \in \mathbb{Q}\}$ of $K \otimes_{\mathbb{Q}} V$ is

$$V = \left\{ \sum_{\chi \in \hat{G}} \left(\sum_{g \in G} \chi(g) v_g \right) e_\chi \mid v_g \in \mathbb{Q} \right\}.$$

Note that for $\chi \in \hat{G} \setminus \{1_{\hat{G}}\}$ we have

$$\{\chi(g) \mid g \in G\} = \{1, \omega, \omega^2, \dots, \omega^{p-1}\}.$$

The minimal polynomial of ω over $\mathbb{Q}$ is $1 + x + x^2 + \dots + x^{p-1}$. Therefore $\sum_{g \in G} \chi(g) z_g = 0$ for some $z = \sum_{g \in G} z_g \delta_g \in V$ and $\chi \in \hat{G} \setminus \{1_{\hat{G}}\}$ if and only if $z = c \sum_{g \in G} \delta_g$ for some $c \in \mathbb{Q}$, or in other words, $z_g = c$ for all $g \in G$. Moreover, in this case $z = c p e_{1_{\hat{G}}}$. So

$$V \subset \mathbb{Q} e_{1_{\hat{G}}} \cup \left\{ \sum_{\chi \in \hat{G}} c_\chi e_\chi \mid c_\chi \in K, c_\chi \neq 0 \text{ for } \chi \neq 1_{\hat{G}} \right\}.$$

If both v and w belong to $\mathbb{Q} \sum_{g \in G} \delta_g$, then $v = c_1 \sum_{g \in G} \delta_g = c_1 p e_{1_{\hat{G}}}$, $w = c_2 \sum_{g \in G} \delta_g = c_2 p e_{1_{\hat{G}}}$, hence by 8 we have $c_1 p = x_{1_{\hat{G}}}(v) = x_{1_{\hat{G}}}(w) = c_2 p$, implying that $c_1 = c_2$, and therefore $v = w$.

If at least one of v, w , say v does not belong to $\mathbb{Q} \sum_{g \in G} \delta_g$, then take any $\chi \notin \hat{G} \setminus \{1_{\hat{G}}\}$. We have that $(x_\chi x_{\chi^{-1}})(v) \neq 0$, whence by 8 we get $(x_\chi x_{\chi^{-1}})(w) \neq 0$, implying in turn that w does not belong to $\mathbb{Q} \sum_{g \in G} \delta_g$.

So it remains to deal with the case when none of v and w belong to $\mathbb{Q} \sum_{g \in G} \delta_g$. Then their coordinates with respect to the basis $\{e_\chi \mid \chi \in \hat{G}\}$ are all non-zero, except possibly the coordinate corresponding to $e_{1_{\hat{G}}}$. By 8 and Proposition 1 we conclude that $G \cdot v = G \cdot w$. $\square$

Remark 2. It is known in the signal processing literature that if all the Fourier coefficients of a real vector are non-zero, then its orbit is determined by the invariants of degree at most 3 (see [29]). The novelty in Theorem 1 is the observation that in prime dimension, the Fourier coefficients of a non-constant rational vector are non-zero (except possibly the Fourier coefficient corresponding to the trivial representation), and this is already sufficient to conclude by the approach of Section 3 that invariants of degree at most 3 separate the orbits.

Corollary 1. For the cyclic group C_p of prime order p we have the equality

$$\rho_{\text{sep}}^{\mathbb{Q}}(C_p) = \begin{cases} 3 & \text{for } p \geq 3; \\ 2 & \text{for } p = 2. \end{cases}$$

Proof. For $p = 2$ we have $\beta_{\text{sep}}^{\mathbb{Q}}(C_2) \leq 2$ by 2, and the regular representation of C_2 shows that we have equality here. For $p > 2$ we know that $\beta_{\text{sep}}(C_p, \mathcal{F}(C_p, \mathbb{Q})) \leq 3$ by Theorem 1. Moreover, any finite dimensional representation of C_p over $\mathbb{Q}$ is a direct summand of $\mathcal{F}(C_p, \mathbb{Q})^{\oplus m}$, the direct sum of m copies of the regular representation for some m , hence $\beta_{\text{sep}}^{\mathbb{Q}}(C_p) \leq \max_{m \in \mathbb{N}} \{\beta_{\text{sep}}(C_p, \mathcal{F}(C_p, \mathbb{Q})^{\oplus m})\}$. The latter number equals $\beta_{\text{sep}}(C_p, \mathcal{F}(C_p, \mathbb{Q})^{\oplus 2})$ by [30, Proposition 4.3 and 4.4]. Moreover, we have $\beta_{\text{sep}}(C_p, \mathcal{F}(C_p, \mathbb{Q})^{\oplus 2}) = \beta_{\text{sep}}(C_p, \mathcal{F}(C_p, \mathbb{Q}))$ by [19, Theorem 3.4]. So we proved the inequality $\beta_{\text{sep}}^{\mathbb{Q}}(C_p) \leq 3$.

To prove the reverse inequality for $p \geq 3$, consider the regular representation $\mathcal{F}(C_p, \mathbb{Q})$. Denote by g a generator of C_p . Consider the element $v := \delta_{1_G} - \delta_g$ and its negative $-v$. Denote by $\{x_h \mid h \in G\}$ the basis dual to the basis $\{\delta_h \mid h \in G\}$ in $\mathcal{F}(C_p, \mathbb{Q})$. Then $\mathbb{Q}[V]$ is the polynomial algebra $\mathbb{Q}[x_h \mid h \in G]$, and $g \cdot x_h = x_{gh}$. Since G acts on $\mathbb{Q}[V]$ by permuting the variables, the homogeneous components of $\mathbb{Q}[V]^{C_p}$ are spanned by orbit sums of monomials. The only degree 1 orbit sum $\sum_{h \in C_p} x_h$ vanishes on both v and w . The orbit sum of $x_{1_G}^2$ takes value 2 on both v and w , whereas the orbit sum of $x_{1_G} x_g$ takes value -1 on both v and w . All the other quadratic orbit sums vanish on both v and $-v$. Thus v and $-v$ can not be separated by invariants of degree at most 2. However, they have different C_p -orbits, because the orbit sum of $x_{1_G}^2 x_g$ takes value -1 on v and value 1 on $-v$, when $p > 2$. $\square$

Remark 3.

- (i) For comparison, we mention the well known equality $\beta_{\text{sep}}^{\mathbb{C}}(C_p) = p$. Moreover, it is proved in [6, Proposition 3.13] that even over the field $\mathbb{R}$ of real numbers we have $\beta_{\text{sep}}^{\mathbb{R}}(C_p) = p$.
- (ii) For a prime p , the only irreducible representations of C_p over $\mathbb{Q}$ are the $(p-1)$ -dimensional standard representation and the trivial representation. As we will see in Section 5, this is the special property of the base field $\mathbb{Q}$ and the order p of the cyclic group, that is responsible for Theorem 1 and Corollary 1.

Theorem 1 does not extend to all cyclic groups whose order is not prime, as Proposition 2 below shows:

Proposition 2. The points $v := [3, 4, -3, -4]^T$ and $w := [5, 0, -5, 0]^T$ in $\mathbb{Q}^4$ have different C_4 -orbit, where the cyclic group C_4 acts on $\mathbb{Q}^4$ by cyclically permuting the coordinates of vectors, and all polynomial C_4 -invariants on $\mathbb{Q}^4$ of degree at most 3 take the same value on v and w . In particular, we have

$$\beta_{\text{sep}}^{\mathbb{Q}}(C_4) = 4.$$

Proof. Denote by x_1, x_2, x_3, x_4 the coordinate functions on $\mathbb{Q}^4$, so for a generator g of C_4 we have $g \cdot x_1 = x_2, g \cdot x_2 = x_3, g \cdot x_3 = x_4, g \cdot x_4 = x_1$. The algebra $\mathbb{Q}[x_1, x_2, x_3, x_4]^{C_4}$ of polynomial C_4 -invariants is generated by orbit sums of monomials of degree at most 4. Therefore it is easy to see that $\mathbb{Q}[x_1, x_2, x_3, x_4]^{C_4}$ is minimally generated by $f_1 := x_1 + x_2 + x_3 + x_4, f_2 := x_1^2 + x_2^2 + x_3^2 + x_4^2, f_3 := x_1 x_2 + x_2 x_3 + x_3 x_4 + x_4 x_1, f_4 := x_1^3 + x_2^3 + x_3^3 + x_4^3, f_5 := x_1 x_2^2 + x_2 x_3^2 + x_3 x_4^2 + x_4 x_1^2, f_6 := x_1^4 + x_2^4 + x_3^4 + x_4^4, f_7 := x_1 x_2^3 + x_2 x_3^3 + x_3 x_4^3 + x_4 x_1^3$. Now we have

$$\begin{aligned} [f_1(v), f_2(v), f_3(v), f_4(v), f_5(v), f_6(v), f_7(v)] &= [0, 50, 0, 0, 0, 674, 168] \\ [f_1(w), f_2(w), f_3(w), f_4(w), f_5(w), f_6(w), f_7(w)] &= [0, 50, 0, 0, 0, 1250, 0], \end{aligned}$$

showing that only the degree 4 generators differ on v and w . Thus we have $\beta_{\text{sep}}^{\mathbb{Q}}(C_4) \geq 4$. The reverse inequality holds by 2. $\square$

Proposition 3. Invariants of degree at most 3 are not sufficient to separate all the orbits in the regular representation of S_3 over the field of rational numbers. Moreover, we have

$$\beta_{\text{sep}}^{\mathbb{Q}}(S_3) = 4.$$

Proof. The regular representation of S_3 over $\mathbb{Q}$ contains as a direct summand the sum of the standard 3-dimensional permutation representation of S_3 and the sign representation of S_3 . Therefore it is sufficient to show that the invariants of degree at most 3 do not separate all the orbits in this 4-dimensional representation. The corresponding coordinate ring is $\mathbb{Q}[x_1, x_2, x_3, y]$, a permutation $g \in S_3$ maps x_i to $x_{g(i)}$, and $g \cdot y = \text{sign}(g)y$. It is well known and easy to see that $\mathbb{Q}[x_1, x_2, x_3, y]^{S_3}$ is minimally generated by $s_1 := x_1 + x_2 + x_3, s_2 := x_1 x_2 + x_2 x_3 + x_1 x_3, s_3 := x_1^2 x_2 + x_1 x_2^2 + x_2^2 x_3 + x_2 x_3^2 + x_3^2 x_1 + x_3 x_1^2, s_4 := y^2$, and $a := y(x_2 - x_1)(x_3 - x_2)(x_3 - x_1)$. Set $v := [2, 1, 0, 1]^T \in \mathbb{Q}^4, w := [2, 1, 0, -1]^T \in \mathbb{Q}^4$. Since v and w have the same x -coordinates, $s_i(v) = s_i(w)$ for $i = 1, 2, 3$. Moreover, since $y(v) = -y(w)$, we have $y^2(v) = y^2(w)$. So the invariants of degree at most 3 agree on v and w . However, v and w have different G -orbits, because $a(v) \neq a(w)$. This shows $\beta_{\text{sep}}^{\mathbb{Q}}(S_3) \geq 4$. The reverse inequality holds by 2, because $\beta_{\text{sep}}^{\mathbb{Q}}(S_3) = 4$ (this was shown first in [24]; see [25] for more references). $\square$

5. Representations of abelian groups over non-closed base fields

Throughout this section G is an arbitrary finite abelian group. Let $K = \mathbb{F}(\omega)$ be a cyclotomic extension of $\mathbb{F}$ by an element ω whose multiplicative order is $\exp(G)$, the least common multiple of the orders of elements of G . Note that the existence of K forces that $\text{char}(\mathbb{F})$ does not divide $|G|$. Moreover, K is a Galois extension of $\mathbb{F}$. Denote by Γ the automorphism group of the field extension K of $\mathbb{F}$. Write $\hat{G}$ for the group of characters of G over K ; thus we have $\hat{G} \cong G$ as groups. The Galois group Γ acts naturally on $\hat{G}$ and $\mathcal{F}(G, K)$, namely for $\gamma \in \Gamma$ and $\chi \in \hat{G}$, $\gamma \cdot \chi$ is the character of G mapping $g \in G$ to $\gamma(\chi(g))$, and for $f \in \mathcal{F}(G, K)$, $\gamma(f)$ is the function on G mapping $g \in G$ to $\gamma(f(g))$. The $\mathbb{F}$ -subspace $\mathcal{F}(G, \mathbb{F})$ of $\mathcal{F}(G, K)$ is the fixed point set of Γ in $\mathcal{F}(G, K)$. Throughout this section $\hat{G}/\Gamma$ stands for a chosen set of representatives of the Γ -orbits in $\hat{G}$. The irreducible representations of G over K are all 1-dimensional.

For $\chi \in \widehat{G}$ denote by (K, χ) the 1-dimensional K -vector space K on which G acts via the character χ : for $g \in G$ and $\lambda \in K$ we have $g \cdot \lambda = \chi(g)\lambda$. The irreducible representations of G over $\mathbb{F}$ are in a natural bijection with $\widehat{G}/\Gamma$, as follows.

For each $\chi \in \widehat{G}/\Gamma$ we construct a representation of G over $\mathbb{F}$. The image $\chi(G)$ of G under χ is a subgroup of the multiplicative group $K^\times$ of K , hence is cyclic. Its order d_χ is a divisor of $\exp(G)$. We choose an element $g_\chi \in G$ such that $\omega_\chi := \chi(g_\chi)$ generates the subgroup $\chi(G)$ of $K^\times$ (i.e. the multiplicative order of ω_χ is d_χ). The set of roots of the minimal polynomial $m_{\mathbb{F}}^{\omega_\chi}$ of ω_χ over $\mathbb{F}$ is the Γ -orbit of ω_χ , whence $\ell_\chi := \deg(m_{\mathbb{F}}^{\omega_\chi}) = |\Gamma \cdot \omega_\chi|$. Let $A_\chi \in \mathbb{F}^{\ell_\chi \times \ell_\chi}$ be the companion matrix of $m_{\mathbb{F}}^{\omega_\chi}$, so the characteristic polynomial (and the minimal polynomial) of A_χ is $m_{\mathbb{F}}^{\omega_\chi}$. Then $A_\chi^{d_\chi}$ is the $\ell_\chi \times \ell_\chi$ identity matrix, and the set of eigenvalues of A_χ is the Γ -orbit of ω_χ . Lift to G the representation of $G/\ker(\chi) \cong \chi(G)$ given by $g_\chi^j \ker(\chi) \mapsto A_\chi^j$ for $j = 0, 1, \dots, d_\chi - 1$. Denote by $\rho_\chi : G \rightarrow \text{GL}(\mathbb{F}^{\ell_\chi})$ the corresponding group homomorphism, so $(\mathbb{F}^{\ell_\chi}, \rho_\chi)$ is a representation of G over $\mathbb{F}$. Note that $\ker(\rho_\chi) = \ker(\chi)$ (because $\rho_\chi(g_\chi) = A_\chi$ has eigenvalues with multiplicative order $d_\chi = |G/\ker(\chi)|$). Moreover, we denote by $(K^{\ell_\chi}, \rho_\chi)$ the representation obtained from $(\mathbb{F}^{\ell_\chi}, \rho_\chi)$ by extending the scalars from $\mathbb{F}$ to K . The following statement must be well known, but we do not know a reference for it.

Proposition 4.

- (i) For $\chi \in \widehat{G}/\Gamma$ the representation $(K^{\ell_\chi}, \rho_\chi)$ is isomorphic to $\bigoplus_{\psi \in \Gamma \cdot \chi} (K, \psi)$, where $\Gamma \cdot \chi$ is the Γ -orbit of χ .
- (ii) The representation $(\mathbb{F}^{\ell_\chi}, \rho_\chi)$ is irreducible for all $\chi \in \widehat{G}/\Gamma$.
- (iii) The regular representation $(F(G, \mathbb{F}), \rho_{\text{reg}})$ of G over $\mathbb{F}$ is isomorphic to the direct sum $\bigoplus_{\chi \in \widehat{G}/\Gamma} (\mathbb{F}^{\ell_\chi}, \rho_\chi)$, where $\widehat{G}/\Gamma$ stands for a complete list of representatives of the Γ -orbits in $\widehat{G}$.
- (iv) $\{(\mathbb{F}^{\ell_\chi}, \rho_\chi) \mid \chi \in \widehat{G}/\Gamma\}$ is a complete irredundant list of representatives of the isomorphism classes of the irreducible representations of G over $\mathbb{F}$.

Proof. (i): Since $A_\chi \in K^{\ell_\chi \times \ell_\chi}$ has ℓ_χ distinct eigenvalues in K , and the set of eigenvalues is the Γ -orbit of ω_χ , the space K^{ℓ_χ} decomposes as the direct sum of 1-dimensional eigenspaces $K^{\ell_\chi} = \bigoplus_{\omega \in \Gamma \cdot \omega_\chi} K v_\omega$, where $A_\chi v_\omega = \omega v_\omega$, implying that $g_\chi \cdot v_\omega = \rho_\chi(g_\chi) v_\omega = A_\chi v_\omega = \omega v_\omega$. Moreover, $\ker(\chi) = \ker(\rho_\chi)$, and since the coset of g_χ generates $G/\ker(\rho_\chi)$, we conclude that the subspace $K v_\omega$ is G -invariant. Consequently, $(K v_\omega, \rho_\chi|_{K v_\omega}) \cong (K, \psi)$ for some $\psi \in \widehat{G}$. We claim that $\psi = \gamma \cdot \chi$, where $\gamma \in \Gamma$ satisfies $\omega = \gamma(\omega_\chi)$. Indeed, we have

$$(\gamma \cdot \chi)(g_\chi) v_\omega = \gamma(\chi(g_\chi)) v_\omega = \gamma(\omega_\chi) v_\omega = \omega v_\omega = A_\chi v_\omega = g_\chi \cdot v_\omega = \psi(g_\chi) v_\omega,$$

showing that the characters $\gamma \cdot \chi$ and ψ agree on g_χ . Since $\ker(\psi) \supseteq \ker(\rho_\chi) = \ker(\chi)$, $\ker(\gamma \cdot \chi) = \ker(\chi)$, and the coset of g_χ generates $G/\ker(\chi)$, we conclude that $\gamma \cdot \chi = \psi$. This shows that $(K v_\omega, \rho_\chi|_{K v_\omega}) \cong (K, \gamma \cdot \chi)$, and thus (i) holds.

(ii): Let V be a non-zero G -invariant subspace in $\mathbb{F}^{\ell_\chi}$ (where G acts on $\mathbb{F}^{\ell_\chi}$ via ρ_χ). The non-zero A_χ -invariant subspace $K \otimes_{\mathbb{F}} V$ of K^{ℓ_χ} contains a non-zero A_χ -eigenvector v . Its eigenvalue ω belongs to $\Gamma \cdot \omega_\chi$. The action of Γ on K induces an action on K^{ℓ_χ} and on $K^{\ell_\chi \times \ell_\chi}$ in the obvious way. The matrix A_χ is fixed by Γ , because its entries belong to $\mathbb{F}$. For $\gamma \in \Gamma$ we have

$$A_\chi \gamma(v) = \gamma(A_\chi) \gamma(v) = \gamma(A_\chi v) = \gamma(\omega v) = \gamma(\omega) \gamma(v). \quad (9)$$

Since V is contained in the fixed point set $\mathbb{F}^{\ell_\chi}$ of Γ in K^{ℓ_χ} , Γ maps $K \otimes_{\mathbb{F}} V$ into itself, so $\gamma(v)$ belongs to $K \otimes_{\mathbb{F}} V$, and it is an A_χ -eigenvector with eigenvalue $\gamma(\omega)$. This holds for all $\gamma \in \Gamma$, so $K \otimes_{\mathbb{F}} V$ contains all the A_χ -eigenvectors in K^{ℓ_χ} . Therefore $K \otimes_{\mathbb{F}} V = K^{\ell_\chi}$, and consequently, $V = \mathbb{F}^{\ell_\chi}$. Thus $\mathbb{F}^{\ell_\chi}$ has no proper non-zero G -invariant subspace, so the representation $(\mathbb{F}^{\ell_\chi}, \rho_\chi)$ is irreducible, i.e. (ii) holds.

(iii) By (i) we see that $\bigoplus_{\chi \in \widehat{G}/\Gamma} (K^{\ell_\chi}, \rho_\chi) \cong \bigoplus_{\psi \in \widehat{G}} (K, \psi) \cong (F(G, K), \rho_{\text{reg}})$. So extending the base field from $\mathbb{F}$ to K the representations $(F(G, \mathbb{F}), \rho_{\text{reg}})$ and $\bigoplus_{\chi \in \widehat{G}/\Gamma} (\mathbb{F}^{\ell_\chi}, \rho_\chi)$ become isomorphic. It follows that these two representations are isomorphic over $\mathbb{F}$.

(iv) Statement (i) implies that for $\chi \neq \chi'$ in $\widehat{G}/\Gamma$, the representations $(\mathbb{F}^{\ell_\chi}, \rho_\chi)$ and $(\mathbb{F}^{\ell_{\chi'}}, \rho_{\chi'})$ are non-isomorphic, so the given list of irreducible representations is irredundant. On the other hand, every irreducible representation of G over $\mathbb{F}$ occurs as a direct summand in the regular representation, hence (iii) implies completeness of the list. $\square$

Example 1. Let $G = C_n = \langle g \rangle$, $\mathbb{F} = \mathbb{Q}$, $K = \mathbb{Q}(\omega)$, where $\omega = e^{2\pi i/n} \in \mathbb{C}$. Then $\widehat{G} = \{\chi_{\omega^k} \mid k = 0, 1, \dots, n-1\}$, where for an n th root ε of 1, χ_ε is given by $\chi_\varepsilon(g) = \varepsilon$. Denote by $\text{ord}(\varepsilon)$ the multiplicative order of ε . It is a divisor d of n , and the Γ -orbit of ε is the set of primitive d th roots of 1. So $\widehat{G}/\Gamma$ is in a natural bijection with the set of positive divisors of n .

The surjection $\mathbb{Q}[x] \rightarrow \mathbb{Q}C_n$ onto the rational group algebra of C_n given by $x \mapsto g$ induces an isomorphism $\mathbb{Q}[x]/(x^n - 1) \cong \mathbb{Q}C_n$. Via this isomorphism we view $\mathbb{Q}[x]/(x^n - 1)$ as a $\mathbb{Q}C_n$ -module. Recall that the irreducible factorization of $x^n - 1$ in $\mathbb{Q}[x]$ is $x^n - 1 = \prod_{d|n} \Phi_d$, where $\Phi_d = \prod_{\text{ord}(\varepsilon)=d} (x - \varepsilon)$ is the d th cyclotomic polynomial. Therefore by the Chinese Remainder Theorem we get the $\mathbb{Q}C_n$ -module decomposition $\mathbb{Q}[x]/(x^n - 1) \cong \bigoplus_{d|n} \mathbb{Q}[x]/(\Phi_d)$, and $\{\mathbb{Q}[x]/(\Phi_d) : d \mid n\}$ is a complete irredundant list of representatives of isomorphism classes of irreducible $\mathbb{Q}C_n$ -modules.

Extending the base field to $K = \mathbb{Q}(\omega)$, the KC_n -module $K[x]/(\Phi_d)$ splits as $K[x]/(\Phi_d) = \bigoplus_{\text{ord}(\varepsilon)=d} K[x]/(x - \varepsilon)$ into the direct sum of the 1-dimensional KC_n -modules corresponding to the characters belonging to the Γ -orbit in $\widehat{G}$ labeled by d .

By Proposition 4 (iii) we have a direct sum decomposition

$$F(G, \mathbb{F}) = \bigoplus_{\chi \in \widehat{G}/\Gamma} V_\chi \quad (10)$$

into minimal G -invariant subspaces, where $(V_\chi, \rho_{\text{reg}}|_{V_\chi}) \cong (\mathbb{F}^{\ell_\chi}, \rho_\chi)$. Extending scalars from $\mathbb{F}$ to K we get

$$F(G, K) = \bigoplus_{\chi \in \hat{G}/\Gamma} K \otimes_{\mathbb{F}} V_\chi. \quad (11)$$

We need the following refinement of Proposition 4 (i):

Lemma 2. For each $\chi \in \hat{G}/\Gamma$, $K \otimes_{\mathbb{F}} V_\chi$ has a K -vector space basis $\{f_\psi \mid \psi \in \Gamma \cdot \chi\}$, where

- (i) Kf_ψ is a G -invariant subspace of $K \otimes_{\mathbb{F}} V_\chi$, on which the representation of G is isomorphic to (K, ψ) ;
- (ii) $\{f_\psi \mid \psi \in \Gamma \cdot \chi\}$ is the Γ -orbit of f_χ , so

$$f_{\gamma \cdot \psi} = \gamma(f_\psi) \text{ for all } \gamma \in \Gamma, \psi \in \Gamma \cdot \chi. \quad (12)$$

Proof. By Proposition 4 (i), $K \otimes_{\mathbb{F}} V_\chi$ contains a unique 1-dimensional G -invariant subspace Kv such that $(Kv, \rho_\chi|_{Kv}) \cong (K, \chi)$ (clearly Kv is the ω_χ -eigenspace of $\rho_\chi(g_\chi) = A_\chi$). Denote by Γ_0 the stabilizer subgroup in Γ of χ , or equivalently, Γ_0 is the stabilizer in Γ of ω_χ (so $\ell_\chi = |\Gamma \cdot \chi| = |\Gamma : \Gamma_0|$, the index of Γ_0 in Γ). Formula 9 shows that the stabilizer of v in Γ (and similarly, of any non-zero element of Kv) is contained in Γ_0 . Pick an element f_χ in Kv such that f_χ has a non-zero coordinate in the fixed field K^{Γ_0} of Γ_0 in K . Then for any $\gamma \in \Gamma_0$, one non-zero coordinate of f_χ coincides with the corresponding coordinate of $\gamma(f_\chi)$. On the other hand, 9 implies that for any $\gamma \in \Gamma_0$, $\gamma(f_\chi)$ is also an ω_χ -eigenvector of A_χ , hence $\gamma(f_\chi) \in Kv = Kf_\chi$. It follows that $\gamma(f_\chi) = f_\chi$, so the stabilizer of f_χ in Γ equals Γ_0 , the stabilizer of χ in Γ . Now for $\psi \in \Gamma \cdot \chi$ we may define f_ψ as follows: take any $\gamma \in \Gamma$ with $\gamma \cdot \chi = \psi$, and set $f_\psi := \gamma(f_\chi)$. By 9 we see that f_ψ is a $\gamma(\omega_\chi)$ -eigenvector of $\rho_\chi(g_\chi)$. Thus $\{f_\psi \mid \psi \in \Gamma \cdot \chi\}$ is a K -vector space basis of $K \otimes_{\mathbb{F}} V_\chi$ satisfying (i) and (ii). $\square$

Choose an $\mathbb{F}$ -vector space basis $\{e_\psi \mid \psi \in \Gamma \cdot \chi\}$ in V_χ (recall that $\dim(V_\chi) = \ell_\chi = |\Gamma \cdot \chi|$, so we can use the elements in the Γ -orbit of χ as labels for the basis vectors). Then by 10, $\{e_\psi \mid \psi \in \hat{G}\}$ is an $\mathbb{F}$ -vector space basis of $F(G, \mathbb{F})$, and also a K -vector space basis of $F(G, K)$. By Lemma 2 and 11, another K -vector space basis of $F(G, K)$ is $\{f_\psi \mid \psi \in \hat{G}\}$. The following statement identifies the $\mathbb{F}$ -subspace $F(G, \mathbb{F})$ of $F(G, K)$ in terms of the coordinates with respect to the K -vector space basis $\{f_\psi \mid \psi \in \hat{G}\}$:

Lemma 3. We have

$$F(G, \mathbb{F}) = \left\{ \sum_{\psi \in \hat{G}} c_\psi f_\psi \in F(G, K) \mid c_{\gamma \cdot \psi} = \gamma(c_\psi) \in K \text{ for all } \gamma \in \Gamma, \psi \in \hat{G} \right\}.$$

Proof. Recall that Γ acts on $F(G, K)$ as $(\gamma(f))(g) = \gamma(f(g))$ for $\gamma \in \Gamma$, $f \in F(G, K)$ and $g \in G$. This is an action on the K -vector space $F(G, K)$ via semilinear transformations. That is, for $f_1, f_2 \in F(G, K)$, $c_1, c_2 \in K$, and $\gamma \in \Gamma$ we have $\gamma(c_1 f_1 + c_2 f_2) = \gamma(c_1) \gamma(f_1) + \gamma(c_2) \gamma(f_2)$. Therefore we have

$$\gamma \left(\sum_{\psi \in \hat{G}} c_\psi f_\psi \right) = \sum_{\psi \in \hat{G}} \gamma(c_\psi) \gamma(f_\psi) = \sum_{\psi \in \hat{G}} \gamma(c_\psi) f_{\gamma \cdot \psi}$$

(the second equality above holds by 12 in Lemma 2), implying that

$$\gamma \left(\sum_{\psi \in \hat{G}} c_\psi f_\psi \right) = \sum_{\psi \in \hat{G}} c_\psi f_\psi \iff \forall \psi \in \hat{G} : \gamma(c_\psi) = c_{\gamma \cdot \psi}. \quad (13)$$

By definition of the Γ -action, and since $\mathbb{F}$ is the fixed subfield of Γ in K , we have $F(G, \mathbb{F}) = \{f \in F(G, K) \mid \forall \gamma \in \Gamma : \gamma(f) = f\}$. So our statement follows by 13. $\square$

For a subset M of $B(\hat{G}) \subset F(G, \mathbb{Z})$ and a subset $I \subseteq \hat{G}$, set

$$M_I := \{m \in M \mid m(\psi) = 0 \text{ for all } \psi \in \hat{G} \setminus I\},$$

and write $\langle M_I \rangle_{\mathbb{Z}}$ for the $\mathbb{Z}$ -submodule of $F(G, \mathbb{Z})$ generated by M_I . Note that when M is a submonoid of $B(\hat{G})$, then M_I is also a submonoid of $B(\hat{G})$. The coordinate ring of $F(G, K)$ is a polynomial algebra $K[x_\psi \mid \psi \in \hat{G}]$, where $\{x_\psi \mid \psi \in \hat{G}\}$ is a basis dual to the basis $\{f_\psi \mid \psi \in \hat{G}\}$ in $F(G, K)$ introduced above. In particular, we have that $g \cdot x_\psi = \psi(g)^{-1} x_\psi$ for $g \in G$. For $m \in B(\hat{G})$ we set $x^m := \prod_{\psi \in \hat{G}} x_\psi^{m(\psi)}$. As we pointed out in 5, $\{x^m \mid m \in B(\hat{G})\}$ is a K -vector space basis of $K[x_\psi \mid \psi \in \hat{G}]^G$. If $m \in M_I$, then x^m belongs to the subalgebra $K[x_\psi \mid \psi \in I]$ of $K[x_\psi \mid \psi \in \hat{G}]$.

Theorem 2. Let M be a subset of $B(\hat{G})$. The polynomial G -invariants $\{x^m \mid m \in M\}$ separate the G -orbits in the subspace $F(G, \mathbb{F})$ of $F(G, K)$ if condition (*) below holds for M :

(*) for all Γ -stable subsets I of $\hat{G}$, we have $\langle M_I \rangle_{\mathbb{Z}} \supseteq B(\hat{G})_I$.

To prove Theorem 2 we need Lemma 4 below. Recall the direct sum decomposition $F(G, \mathbb{F}) = \bigoplus_{\chi \in \hat{G}/\Gamma} V_\chi$ from 10, so $v \in F(G, \mathbb{F})$ can be written as $v = (v_\chi \mid \chi \in \hat{G}/\Gamma)$, where $v_\chi \in V_\chi$. Set $\text{supp}(v) := \{\chi \in \hat{G}/\Gamma \mid v_\chi \neq 0\}$.

Lemma 4. For $v \in F(G, \mathbb{F})$, $\psi \in \hat{G}$, and $m \in B(\hat{G})$ we have

- (i) $x_\psi(v) \neq 0$ if and only if $\psi \in \bigcup_{\chi \in \text{supp}(v)} \Gamma \cdot \chi$.

(ii) $x^m(v) \neq 0$ if and only if $m \in B(\hat{G})_I$ where $I = \bigcup_{\chi \in \text{supp}(v)} \Gamma \cdot \chi$.

Proof. (i) Recall that $v_\chi = \sum_{\lambda \in \Gamma \cdot \chi} x_\lambda(v) f_\lambda$. If $x_\psi(v)$ is non-zero, then $v_\mu \neq 0$ for the unique $\mu \in \hat{G}/\Gamma$ for which $\psi \in \Gamma \cdot \mu$. Then $\mu \in \text{supp}(v)$, and so $\psi \in \bigcup_{\chi \in \text{supp}(v)} \Gamma \cdot \chi$. For the reverse implication assume that $\psi \in \Gamma \cdot \chi$ for some $\chi \in \text{supp}(v)$. So $v_\chi \neq 0$ and thus $x_\lambda(v) \neq 0$ for some λ from $\Gamma \cdot \chi = \Gamma \cdot \psi$. Here $\psi, \lambda \in \hat{G}$ belong to the same Γ -orbit in $\hat{G}$, hence by Lemma 3, $x_\lambda(v) \neq 0$ implies $x_\psi(v) \neq 0$.

(ii) follows from (i). $\square$

Proof of Theorem 2. Suppose that $M \subseteq B(\hat{G})$ satisfies condition (*), and $v, w \in F(G, \mathbb{F})$ with $G \cdot v \neq G \cdot w$. We have to show that there exists an $m \in M$ with $x^m(v) \neq x^m(w)$.

First we deal with the case when $\text{supp}(v) \neq \text{supp}(w)$. Then by symmetry we may assume that there exists a $\chi \in \text{supp}(v) \setminus \text{supp}(w)$. Let I be the Γ -orbit of χ . The element $\text{ord}(\chi)\delta_\chi$ belongs to $B(\hat{G})_I$, therefore by assumption (*) for M , there exist $m, m' \in M_I \subseteq B(\hat{G})_I$ with $\text{ord}(\chi)\delta_\chi = m - m'$. It follows that $m(\chi) > 0$. By Lemma 4 we have $x^m(v) \neq 0$, whereas $x^m(w) = 0$. In particular, we found an $m \in M$ with $x^m(v) \neq x^m(w)$.

From now on we assume that $\text{supp}(v) = \text{supp}(w)$. Since $G \cdot v \neq G \cdot w$, by 1 and 5 we know that there exists a $b \in B(\hat{G})$ with $x^b(v) \neq x^b(w)$. Set $I := \bigcup_{\chi \in \text{supp}(v)} \Gamma \cdot \chi = \bigcup_{\chi \in \text{supp}(w)} \Gamma \cdot \chi$. Then $b \in B(\hat{G})_I$ (otherwise by Lemma 4 (ii) we would have $x^b(v) = 0 = x^b(w)$, contrary to the choice of b). We can write b as $b = m - m'$ for some $m, m' \in M_I$ by assumption (*) on M . By Lemma 4 (ii) we know that none of $x^m(v)$, $x^{m'}(v)$, $x^m(w)$, $x^{m'}(w)$ is zero. Consequently, $x^b(v) = \frac{x^m(v)}{x^{m'}(v)}$ and $x^b(w) = \frac{x^m(w)}{x^{m'}(w)}$. Therefore $x^b(v) \neq x^b(w)$ implies that $x^m(v) \neq x^m(w)$ or $x^{m'}(v) \neq x^{m'}(w)$, and we are done. $\square$

Corollary 2. Let d be a positive integer satisfying that for all Γ -stable subsets I of $\hat{G}$, the monoid $B(\hat{G})_I$ is contained in the $\mathbb{Z}$ -submodule of $F(G, \mathbb{Z})$ generated by $\{m \in B(\hat{G})_I \mid \sum_{\psi \in \hat{G}} m(\psi) \leq d\}$. Then we have

(i) $\beta_{\text{sep}}(G, F(G, \mathbb{F})) \leq d$.

(ii) $\beta_{\text{sep}}^{\mathbb{F}}(G) \leq d$.

Proof. (i) Assume that the positive integer d satisfies that for all Γ -stable subsets I of $\hat{G}$, the monoid $B(\hat{G})_I$ is contained in the $\mathbb{Z}$ -submodule of $F(\hat{G}, \mathbb{Z})$ generated by $\{m \in B(\hat{G})_I \mid \sum_{\psi \in \hat{G}} m(\psi) \leq d\}$. Setting $M := \{m \in B(\hat{G}) \mid \sum_{\psi \in \hat{G}} m(\psi) \leq d\}$ we have that M satisfies condition (*) from Theorem 2, hence the G -invariants $\{x^m \mid m \in M\}$ in $K[F(G, K)]$ separate the G -orbits in the $\mathbb{F}$ -vector subspace $F(G, \mathbb{F})$ of $F(G, K)$. Note that $\text{Span}_K \{x^m \mid m \in M\}$ is the union of the homogeneous components of $K[F(G, K)]^G$ of degree at most d by 5. Recall that for all j , the degree j homogeneous component of $K[F(G, K)]^G$ is spanned as a K -vector space by the degree j homogeneous component of $\mathbb{F}[F(G, \mathbb{F})]^G$. Since the homogeneous components of $K[F(G, K)]^G$ of degree at most d separate the G -orbits in $F(G, \mathbb{F})$, the same holds for its spanning subset, consisting of the elements of degree at most d in $\mathbb{F}[F(G, \mathbb{F})]^G$.

(ii) Every finite dimensional representation of G is a direct summand in a direct sum of several copies of the regular representation. Therefore it is sufficient to show that $\beta_{\text{sep}}^{\mathbb{F}}(G, V) \leq d$ where $V = F(G, \mathbb{F}) \oplus \cdots \oplus F(G, \mathbb{F}) = F(G, \mathbb{F})^{\oplus n}$. Then $K \otimes_{\mathbb{F}} V \cong \bigoplus_{\psi \in \hat{G}} (K, \psi)^{\oplus n}$, and the coordinate ring $K[K \otimes_{\mathbb{F}} V]$ has variables $\{x_\psi^{(1)}, \dots, x_\psi^{(n)} \mid \psi \in \hat{G}\}$ with $g \cdot x_\psi^{(j)} = \psi^{-1}(g)x_\psi^{(j)}$. A variant of Lemma 3, Lemma 4, and Theorem 2 for this more general setup can be proved in the same way as before, the only difference is that the notation becomes considerably more complicated. Alternatively, if $\mathbb{F}$ is large enough (say $\mathbb{F}$ is infinite), then one may refer to [19, Theorem 3.4 (ii)] implying that $\beta_{\text{sep}}(G, F(G, \mathbb{F})^{\oplus n}) = \beta_{\text{sep}}(G, F(G, \mathbb{F}))$. $\square$

Remark 4. A characterization of the subsets $M \subseteq B(\hat{G})$ such that $\{x^m \mid m \in M\}$ separates the G -orbits in $F(G, K)$ was given in [9, Theorem 2.1] (see [31] and [32, Proposition 3.2] for some additional information on separating monomials), yielding in [9, Corollary 2.6] a combinatorial characterization of $\beta_{\text{sep}}^K(G)$ in terms of the block monoid of $\hat{G}$. Theorem 2 and Corollary 2 generalize [9, Proposition 2.3] (one direction of [9, Theorem 2.1]) and one inequality of [9, Corollary 2.6] for the case of base fields that are not necessarily algebraically closed.

As an application (and illustration) of Corollary 2 we compute the separating Noether number over the field $\mathbb{R}$ of real numbers of the direct product $C_3 \times C_3$ of two copies of the cyclic group C_3 of order 3:

Proposition 5. We have the equality $\beta_{\text{sep}}^{\mathbb{R}}(C_3 \times C_3) = 3$.

Proof. Since C_3 is a homomorphic image of $C_3 \times C_3$ and $\beta_{\text{sep}}^{\mathbb{R}}(C_3) = 3$ by [6, Proposition 3.13], we have $\beta_{\text{sep}}^{\mathbb{R}}(C_3 \times C_3) \geq 3$. The reverse inequality $\beta_{\text{sep}}^{\mathbb{R}}(C_3 \times C_3) \leq 3$ can be obtained applying Corollary 2 for $\mathbb{F} = \mathbb{R}$, $K = \mathbb{C}$, and $G = C_3 \times C_3$. Then Γ is the automorphism group of the field extension $\mathbb{C}$ of $\mathbb{R}$, so Γ is the two-element group generated by complex conjugation. In particular, the Γ -orbit of a character χ of G consists of the character χ and its inverse $\chi^{-1} \in \hat{G}$. The character group $\hat{G}$ is also isomorphic to $C_3 \times C_3$, so it is generated by two order 3 characters ψ_1 and ψ_2 . Writing $\chi_{(i,j)} := \psi_1^i \psi_2^j$, we have $\hat{G} = \{\chi_{(i,j)} \mid (i,j) \in \{0, 1, 2\} \times \{0, 1, 2\}\}$. The partition of $\hat{G}$ into the disjoint union of Γ -orbits is the following:

$$\hat{G} = \{\chi_{(0,0)}\} \sqcup \{\chi_{(1,0)}, \chi_{(2,0)}\} \sqcup \{\chi_{(0,1)}, \chi_{(0,2)}\} \sqcup \{\chi_{(1,1)}, \chi_{(2,2)}\} \sqcup \{\chi_{(1,2)}, \chi_{(2,1)}\}$$

In order to have a simpler notation for the elements of $F(\hat{G}, \mathbb{Z})$, write $\delta_{(i,j)} := \delta_{\chi_{(i,j)}}$ for the basis elements. The additive monoid $B(\hat{G})$ is generated by its irreducible elements, where an element of $B(\hat{G})$ is said to be *irreducible* if it is not the sum of two non-zero elements of $B(\hat{G})$. Recall that the length of $b \in B(\hat{G})$ is $|b| = \sum_{\chi \in \hat{G}} b(\chi)$. Clearly $\delta_{(0,0)}$ is the only length 1 element of $B(\hat{G})$, and $\delta_\chi + \delta_{\chi^{-1}}$ for

$\chi \neq \chi_{(0,0)}$ are the only length 2 irreducible elements in B_G . The automorphism group of the group $\hat{G}$ acts naturally by $\mathbb{Z}$ -module automorphisms on $F(\hat{G}, \mathbb{Z})$ and by monoid automorphisms of the submonoid $B(\hat{G})$. We claim that up to such automorphisms, the only irreducible elements in $B(\hat{G})$ with length greater than 2 are

$$\begin{aligned} 3\delta_{(1,0)}, \text{Quad}\delta_{(1,0)} + \delta_{(0,1)} + \delta_{(2,2)}, \\ b_1 := \delta_{(1,0)} + \delta_{(0,1)} + 2\delta_{(1,1)}, \text{Quad}b_2 := \delta_{(1,0)} + 2\delta_{(0,1)} + \delta_{(2,1)}, \\ b_3 := 2\delta_{(1,0)} + 2\delta_{(0,1)} + \delta_{(1,1)}. \end{aligned}$$

Indeed, if for an irreducible $b \in B(\hat{G})$ with $|b| > 2$ there are two different non-trivial characters σ_1, σ_2 with $b(\sigma_1) \neq 0$ and $b(\sigma_2) \neq 0$, then applying an automorphism of $\hat{G}$ we may reduce to the case $\sigma_1 = \chi_{(1,0)}$ and $\sigma_2 = \chi_{(0,1)}$. Moreover, $b(\chi_{(1,0)}) \in \{1, 2\}$ and $b(\chi_{(0,1)}) \in \{1, 2\}$. After these observations it is easy to sort out the few possibilities, and conclude the claim. In particular, b_1, b_2, b_3 represent the orbits of all irreducible elements in $B(\hat{G})$ with length strictly greater than 3.

Set $M := \{b \in B(\hat{G}) \mid |b| \leq 3\}$. If $b_1 \in B(\hat{G})_I$ for some Γ -stable subset I of $\hat{G}$, then $\chi_{(1,0)}, \chi_{(0,1)}, \chi_{(1,1)}, \chi_{(2,2)} \in I$, and the equality

$$\delta_{(1,0)} + \delta_{(0,1)} + 2\delta_{(1,1)} = (\delta_{(1,0)} + \delta_{(0,1)} + \delta_{(2,2)}) + 2(\delta_{(1,1)} + \delta_{(2,2)}) - 3\delta_{(2,2)}$$

shows that $b_1 \in \langle M_I \rangle_{\mathbb{Z}}$.

If $b_2 \in B(\hat{G})_I$ for some Γ -stable subset I of $\hat{G}$, then $\chi_{(1,0)}, \chi_{(0,1)}, \chi_{(2,1)}, \chi_{(0,2)} \in I$, and the equality

$$\delta_{(1,0)} + 2\delta_{(0,1)} + \delta_{(2,1)} = (\delta_{(1,0)} + \delta_{(0,2)} + \delta_{(2,1)}) + 2(\delta_{(0,1)} + \delta_{(0,2)}) - 3\delta_{(0,2)}$$

shows that $b_2 \in \langle M_I \rangle_{\mathbb{Z}}$.

If $b_3 \in B(\hat{G})_I$ for some Γ -stable subset I of $\hat{G}$, then $\chi_{(1,0)}, \chi_{(0,1)}, \chi_{(1,1)}, \chi_{(2,2)} \in I$, and the equality

$$2\delta_{(1,0)} + 2\delta_{(0,1)} + \delta_{(1,1)} = 2(\delta_{(1,0)} + \delta_{(0,1)} + \delta_{(2,2)}) + (\delta_{(1,1)} + \delta_{(2,2)}) - 3\delta_{(2,2)}$$

shows that $b_3 \in \langle M_I \rangle_{\mathbb{Z}}$.

Thus we verified that the condition of [Corollary 2](#) is satisfied by $d = 3$, hence the desired inequality $\beta_{\text{sep}}^{\mathbb{R}}(C_3 \times C_3) \leq 3$ holds. $\square$

Remark 5. It is shown in [[10](#), Theorem 1.2] that $\beta_{\text{sep}}^{\mathbb{C}}(C_3 \times C_3) = 4$ (the inequality $\beta_{\text{sep}}^{\mathbb{C}}(C_3 \times C_3) \leq 4$ follows essentially from the equality $b_3 = b_1 + b_2 - 3\delta_{(1,1)}$). Moreover, $\beta^{\mathbb{R}}(C_3 \times C_3) = \beta^{\mathbb{C}}(C_3 \times C_3) = 5$ (see [[25](#)] for information on $\beta^{\mathbb{F}}(G)$).

6. An example

We give an example showing that the results of the present paper yield a notable decrease in the size of a separating set of invariants for a real representation of a finite abelian group, compared to systems of polynomial invariants whose separating property is guaranteed by the prior known results. Consider $V := \mathbb{R}^6$ endowed with the natural representation of the matrix group G generated by

$$\begin{pmatrix} -\frac{1}{2} & -\frac{\sqrt{3}}{2} & 0 & 0 & 0 & 0 \\ \frac{\sqrt{3}}{2} & -\frac{1}{2} & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & -\frac{1}{2} & -\frac{\sqrt{3}}{2} \\ 0 & 0 & 0 & 0 & \frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix} \text{ and } \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & -\frac{1}{2} & -\frac{\sqrt{3}}{2} & 0 & 0 \\ 0 & 0 & \frac{\sqrt{3}}{2} & -\frac{1}{2} & 0 & 0 \\ 0 & 0 & 0 & 0 & -\frac{1}{2} & -\frac{\sqrt{3}}{2} \\ 0 & 0 & 0 & 0 & \frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix}.$$

The group G is isomorphic to $C_3 \times C_3$, hence by [Proposition 5](#), $\beta_{\text{sep}}^{\mathbb{R}}(G, V) \leq 3$. A minimal homogeneous system of generators of $\mathbb{R}[V]^G$ can be computed by the online CoCalc platform [[33](#)], and we get that the G -orbits in V are separated by the following invariants (the elements of degree at most 3 in the minimal homogeneous generating system):

$$\begin{aligned} x_5^2 + x_6^2, \quad x_3^2 + x_4^2, \quad x_1^2 + x_2^2, \quad x_5^2 x_6 - \frac{1}{3} x_6^3, \quad x_5^3 - 3x_5 x_6^2, \\ x_2 x_3 x_5 + x_1 x_4 x_5 - x_1 x_3 x_6 + x_2 x_4 x_6, \quad x_1 x_3 x_5 - x_2 x_4 x_5 + x_2 x_3 x_6 + x_1 x_4 x_6, \\ x_3^2 x_4 - \frac{1}{3} x_4^3, \quad x_3^3 - 3x_3 x_4^2, \quad x_1^2 x_2 - \frac{1}{3} x_2^3, \quad x_1^3 - 3x_1 x_2^2 \end{aligned}$$

The known results prior to this paper guaranteed that $\beta_{\text{sep}}^{\mathbb{R}}(G, V) \leq \beta_{\text{sep}}^{\mathbb{C}}(G, \mathbb{C} \otimes_{\mathbb{R}} V) \leq 4$ (see [[9](#)]). Diagonalizing the representation over $\mathbb{C}$, one can deduce from [[9](#), Proposition 2.4] that in order to separate the orbits in the complexification $\mathbb{C}[\mathbb{C} \otimes_{\mathbb{R}} V]$, we need to include the following 6 degree 4 invariants:

$$\begin{aligned} x_1 x_3 x_5^2 - x_2 x_4 x_5^2 - 2x_2 x_3 x_5 x_6 - 2x_1 x_4 x_5 x_6 - x_1 x_3 x_6^2 + x_2 x_4 x_6^2, \\ x_2 x_3 x_5^2 + x_1 x_4 x_5^2 + 2x_1 x_3 x_5 x_6 - 2x_2 x_4 x_5 x_6 - x_2 x_3 x_6^2 - x_1 x_4 x_6^2, \\ x_1 x_3^2 x_5 + 2x_2 x_3 x_4 x_5 - x_1 x_4^2 x_5 + x_2 x_3^2 x_6 - 2x_1 x_3 x_4 x_6 - x_2 x_4^2 x_6, \\ x_2 x_3^2 x_5 - 2x_1 x_3 x_4 x_5 - x_2 x_4^2 x_5 - x_1 x_3^2 x_6 - 2x_2 x_3 x_4 x_6 + x_1 x_4^2 x_6, \end{aligned}$$

$$x_1^2 x_3 x_5 - x_2^2 x_3 x_5 + 2x_1 x_2 x_4 x_5 - 2x_1 x_2 x_3 x_6 + x_1^2 x_4 x_6 - x_2^2 x_4 x_6, \\ x_1 x_2 x_3 x_5 - \frac{1}{2} x_1^2 x_4 x_5 + \frac{1}{2} x_2^2 x_4 x_5 + \frac{1}{2} x_1^2 x_3 x_6 - \frac{1}{2} x_2^2 x_3 x_6 + x_1 x_2 x_4 x_6$$

The minimal generating system of $\mathbb{R}[V]^G$ is even larger, since it contains also the following 6 degree 5 invariants:

$$x_2 x_3^2 x_5^2 - 2x_1 x_3 x_4 x_5^2 - x_2 x_4^2 x_5^2 + 2x_1 x_3^2 x_5 x_6 + 4x_2 x_3 x_4 x_5 x_6 - 2x_1 x_4^2 x_5 x_6 \\ - x_2 x_3^2 x_6^2 + 2x_1 x_3 x_4 x_6^2 + x_2 x_4^2 x_6^2, \\ x_1 x_3^2 x_5^2 + 2x_2 x_3 x_4 x_5^2 - x_1 x_4^2 x_5^2 - 2x_2 x_3^2 x_5 x_6 + 4x_1 x_3 x_4 x_5 x_6 + 2x_2 x_4^2 x_5 x_6 \\ - x_1 x_3^2 x_6^2 - 2x_2 x_3 x_4 x_6^2 + x_1 x_4^2 x_6^2, \\ x_1 x_2 x_3 x_5^2 - \frac{1}{2} x_1^2 x_4 x_5^2 + \frac{1}{2} x_2^2 x_4 x_5^2 - x_1^2 x_3 x_5 x_6 + x_2^2 x_3 x_5 x_6 - 2x_1 x_2 x_4 x_5 x_6 \\ - x_1 x_2 x_3 x_6^2 + \frac{1}{2} x_1^2 x_4 x_6^2 - \frac{1}{2} x_2^2 x_4 x_6^2, \\ x_1^2 x_3 x_5^2 - x_2^2 x_3 x_5^2 + 2x_1 x_2 x_4 x_5^2 + 4x_1 x_2 x_3 x_5 x_6 - 2x_1^2 x_4 x_5 x_6 + 2x_2^2 x_4 x_5 x_6 \\ - x_1^2 x_3 x_6^2 + x_2^2 x_3 x_6^2 - 2x_1 x_2 x_4 x_6^2, \\ x_1 x_2 x_3^2 x_5 + x_1^2 x_3 x_4 x_5 - x_2^2 x_3 x_4 x_5 - x_1 x_2 x_4^2 x_5 + \frac{1}{2} x_1^2 x_3^2 x_6 - \frac{1}{2} x_2^2 x_3^2 x_6 \\ - 2x_1 x_2 x_3 x_4 x_6 - \frac{1}{2} x_1^2 x_4^2 x_6 + \frac{1}{2} x_2^2 x_4^2 x_6, \\ x_1^2 x_3^2 x_5 - x_2^2 x_3^2 x_5 - 4x_1 x_2 x_3 x_4 x_5 - x_1^2 x_4^2 x_5 + x_2^2 x_4^2 x_5 - 2x_1 x_2 x_3^2 x_6 \\ - 2x_1^2 x_3 x_4 x_6 + 2x_2^2 x_3 x_4 x_6 + 2x_1 x_2 x_4^2 x_6$$

Data availability

No data was used for the research described in the article.

Acknowledgements

This research was partially supported by the Hungarian National Research, Development and Innovation Office, NKFIH K 138828.

References

- [1] A.S. Bandeira, B. Blum-Smith, J. Kileel, J. Niles-Weed, A. Perry, A.S. Wein, Estimation under group actions: recovering orbits from invariants, *Appl. Comput. Harmon. Anal.* 66 (2023) 236–319.
- [2] A.S. Bandeira, J. Niles-Weed, P. Rigollet, Optimal rates of estimation for multi-reference alignment, *Math. Stat. Learn.* 2 (2019) 25–75.
- [3] A. Perry, J. Weed, A.S. Bandeira, P. Rigollet, A. Singer, The sample complexity of multireference alignment, *SIAM J. Math. Data Sci.* 1 (3) (2019) 497–517.
- [4] D. Edidin, J. Katz, Orbit recovery from invariants of low degree in representations of finite groups, in: 2025 International Conference on Sampling Theory and Applications (SampTA), Vienna, Austria, 2025, pp. 1–5.
- [5] B. Blum-Smith, H. Derksen, Generic orbits, normal bases, and generation degree for fields of rational invariants, 2026, arXiv:2506.05650.
- [6] B. Blum-Smith, T. García, R. Hidalgo, C. Rodríguez, Degree bounds for fields of rational invariants of $\mathbb{Z}/p\mathbb{Z}$ and other finite groups, *J. Pure Appl. Algebra* 228 (2024), 107693.
- [7] K. Csiszter, M. Domokos, Lower bounds on the Noether number, *Transform. Groups* 24 (2019) 823–834.
- [8] D.R. Richman, Invariants of finite groups over fields of characteristic p , *Adv. Math.* 124 (1996) 25–48.
- [9] M. Domokos, Degree bound for separating invariants of finite abelian groups, *Proc. Amer. Math. Soc.* 145 (2017) 3695–3708.
- [10] B. Scheffler, The separating Noether number of the direct sum of several copies of a cyclic group, *Proc. Amer. Math. Soc.* 153 (2025) 69–79.
- [11] B. Scheffler, The separating Noether number of abelian groups of rank two, *J. Comb. Theory, Ser. A* 209 (2025). Paper no. 105951.
- [12] B. Scheffler, K. Zhao, Q. Zhong, On the separating Noether number of finite abelian groups, *Eur. J. Combinat.* 133 (2026). Paper no. 104302.
- [13] J. Cahill, J.W. Iverson, D.G. Mixon, Towards a bilipschitz invariant theory, *Appl. Comput. Harmon. Anal.* 72 (2024), 27, Article ID 101669.
- [14] J. Cahill, J.W. Iverson, D.G. Mixon, D. Packer, Group-invariant max filtering, *Foundat. Comput. Math.* 25 (2025) 1047–1084.
- [15] M. Domokos, Separating monomials for diagonalizable actions, *Bull. Lond. Math. Soc.* 55 (2023) 205–223.
- [16] E. Dufresne, J. Jeffries, Mapping toric varieties into low dimensional spaces, *Trans. Amer. Math. Soc.* (2026), To appear, <https://doi.org/10.1090/tran/7026>, arXiv:1602.07585v2.
- [17] H. Derksen, G. Kemper, Computational Invariant Theory, *Encyclopaedia of Mathematical Sciences* 130, Invariant Theory of Algebraic Transformation Groups VIII, Second Edition, Berlin, Heidelberg, Springer-Verlag, 2015.
- [18] G. Kemper, Separating invariants, *J. Symb. Comput.* 44 (2009) 1212–1222.
- [19] J. Draisma, G. Kemper, D. Wehlau, Polarization of separating invariants, *Canad. J. Math.* 60 (2008) 556–571.
- [20] P. Fleischmann, The Noether bound in invariant theory of finite groups, *Adv. Math.* 156 (2000) 23–32.
- [21] J. Fogarty, On Noether's bound for polynomial invariants of a finite group, *Electron. Res. Announc. Amer. Math. Soc.* 7 (2001) 5–7.
- [22] E. Noether, Der Endlichkeitssatz der Invarianten endlicher Gruppen, *Math. Ann.* 77 (1916) 89–92.
- [23] M. Kohls, H. Kraft, Degree bounds for separating invariants, *Math. Res. Lett.* 17 (2010) 1171–1182.
- [24] B.J. Schmid, Finite groups and invariant theory, in *Topics in Invariant Theory* M.-P. Malliavin, ed., 1478, Springer, 1989, 35–66. Lecture notes in mathematics.
- [25] K. Csiszter, M. Domokos, I. Szöllösi, The Noether numbers and the Davenport constants of the groups of order less than 32, *J. Algebra* 510 (2018) 513–541.
- [26] W. Narkiewicz, Finite abelian groups and factorization problems, *Colloq. Math.* 17 (1979) 319–330.
- [27] T. Bendory, N. Boumal, C. Ma, Z. Zhao, A. Singer, Bispectrum inversion with application to multireference alignment, *IEEE Trans. Signal Process* 66 (4) (2018) 1037–1050.
- [28] J.-P. Serre, Linear Representations of Finite Groups, *Graduate Texts in Mathematics* 42, Springer Verlag, New York, 1977.

- [29] F. Smach, C. Lemaitre, J.-P. Gauthier, J. Miteran, M. Atri, Generalized Fourier descriptors with applications to objects recognition in SVM context, *J. Math. Imaging Vision* 30 (2008) 43–71.
- [30] M. Domokos, Typical separating invariants, *Transform. Groups* 12 (2007) 49–63.
- [31] M. Neusel, M. Sezer, Separating invariants for modular p -groups and groups acting diagonally, *Math. Res. Lett.* 16 (2009) 1029–1036.
- [32] J. Cahill, A. Contreras, A.C. Hip, Stable separation of orbits for finite abelian group actions, *J. Fourier Anal. Appl.* 30 (12) (2024) 16.
- [33] Sagemath, Inc., CoCalc - Collaborative Calculation and Data Science, 2020. <https://cocalc.com>.