

SEPARATING VERSUS ORDINARY NOETHER NUMBERS

MÁTYÁS DOMOKOS AND BARNA SCHEFLER

ABSTRACT. Let G be a finite group and K a field containing an element of multiplicative order $|G|$. It is shown that if G has a cyclic subgroup of index at most 2, then the separating Noether number over K of G coincides with the Noether number over K of G . The same conclusion holds when G is the direct product of a dihedral group and the 2-element group. On the other hand, the smallest non-abelian groups G are found for which the separating Noether number over K is strictly less than the Noether number over K . Along the way the exact value of the separating Noether number is determined for all groups of order at most 16. The results show in particular that unlike the ordinary Noether number, the separating Noether number of a non-abelian finite group may well be equal to the separating Noether number of a proper direct factor of the group.

1. INTRODUCTION

The separating Noether number over a field K of a finite group G is the minimal positive integer d such that for any finite dimensional K -linear representation of G , any two distinct G -orbits can be distinguished by a polynomial G -invariant of degree at most d . For a finite dimensional vector space V over K we write $K[V]$ for the coordinate ring of V identified with the n -variable polynomial algebra $K[x_1, \dots, x_n]$, where the variables $x_1, \dots, x_n$ represent the coordinate functions on V with respect to a chosen basis. Let G be a finite group, and $\rho : G \rightarrow \mathrm{GL}(V)$ a representation of G on V . We shall say that (V, ρ) is a KG -module in this case; mostly we shall suppress ρ from the notation and we will say that V is a KG -module. Sometimes we write V_K instead of V when we want to make explicit the actual base field. The action of G on V induces an action on $K[V]$ via K -algebra automorphisms, such that the variables $x_1, \dots, x_n$ span a KG -submodule isomorphic to V^* (the G -module dual to V), and $K[V]$ is the symmetric tensor algebra of V^* . Consider

$$K[V]^G = \{f \in K[V] \mid \forall g \in G : g \cdot f = f\},$$

the subalgebra of G -invariants in $K[V]$. For $v \in V$ we shall denote by $G \cdot v$ the G -orbit of v , and by $\mathrm{Stab}_G(v) := \{g \in G \mid gv = v\}$ the stabilizer subgroup in G of v .

It is well known that for $v, w \in V$ with $G \cdot v \neq G \cdot w$, there exists an invariant $f \in K[V]^G$ with $f(v) \neq f(w)$ (see for example [15, Theorem 3.12.1], [31, Theorem 16] or [22, Lemma 3.1]). Therefore the general notion of a "separating set of invariants" (see [15, Definition 2.4.1]) reduces to the following in the case of finite groups:

2020 *Mathematics Subject Classification*. Primary 13A50; Secondary 13P15, 20C15.

Key words and phrases. polynomial invariants, separating sets, degree bounds, finite groups, Noether number.

Definition 1.1. A subset S of $K[V]^G$ is called a separating set if for any $v, w \in V$, $f(v) = f(w)$ for all $f \in S$ implies that v and w have the same G -orbit.

The result mentioned before Definition 1.1 implies that every generating set of the algebra $K[V]^G$ is a separating set. In the structural study of algebras of polynomial invariants of finite groups the focus on separating sets (instead of the more special generating sets) turned out to be useful in finding strengthened versions of known theorems in the invariant theory of finite groups, see for example [23], [24]. Considering explicit computations of invariants, the class of modular representations for which generators of the corresponding algebra of invariants is known is very limited. On the other hand, in several such cases explicit finite separating sets are known, see for example [47], [35]. The minimal possible size of a separating set is investigated in [25]. In the non-modular case, an explicit separating set of multisymmetric polynomials is given in [37]. The systematic study of separating invariants over finite fields began recently in [32], [36].

1.1. Degree bounds. Endow $K[V]$ with the standard grading, so the variables $x_1, \dots, x_n$ span the degree 1 homogeneous component of $K[V]$. We shall denote by $\deg(f)$ the degree of a non-zero homogeneous element of $K[V]$. Obviously, $K[V]^G$ is spanned by homogeneous elements, so it inherits the grading from $K[V] = \bigoplus_{d=0}^{\infty} K[V]_d$. We shall write $K[V]_{\leq d}^G$ for the sum of the homogeneous components of degree at most d . Degree bounds for generators of algebras of invariants have always been in the focus of invariant theory (see e.g. [48]). We set

$$\begin{aligned}\beta(G, V) &:= \min\{d \in \mathbb{N}_0 \mid K[V]_{\leq d}^G \text{ generates the } K\text{-algebra } K[V]^G\}, \\ \beta^K(G) &:= \sup\{\beta(G, V) \mid V \text{ is a finite dimensional } KG\text{-module}\}.\end{aligned}$$

The quantity $\beta^K(G)$ is called the *Noether number of G (over K)* because of the classical inequality $\beta^{\mathbb{C}}(G) \leq |G|$ due to E. Noether [38] (the inequality was extended to the non-modular case in [27], [28]). Its systematic study was initiated in [45]. The results of [45] were improved first in [19], [46] and later in [10], [11]. In particular, [14, Table 1] gives the exact value of the Noether number for all non-abelian groups of order less than 32, and [11] gives the Noether number for all groups containing a cyclic subgroup of index two.

Following [34, Definition 2] (see also [31]) we set

$$\beta_{\text{sep}}(G, V) := \min\{d \in \mathbb{N}_0 \mid K[V]_{\leq d}^G \text{ is a separating set}\},$$

and

$$\beta_{\text{sep}}^K(G) := \sup\{\beta_{\text{sep}}(G, V) \mid V \text{ is a finite dimensional } G\text{-module over } K\}.$$

We shall refer to the above quantities as the *separating Noether number of G over K* . As different orbits of a finite group can be separated by polynomial invariants, we have the obvious inequality $\beta_{\text{sep}}(G, V) \leq \beta(G, V)$ for any V , and hence

$$(1) \quad \beta_{\text{sep}}^K(G) \leq \beta^K(G).$$

A major difference between the Noether number and its separating version is that if the characteristic of the base field K divides the order of G , then $\beta^K(G) = \infty$ by [40], whereas $\beta_{\text{sep}}^K(G) \leq |G|$ also in the modular case (see for example the proof of [15, Theorem 3.12.1],

[31, Theorem 16] or [22, Lemma 3.1]). For some results on degree bounds on separating invariants in the modular case see [34, Theorem C], [26]. However, in the present paper our focus is on the non-modular setup, when the characteristic of the base field does not divide the order of G . Interest in these degree bounds (over the real or complex field) arose also in recent applications for data science and machine learning, see [1], [5], [6], [7]. We mention also that problems in signal processing motivated the study of a variant of the Noether number for rational invariants in [4] (see [2] for a very recent result on this).

In this non-modular context an interesting and generally open question is the following:

Question 1.2. *To what extent is the change from "generating sets" to "separating sets" reflected in the corresponding degree bounds?*

It is proved in [17, Corollary 3.11] that for an abelian group G and a field K containing an element of multiplicative order $\exp(G)$, typically $\beta_{\text{sep}}^K(G)$ is strictly smaller than $\beta^K(G)$. It is natural to expect similar typical behavior for non-abelian finite groups as well, but as far as we know, the only information in the literature concerning this question is in [9], where the separating Noether number of the non-abelian groups of order $3p$ for some prime p congruent to 1 modulo 3 is determined. One of the obstacles is that the exact value of the Noether number is known only for a limited class of groups. This is the case already for abelian groups, whose Noether number equals their Davenport constant. However, the separating Noether number was determined recently for classes of abelian groups whose Noether number (Davenport constant) is not known, see [42], [44]. This may be a hint that perhaps the separating Noether number can be computed also for groups whose Noether number is out of reach. As a natural start one should first compute the separating Noether number at least for those groups whose Noether number is known. This is done in [43], [44] in the case of abelian groups, and we begin this project for non-abelian groups in the present paper. The Noether numbers of all the groups with a cyclic subgroup of index at most 2 and for the remaining groups of order less than 32 were computed in [11] and [14], respectively.

Here we determine the separating Noether numbers for the groups with a cyclic subgroup of index at most 2 (as well as for the direct product of a dihedral group and the 2-element group), and for all groups of order at most 16, working over a base field K having an element whose multiplicative order equals the order of the group (note that it turns out that the smallest non-abelian groups G with $\beta_{\text{sep}}(G) < \beta(G)$ have order 16). Our arguments do not rely on computer calculations (see Section 7 for comments on possible use of computers and its theoretical limitations in computation of the separating Noether number for concrete groups). The present work is a shortened version of our preprint [20], whose other results (covering the remaining groups of order less than 32) will be published elsewhere.

Running assumption. Throughout this paper G will stand for a finite group, and K for a field. Unless explicitly stated otherwise, it is assumed that the characteristic of K does not divide $|G|$.

2. MAIN RESULTS

Our first result builds on [11] (see the equality (9)) and shows that for a group with a cyclic subgroup of index 2 (their classification will be recalled in Section 4) the inequality (1) holds with equality, namely:

Theorem 2.1. *Let G be a non-cyclic finite group with a cyclic subgroup of index 2, and assume that K contains an element of multiplicative order $|G|$. Then we have the equality*

$$\beta_{\text{sep}}^K(G) = \frac{1}{2}|G| + \begin{cases} 2 & \text{if } G = \text{Dic}_{4m}, m > 1; \\ 1 & \text{otherwise.} \end{cases}$$

Using [11, Corollary 5.5] we are able to determine the separating Noether number for another infinite sequence of non-abelian finite groups:

Theorem 2.2. *For $n \geq 2$ even consider the direct product $G := D_{2n} \times C_2$ of the dihedral group of order $2n$ and the cyclic group C_2 of order 2. Assume that K has an element with multiplicative order n . Then we have*

$$\beta_{\text{sep}}^K(D_{2n} \times C_2) = n + 2.$$

There are 16 non-abelian groups of order less than 32 not covered by Theorem 2.1 or Theorem 2.2. We discuss them in the following theorem:

Theorem 2.3. *Let G be a group of order at most 16 that does not contain a cyclic subgroup of index at most 2, and G is not isomorphic to $D_{2n} \times C_2$. Assume that K contains an element of multiplicative order $|G|$. The value of $\beta_{\text{sep}}^K(G)$ is given in the following table:*

GAP	G	$\beta^K(G)$	$\beta_{\text{sep}}^K(G)$	reference for $\beta_{\text{sep}}^K(G)$
(8, 5)	$C_2 \times C_2 \times C_2$	4	4	[17, Theorem 3.10]
(9, 2)	$C_3 \times C_3$	5	4	[42, Theorem 1.2]
(12, 3)	A_4	6	6	Theorem 5.2
(16, 2)	$C_4 \times C_4$	7	6	[42, Theorem 1.2]
(16, 3)	$(C_2 \times C_2) \rtimes C_4 = (C_4 \times C_2) \rtimes_{\psi} C_2$	6	6	Theorem 5.3
(16, 4)	$C_4 \rtimes C_4$	7	6	Theorem 6.14
(16, 10)	$C_2 \times C_2 \times C_4$	6	6	[17, Theorem 3.10]
(16, 12)	$\text{Dic}_8 \times C_2$	7	6	Theorem 6.8
(16, 13)	$(\text{Pauli}) = (C_4 \times C_2) \rtimes_{\phi} C_2$	7	7	Theorem 5.4
(16, 14)	$C_2 \times C_2 \times C_2 \times C_2$	5	5	[17, Theorem 3.10]

The first column in the above table contains the identifier of G in the Small Groups Library of GAP (see [29]); that is, a pair of the form `(order, i)`, where the GAP command `SmallGroup(order, i)` returns the i -th group of order `order` in the catalogue. The second column gives G in a standard notation or indicates its structure as a direct product or semidirect product (the symbol $\rtimes$ always stands for a semidirect product that is not a direct product, and ψ and ϕ in the rows (16, 3) and (16, 13) stand for two different involutive automorphisms of $C_4 \times C_2$). The presentation of G in terms of generators and relations can be found in the beginning of the section that contains the theorem referred to

in the last column for the value of $\beta_{\text{sep}}^K(G)$. The third column of the table contains $\beta^K(G)$; these values are taken from [14]. The fourth column contains $\beta_{\text{sep}}^K(G)$.

Note that in some cases the value for $\beta_{\text{sep}}^K(G)$ given in the table holds under weaker restrictions on K than the restrictions stated in Theorem 2.3. The exact conditions on K needed for the validity of our arguments are contained in the statement quoted in the last column of the table.

2.1. Comments on the base field. We would like to stress that the separating Noether number is more sensitive for the choice of the base field than the Noether number. It is shown in [33, Corollary 4.2] that the Noether number of a finite group depends only on the characteristic of the base field, so

$$\beta^K(G) = \begin{cases} \beta^{\mathbb{F}_p}(G) & \text{if } \text{char}(K) = p > 0; \\ \beta^{\mathbb{C}}(G) & \text{if } \text{char}(K) = 0. \end{cases}$$

Moreover, by [33, Theorem 4.7], for all but finitely many primes p we have $\beta^{\mathbb{F}_p}(G) \geq \beta^{\mathbb{C}}(G)$.

On the other hand, the behavior of the separating Noether number in this respect is very different. For example, it is proved in [18] that for any prime order group C_p we have $\beta_{\text{sep}}^{\mathbb{Q}}(C_p) = 3$ (except for $p = 2$, when $\beta_{\text{sep}}^{\mathbb{Q}}(C_2) = 2$), whereas it is well known and easy to see that $\beta_{\text{sep}}^{\mathbb{C}}(C_p) = p$ (and also $\beta_{\text{sep}}^{\mathbb{R}}(C_p) = p$ by [4, Proposition 3.13]).

However, let us record some general facts relating the dependence of the separating Noether number on the base field.

Lemma 2.4. *Let F be a subfield of a field L , and let V_F be an FG -module.*

- (i) *For any non-negative integer d , the L -vector space $L[V_L]_d^G$ is spanned by its subset $F[V_F]_d^G$.*
- (ii) *We have the inequality $\beta_{\text{sep}}(G, V_F) \leq \beta_{\text{sep}}(G, V_L)$.*
- (iii) *We have the inequality $\beta_{\text{sep}}^F(G) \leq \beta_{\text{sep}}^L(G)$.*

Proof. (i) It is well known, and follows from the fact that the space of solutions over L of a system of homogeneous linear equations with coefficients in F is spanned by the subset of solutions over F .

(ii) Take any $v, v' \in V_F \subseteq V_L$ with $G \cdot v \neq G \cdot v'$. Then there exists an $f \in L[V_L]_d^G$ with $d \leq \beta_{\text{sep}}(G, V_L)$ such that $f(v) \neq f(v')$. It follows by (i) that there exists an $h \in F[V_F]_d^G$ with $h(v) \neq h(v')$. This clearly shows the desired inequality.

(iii) is an immediate consequence of (ii). □

Proposition 2.5. *Let G be a finite abelian group. Then we have*

$$(2) \quad \beta_{\text{sep}}^K(G) \leq \beta_{\text{sep}}^{\mathbb{C}}(G), \text{ with equality when } K \text{ contains an element} \\ \text{whose multiplicative order equals the exponent of } G.$$

Proof. In [17, Corollary 2.6], a characterization purely in terms of G (and not referring to K) is given for $\beta_{\text{sep}}^K(G)$, valid when K contains an element whose multiplicative order equals the exponent of G (in fact [17] assumes that the base field is algebraically closed, but the proof of the quoted result works verbatim under the present weaker assumption

on K). So $\beta_{\text{sep}}^K(G) = \beta_{\text{sep}}^{\mathbb{C}}(G)$ when K contains an element of multiplicative order $|G|$. In particular, for any K we have $\beta_{\text{sep}}^{\overline{K}}(G) = \beta_{\text{sep}}^{\mathbb{C}}(G)$, where $\overline{K}$ is the algebraic closure of K (recall the running assumption that $|G|$ is invertible in K). Note finally that by Lemma 2.4 (iii) we have $\beta_{\text{sep}}^K(G) \leq \beta_{\text{sep}}^{\overline{K}}(G)$. $\square$

2.2. Failure of strict monotonicity. For a normal subgroup N of G , all representations of G/N can be viewed as a representation of G whose kernel contains N . Therefore we have the obvious inequalities

$$(3) \quad \beta^K(G) \geq \beta^K(G/N) \text{ and } \beta_{\text{sep}}^K(G) \geq \beta_{\text{sep}}^K(G/N).$$

Moreover, both the Noether number and the separating Noether number are monotone for subgroups as well; that is, for any subgroup H of a finite group G we have

$$(4) \quad \beta^K(G) \geq \beta^K(H) \text{ (see [45]) and } \beta_{\text{sep}}^K(G) \geq \beta_{\text{sep}}^K(H) \text{ (see [34, Theorem B]).}$$

The first inequality (4) was sharpened in [12, Theorem 1.2], where the following strict monotonicity of the Noether number was proved:

$$(5) \quad \begin{aligned} &\beta^K(G) > \beta^K(H) \text{ for any subgroup } H \neq G; \\ &\beta^K(G) > \beta^K(G/N) \text{ for any normal subgroup } N \neq \{1_G\} \text{ of } G. \end{aligned}$$

The results of Theorem 2.1 and Theorem 2.3 show that the analogues of (5) (i.e. strict monotonicity) does not hold for the separating Noether number. Indeed, for K as in the cited theorems, we have

$$\beta_{\text{sep}}^K(\text{Dic}_8) = 6 = \beta_{\text{sep}}^K(\text{Dic}_8 \times \text{C}_2),$$

and $\text{Dic}_8 \times \text{C}_2$ has a proper direct factor isomorphic to Dic_8 . Similar examples exist among the abelian groups. For example, we have

$$\beta_{\text{sep}}^K(\text{C}_6 \oplus \text{C}_6 \oplus \text{C}_6) = 12 = \beta_{\text{sep}}^K(\text{C}_6 \oplus \text{C}_6 \oplus \text{C}_3)$$

by [42, Theorem 6.1].

2.3. Comments on the methods used. We make an essential use of the known results on exact values of the Noether numbers (as summarized in [14]) of the groups considered here. In particular, in each case when the Noether number and the separating Noether number happen to coincide, we just need to come up with a representation and two points with distinct orbits that can not be separated by invariants of strictly smaller degree than the Noether number. In all such cases it turns out that rather small dimensional representations suffice to provide such examples. On the other hand, to settle the cases when the separating Noether number is strictly smaller than the Noether number requires elaborate work: we need a thorough analysis of concrete representations, discussions of stabilizers, group automorphisms, construction of invariants and relative invariants, as well as several ad hoc ideas that help to understand the set of solutions of systems of polynomial equations. What makes these computations feasible is that by general principles (see the

notion of Helly dimension and Lemma 6.2 below) it is sufficient to deal with representations having a small number of irreducible summands.

2.4. Organization of the paper. In Section 3 we introduce notation and collect general facts used throughout the paper. We turn in Section 4 to the proof of Theorem 2.1 and Theorem 2.2. In Section 5 we deal with the remaining groups of order less than or equal to 16 for which the separating Noether number equals the Noether number, namely with the alternating group A_4 , the non-abelian semi-direct product $(C_2 \times C_2) \rtimes C_4$, and the Pauli group. In Section 6 we discuss the smallest non-abelian groups whose separating Noether number is strictly smaller than the Noether number, namely $\text{Dic}_8 \times C_2$ and $C_4 \rtimes C_4$. In Section 7 we sketch an algorithm (implemented in SageMath) that can compute the separating Noether number of a small group G over the algebraic closure of a chosen base field K (and hence provides an upper bound for the separating Noether number $\beta_{\text{sep}}^K(G)$).

3. PRELIMINARIES

3.1. Notational convention. Denote by $\widehat{G}$ the group of characters of G (i.e. the group of homomorphisms $G \rightarrow K^\times$, written multiplicatively). For $\chi \in \widehat{G}$ denote by U_χ the 1-dimensional vector space K endowed with the representation χ ; that is, $g \cdot \lambda = \chi(g)\lambda$ for $g \in G$ and $\lambda \in K$. In several cases we shall deal with a KG -module

$$(6) \quad V = W \oplus U, \quad W = W_1 \oplus \cdots \oplus W_l, \quad U = U_{\chi_1} \oplus \cdots \oplus U_{\chi_m},$$

where the W_i are pairwise non-isomorphic irreducible KG -modules of dimension at least 2, the $\chi_1, \dots, \chi_m$ are distinct characters of G . We shall denote by $x_1, x_2, \dots$ the coordinate functions on W_1 , by $y_1, y_2, \dots$ the coordinate functions on W_2 , $z_1, z_2, \dots$ the coordinate functions on W_3 , etc., and denote by t_χ the coordinate function on U_χ . Usually we shall specify a concrete representation of G (in other words, a KG -module) by giving a group homomorphism $\psi : G \rightarrow \text{GL}_n(K)$. The underlying vector space is then the space of column vectors $V = K^n$, on which $g \in G$ operates via multiplication by the matrix $\psi(g)$. The action of G on the variables $x_1, \dots, x_n$ (which form a basis in the dual space V^* of V) is given explicitly by the following formula:

$$g \cdot x_j = \sum_{i=1}^n \psi(g^{-1})_{ji} x_i,$$

whereas we have $g \cdot t_\chi = \chi(g^{-1})t_\chi$. Associated to the above direct sum decomposition of V is an $\mathbb{N}_0^{l+m}$ -grading on $K[V]$: this corresponds to the action of the torus $(K^\times)^{l+m}$ given by $(\lambda_1, \dots, \lambda_{l+m}) \cdot (w_1, \dots, w_l, u_1, \dots, u_m) = (\lambda_1 w_1, \dots, \lambda_{l+m} u_m)$. The phrase ‘multihomogeneous’ will refer to this multigrading. Since the above torus action commutes with the G -action on V , the algebra $K[V]^G$ is spanned by multihomogeneous elements. In particular, for $v, v' \in V$ and a positive integer d , we have that

$$(7) \quad \begin{aligned} &v, v' \text{ can be separated by a homogeneous invariant of degree } d \\ \iff &v, v' \text{ can be separated by a multihomogeneous invariant of degree } d. \end{aligned}$$

We shall write A^T for the transpose of the matrix (e.g. row vector) A .

3.2. Relative invariants. An element $f \in K[V]$ is a *relative invariant of weight* $\chi \in \widehat{G}$ if $g \cdot f = \chi(g^{-1})f$ for all $g \in G$ (so $f(gv) = \chi(g)f(v)$ for all $g \in G$ and $v \in V$). We set

$$K[V]^{G,\chi} := \{f \in K[V] \mid f \text{ is a relative invariant of weight } \chi\}.$$

For example, if V is as in (6), then the variable t_χ is a relative invariant of weight χ . Any multihomogeneous element in $K[V]$ is of the form ft , where $f \in K[W]$ and $t = \prod_{j=1}^m t_{\chi_j}^{n_j}$. Note that t is a relative invariant of weight $\prod_{j=1}^m \chi_j^{n_j}$. So ft is a G -invariant if and only if f is a relative invariant whose weight is the inverse of the weight of t .

4. GROUPS WITH A CYCLIC SUBGROUP OF INDEX TWO

Denote by C_n the cyclic group of order n . We use the notation for semidirect products

$$C_m \rtimes_d C_n = \langle a, b \mid a^m = 1, b^n = 1, bab^{-1} = a^d \rangle \quad \text{where } d \in \mathbb{N} \text{ is coprime to } m.$$

We need the following classification of finite groups with a cyclic subgroup of index 2 (see [11, Section 10] for details and references):

Proposition 4.1. *Any finite group containing a cyclic subgroup of index two is isomorphic to*

$$(8) \quad C_s \times (C_r \rtimes_{-1} H)$$

where r, s are coprime odd integers, $C_r \rtimes_{-1} H$ is the semidirect product where the kernel of the action of H on C_r contains an index two cyclic subgroup $\langle a \rangle$ of H , $b \in H \setminus \langle a \rangle$ acts via inversion on C_r (i.e. $bx b^{-1} = x^{-1}$ for all $x \in C_r$), and H is one of the following 2-groups:

- (i) C_{2^n} ($n \geq 1$);
- (ii) $C_{2^{n-1}} \times C_2$ ($n \geq 2$);
- (iii) $M_{2^n} := C_{2^{n-1}} \rtimes_d C_2$, $d = 2^{n-2} + 1$ ($n \geq 3$);
- (iv) $D_{2^n} := C_{2^{n-1}} \rtimes_{-1} C_2$ ($n \geq 4$);
- (v) $SD_{2^n} := C_{2^{n-1}} \rtimes_d C_2$, $d = 2^{n-2} - 1$ ($n \geq 4$);
- (vi) $\text{Dic}_{2^n} := \langle a, b \mid a^{2^{n-1}} = 1, b^2 = a^{2^{n-2}}, bab^{-1} = a^{-1} \rangle$ ($n \geq 3$).

Among the groups listed in Proposition 4.1 are the dicyclic groups. For a positive integer $m > 1$, the *dicyclic group* is

$$\text{Dic}_{4m} = \begin{cases} C_r \rtimes_{-1} \text{Dic}_{2^n} & \text{for } m = 2^{n-2}r \text{ even} \\ C_m \rtimes_{-1} C_4 & \text{for } m > 1 \text{ odd.} \end{cases}$$

Note that Dic_8 is the *quaternion group* of order 8.

Proposition 4.2. *Let G be a non-cyclic group with a cyclic subgroup of index two. Assume that K has an element of multiplicative order $|G|$. Then*

$$\beta_{\text{sep}}^K(G) \geq \frac{1}{2}|G| + \begin{cases} 2 & \text{if } G = \text{Dic}_{4m}, m > 1; \\ 1 & \text{otherwise.} \end{cases}$$

Proof. Let G be a group as in (8) in Proposition 4.1, where H is a semidirect product of a cyclic group and the two-element group (so H is C_2 or H is of type (ii), (iii), (iv), or (v) from Proposition 4.2). Then G has a matrix representation generated by the matrices

$$\begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & -1 \end{bmatrix}, \quad \begin{bmatrix} \xi & 0 & 0 \\ 0 & \xi^k & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} \rho & 0 & 0 \\ 0 & \rho^{-1} & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} \varepsilon & 0 & 0 \\ 0 & \varepsilon & 0 \\ 0 & 0 & 1 \end{bmatrix},$$

where k is some positive integer coprime to 2^{n-1} depending on the type of H , and ξ, ρ, ε are roots of 1 of multiplicative order 2^{n-1} , r, s . Consider the corresponding algebra $K[x_1, x_2, t]^G$, where x_1, x_2, t are the coordinate functions on the vector space K^3 , on which the group G acts via the given matrix representation. Setting $m := sr2^{n-1}$, the monomials x_1^m and x_2^m are fixed by the cyclic index two subgroup A of G generated by the second, third, and fourth matrices above. Moreover, they are interchanged by the first matrix. It follows that $(x_1^m - x_2^m)t$ is a G -invariant. This degree $m+1$ invariant takes different values on the vectors $v := [1, 0, 1]^T$ and $v' := [1, 0, -1]^T$ in K^3 .

Note that our representation is the direct sum of a 2-dimensional and a 1-dimensional representation. So by (7) it is sufficient to show that v and v' can not be separated by a *multihomogeneous* invariant of degree at most m . Suppose for contradiction that $f(v) \neq f(v')$, where f is a multihomogeneous invariant of degree at most m . So $f = t^d f_1(x_1, x_2)$. Since the projections of these two vectors in the x_1, x_2 coordinate plane are the same, no invariant depending only on x_1 and x_2 can separate them. Thus we have $d > 0$. The invariants depending only on t are the polynomials in t^2 , which take the same value (namely 1) on these vectors, hence $\deg(f_1) > 0$. Since t is A -invariant, $f_1(x_1, x_2) \in K[x_1, x_2]^A$, so f_1 is a K -linear combination of A -invariant monomials in x_1 and x_2 . The monomials having positive degree in x_2 vanish on both v and v' . It follows that f_1 must have an A -invariant monomial depending only on x_1 . The only such monomials are the powers of x_1^m . Thus $\deg(f) \geq m + d > m$, a contradiction.

Assume next that G is a dicyclic group Dic_{4m} . It is isomorphic to the matrix group generated by

$$\begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}, \quad \begin{bmatrix} \rho & 0 \\ 0 & \rho^{-1} \end{bmatrix}$$

where i is an element of K with multiplicative order 4 (so $i^2 = -1$) and ρ is an element of K of multiplicative order $2m$. It is an easy exercise to show that the corresponding algebra of invariants is generated by $x_1^{2m} - x_2^{2m}$, $(x_1 x_2)^2$, $(x_1^{2m} + x_2^{2m})x_1 x_2$ when m is odd, and by $x_1^{2m} + x_2^{2m}$, $(x_1 x_2)^2$, $(x_1^{2m} - x_2^{2m})x_1 x_2$ when m is even. If m is odd, the vectors $[1, 1]^T$ and $[1, -1]^T$ are separated by the degree $2m+2$ generator, but all the smaller degree generators agree on them. By assumption K has an element ν of multiplicative order $4m = |G|$. For even m the vectors $[\nu, 1]^T$ and $[\nu, -1]^T$ are separated by the degree $2m+2$ generator, whereas the smaller degree generators coincide on them.

A matrix representation of $C_s \times \text{Dic}_{4m}$ (where $s > 1$ is odd and is co-prime to m) is generated by

$$\begin{bmatrix} 0 & i & 0 \\ i & 0 & 0 \\ 0 & 0 & -1 \end{bmatrix}, \quad \begin{bmatrix} \rho & 0 & 0 \\ 0 & \rho^{-1} & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} \varepsilon & 0 & 0 \\ 0 & \varepsilon & 0 \\ 0 & 0 & 1 \end{bmatrix},$$

where ρ and ε are roots of 1 with multiplicative order $2m$ and s . The vectors $v := [1, 0, 1]^T$ and $v' := [1, 0, -1]^T$ are separated by the invariant $(x_1^{2ms} - x_2^{2ms})t$ when m is odd and by $(x_1^{2ms} + x_2^{2ms})t$ when m is even. On the other hand, any invariant of degree at most $2ms$ takes the same value on v and v' (this can be seen similarly to the argument in the second paragraph of the proof).

It remains to deal with the case when $G \cong C_s \times (C_r \rtimes_{-1} C_{2^n})$ where $n \geq 3$. A matrix representation of this group is generated by

$$\begin{bmatrix} 0 & \omega & 0 \\ \omega & 0 & 0 \\ 0 & 0 & -1 \end{bmatrix}, \quad \begin{bmatrix} \rho & 0 & 0 \\ 0 & \rho^{-1} & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} \varepsilon & 0 & 0 \\ 0 & \varepsilon & 0 \\ 0 & 0 & 1 \end{bmatrix},$$

where ω , ρ and ε are roots of 1 with multiplicative order 2^n , r , and s . The square of the first matrix together with the second and the third generate a cyclic subgroup A of G of order $m := 2^{n-1}rs$, acting on the line spanned by $[1, 0, 0]^T$ via a character of order m . The invariant $(x_1^m + x_2^m)t$ separates $v := [1, 0, 1]^T$ and $v' := [1, 0, -1]^T$, and any invariant of degree at most m takes the same value on v and v' (this can be seen similarly to the argument in the second paragraph of the proof). $\square$

Proof of Theorem 2.1. The Noether number $\beta^K(G)$ was computed for all groups with a cyclic subgroup of index 2 in [11, Theorem 10.3], where (as a special case of a statement on the so-called generalized Noether number) it was shown that if G is a non-cyclic group with a cyclic subgroup of index two and $\text{char}(K)$ is not a divisor of $|G|$, then

$$(9) \quad \beta^K(G) = \frac{1}{2}|G| + \begin{cases} 2 & \text{if } G = \text{Dic}_{4m}, \ m > 1; \\ 1 & \text{otherwise.} \end{cases}$$

Therefore the desired result on the separating Noether number is an immediate consequence of Proposition 4.2, the obvious inequality $\beta_{\text{sep}}^K(G) \leq \beta^K(G)$, and (9). $\square$

4.1. The groups $D_{2n} \times C_2$. In this section $n \geq 2$ is even, and

$$G = D_{2n} \times C_2 = \langle a, b, c \mid a^n = b^2 = c^2 = 1, \ bab = a^{-1}, \ ac = ca, \ bc = cb \rangle.$$

Proposition 4.3. *Assume that K contains an element of multiplicative order n . Then we have the inequality $\beta_{\text{sep}}^K(G) \geq n + 2$.*

Proof. Let ρ denote an element of K of multiplicative order n . Take the direct sum of the representations

$$\begin{aligned} a &\mapsto \begin{bmatrix} \rho & 0 \\ 0 & \rho^{-1} \end{bmatrix}, & b &\mapsto \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, & c &\mapsto \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \\ a &\mapsto 1, \quad b \mapsto -1, \quad c \mapsto -1 & \text{and} & a \mapsto 1, \quad b \mapsto 1, \quad c \mapsto -1. \end{aligned}$$

Recall that x_1, x_2 stand for the standard coordinate functions on the 2-dimensional summand, and t_1, t_2 stand for the coordinate functions on the 1-dimensional summands. The invariant $(x_1^n - x_2^n)t_1t_2$ separates the points $v := ([1, 0]^T, 1, 1)$ and $v' := ([1, 0]^T, 1, -1)$ in K^4 . It is sufficient to show that v and v' can not be separated by an invariant of degree at most $n + 1$. Suppose for contradiction that $h(v) \neq h(v')$ for some homogeneous $h \in K[x_1, x_2, t_1, t_2]^G$ of degree at most $n + 1$. We may assume by (7) that h is multihomogeneous (so it is homogeneous both in t_1 and t_2), and has minimal possible total degree. So $h = t_1^{k_1}t_2^{k_2}h_1(x_1, x_2)$. Since the (x_1, x_2, t_1) -coordinates of v and v' are the same, we have $k_2 > 0$. Since h_1 is $\langle c \rangle$ -invariant, $k_1 + k_2$ must be even. Moreover, $K[t_1, t_2]^G = K[t_1^2, t_2^2]$, and $t_1^2(v) = 1 = t_1^2(v')$, $t_2^2(v) = 1 = t_2^2(v')$, so $\deg(h_1) > 0$, and (since h has minimal possible degree) $h = t_1t_2h_1$. Thus h_1 is a relative G -invariant of degree at most $n - 1$, on which G acts via the character $a \mapsto 1$, $b \mapsto -1$, $c \mapsto 1$. The action of G on K^2 factors through the action of the dihedral group $D_{2n} \cong G/\langle c \rangle$, and it is well known (and easy to see) that the smallest degree relative invariant in $K[x_1, x_2]$ with the above weight is $x_1^n - x_2^n$. We reached the desired contradiction. $\square$

Proof of Theorem 2.2. We have the isomorphism

$$D_{2n} \times C_2 \cong (C_n \times C_2) \rtimes_{-1} C_2.$$

Therefore by [11, Corollary 5.5] we have

$$\beta^K(D_{2n} \times C_2) = D(C_n \times C_2) + 1,$$

where $D(C_n \times C_2)$ is the Davenport constant of the abelian group $C_n \times C_2$ (the maximal length of an irreducible product-one sequence over $C_n \times C_2$). By [39] we have $D(C_n \times C_2) = n + 1$, implying in turn that $\beta_{\text{sep}}^K(D_{2n} \times C_2) \leq n + 2$. The reverse inequality holds by Proposition 4.3. $\square$

5. FURTHER GROUPS WITH ORDER ≤ 16

5.1. The alternating group A_4 .

Proposition 5.1. *For $n \geq 4$ we have the inequality $\beta_{\text{sep}}^K(A_n) \geq n(n - 1)/2$.*

Proof. Our running assumption that $\text{char}(K)$ does not divide $|G|$ forces for $G = A_n$ that $|K| \geq n$ if $n \geq 4$. Therefore K has n distinct elements $v_1, \dots, v_n$. The vectors $v := [v_1, v_2, v_3, \dots, v_n]^T$ and $v' := [v_2, v_1, v_3, v_4, \dots, v_n]^T$ belong to the same orbit under the symmetric group S_n acting on K^n via permuting the coordinates, but v and v' have different orbits with respect to the alternating subgroup A_n . It is well known that the corresponding algebra of invariants is

$$K[x_1, \dots, x_n]^{A_n} = K[x_1, \dots, x_n]^{S_n} \oplus \Delta K[x_1, \dots, x_n]^{S_n},$$

where $\Delta := \sum_{1 \leq i < j \leq n} (x_i - x_j)$. This shows that all A_n -invariants of degree less than $n(n - 1)/2$ are in fact S_n -invariants. So they can not separate v and v' , which have different A_n -orbits. $\square$

It is known that $\beta^K(A_4) = 6$ (see [10, Theorem 3.4]), hence Proposition 5.1 has the following consequence:

Theorem 5.2. *We have the equality $\beta_{\text{sep}}^K(A_4) = 6$.*

5.2. The non-abelian group $(C_2 \times C_2) \rtimes C_4$. In this section

$$G := \langle a, b, c \mid a^2 = b^2 = c^4 = 1, \quad ab = ba, \quad cac^{-1} = b, \quad cbc^{-1} = a \rangle.$$

Theorem 5.3. *Assume that K has an element i of multiplicative order 4. Then we have the equality $\beta_{\text{sep}}^K((C_2 \times C_2) \rtimes C_4) = 6$.*

Proof. The equality $\beta^K(G) = 6$ is proved in [14, Proposition 3.10], so it is sufficient to prove that $\beta_{\text{sep}}^K(G) \geq 6$. The element c^2 belongs to the center of G , and the factor group $G/\langle c^2 \rangle$ is isomorphic to the dihedral group D_8 . The representation

$$a \mapsto \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad b \mapsto \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix}, \quad c \mapsto \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

has c^2 in its kernel and gives the defining representation of D_8 as the group of symmetries of a square in the euclidean plane. The element ab also belongs to the center of G , and the factor group $G/\langle ab \rangle \cong C_4 \times C_2$ is generated by the coset of c and the coset of a . Thus G has the 1-dimensional representations

$$a \mapsto 1, \quad b \mapsto 1, \quad c \mapsto i \quad \text{and} \quad a \mapsto -1, \quad b \mapsto -1, \quad c \mapsto i.$$

Take the direct sum of the above 2-dimensional and 1-dimensional representations, and denote by x_1, x_2 the standard coordinate functions on the 2-dimensional summand, and by t_1, t_2 the coordinate functions on the 1-dimensional summands. The corresponding ring $K[x_1, x_2, t_1, t_2]^G$ of invariants contains the invariant $h := (x_1^2 - x_2^2)t_1^3t_2$, separating the points $v := ([1, 0]^T, 1, 1)$ and $v' := ([1, 0]^T, 1, -1)$ in K^4 . By (7), in order to prove $\beta_{\text{sep}}^K(G) \geq 6$, it is sufficient to show that v and v' can not be separated by a multihomogeneous invariant of degree at most 5. Suppose for contradiction that $f(v) \neq f(v')$, where f is a multihomogeneous invariant of degree at most 5. It has positive degree in t_2 , because the (x_1, x_2, t_1) coordinates of v and v' are the same. Any G -invariant depending only on t_1 and t_2 is a polynomial in $t_1^4, t_1^2t_2^2, t_2^4$, and all these polynomials take the value 1 both at v and v' . So $f = t_1^{k_1}t_2^{k_2}f_1(x_1, x_2)$, where $0 < k_1 + k_2 \leq 4$, $\deg(f_1) > 0$, and k_2 is odd. Note that $t_1^{k_1}t_2^{k_2}$ is a relative G -invariant, hence $f_1(x_1, x_2)$ must be a relative G -invariant, on which G acts by the inverse character. Since c^2 fixes f_1 , it must fix also $t_1^{k_1}t_2^{k_2}$, so $k_1 + k_2$ is even. Consequently, $(k_1, k_2) \in \{(1, 1), (3, 1), (1, 3)\}$, and $f_1 \in K[x_1, x_2]$ is a relative $D_8 \cong G/\langle c^2 \rangle$ -invariant of degree at most $5 - (k_1 + k_2)$. There is no degree 1 relative G -invariant in $K[x_1, x_2]$, hence $t_1^{k_1}t_2^{k_2} = t_1t_2$, and so f is a relative invariant of degree at most 3. It is easy to see that up to non-zero scalar multiples, the only relative G -invariants in $K[x_1, x_2]_{\leq 3}$ with non-trivial weight are x_1x_2 and $x_1^2 - x_2^2$, but none of $x_1x_2t_1t_2$ or $(x_1^2 - x_2^2)t_1t_2$ is a G -invariant. We arrived at the desired contradiction, finishing the proof. $\square$

5.3. The Pauli group. Assume that the field K has an element i of multiplicative order 4. In this section G stands for the subgroup of $\mathrm{GL}(K^2)$ generated by the matrices

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \quad \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

Theorem 5.4. *Assume that K has an element of multiplicative order 4. We have the equality $\beta_{\mathrm{sep}}^K(G) = 7$.*

Proof. Since G is generated by reflections on the space K^2 , by the Sheppard-Todd-Chevalley Theorem (see e.g. [3, Theorem 7.2.1] or [15, Section 3.9.4]), $K[x_1, x_2]^G$ is a polynomial algebra with two generators. In fact it is generated by $x_1^4 + x_2^4$ and $(x_1 x_2)^2$. Moreover, the factor of $K[x_1, x_2]$ modulo the Hilbert ideal (the ideal generated by $x_1^4 + x_2^4$ and $(x_1 x_2)^2$) is isomorphic to the regular representation of G (see [8]). The element $f := (x_1^4 - x_2^4)x_1 x_2$ has the property that $g \cdot f = -f$ where g is any of the above three generators of G . One can easily see that f does not belong to the Hilbert ideal. Take an extra indeterminate t and extend the action of G to $K[x_1, x_2, t]$ by setting $g \cdot t = -t$ for any of the above three generators of G . Then ft is a degree 7 G -invariant separating $v := [1, 1, 1]^T$ and $v' := [1, 1, -1]^T$. We claim that v and v' can not be separated by an invariant of degree at most 6. Suppose for contradiction that h is a multihomogeneous G -invariant of degree at most 6 with $h(v) \neq h(v')$ (cf. (7)). Then h is homogeneous in t . Since v and v' have the same (x_1, x_2) coordinates, any element of $K[x_1, x_2]$ takes the same value on them, so h has positive degree in t . Moreover, since t^2 is G -invariant, we may assume that $h = th_1$ for some $h_1 \in K[x_1, x_2]$, where h_1 is homogeneous of degree at most 5. By G -invariance of h we must have that $g \cdot h_1 = -h_1$ for any of the above three generators g of G . However, this 1-dimensional representation of G occurs only once as a summand in the factor of $K[x_1, x_2]$ modulo the Hilbert ideal, and we found already one occurrence in the degree 6 homogeneous component. This contradiction proves the inequality $\beta_{\mathrm{sep}}^K(G) \geq 7$. The reverse inequality $\beta_{\mathrm{sep}}^K(G) \leq 7$ follows from the equality $\beta^K(G) = 7$ proved in [13, Example 5.4]. $\square$

6. THE SMALLEST NON-ABELIAN GROUPS WITH $\beta_{\mathrm{sep}}^K(G) < \beta^K(G)$

6.1. Reduction to multiplicity-free representations and the Helly dimension.

We record a consequence of the results of [22] and Lemma 2.4:

Lemma 6.1. *Let $V_1, \dots, V_q$ be a complete irredundant list of representatives of the isomorphism classes of simple KG -modules. Assume that*

$$|K| > (\max\{\dim(V_j) \mid j = 1, \dots, q\} - 1)|G|.$$

Then we have the equality

$$\beta_{\mathrm{sep}}^K(G) = \beta_{\mathrm{sep}}(G, V_1 \oplus \dots \oplus V_q).$$

Proof. An arbitrary KG -module V is isomorphic to $V_1^{m_1} \oplus \dots \oplus V_q^{m_q}$, where W^m stands for the direct sum $W \oplus \dots \oplus W$ of m copies of W . By [22, Corollary 2.6] we have $\beta_{\mathrm{sep}}(G, V) \leq \beta_{\mathrm{sep}}(G, V_1^{\dim(V_1)} \oplus \dots \oplus V_q^{\dim(V_q)})$, and by [22, Theorem 3.4 (ii)] and [22, Proposition 3.3 (ii)] we have $\beta_{\mathrm{sep}}(G, V_1^{\dim(V_1)} \oplus \dots \oplus V_q^{\dim(V_q)}) = \beta_{\mathrm{sep}}(G, V_1 \oplus \dots \oplus V_q)$. $\square$

Therefore to compute $\beta_{\text{sep}}^K(G)$ it is sufficient to deal with multiplicity-free representations of G (unless possibly if K is a finite field with too few elements). Lemma 6.1 can be improved for groups whose Helly dimension is 'small'. The *Helly dimension* $\kappa(G)$ is the minimal positive integer k having the following property: any set of cosets in G with empty intersection contains a subset of at most k cosets with empty intersection; this quantity was introduced in [16, Section 4]. Here we introduce a refinement, yielding sharper results in the present applications. Let $V = V_1 \oplus \cdots \oplus V_n$ be a KG -module with a fixed direct sum decomposition. Denote by $\kappa(G, V)$ the minimal positive integer k such that if $C_1, \dots, C_n$ are cosets in G , where C_i is a left coset with respect to the stabilizer subgroup in G of some element v_i in V_i , and $\cap_{i=1}^n C_i = \emptyset$, then there exists $1 \leq i_1 < \cdots < i_k \leq n$ with $\cap_{j=1}^k C_{i_j} = \emptyset$. Clearly $\kappa(G, V) \leq \kappa(G)$. The following statement is a variant of [21, Lemma 4.1].

Lemma 6.2. *Under the assumptions and notation of Lemma 6.1, there exists a $k \leq \kappa(G, V_1 \oplus \cdots \oplus V_q)$ and $1 \leq j_1 < \cdots < j_k \leq q$ with $\beta_{\text{sep}}^K(G) = \beta_{\text{sep}}(G, V_{j_1} \oplus \cdots \oplus V_{j_k})$.*

Proof. By Lemma 6.1 we have $\beta_{\text{sep}}^K(G) = \beta_{\text{sep}}(G, V)$, where $V = V_1 \oplus \cdots \oplus V_q$.

Assume that $d \geq \beta_{\text{sep}}(G, V_{i_1} \oplus \cdots \oplus V_{i_k})$ for all $1 \leq i_1 < \cdots < i_k \leq q$, where $k = \kappa(G, V)$. Take $v = (v_1, \dots, v_q)$ and $v' = (v'_1, \dots, v'_q)$ such that $f(v) = f(v')$ for all $f \in K[V]_{\leq d}^G$. Then $(v_{i_1}, \dots, v_{i_k})$ and $(v'_{i_1}, \dots, v'_{i_k})$ belong to the same G -orbit in $V_{i_1} \oplus \cdots \oplus V_{i_k}$ by the choice of d . In particular, $G \cdot v_j = G \cdot v'_j$ for $j = 1, \dots, q$. Set $C_j := \{g \in G \mid g \cdot v_j = v'_j\}$, then C_j is a left coset in G with respect to the stabilizer subgroup in G of v_j . Moreover, $\cap_{j=1}^k C_{i_j} \neq \emptyset$ (an element g with $g \cdot (v_{i_1}, \dots, v_{i_k}) = (v'_{i_1}, \dots, v'_{i_k})$ belongs to this intersection). This holds for all $1 \leq i_1 < \cdots < i_k \leq q$, hence by definition of $\kappa(G, V)$ we conclude that $\cap_{j=1}^q C_j \neq \emptyset$. For $g \in \cap_{j=1}^q C_j \neq \emptyset$ we have $g \cdot v = v'$. This shows the inequality $\beta_{\text{sep}}(G, V) \leq d$. In particular,

$$(10) \quad \beta_{\text{sep}}(G, V) \leq \beta_{\text{sep}}(G, V_{j_1} \oplus \cdots \oplus V_{j_k}),$$

where $\beta_{\text{sep}}(G, V_{j_1} \oplus \cdots \oplus V_{j_k}) = \max\{\beta_{\text{sep}}(G, V_{i_1} \oplus \cdots \oplus V_{i_k}) \mid 1 \leq i_1 < \cdots < i_k \leq q\}$.

The projection of V onto its direct summand $V_{j_1} \oplus \cdots \oplus V_{j_k}$ induces a degree-preserving embedding of $K[V_{j_1} \oplus \cdots \oplus V_{j_k}]^G$ into $K[V]^G$, hence $\beta_{\text{sep}}(G, V_{j_1} \oplus \cdots \oplus V_{j_k}) \leq \beta_{\text{sep}}(G, V)$, showing the reverse inequality to (10). $\square$

In view of Lemma 6.2, it is helpful to find upper bounds on the Helly dimension. By [16, Lemma 4.2] we have the inequality

$$(11) \quad \kappa(G) \leq \mu(G) + 1,$$

where $\mu(G)$ stands for the maximal size of an intersection independent set of subgroups of G . Recall that a set of subgroups of G is *intersection independent* if none contains the intersection of the others.

Lemma 6.3. *If a set S of intersection independent subgroups in a group contains a cyclic subgroup of prime power order, then $|S| \leq 2$.*

Proof. Let S be an intersection independent set of subgroups of a group G with $|S| \geq 2$ and $H \in S$ cyclic with $|H|$ a prime power. Take $J \in S$ with $J \cap H$ of minimal possible order. Since the lattice of subgroups of H is a chain, for any $L \in S$ we have $L \cap H \supseteq H \cap J$, hence

in particular $L \supseteq H \cap J$. Since S is intersection independent, it follows that $L \in \{H, J\}$. As $L \in S$ was arbitrary, it means that $S = \{H, J\}$. $\square$

6.2. The use of automorphisms. The natural action of the automorphism group of G on the isomorphism classes of representations of G helps to save some computations later, thanks to the following statements:

Lemma 6.4. *Let (V, ρ) be a KG -module and α an automorphism of the group G .*

(i) *For any $\chi \in \widehat{G}$ we have*

$$K[(V, \rho)]^{G, \chi} = K[(V, \rho \circ \alpha)]^{G, \chi \circ \alpha}.$$

In particular,

$$K[(V, \rho)]^G = K[(V, \rho \circ \alpha)]^G.$$

(ii) *We have*

$$\beta(G, (V, \rho)) = \beta(G, (V, \rho \circ \alpha)) \text{ and } \beta_{\text{sep}}(G, (V, \rho)) = \beta_{\text{sep}}(G, (V, \rho \circ \alpha)).$$

(iii) *Assume that $(V, \rho) \cong (V, \rho \circ \alpha)$ as KG -modules, so there exists a K -vector space isomorphism $T : V \rightarrow V$ with $T \circ \rho(g) = (\rho \circ \alpha)(g) \circ T$ for all $g \in G$. Then the map $f \mapsto f \circ T$ induces a K -vector space isomorphism*

$$K[(V, \rho)]^{G, \chi} \cong K[(V, \rho)]^{G, \chi \circ \alpha}.$$

Proof. (i) and (ii): The subset $\rho(G)$ of $\text{GL}(V)$ coincides with the subset $(\rho \circ \alpha)(G)$ of $\text{GL}(V)$, therefore the representations ρ and $\rho \circ \alpha$ yield the same partition of V into the union of G -orbits, and the same polynomials in $K[V]$ are invariants (respectively relative invariants) for the G -action given by ρ as for the G -action given by $\rho \circ \alpha$. Moreover, if $f \in K[(V, \rho)]^{G, \chi}$, $g \in G$ and $v \in V$, then $f((\rho \circ \alpha)(g)(v)) = f(\rho(\alpha(g))(v)) = \chi(\alpha(g))f(v) = (\chi \circ \alpha)(g)f(v)$. So if a relative invariant $f \in K[V]$ has weight χ with respect to ρ , then it has weight $\chi \circ \alpha$ with respect to $\rho \circ \alpha$. This explains both statements.

(iii): For each $g \in G$ we have

$$(f \circ T)(gv) = f((T \circ \rho(g))(v)) = f((\rho \circ \alpha)(g)(T(v))) = \chi(\alpha(g))f(T(v)) = (\chi \circ \alpha)(g)(f \circ T)(v).$$

$\square$

6.3. The group $\text{Dic}_8 \times C_2$. In this section

$$G = \text{Dic}_8 \times C_2 = \langle a, b \mid a^4 = 1, b^2 = a^2, ba = a^3b \rangle \times \langle c \mid c^2 = 1 \rangle$$

is the direct product of the quaternion group of order 8 and the group of order 2. Assume that K has an element i of multiplicative order 4. Then G has two irreducible 2-dimensional representations (up to isomorphism), namely

$$\psi_1 : a \mapsto \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}, \quad b \mapsto \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \quad c \mapsto \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

(this is the only 2 dimensional representation of Dic_8 lifted to G by the projection from G to its direct factor C_2), and

$$\psi_2 : a \mapsto \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}, \quad b \mapsto \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \quad c \mapsto \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix},$$

the representation ψ_1 tensored with the non-trivial representation $c \mapsto -1$ of C_2 . The other irreducible representations of G are 1-dimensional, and can be labeled by the elements of the subgroup $\widehat{G} := \{\pm 1\} \times \{\pm 1\} \times \{\pm 1\}$ of $K^\times \times K^\times \times K^\times$ as follows: identify $\chi = (\chi_1, \chi_2, \chi_3) \in \widehat{G}$ with the representation $\chi : G \rightarrow K^\times$ given by

$$\chi : a \mapsto \chi_1, \quad b \mapsto \chi_2, \quad c \mapsto \chi_3.$$

Denote by W_j the vector space K^2 endowed with the representation ψ_j for $j = 1, 2$, and for $\chi \in \widehat{G}$ denote by U_χ the vector space K endowed with the representation χ . Set

$$U := \bigoplus_{\chi \in \widehat{G}} U_\chi.$$

The coordinate functions on W_1 are denoted by x_1, x_2 , the coordinate functions on W_2 are y_1, y_2 , and the coordinate function on U_χ is t_χ for $\chi \in \widehat{G}$ (see Section 3.1).

Proposition 6.5. *For $i = 1, 2$ we have $\beta(G, W_i \oplus U) = 6$.*

Proof. First we deal with the case $i = 1$. It is well known (see for example the proof of Proposition 4.2) that

$$(12) \quad K[W_1]^G = K[(x_1 x_2)^2, x_1^4 + x_2^4, x_1 x_2 (x_1^4 - x_2^4)].$$

Denote by $\mathcal{H}(G, W_1)$ the ideal in $K[W_1]$ generated by the above three generators of $K[W_1]^G$ (called the *Hilbert ideal*). It is easy to verify that a Gröbner basis with respect to the lexicographic term order induced by $x_1 > x_2$ of the Hilbert ideal $\mathcal{H}(G, W_1)$ is $x_1^2 x_2^2, x_1^4 + x_2^4, x_2^6, x_1 x_2^5$. Using this Gröbner basis one can show that setting

$$s_{(1,-1,1)} := x_1 x_2, \quad s_{(-1,1,1)} := x_1^2 + x_2^2, \quad s_{(-1,-1,1)} := x_1^2 - x_2^2,$$

a KG -module direct complement in $K[x_1, x_2]$ of the Hilbert ideal $\mathcal{H}(G, W_1)$ is

$$\begin{aligned} & K \oplus \text{Span}_K\{x_1, x_2\} \oplus K s_{(1,-1,1)} \oplus K s_{(-1,1,1)} \oplus K s_{(-1,-1,1)} \oplus \text{Span}_K\{x_1^3, x_2^3\} \\ & \oplus \text{Span}_K\{x_1^2 x_2, x_1 x_2^2\} \oplus K s_{(1,-1,1)} s_{(-1,1,1)} \oplus K s_{(1,-1,1)} s_{(-1,-1,1)} \\ & \oplus K s_{(-1,1,1)} s_{(-1,-1,1)} \oplus \text{Span}_K\{x_1^5, x_2^5\}. \end{aligned}$$

The direct summands above are minimal G -invariant subspaces, and $s_\chi \in K[W_1]^{G, \chi}$. Recall that every multihomogeneous element of $K[W_1 \oplus U]^G$ is of the form ft , where $f \in K[W_1]$ and $t = \prod_{\chi \in \widehat{G}} t_\chi^{n_\chi}$ is a monomial. It follows that $K[W_1 \oplus U]^G$ is generated over $K[W_1]^G$ by products of elements from

$$(13) \quad \{s_\chi, \quad t_{\chi'} \mid \chi \in \{(1, -1, 1), (-1, 1, 1), (-1, -1, 1)\}, \chi' \in \widehat{G}\},$$

with no G -invariant proper subproduct. Moreover, it is sufficient to consider products from (13) with at most two factors of the form s_χ , because any product of three factors of

the form s_χ can be rewritten modulo the Hilbert ideal $\mathcal{H}(G, W_1)$ as a linear combination of shorter products of the s_χ . Any unordered sequence of 5 elements from $\widehat{G}$ has a proper product-one subsequence, since the Davenport constant of the group $\widehat{G}$ is 4 (for information about the Davenport constant and its relevance for the invariant theory of abelian groups see for example [13]). Thus the algebra $K[W_1 \oplus U]^G$ is generated by the generators of $K[W_1]^G$ and the products in (13) with at most two factors of the form s_χ , and with at most 4 factors in total. All these polynomials have degree at most 6.

The case $i = 2$ is essentially the same. Indeed, the map $x_1 \mapsto y_1, x_2 \mapsto y_2$ extends to a K -algebra isomorphism between $K[W_1]$ and $K[W_2]$, which is also a Dic_8 -module isomorphism. The subgroup $\langle c \rangle$ acts trivially on $K[W_1]$, and acts by multiplication by -1 of the variables y_1, y_2 in $K[W_2]$. Therefore replacing x_1 by y_1 and x_2 by y_2 in the corresponding formulae above, we get the generators of $K[W_2]^G$, as well as a direct sum decomposition into minimal G -invariant subspaces of a KG -module direct complement in $K[W_2]$ of the Hilbert ideal. So in the same way as in the above paragraph, we get the conclusion $\beta(W_2 \oplus U) = 6$. $\square$

Proposition 6.6. *We have $\beta(G, W_1 \oplus W_2) = 6$.*

Proof. The element $a^2 \in G$ multiplies each of the indeterminates x_1, x_2, y_1, y_2 by -1 . Since G -invariants are a^2 -invariant, they must involve only monomials of even degree. Thus $\beta(G, W_1 \oplus W_2)$ is even. On the other hand, $\beta^K(G) = 7$ by [14, Proposition 3.2]. We conclude that $\beta(G, W_1 \oplus W_2) \leq 6$. Note also that $\beta(G, W_1 \oplus W_2) \geq \beta(G, W_1)$, and we saw in the course of the proof of Proposition 6.5 that $\beta(G, W_1) = 6$ (the third generator in (12) is not symmetric in x_1 and x_2 , hence can not be expressed by the first two). $\square$

Proposition 6.7. *Let $v := (w_1, w_2) \in W_1 \oplus W_2$ with $w_1 \neq 0$ and $w_2 \neq 0$. Then for any $\chi \in \widehat{G}$ there exists a relative invariant f of weight χ such that $\deg(f) \leq 4$ and $f(v) \neq 0$.*

Proof.

χ	relative invariants
$(-1, 1, 1)$	$f_1 := x_1^2 + x_2^2, \quad f_2 := x_1 x_2 (x_1^2 - x_2^2)$
$(-1, 1, -1)$	$f_1 := x_1 y_1 + x_2 y_2, \quad f_2 := x_1 x_2 (x_1 y_1 - x_2 y_2), \quad f_3 := x_2^3 y_1 - x_1^3 y_2$
$(1, 1, -1)$	$f_1 := x_1 y_2 - x_2 y_1, \quad f_2 := x_1 x_2 (x_1 y_2 + x_2 y_1), \quad f_3 := x_2^3 y_2 + x_1^3 y_1$

A row in the above table contains a character $\chi \in \widehat{G}$ and relative invariants of weight χ of degree at most 4, such that the common zero-set of these relative invariants is contained in the union of $W_1 \oplus \{0\}$ and $W_2 \oplus \{0\}$. For the other non-trivial weights the result can be deduced without further computation using Lemma 6.4. Indeed, the automorphism group of G contains the automorphism group of its subgroup Dic_8 as a subgroup. The automorphism group of Dic_8 acts (on the right) therefore on $\widehat{G}$ (an automorphism α sends χ to $\chi \circ \alpha$), and any non-trivial $\chi \in \widehat{G}$ is in the orbit of one of the three weights in the above table. Moreover, for an automorphism α of Dic_8 (viewed as an automorphism of G) we have that $\psi_1 \circ \alpha \cong \psi_1$ and $\psi_2 \circ \alpha \cong \psi_2$. Observe that for $(w_1, w_2) \in W_1 \oplus W_2$, the condition that none of w_i ($i = 1, 2$) is zero is equivalent to the condition that $\{g \cdot (w_1, w_2) \mid g \in G\}$ spans $W_1 \oplus W_2$ as a K -vector space. Therefore by Lemma 6.4 (iii), no (w_1, w_2) with $w_1 \neq 0$,

$w_2 \neq 0$ is contained in the common zero locus $\mathcal{V}(f \mid f \in K[W_1 \oplus W_2]^{G, \chi^\alpha}, \deg(f) \leq 4)$ if no such element of $W_1 \oplus W_2$ is contained in $\mathcal{V}(f \mid f \in K[W_1 \oplus W_2]^{G, \chi}, \deg(f) \leq 4)$.

Note finally that for the trivial weight $(1, 1, 1) \in \widehat{G}$ we may take $f = 1 \in K[W_1 \oplus W_2]^G$. $\square$

Theorem 6.8. *Assume that K contains an element of multiplicative order 8. Then we have $\beta_{\text{sep}}^K(\text{Dic}_8 \times C_2) = 6$.*

Proof. By Theorem 2.1 we know that $\beta_{\text{sep}}^K(\text{Dic}_8) = 6$, and since Dic_8 is a direct factor of G , we have $\beta_{\text{sep}}^K(G) \geq \beta_{\text{sep}}^K(\text{Dic}_8) = 6$.

Now we turn to the reverse inequality. By Lemma 2.4 (iii) it is sufficient to deal with the case when $|K|$ is large enough so that we can apply Lemma 6.1. Therefore it remains to prove that $\beta_{\text{sep}}(G, V) \leq 6$ where $V = W_1 \oplus W_2 \oplus U$. That is, we have to show that if all invariants of degree at most 6 take the same value on $v, v' \in V$, then $G \cdot v = G \cdot v'$. So $v = (w_1, w_2, u_\chi \mid \chi \in \widehat{G})$ and $v' = (w'_1, w'_2, u'_\chi \mid \chi \in \widehat{G})$. It follows from Proposition 6.6 that replacing v' by an appropriate element in its G -orbit, we may assume that $w_1 = w'_1$ and $w_2 = w'_2$. If $w_1 = 0$ or $w_2 = 0$, then v and v' belong to the same orbit by Proposition 6.5. For any $\chi \in \widehat{G}$ there exists a relative invariant $f \in K[W_1 \oplus W_2]^{G, \chi^{-1}}$ with $\deg(f) \leq 4$ and $f(w_1, w_2) \neq 0$ by Proposition 6.7. Consider the invariant $ft_\chi \in K[V]^G$: it has degree at most 5, and so from $(ft_\chi)(v) = (ft_\chi)(v')$ we deduce $u_\chi = u'_\chi$. This holds for all $\chi \in \widehat{G}$, thus we showed $v = v'$, as claimed. $\square$

6.4. The group $C_4 \rtimes C_4$. In this section

$$G = C_4 \rtimes C_4 = \langle a, b \mid a^4 = 1 = b^4, \quad bab^{-1} = a^3 \rangle.$$

Assume that K has an element i of multiplicative order 4. Then G has two irreducible 2-dimensional representations (up to isomorphism), namely

$$\psi_1 : a \mapsto \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}, \quad b \mapsto \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad \psi_2 : a \mapsto \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}, \quad b \mapsto \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}.$$

The other irreducible representations of G are 1-dimensional, and can be labeled by the elements of the subgroup $\widehat{G} := \{\pm 1\} \times \{\pm 1, \pm i\}$ of $K^\times \times K^\times$ as follows: identify $\chi = (\chi_1, \chi_2) \in \widehat{G}$ with the representation $\chi : G \rightarrow K^\times$ given by

$$\chi : a \mapsto \chi_1, \quad b \mapsto \chi_2.$$

Denote by W_j the vector space K^2 endowed with the representation ψ_j for $j = 1, 2$, and for $\chi \in \widehat{G}$ denote by U_χ the vector space K endowed with the representation χ . Set $U := \bigoplus_{\chi \in \widehat{G}} U_\chi$. Note that none of ψ_1 or ψ_2 is faithful: $\ker(\psi_1) = \langle b^2 \rangle$, $G/\ker(\psi_1) \cong D_8$, and ψ_1 is the lift to G of the only 2-dimensional representation of D_8 . On the other hand, $\ker(\psi_2) = \langle a^2 b^2 \rangle$, $G/\ker(\psi_2) \cong \text{Dic}_8$, and ψ_2 is the lift to G of the only 2-dimensional irreducible representation of the quaternion group. The coordinate functions on W_1 are denoted by x_1, x_2 , the coordinate functions on W_2 are y_1, y_2 , and the coordinate function on U_χ is t_χ for $\chi \in \widehat{G}$. It is well known and easy to see that

$$K[x_1, x_2]^G = K[x_1 x_2, x_1^4 + x_2^4],$$

$$K[y_1, y_2]^G = K[(y_1 y_2)^2, y_1^4 + y_2^4, y_1 y_2 (y_1^4 - y_2^4)].$$

Consider the following relative invariants (their index indicates their weight):

$$\begin{aligned} r_{(-1,1)} &:= x_1^2 + x_2^2, & r_{(-1,-1)} &:= x_1^2 - x_2^2, & r_{(1,-1)} &:= r_{(-1,1)} r_{(-1,-1)} = x_1^4 - x_2^4 \\ s_{(1,-1)} &:= y_1 y_2, & s_{(-1,1)} &:= y_1^2 + y_2^2, & s_{(-1,-1)} &:= y_1^2 - y_2^2. \end{aligned}$$

Using the above observations, one can prove by arguments similar to the proof of Proposition 6.5 the following:

Proposition 6.9. *For $i = 1, 2$ we have $\beta(G, W_i \oplus U) = 6$.*

Proposition 6.10. *We have $\beta(G, W_1 \oplus W_2) \leq 6$.*

Proof. We know that $\beta^K(G) \leq 7$ by [14, Proposition 3.1]. On the other hand, the element $a^2 \in G$ acts on $W_1 \oplus W_2$ as multiplication by the scalar -1 , hence any homogeneous element of $K[W_1 \oplus W_2]^G$ has even degree. It follows that $\beta(G, W_1 \oplus W_2)$ is an even number, less than or equal to 7. Consequently, $\beta(G, W_1 \oplus W_2) \leq 6$. $\square$

Proposition 6.11. *We have $\beta_{\text{sep}}(W_1 \oplus W_2 \oplus U_{(1,i)}) \leq 6$.*

Proof. Let $v = (w_1, w_2, u) \in V$ and $v' = (w'_1, w'_2, u') \in V$ such that $f(v) = f(v')$ for all $f \in K[V]^G$ with $\deg(f) \leq 6$ (here $w_i, w'_i \in W_i$ and $u, u' \in U$). We need to show that v and v' have the same G -orbit. By Proposition 6.10, (w_1, w_2) and (w'_1, w'_2) are in the same G -orbit. Replacing v by an appropriate element in its G -orbit, we may assume that $w_1 = w'_1$ and $w_2 = w'_2$. If $w_1 = 0$ or $w_2 = 0$, then we have $G \cdot v = G \cdot v'$ by Proposition 6.9. From now on we assume that none of w_1 or w_2 is zero. Set

$$r_{(1,-i)}^{(1)} := x_1 y_2 + i x_2 y_1, \quad r_{(1,-i)}^{(2)} := x_1 y_1^3 - i x_2 y_2^3, \quad r_{(1,i)} := x_1 y_2 - i x_2 y_1.$$

Then $r_{(1,-i)}^{(1)}, r_{(1,-i)}^{(2)}, t^3$ are relative invariants of weight $(1, -i) \in \widehat{G}$, whereas $r_{(1,i)}, t$ are relative invariants of weight $(1, i)$. Therefore we have the invariants

$$f_1 := t^4, \quad f_2 := r_{(1,-i)}^{(1)} t, \quad f_3 := r_{(1,-i)}^{(2)} t, \quad f_4 := r_{(1,i)} t^3.$$

All of the above invariants have degree at most 5. By assumption, $f_j(v) = f_j(v')$ for $j = 1, 2, 3, 4$. The equality $t^4(v) = t^4(v')$ implies that $u' \in \{u, -u, iu, -iu\}$. In particular, if $u = 0$, then $u' = 0$, and hence $v = v'$. It remains to deal with the case $u \neq 0$. Moreover, $u = u'$ if and only if $t(v) = t(v')$ if and only if $t^3(v) = t^3(v')$. Suppose for contradiction that $u \neq u'$. Then $f_j(v) = f_j(v')$ for $j = 2, 3, 4$ and $(w_1, w_2) = (w'_1, w'_2)$ imply that

$$0 = r_{(1,-i)}^{(1)}(v) = r_{(1,-i)}^{(2)}(v) = r_{(1,i)}(v).$$

From $0 = r_{(1,-i)}^{(1)}(v) = r_{(1,i)}(v)$ we conclude $0 = x_1(v)y_2(v) = x_2(v)y_1(v)$. Taking into account that $w_1 \neq 0$ and $w_2 \neq 0$, we conclude that $0 = x_1(v) = y_1(v)$ or $0 = x_2(v) = y_2(v)$. Then $r_{(1,-i)}^{(2)}(v) = 0$ yields that both $x_1(v)y_1(v)$ and $x_2(v)y_2(v)$ are zero. We deduce $w_1 = 0$ or $w_2 = 0$, a contradiction. $\square$

Proposition 6.12. *We have $\beta_{\text{sep}}(G, W_1 \oplus W_2 \oplus U_{(-1,1)}) \leq 6$ and $\beta_{\text{sep}}(G, W_1 \oplus W_2 \oplus U_{(1,-1)}) \leq 6$.*

Proof. First we deal with $V := W_1 \oplus W_2 \oplus U_{(-1,1)}$. Let $v = (w_1, w_2, u) \in V$ and $v' = (w'_1, w'_2, u') \in V$ such that $f(v) = f(v')$ for all $f \in K[V]^G$ with $\deg(f) \leq 6$. We need to show that v and v' have the same G -orbit. In the same way as in the proof of Proposition 6.11, we may assume that $w_1 = w'_1$, $w_2 = w'_2$ and none of w_1 or w_2 is zero. It follows that

$$r_{(-1,1)} = x_1^2 + x_2^2, \quad r_{(-1,-1)}s_{(1,-1)} = (x_1^2 - x_2^2)y_1y_2, \quad s_{(-1,1)} = y_1^2 + y_2^2$$

can not all vanish at v . Suppose that f is one of the above polynomials, with $f(v) \neq 0$. Since f is a relative invariant of weight $(-1, 1)$ of degree at most 4, we get that $ft \in K[V]^G$ has degree at most 5. Moreover, the equality $(ft)(v) = (ft)(v')$ implies $u = u'$, hence $v = v'$.

The proof for $V = W_1 \oplus W_2 \oplus U_{(1,-1)}$ is similar, the only difference is that we use the relative invariants

$$s_{(1,-1)} = y_1y_2, \quad s_{(-1,1)}r_{(-1,-1)} = (y_1^2 + y_2^2)(x_1^2 - x_2^2), \quad s_{(-1,-1)}r_{(-1,1)} = (y_1^2 - y_2^2)(x_1^2 + x_2^2).$$

□

Proposition 6.13. *We have $\mu(G) \leq 2$, and hence $\kappa(G) \leq 3$.*

Proof. Let S be an intersection independent set of subgroups of G with $|S| = \mu(G)$. Clearly $G \notin S$. If S contains a cyclic subgroup of prime power order, then $|S| \leq 2$ by Lemma 6.3. From now on assume that S contains no cyclic subgroup of prime power order. All such proper subgroups of G contain the subgroup $\langle a^2, b^2 \rangle$. If $\langle a^2, b^2 \rangle \in S$, then $|S| = 1$. Otherwise S consists of two order 8 subgroups of G . In either case, $|S| \leq 2$. The inequality $\mu(G) \leq 2$ is proved, and hence $\kappa(G) \leq 1 + \mu(G) \leq 3$ holds by (11). □

Theorem 6.14. *Assume that K has an element of multiplicative order 8. Then we have $\beta_{\text{sep}}(\mathbb{C}_4 \rtimes \mathbb{C}_4) = 6$.*

Proof. The factor group of G modulo its central normal subgroup $\langle a^2b^2 \rangle$ is isomorphic to the quaternion group Dic_8 of order 8. Therefore $\beta_{\text{sep}}^K(G) \geq \beta_{\text{sep}}^K(\text{Dic}_8) = 6$ (in fact we have $\beta_{\text{sep}}(G, W_2) = 6$, as we saw in Section 4).

To prove the reverse inequality, by Lemma 2.4 we may assume that K is large enough so that Lemma 6.1 applies and we can reduce to the study of multiplicity-free representations. By Proposition 6.13 we have $\kappa(G) \leq 3$, and therefore by Lemma 6.2 it is sufficient to show that $\beta_{\text{sep}}(V) \leq 6$ if V is the direct sum of three pairwise non-isomorphic KG -modules. Assume that V is such a KG -module. By Proposition 6.10, Proposition 6.9 we know that $\beta_{\text{sep}}(G, V) \leq \beta(G, V) \leq 6$, unless $V = W_1 \oplus W_2 \oplus U_\chi$ for some non-trivial character $\chi \in \widehat{G}$. The cases when $\chi \in \{(1, i), (-1, 1), (1, -1)\}$ are covered by Proposition 6.11, Proposition 6.12. The remaining representations are of the form $\rho \circ \alpha$, where ρ is one of the above three representations, and α is an automorphism of G . So the proof is complete by Lemma 6.4. □

7. COMMENTS ON COMPUTATIONAL ASPECTS

It is not possible to obtain the results of this paper on small groups by computer for two reasons. They are valid in infinitely many different characteristics and there are no known

general principles for relating the separating Noether numbers of a group over fields of different characteristic (unlike for the Noether number, for which some interesting results in this direction can be found in [33, Theorem 4.7]). Moreover, our results are proved also over fields that are not algebraically closed. While by Lemma 2.4 (iii) one can get an upper bound on the separating Noether number by passing to the algebraic closure of the base field, there seems to be no algorithm for finding the exact value of the separating Noether number over an infinite algebraically non-closed base field (in other words, our arguments giving lower bound for separating Noether numbers can not be replaced by computer calculations). Note that for algebraically closed base fields and not necessarily finite reductive groups, an algorithm to compute a separating set of invariants is given in [30] (without a prior computation of a generating set of invariants).

However, one can in principle verify by computer for chosen base fields that our claimed value is at least an upper bound for the separating Noether number as follows. We can pass to the algebraic closure of the base field, and by Lemma 2.4 (iii) the separating Noether number for the algebraic closure is an upper bound for the separating Noether number over the original base field. There are computer algebra packages that can compute minimal systems of generators for rings of invariants of finite groups. Using a minimal homogeneous generating system of $K[V]^G$ as input, assuming that K is algebraically closed, a simple algorithm computes $\beta_{\text{sep}}(G, V)$, based on the following statement.

Proposition 7.1. *Let V be a KG -module, where K is algebraically closed. Let $\mathcal{A}$ be a minimal homogeneous generating system of $K[V]^G = K[x_1, \dots, x_n]^G$. Take additional variables $y_1, \dots, y_n$, and denote by $\delta : K[x_1, \dots, x_n] \rightarrow K[x_1, \dots, x_n, y_1, \dots, y_n]$ the map $f \mapsto f(x_1, \dots, x_n) - f(y_1, \dots, y_n)$. For a positive integer d we have that $\beta_{\text{sep}}(G, V) \leq d$ if and only if for all $f \in \mathcal{A}$ with $\deg(f) > d$ we have that $\delta(f)$ is contained in the radical of the ideal $(\delta(h) \mid h \in \mathcal{A}, \deg(h) \leq d)$. Consequently,*

$$\beta_{\text{sep}}(G, V) = \min\{d \mid \forall f \in \mathcal{A}: \delta(f) \in \sqrt{(\delta(h) \mid h \in \mathcal{A}, \deg(h) \leq d)}\}.$$

Proof. This is a straightforward consequence of Definition 1.1, the definition of $\beta_{\text{sep}}(G, V)$, and Hilbert's Nullstellensatz. $\square$

We have implemented in SageMath an algorithm based on Proposition 7.1. In the case $K = \mathbb{C}$, we verified the values of $\beta_{\text{sep}}^K(G)$ for the non-abelian groups given in Theorem 2.3 using the online CoCalc platform [41] and some good apriori upper bounds on the Helly dimension $\kappa(G)$ or $\kappa(G, V)$ (cf. Section 6.1).

DECLARATIONS

Ethical Approval: not applicable

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

Availability of data and materials: not applicable

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] B. Blum-Smith, H. Derksen, Generic orbits, normal bases, and generation degree for fields of rational invariants, *arXiv:2506.05650*.
- [3] D. J. Benson, *Polynomial Invariants of Finite Groups*, London Math. Society. Lecture Notes Series 190, Cambridge University Press, 1993.
- [4] B. Blum-Smith, T. Garcia, R. Hidalgo, C. Rodriguez, Degree bounds for fields of rational invariants of $\mathbb{Z}/p\mathbb{Z}$ and other finite groups, *J. Pure Appl. Algebra* 228 (2024), Article ID 107693.
- [5] J. Cahill, A. Contreras, A. C. Hip, Stable separation of orbits for finite abelian group actions, *J. Fourier Anal. Appl.* 30 (2024), Paper No. 12, 16 p.
- [6] J. Cahill, J. W. Iverson, D. G. Mixon, Towards a bilipschitz invariant theory, *Appl. Comput. Harmon. Anal.* 72 (2024), Article ID 101669, 27 p.
- [7] J. Cahill, J. W. Iverson, D. G. Mixon, D. Packer, Group-invariant max filtering, *Foundations of Computational Mathematics* (2024), <https://doi.org/10.1007/s10208-024-09656-9>
- [8] C. Chevalley, Invariants of finite groups generated by reflections, *Amer. J. Math.* 77 (1955), 778-792.
- [9] K. Cziszter, The Noether number of the non-abelian group of order $3p$, *Period. Math. Hung.* 68 (2014), 150-159.
- [10] K. Cziszter and M. Domokos, Groups with large Noether bound, *Ann. Inst. Fourier (Grenoble)* 64, no. 3 (2014), 909-944.
- [11] K. Cziszter, M. Domokos, The Noether number for the groups with a cyclic subgroup of index two, *J. Algebra* 399 (2014), 546-560.
- [12] K. Cziszter, M. Domokos, Lower bounds on the Noether number, *Transform. Groups* 24 (2019), 823-834.
- [13] K. Cziszter, M. Domokos, A. Geroldinger, The interplay of invariant theory with multiplicative ideal theory and with arithmetic combinatorics, in: Scott T. Chapman, M. Fontana, A. Geroldinger, B. Olberding (Eds.), *Multiplicative Ideal Theory and Factorization Theory*, Springer-Verlag, 2016, pp. 43-95.
- [14] K. Cziszter, M. Domokos, I. Szöllősi, The Noether numbers and the Davenport constants of the groups of order less than 32, *J. Algebra* 510 (2018), 513-541.
- [15] H. Derksen, G. Kemper, *Computational Invariant Theory*, Second Edition, *Encyclopaedia of Mathematical Sciences* 130, *Invariant Theory of Algebraic Transformation Groups VIII*, Springer-Verlag, Berlin, Heidelberg, 2015.
- [16] M. Domokos, Typical separating invariants, *Transform. Groups* 12 (2007), 49-63.
- [17] M. Domokos, Degree bound for separating invariants of finite abelian groups, *Proc. Amer. Math. Soc.* 145 (2017), 3695-3708.
- [18] M. Domokos, Separating polynomial invariants over non-closed fields of finite abelian groups, *arXiv:2506.22889*
- [19] M. Domokos, P. Hegedűs, Noether's bound for polynomial invariants of finite groups, *Arch. Math.* 74 (2000), 161-167.
- [20] M. Domokos, B. Scheffler, The separating Noether number of small groups, *arXiv:2412.08621v2*
- [21] M. Domokos, E. Szabó, Helly dimension of algebraic groups, *J. London Math. Soc. (2)* 84 (2011), 19-34.
- [22] J. Draisma, G. Kemper, D. Wehlau, Polarization of separating invariants, *Canad. J. Math.* 60 (2008) 556-571.
- [23] E. Dufresne, Separating invariants and finite reflection groups, *Adv. Math.* 221 (2009), 1979-1989.
- [24] E. Dufresne, J. Elmer, M. Kohls, The Cohen-Macaulay property of separating invariants of finite groups, *Transform. Groups* 14 (2009), 771-785.
- [25] E. Dufresne, J. Jeffries, Separating invariants and local cohomology, *Adv. Math.* 270 (2015), 565-581.

- [26] J. Elmer, M. Kohls, Zero-separating invariants for finite groups, *J. Algebra* 411 (2014), 92-113.
- [27] P. Fleischmann, The Noether bound in invariant theory of finite groups, *Adv. Math.* 156 (2000), 23-32.
- [28] J. Fogarty, On Noether's bound for polynomial invariants of a finite group, *Electron. Res. Announc. Amer. Math. Soc.* 7 (2001), 5-7.
- [29] The GAP Group: GAP – Groups, Algorithms, and Programming, Version 4.12.2; 2022, <https://www.gap-system.org>.
- [30] G. Kemper, Computing invariants of reductive groups in positive characteristic, *Transform. Groups* 8 (2003), 159-176.
- [31] G. Kemper, Separating invariants, *J. Symb. Comput.* 44 (2009), 1212-1222.
- [32] G. Kemper, A. Lopatin, F. Reimers, Separating invariants over finite fields, *J. Pure Appl. Algebra* 226 (2022), paper no. 106904
- [33] F. Knop, On Noether's and Weyl's bound in positive characteristic, in "Invariant Theory in All Characteristics", (Ed.: H. E. A. Eddy Campbell and D. L. Wehlau), CRM Proceedings and Lecture Notes 35, Amer. Math. Soc., Providence, Rhode Island, pp. 175-188, 2004.
- [34] M. Kohls, H. Kraft, Degree bounds for separating invariants, *Math. Res. Lett.* 17 (2010), 1171-1182.
- [35] M. Kohls, M. Sezer, Separating invariants for the Klein four group and cyclic groups, *Int. J. Math.* 24 (2013), Article ID 1350046.
- [36] A. Lopatin, P. A. Muniz, Separating invariants for two-dimensional orthogonal groups over finite fields, *Lin. Alg. Appl.* 692 (2024), 71-83.
- [37] A. Lopatin, F. Reimers, Separating invariants for multisymmetric polynomials, *Proc. Amer. Math. Soc.* 149 (2021), 497-508.
- [38] E. Noether, Der Endlichkeitssatz der Invarianten endlicher Gruppen, *Math. Ann.* 77 (1916), 89-92.
- [39] J. E. Olson, A combinatorial problem on finite abelian groups II, *J. Number Theory* 1 (1969), 195-199.
- [40] D. R. Richman, Invariants of finite groups over fields of characteristic p , *Adv. Math.* 124 (1996), 25-48.
- [41] Sagemath, Inc., CoCalc – Collaborative Calculation and Data Science, 2020, <https://cocalc.com>.
- [42] 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.
- [43] B. Scheffler, The separating Noether number of abelian groups of rank two, *J. Comb. Theory, Ser. A* 209 (2025), Paper no. 105951.
- [44] B. Scheffler, K. Zhao, Q. Zhong, On the separating Noether number of finite abelian groups, [arXiv:2503.01296v2](https://arxiv.org/abs/2503.01296v2)
- [45] B. J. Schmid, Finite groups and invariant theory, in "Topics in invariant theory" (M.-P. Malliavin, ed.), *Lecture notes in mathematics*, no. 1478, Springer, 1989-90, pp. 35-66.
- [46] M. Sezer, Sharpening the generalized Noether bound in the invariant theory of finite groups, *J. Algebra* 254 (2002), 252-263.
- [47] M. Sezer, Explicit separating invariants for cyclic P -groups, *J. Comb. Theory, Ser. A* (2011), 681-689.
- [48] D. L. Wehlau, The Noether number in invariant theory, *C. R. Math. Acad. Sci., Soc. R. Can.* 28 (2006), 39-62.

HUN-REN ALFRÉD RÉNYI INSTITUTE OF MATHEMATICS, REÁLTANODA UTCA 13-15, 1053 BUDAPEST, HUNGARY, ORCID ID: <https://orcid.org/0000-0002-0189-8831>

Email address: domokos.matyas@renyi.hu

EÖTVÖS LORÁND UNIVERSITY, PÁZMÁNY PÉTER SÉTÁNY 1/C, 1117 BUDAPEST, HUNGARY

Email address: schefflerbarna@yahoo.com