GROUPS WITH LARGE RELATIVE NOETHER BOUND

KÁLMÁN CZISZTER AND MÁTYÁS DOMOKOS

Abstract. The finite groups having an indecomposable polynomial invariant whose degree is at least half of the order of the group are classified. Apart from four sporadic exceptions these are exactly the groups having a cyclic subgroup of index at most two. The Noether bound is determined for these groups, and estimates are given for various other groups as well.

1. Introduction and main results

Fix a base field $\mathbb{F}$, let G be a finite group and V a finite dimensional G-module over $\mathbb{F}$. By a classical theorem of E. Noether [23] the *algebra of polynomial invariants* on V, $\mathbb{F}[V]^G$ is generated by finitely many homogeneous elements. Set

$$\beta(G,V) := \min\{d \in \mathbb{N} \mid \mathbb{F}[V]^G \text{ is generated by elements of degree at most } d\},$$
$$\beta(G) := \sup\{\beta(G,V) \mid V \text{ is a finite dimensional } G\text{-module over } \mathbb{F}\}.$$

(The dependence of $\beta(G)$ from the base field $\mathbb{F}$ is suppressed in the notation; in fact, it might depend only on the characteristic of $\mathbb{F}$, see e.g. section 4 in Knop [20].) It is well known that $\beta(G) = \infty$ when $\mathrm{char}(\mathbb{F})$ divides $|G|$ (see Richman [28]). In the rest of this paper we shall deal only with the case when $\mathrm{char}(\mathbb{F})$ does not divide the order of G. Under this assumptiom the famous theorem on the *Noether bound* asserts that

$$\beta(G) \leq |G|$$

(see Noether [22] in characteristic zero and Fleischmann [10] and Fogarty [11] in non-modular positive characteristic). We define the *relative Noether bound*

$$\gamma(G) := \frac{\beta(G)}{|G|}.$$

Working over the field of complex numbers, Schmid [30] proved that $\gamma(G) = 1$ holds only when G is cyclic. This was sharpened by Domokos and Hegedűs [9] by proving that $\gamma(G) \leq 3/4$ for all non-cyclic G; the result was extended to non-modular positive characteristic by Sezer [32]. The constant $3/4$ is optimal here. On the other hand, a straightforward lower bound on $\gamma(G)$ can be obtained as follows: $\beta(G) \geq \beta(H)$ for all subgroups H of G, as Schmid [30] showed, hence in particular, $\beta(G)$ is bounded from below by the maximal order of elements in G. Therefore $\gamma(G) \geq 1/2$ whenever G contains a cyclic subgroup of index two —and obviously there are infinitely many isomorphism classes of such non-cyclic groups. The main result of the present paper is that the converse of this statement is essentially true, apart from four sporadic exceptions:

Date: May 24, 2011.
2000 *Mathematics Subject Classification.* Primary: 13A50; Secondary: 11B50.
The second author is partially supported by OTKA NK72523, NK81203.

Theorem 1.1. *For a finite group G with $2|G| \in \mathbb{F}^\times$ we have $\gamma(G) \geq 1/2$ if and only if G contains a cyclic subgroup of index at most 2, or G is isomorphic to $Z_3 \times Z_3$, $Z_2 \times Z_2 \times Z_2$, the alternating group A_4, or the binary tetrahedral group $\tilde{A}_4$.*

This Theorem is a novelty even for the case $\mathbb{F} = \mathbb{C}$. In fact the assumption that $|G| \in \mathbb{F}^\times$ is sufficient except possibly when 21 divides $|G|$ (see Remark 12.1).

Our article can be divided into three main parts. The first part introduces some new concepts and technical tools, most notably the generalized Noether number $\beta_k(G)$ and a series of related reduction lemmata in Section 2. These are refinements of Schmid's original reduction lemmata. They give better results even in the simplest cases, as it is seen from Section 3, where we also explain how additive number theory and questions concerning zero-sum sequences enter the picture, and we recapitulate some basic results in this domain (see also the end of Section 5). A new lower bound on the Noether number is given in Section 4.

The second part gives explicit bounds on the (generalized) Noether number for several particular groups, such as the dihedral groups in Section 6, the alternating group A_4 (and the binary tetrahedral group $\tilde{A}_4$) in Section 10, the semidirect product $Z_p \rtimes Z_q$ in Section 9. The characterization of the so called extremal invariants of the dihedral group in Section 7 leads us to estimate the Noether number for the groups $Z_p \rtimes Z_4$, where Z_4 acts faithfully, respectively for the groups $Z_p \rtimes Z_{2^n}$ where the generator of Z_{2^n} acts by inversion. Finally, we treat the case of the non-abelian semidirect product $(Z_2 \times Z_2) \rtimes Z_9$ in Section 10.1. The common technical framework for these sections is introduced in Section 5.

In the third part we prove the following, purely group theoretical structure theorem:

Theorem 1.2. *For any finite group G one of the following thirteen options holds:*

- *(1) G is isomorphic to $Z_3 \times Z_3$, $Z_2 \times Z_2 \times Z_2$, A_4, or $\tilde{A}_4$;*
- *(2) G contains a cyclic subgroup of index at most 2;*
- *(3) G has a subgroup isomorphic to $Z_p \times Z_p$, where $p \geq 5$ is a prime;*
- *(4) G has a subgroup H properly contained in its normalizer, where H is*
  - *(a) $Z_3 \times Z_3$;*
  - *(b) $Z_2 \times Z_2 \times Z_2$;*
  - *(c) A_4 or $\tilde{A}_4$;*
- *(5) G has a subquotient isomorphic to*
  - *(a) an extension of $Z_2 \times Z_2$ by itself;*
  - *(b) an extension of the dihedral group D_{2p} (p an odd prime) by $Z_2 \times Z_2$;*
  - *(c) $D_{2p} \times D_{2q}$ where p, q are distinct odd primes;*
  - *(d) a non-abelian semidirect product $Z_p \rtimes Z_q$ where $p \neq q$ are odd primes;*
  - *(e) $Z_p \rtimes Z_4$, where p is an odd prime and Z_4 acts faithfully on Z_p;*
  - *(f) the non-abelian semidirect product $(Z_2 \times Z_2) \rtimes Z_9$*
  - *(g) the alternating group A_5.*

Theorem 1.2 can be seen as a "roadmap" of our work, and it also accounts for the choice of the groups examined in the second part. Combining the reduction lemmata from Section 2 with the explicit bounds from the second part we shall show in Section 12 that $\gamma(G) < 1/2$ if G falls under case (3), (4), or (5) of this theorem.

As for the groups containing a cyclic subgroup of index 2, they can be easily classified by a result of Burnside. In Section 8 we shall determine in addition the value of $\beta(G)$ for each of these groups, see Table 1. Based on these results it will also follow that

Corollary 1.3. *Let $\mathcal{C}$ be the set of isomorphism classes of all finite, non-cyclic groups G. Then*

$$\limsup_{G\in\mathcal{C}} \gamma(G) = \frac{1}{2}$$

1.1. **Preliminaries.** Throughout this paper $\mathbb{F}$ stands for a fixed base field, and all vector spaces are understood over $\mathbb{F}$. We shall always tacitly assume that $\mathrm{char}(\mathbb{F})$ does not divide the order of G. As we noted above, the Noether bound (and similarly the generalized Noether bound) of a finite group G depend only on the characteristic of $\mathbb{F}$. Therefore we may and shall always tacitly assume in our constructions and arguments that $\mathbb{F}$ is algebraically closed; our statements are of course valid when $\mathbb{F}$ is not algebraically closed. Given a finite group G and a finite dimensional G-module V write $\mathbb{F}[V]$ for the coordinate ring of V, so $\mathbb{F}[V]$ is the symmetric tensor algebra of the dual V^* of V. We view V^* as a right G-module, so G acts from the right on $\mathbb{F}[V]$ via graded $\mathbb{F}$-algebra automorphisms. The subalgebra

$$\mathbb{F}[V]^G := \{f \in \mathbb{F}[V] \mid f^g = f \quad \forall g \in G\}$$

is called the *algebra of polynomial invariants* on V.

In Lemma 1.4 below we summarize some known reductions to bound $\gamma(G)$.

Lemma 1.4. *We have $\gamma(G) \le \gamma(K)$ for any subquotient K of G.*

Proof. We have $\beta(G) \le \beta(H)[G : H]$ by Lemma 3.2 of Schmid [30] when $\mathrm{char}(\mathbb{F}) = 0$ and by Proposition 2 of Sezer [32] when $0 < \mathrm{char}(\mathbb{F}) \nmid |G|$. Given that $|G| = |H|[G : H]$, our claim follows by the definition of γ for the case when $H \le G$ is a subgroup.

Also $\beta(G) \le \beta(N)\beta(G/N)$ for any $N \triangleleft G$ by Lemma 3.1 of Schmid [30] when $\mathrm{char}(\mathbb{F}) = 0$ and by Proposition 4 of Sezer [32] when $0 < \mathrm{char}(\mathbb{F}) \nmid [G : N]$. Hence our claim follows again by dividing with $|G| = |N||G/N|$. ☐

Let $H \le G$ be a subgroup and let S be a set of right H-coset representatives in G. The *transfer* map τ_H^G is defined as

$$\tau_H^G(u) := \sum_{g\in S} u^g \qquad \text{where } u \in \mathbb{F}[V]^H. \tag{1}$$

This does not depend on the choice of S. We shall abbreviate τ_H^G with τ whenever this is possible without confusion. The following properties of τ are well known, see e.g. [21] p. 33f:

Proposition 1.5. *The map $\tau : \mathbb{F}[V]^H \to \mathbb{F}[V]^G$ is a degree preserving $\mathbb{F}[V]^G$-module homomorphism, and it is surjective if $[G : H]$ is invertible in $\mathbb{F}$.*

Given a graded algebra $R = \bigoplus_{d=0}^{\infty} R_d$ (such as $\mathbb{F}[V]$ or $\mathbb{F}[V]^G$) and a positive integer m set

$$R_{\ge m} := \bigoplus_{d\ge m} R_d, \quad R_+ := R_{\ge 1}, \quad (R_+)_{\le m} := \bigoplus_{d=1}^{m} R_d.$$

Observe that $R_{\ge m} = R_+^m$. For subspaces I, J in an algebra R write IJ for the subspace spanned by the products ij with $i \in I$ and $j \in J$.

2. The generalized Noether number

Definition 2.1. Let G be a finite group, V a representation of G over a field $\mathbb{F}$, and set $R := \mathbb{F}[V]^G$. For any positive integer k define

$$\beta_k(G,V) := \max\{d \in \mathbb{N} \mid R_d \not\subseteq (R_+)^{k+1}\}.$$

We also define

$$\beta_k(G) := \sup\{\beta_k(G,V) \mid V \text{ is a finite dimensional } G\text{-module over } \mathbb{F}\}.$$

We shall refer to these numbers as the *generalized Noether numbers* of G.

In the special case $k = 1$ we recover $\beta_1(G,V) = \beta(G,V)$ and $\beta_1(G) = \beta(G)$.

Lemma 2.2. *For any positive integers $r \le k$ we have the inequality*

$$\beta_k(G,V) \le \frac{k}{r}\beta_r(G,V).$$

In particular, $\beta_k(G,V) \le k\beta(G,V)$, hence $\beta_k(G)$ is finite when the order of G is invertible in $\mathbb{F}$.

Proof. Suppose to the contrary that $\beta_k(G) > \frac{k}{r}\beta_r(G,V)$. Then there exist homogeneous G-invariants $f_1, \dots, f_l \in \mathbb{F}[V]^G_+$ such that $l \le k$, $f := f_1 \cdots f_l$ is not contained in $(\mathbb{F}[V]^G_+)^{l+1}$, and $\deg(f) > \frac{k}{r}\beta_r(G,V)$ (this forces that $l > r$). We may suppose that $\deg(f_1) \ge \dots \ge \deg(f_l)$. Then we have $\deg(f_1 \cdots f_r) > \beta_r(G,V)$, implying that $h := f_1 \cdots f_r \in (\mathbb{F}[V]^G_+)^{r+1}$, hence $f = hf_{r+1} \cdots f_l \in (\mathbb{F}[V]^G_+)^{l+1}$, a contradiction. □

Remark 2.3. By Lemma 2.2 the sequence $\frac{\beta_k(G)}{k}$ is monotonically decreasing, hence it converges to a limit. So $\beta_k(G)$ as a function of k is asymptotically linear.

The following characterization of the generalized Noether number will be sometimes useful:

Proposition 2.4. *Suppose that the characteristic of the field $\mathbb{F}$ does not divide the order of the finite group G. Then $\beta_k(G)$ is the minimal positive integer d having the following property: for any finitely generated commutative graded $\mathbb{F}$-algebra L (with $L_0 = \mathbb{F}$) on which G acts via graded $\mathbb{F}$-algebra automorphisms we have*

$$L^G \cap L_+^{d+1} \subseteq (L_+^G)^{k+1}.$$

Proof. Let L be a finitely generated commutative graded $\mathbb{F}$-algebra L with $L_0 = \mathbb{F}$ on which G acts via graded $\mathbb{F}$-algebra automorphisms. There exists a finite dimensional G-module V and a G-equivariant $\mathbb{F}$-algebra surjection $\pi : \mathbb{F}[V] \to L$ mapping $\mathbb{F}[V]_+$ onto L_+. Moreover, π restricts to a surjection $\mathbb{F}[V]^G_+ \to L^G_+$ by the assumption on the characteristic of $\mathbb{F}$. So we have

$$L^G \cap L_+^{\beta_k(G)+1} = \pi(\mathbb{F}[V]^G_{\ge \beta_k(G)+1}) \subseteq \pi((\mathbb{F}[V]^G_+)^{k+1}) = (L^G_+)^{k+1}.$$

Conversely, take $L := \mathbb{F}[V]$ for a finite dimensional G-module V with $\beta_k(G,V) = \beta_k(G)$. □

Lemma 2.5. *Suppose that* $\mathrm{char}(\mathbb{F}) \nmid |G|$ *and N is a normal subgroup of G. Then*

$$\beta_k(G) \le \beta_{\beta_k(G/N)}(N)$$

Proof. We shall apply Proposition 2.4 for the algebra $L := \mathbb{F}[V]^N$, where V is an arbitrary finite dimensional G-module, and write $R := \mathbb{F}[V]^G$. Then the subalgebra L of $\mathbb{F}[V]$ is G-stable, and the action of G on L factors through G/N, and $R = L^{G/N}$. Setting $s := \beta_{\beta_k(G/N)}(N)$, we have

$$R \cap \mathbb{F}[V]_{\geq s+1} = R \cap \mathbb{F}[V]^N_{\geq s+1} \subseteq L^{G/N} \cap L_+^{\beta_k(G/N)+1} \subseteq (L_+^{G/N})^{k+1} = (R_+)^{k+1}.$$

This holds for any V, showing the desired inequality. □

Proposition 2.6. *Let L be a commutative $\mathbb{F}$-algebra and G a finite group of its automorphisms. Let $J \subset L$ be a G-stable subalgebra (non-unitary) and $H \leq G$ a subgroup. Suppose that one of the following conditions holds:*

(i) $\mathrm{char}(\mathbb{F}) = 0$ *or* $\mathrm{char}(\mathbb{F}) > [G:H]$, *or*

(ii) *H is normal in G and* $\mathrm{char}(\mathbb{F})$ *does not divide* $[G:H]$.

Then

$$(J^H)^{[G:H]} \subseteq J^H J^G + J^G$$

Proof. (i) Any $f \in J^H$ is a root of the monic polynomial $\prod_{g\in\mathcal{S}}(t - f^g) \in J[t]$, where $\mathcal{S}$ is a system of right H-coset representatives in G. Obviously all coefficients of this polynomial are G-invariant. Consequently, $f^{[G:H]} \in J^H J^G + J^G$ holds for all $f \in J^H$. Take arbitrary $f_1, \dots, f_r \in J^H$ where $r = [G:H]$. Then the product $r! f_1 \cdots f_r$ can be written as an alternating sum of rth powers of sums of subsets of $\{f_1, \dots, f_r\}$ (see e.g. Lemma 1.5.1 in [2]), hence $f_1 \cdots f_r \in J^H J^G + J^G$.

(ii) (This is a variant of a result of Knop (see Theorem 2.1 in [20]); the idea appears in Benson's simplification of Fogarty's argument from [11] (see Lemma 3.8.1 in [8]). Let $\mathcal{S}$ be a system of right H-coset representatives in G. For each $x \in \mathcal{S}$ choose an arbitrary element $a_x \in J^H$. Note that $a_x^y \in J^H$ for all $x, y \in \mathcal{S}$ by normality of H in G. It is easily checked that

$$0 = \sum_{y\in\mathcal{S}} \prod_{x\in\mathcal{S}} (a_x^x - a_x^y) = \sum_{U\subset\mathcal{S}} (-1)^{|U|} \delta_U \qquad \text{where}$$

$$\delta_U := \sum_{y\in\mathcal{S}} \prod_{x\notin U} a_x^x \prod_{x\in U} a_x^y = \prod_{x\notin U} a_x^x \, \tau\left(\prod_{x\in U} a_x\right)$$

(here $\tau : J^H \to J^G$ denotes the transfer map defined by the formula (1)). Clearly $\delta_S \in J^G$ and $\delta_U \in J^H J^G$ for every $U \subsetneq \mathcal{S}$, except for $U = \emptyset$, when we get the term $[G:H]\prod_{x\in\mathcal{S}} a_x^x$. Given that $[G:H] \in \mathbb{F}^\times$ and the elements a_x were arbitrary the claim immediately follows. □

Remark 2.7. Finiteness of G can be replaced by finiteness of $[G:H]$ in the above argument.

Corollary 2.8. *Let L be an $\mathbb{F}$-algebra, G a finite group of its automorphisms, $J \subset L$ a G-stable subalgebra (non-unitary), $H \leq G$ a subgroup. Suppose that (i) or (ii) of Proposition 2.6 holds. Then*

$$(J^H)^{k[G:H]+1} \subseteq J^H (J^G)^k.$$

Proof. By Proposition 2.6 we have

$$(J^H)^{k[G:H]+1} \subseteq (J^H)^{(k-1)[G:H]+1}(J^H J^G + J^G) \subseteq ... \subseteq J^H (J^G)^k.$$ □

Lemma 2.9. *Let V be a finite dimensional G-module and $H \leq G$ a subgroup. Suppose that (i) or (ii) of Proposition 2.6 holds. Then*

$$\beta_k(G,V) \leq \beta_{k[G:H]}(H,V).$$

Proof. Apply Corollary 2.8 to the ideal $J := \mathbb{F}[V]_+$ of the ring $L := \mathbb{F}[V]$, and recall that $\tau := \tau_H^G : L^H \to L^G =: R$ is surjective. By definition of the generalized Noether number, for any $d > \beta_{k[G:H]}(H,V)$ we have $L_d^H \subseteq (J^H)^{k[G:H]+1}$. Consequently,

$$R_d = L_d^G = \tau(L_d^H) \subseteq \tau((J^H)^{k[G:H]+1}) \subseteq \tau(J^H(J^G)^k) \subseteq (J^G)^{k+1} = R_+^{k+1}. \qquad \square$$

Remark 2.10. Combining Lemma 2.2 with Lemma 2.5 and Lemma 2.9 in the special case $k = 1$ and $\mathbb{F} = \mathbb{C}$ one recovers Schmid's reduction lemmata $\beta(G) \leq \beta(G/N)\beta(N)$ and $\beta(G) \leq [G : H]\beta(H)$ (see Lemma 3.1 and 3.2 in [30]). They were extended to non-modular positive characteristic by Sezer [32], see also [20].

The usefulness of Lemmata 2.5 and 2.9 on the generalized Noether number stems from the fact that for $k > 1$ the number $\beta_k(G,V)$ in general is strictly smaller than $k\beta(G,V)$, as we shall observe this in Section 3 already for abelian groups.

3. The Davenport constant

Let A be an abelian group and V a representation of A over the (algebraically closed) base field $\mathbb{F}$. Then V decomposes into the direct sum of irreducible representations of dimension 1. As a result V^* has an A-eigenbasis $\{x_1, ..., x_n\}$, i.e. the action of A on any of these dual vectors can be described by a character $\theta_i \in \widehat{A}$, called its *weight*, such that $x_i^a = \theta_i(a)x_i$. We shall always tacitly choose this A-eigenbasis as the variables in the polynomial algebra $\mathbb{F}[V] = \mathbb{F}[x_1, ..., x_n]$. Let $M(V)$ denote the set of monomials in $\mathbb{F}[V]$; this is a monoid with respect to ordinary multiplication and unit element 1. On the other hand we denote by $\mathcal{M}(A)$ the free commutative monoid generated by the elements of A. Due to our choice of variables in $\mathbb{F}[V]$ we can define a monoid homomorphism $\Phi : M(V) \to \mathcal{M}(A)$ by sending each variable x_i to its weight θ_i, regarded as an element of A under a fixed identification $\widehat{A} \cong A$; we shall call $\Phi(m)$ the *weight sequence* of the monomial $m \in M(V)$. We prefer to write $\widehat{A}$ additively, hence for any character $\theta \in \widehat{A}$ we denote by $-\theta$ the character $a \mapsto \theta(a)^{-1}$, $a \in A$.

An element $S \in \mathcal{M}(A)$ can also be interpreted as a *sequence* $S := (s_1, \dots, s_n)$ of elements of A where repetition of elements is allowed and their order is disregarded. The *length* of S is $|S| := n$. By a *subsequence* of S we mean $S_J := (s_j \mid j \in J)$ for some subset $J \subseteq \{1, \dots, n\}$. Given a sequence R over an abelian group A we write $R = R_1R_2$ if R is the concatenation of its subsequences R_1, R_2, and we call the expression R_1R_2 a *factorization* of R. Given an element $a \in A$ and a positive integer r, write (a^r) for the sequence in which a occurs with multiplicity r. For an automorphism b of A and a sequence $S = (s_1, \dots, s_n)$ we write S^b for the sequence $(s_1^b, \dots, s_n^b)$, and we say that the sequences S and T are *similar* if $T = S^b$ for some b.

Let $\sigma : \mathcal{M}(A) \to A$ be the monoid homomorphism which assigns to each sequence over A the sum of its elements. The value $\sigma(\Phi(m)) \in A$ is called the *weight of the monomial* $m \in M(A)$ and it will be abbreviated by $\theta(m)$. The kernel of σ is called the *block monoid* of A, denoted by $\mathcal{B}(A)$, and its elements are called zero-sum sequences. Our interest in zero-sum sequences and the related results in additive number theory stems from the observation that the invariant ring $\mathbb{F}[V]^A$ is spanned as a vector space by all those monomials for which $\Phi(m)$ is a zero-sum sequence. Moreover, as an algebra, $\mathbb{F}[V]^A$ is minimally generated by those monomials m for which $\Phi(m)$ does not contain any proper zero-sum subsequences. These are called *irreducible* zero-sum sequences, and they form the Hilbert basis of the monoid $\mathcal{B}(A)$. A sequence is *zero-sum free* if it has no non-empty zero-sum subsequence.

The *Davenport constant* $\mathsf{D}(A)$ of A is defined as the length of the longest irreducible zero-sum sequence over A. It is an extensively studied quantity, see for example [13]. As it is seen from our discussion:

$$\mathsf{D}(A) = \beta(A). \tag{2}$$

The *generalized Davenport constant* $\mathsf{D}_k(A)$ is introduced in [16] as the length of the longest zero-sum sequence that cannot be factored into more than k non-empty zero-sum sequences. Obviously $\mathsf{D}_1(A) = \mathsf{D}(A)$ and $\mathsf{D}_k(A) \leq k\,\mathsf{D}(A)$, and for cyclic groups $\mathsf{D}_k(Z_q) = kq$. It can be viewed as the ancestor of the generalized Noether number for abelian groups, as similarly to (2) we have the equality

$$\beta_k(A) = \mathsf{D}_k(A) \tag{3}$$

for any finite abelian group A whose order is invertible in $\mathbb{F}$, and for any positive integer k. In view of (3), Lemma 2.5 applied to abelian groups yields $\mathsf{D}_k(A) \leq \mathsf{D}_{\mathsf{D}_k(A/B)}(B)$ for any subgroup $B \leq A$. Equivalently, $\mathsf{D}_k(A) \leq \mathsf{D}_{\mathsf{D}_k(B)}(A/B)$ for all $B \leq A$; this appears as Proposition 2.6 in [7].

We close this section with two results on D_k that will be used later on.

Proposition 3.1 (Halter-Koch, [16] Proposition 5)**.** *For any $n \mid m$ we have*

$$\mathsf{D}_k(Z_n \times Z_m) = km + n - 1.$$

Proposition 3.2 (Delorme-Ordaz-Quiroz, [7] Lemma 3.7)**.**

$$\mathsf{D}_k(Z_2 \times Z_2 \times Z_2) = \begin{cases} 4 & \text{if } k = 1 \\ 2k+3 & \text{if } k > 1 \end{cases}$$

By the structure theorem of finite abelian groups we have $A \cong Z_{n_1} \times \cdots \times Z_{n_s}$, where $1 < n_1 \mid \cdots \mid n_s$ are positive integers and Z_n stands for the cyclic group of order n. It was proved by Olson [24], [25] that when A is a p-group or A has rank $s = 2$, then

$$\mathsf{D}(A) = n_1 + \ldots + n_s - s + 1. \tag{4}$$

Now we are in the position to give the list of abelian groups A with $\gamma(A) \geq 1/2$:

Proposition 3.3. *Let A be a finite abelian group and suppose that $|A| \in \mathbb{F}^\times$. We have $\gamma(A) \geq \frac{1}{2}$ if and only if one of the following holds:*

(i) *$A \cong Z_m$ where $m \geq 1$ and then $\gamma(A) = 1$.*
(ii) *$A \cong Z_2 \times Z_{2m}$ where $m \geq 1$ and then $\gamma(A) = \frac{1}{2} + \frac{1}{4m}$.*
(iii) *$A \cong Z_3 \times Z_3$ and then $\gamma(A) = \frac{5}{9}$.*
(iv) *$A \cong Z_2 \times Z_2 \times Z_2$ and then $\gamma(A) = \frac{1}{2}$.*

Proof. Assume $A \cong Z_{n_1} \times \cdots \times Z_{n_s}$ where $s \geq 2$, $1 < n_1 \mid \ldots \mid n_s$ and $\gamma(A) \geq 1/2$. If $s = 2$ then Olson's formula (4) implies that (ii) or (iii) holds for A. Moreover, taking into account Lemma 1.4 we conclude that if $s \geq 3$, then $Z_3 \times Z_3 \times Z_3$ or $Z_2 \times Z_2 \times Z_2$ is a subgroup of A. By (4) the relative Noether number of the first group is strictly less than 1/2, hence this case is ruled out. If $Z_2 \times Z_2 \times Z_2$ is a subgroup of index m in A, then by Lemma 2.5 and by Proposition 3.2 we have $\gamma(A) \leq \frac{2m+3}{8m}$, which is strictly less than one half when $m > 1$. ☐

4. A lower bound

Schmid [30] proved that the Noether number is monotone with respect to taking subgroups. Her argument extends for the generalized Noether number as well:

Lemma 4.1. *Let W be a finite dimensional H-module, where H is a subgroup of a finite group G, and denote by V the G-module induced from W. Then the inequality $\beta_k(G,V) \geq \beta_k(H,W)$ holds for all positive integers k.*

Proof. View W as an H-submodule of

$$V = \bigoplus_{g \in G/H} gW \tag{5}$$

where G/H stands for a system of left H-coset representatives. Restriction of functions from V to W gives a graded $\mathbb{F}$-algebra surjection $\phi : \mathbb{F}[V] \to \mathbb{F}[W]$. Clearly ϕ is H-equivariant, hence maps $\mathbb{F}[V]^G$ into $\mathbb{F}[W]^H$. Even more, as observed in the proof of Propositon 5.1 of [30], we have $\phi(\mathbb{F}[V]^G) = \mathbb{F}[W]^H$: indeed, the projection from V to W corresponding to the direct sum decomposition (5) identifies $\mathbb{F}[W]$ with a subalgebra of $\mathbb{F}[V]$, and for an arbitrary $f \in \mathbb{F}[W]^H \subset \mathbb{F}[W] \subset \mathbb{F}[V]$, we have $\tau(f) := \sum_{g \in G/H} f^g \in \mathbb{F}[V]^G$ is a G-invariant mapped to f by ϕ. It follows that if for some positive integer d we have $\mathbb{F}[V]^G_d \subseteq (\mathbb{F}[V]^G_+)^{k+1}$, then $\mathbb{F}[W]^H_d = \phi(\mathbb{F}[V]^G_d) \subseteq \phi((\mathbb{F}[V]^G_+)^{k+1}) = (\mathbb{F}[W]^H_+)^{k+1}$. By definition of the generalized Noether number we conclude $\beta_k(G,V) \geq \beta_k(H,W)$. ☐

Corollary 4.2. *Let H be a subgroup of a finite group G, and suppose that* $\mathrm{char}(\mathbb{F})$ *does not divide the order of G. Then for all positive integers k we have the inequality $\beta_k(H) \leq \beta_k(G)$.*

Next we give a strengthening of Corollary 4.2 in the special case when H is normal in G and the factor group G/H is abelian. For a character $\theta \in \widehat{G/H}$ denote by $\mathbb{F}[V]^{G,\theta}$ the space $\{f \in \mathbb{F}[V] \mid f^g = \theta(g)f \quad \forall g \in G\}$ of *relative G-invariants of weight θ*. Generalizing the construction in the proof of Lemma 4.1, for $f \in \mathbb{F}[W]^H \subset \mathbb{F}[V]$ (here again $V = \mathrm{Ind}_H^G W$) set

$$\tau^\theta(f) := \sum_{g \in G/H} \theta(g)^{-1} f^g \in \mathbb{F}[V]^{G,\theta}.$$

Then $\phi(\tau^\theta(f)) = f$, hence

$$\phi(\mathbb{F}[V]^{G,\theta}) = \mathbb{F}[W]^H \text{ holds for all } \theta \in \widehat{G/H}. \tag{6}$$

Suppose that $U := \bigoplus_{i=1}^d U_i$ is a direct sum of one-dimensional G/H-modules U_i. Making the identification $\mathbb{F}[U \oplus V] = \mathbb{F}[U] \otimes \mathbb{F}[V] = \bigoplus_{\alpha \in \mathbb{N}_0^d} x^\alpha \otimes \mathbb{F}[V]$ (where following the convention introduced in Section 3, the variables $x_1, \dots, x_d$ in $\mathbb{F}[U]$ are G/H-eigenvectors with weight denoted by $\theta(x_i)$), we have

$$\mathbb{F}[U \oplus V]^G = \bigoplus_{\alpha \in \mathbb{N}_0^d} x^\alpha \otimes \mathbb{F}[V]^{G, -\theta(x^\alpha)} \tag{7}$$

Setting $\tilde{\phi} := \mathrm{id} \otimes \phi : \mathbb{F}[U \oplus V] \to \mathbb{F}[U] \otimes \mathbb{F}[W]$, (6) and (7) imply that

$$\tilde{\phi}(\mathbb{F}[U \oplus V]^G_+) = \mathbb{F}[U]^G_+ \oplus \bigoplus_{\alpha \in \mathbb{N}_0^d} x^\alpha \otimes \mathbb{F}[W]^H_+. \tag{8}$$

Theorem 4.3. *Let H be a normal subgroup of a finite group G with G/H abelian, and suppose that* $\mathrm{char}(\mathbb{F})$ *does not divide the order of G. Then for all positive integers k we have the inequality*

$$\beta_k(G) \geq \beta_k(H) + \mathsf{D}(G/H) - 1.$$

Proof. Take $W, V, U = \bigoplus_{i=1}^d U_i$ as above, where in addition we have $\beta_k(H) = \beta_k(H, W)$, and the characters $\theta_1, \ldots, \theta_d$ of the summands U_i constitute a maximal length zero-sum free sequence over the abelian group $\widehat{G/H}$. In particular, $d = \mathsf{D}(G/H) - 1$ (since we may assume that $\mathbb{F}$ is algebraically closed). Choose a homogeneous H-invariant $f \in \mathbb{F}[W]^H$ of degree $\beta_k(H, W)$, not contained in $(\mathbb{F}[W]^H_+)^{k+1}$, and consider the G-invariant

$$t := x_1 \cdots x_d \otimes \tau^\theta(f) \in \mathbb{F}[U \oplus V]^G,$$

where $\theta = \sum_{i=1}^d \theta_i$ (we write the character group $\widehat{G/H}$ additively). Then $t \in \mathbb{F}[U \oplus V]^G$ is homogeneous of degree $d + \beta_k(H, W)$. We shall show that $t \notin (\mathbb{F}[U \oplus V]^G_+)^{k+1}$, implying $\beta_k(G, U \oplus V) \geq \beta_k(H, W) + d = \beta_k(H) + d$. Indeed, assume to the contrary that $t \in (\mathbb{F}[U \oplus V]^G_+)^{k+1}$. Then by (8) we have

$$x_1 \cdots x_d \otimes f = \tilde{\phi}(t) \in (\mathbb{F}[U]^G_+ \oplus \bigoplus_{\alpha \in \mathbb{N}_0^d} x^\alpha \otimes \mathbb{F}[W]^H_+)^{k+1}.$$

Since $\mathbb{F}[U]^G_+$ is spanned by monomials not dividing the monomial $x_1 \cdots x_d$ (recall that $\theta_1, \ldots, \theta_d$ is a zero-sum free sequence), we conclude that

$$x_1 \cdots x_d \otimes f \in (\bigoplus_{\alpha \in \mathbb{N}_0^d} x^\alpha \otimes \mathbb{F}[W]^H_+)^{k+1}. \tag{9}$$

Denote by $\rho : \mathbb{F}[U] \otimes \mathbb{F}[V] \to \mathbb{F}[V]$ the $\mathbb{F}$-algebra homomorphism given by the specialization $x_i \mapsto 1$ $(i = 1, \ldots, d)$. Applying ρ to (9) we get that $f \in (\mathbb{F}[W]^H_+)^{k+1}$, contradicting the choice of f. □

Remark 4.4. (i) Lemma 4.1, Corollary 4.2, and Theorem 4.3 remain true with the same proofs under the weaker condition that $[G : H]$ is finite.

(ii) If G is abelian, we get that $\mathsf{D}_k(G) \geq \mathsf{D}_k(H) + \mathsf{D}(G/H) - 1$ for any subgroup $H \leq G$. For the case $G = H \oplus H_1$, this is shown in Proposition 3 (i) of [16].

5. Extending Goebel's algorithm

In sections 6 - 10 we shall study groups of the form $G = A_0 \rtimes B_0$ where A_0 is abelian and B_0 is cyclic. Even more, A_0 is the commutator subgroup of G. Denoting by C the centralizer of A_0 in B_0, set $A := A_0 \times C$ and $B := B_0/C$. In the cases we shall encounter B has prime order or has order 4, and A_0 is cyclic or is Klein's four group. (Note also that for most of the cases we shall have $A = A_0$ and $B = B_0$.) Thus A is an abelian normal subgroup of G, and the conventions introduced in Section 3 shall apply with respect to A (in particular, our variables will always be A-eigenvectors). The conjugation action of G on A factors through B. This action induces an action on $\widehat{A}$, and apart from the characters factoring through $A/A_0 = C$, all other characters have trivial stabilizer in B. The action of B on A induces an action on sequences over A in the obvious manner. As it is explained in [31] ch. 8.2, any representation W of such a group G over a field $\mathbb{F}$ with $\mathrm{char}(\mathbb{F}) \nmid |G|$ decomposes as $W = W^{A_0} \oplus W_{\perp}^{A_0}$ where

(I) W^{A_0} is the direct sum of 1-dimensional representations of $B_0 = G/A_0$ lifted to G; therefore $\mathbb{F}[W^{A_0}] = \mathbb{F}[z_1, ..., z_s]$ where each z_j is a B_0-eigenvector on which A_0 acts trivially.

(II) $W_{\perp}^{A_0} = U_1 \oplus ... \oplus U_s$ where each U_i is an irreducible representation induced from a 1-dimensional representation of A that is non-trivial on A_0; then each U_i^* has an A-eigenbasis $\{x_{i,1}, ..., x_{i,n_i}\}$, where $n_i = \dim(U_i)$. Moreover, up to non-zero scalar multiples, B permutes the basis elements regularly (i.e. transitively and with trivial stabilizers in B). We shall always tacitly assume that we fixed the decomposition $W = W^{A_0} \oplus U_1 \oplus \cdots \oplus U_s$ above, and submodules of the form $V = U_{i_1} \oplus ... \oplus U_{i_n}$ will be called *admissible* (in particular, the isotypic components of $W_{\perp}^{A_0}$ are admissible). Moreover, it is also tacitly assumed that the variables z_i, $x_{j,l}$ above are our variables in the polynomial ring $\mathbb{F}[W]$. We define accordingly the map $\Phi : M(W) \to \mathcal{M}(A)$ which assigns to each monomial m its weight sequence. Note also that for $g \in G$ and $m \in M(W)$, m^g is a non-zero scalar multiple of a monomial (depending only on the image of g in B under the natural surjection $G \to G/A = B$), and $\theta(m^g) = \theta(m)^g$.

For an admissible subrepresentation of the form $V = U_{i_1} \oplus ... \oplus U_{i_n}$ we shall write $V_{\perp}$ for the direct complement $W^{A_0} \oplus U_{j_1} \oplus ... \oplus U_{j_s}$ and by the canonic isomorphism $\mathbb{F}[W] \cong \mathbb{F}[V] \otimes \mathbb{F}[V_{\perp}]$ the monomial $m \in M(W)$ has a unique factorization $m = vu$ such that $v \in M(V)$ and $u \in M(V_{\perp})$; by $\Phi_V(m)$ we shall denote the weight sequence of this uniquely determined divisor $v \mid m$.

Any sequence $S \in \mathcal{M}(A)$ has a unique factorization $S = R_1 R_2 ... R_h$ such that $R_1 \supseteq ... \supseteq R_h$; we call this the row decomposition of S and we refer to R_i as the i-th row of S. (The intuition behind this terminology is that we like to think of $\Phi(m)$ as a Young diagram where the multiplicities in S of the different elements of A are represented by the heights of the columns.) The non-increasing sequence

$$\lambda(S) := (|R_1|, ..., |R_h|)$$

will be called the *shape* of S while $h(S) := h$ its *height*. The set of the shapes is equipped with the usual reverse lexicographic ordering (i.e. $\lambda(S) \prec \lambda(S')$ if there is a smallest index i such that $|R_i| \neq |R_i'|$ and we have $|R_i| > |R_i'|$ for this i). Observe that $\lambda(S) \prec \lambda(S')$ does not imply $\lambda(ST) \prec \lambda(S'T)$, however $\lambda(ST) \prec \lambda(S)$ always holds. By $\lambda^c(S)$ we denote the prefix of length $c > 0$ in $\lambda(S)$; note that $\lambda^c(S) \prec \lambda^c(T)$ for some c implies $\lambda(S) \prec \lambda(T)$. Abusing notation we write $\lambda(m) := \lambda(\Phi(m))$ for any monomial $m \in M(W)$ and also $\lambda_V(m) := \lambda(\Phi_V(m))$. Similarly, we extend the name row-decomposition to any factorization $m = r_1 ... r_h$ where the $\Phi(r_i)$'s are the rows of $\Phi(m)$; care should be taken though that a row decomposition of a monomial is usually not unique.

Our starting point is the observation that $\mathbb{F}[W]^A$ is spanned by the A-invariant monomials in $M(W)$, and B permutes these monomials, up to non-zero scalar multiples; this allows us to adapt to our case Goebel's method (see [15], [21], [8]) originally developed for permutation-representations. To simplify notation, set $I := \mathbb{F}[W]^A$, $R := \mathbb{F}[W]^G$ and write $\tau := \tau_A^G : I \to R$ for the relative transfer map. The key of our method is the rewriting procedure described below:

Definition 5.1. Let $V \leq W$ be an admissible subrepresentation and $m \in M(W)$ a monomial. Suppose that in the row decomposition $\Phi_V(m) = S_1 ... S_h$

(1) there is an index t such that $S_t = S_{t+1} =: S$ and $\mathrm{Stab}_B(S) = \{1\}$
(2) $\Phi(m) = EF$ for a sequence E and a zero-sum sequence F such that $E \supseteq S_t \prod_{i \in I} S_i$ while $F \supseteq S_{t+1} \prod_{j \in J} S_j$ for a bipartition $I \dot\cup J = \{1, ..., t-1\}$.

In this case m is called *non-terminal* over V and otherwise *terminal* over V. Further, the phrase "terminal over $W_\perp^{A_0}$" will be abbreviated as "terminal".

Lemma 5.2. *Given an admissible submodule $V \leq W_\perp^{A_0}$, any monomial $m \in M(W)$ can be expressed modulo $\mathbb{F}[W]_+^{A,\theta(m)} R_+$ as a linear combination of monomials terminal over V. In particular, an A-invariant monomial $m \in M(W)$ can be expressed modulo $I_+ R_+$ as a linear combination of terminal monomials.*

Proof. We may suppose that m is not terminal over V, so it has a factorization $m = uv$ with $\Phi(u) = E$ and $\Phi(v) = F$ as in Definition 5.1. Consider the relation:

$$\sum_{b \in B} uv^b = u\tau(v) \in \mathbb{F}[W]_+^{A,\theta(m)} (R_+)_{\deg(v)} \tag{10}$$

Then by construction $\lambda_V^t(uv^b) \prec \lambda_V^t(uv)$ for every $b \neq 1$ by the assumption $S^b \neq S$, implying in turn that $\lambda_V(uv^b) \prec \lambda_V(m)$. Our claim follows by induction on $\prec$. □

Lemma 5.2 allows us to concentrate only on terminal monomials: that is, R is spanned by the $\tau(m)$ where m is an A-invariant terminal monomial.

In the remaining part of this section we collect for further reference some facts about zero-sum sequences over the cyclic group Z_n. We shall repeatedly use the Cauchy-Davenport Theorem, asserting that $|A+B| \geq \min\{p, |A|+|B|-1\}$ for any non-empty subsets A, B in Z_p, where p is a prime.

Lemma 5.3 (cf. [14] Thm. 5.3.1)**.** *Let $R_1, ..., R_h \subseteq Z_p \setminus \{0\}$ be given sets such that $|R_1| + ... + |R_h| \geq p$. Then there are elements $s_1, ..., s_n$ and indices $i_1 < ... < i_n \leq h$ such that $s_t \in R_{i_t}$ for every $t = 1, ..., n$ and $s_1 + ... + s_n = 0$.*

Proof. The assumption implies that $h \geq 2$. Set $T_i := R_i \dot\cup \{0\}$ for every $i = 1, ..., h$. To verify our claim suppose indirectly that a sequence as described above does not exist. This means that $0 \notin R_1 + ... + R_h$. Using the Cauchy-Davenport theorem one proves by induction on i that $|T_1 + ... + T_i| \geq |R_1| + ... + |R_i| + 1$ for every $i = 1, ..., h$. Hence by assumption $|T_1 + ... + T_h| \geq p + 1$, but this is impossible. □

Definition 5.4. For any sequence $S = (s_1, ..., s_d)$ over a group A the set of its partial sums is $\Sigma(S) := \{\sum_{i \in I} s_i : I \subseteq \{1, ..., d\}\}$.

Lemma 5.5. *Let p be a prime and $S = (s_1, ..., s_d)$ a sequence of non-zero elements of Z_p. Then $|\Sigma(S)| \geq \min\{p, d+1\}$.*

Proof. We use induction on d; the case $d = 1$ is trivial. Otherwise by the Cauchy-Davenport theorem $|\Sigma(S)| \geq |\Sigma(s_1, ..., s_{d-1})| + |\{0, s_d\}| - 1 = d + 2 - 1$ if $d < p$. □

Lemma 5.6 (Freeze-Smith [12])**.** *For any zero-sum free sequence S over Z_n of length d and maximal multiplicity h it holds that*

$$|\Sigma(S)| \geq 2d - h + 1.$$

6. Groups of dihedral type

Definition 6.1. A sequence C over an abelian group A is called a *zero-corner* if C has a factorization $C = EFH$ into non-empty subsequences E, F, H such that EF and EH are zero-sum sequences. We denote by $\rho(C)$ the minimal value of $\max\{|EF|, |EH|, |FH|\}$ over all factorizations $C = EFH$ satisfying the above properties, and we call it the *diameter* of C.

Lemma 6.2. *Let $S = (s_1, \dots, s_l)$ be a sequence over A consisting of non-zero elements. Suppose that S contains a maximal zero-sum free subsequence of length $d \le l - 3$. Then S contains as a subsequence a zero-corner C with $\rho(C) \le d + 1$.*

Proof. For $I \subseteq \{1, ..., l\}$ we denote by S_I the subsequence $(s_i : i \in I)$. We may suppose that a maximal zero-sum free subsequence of S is S_J where $J = \{1, ..., d\}$. For each $i = 1, 2, 3$ a nonempty subset $H_i \subseteq J \cup \{d + i\}$ exists such that S_{H_i} is an irreducible zero-sum sequence and $d + i \in H_i$. Observe that $|H_i| \ge 2$ as the zero-sum sequence S_{H_i} must consist of non-zero elements. There are two cases:

(i) If the three sets H_i are pairwise disjoint then by definition $C := S_{H_1} S_{H_2} S_{H_3}$ is a zero-corner with $\rho(C) \le d + 3 - \min\{|H_1|, |H_2|, |H_3|\} \le d + 1$.

(ii) Otherwise, if e.g. $H_1 \cap H_2 \neq \emptyset$ then $C := S_{H_1 \cup H_2}$ is a zero-corner with $\rho(C) \le \max\{|H_1|, |H_2|, d+2-|H_1 \cap H_2|\} \le d+1$; indeed, $C = EFH$ with $E := S_{H_1 \cap H_2}$, $F := S_{H_1 \setminus H_2}$, $H := S_{H_2 \setminus H_1}$. □

Keeping conventions, notations and terminology introduced in Sections 3 and 5, we turn to the group $G = A \rtimes_{-1} Z_2 = A \rtimes_{-1} \langle b \rangle$ where A is a non-trivial abelian group, and $a^b = a^{-1}$ for all $a \in A$. Let W be a G-module over $\mathbb{F}$, $I = \mathbb{F}[W]^A$, $R = \mathbb{F}[W]^G$ and $\tau : I \to R$ is the transfer.

Proposition 6.3. *Let $m \in M(W)$ be an A-invariant monomial. Then $m \in I_+ R_+^k$ for some $k \ge 0$ provided that*

(i) $\deg(m) \ge k\,\mathsf{D}(A) + 2$*, or*

(ii) $\deg(m) \ge (k-1)\,\mathsf{D}(A) + d + 2$ *where $\Phi(m)$ contains a zero-corner with diameter d*

Proof. We apply induction on k. The case $k = 0$ is trivial so we may suppose $k \ge 1$. Assume condition (ii). Thus $m = nr$ where the monomial $n = efh$ is such that ef and eh are A-invariant monomials, and $\max\{\deg(ef), \deg(eh), \deg(fh)\} = d$. Setting $\theta(e) =: a \in A$ we have $\theta(f) = \theta(h) = -a$ and $\theta(r) = \theta(e) = a$. By the definition of G the generator b of Z_2 transforms each monomial of weight a into a monomial of weight $-a$, and vice versa, hence fh^b and $e^b r$ are both A-invariant. Now consider the relation:

$$2m = \tau(ef)hr + \tau(eh)fr - \tau(fh^b)e^b r. \tag{11}$$

After division by $2 \in \mathbb{F}^\times$ we get from (11) that $m \in I_{\ge \deg(m)-d}(R_+)_{\le d}$. Given that $\deg(m) - d \ge (k-1)\,\mathsf{D}(A) + 2$ by assumption, the induction hypothesis applies, whence $I_{\ge \deg(m)-d} \subseteq R_+^{k-1} I_+$ and $m \in I_+ R_+^k$ as claimed. Suppose next that condition (i) holds. If m contains three A-invariant variables, then $\Phi(m)$ contains the zero corner $(0, 0, 0)$ with diameter 2, hence we are back in case (ii). Otherwise $\Phi(m)$ contains a subsequence of length at least $k\,\mathsf{D}(A)$ of non-zero elements. If $k > 1$, then by Lemma 6.2 $\Phi(m)$ has a zero-corner of diameter at most $\mathsf{D}(A)$, so again we are back in case (ii). It remains that $k = 1$. If m contains one or two A-invariant variables, then $m \in I_+^3 \subseteq I_+R_+$ by Corollary 2.8. Otherwise m contains a subsequence of length at least $\mathsf{D}(A)+2$ of non-zero elements, hence by Lemma 6.2 $\Phi(m)$ contains a zero-corner of diameter at most $\mathsf{D}(A)$. We are done by case (ii). □

Theorem 6.4. *Let $G = A \rtimes_{-1} Z_2$ and suppose $|G|$ is not divisible by* char($\mathbb{F}$). *Then*

$$\mathsf{D}_k(A) + 1 \leq \beta_k(G) \leq k\,\mathsf{D}(A) + 1$$

Proof. For $d \geq k\,\mathsf{D}(A)+2$ we have $R_d \subseteq R_+^{k+1}$ by Proposition 6.3, and consequently $\beta_k(G) \leq k\,\mathsf{D}(A)+1$. The lower bound is given by Theorem 4.3. □

Since $\mathsf{D}_k(Z_n) = k\,\mathsf{D}(Z_n)$, one concludes:

Corollary 6.5. *For the dihedral group D_{2n} of order $2n$ and an arbitrary positive integer k we have $\beta_k(D_{2n}) = nk+1$, provided that* char($\mathbb{F}$) *does not divide $2n$.*

The special case $k = 1$ of Corollary 6.5 is due to Schmid [30] when char($\mathbb{F}$) $= 0$ and to Sezer [32] in non-modular positive characteristic.

7. Extremal invariants

Definition 7.1. Let $R = \mathbb{F}[W]^G$; then an A-invariant monomial $u \in M(W)$ is called (k,ϵ)-*extremal with respect to* τ if $\deg(u) \geq \beta_k(G) - \epsilon$ while $\tau(u) \notin R_+^{k+1}$. A $(k,0)$-extremal monomial is also called k-*extremal*.

Specialize to the case when $A = Z_n$ is the cyclic group of order $n \geq 3$, and $G = A \rtimes_{-1} Z_2 \cong D_{2n}$ is the dihedral group of order $2n$.

Proposition 7.2. *If $m \in I = \mathbb{F}[W]^A$ is a k-extremal monomial then $\Phi(m) = (0, a^{kn})$ where $\langle a \rangle = Z_n$.*

Proof. The assumption means that $\deg(m) = \beta_k(D_{2n}) = kn+1$ by Corollary 6.5. The weight 0 variables are $B = Z_2$-eigenvectors of eigenvalues ± 1, hence if m is divisible by the product of two weight zero variables, then $m = uv$ where u is a G-invariant of degree 1 or 2. Here $\deg(v) > (k-1)n+1$ (recall that $n > 2$), therefore $v \in I_+R_+^{k-1}$ by Proposition 6.3 (i). Thus $m \in I_+R_+^k$, contradicting the assumption that $\tau(m) \notin R_+^{k+1}$. It follows that the multiplicity of 0 in $\Phi(m)$ is at most one. Let $H \subseteq Z_n$ be the set of nonzero values occurring in $\Phi(m)$. Suppose $|H| \geq 2$; if $\Phi(m)$ contains a zero-corner of the form $(w, w, -w)$ with diameter 2, then $\tau(m) \in R_+^{k+1}$ by Proposition 6.3 (ii), a contradiction. We are done if $n = 3$, so assume for the rest that $n \geq 4$. Hence $\Phi(m)$ contains a zero-sum free subsequence of length 2, consisting of two distinct elements. By Lemma 5.6 this extends to a maximal zero-sum free subsequence of length at most $n-2$. If $k > 1$ or $0 \notin \Phi(m)$, then $\tau(m) \in R_+^{k+1}$ by Lemma 6.2 and Proposition 6.3, a contradiction. If $k = 1$ and $0 \in \Phi(m)$, then $m \in I_+^3$, hence $\tau(m) \in R_+^2$ by Proposition 2.4, a contradiction again. Consequently $|H| = 1$, so $\Phi(m) = (0, a^{kn})$. Taking into account Proposition 2.4, a must be a generator of $Z_n = \widehat{A}$, whence our claim. □

We can say even more about the extremal monomials if $n = p$ is a prime:

Proposition 7.3. *Let $p \geq 5$ be an odd prime and $\epsilon \leq \frac{p-3}{2}$. If $m \in I$ is a (k,ϵ)-extremal monomial, then in the row-decomposition $\Phi(m) = S_1 ... S_h$ we have $h \geq kp - 2\epsilon$, $|S_j| = 1$ for every $j \geq p - \epsilon - 1$ and $\sigma(S_i) \neq 0$ for every $i \geq 1$.*

Proof. The same argument as in the beginning of the proof of Proposition 7.2 shows that the multiplicity of 0 in $\Phi(m)$ is at most 1.

Let S_1^* be the sequence obtained form S_1 by deleting that single occurrence of 0, if it exists. Consider the truncated sequence $T := S_1^* S_2 ... S_{p-\epsilon-1}$. If $|T| \geq p$, then T contains by Lemma 5.3 a zero-sum sequence $C = (s_1, ..., s_n)$ where each s_i belongs to a different row of T, hence $n \leq p - \epsilon - 1$. Given that p is a prime, it is impossible that $s_1 = ... = s_n$, hence there is a smallest index t such that $s_t \neq s_1$. But then $s_t \in S_1^*$ and the sequence $(s_t)C$ forms a zero-corner of diameter $\leq p - \epsilon - 1$. As a result $\tau(m) \in R_+^{k+1}$ by Proposition 6.3, a contradiction. Hence $|T| \leq p - 1$. It follows that $|S_{p-\epsilon-1}| = 1$, for otherwise we would have $|T| \geq 2(p - \epsilon - 1) = p + 1$, a contradiction. Hence each row S_i for $i \geq p - \epsilon - 1$ must consist of the same non-zero element $a \in Z_p$. We also get that $h(S) \geq h(T) + (\deg(m) - 1 - |T|) \geq kp - 2\epsilon$. We have also seen that $\sigma(S_h) \neq 0$. Now suppose indirectly that $\sigma(S_i) = 0$ for some $i \leq h - 1$. Let $S_i = S_{i1} ... S_{in}$ be a decomposition into irreducible zero-sum sequences; by changing indices we may suppose that $S_h \subseteq S_{i1}$. Then the sequence $S_h S_{i1}$ is a zero-corner of diameter $\rho \leq |S_{i1}| \leq \frac{p-1}{2}$ (since $p \geq 5$), hence again $\tau(m) \in R_+^{k+1}$ by Proposition 6.3, a contradiction. □

7.1. **The group $Z_p \rtimes Z_4$, where Z_4 acts faithfully.**

Proposition 7.4. *Let $G := A \rtimes Z_4$ where $A = Z_p$ and $Z_4 = \langle b \rangle$ for an odd prime p such that 4 divides $p - 1$, and conjugation by b is an order 4 automorphism of A. Suppose that $\mathrm{char}(\mathbb{F})$ does not divide $4p$. Then $\beta(G) \leq \frac{3}{2}(p + 1)$.*

Proof. Observe that the subgroup $\langle A, b^2 \rangle \cong A \rtimes Z_2$ of G is isomorphic to the dihedral group D_{2p} of order $2p$. Now let V be an arbitrary finite dimensional G-module and consider the maps:

$$\mathbb{F}[V]^A \xrightarrow{\mu} \mathbb{F}[V]^{D_{2p}} \xrightarrow{\nu} \mathbb{F}[V]^G$$

where $\mu := \tau_A^{D_{2p}}$ and $\nu := \tau_{D_{2p}}^G$ are the relative transfer maps. Note that $\tau := \nu\mu$ is in fact the transfer τ_A^G. We also denote $I := \mathbb{F}[V]^A$, $J := \mathbb{F}[V]^{D_{2p}}$, $R := \mathbb{F}[V]^G$.

We need to show that $R_d \subseteq R_+^2$ for $d \geq p + 4 + \epsilon$, where $\epsilon = \frac{p-3}{2}$. We know that R_d is spanned by its elements of the form $\tau(m)$ where $m \in I_d$ is a monomial. Given that $\beta_2(D_{2p}) - d \leq 2p + 1 - (p + 4 + \epsilon) = \epsilon$, we may suppose that m is $(2, \epsilon)$-extremal with respect to μ, for otherwise we have $\mu(m) \in J_+^3$, whence $\tau(m) = \nu(\mu(m)) \in R_+^2$ by Proposition 2.4 applied for G/D_{2p} acting on J. Proposition 7.3 describes the weight sequence of m and its row-decomposition $S_1 ... S_h$: we get first of all that $h \geq 2p - 2\epsilon = p + 3$ and that $|S_h| = |S_{h-1}| = 1$. Moreover as $\sigma(S_i) \neq 0$ for every i, we get by Lemma 5.5 that the sequence $(\sigma(S_1), ..., \sigma(S_{h-2}))$ contains a subsequence of total weight equal to $-\theta(S_h)$. Therefore we get a factorization $\Phi(m) = EF$ as in Definition 5.1 (note that $\mathrm{Stab}_{\langle b \rangle}(S_h) = \{1\}$), showing that m is non-terminal. Then by Lemma 5.2 we can rewrite m modulo $I_+ R_+$ as a linear combination of terminal monomials m', which cannot be $(2, \epsilon)$-extremal with respect to μ any longer, whence $\tau(m) \in R_+^2$ follows. □

7.2. **The groups $Z_r \rtimes_{-1} Z_{2^{n+1}}$.** Let $B \leq A$ be a subgroup of an abelian group A. For any zero-sum sequence $S = (s_1, ..., s_d)$ over A the sequence $(s_1 + B, ..., s_d + B)$ over A/B will be denoted by S/B. By a *B-contraction* of S we mean a sequence over B of the form $(\sigma(S_1), \ldots, \sigma(S_l))$ where $S = S_1 \cdots S_l$ is a factorization of S such that each S_i/B is an irreducible zero-sum sequence over A/B, hence indeed $\sigma(S_i) \in B$.

We will study here the invariants of the groups $G_n := Z_r \rtimes_{-1} Z_{2^{n+1}}$ where $r \geq 3$ is odd. For $n = 0$ this is the dihedral group of order $2r$. Assume that $n > 0$ for the rest of the section. The group G_n contains a unique cyclic normal subgroup $A_n \cong Z_{r2^n}$ of index two, playing the role of the distinguished abelian normal subgroup A in this section. For $j = 0, \dots, n$, denote by C_j the unique subgroup Z_{2^j} of A_n; it is central in G_n, and $G_n/C_j \cong G_{n-j}$. The restriction of the natural surjection $G_n \to G_{n-j}$ to $A_n \to A_{n-j}$ induces an embedding of the character group $\widehat{A}_{n-j} = Z_{r2^{n-j}}$ as the unique index 2^j subgroup $Z_{r2^{n-j}}$ of $\widehat{A}_n \cong Z_{r2^n}$. Fix an element $b \in G_n \setminus A_n$; identifying $\widehat{A}_n$ with $\mathbb{Z}/2^n r\mathbb{Z}$ and a generator $\widehat{A}_n$ with the residue class of 1, we have

$$1^b \equiv -1 \pmod r \quad \text{and} \quad 1^b \equiv 1 \pmod{2^n} \tag{12}$$

hence $1^b \neq \pm 1$ whenever $n \geq 2$. Moreover for $n = 2$ we have $1^b = 2r - 1$.

Given a G_n-module V, the subalgebra $\mathbb{F}[V]^{C_j} \leq \mathbb{F}[V]$ is G_n-stable, and the action of G_n on it factors through an action of G_{n-j} on $\mathbb{F}[V]^{C_j}$ via graded $\mathbb{F}$-algebra automorphisms.

Lemma 7.5. *There exists a G_{n-j}-module U and a G_{n-j}-equivariant $\mathbb{F}$-algebra surjection $\pi_j : \mathbb{F}[U] \to \mathbb{F}[V]^{C_j}$ such that for any C_j-invariant monomial $m \in M(V)$ and for an arbitrary $Z_{r2^{n-j}}$-contraction S of the weight sequence $\Phi(m)$ there exists a monomial $\tilde{m} \in M(U)$ with $\pi_j(\tilde{m}) = m$ and $\Phi(\tilde{m}) = S$.*

Proof. Let $\mathcal{E}$ be the Hilbert basis of $\mathbb{F}[V]^{C_j}$; that is, $\mathcal{E}$ is the finite set of C_j-invariant monomials minimally generating $\mathbb{F}[V]^{C_j}$. Recall from Section 5 that the A-invariant monomials in $\mathbb{F}[V]$ are involutively permuted by b up to non-zero scalar multiples. It follows that the elements of $\mathcal{E}$ are involutively permuted by b up to non-zero scalar multiples as well, hence $\mathcal{E}$ can be partitioned into the disjoint union of one or two-element sets $\mathcal{E}_i$, $i = 1, \dots, s$, such that each $\mathcal{E}_i$ is spanning an irreducible G_{n-j}-module U_i in which $\mathcal{E}_i$ is the A_{n-j}-eigenbasis. Now set $U := \bigoplus_{i=1}^s U_i^\star$. The obvious identification of the linear component $U^\star$ of $\mathbb{F}[U]$ with $\mathrm{Span}_\mathbb{F}(\mathcal{E})$ induces an $\mathbb{F}$-algebra surjection π_j which is G_{n-j}-equivariant by construction. Note that π_j restricts to a bijection between the set of variables in $\mathbb{F}[U]$ and the Hilbert basis $\mathcal{E}$ in $\mathbb{F}[V]^{C_j}$. Take a C_j-invariant monomial $m \in M(V)$, and a $Z_{r2^{n-j}}$-contraction $S = (\sigma(S_1), \dots, \sigma(S_l))$ of $\Phi(m) = S_1 \cdots S_l$. The monomial m has a corresponding factorization $m = e_1 \cdots e_d$ where $\Phi(e_i) = S_i$. Since S is a $Z_{r2^{n-j}}$-contraction of $\Phi(m)$, it follows that e_i belongs to the Hilbert basis $\mathcal{E}$. Denote by y_i the unique variable in $\mathbb{F}[U]$ with $\pi_j(y_i) = e_i$, and set $\tilde{m} := y_1 \cdots y_d$. Then we have $\pi_j(\tilde{m}) = m$ and $\Phi(\tilde{m}) = S$. □

Lemma 7.6. *Let $S_1, ..., S_l$, for $l \geq 4$ be sequences over A_n such that each S_i/A_{n-j} is an irreducible zero-sum sequence over Z_{2^j} and all A_{n-j}-contractions of $S = S_1 ... S_l$ are similar to (e, f^{l-1}) where $e \neq f$. Then for any subsequences $I \subset S_1$, $J \subset S_2$ such that $\delta := \sigma(I) - \sigma(J) \in A_{n-j}$ we have $\delta \in \{0, \sigma(S_1) - \sigma(S_2)\}$.*

Proof. Swap I and J, i.e. consider the sequences $S_1' := JS_1 \backslash I$ and $S_2' := IS_2 \backslash J$. The A_{n-j}-contraction $(\sigma(S_1'), \sigma(S_2'), \sigma(S_3), ..., \sigma(S_l))$ is either $(e, f^{l-3}, f + \delta, f - \delta)$ or $(e \pm \delta, f \mp \delta, f^{l-2})$ and this must be similar to (e, f^{l-1}) by assumption. Suppose $\delta \neq 0$; then the sequence $(e, f^{l-3}, f + \delta, f - \delta)$ contains three different elements so it cannot be similar to (e, f^{l-1}). It remains that $(e \pm \delta, f \mp \delta, f^{l-2})$ is similar to (e, f^{l-1}), hence equals (e, f^{l-1}) because $l - 2 \geq 2$. Consequently $\delta = f - e$ if $\sigma(S_1) = f$ and $\sigma(S_2) = e$, whereas $\delta = e - f$ if $\sigma(S_1) = e$ and $\sigma(S_2) = f$. □

Lemma 7.7. *Let S be a zero-sum sequence over $A_n = \mathbb{Z}/2^n r\mathbb{Z}$ of length at least $2^n rk+1$ not similar to $(0, 1^{2^n rk})$. Suppose that $n \geq 2$. Then a factorization $S = EF$ exists where E, F are zero-sum sequences over A_n, $|E| \leq 2^n$ and either S or $E^b F$ has a Z_r-contraction of length at least $rk+1$ which is not similar to $(0, (2^n)^{rk})$ (where 2^n is a generator of the unique subgroup Z_r in A_n).*

Proof. Suppose that $|S| \geq 2^n rk + 1$ and all Z_r-contraction of S are similar to $(0, (2^n)^{rk})$. Assume first that $n - 1 \geq 2$ and let $S = S_1 \cdots S_l$ be a factorization where each S_i/A_{n-1} equals $(1, 1)$ or (0). By induction on n we may suppose that $\sigma(S_1) = 0$, $\sigma(S_2) = \cdots = \sigma(S_l) = 2$ and $l = 2^{n-1}rk + 1$. Either $|S| = 2^n rk + 2$ or $|S| = 2^n rk + 1$. If $|S| = 2^n rk + 2$ then $S_i/A_{n-1} = (1, 1)$ for all i and up to similarity $S_2 \cdots S_l = (1^{2^n rk})$ and $S_1 = (-1, 1)$ by Lemma 7.6. If $|S| = 2^n rk + 1$ then $S_t/A_{n-1} = (0)$ for a single index t. If $t = 1$ then $S_1 = (0)$ and $S_2...S_l = (1^{2^n rk})$, a contradiction. If $t > 1$ then $S_1 = (2)$ and $S_2...S_l = (-1, 1^{2^n rk-1})$ by Lemma 7.6. So we have a factorization $S = EF$:

$$\begin{array}{rcll} (-1, 1^{2^n rk+1}) & = & (-1, 1) & (1^{2^n rk}) \\ (-1, 1^{2^n rk-1}, 2) & = & (-1, 1) & (1^{2^n rk-2}, 2) \end{array}$$

Here $E^b F$ is not similar to any of $(0, 1^{2^n rk})$, $(-1, 2, 1^{2^n rk-1})$, or $(-1, 1^{2^n rk+1})$, because $1^b \neq \pm 1$ as $n \geq 2$ by (12). Consequently by what has been said not all A_{n-1}-contractions of $E^b F$ can be similar to $(0, 2^{2^{n-1}rk})$. Applying the induction hypothesis for such an A_{n-1}-contraction our claim follows for S.

It remains the case $n = 2$. Let $S = S_1...S_{rk+1}$ where each S_i/Z_r is an irreducible zero-sum sequence over Z_4, hence is similar to $(1^4), (1^2, 2), (1, 3), (2, 2)$ or (0). The constraint $|S| \geq 4rk+1$ delimits the possible sequences S/Z_r; up to similarity, their complete list is given in the leftmost column of the table below. In each case we distinguish subcases according to S_1/Z_r, where again S_1 is the unique factor for which $\sigma(S_1) = 0$. Then S can be reconstructed as above by repeated applications of Lemma 7.6 (note that $rk + 1 \geq 4$). It is easy to check that up to similarity the following is a complete and irredundant list:

S/Z_r	$S = EF$
$(0)(1^4)^{rk}$	$(0, 1^{4rk})$
	$(-3, 1^3)(4, 1^{4rk-4})$
$(1^4)^{rk+1}$	$(-3, 1^3)(1^{4rk})$
$(1, 3)(1^4)^{rk}$	$(-1, 1)(1^{4rk})$
	$(-3, 1^3)(3, 1^{4rk-3})$
$(2, 2)(1^4)^{rk}$	$(-2, 1^2)(2, 1^{4rk-2})$
	$(-3, 1^3)(2, 2, 1^{4rk-4})$
$(2, 2)(1^2, 2)(1^4)^{rk-1}$	$(-2, 1^2)(2, 2, 1^{4rk-4})$
$(1, 3)(1^2, 2)(1^4)^{rk-1}$	$(-1, 1)(2, 1^{4rk-2})$
	$(-3, 1^3)(3, 2, 1^{4rk-5})$
	$(-2, 1^2)(3, 1^{4rk-3})$
$(1^2, 2)^e(1^4)^{rk+1-e}$	$(-3, 1^3)(2^e, 1^{4rk-2e})$
$e = 1, 2, 3$	$(-2, 1^2)(2^{e-1}, 1^{4rk+2-2e})$

The case when S is similar to $(0, 1^{4rk})$ was excluded. In the rest 1 is the unique element which has multiplicity at least $4rk - 5$ both in EF and $E^b F$. The element $1^b = 2r - 1 \not\equiv \pm 1, \pm 2, \pm 3, 4 \mod 4r$ is missing from EF while it occurs in $E^b F$.

Hence E^bF is not similar to any of the sequences above, consequently it has a Z_r-contraction not similar to $(0, 4^{rk})$. □

In what follows let $\tau_n := \tau_{A_n}^{G_n}$. Observe that $\tau_0 = \tau_{Z_r}^{D_{2r}}$ and if $\pi_j : \mathbb{F}[U] \to \mathbb{F}[V]^{C_j}$ is the surjection constructed in Lemma 7.5 then the following diagram commutes for every $n \geq j \geq 0$:

$$\begin{array}{ccc} \mathbb{F}[U]^{A_{n-j}} & \xrightarrow{\pi_j} & \mathbb{F}[V]^{A_n} \\ \downarrow \tau_{n-j} & & \downarrow \tau_n \\ \mathbb{F}[U]^{G_{n-j}} & \xrightarrow{\pi_j} & \mathbb{F}[V]^{G_n} \end{array}$$

Theorem 7.8. *If $n \geq 2$ then $\beta_k(G_n) = 2^n rk + 1$. Moreover, if $m \in \mathbb{F}[V]^{A_n}$ is a k-extremal monomial with respect to τ_n, then $\Phi(m)$ is similar to $(0, 1^{2^n rk})$.*

Proof. The lower bound $\beta_k(G_n) \geq 2^n rk + 1$ is given by Theorem 4.3. Therefore as m is k-extremal with respect to τ_n, we must have $\deg(m) = \beta_k(G_n) \geq 2^n rk + 1$. Suppose indirectly that $\Phi(m)$ is not similar to $(0, 1^{2^n rk})$. Let $\Phi(m) = EF$ be the factorization given by Lemma 7.7 and $m = uv$ such that $\Phi(u) = E$ and $\Phi(v) = F$. We have two cases:

(i) if EF has a Z_r-contraction S of length at least $rk+1$ which is not similar to $(0, (2^n)^{rk})$ then by Lemma 7.5 a monomial $\tilde{m} \in \mathbb{F}[U]$ exists such that $\pi_n(\tilde{m}) = m$ and $\Phi(\tilde{m}) = S$. Here $\tau_0(\tilde{m}) \in (\mathbb{F}[U]_+^{G_0})^{k+1}$ by Proposition 7.2 and consequently $\tau_n(m) = \tau_n(\pi_n(\tilde{m})) = \pi_n(\tau_0(\tilde{m})) \in (\mathbb{F}[V]_+^{G_n})^{k+1}$, a contradiction.

(ii) if E^bF has a Z_r-contraction of length at least $rk+1$ not similar to $(0, (2^n)^{rk})$ then by the same argument $\tau_n(u^bv) \in (\mathbb{F}[V]_+^{G_n})^{k+1}$. Now consider the relation:

$$\tau_n(m) = \tau_n(u)\tau_n(v) - \tau_n(u^bv) \tag{13}$$

Here $\deg(u) \leq 2^n$ hence $\deg(v) \geq 2^n(rk-1)+1 \geq 2^n r(k-1)+2$. By induction on k we conclude that $\tau_n(v) \in (\mathbb{F}[V]_+^{G_n})^k$. This implies again that $\tau_n(m) \in (\mathbb{F}[V]_+^{G_n})^{k+1}$, a contradiction. □

Theorem 7.9. *We have $\beta_k(G_1) = 2rk + 2$.*

Proof. The inequality $\beta_k(G_1) \leq \beta_{\beta_k(G_1/C_1)}(C_1) = 2rk+2$ holds by Lemma 2.5 and Corollary 6.5. To see the reverse inequality consider the representation on $V = \mathbb{F}^2$ of G_1 given by the matrices:

$$A = \begin{pmatrix} \omega & 0 \\ 0 & \omega^{-1} \end{pmatrix} \qquad B = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

where ω is a primitive r-th root of unity and $i = \sqrt{-1}$ is a primitive fourth root of unity. Then $\mathbb{F}[V] = \mathbb{F}[x, y]$ where x, y are the usual coordinate functions on $\mathbb{F}^2$. Obviously $(xy)^2$ is invariant under A and B alike; from this it is easily seen that $R = \mathbb{F}[V]^{G_1}$ is generated by $(xy)^2$, $\tau(x^{2r})$ and $\tau(x^{2r+1}y)$. This shows that any element of R_+^{k+1} not divisible by $(xy)^2$ must have degree at least $2r(k+1)$. As a result $(R_+^{k+1})_{2rk+2} \subseteq \langle (xy)^2 \rangle$. The invariant $\tau(x^{2rk+1}y) \in R_+$ of degree $2rk+2$ does not belong to the ideal $\langle (xy)^2 \rangle$ showing that $\beta_k(G_1) \geq 2rk+2$. □

8. Groups with a cyclic subgroup of index two

We shall use for the semidirect product of cyclic groups the notation:

$$Z_m \rtimes_r Z_n = \langle a, b : a^m = 1, b^n = 1, a^b = a^r \rangle \quad \text{where } r \in (\mathbb{Z}/m\mathbb{Z})^\times$$

The 2-groups containing a cyclic subgroup of index 2 were classified by Burnside. The following is a complete and irredundant list (see for example [3] ch. IV.4):

(1) $Z_{2^n} \quad (n \geq 1)$
(2) $Z_{2^{n-1}} \times Z_2 \quad (n \geq 2)$
(3) $D_{2^n} := Z_{2^{n-1}} \rtimes_{-1} Z_2 \quad (n \geq 3)$
(4) $M_{2^n} := Z_{2^{n-1}} \rtimes_r Z_2 \quad r = 2^{n-2} + 1 \quad (n \geq 4)$
(5) $SD_{2^n} := Z_{2^{n-1}} \rtimes_r Z_2 \quad r = 2^{n-2} - 1 \quad (n \geq 4)$
(6) $Q_{2^n} = Dic_{2^n} := \langle a, b \mid a^{2^{n-1}} = 1, b^2 = a^{2^{n-2}}, a^b = a^{-1} \rangle \quad (n \geq 3)$

Let H be a 2-group with a cyclic subgroup H_0 of index two. So H belongs to the above list. It is easy to see that the automorphism group of H acts transitively on the set of the index two cyclic subgroups of H, hence we may assume without loss of generality that $H_0 = \langle a \rangle$ in cases (2), (3), (4), (5), (6) (and of course H_0 is the unique index two subgroup when H is cyclic). For an odd positive integer r write $Z_r \rtimes_{-1} H$ for the semidirect product where for $h \in H \setminus H_0$ and $a \in Z_r$ we have $a^h = a^{-1}$.

Proposition 8.1. *A complete irredundant list of the isomorphism classes of finite groups containing a cyclic subgroup of index two is*

$$Z_l \times (Z_r \rtimes_{-1} H)$$

where r, l are coprime odd integers, and H is a 2-group from the list (1)–(6) above.

Proof. Let G be a finite group with an index two cyclic subgroup C. Then C uniquely decomposes as $C = Z_m \times Z_{2^{n-1}}$ for some odd positive integer m and $n \geq 1$. Since Z_m is a characteristic subgroup of C, it is normal in G. Hence by the Schur-Zassenhaus theorem $G = Z_m \rtimes H$ for a Sylow 2-subgroup H of G. Moreover, the characteristic direct factor $Z_{2^{n-1}}$ is also normal in G, hence is contained in the Sylow subgroup H as its index two cyclic subgroup H_0 (with the notation introduced before the statement). Now Z_m uniquely decomposes as a direct product $Z_m = P_1 \times \cdots \times P_r$ of its Sylow subgroups. After a possible renumbering we may assume that H centralizes $P_1, \ldots, P_s$, and H/H_0 acts on $P_{s+1}, \ldots, P_r$ via the automorphism $x \mapsto x^{-1}$. Setting $Z_l := P_1 \times \cdots \times P_r$, $Z_r := P_{s+1} \times \cdots \times P_r$ we obtain the desired conclusion. □

For an odd integer $r \geq 3$ recall the standard notation $D_{2^n r} := Z_r \rtimes_{-1} D_{2^n}$ $(n \geq 1)$, $M_{2^n r} := Z_r \rtimes_{-1} M_{2^n}$ $(n \geq 4)$, $SD_{2^n r} := Z_r \rtimes_{-1} SD_{2^n}$ $(n \geq 4)$, $Dic_{2^n r} := Z_r \rtimes_{-1} Q_{2^n r}$ $(n \geq 3)$. Note the isomorphism

$$Z_r \rtimes_{-1} (Z_{2^{n-1}} \times Z_2) \cong Z_{2^{n-1}} \times D_{2r}$$

and recall that the groups $Z_r \rtimes_{-1} Z_{2^n}$ were studied in Section 7.2.

Proposition 8.2. *For coprime integers $n \geq 1$, $m \geq 3$ and a positive integer k we have that*

$$\beta_k(Z_n \times D_{2m}) = \beta_k(Z_n \times SD_{2m}) = \beta_k(Z_n \times M_{2m}) = knm + 1$$

where m is divisible by 8 for the latter two groups.

Proof. If G is any group with a cyclic subgroup $A = \langle a \rangle$ of index 2, then Theorem 4.3 gives us the following lower bound:

$$\beta_k(G) \geq \beta_k(A) + \mathsf{D}(G/A) - 1 = k|A| + \mathsf{D}(Z_2) - 1 = \tfrac{1}{2}|G| + 1$$

For the converse inequalities we need to calculate first the generalized Noether numbers β_s for the groups D_{2m}, SD_{2m}, M_{2m} for an arbitrary integer $s \geq 1$. Theorem 6.4 states that

$$\beta_s(D_{2m}) \leq sm + 1 \tag{14}$$

In the group SD_{2m} consider the subgroup $B = \langle a^2, b \rangle \cong D_m$. Observe that B is a normal subgroup, as it has index 2, hence by Lemma 2.5 and (14) we get that

$$\beta_s(SD_{2m}) \leq \beta_{\beta_s(Z_2)}(B) = \beta_{2s}(D_m) \leq sm + 1 \tag{15}$$

As for the group M_{2m}, consider the subgroup $C = \langle a^2, b \rangle \cong Z_{m/2} \times Z_2$. Observe that C is a normal subgroup as it has index 2 in M hence by Lemma 2.5 and Proposition 3.1 we get that

$$\beta_s(M_{2m}) \leq \beta_{\beta_s(Z_2)}(C) \leq \beta_{2s}(Z_{m/2} \times Z_2) = sm + 1 \tag{16}$$

Finally, our claim follows by setting $s = \beta_k(Z_n) = kn$ in the inequalities (14), (15) and (16) an then applying Lemma 2.5 in the last step. ☐

Proposition 8.3. *Let n, m be coprime positive integers with m divisible by 4, and $k \geq 1$. Then*

$$knm + 1 \leq \beta_k(Z_n \times Dic_{2m}) \leq knm + 2$$

and $\beta_k(Dic_{2m}) = km + 2$.

Proof. Let $G := Z_n \times Dic_{2m}$. Then $G/Z(Dic_{2m}) \cong Z_n \times D_m$, hence $\beta_k(G) \leq 2\beta_k(Z_n \times D_m) = knm + 2$ by Lemma 2.5 and Proposition 8.2. The inequality $\beta_k(Z_n \times Dic_{2m}) \geq knm + 1$ follows from Theorem 4.3 as in the proof of Proposition 8.2. Taking ω a primitive mth root of unity in the proof of Theorem 7.9 one gets the inequality $\beta_k(Dic_{2m}) \geq km + 2$. ☐

Our results on the generalized Noether number of the groups with a cyclic subgroup of index 2 are summarized in Table 1.

G	$\beta_k(G) - \frac{k}{2}\lvert G\rvert$
$Z_n \times D_{2m}$	1
$Z_n \times SD_{2m}$	1
$Z_n \times M_{2m}$	1
Dic_{2m}	2
$Z_n \times Dic_{2m}$	1 or 2
$Z_r \rtimes_{-1} Z_4$	2
$Z_n \times (Z_r \rtimes_{-1} Z_4)$	1 or 2
$Z_n \times (Z_r \rtimes_{-1} Z_{2^n})$ $n > 2$	1

TABLE 1. β_k for the groups with a cyclic subgroup of index 2

9. The semidirect product $Z_p \rtimes Z_q$

Let W be a representation of the non-abelian semidirect product $G = Z_p \rtimes Z_q$ (where p and q are odd primes, q necessarily dividing $p-1$). We work under the conventions of Section 5, with $A := Z_p \triangleleft G$, $I := \mathbb{F}[W]^A$, $R := \mathbb{F}[W]^G$ and $\tau : I \to R$ the transfer. Let $V \leq W_\perp^A$ be an isotypic admissible subrepresentation; we say that a monomial $m \in M(W)$ is *gapless* over V if

$$\lambda_V(m)_i = \lambda_V(m)_{i+1} \quad \Rightarrow \quad \lambda_V(m)_i = q$$

(note that $\lambda_V(m)_i = q$ means that the ith row in the row decomposition of $\Phi_V(m)$ is a full Z_q-orbit). For an arbitrary admissible submodule $U \leq W$ with isotypic decomposition $U = V_1 \oplus ... \oplus V_s$ we say that $m \in M(W)$ is *gapless over* U if it is gapless over each V_i. (We shall say simply *gapless* instead of gapless over $W_\perp^A$.) Denote by $\mathcal{T}_d(U)$ the set of degree d gapless monomials in $M(U)$, and $\langle \mathcal{T}_d(U) \rangle$ the subspace of I spanned by the A-invariant monomials having a divisor in $\mathcal{T}_d(U)$. Furthermore, $\mathcal{T}_d := \mathcal{T}_d(W_\perp^A)$ and $\langle \mathcal{T}_d \rangle := \langle \mathcal{T}_d(W_\perp^A) \rangle$. It turns out that in case of this group the terminal monomials of Definition 5.1 have "large" degree gapless divisors.

Proposition 9.1. *Let U be an admissible submodule of W, $d \geq 0$, and let w be an A-invariant monomial of degree $d+p-1$, divisible by a degree d monomial in $M(U)$. Then we have*

$$w \in \langle \mathcal{T}_d(U) \rangle + I_+ R_+ + I_1 I_{d+p-2}.$$

In particular, $I_{d+p-1} \subseteq \langle \mathcal{T}_d \rangle + I_1 I_{d+p-2} + I_+ R_+$.

Proof. If w contains an A-invariant variable, then $m \in I_1 I_{d+p-2}$ and we are done. From now on we assume that this is not the case. Factor $w = nm$ where $m \in M(U)$ and $n \in M(U_\perp)$, so $\deg(m) \geq d$ by assumption. Let $m = m_1 ... m_s$ be the factorization of m corresponding to the isotypic decomposition $U = V_1 \oplus ... \oplus V_s$. Choose a gapless divisor $m_i^* \mid m_i$ of maximal degree for every $i \geq 1$ and set $m^* = m_1^* ... m_s^*$. If $\deg(m^*) \geq d$ then $m \in \langle \mathcal{T}_d(U) \rangle$ and we are done. From now on we suppose that $\deg(m^*) \leq d-1$. Consequently there is a minimal index i such that $m_i^* \neq m_i$, i.e. m_i is not gapless. By Lemma 5.2 we may suppose that $w/(m_1^* ... m_{i-1}^*)$ is terminal over V_i. In the row-decomposition $\Phi(m_i) = S_1 ... S_h$ there is a minimal index t such that $|S_t| = |S_{t+1}| < q$. Observe that $\mathrm{Stab}_{Z_q}(S_t) = \{1\}$ by the primality of q. Let u_0 and v_1 be monomials such that $u_0 v_1 \mid m_i$ and $\Phi(u_0) = S_1 ... S_t$ while $\Phi(v_1) = S_{t+1}$. Set $u_1 := m_1^* ... m_{i-1}^* u_0$ and $f := w/(u_1 v_1)$. Remark that by construction $\deg(u_1 v_1) \leq \deg(m^*) + 1 \leq d$ hence $\deg(f) \geq p-1$. As a result $|\Sigma(\Phi(f))| = p$ by Lemma 5.5, so a monomial $v_2 \mid f$ exists with weight equal to $-\theta(v_1)$. Set $v := v_1 v_2$ and $u := w/(m_1^* ... m_{i-1}^* v)$. Then $\Phi(uv) = \Phi(u)\Phi(v)$ satisfies the requirements of Definition 5.1. Therefore $w/(m_1^* ... m_{i-1}^*)$ is non-terminal over V_i, a contradiction. □

Proposition 9.2. *We have the inequality $\beta(Z_p \rtimes Z_q) \leq p + \frac{q(q-1)^2}{2}$.*

Proof. We shall prove by induction on $t \geq 0$ that if $m \in I$ is a monomial with $\deg(m) \geq p + 1 + t\binom{q}{2}$ then $m \in I_+^{t+2} + I_+ R_+$, whence our claim follows by Corollary 2.8. The case $t = 0$ is trivial, so we may suppose that $t > 0$. If $h(m) \leq \binom{q}{2}$ then by Lemma 5.3 the weight sequence of m contains a non-empty zero-sum sequence of length at most $h(m)$, hence $m = uv$ where $u \in I_+$ and $\deg(u) \leq \binom{q}{2}$, and

$v \in I_+^{t+1} + I_+R_+$ by induction. Similarly we are done if m contains an A-invariant variable, so suppose this is not the case, and suppose $h(m) > \binom{q}{2}$. Then an isotypic component $V \subset W$ exists such that the divisor $n \mid m$ belonging to $\mathbb{F}[V]$ has $\deg(n) \geq h(m) > \binom{q}{2}$. By Proposition 9.1 we may suppose that n has a divisor n_1 gapless over V with $\deg(n_1) > \binom{q}{2}$. This forces that n contains a divisor u whose weight-sequence consists of a Z_q-orbit, so that $u \in I_q$. We are done again by induction. □

For a positive integer $s \leq p$ set

$$\delta(s) := \sup\{d \in \mathbb{N} \mid \langle \mathcal{T}_d \rangle \nsubseteq (I_+)_{\leq s} I\}$$

so a gapless monomial of degree $d > \delta(s)$ has a non-trivial A-invariant divisor of degree at most s.

Proposition 9.3. *Suppose that $\delta(s)$ is finite.*

(i) *If $d \geq p + \delta(s) + st$ for some non-negative integers t and d, then we have $I_d \subseteq (I_+)^{t+1} I_{\geq d-(t+1)s} + I_+R_+$.*

(ii) *We have the inequality*

$$\beta(G, W) \leq p - 1 + \max\{s+1, \delta(s)\} + s(q-2).$$

Proof. (i) Apply induction on t. The case $t = 0$ follows by Proposition 9.1 and the definition of $\delta(s)$. When $t > 0$, by Proposition 9.1 we have $I_d \subseteq \langle \mathcal{T}_{d-p+1} \rangle + I_1 I_{d-1} + I_+R_+ \subseteq \sum_{j=1}^{s} I_j I_{d-j} + I_+R_+$ (the second inclusion holds by the definition of $\delta(s)$). For $j = 1, \ldots, s$ we have $d - j \geq p + \delta(s) + s(t-1)$, hence I_{d-j} is contained in $I_+^t I_{\geq d-j-st} + I_+R_+$ by the induction hypothesis. Consequently, $I_d \subseteq \sum_{j=1}^{s} I_j I_+^t I_{\geq d-s(t+1)} + I_+R_+ \subseteq I_+^{t+1} I_{\geq d-s(t+1)} + I_+R_+$

(ii) Set $\delta := \max\{s+1, \delta(s)\}$. For $d \geq p + \delta + s(q-2)$ by (i) we have $I_d \subseteq I_+^{q-1} I_{\geq p+\delta-s} + I_+R_+$. Note that $p+\delta-s \geq p+1$ by assumption, hence $I_{\geq p+\delta-s} \subseteq I_+^2$. We conclude that $I_d \subseteq I_+^{q+1} + I_+R_+ \subseteq I_+R_+$, since $I_+^{q+1} \subseteq I_+R_+$ by Corollary 2.8. □

The following two propositions provide explicit bounds for $\delta(s)$.

Proposition 9.4. *We have*

$$\delta(q) \leq \tfrac{1}{2}(p - 2 + q(q-2)).$$

Proof. Suppose that $m \in \mathcal{T}_d$ has no non-trivial A-invariant divisor of degree at most q. Then m contains no A-invariant variables, so $m \in M(W_\perp^A)$. Denote by S_i the set of weights occuring in $\Phi_{V_i}(m)$, where V_i ($i = 1, \ldots, \frac{p-1}{q}$) are the isotypic components of $W_\perp^A$. By our assumption $0 \notin S := \bigcup_j S_j$ and $|S_i| \leq q - 1$ for every i.

As each factor m_i is gapless, it is easily seen that $\deg(m_i) \leq \binom{|S_i|+1}{2} \leq \frac{|S_i|q}{2}$, hence

$$\deg(m) \leq \frac{|S|q}{2}. \tag{17}$$

We claim that $|S| \leq q + \frac{p-1}{q} - 2$. Write $T^{\wedge q} := \{t_1 + \cdots + t_q \mid t_i \neq t_j \in T\}$ for a subset T of A. If the claim was false then we would get from the Dias da Silva - Hamidoune theorem (see [6]) that

$$|(S\dot{\cup}\{0\})^{\wedge q}| \geq q(|S|+1) - q^2 + 1 \geq q(q + \frac{p-1}{q}) - q^2 + 1 = p$$

implying that m contains an A-invariant divisor of degree q or $q-1$, which is a contradiction. After plugging in this upper bound on $|S|$ in (17) and taking into account that q is odd we get that $\deg(m) \le \lfloor \frac{q^2-2q+p-1}{2} \rfloor = \frac{1}{2}(p-2+q(q-2))$. □

Proposition 9.5. *Suppose c, e are positive integers such that $c \le q$ and $\binom{c}{2} < p \le \binom{c+1}{2} - \binom{e+1}{2}$ (in particular, this forces that $p < \binom{q+1}{2}$). Then*

$$\delta(c-e) \le p - 1 + \binom{e}{2}.$$

Proof. Suppose that $m \in \mathcal{T}_d$ has no non-trivial A-invariant divisor of degree at most $c-e$. Take the row-decomposition $\Phi(m) = S_1 \cdots S_h$ and set $E := S_1 \cdots S_{c-e}$, $F := S_{c-e+1} \cdots S_h$. We have $|E| \le p-1$, for otherwise by Lemma 5.3 we would get an A-invariant divisor of degree at most $c-e$. It follows that $|S_{c-e}| \le e$, for otherwise the fact that m is gapless and $c \le q$ would lead to the contradiction

$$|E| \ge (e+1) + (e+2) + ... + (e + (c-e)) = \tbinom{c+1}{2} - \tbinom{e+1}{2} \ge p.$$

As a result $|S_{c-e+1}| \le e-1$, hence $|F| \le \binom{e}{2}$ since m is gapless. But then $\deg(m) = |E| + |F| \le p - 1 + \binom{e}{2}$, and this proves our claim. □

Theorem 9.6. *We have the inequality $\gamma(Z_p \rtimes Z_q) < \frac{1}{2}$, with the only possible exception when* $\mathrm{char}(\mathbb{F}) = 2$*, $p = 7$, and $q = 3$.*

Proof. It follows from Proposition 9.2 that $\beta(Z_p \rtimes Z_3) \le p + 6$. (This was already proved by Pawale ([26] for the case $\mathrm{char}(\mathbb{F}) = 0$). Therefore $\gamma(G) \le \frac{1}{3} + \frac{2}{p} < \frac{1}{2}$, provided that $p > 7$. The group $Z_7 \rtimes Z_3$ will be treated separately in Subsection 9.1.

From now on we assume that $q \ge 5$. Combining Proposition 9.3 and Proposition 9.4 we get

$$\frac{\beta(G,V)}{|G|} \le \frac{p - 1 + \frac{1}{2}(p-2+q(q-2)) + q(q-2)}{pq} = \frac{3}{2}\left(\frac{1}{q} + \frac{q-2}{p}\right) - \frac{2}{pq}. \tag{18}$$

It is easy to see that the right hand side is smaller than $1/2$ when $p \ge 4q+1$.

When $p = 2q+1$ we have $c \le q$ for the unique c with $\binom{c}{2} < p < \binom{c+1}{2}$, and Proposition 9.5 applies with this c and $e = 1$. So by Proposition 9.3 we get

$$\frac{\beta(G,V)}{|G|} = \frac{2p - 2 + (q-2)(c-1)}{pq} < \frac{2}{q} + \frac{q-2}{q} \cdot \frac{2}{c} \tag{19}$$

(in the second inequality we used that $c(c-1)/2 < p$). Taking into account that $c(c+1)/2 > p$ one shows easily that the right hand side is less than $1/2$ for all pairs $(q, p = 2q+1)$ except for $q \le 5$.

It remains to deal with the case $q = 5$ and $p = 11$. By taking $c = 5$ and $e = 2$ in Proposition 9.5 we obtain that $\delta(3) \le 11$. Hence $I_{\ge 28} \subseteq I_+^3 I_{\ge 19} + I_+ R_+$ by Proposition 9.3. We claim that $I_{\ge 19} \subseteq (I_+)_{\le 5} I_{\ge 14} + I_+ R_+$. Indeed, take an A-invariant monomial $m \in M(W_\perp^A)$ with $\deg(m) \ge 19$. By Proposition 9.1 we may suppose that m has a gapless divisor $n \in \mathcal{T}_9$. Then $h(\Phi(n)) \le 3$, and hence there is a degree 2 monomial u such that nu divides m and $h(\Phi(nu)) \le 5$. By Lemma 5.3 nu has an A-invariant divisor of degree at most 5, and our claim is proved. Obviously $I_{\ge 14} \subseteq I_+^2$. Putting these together we get $I_{\ge 28} \subseteq I_+^6 + I_+ R_+ \subseteq I_+ R_+$ by Corollary 2.8. This implies as before that $\beta(Z_{11} \rtimes Z_5) \le 27$. □

9.1. **The group $Z_7 \rtimes Z_3$.** In this section we will deal with the group $G = Z_7 \rtimes Z_3$, and suppose that $\mathrm{char}(\mathbb{F}) \neq 2, 3, 7$. We shall identify $A := Z_7$ with the additive group of residue classes modulo 7, and Z_3 with the subgroup $\langle 2 \rangle \leq (\mathbb{Z}/7\mathbb{Z})^\times$, acting by multiplication on $\mathbb{Z}/7\mathbb{Z}$. Then we have three Z_3-orbits in Z_7, namely $A_0 := \{0\}$, $A_+ := \{1, 2, 4\}$, $A_- := \{3, 5, 6\}$. Accordingly G has two non-isomorphic irreducible representations of dimension 3, denoted by V_+ and V_-. Let W be an arbitrary representation of G; it has a decomposition

$$W = V_+^{\oplus n_+} \oplus V_-^{\oplus n_-} \oplus V_0 \tag{20}$$

where V_0 is a a representation of Z_3 lifted to G. Any monomial $m \in \mathbb{F}[W]$ has a canonic factorization $m = m_+ m_- m_0$ given by the isomorphism $\mathbb{F}[W] \cong \mathbb{F}[V_+^{\oplus n_1}] \otimes \mathbb{F}[V_-^{\oplus n_2}] \otimes \mathbb{F}[V_0]$; the degrees of these factors will be denoted by $d_+(m), d_-(m), d_0(m)$. Finally we set $I = \mathbb{F}[W]^{Z_7}, R = \mathbb{F}[W]^G$ and $\tau : I \to R$ is the transfer map.

Proposition 9.7. *Let $m \in M(W_\perp^A)$ be a Z_7-invariant monomial with* $\deg(m) \geq 7$ *and* $2 \leq d_+(m), d_-(m) \leq 6$*. Then $m \in I_2 I_+ + I_+ R_+$.*

Proof. Denote by S the weight sequence of m, and let S_1 be its first row. Suppose that $m \notin I_2 I_+ + I_+ R_+$. Then $S_1 \cap -S_1 = \emptyset$ hence in particular $|S_1| \leq 3$. Moreover $|S_1| > 1$ since $d_+(m), d_-(m)$ are both positive. Suppose now that $|S_1| = 2$. If $\deg(m) \geq 8$ then non-empty zero-sum sequences U, V exist such that $S = UV$. If moreover $\deg(m) = 7$ then $h(m) = 5$ or 4, hence a similar decomposition exists by Lemma 5.6. It also follows from our assumptions that none of U or V can be of the form (a^7) for some $a \in Z_7$, hence their first rows U_1, V_1 have length two. Therefore S is non-terminal by Definition 5.1 and this case can be discarded by Lemma 5.2.

It remains that $|S_1| = 3$. Up to similarity, we may suppose that $S_1 \cap A_+ = \{1\}$, hence $S_1 \cap A_- = \{3, 5\}$. The irreducible zero-sum sequences with support contained in the set $\{1, 3, 5\}$ are the following:

$$(1^2 5),\ (3^3 5),\ (135^2),\ (1^4 3),\ (3^2 5^3),\ (15^4),\ (13^2),\ (1^7),\ (3^7),\ (5^7)$$

If $U = (135^2)$ is a subsequence in S then let $S = UV$. By the assumption $d_+(m) \geq 2$ we have that $1 \in V$. Then $m = uv$ with $\Phi(u) = (3, 5^2)$, and v is not terminal over V_+. By Lemma 5.2, m can be rewritten modulo $I_+ R_+$ as a linear combination of monomials whose weight sequence has first row of length at least 4.

If (135^2) is not a subsequence of S then as (135) is still contained in S by assumption we get that the multiplicity of 5 is one. Hence from the irreducible zero-sum sequences listed above only $(3^3 5), (1^2 5), (1^4 3), (13^2)$ can occur as irreducible subsequences of S. It follows that S contains one of the following subsequences: $(3^3 5)(13^2), (3^3 5)(1^4 3), (1^2 5)(1^4 3), (1^2 5)(13^2)(13^2)$. A quick look to these shows that using (10), m can be reduced modulo $I_+ R_+$ to a linear combination of monomials having an A-invariant divisor of degree 2. □

Corollary 9.8. *Let $m \in M(W)$ be a Z_7-invariant monomial with* $\deg(m) \geq 10$ *and $d_+(m), d_-(m) \leq 6$. Then $m \in I_+ R_+$.*

Proof. Obeserve that if $h\Phi(n)) \leq 4$ and $\deg(n) \geq 5$, then n contains an A-invariant divisor by Lemma 5.6. Using this observation, and applying Proposition 9.7 repeatedly we get that $m \in I_+^4$. Now recall that $I_+^4 \subseteq I_+ R_+$ by Corollary 2.8. □

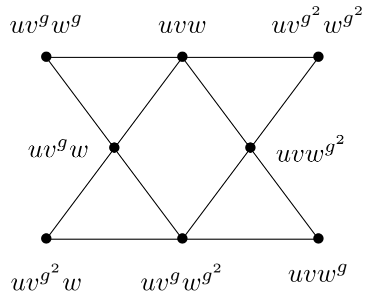
Lemma 9.9. *Let $G = A \rtimes \langle g \rangle$ where $\langle g \rangle \cong Z_3$ and A is an arbitrary Abelian group. If $3 \in \mathbb{F}^\times$ then for any monomials $u, v, w \in I_+$ the following relation holds:*

$$uvw \equiv uv^g w^{g^2} \mod I_+(R_+)_{\leq deg(vw)}$$

Proof. The following identity can be checked by mechanic calculation:

$$3\left(uvw - uv^g w^{g^2}\right) = uv\tau(w) + uw\tau(v) + u\tau(vw) - u\tau(vw^g) - uw^{g^2}\tau(v) - uv^g\tau(w)$$

Alternatively, the reader might check that the three members with positive sign on the right hand side correspond in the diagram below to the three "lines" through uvw, while the other three members to the three "lines" through $uv^g w^{g^2}$:



(A second relation can be obtained by interchanging the role of g and g^2.) □

Proposition 9.10. *If $m \in M(W)$ is a Z_7-invariant monomial with $\deg(m) \geq 10$ then $m \in I_+R_+$ provided that one of the following conditions holds:*

(i) *$n_+ \leq 3$, $d_+(m) \geq 7$ or $n_- \leq 3$, $d_-(m) \geq 7$;*
(ii) *$n_+ \leq 4$, $d_+(m) \geq 9$ or $n_- \leq 4$, $d_-(m) \geq 9$.*

Proof. Suppose that $n_+ \leq 3$ and $d_+(m) \geq 7$. Moreover, treat first the case when m contains no A-invariant variables. The isomorphism $\mathbb{F}[V_+^{\oplus 3}] \cong \mathbb{F}[V_+]^{\otimes 3}$ gives a factorization $m_+ = m_1 m_2 m_3$. Since $d_+(m) = \deg(m_1) + \deg(m_2) + \deg(m_3)$, at least one of these monomials, say m_1 has degree at least 3. Let us introduce the variables x_i, y_i, z_i of weight $1, 2$ and 4, respectively, so that $\mathbb{F}[x_i, y_i, z_i] \cong \mathbb{F}[V_+]$ for each $i = 1, 2, 3$. By Proposition 9.1 (applied when U is the first summand V_+ of $V_+^{\oplus 3}$) we may assume that m_1 has a gapless divisor of degree at least 3 if $\deg(m_1) = 3$, and m_1 has a gapless divisor of degree 4 if $\deg(m_1) > 3$. Note that $x_1 y_1 z_1$ is a G-invariant, so we are done if m is divisible by $x_1 y_1 z_1$. Otherwise $\deg(m_1) = 3$ and by symmetry we may assume that m_1 is divisible by $x_1^2 y_1$. Applying again Proposition 9.1 with $U = V_+^{\oplus 3}$, we may achieve that m_+ has a gapless divisor of degree 4, and keep the property that m_1 is gapless. By symmetry we may assume therefore that m is divisible by $u := x_1 y_1 z_i$. If m/u factors as the product of non-empty A-invariant monomials vw, then from Lemma 9.9 we get that $uvw \equiv uv^b w^{b^2}$ modulo I_+R_+, where $b \in \{g, g^2\}$ can be chosen so as to assure that $uv^b w^{b^2}$ is divisible by the G-invariant monomial $x_1 y_1 z_1$; whence $m = uvw \in I_+R_+$. The only missing case is when $\Phi(m_+/w) = (1^7)$, i.e. when $m = x_1^2 y_1 X^6 Z$, where X, Y, Z stands for any of the variables x_i, y_i, z_i for any $i = 1, 2, 3$. Here we can employ the relations:

$$x_1^2y_1X^6Z = x_1y_1X^4\ \tau(x_1X^2Z) - x_1y_1z_1X^4Z^2Y - x_1y_1^2X^5Y^2$$
$$x_1y_1^2X^5Y^2 = x_1y_1Y^2\ \tau(y_1X^5) - x_1y_1z_1Y^7 - x_1^2y_1Y^2Z^5$$

to prove that $m \equiv x_1^2y_1Y^2Z^5 \mod I_+R_+$, and this later monomial already belongs to I_+R_+ by our former argument.

If m contains at least two A-invariant variables, then $m \in I_+^4 \subseteq I_+R_+$ by Corollary 2.8. If m contains a single A-invariant variable w, then m_1 can be assumed to have a gapless divisor of degree 3, so we are done unless m is divisible by $x_1^2y_1$. Since $|\Phi(m/wx_1^2y_1)| = 6$, there must exist a factorization $m = uvw$ where $u = x_1y_1n$, $v = x_1n'$ are A-invariant. We finish using Lemma 9.9 as above.

Suppose next that $n_+ \leq 4$ and $d_+(m) \geq 9$. Let $m_+ = m_1m_2m_3m_4$ be the factorization coming from the isomorphism $\mathbb{F}[V_+^{\oplus 4}] \cong \mathbb{F}[V_+]^{\otimes 4}$. By symmetry we may assume $\deg(m_1) \geq 3$. Now the same argument as before yields $m \in I_+R_+$. □

We shall use several times the following result:

Proposition 9.11 (Knop, Theorem 6.1 in [20]). *Let U and V be finite dimensional G-modules. If $n_0 \geq \max\{\dim(V), \frac{\beta(G)}{\mathrm{char}(\mathbb{F})-1}\}$ and S is a generating set of $\mathbb{F}[U \oplus V^{\oplus n_0}]^G$ then $\mathbb{F}[U \oplus V^{\oplus n}]^G$ for any $n \geq n_0$ is generated by the polarization (with respect to the type-V variables) of S.*

Theorem 9.12. *If* $\mathrm{char}(\mathbb{F}) \neq 2, 3, 7$ *then* $\beta(G) = 9$.

Proof. The lower bound $\beta(G) \geq 9$ follows from Theorem 4.3. As for the converse we have $\beta(G) \leq 13$ by Proposition 9.2. Therefore it is sufficient to show that $\tau(m) \in R_+^2$ for any Z_7-invariant monomial $m \in M(W)$ with $10 \leq \deg(m) \leq 13$, where W is a G-module as in (20).

Suppose first that $\mathrm{char}(\mathbb{F}) > 7$. Then $\max\{\dim(V_+), \dim(V_-), \frac{\beta(G)}{\mathrm{char}(\mathbb{F})-1}\} = 3$, hence by Proposition 9.11 it is sufficient to deal with the case when $n_+, n_- \leq 3$. Then either $d_+(m)$ or $d_-(m) \geq 7$, and we are done by Proposition 9.10 (i), or $d_+(m), d_-(m) \leq 6$, and we are done by Corollary 9.8.

Finally suppose that $\mathrm{char}(\mathbb{F}) = 5$, hence $\max\{\dim(V_+), \dim(V_-), \frac{\beta(G)}{\mathrm{char}(\mathbb{F})-1}\} \leq 4$. Therefore by Proposition 9.11 it is sufficient to deal with the case when $n_+, n_- \leq 4$. Then we are done by Proposition 9.10 (ii) provided that $d_+(m) \geq 9$ or $d_-(m) \geq 9$. From now on we assume that $d_+(m), d_-(m) \leq 9$. Since $9 \leq 3(\mathrm{char}(\mathbb{F}) - 1)$, by formula (6.3) and Theorem 5.1 in [20] we conclude that $\tau(m)$ is contained in the polarization (with respect to V_+ and V_-) of $\mathbb{F}[V_+^{\oplus 3} \oplus V_-^{\oplus 3} \oplus V_0]^G$. The latter algebra is generated in degree at most 9 by Corollary 9.8 and Proposition 9.10 (i) as in the above paragraph, implying in turn that $\tau(m) \in R_+^2$. □

Remark 9.13. Pawale in [26] has proved, in fact for the whole non-modular case, that $\beta(G, W) = 9$ whenever $n_+, n_- = 2$. From this he concluded using Weyl's Theorem on polarization that $\beta(G) = 9$ in characteristic 0.

10. The alternating group A_4

Throughout this section $G := A_4$, the alternating group of degree four. The double transpositions and the identity constitute a normal subgroup $A \cong Z_2 \times Z_2$ in G, and $G = A \rtimes Z_3$ where $Z_3 = \{1, g, g^2\}$. Denote by a, b, c the involutions in A, conjugation by g permutes them cyclically. Let $\mathbb{F}$ be a field whose characteristic is different from 2 or 3. Apart from the one-dimensional representations of G factoring through the natural surjection $G \to Z_3$, up to isomorphism there is a single irreducible G-module V, the 3-dimensional summand in the natural 4-dimensional permutation representation of G. An arbitrary finite dimensional G-module W decomposes as $W = W^A \oplus V^{\oplus n}$, where W^A is a sum of one-dimensional G-modules. We follow our conventions introduced in Section 5: $\mathbb{F}[V^{\oplus n}] = \otimes_{i=1}^n \mathbb{F}[x_i, y_i, z_i]$ where x_i, y_i, z_i are A-eigenvectors of weight a, b, c which are permuted cyclically by g. We set $I := \mathbb{F}[W]^A$, $R := \mathbb{F}[W]^G$, $\tau := \tau_A^G : I \to R$.

We begin with a quick overview of the zero-sum sequences over $Z_2 \times Z_2$. The irreducible ones are: (0) , (a, a), (b, b), (c, c), (a, b, c), and between them we have the relation $(a, b, c)(a, b, c) = (a, a)(b, b)(c, c)$. Hence the factorization of a zero-sum sequence S over $Z_2 \times Z_2$ into maximally many irreducible ones is of the form

$$S = (0)^q (a^2)^r (b^2)^s (c^2)^t (a, b, c)^e \qquad \text{where } e = 0 \text{ or } 1. \tag{21}$$

Observe also that the multiplicities of a, b and c in S must have the same parity.

Proposition 10.1. *Any A-invariant monomial $m \in M(V^{\oplus 3})$ of degree at least 7 belongs to $I_+(R_+)_{\leq 4}$.*

Proof. Let $m = m_1 m_2 m_3$ be the factorization given by the map $\mathbb{F}[V^{\oplus 3}] \cong \mathbb{F}[V]^{\otimes 3}$; by symmetry we may suppose that $\deg(m_1) \geq 3$. If the G-invariant $x_1 y_1 z_1$ divides m then we are done. Using relation (10) we may assume that $\Phi(m_1)$ contains at least two different weights, say $x_1 y_1^2 \mid m_1$. If the multiplicity of b is at least 3 in S, then $m / x_1 y_1^2 y_i$ has an A-invariant divisor w with $\deg(w) = 2$. Set $v := y_1 y_i$, then $u := m/uv$ is divisible by $x_1 y_1$. By Lemma 9.9 we can replace m with the monomial $uv^g w^{g^2}$, which is divisible by the G-invariant $x_1 y_1 z_1$. Finally, if the multiplicity of b in $\Phi(m)$ is 2, then the multiplicity of a and c is even, hence $\deg(m/x_1 y_1^2) \geq 5$. It follows that m has an A-invariant factorization $m = uvw$ with $x_1 y_1^2 \mid u$, and $\deg(v) = \deg(w) = 2$. By Lemma 9.9 m can be replaced by $uv^g w^{g^2}$ or $uv^{g^2} w^g$ so as to get back to the case treated before. □

Proposition 10.2. *Suppose that* $\operatorname{char}(\mathbb{F})$ *is different from* 2 *or* 3*. For any positive integer k and $W = U \oplus V^{\oplus 3}$ we have the inequality $\beta_k(A_4, W) \leq 4k + 2$.*

Proof. We show by induction on k that if m is an A-invariant monomial of degree at least $4k + 3$, then $m \in I_+ R_+^k$ (implying in turn that $\tau(m) \in R_+^{k+1}$). The case $k = 0$ is trivial. Assume $k > 0$. Let m_0 and m_+ denote the divisors of m belonging to U and $V^{\oplus 3}$, respectively. If $\deg(m_+) \geq 7$, then by Proposition 10.1 $m \in (R_+)_{\leq 4} I_{\geq 4(k-1)+3} \subseteq I_+ R_+^k$, since $I_{\geq 4(k-1)+3} \subseteq I_+ R_+^{k-1}$ by the induction hypothesis. If $\deg(m_+) \leq 6$, then $m \in I_+^{4k} \subseteq I_+^{3k+1} \subseteq I_+ R_+^k$ by Corollary 2.8. □

Theorem 10.3. *If* $\operatorname{char}(\mathbb{F}) \neq 2, 3$ *then* $\beta(A_4) \leq 6$*. Moreover for* $k \geq 2$ *we have:*

$$\beta_k(A_4) \leq \begin{cases} 4k + 2 & \text{if } \operatorname{char}(\mathbb{F}) = 0 \\ 5k & \text{if } \operatorname{char}(\mathbb{F}) > 0 \end{cases}$$

Proof. Note that Proposition 10.2 applies in particular when $V = V_{reg}$ is the regular representation of A_4. It was observed in [30] that when $\operatorname{char}(\mathbb{F}) = 0$, Weyl's theorem on polarization (cf [35]) implies the equality $\beta(G) = \beta(G, V_{reg})$. The argument in [30] can be easily extended to conclude the equality $\beta_k(G) = \beta_k(G, V_{reg})$ for an arbitrary positive integer k in characteristic zero, hence for this case the claim follows by Proposition 10.2. Suppose next that $\mathbb{F}$ has positive characteristic p

different from 2 or 3. Take an arbitrary finite dimensional G-module $W = U \oplus V^{\oplus n}$. We know already the conclusion when $n \leq 3$. So suppose that $n > 3$. We have $\beta(A_4) \leq \beta_3(Z_2 \times Z_2) = 7$ by Lemma 2.9. View $W_0 := U \oplus V^{\oplus 3}$ as a direct summand of $W = W_0 \oplus V^{\oplus n-3}$ in the obvious way. Correspondingly the algebra $S := \mathbb{F}[W_0]^G$ is a retraction of the algebra $R := \mathbb{F}[W]^G$. There is a natural action of the general linear group GL_n on $\mathbb{F}[W]$ via graded $\mathbb{F}$-algebra automorphisms (see e.g. [30] for the details). This action commutes with the action of G, hence preserves R. Moreover, it was proved by Knop (see [20], formula (6.3) in the proof of Theorem 6.1) that $R_d = GL_n \cdot S_d$ (the GL_n-submodule generated by S_d) provided that $d \leq 3(p-1)$ (where 3 is the number of summands V in W_0). Since $p \geq 5$, this holds for all $d \leq 12$. In particular $R_7 = GL_n \cdot S_7$. On the other hand $S_7 \subseteq S_+^2$ by Proposition 10.2. It follows that $R_7 \subseteq GL_n \cdot (S_+)^2 \subseteq (GL_n \cdot S_+)^2 \subseteq R_+^2$, hence $\beta(G, V) \leq 6$ also in this case, and the proof of the inequality $\beta(A_4) \leq 6$ is finished.

Furthermore, we know already that $\beta_2(G, W) \leq 2\beta(A_4) \leq 12$ by Lemma 2.2. Applying the result of Knop cited above for $d = 11$ or $d = 12$ we have that $R_d = GL_n \cdot S_d$. On the other hand for $d = 11$ or $d = 12$ we have $S_d \subseteq S_+^3$ by Proposition 10.2. Summarizing, we obtain $R_d \subseteq GL_n \cdot (S_+)^3 \subseteq (GL_n \cdot S_+)^3 \subseteq R_+^3$. Consequently, $\beta_2(G, W) \leq 10$ in this case as well. Since W was arbitrary, we conclude $\beta_2(A_4) \leq 10$. Finally, for $k \geq 2$ we have $\beta_k(A_4) \leq \frac{k}{2}\beta_2(A_4) = 5k$ by Lemma 2.2. □

Corollary 10.4. *Suppose that the characteristic of* $\mathbb{F}$ *is different from* 2 *or* 3. *Then we have* $\beta(A_4) = 6$ *and* $\beta(\tilde{A}_4) = 12$.

Proof. The inequality $\beta(A_4) \leq 6$ holds by Theorem 10.3, and since $\tilde{A}_4$ has a two-element normal subgroup N with $\tilde{A}_4/N \cong A_4$, the inequality $\beta(\tilde{A}_4) \leq 12$ follows by Lemma 1.4. Note that it is sufficient to prove the reverse inequalities in characteristic zero by Theorem 4.7 of [20]. Now consider the ring of invariants of the 2-dimensional complex representation of $\tilde{A}_4$ realizing it as the binary tetrahedral group. It is well known (see for example the first row in the table of Lemma 4.1 in [18] or Section 0.13 in [27]) that this algebra is minimally generated by three elements of degree $6, 8, 12$, implying the inequality $\beta(\tilde{A}_4) \geq 12$. □

Remark 10.5. Working over the field of complex numbers Schmid [30] already gave a computer aided proof of the equality $\beta(A_4) = 6$.

10.1. **The group** $(Z_2 \times Z_2) \rtimes Z_9$**.**

Proposition 10.6. *Take the non-abelian semidirect product* $G := (Z_2 \times Z_2) \rtimes Z_9$, *and suppose that the characteristic of* $\mathbb{F}$ *is different from* 2 *or* 3. *Then we have* $\beta(G) \leq 17$.

Let $K := Z_2 \times Z_2 = \{0, a, b, c\}$ and $Z_9 = \langle g \rangle$. Then conjugation by g permutes a, b, c cyclically, say $a^g = b$, $b^g = c$, $c^g = a$. G contains the abelian normal subgroup $A := K \times C$ where $C := \langle g^3 \rangle \cong Z_3$. For an arbitrary G-module W we set $J = \mathbb{F}[W]^C$, $I = \mathbb{F}[W]^A$, $R = \mathbb{F}[W]^G$; we use the transfer maps $\mu : J \to R$, $\tau : I \to R$.

Proof. Since $G/C \cong A_4$ and $\beta(A_4) = 6$, by Lemma 1.4 we conclude that $\beta(G) \leq 18$. Take a monomial $m \in I$ with $\deg(m) = 18$. Using the notation introduced at the beginning of Section 7.2, we may restrict our attention to the case when $\Phi(m)/K = (h^{18})$ where $h \in \{g^3, g^6\}$ for otherwise $m \in J_+^7$ and we get by Proposition 2.4 applied for G/C acting on J that $\mu(m) \in R^2_+$. We claim that in this case $\Phi(m)$ must contain at least 2 zero-sum sequences over A of length at most 3, and consequently $m \in I^4_+$ (since $\beta(A) = 7$ by Proposition 3.1), whence $\tau(m) \in R^2_+$ again by Proposition 2.4.

To verify this claim, factor $m = uv$ where $\Phi(v)/C = (0^n)$ and $\Phi(u)/C$ does not contain 0. By Lemma 5.2 we may also suppose that u is terminal. If $n \geq 3s$ then $\Phi(v)$ contains at least s zero-sum sequences of length at most 3. Therefore it suffices to show that $\Phi(u)/C$ contains the subsequence (a, b, c) whenever $\deg(u) \geq 13$, because then the corresponding subsequence of $\Phi(u)$ is a zero-sum sequence over A. Suppose indirectly that this is false and that $\Phi(u)/C$ contains e.g. only a and b. This means that $\Phi(u)/C = (a^{2x}, b^{2y})$ where $2(x + y) = \deg(u)$. By symmetry we may suppose that $x \geq y$ and hence $x \geq 4$. Now $\Phi(u)/C$ decomposes as follows:

$$\begin{aligned} &(a^4, b^2) \cdot (a^{2x-4}, b^{2y-2}) && \text{if } y \geq 2 \\ &(a^6) \cdot (a^{2x-6}, b^{2y}) && \text{if } y \leq 1 \end{aligned}$$

Observe that the first factor has degree 6, hence it corresponds to a zero-sum sequence over A. By Definition 5.1 we get a contradiction with the assumption that u was terminal. □

11. Details of the structure theorem

11.1. **p-groups.** By [29] a non-cyclic p-group contains a normal subgroup isomorphic to $Z_p \times Z_p$, except when $p = 2$ and the group contains a cyclic subgroup of index two (see also III. 7. 6 in [19]). Henceforth (3) or (4a) of Theorem 1.2 holds for non-cyclic odd order p-groups, except for $Z_3 \times Z_3$.

Proposition 11.1. *Let G be a 2-group. Then one of the following holds for G:*

(i) *G has a cyclic subgroup of index 2;*
(ii) *$G \cong Z_2 \times Z_2 \times Z_2$;*
(iii) *G has a subquotient which is an extension of $Z_2 \times Z_2$ by itself.*

Proof. Denote by $r := r(G)$ and $s := s(G)$ the ranks of the elementary abelian 2-groups $G/\Phi(G)$ and $\Phi(G)/\Phi(\Phi(G))$, where $\Phi(H)$ stands for the Frattini subgroup of a group H. If $s = 0$, then G is elementary abelian of rank r, so either $r \leq 3$ and then (i) or (ii) holds, or $r \geq 4$, and then the direct product of two copies of $Z_2 \times Z_2$ is a subgroup of G, thus (iii) holds. If $r = 1$ then G is cyclic. If $r \geq 4$ then $G/\Phi(G)$ contains an elementary abelian subgroup of rank 4 and (iii) holds.

If $(r, s) = (2, 1)$, then (i) holds: Indeed, $\Phi(G) = \langle c \rangle$ is cyclic in this case. Take elements a, b whose images generate $G/\Phi(G) \cong Z_2 \times Z_2$. Then $1, a, b, ab$ represent all the elements of $G/\Phi(G)$. Suppose that $a^2, b^2, (ab)^2$ all belong to $\langle c^2 \rangle$. Then a standard calculation shows that a and b commute modulo the normal subgroup $\langle c^2 \rangle$ of G, hence $G/\langle c^2 \rangle \cong Z_2 \times Z_2 \cong G/\langle c \rangle$, a contradiction. Consequently, one of $a^2, b^2, (ab)^2$ generates $\langle c \rangle$, implying in turn that one of a, b, ab generates a subgroup of index two in G. .

If $(r, s) = (3, 1)$, then (iii) holds: Indeed, $\Phi(G) = \langle d \rangle$ is cyclic, and passing to the factor group $G/\langle d^2 \rangle$ we may assume $d^2 = 1$ and $|G| = 16$. If $g \in G \setminus \Phi(G)$ has order 2, then $N := \langle g, d \rangle \cong Z_2 \times Z_2$ is a normal subgroup with $N \cong G/N$, hence (iii) holds. Assume next that d is the only order two element of G. It follows that any index 2 subgroup of G is isomorphic to Q_8, the quaternion group of order 8. Thus $\langle a, b \rangle \cong Q_8 \cong \langle a, c \rangle$, where a, b, c are elements of G whose images generate $G/\Phi(G)$. Consequently, $cac^{-1} = a^{-1}$ and $cbc^{-1} = b^{-1}$, implying $c(ab)c^{-1} = a^{-1}b^{-1} = ab$

(the latter equality follows from $a^2 = b^2 = d$ and $d^2 = 1$). It means that c commutes with ab, hence $\langle ab, c\rangle \cong Z_4 \times Z_2$, a contradiction.

If $s = 2$, then (iii) holds: Indeed, take a subgroup $L \supseteq \Phi(G)$ with $L/\Phi(G) \cong Z_2 \times Z_2$. The chain $\Phi(\Phi(G)) \triangleleft \Phi(G) \triangleleft L$ shows that the subquotient $L/\Phi(\Phi(G))$ of G is an extension of $Z_2 \times Z_2$ by itself.

If $s \geq 3$, then $G/\Phi(\Phi(G))$ contains a subgroup H of order 16 with $Z_2 \times Z_2 \times Z_2$ as a subgroup of H. Then H has no cyclic subgroup of index two, hence by the above considerations the pair $(r(H), s(H))$ belonging to H is not $(2, 1)$ or $(1, 0)$. It remains that $(r(H), s(H))$ is one of $(4, 0)$, $(3, 1)$, or $(2, 2)$, hence (iii) holds for H. □

Corollary 11.2. *(3), (4a), (4b), or (5a) of Theorem 1.2 holds for the finite group G unless the Sylow p-subgroups for $p \geq 5$ are cyclic, the Sylow 3-subgroup is cyclic or $Z_3 \times Z_3$, the Sylow 2-subgroup contains a cyclic subgroup of index at most two or is isomorphic to $Z_2 \times Z_2 \times Z_2$.*

11.2. **Solvable groups.**

Proposition 11.3. *If all Sylow subgroups of G are cyclic, then (2), (5d), or (5e) of Theorem 1.2 holds for G.*

Proof. By a well known theorem of Burnside from 1905 (see page 163 in [4]), if all Sylow subgroups of G are cyclic, then G is isomorphic to a semidirect product $Z_n \rtimes Z_m = Z_n \rtimes \langle b\rangle$ of cyclic groups, where n, m are coprime positive integers.

If all Sylow subgroups of Z_n are centralized by b^2, then G contains a cyclic subgroup of index at most 2. Otherwise there is an odd prime p and a subgroup of G of the form $Z_{p^k} \rtimes \langle b\rangle$, where b^2 does not centralize Z_{p^k}. Factoring out the centalizer of Z_{p^k} in $\langle b\rangle$ we may assume that $\langle b\rangle$ acts faithfully on Z_{p^k}. Then $\langle b\rangle$ has an element c whose order q is an odd prime or $q = 4$. Thus the subgroup $Z_{p^k} \rtimes \langle c\rangle$ is isomorphic to $Z_{p^k} \rtimes Z_q$, and c^2 does not centralize Z_{p^k}. Denote by P the unique p-element subgroup of Z_{p^k}. If $\langle c\rangle$ acts faithfully on P, then $P \rtimes \langle c\rangle$ is a subquotient of G of the desired form. Otherwise P is contained in the center of $Z_{p^k} \rtimes \langle c^2\rangle$ (recall that $\langle c^2\rangle = \langle c\rangle$ when q is odd). Since $Z_{p^k} \rtimes \langle c^2\rangle$ is non-abelian, its factor group $Z_{p^k} \rtimes \langle c^2\rangle/P \cong Z_{p^{k-1}} \rtimes \langle c^2\rangle$ is non-cyclic, so c^2 acts faithfully on $Z_{p^k}/P \cong Z_{p^{k-1}}$. By induction on k we conclude that $(Z_{p^k} \rtimes \langle c\rangle)/P$ has a subquotient of the desired form. □

Proposition 11.4. *Let G be a semidirect product $G \cong Z_n \rtimes Q$ where n is odd and Q is a 2-group containing a cyclic subgroup of index two. Then (2) or (5b) or (5c) or (5e) of Theorem 1.2 holds for G.*

Proof. When Q is cyclic, the statement follows from Proposition 11.3. From now on suppose that Q is non-cyclic. Denote by $a \in Q$ an element generating an index two subgroup (say the generator denoted by a in the list of such groups). If a centralizes Z_n, then G contains a cyclic subgroup of index two. From now on we assume that a does not centralize Z_n. Denote by C the centralizer of Z_n in Q. Since the automorphism group of Z_n is abelian, C contains the commutator subgroup of Q, hence C is normal in Q, and Q/C is abelian. Moreover, C is normal in G, and we have the factor group $G/C \cong Z_n \rtimes (Q/C)$, where Q/C acts faithfully on Z_n.

Case I: Q/C is not cyclic. Then Q/C contains a subgroup isomorphic to $Z_2 \times Z_2$, and $Z_n \rtimes (Z_2 \times Z_2)$ (where $Z_2 \times Z_2$ acts faithfully on Z_n) is a subquotient of G.

Write $Z_n = P_1 \times \cdots \times P_r$, where P_i is a Sylow p_i-subgroup. The only involutive automorphism of P_i is $x \mapsto x^{-1}$. Denote by c, d generators of $Z_2 \times Z_2$. Factoring out the Sylow subgroups centralized by both c and d we may assume that for each $i = 1, \dots, r$, c or d acts non-identically on P_i. Not both c and d act involutively on all the P_i, since otherwise cd acts identically on Z_n. By symmetry we may assume that c acts involutively on P_1 and d acts identically on P_1. There is an $i > 1$ such that d acts involutively on P_i, say $i = 2$. Consider the subgroup $(P_1 \times P_2) \rtimes (Z_2 \times Z_2)$. Replacing the generator c by cd if necessary, we may assume that c acts involutively on P_1 and identically on P_2, whereas d acts involutively on P_2 and identically on P_1. Taking the prime element subgroups in P_1 and P_2 we find a subgroup $(Z_p \times Z_q) \rtimes (Z_2 \times Z_2)$, where p, q are distinct odd primes, c centralizes Z_q whereas $x^c = x^{-1}$ for $x \in Z_p$, and d centralizes Z_p whereas $x^d = x^{-1}$ for $x \in Z_q$. Clearly this group is isomorphic to $D_{2p} \times D_{2q}$.

Case II: Q/C is cyclic. Then Q/C is generated by the image $\bar{a}$ of $a \in Q$. If the order of $\bar{a}$ is at least 4, then G/C contains a subgroup isomorphic to $Z_{p^k} \rtimes Z_4$, where p is an odd prime and Z_4 acts faithfully on Z_{p^k} (take a Sylow subgroup Z_{p^k} of Z_n), and as explained in the proof of Proposition 11.3, it follows that $Z_p \rtimes Z_4$ is a subquotient of G/C. From now on we assume that $a^2 \in C$, i.e. $Q/C \cong Z_2$. If C is cyclic, then G contains a cyclic subgroup of index two. Suppose from now on that C is not cyclic. Then $C/\Phi(C) \cong Z_2 \times Z_2$, where $\Phi(C)$ denotes the Frattini subgroup of C. Since $\Phi(C)$ is a characteristic subgroup of the normal subgroup C of G, it follows that $\Phi(C)$ is normal in G. Set $\hat{G} := G/\Phi(C)$ and $\hat{C} := C/\Phi(C)$. Then $\hat{C} \cong Z_2 \times Z_2$ is a normal subgroup of $\hat{G}$, and $\hat{G}/\hat{C} \cong Z_n \rtimes \langle \bar{a} \rangle \cong Z_n \rtimes Z_2$, a non-abelian semidirect product. It follows that $\hat{G}/\hat{C}$ contains a subgroup isomorphic to a dihedral group D_{2p} for some odd prime p. Summarizing, an extension of D_{2p} by $Z_2 \times Z_2$ occurs as a subquotient of G. □

Proposition 11.5. *Let G be a metacyclic group whose all odd order subquotients are cyclic, and whose Sylow 2-subgroups contain a cyclic subgroup of index 2. Then (2) or (5b) or (5e) of Theorem 1.2 holds for G.*

Proof. Let $2 = p_1 < p_2 < \cdots < p_r$ be the prime divisors of $|G|$, and $P_1, \dots, P_r$ the corresponding Sylow subgroups. By Lemma 2.6 in [33], P_r, $P_{r-1}P_r$, …, $P_2P_3 \cdots P_r$ are all normal subgroups in G. Thus $P_2P_3 \cdots P_r \cong Z_n$ for an odd n, and $G \cong Z_n \rtimes Q$, where $Q = P_1$ is a Sylow 2-subgroup of G. Therefore the statement follows from Proposition 11.4 above, since $D_{2p} \times D_{2q}$ is not metacyclic, so the case (5c) of Theorem 1.2 does not occur now. □

Proposition 11.6. *Let G be a 2-group with a cyclic subgroup of index 2. Then G has a non-trivial odd order automorphism α if and only if $G \cong Z_2 \times Z_2$ or $G \cong Q_8$ (the quaternion group of order 8), and in this case α has order three.*

Proof. It is well known that both $Z_2 \times Z_2$ and Q_8 have order three automorphisms. The automorphism group of a cyclic 2-group is a 2-group, hence has no non-trivial odd order automorphism. Suppose that G is non-cyclic with an odd order automorphism α. Then α acts identically on the cyclic characteristic subgroup $\Phi(G)$, hence induces an automorphism of $G/\Phi(G) \cong Z_2 \times Z_2$ of the same order as α. Consequently the order of α is three. One sees from the list of the 2-groups with a cyclic subgroup of index 2 (see Section 8) that the factor group $\tilde{G} := G/\langle a^4 \rangle$ is isomorphic to the dihedral group D_8 or $Z_4 \times Z_2$ unless $G \cong Q_8$ or $G \cong Z_2 \times Z_2$.

Since α acts identically on the cyclic characteristic subgroup $\langle a^4\rangle$, it induces an order three automorphism of $\tilde{G}$. Note finally that neither D_8 nor $Z_4 \times Z_2$ have non-trivial odd order automorphisms. □

Remark 11.7. The semidirect products with Z_3 given by the order three automorphism of $Z_2 \times Z_2$ and Q_8 are $A_4 \cong (Z_2 \times Z_2) \rtimes Z_3$ and $\tilde{A}_4 \cong Q_8 \rtimes Z_3$.

Proposition 11.8. *Suppose $G = Q \rtimes Z_n$ where Q is a 2-group containing a cyclic subgroup of index 2, and n is odd. Then one of the following holds:*

(i) G contains a cyclic subgroup of index two;
(ii) The non-abelian semidirect product $(Z_2 \times Z_2) \rtimes Z_9$ is a factor group of G;
(iii) $G \cong A_4 \times Z_k$ or $G \cong \tilde{A}_4 \times Z_k$ for an odd integer k not divisible by 3.

Proof. If Z_n centralizes Q, then G contains a cyclic subgroup of index two, hence we are in case (i). From now on we assume that G does not contain a cyclic subgroup of index two. Then conjugation by the generator a of the subgroup $Z_n \leq G$ is a non-trivial odd order automorphism α of Q, hence by Proposition 11.6 $Q \cong Z_2 \times Z_2$ or $Q \cong Q_8$ (the quaternion group of order 8) and the order of α is 3. We distinguish two cases. First if n is divisible by 9, then a^9 centralizes Q, hence $N := \Phi(Q)\langle a^9\rangle$ is a normal subgroup of G, and G/N is a non-abelian semidirect product $(Z_2 \times Z_2) \rtimes Z_9$, so we are in case (ii). The second case is when $n = 3k$ where k is not divisible by 3. Then $G \cong A_4 \times Z_k$ or $G \cong \tilde{A}_4 \times Z_k$, so we are in case (iii). □

Proposition 11.9. *Let G be a solvable group whose all odd order subquotients are cyclic, and whose Sylow 2-subgroup contains a cyclic subgroup of index two. If G is not metacyclic, then one of (1), (4c), (5b), (5c), (5e), or (5f) of Theorem 1.2 holds for G.*

Proof. By assumption G has a subnormal chain $G_1 \triangleleft G_2 \triangleleft G_3 \triangleleft \cdots \triangleleft G_s = G$ with cyclic factors, such that G_3 is not metacyclic, hence G_2 is non-cyclic; moreover, either $G_3 = G$ or G_3 is a proper normal subgroup of G_4. Therefore if any of (4c), (5a), (5b), (5c), (5d), (5e), (5f) holds for G_3 or G_2, then it holds for G, and if (1) holds for G_3 then (1) or (4c) holds for G. It is sufficient to deal with the case when none of (1), (5a), (5b), (5c), (5d), (5e), (5f) holds for G_3 and $G_3 = G$. From now on we assume that this is the case. We conclude by Proposition 11.5 that G_2 has a cyclic subgroup of index 2. Denote by K_1 the odd order cyclic characteristic subgroup of G_2 such that G_2/K_1 is a 2-group (cf. Section 8). Since K_1 is a characteristic subgroup in G_2, it is normal in G. Recall that $G_2 = K_1 \rtimes Q_1$ for a Sylow 2-subgroup Q_1 of G_2. Now embed Q_1 into a Sylow 2-subgroup Q of G. Then $G_2 \leq N := K_1Q$ is a normal subgroup of G, and $G/N \cong Z_m$ is an odd order cyclic group. Note that N has a cyclic subgroup of index two by Proposition 11.4, hence G/N is non-trivial. If $K_1 = \{1\}$, then $G \cong Q \rtimes Z_m$, and (4c) holds for G by Proposition 11.8. From now on we assume that none of K_1 or G/N is trivial.

By the Schur-Zassenhaus Theorem, there is a subgroup K_2 of G/K_1 such that $G/K_1 = Q \rtimes K_2$; write K for the preimage of K_2 under the natural surjection $G \to G/K_1$. Then K is an odd order subgroup of G, hence $K = \langle a\rangle$ is cyclic. Moreover, we have $K_1 = \langle a^m\rangle$ and $G = Q\langle a\rangle$.

Observe that $\bar{G} := G/K_1$ is not metacyclic. Indeed, otherwise by Propositions 11.5 $\bar{G}$ contains a cyclic subgroup of index two. Then K_2 is the odd order cyclic characteristic subgroup of $\bar{G}$ whose index is a 2-power, and hence K is a normal subgroup of G. It follows that $G \cong Z_n \rtimes Q$ (where n is odd), and we arrive at a contradiction by Proposition 11.4.

By Proposition 11.8 we conclude that either (5f) or (4c) holds for $G/K_1 = Q \rtimes K_2$, but (5f) can not hold by our assumption. Therefore $m = 3k$ for an odd integer k not divisible by 3 and $\bar{G} \cong A_4 \times Z_k$ or $\bar{G} \cong \tilde{A}_4 \times Z_k$, implying that $Q \cong Z_2 \times Z_2$ or $Q \cong Q_8$. In particular, conjugation by a is an order $3s$ (where s is odd) automorphism of N, since it induces an order three automorphism on $N/K_1 = Q$. Since a centralizes K_1, conjugation by a preserves the centralizer C of K_1 in $N = K_1Q$. Since N has a cyclic subgroup of index 2, either $C = N$ or $[N : C] = 2$ (hence $C \supset \Phi(Q)$). In the latter case a operates trivially on N/C, hence conjugation by a can not induce an order three automorphism of $N/K_1\Phi(Q) \cong Z_2 \times Z_2$. Consequently $C = N$, implying in turn that Q is a characteristic subgroup of N, hence Q is normal in G and $G = Q \rtimes \langle a \rangle = Q \rtimes Z_{3kl}$ where $l = |K_1| > 1$. Note that 3 does not divide l, since otherwise (5f) would hold for G contradicting to our assumption. Thus $G \cong A_4 \times Z_{kl}$ or $G \cong \tilde{A}_4 \times Z_{kl}$, hence (4c) holds for G. □

Proposition 11.10. *Suppose G is an odd order group with cyclic Sylow subgroups, except the Sylow 3-subgroup which is isomorphic to $Z_3 \times Z_3$. Then (1), (4a), or (5d) of Theorem 1.2 holds for G.*

Proof. Assume that G properly contains its Sylow 3-subgroup P, and (5d) does not hold for G. Then by Proposition 11.3 a subquotient of G is cyclic unless its order is divisible by 9. Then $P \subseteq G^{(d-2)}$, where $G = G^{(0)} \supset G^{(1)} \supset \cdots \supset G^{(d-1)} \supset G^{(d)} = \{1\}$ is the derived series of G. If P is contained in the abelian group $G^{(d-1)}$, then P is a proper normal subgroup of $G^{(d-1)}$ or $P = G^{(d-1)}$ is a proper normal subgroup of $G^{(d-2)}$, hence (4a) holds. Otherwise $G^{(d-1)}$ is cyclic and P is properly contained in $G^{(d-1)}P$. As the non-abelian semidirect product $Z_p \rtimes Z_3$ is not a subquotient of $G^{(d-1)}P$, the group $G^{(d-1)}P$ is abelian, and so (4a) holds. □

Corollary 11.11. *If none of (1), (3), (4a), or (5d) of Theorem 1.2 holds for a solvable group G, then all its odd order subquotients are cyclic, or $|G| = 2^\alpha 3^2$ and the Sylow 3-subgroup of G is isomorphic to $Z_3 \times Z_3$.*

Proof. Apply Propositions 11.3 and 11.10 for the maximal odd order Hall subgroup of G. □

Proposition 11.12. *Let G be a group of order $2^\alpha 3^2$ ($\alpha \geq 1$), with Sylow 3-subgroup $Z_3 \times Z_3$. Then (5a), (5b), (4a), or (4c) holds for G.*

Proof. Suppose that none of (5a), (5b), or (4a) hold for G. Denote by P the Sylow 3-subgroup of G and Q the Sylow 2-subgroup of G. Since P is self-normalizing by assumption, its index is congruent to 1 modulo 3 by Sylow's Theorem, hence $|Q| \neq 8$. We deduce by Proposition 11.1 that Q contains a cyclic subgroup of index 2. If $P \cap P^y = \{1\}$ for all $y \in G \setminus P$, then Q is normal in G, hence $G \cong Q \rtimes P$. Since P is not normal in G, this is a non-abelian semidirect product, and $G \cong A_4 \times Z_3$ by Proposition 11.8, hence (4c) holds. It remains to deal with the case when $P \cap P^y = \langle a \rangle$ for some $y \in G \setminus P$ and an order 3 element a of P. Denote by C the centralizer of a in G; the assumptions on G hold for C. Now $C/\langle a \rangle$ is not metacyclic since otherwise its Sylow 3-subgroup is normal in C by Lemma 2.6 in [33], hence P would be a proper normal subgroup in C. It follows by Proposition 11.9 that

$C/\langle a\rangle$ contains a subgroup $H/\langle a\rangle \cong A_4$ or $\tilde{A}_4$. The Sylow 2-subgroup S of H is characteristic in $S\langle a\rangle \triangleleft H$, hence S is normal in H. We conclude that $H \cong A_4 \times Z_3$ or $\tilde{A}_4 \times Z_3$. Thus (4c) holds for H and consequently for G. □

Proposition 11.13. *Let G be a solvable group properly containing its Sylow 2-subgroup $Z_2 \times Z_2 \times Z_2$, and suppose that all odd order subquotients of G are cyclic. Then one of (4b), (4c), (5b), (5c), (5f) holds for G.*

Proof. The condition on the Sylow 2-subgroup implies that G is not metacyclic. We may take a subnormal chain $G_1 \triangleleft G_2 \triangleleft G_3 \cdots \triangleleft G_s = G$ with cyclic factors, such that G_3 is not metacyclic, hence G_2 is non-cyclic. If $|G_3|$ is not divisible by 8, then the claim follows by Propositon 11.9. Otherwise if G_2 is a 2-group, then the Sylow 2-subgroup $Z_2 \times Z_2 \times Z_2$ of G_3 is a proper normal subgroup of G_3 or G_4, hence (4b) holds. Finally, suppose G_2 is not a 2-group. Proposition 11.5 applies for G_2, hence G_2 contains a cyclic subgroup of index 2. Denoting by K the maximal odd order characteristic subgroup of G_2, it is normal in G_3, so G_3 contains a semidirect product $K \rtimes Q$, with $Q \cong Z_2 \times Z_2 \times Z_2$. This is not a direct product. If the centralizer C of K in Q has at most 2 elements, then (5c) holds for G. If $C \cong Z_2 \times Z_2$, then it is a normal subgroup in KQ and KQ/C is a dihedral group, so (5b) holds for G. □

11.3. **Finite simple groups.**

Proposition 11.14. *At least one of (4a), (4b), (5d), (5e), (5g) holds for a finite non-abelian simple group.*

Proof. A *minimal simple group* is a non-abelian simple group all of whose proper subgroups are solvable (cf. [34]). It is shown in [1] that every non-abelian simple group contains a minimal simple group. Therefore it is sufficient to show our statement for minimal simple groups. According to Corollary 1 in [34], every minimal simple group is isomorphic to one of the following minimal simple groups:

(a) $L_2(2^p)$, p any prime.
(b) $L_2(3^p)$, p any odd prime.
(c) $L_2(p)$, $p > 3$ prime with $p^2 + 1 \equiv 0 \pmod 5$.
(d) $Sz(2^p)$, p any odd prime.
(e) $L_3(3)$.

The group $L_2(2^2)$ is isomorphic to the alternating group A_5. The group $L_2(2^p)$ contains as a subgroup the additive group of the field of 2^p elements. Hence when $p > 3$ then (4b) and (5a) hold inside the Sylow 2-subgroup, and if $p = 3$, then the Sylow 2-subgroup $Z_2 \times Z_2 \times Z_2$ is properly contained in its normalizer (a Borel subgroup). Similarly, $L_2(3^p)$ contains as a subgroup the additive group of the field of 3^p elements. The subgroup of unipotent upper triangular matrices in $L_3(3)$ is a non-abelian group of order 27, hence contains $Z_3 \times Z_3$ as a normal subgroup, see Subsection 11.1. The subgroup in $SL_2(p)$ consisting of the upper triangular matrices is isomorphic to the semidirect product $Z_p \rtimes Z_{p-1}$. Its image in $L_2(p)$ contains the non-abelian semidirect product $Z_p \rtimes Z_q$ for any odd prime divisor q of $p-1$. When p is a Fermat prime, then $L_2(p)$ contains $Z_p \rtimes Z_4$ (where Z_4 acts faithfully on Z_p), except for $p = 5$, but we need to consider only primes p with $p^2 + 1 \equiv 0 \pmod 5$. The Sylow 2-subgroup of $Sz(q)$ is a so-called Suzuki 2-group of order q^2, that is, a non-abelian 2-group with more than one involution, having a cyclic group of automorphisms which permutes its involutions transitively. It turns our that the involutions plus the identity constitute the center, the center has order q, see for example [17], [5]. It follows that the Sylow 2-subgroup Q of $Sz(2^p)$ (p an odd prime) properly contains an elementary abelian 2-group of rank p in its Sylow 2-subgroup. □

11.4. **Proof of Theorem 1.2.** For solvable groups the result follows from Propositions 11.5, 11.9, Corollaries 11.2, 11.11, Propositions 11.12, and 11.13.

Now suppose that G is not solvable. Then G contains subgroups N, H such that N is solvable and is normal in H, and the factor group H/N is non-abelian simple. If N is trivial then our statement is an immediate corollary of Proposition 11.14. If N is notrivial and one of (5d), (5e), (5g) holds for H/N then it holds for H and hence for G. If (4a) or (4b) holds for H/N, then take the inverse image C in H under the natural surjection $H \to H/N$ of the subgroup D containing $Z_3 \times Z_3$ or $Z_2 \times Z_2 \times Z_2$ as a proper normal subgroup. Obviously we may assume that D is solvable. Then one of (3), (4a), (4b), (4c), (5a), (5b), (5c), (5d), (5e), (5f) holds for C by the solvable case.

12. Proof of the main results

Proof of Theorem 1.1. To prove Theorem 1.1 it suffices to consider the cases listed in Theorem 1.2. The "if part" follows from case (1)-(2) and the "only if" part from case (2)-(3):

(1) $\gamma(Z_3 \times Z_3) = \frac{5}{9} > \frac{1}{2}$ and $\gamma(Z_2 \times Z_2 \times Z_2) = \frac{1}{2}$ by Proposition 3.3. The equalities $\gamma(A_4) = \frac{1}{2}$ and $\gamma(\tilde{A}_4) = \frac{1}{2}$ are given in Corollary 10.4.

(2) $\gamma(G) = 1$ if G is cyclic. If G contains a cyclic subgroup of index two, then $\beta(G) \geq \frac{|G|}{2} + 1$ by Theorem 4.3, hence $\gamma(G) > \frac{1}{2}$.

(3) $\gamma(Z_p \times Z_p) < 1/2$ for $p \geq 5$ by Proposition 3.3, hence $\gamma(G) < 1/2$ by Lemma 1.4 if $Z_p \times Z_p$ (with $p \geq 5$) is a subgroup of G.

(4) Suppose H is a subgroup of G which has index $k \geq 2$ in its normalizer $N := N_G(H)$; then $\gamma(G) \leq \gamma(N) \leq \gamma(H)$ by Lemma 1.4; moreover:

(a) if $H \cong Z_3 \times Z_3$ then by Proposition 3.1 and Lemma 2.5

$$\gamma(N) \leq \frac{1}{9k}\beta_k(Z_3 \times Z_3) = \frac{1}{3} + \frac{2}{9k} \leq \frac{4}{9}$$

(b) if $H \cong Z_2 \times Z_2 \times Z_2$ then by Proposition 3.2 and Lemma 2.5

$$\gamma(N) \leq \frac{1}{8k}\beta_k(Z_2 \times Z_2 \times Z_2) = \frac{1}{4} + \frac{3}{8k} \leq \frac{7}{16}$$

(c) if $H \cong A_4$ or $H \cong \tilde{A}_4$ then by Theorem 10.3 and Lemma 2.5

$$\gamma(N) \leq \frac{5k}{12k} = \frac{5}{12}$$

(5) For any subquotient K of G we have $\gamma(G) \leq \gamma(K)$ by Lemma 1.4;

(a) if $K/N \cong Z_2 \times Z_2$ for some normal subgroup $N \cong Z_2 \times Z_2$ then by Lemma 2.5 and Proposition 3.1:

$$\gamma(K) \leq \frac{1}{16}\beta_{\beta(Z_2 \times Z_2)}(Z_2 \times Z_2) = \frac{1}{16}\beta_3(Z_2 \times Z_2) = \frac{7}{16}$$

(b) if $K/N \cong D_{2p}$ for some normal subgroup $N \cong Z_2 \times Z_2$ then by Lemma 2.5 and Corollary 6.5:

$$\gamma(G) \leq \frac{1}{8p}(\beta_{\beta(D_{2p})}(Z_2 \times Z_2)) \leq \frac{2p+3}{8p} \leq \frac{3}{8}$$

(c) if $K \cong D_{2p} \times D_{2q}$ where p, q are distinct odd primes then by Lemma 2.5 and Corollary 6.5:

$$\gamma(G) \leq \frac{1}{4pq}(\beta_{\beta(D_{2q})}(D_{2p})) \leq \frac{p(q+1)+1}{4pq} \leq \frac{19}{60}$$

(d) if $K \cong Z_p \rtimes Z_q$ then $\gamma(K) < \frac{1}{2}$ by Theorem 9.6

(e) if $K \cong Z_p \rtimes Z_4$, where Z_4 acts faithfully, then by Proposition 7.4

$$\gamma(K) \leq \frac{3(p+1)}{8p} \leq \frac{9}{20}$$

(f) if $K \cong (Z_2 \times Z_2) \rtimes Z_9$ then $\gamma(K) \leq \frac{17}{36}$ by Proposition 10.6

(g) if $K \cong A_5$ then as $\mathrm{char}(\mathbb{F}) \nmid |A_5| = 60$ by assumption, $\mathrm{char}(\mathbb{F}) > 5$ hence Lemma 2.9 applies. Together with Theorem 10.3 this gives

$$\gamma(A_5) \leq \frac{1}{60}\beta_5(A_4) \leq \frac{5}{12} \quad (\text{resp. } \gamma(A_5) \leq \frac{11}{30} \text{ if } \mathrm{char}(\mathbb{F}) = 0)$$

□

Remark 12.1. In the above proof (5d) is the only point where we need the additional assumption that $\mathrm{char}(\mathbb{F}) \neq 2$ to deal with the group $Z_7 \rtimes Z_3$.

Proof of Corollary 1.3 . If G is a non-cyclic group with $\gamma(G) > \frac{1}{2}$, then either $G = Z_3 \times Z_3$ or by Theorem 1.1 it must be a group with a cyclic subgroup of index 2. Hence by the results summarized in Table 1. we have

$$\gamma(G) \leq \frac{1}{2} + \frac{2}{|G|} \to \frac{1}{2} \qquad \text{as } |G| \to \infty$$

Hence for any $\epsilon > 0$ there are only finitely many isomorphism types of groups such that $\gamma(G) \geq \frac{1}{2} + \epsilon$ and this was to be proved. □

References

[1] M. J. J. Barry and M. B. Ward, Simple groups contain minimal simple groups, Publicacions Matématiques 41 (1997), 411-415.

[2] D. J. Benson, Polynomial Invariants of Finite Groups, Cambridge University Press, 1993.

[3] K. Brown, Cohomology of Groups, Springer GTM 87, 1982.

[4] W. Burnside, Theory of Groups of Finite Order, Second edition, Cambridge University Press, 1911.

[5] M. J. Collins, The characterization of the Suzuki groups by their Sylow 2-subgroups, Math. Z. 123 (1971), 32-48.

[6] J. A. Dias da Silva and Y. O. Hamidoune, Cyclic spaces for Grassmann derivatives and additive theory, Bull. London Math. Soc. 26 (1994), 140-146.

[7] Ch. Delorme, O. Ordaz, and D. Quiroz, Some remarks on Davenport constant, Discrete Math. 237 (2001), 119-128.

[8] H. Derksen and G. Kemper, Computational Invariant Theory, Springer-Verlag, Berlin, 2002.

[9] M. Domokos and P. Hegedűs, Noether's bound for polynomial invariants of finite groups, Arch. Math. 74 (2000), 161-167.

[10] P. Fleischmann, The Noether bound in invariant theory of finite groups, Adv. Math. 156 (2000), 23-32.

[11] J. Fogarty, On Noether's bound for polynomial invariants of a finite group, Electron. Res. Announc. Amer. Math. Soc. 7 (2001), 5-7.
[12] M. Freeze and W. W. Smith, Sumsets of zerofree sequences, Arab J. Sci. Eng. Section C: Theme Issues 26 (2001), 97-105.
[13] W. Gao and A. Geroldinger, Zero-sum problems in finite abelian groups: A survey, Expo. Math. 24 (2006), 337-369.
[14] A. Geroldinger and F. Halter-Koch, Non-unique factorizations. Algebraic, combinatorial and analytic theory, Monographs and Textbooks in Pure and Applied Mathematics, Chapman & Hall/CRC, 2006.
[15] M. Göbel, Computing bases of permutation-invariant polynomials, J. Symbolic Computation 19 (1995), 285-291.
[16] F. Halter-Koch, A generalization of Davenport's constant and its arithmetical applications, Colloquium Mathematicum 63 (1992), 203-210.
[17] G. Higman, Suzuki 2-groups, Illinois J. Math. 7(1963), 79-95.
[18] W. C. Huffman, Polynomial invariants of finite linear groups of degree two, Canad. J. Math. 32 (1980), 317-330.
[19] B. Huppert, Endliche Gruppen I, Springer-Verlag, Berlin-Heidelberg-New York, 1967.
[20] 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, 2004.
[21] M. Neusel and L. Smith, Invariant theory of finite groups, AMS, 2001.
[22] E. Noether, Der Endlichkeitssatz der Invarianten endlicher Gruppen, Math. Ann. 77 (1916), 89-92.
[23] E. Noether, Der Endlichkeitssatz der Invarianten endlicher linearer Gruppen der Charakteristik p, Nachr. Ges. Wiss. Göttingen (1926), 28-36.
[24] J. E. Olson, A combinatorial problem on finite abelian groups I, J. Number Theory 1 (1969), 8-10.
[25] J. E. Olson, A combinatorial problem on finite abelian groups II, J. Number Theory 1 (1969), 195-199.
[26] Vivek M. Pawale, Invariants of semidirect products of cyclic groups, Ph.D. Thesis, Brandeis University, 1999.
[27] V. L. Popov and E. B. Vinberg, Invariant theory, in: Algebraic Geometry IV, Encyclopaedia of Mathematical Sciences 55, Springer-Verlag, Berlin, Heidelberg, 1994.
[28] D. R. Richman, Invariants of finite groups over fields of characteristic p, Adv. Math. 124 (1996), 25-48.
[29] P. Roquette, Realisierung von Darstellungen endlicher nilpotenten Gruppen, Arch. Math. 9 (1958), 241-250.
[30] B. J. Schmid, Finite groups and invariant theory, "Topics in Invariant Theory", Lect. Notes in Math. 1478 (1991), 35-66.
[31] J.P. Serre, Represésentations linéaires des groupes finis, Hermann, Paris 1998
[32] M. Sezer, Sharpening the generalized Noether bound in the invariant theory of finite groups, J. Algebra 254 (2002), 252-263.
[33] H.-S. Sim, Metacyclic groups of odd order, Proc. London Math. Soc. (3) 69 (1994), 47-71.
[34] J. G. Thompson, Nonsolvable finite groups all of whose local subgroups are solvable, Bull. Amer. Math. Soc. 74 (1968), 383-437.
[35] H. Weyl, The Classical Groups, Princeton University Press, Princeton, 1939.

Central European University, Department of Mathematics, Nádor u. 9, 1051 Budapest, Hungary
E-mail address: `cziszter_kalman-sandor@ceu-budapest.edu`

Rényi Institute of Mathematics, Hungarian Academy of Sciences, Reáltanoda u. 13-15, 1053 Budapest, Hungary
E-mail address: `domokos@renyi.hu`