ANNALES

DE

L'INSTITUT FOURIER

Kálmán CZISZTER & Mátyás DOMOKOS

Groups with large Noether bound

Tome 64, n° 3 (2014), p. 909-944.

<http://aif.cedram.org/item?id=AIF_2014__64_3_909_0>

Ann. Inst. Fourier, Grenoble
64, 3 (2014) 909-944

GROUPS WITH LARGE NOETHER BOUND

by Kálmán CZISZTER & Mátyás DOMOKOS (*)

Abstract. — The finite groups having an indecomposable polynomial invariant of degree at least half the order of the group are classified. It turns out that –apart from four sporadic exceptions– these are exactly the groups with a cyclic subgroup of index at most two.

Résumé. — Nous classifions les groupes finis ayant un invariant polynômial indécomposable de degré au moins la moitié de l'ordre du groupe. Il est démontré qu'en exceptant quatre groupes particuliers, ce sont exactement les groupes avec un sous-groupe cyclique d'indice au plus deux.

1. Introduction

1.1. Outline of the main results

Let G be a finite group and V a G-module of finite dimension over a field $\mathbb{F}$. By a classical theorem of E. Noether [31] the *algebra of polynomial invariants* on V, denoted by $\mathbb{F}[V]^G$, is finitely generated. 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 famous theorem on the *Noether bound* asserts that

$$\beta(G) \leqslant |G| \tag{1.1}$$

provided that $\mathrm{char}(\mathbb{F})$ does not divide the order of G (see Noether [30] in characteristic 0 and Fleischmann [16], Fogarty [17] in positive characteristic). Schmid proved in [36] that over the field of complex numbers

Keywords: Noether bound, polynomial invariant, zero-sum sequence.
Math. classification: 13A50, 11B50.
(*) The paper is based on results from the PhD thesis of the first author written at the Central European University.
Partially supported by OTKA NK81203 and K101515.

$\beta(G) = |G|$ holds only when G is cyclic. This was sharpened by Domokos and Hegedűs in [14] by proving that $\beta(G) \leqslant \frac{3}{4}|G|$ for all non-cyclic G; the result was extended to non-modular positive characteristic by Sezer [38]. The constant $3/4$ is optimal here. On the other hand, a straightforward lower bound on $\beta(G)$ can be obtained based on the result of Schmid in [36], that $\beta(G) \geqslant \beta(H)$ holds for all subgroups H of G. In particular, $\beta(G)$ is bounded from below by the maximal order of the elements in G. Therefore $\beta(G) \geqslant \frac{1}{2}|G|$ 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 article is that –apart from four sporadic exceptions– these are the only groups for which the ratio of the Noether number and the group order is so large:

THEOREM 1.1. — *For a finite group G with order not divisible by* $\mathrm{char}(\mathbb{F})$ *we have $\beta(G) \geqslant \frac{1}{2}|G|$ if and only if G has a cyclic subgroup of index at most two, 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 $\mathbb{F} = \mathbb{C}$. The main technical tool of its proof is a generalization of the Noether number which allows us to formulate some reduction lemmata in Section 1.3 that can be used to infer estimates on the Noether number of a group from the knowledge of the (generalized) Noether number of its subgroups and homomorphic images. Theorem 4.1 then isolates a list of some groups such that an arbitrary finite group G must contain one of them as a subgroup or a subquotient, unless G contains a cyclic subgroup of index at most two. Finally, the proof is made complete in Sections 2–3, where we compute or estimate the (generalized) Noether number for the particular groups on this list.

The quest for degree bounds has always been in the focus of invariant theory. A practical motivation is that good initial degree bounds may potentially decrease the running time of algorithms to compute generators of invariant rings. On the other hand, the exact value of the Noether bound is known only for very few groups. To indicate the difficulties we mention the paper of Dixmier [13], investigating the Noether number for irreducible representations of the symmetric group of degree 5. It can be seen in the present paper as well that the discussion of some small groups, the estimation of the Noether bound takes relatively large space (especially where the exact value is found).

We finish the introduction by noting that the constant $1/2$ in Theorem 1.1 has a remarkable theoretical status. In a parallel paper [9] we determine the (generalized) Noether number for each non-cyclic group G with

a cyclic subgroup of index 2: it turns out that for such a G we have $\beta(G) - \frac{1}{2}|G| \in \{1, 2\}$. Consequently, for any $c > 1/2$, up to isomorphism there are only finitely many non-cyclic groups G with $\beta(G)/|G| > c$, whereas there are infinitely many isomorphism classes of non-cyclic groups G with $\beta(G)/|G| > 1/2$. In particular, the set $\{\beta(G)/|G| : G \text{ finite group}\} \subset \mathbb{Q}$ has no limit point strictly between $1/2$ and 1.

1.2. The Noether number and its generalization

Throughout this article $\mathbb{F}$ is a fixed algebraically closed base field and G is a finite group of order not divisible by $\mathrm{char}(\mathbb{F})$, unless explicitly stated otherwise.

By a *graded module* we mean an $\mathbb{N}$-graded $\mathbb{F}$-vector space $M = \bigoplus_{d=0}^{\infty} M_d$, which is a graded module over a commutative $\mathbb{N}$-graded $\mathbb{F}$-algebra $R = \bigoplus_{d=0}^{\infty} R_d$ such that $R_0 = \mathbb{F}$ is the base field when R is unital, or $R_0 = \{0\}$ otherwise (in the latter case we still assume that the multiplication map is $\mathbb{F}$-bilinear). We set $M_{\geqslant s} := \bigoplus_{d \geqslant s} M_d$, $M_{\leqslant s} := \bigoplus_{d=0}^{s} M_d$, and $M_{>s} := \bigoplus_{d>s} M_d$. We also use the notation $M_+ := M_{\geqslant 1}$, so if we regard R as a module over itself, its maximal homogeneous ideal is R_+. If M is generated as an R-module in bounded degree then set

$$\beta(M, R) := \min\{s \in \mathbb{N} : M \text{ is generated as an } R\text{-module by } M_{\leqslant s}\}$$

and write $\beta(M, R) = \infty$ otherwise. By the graded Nakayama Lemma, a module M is generated by its homogeneous elements $\{m_\lambda \mid \lambda \in \Lambda\}$ if and only if the $\mathbb{F}$-vector space M/R_+M is spanned by the images $\{\overline{m}_\lambda \mid \lambda \in \Lambda\}$. As a consequence, $\beta(M, R)$ is the top degree of the factor space M/R_+M, inheriting the grading from M. Here by the top degree of an $\mathbb{N}$-graded vector space we mean the supremum of the degrees of non-zero homogeneous components (for the zero space the top degree is defined to be zero). Obviously we have $\beta(M, R) = \beta(M, R_+)$.

The subalgebra of R generated by $R_{\leqslant s}$ will be denoted by $\mathbb{F}[R_{\leqslant s}]$. For subspaces S, T of an $\mathbb{F}$-algebra L we write ST for the subspace spanned by the products $\{st \mid s \in S, t \in T\}$, and use the notation $S^k := S \dots S$ (k factors) accordingly.

We set $\beta(R) := \beta(R_+, R)$. It is zero if $R = R_0$ and otherwise it is the supremum of the degrees of homogeneous elements in $R_+ \setminus R_+^2$. In other words, $\beta(R)$ is the minimal n such that R is generated as an $\mathbb{F}$-algebra by homogeneous elements of degree at most n when R is generated in bounded degree, and $\beta(R) = \infty$ when R is not generated in bounded degree.

Let us apply the above concepts in the more particular setting of invariant theory. Here we are given a group G and a finite dimensional $\mathbb{F}$-vector space V equipped with a group homomorphism $G \to \mathrm{GL}(V)$; in this situation we also say that V is a (left) G-module. As an affine space, V has a coordinate ring $\mathbb{F}[V]$ which is defined in abstract terms as the symmetric tensor algebra of the dual space V^*. Thus $\mathbb{F}[V]$ is isomorphic to a polynomial ring in $\dim(V)$ variables, so in particular it is a graded ring and $\mathbb{F}[V]_1 \cong V^*$. The left action of G on V induces a right action on V^* given as $x^g(v) = x(gv)$ for any $g \in G, v \in V$ and $x \in V^*$. This right action of G on V^* extends multiplicatively onto the whole $\mathbb{F}[V]$. Our basic object of study is the *ring of polynomial invariants* defined as

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

$\beta(G,V) := \beta(\mathbb{F}[V]^G)$ is called the *Noether number* of the G-module V.

By a classic result of Hilbert in [24] $\beta(G,V)$ is finite if G is *linearly reductive*. When G is finite even more can be said. The *global degree bound* for a finite group G is defined as

$$\beta(G) := \sup_V \beta(G,V)$$

where V runs through all G-modules over the field $\mathbb{F}$. By Noether's degree bound (1.1), if $|G|$ is not divisible by $\mathrm{char}(\mathbb{F})$ then $\beta(G)$ is finite. The converse of this statement is also true: it was proved in [12] for $\mathrm{char}(\mathbb{F}) = 0$ and subsequently in [4] for the whole non-modular case that the finiteness of $\beta(G)$ implies the finiteness of the group G, as well. As for the modular case, i.e. when $\mathrm{char}(\mathbb{F})$ divides $|G|$, Richman constructed in [34] a sequence of G-modules $V_1, V_2, \ldots$ such that $\beta(G,V_i) \to \infty$ as $i \to \infty$, so in this case $\beta(G)$ is not finite.

Note that we suppressed $\mathbb{F}$ from the notation $\beta(G)$. The dependence of $\beta(G)$ on the field $\mathbb{F}$ was studied by Knop in [28]. He proved that $\beta(G)$ is the same for every field $\mathbb{F}$ with the same characteristic. In particular this implies that $\beta(G)$ is the same for $\mathbb{F}$ and its algebraic closure. So our running assumption that $\mathbb{F}$ is algebraically closed causes no loss of generality in the results.

Now let us summarize the previously known reduction lemmata by means of which $\beta(G)$ can be bounded through induction on the structure of G:

LEMMA 1.2. — *We have $\beta(G)/|G| \leqslant \beta(K)/|K|$ for any subquotient K of G.*

Proof. — For any subgroup $H \leqslant G$, resp. for any normal subgroup $N \triangleleft G$ the following reduction lemmata hold:

$$\beta(G) \leqslant [G : H]\beta(H); \tag{1.2}$$

$$\beta(G) \leqslant \beta(G/N)\beta(N). \tag{1.3}$$

These were proved for characteristic 0 by Schmid (see Lemma 3.2 and 3.1 in [36]) and subsequently extended to the case when $\mathrm{char}(\mathbb{F}) \nmid |G|$ in [38], [15], [28]. Our claim follows after dividing by $|G|$ the above inequalities and using that $\beta(N)/|N| \leqslant 1$ by (1.1). □

We will introduce here a generalization of the Noether number with the intent of improving and generalizing Schmid's reduction lemmata above: For a graded R-module M and an integer $k \geqslant 1$ set

$$\beta_k(M, R) := \beta(M, R_+^k).$$

Note that $\beta_1(M, R) = \beta(M, R)$. The abbreviation $\beta_k(R) := \beta_k(R_+, R)$ will also be used. For a representation V of a finite group G over the field $\mathbb{F}$ we set $\beta_k(G, V) := \beta_k(\mathbb{F}[V]^G)$. The trivial bound $\beta_k(G, V) \leqslant k\beta(G, V)$ shows that this quantity is finite. We also set

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

suppressing $\mathbb{F}$ from the notation as in the case of $\beta(G)$. We shall refer to these numbers as the *generalized Noether numbers* of the group G.

1.3. Reduction lemmata

Our starting point is the following alternative characterization of the generalized Noether number:

PROPOSITION 1.3. — *$\beta_k(G)$ is the minimal positive integer d having the property that 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. Take a finite dimensional G-submodule $W \subset L_+$ generating L as an $\mathbb{F}$-algebra, and set $V := W^*$. Then the $\mathbb{F}$-algebra surjection $\pi : \mathbb{F}[V] \to L$ extending the canonical isomorphism $\mathbb{F}[V]_1 = W^{**} \cong W \subset L$ is G-equivariant and

maps $\mathbb{F}[V]_+$ onto L_+. Moreover, π restricts to a surjection $\mathbb{F}[V]_+^G \to L_+^G$ by the assumption $\mathrm{char}(\mathbb{F}) \nmid |G|$. So we have

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

For the reverse inequality let $L := \mathbb{F}[V]$, where V is a finite dimensional G-module with $\beta_k(G,V) = \beta_k(G)$. □

Lemma 1.4. — *Let N be a normal subgroup of G. Then for any G-module V we have*

$$\beta_k(G,V) \leqslant \beta_{\beta_k(G/N)}(N,V)$$

Consequently the inequality $\beta_k(G) \leqslant \beta_{\beta_k(G/N)}(N)$ holds, as well.

Proof. — We shall apply Proposition 1.3 for the algebra $L := \mathbb{F}[V]^N$; denote $R := \mathbb{F}[V]^G$. 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 $s := \beta_{\beta_k(G/N)}(N,V)$, we have

$$R_{\geqslant s+1} = R \cap L_{\geqslant s+1} \subseteq L^{G/N} \cap L_+^{\beta_k(G/N)+1} \subseteq (L_+^{G/N})^{k+1} = (R_+)^{k+1}. \square$$

A weaker version of Lemma 1.4 remains true for any subgroup $H \leqslant G$ which is not necessarily normal. To show this we will make use of the following relativized version of the Reynolds operator (see e.g. [29] p. 33): Let $H \leqslant G$ be a subgroup and $g_1, ..., g_n$ a system of right coset representatives of H. For a G-module V the map $\tau_H^G : \mathbb{F}[V]^H \to \mathbb{F}[V]^G$ called the *relative transfer map* is defined by the sum

$$\tau_H^G(u) = \sum_{i=1}^{n} u^{g_i}.$$

In the special case when H is the trivial subgroup $\{1_G\}$, we recover the *transfer map* $\tau^G : \mathbb{F}[V] \to \mathbb{F}[V]^G$. If $\mathrm{char}(\mathbb{F})$ does not divide $[G:H]$ then τ_H^G is a graded $\mathbb{F}[V]^G$-module epimorphism from $\mathbb{F}[V]^H$ onto $\mathbb{F}[V]^G$. We shall use this fact most frequently in the following form:

Proposition 1.5. — *If $\mathrm{char}(\mathbb{F})$ does not divide $[G:H]$, then we have $\beta_k(G,V) \leqslant \beta_k(\mathbb{F}[V]_+^H, \mathbb{F}[V]^G)$.*

Proposition 1.6. — *Let J be a non-unitary commutative $\mathbb{F}$-algebra on which a finite group G acts via $\mathbb{F}$-algebra automorphisms and let $H \leqslant G$ be a subgroup for which one of the following conditions holds:*

(i) $\mathrm{char}(\mathbb{F}) > [G:H]$ *or* $\mathrm{char}(\mathbb{F}) = 0$;
(ii) *H is normal in G and* $\mathrm{char}(\mathbb{F})$ *does not divide* $[G:H]$;
(iii) $\mathrm{char}(\mathbb{F})$ *does not divide* $|G|$.

Then we have

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

Proof. — (i) Let $f \in J^H$ be arbitrary and $\mathcal{S}$ a system of right H-coset representatives in G. Then f is a root of the monic polynomial $\prod_{g\in\mathcal{S}}(t - f^g) \in J[t]$. 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 [1]), hence $f_1 \cdots f_r \in J^H J^G + J^G$.

(ii) (This is a variant of a result of Knop, Theorem 2.1 in [28]; the idea appears in Benson's simplification of Fogarty's argument from [17], see Lemma 3.8.1 in [11]). Let $\mathcal{S}$ be a system of H-coset representatives in G. For each $x \in \mathcal{S}$ choose an arbitrary element $a_x \in J^H$. It is easily checked that

$$0 = \sum_{y\in\mathcal{S}} \prod_{x\in\mathcal{S}} (a_x - a_x^{x^{-1}y}) = \sum_{U\subseteq\mathcal{S}} (-1)^{|U|}\delta_U \qquad \text{where} \tag{1.4}$$

$$\delta_U := \prod_{x\notin U} a_x \sum_{y\in\mathcal{S}} (\prod_{x\in U} a_x^{x^{-1}})^y.$$

Note that $a_x^g \in J^H$ for all $x \in \mathcal{S}$ and $g \in G$ by normality of H in G. Therefore $\delta_U = \prod_{x\notin U} a_x \; \tau_H^G\left(\prod_{x\in U} a_x^{x^{-1}}\right)$. Thus $\delta_{\mathcal{S}} \in J^G$ and $\delta_U \in J^H J^G$ for every $U \subsetneq \mathcal{S}$, except for $U = \emptyset$, when we get the term $[G : H] \prod_{x\in\mathcal{S}} a_x$. Given that $[G : H] \in \mathbb{F}^\times$ and the elements a_x were arbitrary the claim follows.

(iii) Let $\mathcal{S}$ be a system of left H-coset representatives in G. Apply the transfer map $\tau^H : J \to J^H$ to the equality (1.4), and observe that

$$\tau^H(\delta_U) = \prod_{x\notin U} a_x \sum_{h\in H} \sum_{y\in\mathcal{S}} (\prod_{x\in U} a_x^{x^{-1}})^{yh} = \prod_{x\notin U} a_x \tau^G(\prod_{x\in U} a_x^{x^{-1}}). \tag{1.5}$$

This shows that $\tau^H(\delta_U) \in J^H J^G + J^G$ for all non-empty subsets $U \subseteq \mathcal{S}$, and $\tau^H(\delta_\emptyset) = |G| \prod_{x\in\mathcal{S}} a_x$, implying the claim as in (ii). □

Remark 1.7. — Finiteness of G can be replaced by finiteness of $[G : H]$ in (i) and (ii) above.

Corollary 1.8. — *Keeping the assumptions of Proposition 1.6 on G, H and* $\mathrm{char}(\mathbb{F})$*, let V be a G-module, $I := \mathbb{F}[V]^H$, $R := \mathbb{F}[V]^G$. Then for any graded I-module M we have*

$$\beta_k(M, R) \leqslant \beta_{k[G:H]}(M, I). \tag{1.6}$$

In particular we have the inequality

$$\beta_k(G,V) \leqslant \beta_{k[G:H]}(H,V). \tag{1.7}$$

Proof. — Apply Proposition 1.6 for $J := \mathbb{F}[V]_+$. Then $J^H = I_+$ and $J^G = R_+$, so $I_+^{[G:H]} \subseteq I_+R_+ + R_+$. Consequently $(I_+^{[G:H]})^k \subseteq I_+R_+^k + R_+^k$, hence $MI_+^{k[G:H]} \subseteq MR_+^k$. Thus the top degree of the factor space M/MR_+^k is bounded by the top degree of $M/MI_+^{k[G:H]}$, implying the first inequality. For the second note that $\beta_k(G,V) = \beta_k(R) \leqslant \beta_k(I_+,R)$ by Proposition 1.5 and $\beta_k(I_+,R) \leqslant \beta_{k[G:H]}(I_+,I) = \beta_{k[G:H]}(H,V)$. □

Remark 1.9. — It is conjectured that $\beta(G,V) \leqslant [G:H]\beta(H,V)$ holds in fact whenever $\mathrm{char}(\mathbb{F}) \nmid [G:H]$. This open question is mentioned under the name "baby Noether gap" in Remark 3.8.5 (b) in [11] or on page 1222 in [27].

Finally we present some rather technical results which will be used later in Chapter 2 to obtain upper bounds on $\beta(G)$:

Lemma 1.10. — *Let M be a graded module over a graded ring I, and $S \subseteq I$ a graded subalgebra. Then for any integers $k > r \geqslant 1$ we have*

$$\beta_k(M,I) \leqslant \max\{\beta(M,S) + \beta_{k-r-1}(S), \beta_r(M,I) + \beta_{k-r}(S)\}$$

Proof. — Assume that $d \in \mathbb{N}$ is greater than the right hand side of this inequality. Then

$$M_d \subseteq M_{\leqslant \beta(M,S)} S_{>\beta_{k-r-1}(S)} \subseteq MS_+^{k-r}. \tag{1.8}$$

Note that for any positive integer j the top degree of S_+^j/S_+^{j+1} is trivially bounded by the top degree of the larger space S_+/S_+^{j+1}. In other words $\beta(S_+^j,S) \leqslant \beta(S_+,S_+^j) = \beta_j(S)$, thus $MS_+^j \subseteq M(S_+^j)_{\leqslant \beta_j(S)}$. It follows that

$$MS_+^{k-r} = M(S_+^{k-r})_{\leqslant \beta_{k-r}(S)}. \tag{1.9}$$

Combining (1.8), (1.9) with the assumption $d > \beta_r(M,I) + \beta_{k-r}(S)$ we get

$$M_d \subseteq M_{>\beta_r(M,I)} S_+^{k-r} \subseteq MI_+^r S_+^{k-r} \subseteq MI_+^k.$$

This proves that $d > \beta_k(M,I)$. □

Lemma 1.11. — *For a G-module V and subgroup $H \leqslant G$ as in Proposition 1.6 set $L := \mathbb{F}[V]$, $M := L_+/L_+^G L_+$. For any $1 \leqslant r < [G:H]$ and $s \geqslant 1$ we have*

$$\beta(L_+,L^G) \leqslant ([G:H]-r)s + \max\{\beta_r(M,L^H), \beta(M,\mathbb{F}[L^H_{\leqslant s}]) - s\}$$

Proof. — We have $\beta(L_+, L^G) = \beta(M, L^G) \leqslant \beta_{[G:H]}(M, L^H)$ by Corollary 1.8. Applying Lemma 1.10 with $k := [G : H]$, $I := L^H$, $S := \mathbb{F}[I_{\leqslant s}]$ and noting that $\beta_k(S) \leqslant ks$ we obtain the above inequality. □

Remark 1.12. — (i) A version of Lemma 1.11 limited to the abelian case appears in [19] as Lemma 6.1.3.

(ii) The use of Lemma 1.4 and Corollary 1.8 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 it can be seen in Section 1.4 already for abelian groups. See also [8] for more information in this respect.

1.4. The Davenport constant

A *character* of an abelian group A is a group homomorphism from A to the multiplicative group $\mathbb{F}^\times$ of the base field. The set of characters of A is denoted by $\hat{A}$; it is naturally an abelian group, and in fact there is a (non-canonical) isomorphism $\hat{A} \cong A$. Let V be a representation of A over the base field $\mathbb{F}$. Since $\mathbb{F}$ is algebraically closed and $\mathrm{char}(\mathbb{F})$ does not divide $|A|$ by our conventions, V decomposes as a direct sum of 1-dimensional representations. This means that V^* has an A-eigenbasis $\{x_1, ..., x_n\}$. The character $\theta_i \in \hat{A}$ given by $x_i^a = \theta_i(a)x_i$ is called the *weight* of x_i. We shall always tacitly choose such an 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 $\mathcal{M}(\hat{A})$ the free commutative monoid generated by the elements of $\hat{A}$. Due to our choice of variables in $\mathbb{F}[V]$ we can define a monoid homomorphism $\Phi : M(V) \to \mathcal{M}(\hat{A})$ by sending each variable x_i to its weight θ_i. We shall call $\Phi(m)$ the *weight sequence* of the monomial $m \in M(V)$. We prefer to write $\hat{A}$ additively, hence for any character $\chi \in \hat{A}$ we denote by $-\chi$ the character $a \mapsto \chi(a)^{-1}$, $a \in A$.

An element $S \in \mathcal{M}(\hat{A})$ can be interpreted as a *sequence* $S := (s_1, \ldots, s_n)$ of elements of $\hat{A}$ 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 $J \subseteq \{1, \ldots, n\}$. 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 $S = (s_1, \ldots, s_n)$ we write S^b for the sequence $(s_1^b, \ldots, s_n^b)$,

and we say that the sequences S and T are *similar* if $T = S^b$ for some $b \in \mathrm{Aut}(A)$.

Let $\sigma : \mathcal{M}(\hat{A}) \to \hat{A}$ be the monoid homomorphism which assigns to each sequence over A the sum of its elements. The value $\sigma(\Phi(m)) \in \hat{A}$ is called the *weight of the monomial* $m \in M(V)$ and it will be abbreviated by $\theta(m)$. In particular, $\theta(x_i) = \theta_i$ with the notation in the first paragraph of this section. The kernel of σ is called the *block monoid* of $\hat{A}$, denoted by $\mathcal{B}(\hat{A})$, 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 over $\hat{A}$. 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 $\mathcal{B}(\hat{A})$. 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 [18]. As it is seen from our discussion:

$$\mathsf{D}(A) = \beta(A). \tag{1.10}$$

The *generalized Davenport constant* $\mathsf{D}_k(A)$ is introduced in [22] as the length of the longest zero-sum sequence that cannot be factored into more than k non-empty zero-sum sequences. It is evident from the above discussion that $\mathsf{D}_k(A) = \beta_k(A)$. Moreover Lemma 1.4 applied to abelian groups yields for any subgroup $B \leqslant A$ that:

$$\mathsf{D}_k(A) \leqslant \mathsf{D}_{\mathsf{D}_k(A/B)}(B); \tag{1.11}$$

$$\mathsf{D}_k(A) \leqslant \mathsf{D}_{\mathsf{D}_k(B)}(A/B). \tag{1.12}$$

The second inequality follows from the first because A has a subgroup $C \cong A/B$ for which $A/C \cong B$, hence the role of A/B and B can be reversed in this formula. This inequality appears as Proposition 2.6 in [10].

For the cyclic group Z_n we have $\mathsf{D}_k(Z_n) = kn$. We close this section with two more results on D_k which will be used later on.

Proposition 1.13 (Halter-Koch, [22] Proposition 5). — *For any $n \mid m$ we have*

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

PROPOSITION 1.14 (Delorme-Ordaz-Quiroz, [10] Lemma 3.7). —

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

2. The semidirect product

Our main aim in the present chapter is to give upper bounds on $\beta(Z_p \rtimes Z_q)$ for the non-abelian semidirect product $Z_p \rtimes Z_q$, where p, q are odd primes, $q \mid p-1$. It is an open conjecture of Pawale reported in [41] that $\beta(Z_p \rtimes Z_q) = p+q-1$. The lower bound $\beta(Z_p \rtimes Z_q) \geqslant p+q-1$ follows from a more general result in [9] (and can also be seen directly). We provide here upper bounds that improve on [14] and [32], and are sufficient for the proof of Theorem 1.1.

2.1. Extending Goebel's algorithm

Let G be a finite group with a proper abelian normal subgroup A. Consider a monomial representation $G \to \mathrm{GL}(V)$ which maps A to diagonal matrices. This presupposes the choice of a basis $x_1, ..., x_n$ in the dual space V^*, which are A-eigenvectors permuted up to scalars under the action of G/A. We shall always tacitly choose them as the variables in the coordinate ring $L := \mathbb{F}[V]$. Goebel developed an algorithm for the case when V is a permutation representation (see [20], [29], [11]) which we will adapt here to this more general case.

The conjugation action of G on A induces an action on $\hat{A}$ in the standard way, and we consider the corresponding action of G on $\mathcal{M}(\hat{A})$. Extending slightly the notation of Section 1.4 we define the weight sequence and the weight for any non-zero scalar multiple of a monomial: for $m \in M(V)$ and $c \in \mathbb{F}^\times$ set $\Phi(cm) := \Phi(m)$ and $\theta(cm) := \theta(m)$. It is easy to check that for any monomial $m \in M(V)$ and $g \in G$ we have $\Phi(m^g) = \Phi(m)^g$ and consequently $\theta(m^g) = \theta(m)^g$. Enumerate the G-orbits in $\hat{A}$ in a fixed order $O_1, \ldots, O_l$. For a G-orbit O in $\hat{A}$ let S^O be the subsequence of S consisting of its elements belonging to O. Now S has the canonic factorization $S = S^{O_1} \ldots S^{O_l}$. In addition any sequence S over $\hat{A}$ has a unique factorization $S = R_1 R_2 ... R_h$ such that each $R_i \subseteq \hat{A}$ is multiplicity-free and $R_1 \supseteq ... \supseteq R_h$; we call this the *row decomposition* of S and we refer to R_i as the ith *row* of S, whereas $\mathrm{supp}(S) := R_1$ is its *support* and $h(S) := h$ is its *height*.

In other terms $h(S)$ is the maximal multiplicity of the elements in S. The intuition behind this is that we like to think of sequences as Young diagrams where the multiplicities in S of the different elements of $\hat{A}$ are represented by the heights of the columns. Denote by $\mu(S)$ the non-increasing sequence of integers $(\mu_1(S), \dots, \mu_h(S)) := (|R_1|, ..., |R_h|)$. By the *shape* $\lambda(S)$ of S we mean the l-tuple of such partitions

$$\lambda(S) := (\mu(S^{O_1}), \dots, \mu(S^{O_l})).$$

The set of the shapes is equipped with the usual reverse lexicographic order, i.e. $\lambda(S) \prec \lambda(T)$ if $\lambda(S) \neq \lambda(T)$ and for the smallest index i such that $\mu(S^{O_i}) \neq \mu(T^{O_i})$, we have $\mu_j(S^{O_i}) > \mu_j(T^{O_i})$ for the smallest index j with $\mu_j(S^{O_i}) \neq \mu_j(T^{O_i})$. Observe that $\lambda(ST) \prec \lambda(S)$ always holds but on the other hand $\lambda(S) \prec \lambda(S')$ does not imply $\lambda(ST) \prec \lambda(S'T)$. Abusing notation for any monomial $m \in \mathbb{F}[V]$ we write $\lambda(m)$, $h(m)$ and $\mathrm{supp}(m)$ for the shape, height and the support of its weight sequence $\Phi(m)$.

In the following we shall assume that we fixed a subset $\mathcal{V}$ of the variables permuted by G up to non-zero scalar multiples; we adopt the convention that unless explicitly stated otherwise, $\mathcal{V}$ is the set of all variables. Any monomial m factors as $m = m_{\mathcal{V}} m_{\widehat{\mathcal{V}}}$, where $m_{\mathcal{V}}$ is a product of variables belonging to $\mathcal{V}$, and $m_{\widehat{\mathcal{V}}}$ does not involve variables from $\mathcal{V}$. We shall also use the notation $\lambda_{\mathcal{V}}(m) := \lambda(m_{\mathcal{V}})$.

Definition 2.1. — *An A-invariant monomial u is a* good factor *of a monomial $m = uv$ if $\lambda_{\mathcal{V}}(u^b v) \prec \lambda_{\mathcal{V}}(m)$ holds for all $b \in G \setminus A$; note that this forces $0 < \deg(u) < \deg(m)$. We say that m is* terminal *if it has no good factor.*

Lemma 2.2. — *$L_+ = \mathbb{F}[V]_+$ is generated as an L^G-module by the terminal monomials.*

Proof. — We prove by induction on $\lambda_{\mathcal{V}}(m)$ with respect to $\prec$ that if m is not terminal, then it can be expressed modulo $L_+ L_+^G$ as a linear combination of terminal monomials. Indeed, take a good factor u of $m = uv$. Then we have

$$\sum_{b \in G/A} u^b v = \tau_A^G(u) v \in L_+^G L_+. \tag{2.1}$$

Since for every monomial in the sum on the left hand side except for m we have $\lambda_{\mathcal{V}}(u^b v) \prec \lambda_{\mathcal{V}}(m)$, our claim on m holds by the induction hypothesis. □

At this level of generality there might be an element $b \in G \setminus A$ such that $\theta(x_i^b) = \theta(x_i)$ for every variable x_i, and then every monomial qualifies as

terminal by our definition. The concept of terminality is particularly useful when

$$\chi^b \neq \chi \quad \text{for each} \quad b \in G \setminus A \quad \text{and} \quad \chi \in \hat{A} \setminus \{0\}. \tag{2.2}$$

For the rest of this section we assume that (2.2) holds for (G, A). An obvious necessary condition for (2.2) to hold is that A must be a self-centralizing, hence maximal abelian subgroup in G, and the order of G/A must divide $|A| - 1$, hence G is the semidirect product of A and G/A by the Schur-Zassenhaus theorem. In fact condition (2.2) is equivalent to the requirement that G is a Frobenius group with abelian Frobenius kernel A. In this article we will only study in greater detail the non-abelian semidirect products $Z_p \rtimes Z_q$, $Z_p \rtimes Z_{q^n}$ where Z_{q^n} acts faithfully on Z_p, and the alternating group A_4.

Note that if (2.2) holds, then for any non-trivial 1-dimensional A-module U the G-module $\mathrm{Ind}_A^G(U)$ is irreducible by Mackey's irreducibility criterion (cf. [37] ch. 7.4). Moreover, the set of A-characters occurring in $\mathrm{Ind}_A^G(U)$ coincides with the G/A-orbit of the character of A on U, and each A-character occurring in $\mathrm{Ind}_A^G(U)$ has multiplicity one. Hence the G/A-orbits in $\hat{A} \setminus \{0\}$ are in bijection with the isomorphism classes of those irreducible G-modules that are induced from a 1-dimensional A-module.

Definition 2.3. — *A monomial $m \in \mathbb{F}[V]$ or its weight sequence $S = \Phi(m)$ is called a* brick *if S is the orbit of a minimal non-trivial subgroup of G/A.*

Remark 2.4. — (i) If (2.2) holds then every brick is A-invariant. Indeed, when $m \in \mathbb{F}[V]$ is a brick then $\Phi(m)$ is stabilized by some non-identity element $b \in G/A$, hence $\theta(m)$ is fixed by b, which is only possible by (2.2) if $\theta(m) = 0$.

(ii) If a monomial m is not divisible by a brick, then $\Phi(m) \neq \Phi(m^b)$ for each $b \in G \setminus A$.

Definition 2.5. — *A sequence S over $\hat{A}$ with row-decomposition $S = R_1 ... R_h$ is called* gapless *if for all G/A-orbits O and all $i < h$ such that $R_i \cap O \neq \emptyset$ we have $R_i \cap O \neq R_{i+1} \cap O$ or $R_i \cap O = R_{i+1} \cap O = O$. A monomial $m \in \mathbb{F}[V]$ is called* gapless *if its weight sequence $\Phi(m)$ is gapless.*

For our next result we will need the following easy combinatorial fact:

Lemma 2.6. — *For any sequence $S = (s_1, ..., s_d)$ over an abelian group A let $\Sigma(S) := \{\sum_{i \in I} s_i : I \subseteq \{1, ..., d\}\}$. If $A = Z_p$ for a prime p and $S = (s_1, ..., s_d)$ a sequence of non-zero elements of Z_p then*

$$|\Sigma(S)| \geqslant \min\{p, d + 1\}.$$

Proof. — By the Cauchy-Davenport Theorem $|A+B| \geqslant \min\{p, |A|+|B|-1\}$ for any non-empty subsets $A, B \subseteq Z_p$. Our claim follows from this by induction on d, as $|\Sigma(S)| \geqslant |\Sigma(s_1, ..., s_{d-1})| + |\{0, s_d\}| - 1 \geqslant d+2-1$ for any $1 < d < p$, while the case $d = 1$ is trivial. □

PROPOSITION 2.7. — *Let $G = A \rtimes Z_n$ where $A \cong Z_p$ for some prime p and Z_n acts faithfully on A. Let V be a G-module and $L := \mathbb{F}[V]$, $R := \mathbb{F}[V]^G$, and $\mathcal{V}$ any subset of the variables permuted by G up to non-zero scalar multiples. Then L_+/L_+R_+ is spanned by monomials of the form $b_1 \dots b_r m$, where each b_i is an A-invariant variable or a brick composed of variables in $\mathcal{V}$ while $m_{\mathcal{V}}$ has a gapless divisor of degree at least*

$$\min\{\deg(m_{\mathcal{V}}), \deg(m) - p + 1\}.$$

Proof. — Since A has prime order, a non-trivial character $\chi \in \hat{A}$ takes distinct values on the elements of A. As Z_n acts faithfully on A, for any non-identity element g of Z_n there is an $a \in A$ with $a^g \neq a$, thus $\chi^g(a) = \chi(a^g) \neq \chi(a)$. So (2.2) holds for (G, A). By Lemma 2.2 it suffices to show that for any terminal monomial $m \in L_+$ not containing a brick over $\mathcal{V}$ or an A-invariant variable, $m_{\mathcal{V}}$ has a gapless divisor of degree at least $\min\{\deg(m_{\mathcal{V}}), \deg(m) - p + 1\}$. Let m^* be a gapless divisor of $m_{\mathcal{V}}$ of maximal possible degree, and suppose for contradiction that $\deg(m^*) < \min\{\deg(m_{\mathcal{V}}), \deg(m) - p + 1\}$. Then there is a variable x such that m^*x is a divisor of $m_{\mathcal{V}}$ and m^*x is not gapless, moreover, the index of the orbit O_i containing $\theta(x)$ is minimal possible, i.e. for all $j < i$ we have $\Phi(m^*)^{O_j} = \Phi(m_{\mathcal{V}})^{O_j}$. Let $\Phi(m^*)^{O_i} = R_1 R_2 ... R_h$ be the row decomposition of $\Phi(m^*)^{O_i}$, and denote by t the multiplicity of $\theta(x)$ in $\Phi(m^*)$. It is then necessary that $R_t = R_{t+1} \cup \{\theta(x)\}$, for otherwise m^*x would still be gapless. Take a divisor $u \mid m^*$ with $\Phi(u) = R_{t+1}$, hence $\Phi(ux) = R_t$ and the row decomposition of m^*/u is $R_1 \dots R_t R_{t+2} \dots R_h$. Now consider the remainder $m/(m^*x)$: it contains no variables of weight 0, and its degree is at least $p-1$ by assumption, hence $|\Sigma(\Phi(m/(m^*x)))| = p$ by Lemma 2.6. Thus $m/(m^*x)$ has a (possibly trivial) divisor $\hat{u}$ for which $\theta(\hat{u}) = -\theta(ux)$. It is easy to see that $w := xu\hat{u}$ is a good divisor of m. Indeed, set $v := m/w$, and take $b \in G \setminus A$; clearly, m^*/u divides v. For $j < i$, we have $\Phi((w^b v)_{\mathcal{V}})^{O_j} = \Phi(m_{\mathcal{V}})^{O_j}$. Moreover, $\mu_s(\Phi((w^b v)_{\mathcal{V}})^{O_i}) \geqslant \mu_s(\Phi(m_{\mathcal{V}})^{O_i})$ for $s = 1, \dots t$. Here we have strict inequality at least for one s: by our assumption $\Phi((ux)_{\mathcal{V}}) = R_t$ is not divisible by a brick, so $R_t^b \setminus R_t \neq \emptyset$, hence the support of $\Phi(w_{\mathcal{V}}^b)^{O_i}$ is not contained in R_t, implying $\sum_{s=1}^t \mu_s(\Phi((w^b v)_{\mathcal{V}})^{O_i}) > \sum_{s=1}^t \mu_s(\Phi((m^*/u)_{\mathcal{V}})^{O_i})$. This contradicts the assumption that m was terminal. □

2.2. Factorizations of gapless monomials

Denote by $\mathcal{B}$ the ideal of $L = \mathbb{F}[V]$ generated by the bricks, and denote by $\mathcal{G}_d$ the ideal of L generated by the gapless monomials of degree at least d. Moreover, for a set $\mathcal{V}$ of variables as in Proposition 2.7, denote by $\mathcal{G}_d(\mathcal{V})$ the ideal of L spanned by monomials with a gapless divisor of degree at least d composed from variables in $\mathcal{V}$.

PROPOSITION 2.8. — *Let $V = \mathrm{Ind}_A^G U$ be an isotypic G-module belonging to a G-orbit $O \subseteq \hat{A}$, and s the index of a minimal nontrivial subgroup of G/A. Then*

$$\mathcal{G}_d \subseteq \mathcal{B} \qquad \text{where} \quad d = \binom{|O| - s + 1}{2} + 1.$$

Proof. — Let $m \in \mathbb{F}[V]$ be a gapless monomial not divisible by a brick. In the row decomposition $\Phi(m) = R_1 ... R_h$ we then have $|R_{i+1}| < |R_i|$ for every $1 \leqslant i < h$, and $|R_1| \leqslant |O| - s$, so $\deg(m) \leqslant 1 + 2 + ... + (|O| - s) = \binom{|O|-s+1}{2}$. □

COROLLARY 2.9. — *Let $A = Z_p$ and $G = A \rtimes Z_{q^n}$ where Z_{q^n} acts faithfully on A. Setting $c = \frac{p-1}{q^n}$ and $d = \binom{q^n - q^{n-1}+1}{2}$ and $L = \mathbb{F}[W]$, $R = \mathbb{F}[W]^G$ for a G-module W we have*

$$\beta(L_+, R) \leqslant (q^n - 2)q + \max\{cd, p + d - 1, p + q\}.$$

Proof. — By Lemma 1.11 (applied with $s = q$ and $r = 1$) we have $\beta(L_+, R) \leqslant (q^n - 1)q + \max\{p, \beta(L_+/R_+L_+, S) - q\}$, where $S := \mathbb{F}[I_{\leqslant q}]$. Apart from $O_0 := \{0\}$, Z_p contains c different Z_{q^n}-orbits $O_1, \ldots, O_c$, each of cardinality q^n, and the bricks different from O_0 are all of size q. Thus $\beta(L_+/R_+L_+, S) \leqslant \beta(L_+/L_+R_+, \mathcal{B})$, and it is sufficient to show that for $e := \max\{cd + 1, p + d, p + q + 1\}$, $L_{\geqslant e} \subseteq L_+R_+ + \mathcal{B}$.

Denote by $M^{(i)}$ (resp. $M^{(0)}$) the subspace of $L_{\geqslant e}$ spanned by monomials u with $|\Phi(u)^{O_i}| > d$ (resp. $|\Phi(u)^{O_0}| \geqslant 1$). Clearly $L_{\geqslant e} \subseteq \sum_{i=0}^{c} M^{(i)}$. The A-invariant variables are bricks, so $M^{(0)} \subseteq \mathcal{B}$. Apply Proposition 2.7 with $\mathcal{V}$ the set of variables of weight in O_i for some fixed $i \in \{1, \ldots, c\}$. We obtain that the subspace $M^{(i)}$ is contained in $R_+L_+ + \mathcal{B} + \mathcal{G}_{d+1}(\mathcal{V})$. By Proposition 2.8, $\mathcal{G}_{d+1}(\mathcal{V}) \subseteq \mathcal{B}$, showing that $M^{(i)} \subseteq R_+L_+ + \mathcal{B}$. This holds for all i, hence $L_{\geqslant e} \subseteq L_+R_+ + \mathcal{B}$. □

For the rest of this section let G be the non-abelian semidirect product $Z_p \rtimes Z_q$, where p, q are odd primes and $q \mid p - 1$. We set $L := \mathbb{F}[W]$, $I = \mathbb{F}[W]^{Z_p}$, $R = \mathbb{F}[W]^G$ for an arbitrary G-module W and denote by A the normal subgroup Z_p in G. In this case the bricks are the monomials m with

$\Phi(m) = O_i$ for some $i = 0, 1, \ldots, \frac{p-1}{q}$, so a brick is either an A-invariant variable or has degree q. Moreover, multiplying a gapless monomial by a brick we get a gapless monomial. Thus in the statement of Proposition 2.7 all the b_i may be assumed to be A-invariant variables. We need the following consequence of the Cauchy-Davenport Theorem (see Theorem 5.7.3 in [19] for a more general statement):

LEMMA 2.10. — *Let S be a sequence over Z_p with maximal multiplicity h. If $|S| \geqslant p$ then S has a zero-sum subsequence $T \subseteq S$ of length $|T| \leqslant h$.*

COROLLARY 2.11. — *We have the inequality*

$$\beta(L_+, R) \leqslant p + \frac{q(q-1)^2}{2}.$$

Proof. — Applying Lemma 1.11 with $r = 1$ and $s := \binom{q}{2}$, and using $\beta(L_+, I) \leqslant p$ we get

$$\beta(L_+, R) \leqslant (q-1)s + \max\{p, \beta(L_+/R_+L_+, \mathbb{F}[I_{\leqslant s}]) - s\}$$

so our statement follows from the inequality $\beta(L_+/R_+L_+, \mathbb{F}[I_{\leqslant s}]) \leqslant p + s$.

To prove the latter observe that if $h(m) > s$ for a monomial m, then $|\Phi(m)^O| > s$ for some G/A-orbit O in $\hat{A}$. Therefore

$$L_{\geqslant p+s} = N + \sum_{i=0}^{p-1/q} M^{(i)} \tag{2.3}$$

where N is spanned by monomials having a degree $p+s$ divisor m with $h(m) \leqslant s$, $M^{(0)}$ is spanned by monomials involving an A-invariant variable, and for $i = 1, \ldots, \frac{p-1}{q}$, $M^{(i)}$ is spanned by monomials having a divisor m with $\deg(m) \geqslant p + s$ and $|\Phi(m)^{O_i}| > s$; here $O_1, \ldots, O_{p-1/q}$ are the q-element G-orbits in $\hat{A}$.

By Lemma 2.10 the weight sequence $\Phi(m)$ of a monomial $m \in N$ contains a non-empty zero-sum sequence of length at most $h(m) \leqslant s$, hence $m \in \mathbb{F}[I_{\leqslant s}]_+ L_+$. Applying Proposition 2.7 with $\mathcal{V}$ the variables with weight in O_i for a fixed $i \in \{1, \ldots, \frac{p-1}{q}\}$, we get $M^{(i)} \subseteq L_+R_+ + \mathcal{G}_{s+1}(\mathcal{V}) + M^{(0)}$, and by Proposition 2.8 we have $\mathcal{G}_{s+1}(\mathcal{V}) \subseteq \mathcal{B}$. Clearly $M^{(0)} \subseteq \mathcal{B}$. It follows by (2.3) that $L_{\geqslant p+s} \subseteq R_+L_+ + \mathcal{B} + L_+\,\mathbb{F}[I_{\leqslant s}]_+$, and since bricks have degree at most $q \leqslant s$, the inequality $\beta(L_+/R_+L_+, \mathbb{F}[I_{\leqslant s}]) \leqslant p + s$ is proven. □

Remark 2.12. — The above results are getting close to the lower bound mentioned at the beginning of Chapter 2 only for small values of q: we have $p+2 \leqslant \beta(Z_p \rtimes Z_3) \leqslant p+6$ by Corollary 2.11 and $p+3 \leqslant \beta(Z_p \rtimes Z_4) \leqslant p+6$ by Corollary 2.9 (for the lower bounds see [9]). In characteristic zero, the inequality $\beta(Z_p \rtimes Z_3) \leqslant p + 6$ was proved in [32].

PROPOSITION 2.13. — *We have*

$$\mathcal{G}_d \subseteq (I_+)_{\leqslant q}L \qquad \text{if} \quad d \geqslant \min\{p, \tfrac{1}{2}(p+q(q-2))\}.$$

Proof. — Suppose that m is a gapless monomial having no non-trivial A-invariant divisor of degree at most q (hence m is not divisible by a brick). In particular m has no variables of weight 0. Let $m = m_1...m_{p-1/q}$ be the factorization where $\Phi(m_i) = \Phi(m)^{O_i}$, and let S_i denote the support of the weight sequence $\Phi(m_i)$. By our assumption $0 \notin S := \bigcup_j S_j$ and $|S_i| \leqslant q-1$ for every i.

For each factor m_i we have $h(m_i) \leqslant |S_i| \leqslant q-1$, so if $\deg(m) \geqslant p$ then m contains an A-invariant divisor of degree at most $h(m) \leqslant q-1$ by Lemma 2.10, which is a contradiction, hence $\deg(m) \leqslant p-1$. On the other hand, as each factor m_i is gapless, $\deg(m_i) \leqslant \binom{|S_i|+1}{2} \leqslant \frac{|S_i|q}{2}$, and consequently

$$\deg(m) \leqslant \frac{|S|q}{2}. \tag{2.4}$$

We claim that $|S| \leqslant q + \frac{p-1}{q} - 2$. Write $q^\wedge T := \{t_1 + \cdots + t_q \mid t_i \neq t_j \in T\}$ for any subset $T \subseteq \hat{A}$. The Dias da Silva - Hamidoune theorem (see [39]) states that $|q^\wedge T| \geqslant \min\{p, q|T| - q^2 + 1\}$. Now if our claim were false then we would get from this theorem that

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

implying that m contains an A-invariant divisor of degree q or $q-1$, again a contradiction. By plugging in this upper bound on $|S|$ in (2.4) and since q is odd we get $\deg(m) \leqslant \lfloor \frac{q^2-2q+p-1}{2} \rfloor = \frac{1}{2}(p+q(q-2)) - 1$. □

PROPOSITION 2.14. — *Suppose c, e are positive integers such that $c \leqslant q$ and $\binom{c}{2} < p \leqslant \binom{c+1}{2} - \binom{e+1}{2}$ (in particular, this forces that $p < \binom{q+1}{2}$). Then*

$$\mathcal{G}_d \subseteq (I_+)_{\leqslant c-e}L \qquad \text{if} \qquad d \geqslant p + \binom{e}{2}.$$

Proof. — Suppose that m is a gapless monomial having 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 $|E| \leqslant p-1$, for otherwise by Lemma 2.10 we would get an A-invariant divisor of degree at most $c-e$. It follows that $|S_{c-e}| \leqslant e$, for otherwise the fact that m is gapless and $c \leqslant q$ would lead to the contradiction

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

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

To illustrate the use of Proposition 2.14 consider the case when $p = 11$ and $q = 5$. We then have $c = 5$ and $e = 2$, hence any gapless monomial of degree at least 12 contains an A-invariant of degree at most 3. On the other hand $I_{\geqslant 22} \subseteq I_+R_+ + (\mathcal{G}_{12} \cap I_{\geqslant 22}) \subseteq I_+R_+ + (I_+)_{\leqslant 3}I_{\geqslant 19}$ by Proposition 2.7, hence $I_{\geqslant 28} \subseteq I_+^3 I_{\geqslant 19} + I_+R_+$. Furthermore $I_{\geqslant 19} \subseteq I_+R_+ + (\mathcal{G}_9 \cap I_{\geqslant 19})$ by Proposition 2.7. A monomial $m \in \mathcal{G}_9 \cap I_{\geqslant 19}$ has a gapless divisor u of degree at least 9. It is easily seen that $h(u) \leqslant 3$, hence u can be completed to a monomial $v \mid m$ of degree 11 and height $h(v) \leqslant 5$, which will contain an A-invariant divisor of degree at most 5 by Lemma 2.10. We get that $I_{\geqslant 19} \subseteq (I_+)_{\leqslant 5}I_{\geqslant 14} + I_+R_+$. Finally $I_{\geqslant 14} \subseteq I_+^2$ and putting all these together yields $I_{\geqslant 28} \subseteq I_+^6 + I_+R_+ \subseteq I_+R_+$ by Proposition 1.6. As a result

$$\beta(Z_{11} \rtimes Z_5) \leqslant 27. \tag{2.5}$$

Proposition 2.15. — *For any odd primes p, q such that $q \mid p-1$ we have the following estimates:*

$$\beta(L_+, R) \leqslant \begin{cases} \frac{3}{2}(p + (q-2)q) - 2 & \text{if } p > q(q-2); \\ 2p + (q-2)q - 2 & \text{if } p < q(q-2); \\ 2p + (q-2)(c-1) - 2 & \text{if } c(c-1) < 2p < c(c+1), c \leqslant q. \end{cases}$$

Proof. — Let d be a positive integer such that $\mathcal{G}_d \subseteq (I_+)_{\leqslant q}I$. Given that $\mathcal{B} \subseteq (I_+)_{\leqslant q}I$, we get $\beta(L_+/R_+L_+, \mathbb{F}[I_{\leqslant q}]) \leqslant p + d - 2$ by Proposition 2.7. Using Lemma 1.11 it follows $\beta(L_+, R) \leqslant (q-2)q + p + d - 2$. Our first two estimates follow by substituting the value of d given in Proposition 2.13. The last one follows similarly by deducing from Proposition 2.14 that $\beta(L_+/R_+L_+, \mathbb{F}[I_{\leqslant c-1}]) \leqslant 2p - 2$, and then applying Lemma 1.11. □

Theorem 2.16. — *For the non-abelian semidirect product $Z_p \rtimes Z_q$, where p, q are odd primes we have $\beta(Z_p \rtimes Z_q) < \frac{pq}{2}$.*

Proof. — Recall that $\beta(G, W) \leqslant \beta(L_+, R)$ by Proposition 1.5. Hence by Corollary 2.11 we have $\beta(Z_p \rtimes Z_3) \leqslant p + 6$, hence $\beta(G) < |G|/2$ for $q = 3$ and $p > 7$. The case $p = 7$ will be treated below, with the result $\beta(Z_7 \rtimes Z_3) = 9$ in Theorem 2.25. For the rest we may assume that $q \geqslant 5$. Suppose indirectly that $pq \leqslant 2\beta(Z_p \rtimes Z_q)$. Then by the first estimate in Proposition 2.15

$$p(q-3) \leqslant 3q(q-2) - 4.$$

Suppose first that $4q + 1 \leqslant p$. In this case $q^2 - 5q + 1 \leqslant 0$, whence $q < 5$, a contradiction. It remains that $p = 2q + 1$. Since by (2.5) our statement is true for $q = 5, p = 11$, it remains that $q \geqslant 11$ (as $2q + 1$ is not prime for $q = 7$). Then $2p < q(q+1)$, so we can apply the third estimate in

Proposition 2.15. By the indirect assumption and the fact that $c(c-1) < 2p$ we get that

$$\frac{pq}{2} < 2p + (q-2)\frac{2p}{c}.$$

Here $c \geqslant 7$ as $p \geqslant 23$, but then by this inequality $q \leqslant 6$, a contradiction. □

2.3. 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 $\mathrm{char}(\mathbb{F}) \neq 3, 7$. The character group $\hat{A}$ of the abelian normal subgroup $A = Z_7$ of G will be identified with the additive group of residue classes modulo 7, so the generator b of $G/A = Z_3$ acts on $\hat{A}$ by multiplication with $2 \in (\mathbb{Z}/7\mathbb{Z})^\times$. Then we have three G/A-orbits in $\hat{A}$, 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

$$W = V_+^{\oplus n_+} \oplus V_-^{\oplus n_-} \oplus V_0 \tag{2.6}$$

where V_0 is 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 canonic isomorphism $\mathbb{F}[W] \cong \mathbb{F}[V_+^{\oplus n_+}] \otimes \mathbb{F}[V_-^{\oplus n_-}] \otimes \mathbb{F}[V_0]$; the degrees of these factors will be denoted by $d_+(m), d_-(m), d_0(m)$. Finally we set $I = \mathbb{F}[W]^A$, $R = \mathbb{F}[W]^G$ and let $\tau = \tau_A^G : I \to R$ denote the transfer map.

Proposition 2.17. — *Let $m \in \mathbb{F}[W]$ be a Z_7-invariant monomial with $\deg(m) \geqslant 7$, $d_0(m) = 0$ and $d_+(m), d_-(m) \geqslant 1$. Then $m \in I_2 I_+ + I_+ R_+$.*

Proof. — Denote by S the support of the weight sequence $\Phi(m)$ and by ν_w the multiplicity of $w \in \hat{A}$ in $\Phi(m)$. Observe that $|S| \geqslant 2$ since $d_+(m), d_-(m)$ are both positive. This also implies that $m \in I_+^2$, since any irreducible zero-sum sequence of length at least 7 is similar to (1^7). We have the following cases:

(i) if $|S| \geqslant 4$ then $S \cap -S \neq \emptyset$ hence already $m \in I_2 I_+$.

(ii) if $|S| = 3$ then up to similarity, we may suppose that $S \cap A_+ = \{1\}$ and $S \cap A_- = \{3, 5\}$. If a factorization $m = uv$ exists where u, v is Z_7-invariant and $1 \in \Phi(u)$, $(35) \subseteq \Phi(v)$ then obviously $m - u\tau(v) \in I_2 I_+$. This certainly happens if $\Phi(m)$ contains (1^7) or one of the irreducible zero-sum sequences with support $\{3, 5\}$, namely $(35^5), (3^2 5^3)$, or $(3^3 5)$. Otherwise it remains that $\nu_1 \leqslant 6$, $\nu_3 \leqslant 2$ and $\nu_5 \leqslant 4$. Now, if $\Phi(u) = (135^2)$ then necessarily either $1 \in \Phi(v)$ or $(35) \subseteq \Phi(v)$, and in both cases $m - u\tau(v) \in I_2 I_+$. It

remains that $\nu_5 = 1$, and therefore $\Phi(m)$ equals $(1^3 3^2 5)$ or $(1^6 35)$. The first case is excluded since $\deg(m) \geqslant 7$. In the second take $\Phi(u) = (1^4 3)$, $\Phi(v) = (1^2 5)$ and observe that $\Phi(uv^{b^2})$ falls under case (i), while $\Phi(uv^b) = (1^4 2^2 3^2)$ is similar to the sequence $(1^2 3^2 5^4)$ which was already dealt with.

(iii) if $|S| = 2$ then again $m = uv$ for some $u, v \in I_+$. Denote by U and V the support of $\Phi(u)$ and $\Phi(v)$, respectively. If $|U| \geqslant 2$ or $|V| \geqslant 2$ then after replacing m by $m - u\tau(v)$ we get back to case (ii) or (i). Otherwise $\Phi(m) = (a^{7i} b^{7j})$ for some $a \in A_+, b \in A_-$ and $i, j \geqslant 1$; but then an integer $1 \leqslant n \leqslant 6$ exists such that $(ab^n)(a^{7i-1} b^{7j-n})$ is a Z_7-invariant factorization, and we are done as before. □

Corollary 2.18. — *If $m \in \mathbb{F}[W]$ is a Z_7-invariant monomial such that $\deg(m) \geqslant 10$ and $d_0(m) \geqslant 2$ or $\min\{d_+(m), d_-(m)\} \geqslant 3 - d_0(m)$ then $m \in I_+ R_+$.*

Proof. — By Corollary 1.8 it is enough to prove that $m \in I_+^4$. This is immediate if $d_0(m) \geqslant 2$. If $d_0(m) = 1$ then applying Proposition 2.17 two times shows that $m \in I_1 I_2^2 I_+$. Finally, if $d_0(m) = 0$ then again after two applications of Proposition 2.17 we may suppose that $m = uv$ where $\deg(v) \geqslant 6$, $d_+(v), d_-(v) \geqslant 1$ and $u \in I_2^2$. It is easily checked that any irreducible zero-sum sequence over Z_7 of length at least 6 is similar to (1^7) or $(1^5 2)$, none of which can be isomorphic to $\Phi(v)$. Therefore $v \in I_+^2$ follows and again $m \in I_+^4$. □

Lemma 2.19. — *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 $u, v, w \in I_+$*

$$uvw - uv^g w^{g^2} \in I_+(R_+)_{\leqslant deg(vw)}.$$

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

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

Proposition 2.20. — *Let $m \in \mathbb{F}[W]$ be a Z_7-invariant monomial with m_+ factorized as $m_+ = m_1 ... m_n$ (where $n := n_+$) through the isomorphism $\mathbb{F}[V_+^{\oplus n}] \cong \mathbb{F}[V_+]^{\otimes n}$. If $\deg(m) \geqslant 10$, $d_0(m) \leqslant 1$ and $\max_{i=1}^n \deg(m_i) \geqslant 3$ then $m \in I_+ R_+$.*

Proof. — We shall denote by x, y, z the variables of weight $1, 2, 4$ belonging to that copy of V_+ for which $\deg(m_i)$ is maximal, while X, Y, Z will stand for the variables of the same weights which belong to any other copy of V_+.

Since $d_0(m) \leqslant 1$ by assumption, using Proposition 2.7 with $\mathcal{V} := \{x, y, z\}$ we may assume that $m_{\mathcal{V}}$ has a gapless divisor t of degree at least 3. Let $S \subseteq \hat{A}$ be the support of the weight sequence $\Phi(t)$; clearly $|S| \geqslant 2$. If $|S| = 3$ then $m_{\mathcal{V}}$ is divisible by the G-invariant xyz, and we are done. It remains that $|S| = 2$ hence by symmetry we may suppose that $m_{\mathcal{V}}$ is divisible by $t = x^2y$.

If $d_0(m) = 1$ then m contains an A-invariant variable w and by Lemma 2.6 $|\Sigma(\Phi(m/tw))| = 7$. This gives an A-invariant factorization $m/w = uv$ such that $xy \mid u$ and $x \mid v$. By Lemma 2.19 we get that $m \equiv uv^b w^{b^2} \mod I_+R_+$, where $uv^b w^{b^2}$ contains xyz for a suitable choice of $b \in \{g, g^2\}$, so we are done.

It remains that $d_0(m) = 0$. By a similar argument as in the proof of Proposition 2.7, we may assume that m_+ has a gapless divisor of degree 4, while $m_{\mathcal{V}}$ still contains a gapless divisor of degree 3. Therefore we may suppose that m_+ contains $u := xyZ$ while $m_{\mathcal{V}}$ still contains x^2y. Now if $m/u \in I_+^2$ then we get an A-invariant factorization $m = uvw$ such that $xy \mid u$ and $x \mid v$, so we are done again by using Lemma 2.19. Finally, if m/u is irreducible then necessarily $\Phi(m/u) = (1^7)$, so that $m = x^2yX^6Z$. Here we can employ the following relations:

$$x^2yX^6Z = xyX^4\,\tau(xX^2Z) - xyzX^4Z^2Y - xy^2X^5Y^2$$
$$xy^2X^5Y^2 = xyY^2\,\tau(yX^5) - xyzY^7 - x^2yY^2Z^5.$$

This proves that $m \equiv x^2yY^2Z^5 \mod I_+R_+$, and as $xY^2Z^4 \in I_+^2$, the latter monomial already belongs to I_+R_+ by the first part of this paragraph. □

Corollary 2.21. — *If W is the regular representation V_{reg} of $Z_7 \rtimes Z_3$ then we have $\beta(I_+, R) \leqslant 9$.*

Proof. — Here we have $n_+ = n_- = 3$. Let $m \in I_+$ be a monomial with $\deg(m) \geqslant 10$. If Corollary 2.18 can be applied then $m \in I_+R_+$ already holds. Otherwise $d_0(m) \leqslant 1$ and say $d_-(m) \leqslant 2 - d_0(m)$, whence $d_+(m) \geqslant 8$. Then one of the monomials in the factorization $m_+ = m_1m_2m_3$, say m_1 has degree at least 3, and we are done by Proposition 2.20. □

It was observed by Schmid that $\beta(G) = \beta(G, V_{\mathrm{reg}})$ for any finite group G if $\mathrm{char}(\mathbb{F}) = 0$. This is based on Weyl's theorem on polarization (see [42]). If $\mathrm{char}(\mathbb{F}) > 0$, then Weyl's theorem on polarizations fails even in the non-modular case; instead of that, if $\mathrm{char}(\mathbb{F})$ does not divide $|G|$ then by a result of Grosshans in [21] for any G-module W containing V_{reg} as a submodule, the ring $\mathbb{F}[W]^G$ is the p-root closure of its subalgebra generated by the polarization of $\mathbb{F}[V_{\mathrm{reg}}]^G$.

Corollary 2.21 is an improvement of Pawale's result who proved in [32] in characteristic 0 that $\beta(G,W) = 9$ for $n_+, n_- = 2$, and from this he concluded $\beta(G) = 9$ using a version of Weyl's Theorem on polarization. For positive characteristic we will use the following result:

PROPOSITION 2.22 (Knop, Theorem 6.1 in [28]). — *Let U and V be finite dimensional G-modules. If $n_0 \geqslant \max\{\dim(V), \frac{\beta(G)}{\mathrm{char}(\mathbb{F})-1}\}$ 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 $n \geqslant n_0$ is generated by the polarization (with respect to the type-V variables) of S.*

PROPOSITION 2.23. — *If $\mathrm{char}(\mathbb{F}) \neq 2, 3, 7$ then $\beta(G) \leqslant 9$.*

Proof. — We already know that $\beta(G) \leqslant 13$ from Corollary 2.11. Therefore it is sufficient to show that $R_d \subseteq R_+^2$ whenever $10 \leqslant d \leqslant 13$. 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 2.22 a generating set of $\mathbb{F}[W]^G$ can be obtained by polarizations from a generating set of $\mathbb{F}[V_{\mathrm{reg}}]^G$, so $\beta(G) \leqslant \beta(G, V_{\mathrm{reg}}) \leqslant 9$ by Corollary 2.21.

Finally let $\mathrm{char}(\mathbb{F}) = 5$, so that $\max\{\dim(V_+), \dim(V_-), \frac{\beta(G)}{\mathrm{char}(\mathbb{F})-1}\} \leqslant 4$. By Proposition 2.22 here we can obtain the generators of R by polarizing the generators of $S := \mathbb{F}[V_+^4 \oplus V_-^4 \oplus V_0]^G$. S is spanned by elements f that are multihomogeneous in the sense that for all monomials m occurring in f the triple $(d_+(m), d_-(m), d_0(m))$ is the same; denote it by $(d_+(f), d_-(f), d_0(f))$. We know from formula (6.3) and Theorem 5.1 in [28] that f is contained in the polarization of $\mathbb{F}[V_{\mathrm{reg}}]$ (taken with respect to $V_+^{\oplus 3}$ and then to $V_-^{\oplus 3}$ separately), if $d_+(f), d_-(f) \leqslant 3(\mathrm{char}(\mathbb{F}) - 1) = 12$. So for the rest we may suppose that say $d_+(f) \geqslant 13$. Then let $f_+ = f_1 f_2 f_3 f_4$ be the factorization given by the isomorphism $\mathbb{F}[V_+^{\oplus 4}] \cong \mathbb{F}[V_+]^{\otimes 4}$, and observe that $\deg(f_i) \geqslant 4$ for some $i \leqslant 4$, whence $f \in I_+ R_+$ by Proposition 2.20. □

2.4. The case of characteristic 2

The polarization arguments at the end of the previous section does not cover the case $\mathrm{char}(\mathbb{F}) = 2$. Here we need a closer look at the interplay between our extended Goebel algorithm and the elementary polarization operators

$$\Delta_{i,j} := x_j \frac{\partial}{\partial x_i} + y_j \frac{\partial}{\partial y_i} + z_j \frac{\partial}{\partial z_i}$$

where as before $\mathbb{F}[V_+^{\oplus n}] = \otimes_{i=1}^n \mathbb{F}[x_i, y_i, z_i]$ and the variables x_i, y_i, z_i have weight $1, 2, 4$, respectively. The operators $\Delta_{i,j}$ are G-equivariant, hence

map G-invariants to G-invariants. Moreover, by the Leibniz rule it also holds that:

$$\Delta_{i,j}(I_+R_+) \subseteq I_+R_+. \tag{2.7}$$

PROPOSITION 2.24. — *If* $\mathrm{char}(\mathbb{F}) = 2$ *then* $\beta(I_+, R) \leqslant 9$.

Proof. — Let $m \in I$ be a monomial with $\deg(m) \geqslant 10$. It is sufficient to show that $m \in I_+R_+$. We may suppose by symmetry that $d_+(m) \geqslant d_-(m)$. It suffices to deal with the cases not covered by Corollary 2.18 so we may suppose that $d_0(m) \leqslant 1$, $d_-(m) \leqslant 2 - d_0(m)$, whence $d_+(m) \geqslant 8$. By Proposition 2.7 we can assume that m_+ contains a gapless monomial of degree 3. We have several cases:

(i) Let $m_+ = m_1...m_n$ where each monomial m_i belongs to a different copy of V_+. If $\deg(m_i) \geqslant 3$ for some $i \geqslant 1$ then $m \in I_+R_+$ by Proposition 2.20. So for the rest we may suppose that $\deg(m_i) \leqslant 2$ for every $i = 1, ..., n$.

(ii) If m_+ contains the square of a variable, say x_1^2 then a variable of weight 2 or 4 must also divide m, say $m = x_1^2y_2u$, because we assumed that m_+ contains a gapless divisor of degree 3. Here we have

$$\Delta_{1,2}x_1^2y_1u = 2x_1y_1x_2u + x_1^2y_2u = m$$

as $\mathrm{char}(\mathbb{F}) = 2$. In view of case (i) and (2.7) this shows that $m \in I_+R_+$.

(iii) If m_+ is square-free, but still $\deg(m_i) = 2$ for some i, say $x_1y_1 \mid m$, then our goal will be to find three monomials $u, v, w \in I_+$ such that $m = uvw$ and $x_1 \mid u$, $y_1 \mid v$. For then $m \equiv uv^bw^{b^2} \mod I_+R_+$ by Lemma 2.19 where b can be chosen so that $uv^bw^{b^2}$ contains x_1^2, and then m will fall under case (ii). Here are some conditions under which this goal can be achieved:

(a) If $d_0(m) = 1$ then let w be the Z_7-invariant variable in m; given that $|\Sigma(\Phi(m/wx_1y_1))| = 7$ by Lemma 2.6, suitable factors u, v must exist.

(b) It remains that $d_0(m) = 0$. Again by Proposition 2.7 (with $\mathcal{V}$ the set of variables in $\mathbb{F}[V_+^n]$) we assure that m_+ contains a gapless monomial of degree 4, hence also a Z_7-invariant $u := x_1y_1Z$. Suppose now that $m/u = vw$ for some $v, w \in I_+$. Up to equivalence modulo I_+R_+ we may also suppose that one of these two monomials, say v contains a variable X (or Y). After swapping x_1 and X (or y_1 and Y) in u and v we are done.

(c) If $d_-(m) > 0$, then m/u has a variable t such that some $f \in \{x_1t, y_1t, Zt\}$ belongs to I; as $\deg(m/f) \geqslant 8$, the desired factorization of m is given by Lemma 2.6.

(d) It remains that $d_0(m) = d_-(m) = 0$ and $\Phi(m/u)$ is an irreducible zero-sum sequence. Since $\deg(m/u) \geqslant 7$ it follows that $\Phi(m/u)$ equals (2^7), (1^7) or (4^7). In the first case we use the relation:

$$m = x_1y_1ZY^7 = \tau(x_1Y^3)y_1ZY^4 - y_1^2Y^4Z^4 - z_1y_1X^3Y^4Z$$

where the two monomials on the right hand side fall under case (ii) or (iii/b). The case $\Phi(m/u) = (1^7)$ is similar. Finally, if $\Phi(m/u) = (4^7)$ then we replace m with $m - u\tau(m/u)$ to reduce to the other two cases.

(iv) If m is multilinear: here we can again assume that $(124) \subseteq \Phi(m)$. If $d_0(m) = 0$ then this is achieved using Proposition 2.7. Otherwise, if there is a Z_7-invariant variable w in m then we may still suppose by Proposition 2.7 that e.g. $x_1y_2x_3 \mid m$ and the same argument as above at (iii/a) gives a factorization $m/w = uv$ such that $x_1y_2 \mid u$ and $x_3 \mid v$, so our goal is achieved by Lemma 2.19. Now we may suppose that $m = x_1y_2z_3u$, say. We have:

$$\Delta_{1,2}z_1x_1y_3u + \Delta_{3,1}z_2x_3y_3u = (z_1x_2y_3 + z_2x_3y_1)u = m + \tau(x_1y_2z_3)u$$

The monomials $z_1x_1y_3u$ and $z_2x_3y_3u$ fall under case (iii), so $m \in I_+R_+$. □

Comparing Proposition 2.23 and Proposition 2.24 with the lower bound mentioned at the beginning of Chapter 2, we have proved:

THEOREM 2.25. — *If* $\mathrm{char}(\mathbb{F}) \neq 3, 7$ *then* $\beta(Z_7 \rtimes Z_3) = 9$.

In a subsequent paper [7] the first author proved that $\beta(Z_p \rtimes Z_3) = p+2$ for any prime p congruent to 1 modulo 3.

3. Some further particular cases

3.1. The group $Z_5 \rtimes Z_4$, where Z_4 acts faithfully

The following is proved (without explicitly being stated) by Schmid [36] for $\mathrm{char}(\mathbb{F}) = 0$ and by Sezer [38] in non-modular positive characteristic:

PROPOSITION 3.1. — *Suppose that* $2n \in \mathbb{F}^\times$. *For any module* V *of the dihedral group* $D_{2n} = Z_n \rtimes_{-1} Z_2$ *we have*

$$\beta(D_{2n}, V) \leqslant \beta(\mathbb{F}[V]_+^{Z_n}, \mathbb{F}[V]^{D_{2n}}) \leqslant n + 1.$$

Let $G := Z_5 \rtimes Z_4$ where $Z_4 = \langle b \rangle$ and conjugation by b is an order 4 automorphism of the normal subgroup $A = Z_5$. Take a G-module V and set $L := \mathbb{F}[V]$, $R := \mathbb{F}[V]^G$, $I := \mathbb{F}[V]^A$, $S := \mathbb{F}[V]^H$, where $H \cong D_{10}$ is the subgroup of G generated by A and b^2.

PROPOSITION 3.2. — *If* $\mathrm{char}(\mathbb{F}) \neq 2, 5$ *then* $\beta(I_+, R) = 8$.

Proof. — The lower bound $\beta(I_+, R) \geqslant 8$ follows from a result in [9]. By Corollary 2.9 we have $\beta(I_+, R) \leqslant 5 + 6 = 11$. Therefore it is sufficient to show that if m is an A-invariant monomial with $9 \leqslant \deg(m) \leqslant 11$, then $m \in I_+R_+$. Suppose there are three variables e, f, h such that $m = efhr$ and both ef and eh are A-invariant. The relation

$$2m = \tau_A^H(ef)hr + \tau_A^H(eh)fr - \tau_A^H(fh^{b^2})e^{b^2}r. \tag{3.1}$$

implies that $m \in S_2I_{\geqslant 7}$, and since $\beta(I_+, S) \leqslant 6$ by Proposition 3.1 we get $m \in I_+S_+^2 \subseteq I_+R_+$ (the latter inclusion follows by Proposition 1.6). If m contains two A-invariant variables then $m \in I_1^2I_{\geqslant 7} \subseteq I_{\geqslant 7}S_+$ by Proposition 1.6. As above, $I_{\geqslant 7} \subseteq I_+S_+$, so $m \in I_+S_+^2 \subseteq I_+R_+$. From now on suppose that none of the above two cases hold for m. Then $m = m_0m_+$, where $m_0 = 1$ or m_0 is an A-invariant variable, m_+ involves no A-invariant variables, and $8 \leqslant \deg(m_+) \leqslant 11$. This forces that the support of $\Phi(m_+)$ has at most two elements (not opposite to each other). The action of G/A preserves I_+R_+, therefore it is sufficient to deal with the case when $\Phi(m_+) = (1^k, 2^l)$ or $\Phi(m_+) = (1^k, 3^l)$ where $k \geqslant l$. If $l \geqslant 2$ then $m_+ = ef$ where e, f are A-invariant and $\operatorname{supp}(\Phi(e)) = \operatorname{supp}(\Phi(f)) = \operatorname{supp}(\Phi(m_+))$; now each monomial of $m - e\tau_A^G(f)$ belongs to I_+R_+ by the cases considered already. Finally, if $l \leqslant 1$, then $m_+ = ef$ where $\Phi(f) = 1^5$; again all monomials of $\tau_A^G(f)$ belong to I_+R_+ by the prior cases. □

3.2. The alternating group A_4

Throughout this chapter let $G := A_4$, 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 $\hat{A}$, conjugation by g permutes them cyclically. Remark for future reference that the only irreducible zero-sum sequences over $\hat{A}$ are: (0), (a, a), (b, b), (c, c), (a, b, c). Hence the factorization of any zero-sum sequence over $Z_2 \times Z_2$ into maximally many irreducible ones is of the form

$$(0)^q(a, a)^r(b, b)^s(c, c)^t(a, b, c)^e \qquad \text{where } e = 0 \text{ or } 1. \tag{3.2}$$

In particular the multiplicities of a, b and c must have the same parity.

Let $\mathbb{F}$ be a field with characteristic different from 2 or 3. Apart from the one-dimensional representations of G factoring through the natural surjection $G \to Z_3$, there is a single irreducible G-module V, hence an arbitrary finite dimensional G-module W shall decompose as

$$W = U \oplus V^{\oplus n}$$

where $U = W^A$ consists of one-dimensional G-modules. V is the 3-dimensional summand in the natural 4-dimensional permutation representation of G. Let x, y, z denote the corresponding basis in V^* and following our conventions introduced in Section 2.1 let $\mathbb{F}[V^{\oplus n}] = \otimes_{i=1}^n \mathbb{F}[x_i, y_i, z_i]$, so that x_i, y_i, z_i are A-eigenvectors of weight a, b, c which are permuted cyclically by g. We write $I := \mathbb{F}[W]^A$, $R := \mathbb{F}[W]^G$ and $\tau := \tau_A^G : I \to R$.

PROPOSITION 3.3. — *If $n = 3$ then $R_{\geqslant 7} \subseteq (R_+)_{\leqslant 4} R_+$.*

Proof. — It is sufficient to show that $I_{\geqslant 7} \subseteq (R_+)_{\leqslant 4} I + (I_+)_{\leqslant 4} R$. Take a monomial $m \in I_{\geqslant 7}$ with $\deg(m_+) \geqslant 7$. We claim that $m \in I_+(R_+)_{\leqslant 4}$ in this case. Consider the factorization $m_+ = m_1 m_2 m_3$ given by the map $\mathbb{F}[V^{\oplus 3}] \cong \mathbb{F}[V]^{\otimes 3}$; by symmetry we may assume that $\deg(m_1) \geqslant 3$. If the G-invariant $x_1 y_1 z_1$ divides m then we are done. Using relation (2.1) we may assume that $\Phi(m_1)$ contains at least two different weights, say $x_1 y_1^2 \mid m_1$. Suppose that the multiplicity of b is at least 3 in $\Phi(m)$; then the remainder $m/x_1 y_1^2 y_i$ must contain an A-invariant divisor w with $\deg(w) = 2$. Set $v := y_1 y_i$ and $u := m/vw$ so that u is divisible by $x_1 y_1$. By Lemma 2.19 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 must be even, too. Then $\deg(m) \geqslant 8$ and m has an A-invariant factorization $m = uvw$ with $x_1 y_1^2 \mid u$, and $\deg(v) = \deg(w) = 2$. By Lemma 2.19 m can be replaced by $uv^g w^{g^2}$ or $uv^{g^2} w^g$ so that we get back to the case treated before.

It remains that $\deg(m_+) \leqslant 6$. If $\deg(m_0) \geqslant 3$ then $m_0 \in (R_+)_{\leqslant 3} I$ and we are done. So for the rest $\deg(m_0) \leqslant 2$. Given that $\mathsf{D}(A) = 3$ and $\mathsf{D}_2(A) = 5$ by Proposition 1.13, we have $m \in I_1(I_+)^3_{\leqslant 3} I$ or $m \in I_1^2 (I_+)^2_{\leqslant 3} I$. In both cases $m \in I_+^4$ hence $m \in I_+ R_+$ by Proposition 1.6. Taking into account that $\deg(m) \leqslant 8$ we conclude that $m \in (R_+)_{\leqslant 4} I + (I_+)_{\leqslant 4} R$, as claimed. □

THEOREM 3.4. — *If $\mathrm{char}(\mathbb{F}) \neq 2, 3$ then $\beta_k(A_4) = 4k + 2$.*

Proof. — We pove first that $\beta(A_4) \leqslant 6$. To this end consider the subalgebra $S := \mathbb{F}[U \oplus V^{\oplus 3}]^G$ in $R = \mathbb{F}[U \oplus V^{\oplus n}]^G$ where $n \geqslant 3$. Note that $\beta(S) \leqslant 6$ by Proposition 3.3 and in addition $\beta(G) \leqslant \mathsf{D}_3(A) = 7$ by Corollary 1.8 and Proposition 1.13. We have $R_d = \mathbb{F}[\mathrm{GL}_n \cdot S_d]$ for all d if $\mathrm{char}(\mathbb{F}) = 0$ by Weyl's Theorem on polarization (cf. [42]) and in positive characteristic for $d \leqslant \dim(V)(\mathrm{char}(\mathbb{F}) - 1)$ by Theorem 5.1 and formula (6.3) in [28]; in our case $\dim(V)(\mathrm{char}(\mathbb{F}) - 1) \geqslant 12$. It follows that $R_7 = \mathbb{F}[\mathrm{GL}_n \cdot S_7] \subseteq \mathrm{GL}_n \cdot S_+^2 \subseteq R_+^2$, whence $\beta(A_4) \leqslant 6$, indeed.

For the rest it suffices to prove that $R_{\geqslant 7} \subseteq (R_+)_{\leqslant 4} R$ holds for $n \geqslant 3$, as well, because then by induction on k we get $R_{\geqslant 4k+3} \subseteq (R_+)^k_{\leqslant 4} R_+$. Since

R is generated by elements of degree at most 6, it is enough to prove that $\bigoplus_{d=7}^{12} R_d \subseteq (R_+)_{\leqslant 4}R$. Applying polarization as above and Proposition 3.3 we get $\bigoplus_{d=7}^{12} R_d \subseteq \mathbb{F}[\mathrm{GL}_n \cdot \bigoplus_{d=7}^{12} S_d] = \mathbb{F}[\mathrm{GL}_n \cdot (S_+)_{\leqslant 4}S] \subseteq (R_+)_{\leqslant 4}R$.

To prove $\beta_k(A_4) \geqslant 4k+2$ take as V the natural 4-dimensional permutation representation of the symmetric group S_4. It is well known that $R := \mathbb{F}[V]^{A_4}$ has the Hironaka decomposition $R = P \oplus sP$, where P is the subalgebra generated by the elementary symmetric polynomials p_1, p_2, p_3, p_4, and s is the degree 6 alternating polynomial. It is easy to deduce from the Hironaka decomposition that $sp^{k-1} \notin R_+^{k+1}$. □

Remark 3.5. — Working over the field of complex numbers Schmid [36] already gave a computer assisted proof of the equality $\beta(A_4, U \oplus V^{\oplus 2}) = 6$.

COROLLARY 3.6. — *Suppose that* $\mathrm{char}(\mathbb{F}) \neq 2, 3$. *Then* $\beta(\tilde{A}_4) = 12$.

Proof. — We have $\beta(A_4) = 6$ by Theorem 3.4, and since $\tilde{A}_4$ has a two-element normal subgroup N with $\tilde{A}_4/N \cong A_4$, the inequality $\beta(\tilde{A}_4) \leqslant 12$ follows by Lemma 1.2. It is sufficient to prove the reverse inequality for the field $\mathbb{C}$ (as $\beta(G, \mathbb{C}) \leqslant \beta(G, \mathbb{F})$ by Theorem 4.7 in [28]). 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 the first row in the table of Lemma 4.1 in [25] or Section 0.13 in [33]) that this algebra is minimally generated by three elements of degree $6, 8, 12$, whence $\beta(\tilde{A}_4) \geqslant 12$. □

3.3. The group $(Z_2 \times Z_2) \rtimes Z_9$

PROPOSITION 3.7. — *Let* $G := (Z_2 \times Z_2) \rtimes Z_9$ *be the non-abelian semidirect product, and suppose that* $\mathrm{char}(\mathbb{F}) \neq 2, 3$. *Then we have* $\beta(G) \leqslant 17$.

Let $\hat{K} \cong Z_2 \times Z_2 = \{0, a, b, c\}$ 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 distinguished abelian normal subgroup $A := K \times C$ where $C := \langle g^3 \rangle \cong Z_3$. The conventions of Section 2.1 can be applied for (G, A), since every irreducible representation of G is 1-dimensional or is induced from a 1-dimensional representation of A. 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 $\mu := \tau_C^G : J \to R$, $\tau := \tau_A^G : I \to R$. For any sequence S over $\hat{A}$ we denote by $S|_C$ the sequence obtained from S by restricting to C each element $\theta \in S$.

Proof. — Since $G/C \cong A_4$ and $\beta(A_4) = 6$, by Lemma 1.2 we have $\beta(G) \leqslant 18$. Therefore by Lemma 2.2 it is sufficient to show that if $m \in I$ is a terminal monomial of degree 18, then $\tau(m) \in R_+^2$. We may restrict

our attention to the case when $\Phi(m)|_C = (h^{18})$ for a generator h of $\hat{C}$, as otherwise $m \in J_+^7$, and we get that $\tau(m) = \frac{1}{4}\mu(m) \in R_+^2$ by Proposition 1.3 applied for G/C acting on J. We claim that in this case $\Phi(m)$ contains at least 2 zero-sum sequences of length at most 3, whence $m \in I_+^4$ (since $\beta(A) = 7$ by Proposition 1.13), and consequently $\tau(m) \in R_+^2$ again by Proposition 1.3.

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

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

Observe that the first factor has degree 6, hence it corresponds to a zero-sum sequence over $\hat{A}$, and it is a good divisor in the sense of Definition 2.1. This contradicts the assumption that m was terminal. □

4. Classification of the groups with large Noether number

4.1. A structure theorem

The objective of this section is to prove the following purely group theoretical structure theorem:

THEOREM 4.1. — *For any finite group G one of the following ten options holds:*

1. *G contains a cyclic subgroup of index at most 2;*
2. *G contains a subgroup isomorphic to:*
   - (a) *$Z_2 \times Z_2 \times Z_2$;*
   - (b) *$Z_p \times Z_p$, where p is an odd prime;*
   - (c) *A_4 or $\tilde{A}_4$;*
3. *G has a subquotient isomorphic to:*
   - (a) *an extension of $Z_2 \times Z_2$ by $Z_2 \times Z_2$;*
   - (b) *a non-abelian semidirect product $Z_p \rtimes Z_q$ with odd primes p, q;*
   - (c) *$Z_p \rtimes Z_4$, where p is an odd prime and Z_4 acts faithfully on Z_p;*
   - (d) *$D_{2p} \times D_{2q}$, where p, q are distinct odd primes;*

(e) *an extension of* D_{2n} *by* $Z_2 \times Z_2$*, where* n *is odd;*
(f) *the non-abelian semidirect product* $(Z_2 \times Z_2) \rtimes Z_9$.

LEMMA 4.2 (Burnside). — *If the Sylow 2-subgroup* P *of a group* G *is cyclic then* $G = N \rtimes P$ *where* N *is the characteristic subgroup of* G *consisting of its odd order elements.*

PROPOSITION 4.3 (Zassenhaus, Satz 6 in [43]). — *Let* G *be a finite solvable group with a Sylow 2-subgroup* P *containing a cyclic subgroup of index 2. Then* G *has a normal subgroup* K *with a cyclic Sylow 2-subgroup such that* G/K *is isomorphic to one of the groups* Z_2, A_4 *or* S_4.

LEMMA 4.4 (Roquette [35], or [2] Lemma 1.4 or [26] III. 7. 6). — *If* G *is a finite* p*-group which does not contain* $Z_p \times Z_p$ *as a normal subgroup, then either* G *is cyclic or* $p = 2$ *and* G *is isomorphic to one of the groups* $D_{2^n}, SD_{2^n}, Dic_{2^n}$*, where* $n > 3$*, or to the quaternion group* $Q = Dic_{2^3}$.

COROLLARY 4.5. — *Any finite 2-group* G *falls under case (1), (2a) or (3a) of Theorem 4.1.*

Proof. — Suppose that (1) does not hold for G. Then by Lemma 4.4, G has a normal subgroup $N \cong Z_2 \times Z_2$. Consider the factor group G/N: if it is cyclic, i.e. generated by aN for some $a \in G$, then necessarily $\langle a \rangle \cap N = \{1\}$, for otherwise $\langle a \rangle$ would be a cyclic subgroup of index 2 in G. Now we can find a subgroup $Z_2 \times Z_2 \times Z_2$, which is case (2a): if $a^2 \neq 1$ then this is because a^2 necessarily centralizes N, and if $a^2 = 1$ then already a must centralize N, for otherwise $G = (Z_2 \times Z_2) \rtimes Z_2 \cong D_8$, which has a cyclic subgroup of index 2, a contradiction.

It remains that G/N is non-cyclic. If G/N contains a subgroup isomorphic to $Z_2 \times Z_2$, then we get case (3a). Otherwise by Lemma 4.4 G/N contains a cyclic subgroup of index 2. Given that the Frattini subgroup F/N of G/N is cyclic, F is an extension of a cyclic group by $Z_2 \times Z_2$, hence by the same argument as above, F (and hence G) falls under case (2a), unless F is a non-cylic group with a cyclic subgroup of index 2. Then G/Φ (where Φ is the Frattini subgroup of F) is an extension of $F/\Phi \cong Z_2 \times Z_2$ by $G/F \cong Z_2 \times Z_2$, and we get case (3a). □

PROPOSITION 4.6. — *Let* G *be a group of odd order all of whose Sylow subgroups are cyclic. Then either* G *is cyclic or it falls under case (3b) of Theorem 4.1.*

Proof. — By a theorem of Burnside (see p. 163 in [5]) G is isomorphic to $Z_n \rtimes Z_m$ for some coprime integers n, m. Hence either G is cyclic, or this semidirect product is non-abelian. In the latter case there are elements

$a \in Z_n$ and $b \in Z_m$ of prime-power orders p^k and q^r, which do not commute. After factorizing by the centralizer of $\langle a \rangle$ in $\langle b \rangle$ we may suppose that $\langle b \rangle$ acts faithfully on $\langle a \rangle$. Then the order p subgroup of $\langle a \rangle$ and the order q subgroup of $\langle b \rangle$ generate a non-abelian semidirect product $Z_p \rtimes Z_q$. □

PROPOSITION 4.7. — *Let $G = Z_n \rtimes P$, where n is odd and P is a 2-group with a cyclic subgroup of index 2. Then G falls under case (1), (3c), (3d), or (3e) of Theorem 4.1.*

Proof. — Let C be the centralizer of Z_n in P. The factor P/C is isomorphic to a subgroup of $\mathrm{Aut}(Z_n)$, which is abelian, and $G/C = Z_n \rtimes (P/C)$. If P/C contains an element of order 4, then by a similar argument as in Proposition 4.6 we find a subquotient isomorphic to $Z_p \rtimes Z_4$, where Z_4 acts faithfully on Z_p, which is case (3c). Otherwise P/C must be isomorphic to Z_2 or $Z_2 \times Z_2$. If $P/C = Z_2$ then either C is cyclic, and $Z_n \times C$ is a cyclic subgroup of index 2 in G – this is case (1); or else C is non-cyclic, and then $G/\Phi(C)$ (where $\Phi(C)$ is the Frattini subgroup of C) is an extension of the dihedral group $G/C \cong D_{2n}$ by the Klein four-group $C/\Phi(C) \cong Z_2 \times Z_2$ – this is case (3e).

Finally, if $P/C \cong Z_2 \times Z_2$, we get case (3d): indeed, $Z_n = P_1 \times \cdots \times P_r$, where the P_i are the Sylow subgroups of Z_n. If the generators a and b of $Z_2 \times Z_2$ are acting non-trivially on precisely the same set of subgroups P_i, then since the only involutive automorphism of an odd cyclic group is inversion, ab will act trivially on all P_i, hence $ab \in C$, a contradiction. Therefore a P_i exists such that a acts non-trivially, while b acts trivially on it. But an index $j \neq i$ also must exist such that b is acting non-trivially on P_j; after eventually exchanging a with ab we may suppose that a acts trivially on P_j. Then G has a subfactor $(P_i \times P_j) \rtimes (Z_2 \times Z_2) \cong D_{2p^k} \times D_{2q^l}$, which leads to case (3d). □

Proof of Theorem 4.1 for solvable groups. — We shall argue by contradiction: let G be a counterexample of minimal order. Since G does not fall under case (2b), all its odd order Sylow subgroups are cyclic by Lemma 4.4. As G does not fall under case (1) or (3b), its order is even by Proposition 4.6. Finally, as G does not fall under case (2a) or (3a), its Sylow 2-subgroup contains a cyclic subgroup of index 2 by Corollary 4.5. Therefore Proposition 4.3 applies to G, so a normal subgroup K exists such that G/K is isomorphic to Z_2, A_4 or S_4, and using Lemma 4.2, $K = N \rtimes Q$, where Q is a cyclic 2-group while N is a characteristic subgroup consisting of odd order elements, which is also cyclic, for otherwise it would fall under case (3b). The case $G/K \cong S_4$ is ruled out by the minimality of G (since otherwise the subgroup H of G with $H/K \cong A_4$ would fall under

case (1), a contradiction). The case $G/K \cong Z_2$ is also ruled out, since then $G \cong Z_n \rtimes P$ where the Sylow 2-subgroup P of G has a cyclic subgroup of index 2, so it falls under case (1), (3c), (3d), or (3e) by Proposition 4.7.

It remains that $G/K \cong A_4$. Suppose first that N is trivial. Then $K = Q$ and $P/Q \cong Z_2 \times Z_2$ is normal in $G/Q \cong A_4$, hence P is normal in G and by the Schur-Zassenhaus theorem $G = P \rtimes Z_3$. Let $\langle a \rangle$ be the cyclic subgroup of index 2 in P: the subgroup $\langle a^4 \rangle$ has no non-trivial odd order automorphism, hence the factor group $P/\langle a^4 \rangle$ must have a non-trivial automorphism of order 3. But unless P coincides with the group $Z_2 \times Z_2$ or Dic_8, the factor $P/\langle a^4 \rangle$ is isomorphic to D_8 or $Z_4 \times Z_2$, which do not have an automorphism of order 3 (for a list of the 2-groups with a cyclic subgroup of index 2 see [3]). It follows that $G = (Z_2 \times Z_2) \rtimes Z_3 = A_4$ or $G = Dic_8 \rtimes Z_3 \cong \tilde{A}_4$, which is case (2c), a contradiction.

Finally, suppose that N is nontrivial. Since N is characteristic in K, it is normal in G, and G/N is isomorphic to A_4 or $\tilde{A}_4$ by our previous argument. Then N is necessarily cyclic of prime order, for otherwise a proper subgroup $M \leqslant N$ would exist which is normal is G, and G/M would contain a cyclic subgroup of index at most 2 by the minimality assumption on G, but this is impossible since A_4 is a homomorphic image of G/M. Consequently it also follows that $N = Z_3$, for otherwise $|N|$ and $|G/N|$ are coprime, so that $G = N \rtimes (G/N)$ by the Schur-Zassenhaus theorem, and again G would fall under case (2c), a contradiction. Let C denote the centralizer of N in G/N: on one hand G/C must be isomorphic to a subgroup of $\mathrm{Aut}(Z_3) = Z_2$, but on the other hand Z_2 is not a homomorphic image of A_4 or $\tilde{A}_4$, hence $G = C$. This means that N is central in G, and therefore the Sylow 2-subgroup P is normal in G. Given that the Sylow 3-subgroup of G is cyclic and of order 9 we conclude that $G = P \rtimes Z_9$ where P equals Dic_8 or $Z_2 \times Z_2$, and this gives case (3f), a contradiction. □

Proof of Theorem 4.1 for non-solvable groups. — Suppose to the contrary that Theorem 4.1 fails for a non-solvable group G, which has minimal order among the groups with this property. Then any proper subgroup H of G is solvable: indeed, otherwise (2) or (3) of Theorem 4.1 holds for H, hence also for G, a contradiction. It follows that G has a solvable normal subgroup N such that G/N is a minimal simple group (i.e. all proper subgroups of G/N are solvable). If $G/N \cong A_5$, then denote by H the inverse image in G of the subgroup $A_4 \subseteq A_5$ under the natural surjection $G \to G/N$. Then H is solvable, and has A_4 as a factor group. Thus H has no cyclic subgroup of index at most two. Therefore by the solvable case of Theorem 4.1, (2) or (3) holds for H, hence it holds also for G, a contradiction.

According to Corollary 1 in [40], any minimal simple group is isomorphic to one of the following:

(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. Finally we show that for the remaining minimal simple groups (2a), (2b), or (3) holds, hence G/N can not be isomorphic to any of them (note that if (2a), (2b), or (3) holds for G/N, then (2a), (2b), or (3) holds for G by Sylow's theorem, Lemma 4.4 and Corollary 4.5).

The group $L_2(2^p)$ contains as a subgroup the additive group of the field of 2^p elements. Hence when $p \geqslant 3$ then (2a) holds. Similarly, $L_2(3^p)$ contains as a subgroup the additive group of the field of 3^p elements, hence (2b) holds. The subgroup of unipotent upper triangular matrices in $L_3(3)$ is a non-abelian group of order 27, hence (2b) holds for it. 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. Its center consist of the involutions plus the identity, and it has order q, see for example [23], [6]. 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, hence (2a) holds for it. □

4.2. Proof of the classification theorem

Proof of Theorem 1.1. — It suffices to consider the cases listed in Theorem 4.1:

(1) if G contains a subgroup of index at most 2 then $\beta(G) \geqslant \frac{1}{2}|G|$ by Proposition 5.1 in [36] (in fact $\beta(G) - \frac{1}{2}|G| \in \{1, 2\}$ by [9]).
(2) if G contains a subgroup H of index k such that:
   (a) $H \cong Z_2 \times Z_2 \times Z_2$ then by Proposition 1.14 and Corollary 1.8

$$\frac{\beta(G)}{|G|} \leqslant \frac{1}{8k}\beta_k(Z_2 \times Z_2 \times Z_2) = \frac{1}{4} + \frac{3}{8k}.$$

(b) $H \cong Z_p \times Z_p$ then by Proposition 1.13 and Corollary 1.8

$$\frac{\beta(G)}{|G|} \leqslant \frac{1}{kp^2}\beta_k(Z_p \times Z_p) = \frac{1}{p} + \frac{p-1}{kp^2}.$$

(c) $H \cong A_4$ then by Theorem 3.4 and Corollary 1.8

$$\frac{\beta(G)}{|G|} \leqslant \frac{1}{12k}\beta_k(A_4) = \frac{1}{3} + \frac{1}{6k}.$$

It is easily checked that in all three cases the inequality $\frac{\beta(G)}{|G|} \geqslant \frac{1}{2}$ holds if and only if $k = 1$, and in case (b) it is also necessary that $p = 2$ or 3. Finally, let $H = \tilde{A}_4$; by Lemma 1.4 we have $\beta_k(\tilde{A}_4) \leqslant 2\beta_k(A_4)$ hence $\beta(G) \leqslant \beta_k(\tilde{A}_4) \leqslant 8k + 4$ by Corollary 1.8 and Theorem 3.4, so we get the same upper bound on $\beta(G)/|G|$ as in the case when $H = A_4$.

(3) For any subquotient K of G we have $\beta(G)/|G| \leqslant \beta(K)/|K|$ by Lemma 1.2;

(a) if $K/N \cong Z_2 \times Z_2$ for some normal subgroup $N \cong Z_2 \times Z_2$ then by Lemma 1.4 and Proposition 1.13:

$$\frac{\beta(K)}{|K|} \leqslant \frac{1}{16}\beta_{\beta(Z_2\times Z_2)}(Z_2 \times Z_2) = \frac{1}{16}\beta_3(Z_2 \times Z_2) = \frac{7}{16}.$$

(b) if $K \cong Z_p \rtimes Z_q$ then $\beta(K)/|K| < \frac{1}{2}$ by Theorem 2.16.

(c) if $K \cong Z_p \rtimes Z_4$, where Z_4 acts faithfully, then by Corollary 2.9

$$\frac{\beta(K)}{|K|} \leqslant \frac{p+6}{4p} \leqslant \frac{13}{28}$$

for $p \geqslant 7$, and $\beta(K)/|K| = 2/5$ for $p = 5$ by Proposition 3.2.

(d) if $K \cong D_{2p} \times D_{2q}$ where p, q are distinct odd primes (hence $p \geqslant 3$ and $q \geqslant 5$) then by Lemma 1.2 and Proposition 3.1:

$$\frac{\beta(G)}{|G|} \leqslant \frac{1}{4pq}\beta(D_{2p})\beta(D_{2q}) \leqslant \frac{(p+1)(q+1)}{4pq} \leqslant \frac{2}{5}.$$

(e) if $K/N \cong D_{2p}$ for some normal subgroup $N \cong Z_2 \times Z_2$ then by Lemma 1.4 and Proposition 3.1:

$$\frac{\beta(G)}{|G|} \leqslant \frac{1}{8p}\beta_{\beta(D_{2p})}(Z_2 \times Z_2) \leqslant \frac{2p+3}{8p} \leqslant \frac{3}{8}.$$

(f) if $K \cong (Z_2 \times Z_2) \rtimes Z_9$ then $\beta(K)/|K| \leqslant \frac{17}{36}$ by Proposition 3.7.

To sum up, $\beta(G)/|G| < 1/2$ whenever G falls under case (3) of Theorem 4.1. □

BIBLIOGRAPHY

[1] D. J. Benson, *Polynomial Invariants of Finite Groups*, Cambride University Press, 1993.

[2] Y. Berkovich, *Groups of Prime Power Order*, de Gruyter Expositions in Mathematics, vol. I, de Gruyter, Berlin, New York, 2008.

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

[4] R. M. Bryant & G. Kemper, "Global degree bounds and the transfer principle", *J. Algebra* **284** (2005), no. 1, p. 80-90.

[5] W. Burnside, *Theory of Groups of Finite Order*, second ed., Cambridge University Press, 1911.

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

[7] K. Cziszter, "The Noether number of the non-abelian group of order 3p", *Periodica Math. Hung.* **68** (2014), p. 150-159.

[8] K. Cziszter & M. Domokos, "On the generalized Davenport constant and the Noether number", *Cent. Eur. J. Math.* **11** (2013), no. 9, p. 1605-1615.

[9] ———, "The Noether bound for the groups with a cyclic subgroup of index two", *J. Algebra* **399** (2014), p. 546-560.

[10] C. Delorme, O. Ordaz & D. Quiroz, "Some remarks on Davenport constant", *Discrete Mathematics* **237** (2001), p. 119-128.

[11] H. Derksen & G. Kemper, *Computational Invariant Theory*, Encyclopedia of Mathematical Sciences, vol. 130, Springer-Verlag, 2002.

[12] H. Derksen & G. Kemper, "On Global Degree Bounds for Invariants", *CRM Proceedings and Lecture Notes* **35** (2003), p. 37-41.

[13] J. Dixmier, "Sur les invariants du groupe symétrique dans certaines représentations. II", in *Topics in invariant theory (Paris, 1989/1990)*, Lecture Notes in Math., vol. 1478, Springer, Berlin, 1991, p. 1-34.

[14] M. Domokos & P. Hegedűs, "Noether's bound for polynomial invariants of finite groups", *Arch. Math. (Basel)* **74** (2000), no. 3, p. 161-167.

[15] P. Fleischmann, "On invariant theory of finite groups", in *Invariant theory in all characteristics*, CRM Proc. Lecture Notes, vol. 35, Amer. Math. Soc., Providence, RI, 2004, p. 43-69.

[16] P. Fleishmann, "The Noether bound in invariant theory of finite groups", *Adv. Math.* **156** (2000), no. 1, p. 23-32.

[17] J. Fogarty, "On Noether's bound for polynomial invariants of a finite group", *Electron. Res. Announc. Amer. Math. Soc.* **7** (2001), p. 5-7.

[18] W. Gao & A. Geroldinger, "Zero-sum problems in finite abelian groups: a survey", *Expo. Math.* **24** (2006), p. 337-369.

[19] A. Geroldinger & F. Halter-Koch, *Non-Unique Factorizations. Algebraic, Combinatorial and Analytic Theory*, Monographs and textbooks in pure and applied mathematics, Chapman & Hall/CRC, 2006.

[20] M. Göbel, "Computing bases of permutation-invariant polynomials", *J. Symbolic Computation* **19** (1995), p. 285-291.

[21] F. Grosshans, "Vector invariants in arbitrary characteristic", *Transformation Groups* **12** (2007), p. 499-514.

[22] F. Halter-Koch, "A generalization of Davenport's constant and its arithmetical applications", *Colloquium Mathematicum* **LXIII** (1992), p. 203-210.

[23] G. Higman, "Suzuki 2-groups", *Illinois Journal of Mathematics* **7** (1963), p. 79-95.

[24] D. Hilbert, "Über die Theorie der algebraischen Formen", *Math. Ann.* **36** (1890), p. 473-531.

[25] W. C. Huffman, "Polynomial Invariants of Finite linear Groups of degree two", *Canad. J. Math* **32** (1980), p. 317-330.

[26] B. Huppert, *Endliche Gruppen I*, Springer-Verlag, Berlin-Heidelberg-New York, 1967.

[27] G. Kemper, "Separating invariants", *Journal of Symbolic Computation* **44** (2009), no. 9, p. 1212-1222.

[28] F. Knop, "On Noether's and Weyl's bound in positive characteristic", in *Invariant theory in all characteristics*, CRM Proc. Lecture Notes, vol. 35, Amer. Math. Soc., Providence, RI, 2004, p. 175-188.

[29] M. Neusel & L. Smith, *Invariant Theory of Finite Groups*, AMS, 2001.

[30] E. Noether, "Der Endlichkeitssatz der Invarianten endlicher Gruppen", *Math. Ann.* **77** (1916), p. 89-92.

[31] ———, "Der Endlichkeitssatz der Invarianten endlicher linearer Gruppen der Charakteristik p", *Nachr. Ges. Wiss. Göttingen* (1926), p. 28-36.

[32] V. M. Pawale, "Invariants of semi-direct products of cyclic groups", Ph.D. Thesis, Brandeis University, 1999.

[33] V. L. Popov & E. Vinberg, "Invariant Theory", in *Algebraic Geometry IV*, Encyclopedia of Mathematical Sciences, vol. 55, Springer-Verlag, Berlin-Heidelberg, 1994.

[34] D. R. Richman, "Invariants of finite groups over fields of characteristic p", *Adv. Math.* **124** (1996), p. 25-48.

[35] P. Roquette, "Realisierung von Darstellungen endlicher nilpotenten Gruppen", *Arch. Math.* **9** (1958), p. 241-250.

[36] B. J. Schmid, "Finite groups and invariant theory", in *Topics in invariant theory (Paris, 1989/1990)*, Lecture Notes in Math., vol. 1478, Springer, Berlin, 1991, p. 35-66.

[37] J. P. Serre, *Representations linéares des groupes finis*, Hermann, Paris, 1998.

[38] M. Sezer, "Sharpening the generalized Noether bound in the invariant theory of finite groups", *J. Algebra* **254** (2002), no. 2, p. 252-263.

[39] J. A. Dias da Silva & Y. O. Hamidoune, "Cyclic Spaces for Grassmann Derivatives and Additive Theory", *Bull. London Math. Soc.* **26** (1994), no. 2, p. 140-146.

[40] J. G. Thompson, "Nonsolvable finite groups all of whose local subgroups are solvable", *Bull. Amer. Math. Soc.* **74** (1968), p. 383-437.

[41] D. Wehlau, "The Noether number in invariant theory", *Comptes Rendus Math. Rep. Acad. Sci. Canada* **28** (2006), no. 2, p. 39 - 62.

[42] H. Weyl, *The Classical Groups*, Princeton University Press, Princeton, 1939.

[43] H. Zassenhaus, "Über endliche Fastkörper", *Abhandlungen aus dem Mathematischen Seminar der Hamburgische Universität* **11** (1935), p. 187-220.

Manuscrit reçu le 7 mai 2012,
révisé le 13 septembre 2013,
accepté le 26 septembre 2013.

Kálmán CZISZTER
Central European University,
Department of Mathematics and its Applications,
Nádor u. 9, 1051 Budapest,
Hungary
cziszter_kalman-sandor@ceu-budapest.edu

Mátyás DOMOKOS
Rényi Institute of Mathematics,
Hungarian Academy of Sciences,
Reáltanoda u. 13-15, 1053 Budapest,
Hungary
domokos.matyas@renyi.mta.hu