Improvements on the Noether bound for polynomial invariants of finite groups

By
Kálmán Cziszter

Submitted to
Central European University
Department of Mathematics and its Applications

In partial fulfillment of the requirements
for the degree of
Doctor of Philosophy

Supervisor:
Professor Mátyás Domokos

Budapest, Hungary
2012

Acknowledgements

First and foremost I thank my supervisor, Mátyás Domokos for this great intellectual adventure that I had the privilege to experience on his side in the last couple of years. He conceived the conjectures from which our main results grew out, and the strategy to reach this goal was also envisioned by him. If I was able to transcend my limitations on these pages, this is only due to his guidance, his endless patience and meticulous care for the details.

I also thank Pál Hegedűs and Gergely Harcos for inspiring discussions and Vivek Pawale for making available his unpublished thesis to us.

Finally, I want to express my gratitude to the members of my family for their continued support and encouragement.

I dedicate this work to my beloved wife, Ildikó.

Abstract

The Noether number $\beta(G)$ of a finite group G gives the maximal degree of the elements of a minimal generating system in the ring of polynomial invariants $\mathbb{F}[V]^G$ for any G-module V over a field $\mathbb{F}$. Its precise value is known only for very few particular groups until yet. We developed a new method for calculating the Noether number consisting of a generalization of this notion and a series of related reduction lemmata. By means of this we were able to calculate or estimate $\beta(G)$ for several particular groups, including every finite group with a cyclic subgroup of index two; for this infinite class of groups we proved that the difference $\beta(G) - \frac{1}{2}|G|$ equals 1 or 2. The main result of this thesis states that — apart from four particular groups of small order — the groups with a cyclic subgroup of index at most two are the only finite groups satisfying the inequality $\beta(G) \geq \frac{1}{2}|G|$.

Contents

Chapter 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 [35] 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

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

provided that $\mathrm{char}(\mathbb{F})$ does not divide the order of G (see Noether [34] in characteristic 0 and Fleischmann [16], Fogarty [17] in positive characteristic). We define the *relative Noether bound*

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

Working over the field of complex numbers, Schmid [43] proved that $\gamma(G) = 1$ holds only when G is cyclic. This was sharpened by Domokos and Hegedűs in [14] by proving that $\gamma(G) \leq 3/4$ for all non-cyclic G; the result was extended to non-modular positive characteristic by Sezer [45]. The constant $3/4$ is optimal here. On the other hand, a straightforward lower bound on $\gamma(G)$ can be obtained based on the result of Schmid in [43], that $\beta(G) \geq \beta(H)$ holds for any subgroups H of G, so in particular, $\beta(G)$ is bounded from below by the maximal order of the elements in G. Therefore $\gamma(G) \geq 1/2$ whenever G contains a cyclic subgroup of index two, and obviously there are infinitely

many isomorphism classes of such non-cyclic groups. The first main result of the present thesis is that —apart from four sporadic exceptions— these are the only groups for which the relative Noether number is so large:

Theorem 1.1. *For a finite group G with order not divisible by* $\mathrm{char}(\mathbb{F})$ *we have $\gamma(G) \geq 1/2$ if and only if G has a cyclic subgroup of index at most 2, or G is isomorphic to $Z_3 \times Z_3$, $Z_2 \times Z_2 \times Z_2$, the alternating group A_4, or the binary tetrahedral group $\tilde{A}_4$.*

This Theorem is a novelty even for the case $\mathbb{F} = \mathbb{C}$. Its proof reunites methods of representation theory and commutative algebra with additive combinatorics and group theory. Chapter 2 introduces our main technical tool, the generalized Noether number $\beta_k(G)$, which is the smallest integer d such that the homogeneous invariants of degree strictly greater than d are all contained in the $k+1$-th power of the maximal homogeneous ideal $\mathbb{F}[V]^G_+$. We prove a series of reduction lemmata which will allow us to estimate $\beta_k(G)$ by structural induction on G, using our previous knowledge on the generalized Noether number of some subgroups and homomorphic images of G, such as:

$$\begin{aligned}
\beta_k(G) &\leq \beta_{\beta_k(G/N)}(N) && \text{if } N \lhd G \\
\beta_k(G) &\leq \beta_{k[G:H]}(H) && \text{if } H \leq G \\
\beta_k(G) &\geq \beta_r(G/N) + \beta_{k+1-r}(N) - 1 && \text{if } G' \leq N \lhd G \\
\beta_k(G \times H) &\geq \beta_r(G) + \beta_{k+1-r}(H) - 1 && \text{if } 1 \leq r < k
\end{aligned}$$

(for the precise statement see Lemma 2.3, Corollary 2.7, Theorem 2.15 and Theorem 2.11). These are extensions of Schmid's reduction lemmata and in the same time of some analogous results on the generalized Davenport number $\mathsf{D}_k(A)$, which coincides with $\beta_k(G)$ whenever $G = A$ is abelian (see Chapter 6.1 in [21]). They give typically stronger estimates for the Noether number than Schmid's original reduction lemmata. The general explanation for this is given by Theorem 2.25, which proves that $\beta_k(G)$ as a function of k is linear for sufficiently large values of k, and determines the coefficient of k: it turns out to be another notable quantity in invariant theory.

In the proof of our main result the application of these reduction lemmata is based on Theorem 6.1 which isolates a list of groups such that an arbitrary finite group G must contain one of them as a subgroup or a subquotient. The proof is then made complete in Chapters 3–5, where we compute the (generalized) Noether number for these particular groups.

In Chapter 3 we deal with the surprisingly difficult case of the non-abelian group $Z_p \rtimes Z_q$, where p, q are odd primes and $q \mid p-1$. We rely here in great part on an extended version of Goebel's algorithm described in Section 3.1.

For the general case we were only able to give some estimates leading to the conclusion in Theorem 3.16 that $\gamma(Z_p \rtimes Z_q) < \frac{1}{2}$. Precise values were only obtained for $\beta(Z_7 \rtimes Z_3)$ and $\beta_k(Z_p \rtimes Z_3, V)$ for V multiplicity free in Theorem 3.25 and Theorem 3.29: from these particular cases we can get a picture about the nature and the extent of the difficulties overshadowing the general case.

In Chapter 4 we give the precise value of $\beta_k(A_4)$ (see Theorem 4.5), from which we derive information on two related groups: the binary tetrahedral group $\tilde{A}_4$ and $(Z_2 \times Z_2) \rtimes Z_9$ which is a central extension of A_4 by Z_3.

Chapter 5 contains our second main result, Theorem 5.20, which gives the exact value of $\beta_k(G)$ for every finite group G containing a cyclic subgroup of index 2. We begin with the case of the dihedral group D_{2n}; for this group the value of $\beta(D_{2n})$ was already known before, however our new proof based on the simple combinatorial idea of the so-called "zero-corners" also yields in addition the generalized Noether numbers $\beta_k(D_{2n})$ and a characterization of the k-extremal invariants of $G = D_{2n}$, i.e. those which have degree equal to $\beta_k(G)$ but they still don't belong to $(\mathbb{F}[V]_+^G)^{k+1}$. The knowledge of these k-extremal invariants can then be used to refine our estimates on $\beta_k(G)$ when G has a subgroup or a homomorphic image isomorphic to D_{2p}, as in the case of $G = Z_p \rtimes Z_4$, where Z_4 acts faithfully on Z_p, or as in the case of $G = Z_p \rtimes Z_{2n}$, where Z_{2n} acts by inversion on Z_p. The "contraction method" used in this later case might be adapted in the future for several groups of similar structure. Finally we treat the case of the quaternion group Q and the direct product $Z_p \times Q$ in Theorem 5.17.

The concluding Chapter 6, apart from connecting together the different elements in the proof of Theorem 1.1, also gives some applications, most notably Corollary 6.9 stating that

$$\limsup \gamma(G) = \frac{1}{2} \tag{1.2}$$

where G runs through the isomorphism classes of all non-cyclic finite groups of order coprime to $\mathrm{char}(\mathbb{F})$. This brings to light the remarkable theoretical status of Theorem 1.1: given any $0 < c < 1$, one might aim at classifying finite groups G with $\gamma(G) \geq c$. Theorem 1.1 and Theorem 5.20 show that $1/2$ is a limit point in the set $\{\gamma(G) \mid G \text{ is a finite group}\}$ of rational numbers, and there are no limit points strictly between 1 and $1/2$. Chapter 6 is closed by Theorem 6.13 determining the exact degree bound for separating invariants of the group $Z_p \rtimes Z_3$. The systematic study of the version for separating invariants of the Noether number was recently initiated, see [32].

The practical relevance of our results is the following: every computer algorithm used for finding a minimal generating system of the invariant ring

$\mathbb{F}[V]^G$ is computationally very expensive and their feasibility may depend on the availability of an *a priori* bound of good quality on the degrees of these generators. From now on these algorithms may safely assume the upper bound $\frac{1}{2}|G|$ of (1.2) instead of the classic upper bound $|G|$ in (1.1) — except for the few groups listed in Theorem 1.1.

1.2 Preliminaries

Let M be a graded module over a commutative graded $\mathbb{F}$-algebra R such that $R_0 = \mathbb{F}$ is a field if R is unital and $R_0 = \emptyset$ otherwise. For any $d \in \mathbb{N}$ we denote by M_d the $\mathbb{F}$-vector space of degree d homogeneous elements in M. We set:

$$M_{\geq s} := \bigoplus_{d \geq s} M_d \qquad\qquad M_{\leq s} := \bigoplus_{d=0}^{s} M_d$$

We also use the notation $M_+ := M_{\geq 1}$, so if we regard R as a module over itself, its maximal homogeneous ideal is denoted by R_+. Remark that $M_{\geq s}$ is also a graded R-module, whereas $M_{\leq s}$ is merely a vector space over $\mathbb{F}$; the R-submodule generated by it is $M_{\leq s}R$, while the subalgebra of R generated by $R_{\leq s}$ will be denoted by $\mathbb{F}[R_{\leq s}]$.

Definition 1.2. If M is finitely generated as an R-module then set:

$$\beta(M, R) := \min\{s \in \mathbb{N} : M = M_{\leq s}R\}$$

and write $\beta(M, R) = \infty$ otherwise.

Lemma 1.3 (graded Nakayama Lemma)**.** *M is generated by its homogeneous elements $m_1, ..., m_n$ if and only if the $\mathbb{F}$-vector space M/R_+M is spanned by the images $\overline{m_1}, ..., \overline{m_n}$.*

As a consequence the homogeneous elements $m_1, ..., m_n$ constitute a *minimal* R-module generating system of M if and only if $\overline{m}_1, ..., \overline{m}_n$ is a *basis* of the $\mathbb{F}$-vector space M/R_+M. In particular, every minimal generating system of M has the same cardinality. Note that $M/R_+M := \oplus_{i \in \mathbb{N}} M_i/(R_+M \cap M_i)$ is a graded R-module, and supposing that $\deg(m_1) \leq \deg(m_2) \leq ...$, this degree sequence is uniquely determined by M, since the number of occurrences of any integer d in this degree sequence equals the dimension of the degree d component of M/R_+M. Remark finally that $\beta(M, R) = \max_i \deg(m_i)$.

We set $\beta(R) := \beta(R_+, R)$. In view of Definition 1.2 this gives the maximal degree of a homogeneous element $m \in R_+$ not belonging to R_+^2, i.e. which cannot be expressed as a polynomial of strictly lower degree elements of R_+. Thus R is generated *as an algebra* by its elements of degree at most $\beta(R)$.

Lemma 1.4. *$\beta(M,R)$ has the following elementary properties:*

1. *If S is a graded subalgebra of R then $\beta(M,R) \leq \beta(M,S)$.*
2. *If a degree preserving R-module epimorphism $\tau : N \to M$ exists then $\beta(M,R) \leq \beta(N,R)$.*
3. *$\beta(M \otimes N, R \otimes S) = \beta(M,R) + \beta(N,S)$ where M and N are graded modules over the graded $\mathbb{F}$-algebras R and S, respectively.*

Proof. (1) is trivial. For (2) suppose that $d > \beta(N,R)$; by Definition 1.2 this implies that $N_d \subseteq R_+N$. From the assumption on τ it follows that $M_d = \tau(N_d) \subseteq R_+\tau(N) = R_+M$, whence $\beta(M,R) \leq d$. Finally, for (3) observe that the vector space $M \otimes N/(R \otimes S)_+(M \otimes N)$ can be identified with $M/R_+M \otimes N/S_+N$, whence the claim follows by Lemma 1.3. □

Let us translate the above concepts into the more particular setting of invariant theory. Here we are given a group G and a vector space V over a field $\mathbb{F}$ equipped with a group homomorphism $G \to \mathrm{GL}(V)$; in this situation we also say that V is a representation of G or 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^*. This means in fact that $\mathbb{F}[V]$ is isomorphic to a polynomial ring in $\dim(V)$ variables, so in particular it is a graded ring and we have an identification $\mathbb{F}[V]_1 \cong V^*$. From the left action of G on V we can derive a natural right action on V^* by setting $x^g(v) = x(gv)$ for any $g \in G, v \in V$ and $x \in V^*$. This right action of G on V^* is then extended multiplicatively onto the whole $\mathbb{F}[V]$. The basic object of our 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. The question wether it is finite was answered for the non-modular case by Hilbert in [26] as follows. Suppose that G is *linearly reductive*: this amounts basically to the requirement that there is a G-equivariant R-module projection $\tau : L \to R$, where $L := \mathbb{F}[V]$ and $R := \mathbb{F}[V]^G$; τ is the so called Reynolds operator. The Hilbert ideal R_+L is finitely generated by Hilbert's basis theorem, hence $\beta(L_+,R)$ is finite. But as $\beta(R) \leq \beta(L_+,R)$ by Lemma 1.4 (2), it follows that $\beta(G,V)$ is finite.

Any finite group G is linearly reductive; this is the content of Maschke's theorem, the proof of which actually constructs the Reynolds operator. We shall need in the sequel a relativized version of this construction:

Definition 1.5. (cf. [33] p. 33) Let $H \leq G$ 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* $\tau^G : \mathbb{F}[V] \to \mathbb{F}[V]^G$.

Proposition 1.6. *If* $\mathrm{char}(\mathbb{F})$ *does not divide* $[G : H]$ *then* $\tau := \tau_H^G$ *is a graded* $\mathbb{F}[V]^G$*-module epimorphism onto* $\mathbb{F}[V]^G$*.*

Proof. Remark that τ does not depend on the choice of the coset representatives in Definition 1.5. Indeed, if $f_1, ..., f_n$ is another set of coset representatives of H then $g_i f_i^{-1} \in H$ for every i, hence $\sum_i u^{g_i} = \sum_i u^{(g_i f_i^{-1}) f_i} = \sum_i u^{f_i}$ since u was invariant under H by assumption. Consequently, the image of τ is contained in $\mathbb{F}[V]^G$, since $g_1 f, ..., g_n f$ forms another system of coset representatives of H for any $f \in G$. Moreover for any $u \in \mathbb{F}[V]^G$ and $v \in \mathbb{F}[V]^H$ we have $\tau(uv) = \sum_{i=1}^n (uv)^{g_i} = u \sum_{i=1}^n v^{g_i} = u\tau(v)$ hence τ is an $\mathbb{F}[V]^G$-module homomorphism. Obviously τ is degree preserving. Finally, τ is surjective onto $\mathbb{F}[V]^G$ because by Definition 1.5 we have $\tau(u) = nu$ for any $u \in \mathbb{F}[V]^G$. Then $\tau(n^{-1}u) = u$ since $n = [G : H] \in \mathbb{F}^\times$ by assumption. □

When we turn from the linearly reductive groups to the particular case of finite groups, an interesting new topic emerges. The *global degree bound* for a finite group G is defined as

$$\beta(G, \mathbb{F}) := \sup_V \beta(G, V)$$

where V runs through all G-modules over the field $\mathbb{F}$. By Noether's degree bound (see (1.1)) if $\mathrm{char}(\mathbb{F})$ is coprime to $|G|$ then $\beta(G, V) \leq |G|$ for any G-module V, so that $\beta(G, \mathbb{F})$ is finite. The converse of this statement also holds: it was proved in [13] for $\mathrm{char}(\mathbb{F}) = 0$ and subsequently in [6] for the whole non-modular case that the finiteness of $\beta(G, \mathbb{F})$ 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 [40] a sequence of G-modules $V_1, V_2, ...$ such that $\beta(G, V_i) \to \infty$ as $i \to \infty$, so in this case $\beta(G, \mathbb{F})$ is not finite.

The dependence of $\beta(G, \mathbb{F})$ on the field $\mathbb{F}$ was studied by Knop in [31]. He proved that $\beta(G, \mathbb{F})$ is the same for every field $\mathbb{F}$ with the same characteristic, so that the notation $\beta(G, p)$ would be more appropriate, where $p = \mathrm{char}(\mathbb{F})$. In particular this implies that $\beta(G, \mathbb{F}) = \beta(G, \overline{\mathbb{F}})$ where $\overline{F}$ is the algebraic

closure of $\mathbb{F}$. Knop also proves that $\beta(G,0) \leq \beta(G,p)$ for any prime $p > 0$, with equality for almost all primes. Finally, he raises the question whether there are any examples where $\beta(G,0) \neq \beta(G,p)$; this is still unanswered. It is customary in the literature to suppress the reference to the base field $\mathbb{F}$ and write only $\beta(G)$; we shall do the same when it does not lead to confusions.

If $\mathrm{char}(\mathbb{F}) = 0$ then a classic theorem of Weyl (see [49]) asserts that given some G-modules V_i each of dimension $n_i = \dim(V_i)$, a generating set of the invariant ring $\mathbb{F}[V_1^{\oplus d_1} \oplus ... \oplus V_r^{\oplus d_r}]^G$ can be obtained by polarization from a generating set of the ring $\mathbb{F}[V_1^{\oplus n_1} \oplus ... \oplus V_r^{\oplus n_r}]^G$, provided that $d_i \geq n_i$ for all $i = 1, ..., r$. Since polarization preserves the degree, we get as an immediate consequence the result (due to Schmid) that $\beta(G) = \beta(G, V_{\mathrm{reg}})$ where V_{reg} is the regular representation of G. If $\mathrm{char}(\mathbb{F}) > 0$ this fails to be true even in the non-modular case; instead of that, it follows from a result of Grosshans in [23] that if $\mathrm{char}(\mathbb{F})$ does not divide $|G|$, then 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 $\mathbb{F}[V_{\mathrm{reg}}]^G$. We shall need later the following result of Knop on polarization in positive characteristic:

Proposition 1.7 (Knop, Theorem 6.1 in [31])**.** *Let U and V be finite dimensional G-modules. If $n_0 \geq \max\{\dim(V), \frac{\beta(G)}{\mathrm{char}(\mathbb{F})-1}\}$ and S is a generating set of $\mathbb{F}[U \oplus V^{\oplus n_0}]^G$ then $\mathbb{F}[U \oplus V^{\oplus n}]^G$ for any $n \geq n_0$ is generated by the polarization (with respect to the type-V variables) of S.*

Finally, let us summarize the previously known reduction lemmata by means of which $\gamma(G)$ can be bound through induction on the structure of G:

Lemma 1.8. *We have $\gamma(G) \leq \gamma(K)$ for any subquotient K of G.*

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

$$\beta(G) \leq [G : H]\beta(H) \tag{1.3}$$

$$\beta(G) \leq \beta(G/N)\beta(N) \tag{1.4}$$

These were proved for characteristic 0 by Schmid (see Lemma 3.2 and 3.1 in [43]) and subsequently extended to the case when $\mathrm{char}(\mathbb{F}) \nmid |G|$ by Sezer (see Proposition 2 and 4 in [45]). After dividing by $|G| = [G : H]|H|$ the first inequality yields $\gamma(G) \leq \gamma(H)$, and similarly from the second inequality $\gamma(G) \leq \gamma(G/N)\gamma(N)$, whence $\gamma(G) \leq \gamma(G/N)$, as $\gamma(N) \leq 1$ by (1.1). □

Convention 1.9. Throughout this thesis $\mathbb{F}$ is an algebraically closed base field and G is a finite group of order not divisible by $\mathrm{char}(\mathbb{F})$, unless explicitly stated otherwise. All vector spaces and algebras are over $\mathbb{F}$.

1.3 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-canonic) 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 $\mathrm{char}(\mathbb{F})$ is coprime to $|A|$ by Convention 1.9, V decomposes as direct sum of irreducible representations of dimension 1. This means that V^* has an A-eigenbasis $\{x_1, ..., x_n\}$ and the action of A on each of these dual vectors can be described by a character $\theta_i \in \hat{A}$ such that $x_i^a = \theta_i(a)x_i$; θ_i is called the *weight* of x_i. We shall always tacitly choose this A-eigenbasis as the variables in the polynomial algebra $\mathbb{F}[V] = \mathbb{F}[x_1, ..., x_n]$. Let $M(V)$ denote the set of monomials in $\mathbb{F}[V]$; this is a monoid with respect to ordinary multiplication and unit element 1. On the other hand we denote by $\mathcal{M}(\hat{A})$ 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 $\theta \in \hat{A}$ we denote by $-\theta$ the character $a \mapsto \theta(a)^{-1}$, $a \in A$.

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 $\theta(m)$. 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 [20]. As it is seen from our discussion:

$$\mathsf{D}(A) = \beta(A). \tag{1.5}$$

The *generalized Davenport constant* $\mathsf{D}_k(A)$ is introduced in [24] as the length of the longest zero-sum sequence that cannot be factored into more than k non-empty zero-sum sequences. Obviously $\mathsf{D}_1(A) = \mathsf{D}(A)$, moreover $\mathsf{D}_k(A) \le k\,\mathsf{D}(A)$, and for cyclic groups $\mathsf{D}_k(Z_q) = kq$.

By the structure theorem of finite abelian groups $A \cong Z_{n_1} \times \cdots \times Z_{n_s}$, where $1 < n_1 \mid \cdots \mid n_s$ are positive integers and Z_n stands for the cyclic group of order n. It was proved by Olson [36], [37] that when A is a p-group or A has rank $s = 2$, then

$$\mathsf{D}(A) = n_1 + ... + n_s - s + 1. \tag{1.6}$$

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

Proposition 1.10 (Halter-Koch, [24] Proposition 5)**.** *For any $n \mid m$ we have*

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

Proposition 1.11 (Delorme-Ordaz-Quiroz, [10] Lemma 3.7)**.**

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

Proof. A sequence of length at least 8 over $Z_2 \times Z_2 \times Z_2$ either contains 0 or it contains two identical non-zero elements: in both cases there is a "short" zero-sum sequence of length at most 2 in it. Therefore any zero-sum sequence of length $8+2k$ factors into $k+1$ short zero-sum sequences, plus one of length at least 6, which in turn factors into two, since $\mathsf{D}(Z_2 \times Z_2 \times Z_2) = 4$ by (1.6). This shows that $\mathsf{D}_{k+2} \le 7 + 2k$.

For the converse consider the zero-sum sequence which contains one non-zero element $a \in Z_2 \times Z_2 \times Z_2$ with multiplicity $2k+1$ and every other non-zero element with multiplicity 1. This sequence has length $7 + 2k$, and since (aa) is the only short zero-sum sequence occurring in it, it cannot be factored into more than $k + 2$ non-empty zero-sum sequences. □

Now we are in the position to classify the abelian groups with $\gamma(A) \ge 1/2$:

Proposition 1.12. *Let A be a finite abelian group such that $|A| \in \mathbb{F}^\times$. We have $\gamma(A) \geq \frac{1}{2}$ if and only if A is one of the following groups:*

(i) Z_m *where* $m \geq 1$ *and then* $\gamma(A) = 1$*;*

(ii) $Z_2 \times Z_{2m}$ *where* $m \geq 1$ *and then* $\gamma(A) = \frac{1}{2} + \frac{1}{4m}$*;*

(iii) $Z_3 \times Z_3$ *and then* $\gamma(A) = \frac{5}{9}$*;*

(iv) $Z_2 \times Z_2 \times Z_2$ *and then* $\gamma(A) = \frac{1}{2}$*.*

Proof. Assume $A \cong Z_{n_1} \times \cdots \times Z_{n_s}$ where $s \geq 2$, $1 < n_1 \mid ... \mid n_s$ and $\gamma(A) \geq 1/2$. If $s = 2$ then Olson's formula (1.6) implies that (ii) or (iii) holds for A. Moreover, taking into account Lemma 1.8 we conclude that if $s \geq 3$, then $Z_3 \times Z_3 \times Z_3$ or $Z_2 \times Z_2 \times Z_2$ is a subgroup of A. By (1.6) the relative Noether number of the first group is strictly less than $1/2$, hence this case is ruled out. If $Z_2 \times Z_2 \times Z_2$ is a subgroup of index m in A, then by Lemma 2.3 and by Proposition 1.11 we have $\gamma(A) \leq \frac{2m+3}{8m}$, which is strictly less than $1/2$ when $m > 1$. □

1.4 Results on zero-sum sequences

In the remaining part of this chapter we collect for further reference some facts about zero-sum sequences over the cyclic group Z_n. We shall repeatedly use the Cauchy-Davenport Theorem, asserting that

$$|A + B| \geq \min\{p, |A| + |B| - 1\} \tag{1.7}$$

for any non-empty subsets A, B in Z_p, where p is a prime. There are two extensions of this result: Vosper's theorem (see Theorem 5.9. in [46]) states that equality in (1.7) implies that A and B are arithmetic progressions of the same step, provided that $|A|, |B| \geq 2$ and $|A + B| \leq p - 2$. Moreover, when n is arbitrary by a result of Kemperman and Scherk (see Theorem 5.2.10 in [21]) for any non-empty subsets $A, B \subset Z_n$ we have:

$$|A + B| \geq |A| + |B| - \min_{z \in A+B} r_{A,B}(z) \tag{1.8}$$

where $r_{A,B}(z) := |\{(x, y) : x \in A, y \in B, x + y = z\}|$ counts the number of ways in which an element $z \in Z_n$ can be represented as an element of the sumset $A + B$.

Lemma 1.13 (cf. [21] Thm. 5.3.1)**.** *Let S be a sequence over $Z_n \setminus \{0\}$ with maximal multiplicity h. If $|S| \geq n$ then S has a zero-sum subsequence $T \subseteq S$ of length $|T| \leq h$.*

Proof. Let $R_1 \supseteq ... \supseteq R_h$ be the subsets of $Z_n \backslash \{0\}$ such that $S = R_1 ... R_h$. Set $T_i := R_i \dot{\cup} \{0\}$ for every $i = 1, ..., h$. Suppose indirectly that $0 \notin R_1 + ... + R_h$. This means in particular that $r_{T_1+...+T_i, T_{i+1}}(0) = 1$ for every $i < h$. Using (1.8) we get by induction on i that $|T_1 + ... + T_i| \geq |R_1| + ... + |R_i| + 1$ for every $i \leq h$. As a result $n \geq |T_1 + ... + T_h| \geq |S| + 1$, which contradicts our assumption. □

Definition 1.14. For any sequence $S = (s_1, ..., s_d)$ over an abelian group A the set of its partial sums is $\Sigma(S) := \{\sum_{i \in I} s_i : I \subseteq \{1, ..., d\}\}$.

Lemma 1.15. *Let p be a prime and $S = (s_1, ..., s_d)$ a sequence of non-zero elements of Z_p. Then $|\Sigma(S)| \geq \min\{p, d + 1\}$.*

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

Lemma 1.16 (Freeze – Smith [19])**.** *For any zero-sum free sequence S over Z_n of length d and maximal multiplicity $h = h(S)$ it holds that*

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

Proposition 1.17 (Dias da Silva – Hamidoune [9])**.** *Let p be a prime and $A \subseteq Z_p$ a nonempty subset. Let $s^\wedge A$ denote the set of all sums of s distinct elements of A. Then*

$$|s^\wedge A| \geq \min\{p, s|A| - s^2 + 1\}$$

Proposition 1.18 (Balandraud [1])**.** *Let p be an odd prime and $A \subset Z_p$ such that $A \cap (-A) = \emptyset$. Then*

$$|\Sigma(A)| \geq \min\left\{p, 1 + \frac{|A|(|A| + 1)}{2}\right\}$$

Let e be a generator of the cyclic group Z_n; for an arbitrary element $a \in Z$, the smallest positive integer r such that $a = re$ is denoted by $||a||_e$. For any sequence $S = (a_1, ..., a_l)$ over Z_n we set $||S||_e := ||a_1||_e + ... + ||a_l||_e$. The quantity $||S|| := \min_{\langle e \rangle = Z_n} ||S||_e$ is called the *index* of S.

Proposition 1.19 (Savchev – Chen [42])**.** *Any irreducible zero-sum sequence over Z_n of length $l > \frac{n}{2} + 1$ has index n.*

Finally, we prove two original results, which might have some interest on their own, independently of the context in which we use them later. They are based on an intermediary step in the proof of the Savchev – Chen Theorem (see Proposition 2. in [42]):

Proposition 1.20. *Let $S_1 \subset S_2 \subset ... \subset S_t$ be zero-sum free sequences over the cyclic group Z_n such that $|S_i| = i$ for all $i = 1, ..., t$ and*

$$|\Sigma(S_{i+1})| \geq |\Sigma(S_i)| + 2 \qquad \text{for all } i \leq t-1 \tag{1.9}$$

If moreover $S_t(b)$ is also zero-sum free for some $b \in Z_n$ and $|\Sigma(S_t(b))| = |\Sigma(S_t)| + 1$, then b is the unique element with these two properties.

Lemma 1.21. *Any sequence S over Z_n contains either a zero-sum sequence of length at most $\lceil \frac{n}{2} \rceil$ or an element of multiplicity at least $|S| - \lfloor \frac{n}{2} \rfloor$.*

Proof. Suppose that S does not contain a zero-sum sequence of length at most $\lceil \frac{n}{2} \rceil$ and let $S_1 \subset ... \subset S_t$ be zero-sum free sequences where t is maximal with the property that $|\Sigma(S_{i+1})| \geq |\Sigma(S_i)|+2$ and $|S_i| = i$ for every $i \leq t-1$; let $S = S_t R$. By this assumption $n \geq |\Sigma(S_t)| \geq 2t$. If $t = \lceil \frac{n}{2} \rceil$, which enforces that n is even, then $|\Sigma(S_t)| = n$, hence any $a \in R$ can be completed into a zero-sum sequence $U(a)$ with some $U \subseteq S_t$. By our assumption it is necessary that $|U(a)| > \lceil \frac{n}{2} \rceil$, hence $U = S_t$ and the multiplicity of $a = -\theta(S_t)$ is at least $|R| = |S| - \lceil \frac{n}{2} \rceil$. It remains that $t \leq \lceil \frac{n}{2} \rceil - 1$. Then for any $b \in R$ the sequence $S_t(b)$ of length at most $\lceil \frac{n}{2} \rceil$ must be zero-sum free by our assumption, hence by the maximality property of S_t necessarily $|\Sigma(S(b))| = |\Sigma(S)| + 1$. But we know from Proposition 1.20 that the element b with these two properties is unique, hence b has multiplicity $|R| \geq |S| - \lceil \frac{n}{2} \rceil + 1$. □

Lemma 1.22. *Let S be a zero-sum sequence over Z_n of length $|S| \geq kn+1$, $(k \geq 2)$, which does not factor into more than $k+1$ non-empty zero-sum sequences. Then $S = T_1 T_2 (e^{(k-1)n})$ where $\langle e \rangle = Z_n$ and $||T_1||_e = ||T_2||_e = n$.*

Proof. First we prove that an element $e \in S$ has multiplicity at least $(k-1)n$; if so e will have order n, for otherwise S factors into at least $2(k-1)+2 > k+1$ non-empty zero-sum sequences. Let $S = T_1 S_1$ where T_1 is a non-empty zero-sum sequence of minimal length in S. If $|T_1| > \lceil \frac{n}{2} \rceil$ then $h(S) \geq |S| - \lfloor \frac{n}{2} \rfloor$ by Lemma 1.21, and we are done. If however $|T_1| \leq \lceil \frac{n}{2} \rceil$ then $S_1 = T_2 S_2$ where T_2 is a minimal non-empty zero-sum sequence in S_1; obviously $|T_2| \geq |T_1|$. If $|T_2| > \lceil \frac{n}{2} \rceil$ then $h(S) \geq h(S_1) \geq |S_1| - \lfloor \frac{n}{2} \rfloor \geq |S| - \lceil \frac{n}{2} \rceil - \lfloor \frac{n}{2} \rfloor = |S| - n$ by Lemma 1.21, and we are done again. It remains that $|T_2| \leq \lceil \frac{n}{2} \rceil$. Then $|T_1 T_2| \leq n+1$ and $|S_2| \geq (k-1)n$. Given that S_2 cannot be factored into more than $k-1$ non-empty zero-sum sequences it is necessary that $S_2 = (e^{(k-1)n})$.

Now suppose to the contrary that $||T_1||_e > n$, say. Then $T_1 = U(a)V$ where U, V are non-empty subsequences such that $||U||_e < n$, $||U(a)||_e > n$. But then $(e^n) \cdot T_1 = (e^{n-||U||_e})U \cdot (e^{n-||a||_e} a) \cdot (e^{||U||_e + ||a||_e - n})V$ is a factorization which leads to a decomposition of S into more than $k+1$ non-empty zero-sum sequences, and this is a contradiction. □

Chapter 2

The generalized Noether number

Definition 2.1. Let M be a graded module over a graded $\mathbb{F}$-algebra R as in Section 1.2. We define for any integer $k \geq 1$

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

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 $\beta_k(G, V) \leq k\beta(G, V)$ 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.

2.1 Reduction for normal subgroups

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

Proposition 2.2. *Suppose that* $\mathrm{char}(\mathbb{F})$ *does not divide* $|G|$. *Then* $\beta_k(G)$ *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. There exists a finite dimensional G-module V and a G-equivariant $\mathbb{F}$-algebra surjection $\pi : \mathbb{F}[V] \to L$ mapping $\mathbb{F}[V]_+$ onto L_+. Moreover, π restricts to a surjection $\mathbb{F}[V]_+^G \to L_+^G$ by the assumption on the characteristic of $\mathbb{F}$. So we have

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

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

Lemma 2.3. *Suppose that* $\mathrm{char}(\mathbb{F}) \nmid |G|$ *and* N *is a normal subgroup of* G. *Then for any finite dimensional* G*-module* V *we have*

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

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

Proof. We shall apply Proposition 2.2 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

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

Remark 2.4. In the particular case when $G = A$ is abelian the generalized Noether number equals the generalized Davenport number: $\beta_k(A) = \mathsf{D}_k(A)$ for any $k > 0$. In view of this, Lemma 2.3 applied to abelian groups yields for any subgroup $B \leq A$ that:

$$\mathsf{D}_k(A) \leq \mathsf{D}_{\mathsf{D}_k(A/B)}(B) \tag{2.1}$$
$$\mathsf{D}_k(A) \leq \mathsf{D}_{\mathsf{D}_k(B)}(A/B) \tag{2.2}$$

The second inequality follows from the first by observing that 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].

2.2 Reduction for arbitrary subgroups

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.

Proposition 2.5. *Let J be a non-unitary commutative $\mathbb{F}$-algebra on which a finite group G acts via $\mathbb{F}$-algebra automorphisms and let $H \leq G$ 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 $f_1, \ldots, f_r \in J^H$ 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 $\{f_1, \ldots, f_r\}$ (see e.g. Lemma 1.5.1 in [3]), 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 [31]; the idea appears in Benson's simplification of Fogarty's argument from [17], see Lemma 3.8.1 in [12]). 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

$$0 \;=\; \sum_{y\in\mathcal{S}} \prod_{x\in\mathcal{S}} (a_x - a_x^{x^{-1}y}) = \sum_{U\subseteq\mathcal{S}} (-1)^{|U|}\delta_U \qquad \text{where} \tag{2.3}$$

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

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 (2.3), and observe that

$$\tau^H(\delta_U) = \prod_{x\notin U} a_x \sum_{h\in H}\sum_{y\in\mathcal{S}} (\prod_{x\in U} a_x^{x^{-1}})^{yh} = \prod_{x\notin U} a_x \tau^G(\prod_{x\in U} a_x^{x^{-1}}) \tag{2.4}$$

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

Corollary 2.7. *Keeping the assumptions of Proposition 2.5 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 finitely generated graded I-module M we have*

$$\beta_k(M, R) \leq \beta_{k[G:H]}(M, I). \tag{2.5}$$

In particular we have the inequalities

$$\beta_k(I_+, R) \leq \beta_{k[G:H]}(I_+/R_+^k I_+) \tag{2.6}$$
$$\beta_k(G, V) \leq \beta_{k[G:H]}(H, V). \tag{2.7}$$

Proof. By Proposition 2.3 we have $I_+^{k[G:H]} \subseteq I_+ R_+^k + R_+^k$, and consequently $M I_+^{k[G:H]} \subseteq M R_+^k$, implying the first inequality.

The second inequality follows from the first by setting $M := I_+/R_+^k I_+$ and noting that $\beta_k(I_+, R) = \beta_k(M, R)$ and similarly $\beta_{k[G:H]}(M, I) = \beta_{k[G:H]}(M)$.

Finally, the third is a weakening of the second since by Lemma 1.4 (2) $\beta_k(G, V) = \beta_k(R) \leq \beta_k(I_+, R)$ and $\beta_{k[G:H]}(M) \leq \beta_{k[G:H]}(I) = \beta_{k[G:H]}(H, V)$. □

Remark 2.8. (i) From Lemma 2.3 and Corollary 2.7 in the special case $k = 1$ one recovers Schmid's reduction lemmata mentioned in Lemma 1.8.

(ii) It is conjectured that $\beta(G, V) \leq [G : H]\beta(H, V)$ holds in fact always 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 [12] or on page 1222 in [30].

The use of Lemma 2.3 and Corollary 2.7 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 1.3 already for abelian groups.

2.3 Lower bounds

Schmid [43] proved that the Noether number is monotone with respect to taking subgroups. This extends for the generalized Noether number as well:

Lemma 2.9. *Let W be a finite dimensional H-module, where H is a subgroup of a finite group G, and denote by V the G-module induced from W. Then the inequality $\beta_k(G, V) \geq \beta_k(H, W)$ holds for all positive integers k.*

Proof. View W as an H-submodule of

$$V = \bigoplus_{g \in G/H} gW \tag{2.8}$$

where G/H stands for a system of left H-coset representatives. Restriction of functions from V to W is a graded $\mathbb{F}$-algebra surjection $\phi : \mathbb{F}[V] \to \mathbb{F}[W]$. Clearly ϕ is H-equivariant, hence maps $\mathbb{F}[V]^G$ into $\mathbb{F}[W]^H$. Even more, as observed in the proof of Proposition 5.1 of [43], we have $\phi(\mathbb{F}[V]^G) = \mathbb{F}[W]^H$: indeed, the projection from V to W corresponding to the direct sum decomposition (2.8) identifies $\mathbb{F}[W]$ with a subalgebra of $\mathbb{F}[V]$, and for an arbitrary $f \in \mathbb{F}[W]^H \subset \mathbb{F}[W] \subset \mathbb{F}[V]$, we get that $\tau(f) := \sum_{g^{-1} \in G/H} f^g \in \mathbb{F}[V]^G$ is a G-invariant mapped to f by ϕ. Hence if $\mathbb{F}[V]^G_d \subseteq (\mathbb{F}[V]^G_+)^{k+1}$ for some integer $d > 0$ then $\mathbb{F}[W]^H_d = \phi(\mathbb{F}[V]^G_d) \subseteq \phi((\mathbb{F}[V]^G_+)^{k+1}) = (\mathbb{F}[W]^H_+)^{k+1}$. By definition of the generalized Noether number we get that $\beta_k(G, V) \geq \beta_k(H, W)$. □

Corollary 2.10. *Let H be a subgroup of a finite group G, and suppose that* $\mathrm{char}(\mathbb{F})$ *does not divide the order of G. Then for all positive integers k we have the inequality $\beta_k(H) \leq \beta_k(G)$.*

Next we give a strengthening of Corollary 2.10 in the special case when H is normal in G and the factor group G/H is abelian. For a character $\theta \in \widehat{G/H}$ denote by $\mathbb{F}[V]^{G,\theta}$ the space $\{f \in \mathbb{F}[V] \mid f^g = \theta(g)f \quad \forall g \in G\}$ of the *relative G-invariants of weight θ*. Generalizing the construction in the proof of Lemma 2.9, for $f \in \mathbb{F}[W]^H \subset \mathbb{F}[V]$ (here again $V = \mathrm{Ind}_H^G W$) set

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

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

$$\phi(\mathbb{F}[V]^{G,\theta}) = \mathbb{F}[W]^H \text{ holds for all } \theta \in \widehat{G/H}. \tag{2.9}$$

Let $U := \bigoplus_{i=1}^d U_i$ be a direct sum of one-dimensional G/H-modules U_i. Making the identification $\mathbb{F}[U \oplus V] = \mathbb{F}[U] \otimes \mathbb{F}[V] = \bigoplus_{\alpha \in \mathbb{N}_0^d} x^\alpha \otimes \mathbb{F}[V]$ (where following the convention introduced in Section 1.3, the variables $x_1, \ldots, x_d$ in $\mathbb{F}[U]$ are G/H-eigenvectors with weight denoted by $\theta(x_i)$), we have

$$\mathbb{F}[U \oplus V]^G = \bigoplus_{\alpha \in \mathbb{N}_0^d} x^\alpha \otimes \mathbb{F}[V]^{G, -\theta(x^\alpha)} \tag{2.10}$$

Setting $\tilde{\phi} := \mathrm{id} \otimes \phi : \mathbb{F}[U \oplus V] \to \mathbb{F}[U] \otimes \mathbb{F}[W]$, (2.9) and (2.10) imply that

$$\tilde{\phi}(\mathbb{F}[U \oplus V]^G_+) = \mathbb{F}[U]^G_+ \oplus \bigoplus_{\alpha \in \mathbb{N}_0^d} x^\alpha \otimes \mathbb{F}[W]^H_+. \tag{2.11}$$

Theorem 2.11. *Let H be a normal subgroup of a finite group G with G/H abelian, and suppose that* $\mathrm{char}(\mathbb{F})$ *does not divide the order of G. Then for all positive integers k we have the inequality*

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

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

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

where $\theta = \sum_{i=1}^{d} \theta_i$ (we write the character group $\widehat{G/H}$ additively). Then $t \in \mathbb{F}[U \oplus V]^G$ is homogeneous of degree $d + \beta_k(H, W)$. We will show that $t \notin (\mathbb{F}[U \oplus V]_+^G)^{k+1}$, implying $\beta_k(G, U \oplus V) \geq \beta_k(H, W) + d = \beta_k(H) + d$. Indeed, assume to the contrary that $t \in (\mathbb{F}[U \oplus V]_+^G)^{k+1}$. Then by (2.11) we have

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

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

$$x_1 \cdots x_d \otimes f \in \left(\bigoplus_{\alpha \in \mathbb{N}_0^d} x^{\alpha} \otimes \mathbb{F}[W]_+^H \right)^{k+1}. \tag{2.12}$$

Denote by $\rho : \mathbb{F}[U] \otimes \mathbb{F}[V] \to \mathbb{F}[V]$ the $\mathbb{F}$-algebra homomorphism given by the specialization $x_i \mapsto 1$ $(i = 1, \ldots, d)$. Applying ρ to (2.12) we get that $f \in (\mathbb{F}[W]_+^H)^{k+1}$, contradicting the choice of f. □

Remark 2.12. (i) Lemma 2.9, Corollary 2.10, and Theorem 2.11 remain true with the same proofs under the weaker condition that $[G : H]$ is finite.

(ii) The proof of Theorem 2.11 also yields the stronger conclusion

$$\beta_k(G) \geq \max_{0 \leq s \leq k-1} \beta_{k-s}(H) + \mathsf{D}_{s+1}(G/H) - 1 \tag{2.13}$$

(iii) If G is abelian, we get $\mathsf{D}_k(G) \geq \mathsf{D}_k(H) + \mathsf{D}(G/H) - 1$ for any subgroup $H \leq G$. For the case $G = H \oplus H_1$, this was proved in [24], Proposition 3 (i).

Lemma 2.13. *Let G be a finite group of order coprime to* $\mathrm{char}(\mathbb{F})$*. Then for any G-module V there exists an irreducible G-module U such that*

$$\beta_k(G, V \oplus U) \geq \beta_k(\mathbb{F}[V], \mathbb{F}[V]^G) + 1.$$

Proof. Write $L = \mathbb{F}[V]$, $R = \mathbb{F}[V]^G$ and set $d := \beta_k(L, R)$. By semisimplicity of the G-module L_d its submodule $R_+^k L \cap L_d$ has a direct complement, which is non-zero by the definition of d, hence it contains an irreducible G-submodule U. Choose a basis $e_1, \ldots, e_n$ in U and let $\varepsilon_1, \ldots, \varepsilon_n$ be the corresponding dual basis in U^*. Then $f := \sum_{i=1}^n e_i \varepsilon_i$ is a G-invariant of degree $d+1$ in the ring $\mathbb{F}[V \oplus U] = \mathbb{F}[V] \otimes \mathbb{F}[\varepsilon_1, \ldots, \varepsilon_n]$. We claim that $f \notin S_+^{k+1}$ where $S := \mathbb{F}[V \oplus U]^G$. Note that the action of G on $\mathbb{F}[V \oplus U]$ preserves the total degree both in the variables belonging to V^* and to U^*. Suppose indirectly that $f \in S_+^{k+1}$. Then $f = \sum_i g_i h_i$ where $g_i \in R_+^k$ while $h_i \in S_+$ is linear on U, i.e. $h_i = \sum_{k=1}^n h_{i,k} \varepsilon_k$ for some polynomials $h_{i,k} \in L$. After equating the coefficients of ε_i on both sides we get that $e_i = \sum_k g_i h_{i,k} \in R_+^k L$, contradicting the choice of U. □

Corollary 2.14. *If V is a G-module such that $\beta_k(G, V) = \beta_k(G)$ then*

$$\beta_k(G, V) = \beta_k(\mathbb{F}[V], \mathbb{F}[V]^G) + 1.$$

Proof. For any G-module V it holds that $\beta_k(G, V) \leq \beta_k(L, R) + 1$ where $L = \mathbb{F}[V]$ and $R = \mathbb{F}[V]^G$. Indeed, if $f \in L$ has degree $\deg(f) > \beta_k(L, R) + 1$ then by definition $f \in L_+ L_{>\beta_k(L,R)} \subseteq L_+ R_+^k$, hence by basic properties of the transfer map $\tau : L \to R$ it follows that $\tau(f) \in R_+^{k+1}$. The reverse inequality is an immediate consequence of Lemma 2.13. □

Theorem 2.15. *For any integers $r, s \geq 1$ we have the inequality*

$$\beta_{r+s-1}(G \times H) \geq \beta_r(G) + \beta_s(H) - 1.$$

Proof. First we prove the following extension of Lemma 1.4 (3): if M and N are graded modules over the graded algebras R and S, respectively, then:

$$\beta_{r+s-1}(M \otimes N, R \otimes S) \geq \beta_r(M, R) + \beta_s(N, S) \tag{2.14}$$

Indeed, there are elements $x \in M_{\beta_r(M,R)} \setminus R_+^r M$ and $y \in N_{\beta_s(N,S)} \setminus S_+^s N$. Take a vector space basis $\mathcal{B}_1$ of $R_+^r M$, and extend $\mathcal{B}_1 \cup \{x\}$ to a basis $\mathcal{B}$ of M. Similarly, let $\mathcal{C}_1$ be a basis of $S_+^s N$, and extend $\mathcal{C}_1 \cup \{y\}$ to a basis $\mathcal{C}$ in N. Then $\mathcal{A} := \{u \otimes v \mid u \in \mathcal{B}_1, v \in \mathcal{C} \text{ or } u \in \mathcal{B}, v \in \mathcal{C}_1\}$ is a basis of $T := R_+^r M \otimes N + M \otimes S_+^s N$. On the other hand $\mathcal{A} \cup \{x \otimes y\}$ can be extended to a basis of $M \otimes N$, showing that $x \otimes y \notin T$. But $T \supseteq (R \otimes S)_+^{r+s-1}(M \otimes N)$, whence (2.14) readily follows.

Now take a G-module V with $\beta_r(G,V) = \beta_r(G)$, and an H-module W with $\beta_s(H,W) = \beta_s(H)$. Given that $\mathbb{F}[V \oplus W]^{G\times H} = \mathbb{F}[V]^G \otimes \mathbb{F}[W]^H$ we have the following sequence of implications:

$$\begin{aligned}
\beta_{r+s-1}(G\times H) - 1 &\geq \beta_{r+s-1}(\mathbb{F}[V\oplus W], \mathbb{F}[V\oplus W]_+^{G\times H}) && \text{by Lemma 2.13}\\
&\geq \beta_r(\mathbb{F}[V],\mathbb{F}[V]^G) + \beta_s(\mathbb{F}[W],\mathbb{F}[W]^H) && \text{by (2.14)}\\
&= \beta_r(G) + \beta_s(H) - 2 && \text{by Corollary 2.14}
\end{aligned}$$

□

2.4 The growth rate of β_k

In this section we will study for a fixed commutative graded $\mathbb{F}$-algebra R the behavior of $\beta_k(R)$ as a function of k. The surjection $R_+/R_+^{k+1} \to R_+/R_+^k$ shows that $\beta_k(R) \leq \beta_{k+1}(R)$ for all k. It might seem plausible at first that $\beta_k(R)$ is a strictly increasing function of k, however this is false:

Example 2.16. Consider the ring $R = \mathbb{F}[a,b]/(b^3 - a^9, ab^2 - a^7)$ and define a grading by setting $\deg(a) = 1$ and $\deg(b) = 3$. Then $b^2 \in R_+^2 \setminus R_+^3$, and b^2 spans the degree 6 homogeneous component of R_+^2/R_+^4. In this case for all $l \geq 7$ we have that $R_l \subseteq R_+^5$, hence $6 = \beta_2(R) = \beta_3(R) = \beta_4(R)$.

Lemma 2.17. *$\beta_k(R)$ as a function of k is bounded if and only if there is an integer n such that $R_i = \{0\}$ for all $i \geq n$. In particular if $R_+ \neq \sqrt{0}$ then $\beta_k(R)$ is unbounded.*

Proof. Note that $R_+^{n+1} \subseteq R_{\geq n+1}$. Hence if $R_n \neq \{0\}$, then $R_n \nsubseteq R_+^{n+1}$, implying $\beta_n(R) \geq n$. Conversely, if $R_i = \{0\}$ for all $i \geq n$ then $\beta_i(R) \leq n$. In this case for any $f \in R_+$ there is an integer $r > 0$ such that $r\deg(f) > n$, hence $f^r = 0$, showing that f is nilpotent and that $R_+ \subseteq \sqrt{0}$. □

Lemma 2.18. *For any positive integers $r \leq k$ we have the inequality*

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

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

By Lemma 2.18 the sequence $\frac{\beta_k(G,V)}{k}$ is monotonically decreasing, and as it is also non-negative, it must converge to a certain limit. Our next goal will be to clarify what is the value of this limit.

Definition 2.19. Let R be a graded finitely generated commutative $\mathbb{F}$-algebra with $R_0 = \mathbb{F}$. Set

$$\sigma(R) := \min\{d \in \mathbb{N} : R \text{ is finitely generated as a module over } \mathbb{F}[R_{\leq d}]\}$$

Equivalently, $\sigma(R)$ is the minimal integer d such that $\beta(R, \mathbb{F}[R_{\leq d}])$ is finite.

For any G-module V we write $\sigma(G,V) := \sigma(\mathbb{F}[V]^G)$. This quantity was much studied for G a linearly reductive group (see e.g. [11]), but to our knowledge, the particular case when G is finite has not been considered on its own until yet. Observe first that $\sigma(G,V)$ is finite since by its definition:

$$\sigma(G,V) \leq \beta(G,V) \leq |G| \tag{2.15}$$

We can also set $\sigma(G) := \sup_V \sigma(G,V)$ where V runs through all G-modules. By the above remark $\sigma(G) \leq \beta(G)$. The following gives a more precise result:

Lemma 2.20. *Let $V_1, ..., V_n$ be any G-modules and $W = V_1 \oplus \cdots \oplus V_n$. Then*

$$\sigma(G,W) = \max_{i=1}^{n} \sigma(G,V_i)$$

In particular $\sigma(G) = \max_U \sigma(G,U)$ where U ranges over all isomorphism classes of irreducible G-modules.

Proof. Let $R = \mathbb{F}[W]^G$ and denote by S_i the subalgebra of $\mathbb{F}[V_i]^G$ generated by its elements of degree at most $\sigma(G,V_i)$. As $\mathbb{F}[W] = \otimes_{i=1}^n \mathbb{F}[V_i]$ we get using Lemma 1.4 (3) that $\beta(\mathbb{F}[W], \otimes_{i=1}^n S_i) = \sum_{i=1}^n \beta(\mathbb{F}[V_i], S_i) < \infty$. Since $\otimes_{i=1}^n S_i \subseteq \mathbb{F}[R_{\leq d}]$ where $d := \max_{i=1}^n \sigma(G,V_i)$, it follows by Lemma 1.4 (1) that $\beta(\mathbb{F}[W], \mathbb{F}[R_{\leq d}]) < \infty$, whence $\sigma(G,W) \leq d$ by Definition 2.19.

For the reverse inequality let $T = \mathbb{F}[V_i]^G$ for a fixed i and observe that the restriction gives a graded algebra surjection $\psi : R \to T$. Hence the image under ψ of a finite set of module generators of R over its subalgebra $\mathbb{F}[R_{\leq \sigma(R)}]$ must generate $T = \psi(R)$ as a module over its subalgebra $\psi(\mathbb{F}[R_{\leq \sigma(R)}]) = \mathbb{F}[T_{\leq \sigma(R)}]$, as well. In particular $\sigma(G,V_i) \leq \sigma(G,W)$. □

Corollary 2.21. *If A is an abelian group of exponent* $\exp(A)$ *then*

$$\sigma(A) = \exp(A).$$

Proof. Lemma 2.20 asserts that $\sigma(A) = \max_U \sigma(A, U)$ where U runs through the irreducible representations of A. These are all 1-dimensional (as the base field $\mathbb{F}$ is algebraically closed) and if $U^* = \langle x \rangle$ then $\mathbb{F}[x]^A = \mathbb{F}[x^e]$ where $e \in \mathbb{N}$ is the exponent of the weight of x. This readily implies our claim. □

Proposition 2.22 (Hilbert [27])**.** *The common zero locus of some homogeneous invariants $f_1, ..., f_n \in \mathbb{F}[V]^G$ is $\{0\}$ if and only if the invariant ring $\mathbb{F}[V]^G$ is finitely generated as a module over its subring $\mathbb{F}[f_1, ..., f_n]$.*

Lemma 2.23. *For any G-module V we have $\beta_k(G, V) \geq k\sigma(G, V)$.*

Proof. Let $R := \mathbb{F}[V]^G$ and take homogeneous elements $f_1, \ldots, f_r \in R$ with $\deg(f_i) = \sigma(G, V)$ such that R is a finite module over $\mathbb{F}[R_{\leq \sigma(G,V)-1}, f_1, \ldots, f_r]$. By Proposition 2.22 the common zero locus of $(R_+)_{\leq \sigma(G,V)-1} \cup \{f_1, \ldots, f_r\}$ is $\{0\}$. If $f_i^k \in R_+^{k+1}$, then f_i^k belongs to the ideal generated by $(R_+)_{\leq \sigma(G,V)-1}$, hence the zero locus of f_i contains the common zero locus of $(R_+)_{\leq \sigma(G,V)-1}$. It follows that there is an i such that $f_i^k \notin R_+^{k+1}$, hence $\beta_k(R) \geq k\sigma(R)$. □

Definition 2.24. Let R be a ring as in Definition 2.19. We set:

$$\eta(R) := \beta(R_+, \mathbb{F}[R_{\leq \sigma(R)}])$$

For a G-module V we write $\eta(G, V) := \eta(\mathbb{F}[V]^G)$ and $\eta(G) := \sup_V \eta(G, V)$.

By definition of $\sigma(R)$ the number $\beta(R_+, \mathbb{F}[R_{\leq \sigma(R)}])$ is finite. Moreover by Definition 2.24 any element $f \in R$ with $\deg(f) > \eta(R)$ belongs to the ideal $(R_+)_{\leq \sigma(R)} R_+$. This implies first of all that

$$\beta(R) \leq \eta(R) \tag{2.16}$$

Moreover we know from Lemma 2.17 that an integer k_0 exists such that $\beta_k(R) \geq \eta(R) - \sigma(R)$ holds for any $k \geq k_0$. Hence if $\deg(f) > \beta_k(R) + \sigma(R)$ then $f \in R$ can be written in the form $\sum_i g_i h_i$ where $0 < \deg(g_i) \leq \sigma(R)$ and $\deg(h_i) > \beta_k(R)$, whence $h_i \in R_+^{k+1}$ and $f \in R_+^{k+2}$. This argument shows that for any sufficiently large $k \geq k_0$ we have

$$\beta_{k+1}(R) \leq \beta_k(R) + \sigma(R) \tag{2.17}$$

This simple observation immediately leads us to the following result:

Theorem 2.25. *For any G-module V there are non-negative integers $\beta_0(G, V)$ and $k_0(G, V)$ such that:*

$$\beta_k(G, V) = k\sigma(G, V) + \beta_0(G, V) \quad \text{for every } k \geq k_0(G, V)$$

Proof. Consider the sequence $a_k := \beta_k(G,V) - k\sigma(G,V)$. By (2.17) it is monotonically decreasing and by Lemma 2.23 it is non-negative, therefore it converges to a non-negative limit. But as its elements are integers, in fact it stabilizes after finitely many steps, and this is what has been claimed. □

Corollary 2.26.

$$\lim_{k\to\infty} \frac{\beta_k(G,V)}{k} = \sigma(G,V)$$

Remark 2.27. When $\mathrm{char}(\mathbb{F}) = 0$, then $\beta_k(G) = \beta_k(G, V_{\mathrm{reg}})$ holds for all k by the same argument as in the proof of the special case $k = 1$ in [43] based on Weyl's theorem on polarizations. Hence in this case we have

$$\sigma(G) = \sigma(G, V_{\mathrm{reg}}) = \lim_{k\to\infty} \frac{\beta_k(G, V_{\mathrm{reg}})}{k} = \lim_{k\to\infty} \frac{\beta_k(G)}{k}.$$

In positive characteristic, however, it is unclear wether there is a G-module U such that $\beta_k(G) = \beta_k(G,U)$ holds for every $k \geq 1$. Knop's results in [31] only imply that for any $k \geq 1$ a G-module U_k exists with $\beta_k(G) = \beta_k(G, U_k)$.

Corollary 2.28. *Let G be a finite group and suppose that* $\mathrm{char}(\mathbb{F})$ *does not divide $|G|$. Then for any subgroup H and normal subgroup N of G we have:*

$$\sigma(G) \leq \sigma(G/N)\sigma(N)$$
$$\sigma(H) \leq \sigma(G) \leq [G:H]\sigma(H)$$

Proof. Substitute into the inequality of Lemma 2.3 the linear expression for $\beta_k(G,V)$ given in Theorem 2.25. Then for sufficiently high values of k:

$$k\sigma(G,V) + c_0 = \beta_k(G,V) \leq \beta_{\beta_k(G/N)}(N,V) = \beta_k(G/N)\sigma(N,V) + c_1$$

for some constants c_0, c_1. Our first claim follows after dividing by k and passing to the limit $k \to \infty$; here $\lim_{k\to\infty} \frac{1}{k}\beta_k(G/N) = \sigma(G/N)$ by Remark 2.27, provided that $\mathrm{char}(\mathbb{F}) = 0$. The second claim is proved similarly by substituting the linear expression of $\beta_k(G,V)$ into the inequalities of Lemma 2.9 and Corollary 2.7 and then passing to the limit.

An alternative proof is obtained by adapting the proof of the reduction lemmata for the Noether number to $\sigma(G)$. This works also for $\mathrm{char}(F) > 0$; we omit the details. □

Remark 2.29. This implies in the same way as in Lemma 1.8 that for any subquotient K of G

$$\frac{\sigma(G)}{|G|} \leq \frac{\sigma(K)}{|K|}$$

In the remaining part of this section we will develop a general method for estimating β_k based on the simple idea which lead us to (2.17).

Lemma 2.30. *Let M be a graded module over a graded ring I, and $S \subseteq I$ a graded subalgebra. Then for any integers $k > r \geq 1$ we have*

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

Proof. Let d be greater than the right hand side of this inequality. Then

$$M_d \subseteq M_{\leq \beta(M,S)} S_{>\beta_{k-r-1}(S)} \subseteq M S_+^{k-r} \subseteq M(S_+^{k-r})_{\leq \beta_{k-r}(S)}$$

hence $M_d \subseteq M_{>\beta_r(M,I)} S_+^{k-r} \subseteq M I_+^r S_+^{k-r} \subseteq M I_+^k$, showing that $d > \beta_k(M, I)$. □

Lemma 2.31. *For a G-module V and subgroup $H \leq G$ as in Proposition 2.5 set $L := \mathbb{F}[V]$, $M := L_+/L_+^G L_+$. For any $1 \leq r < [G : H]$ and $s \geq 1$ we have*

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

Proof. We have $\beta(L_+, L^G) = \beta(M, L^G) \leq \beta_{[G:H]}(M, L^H)$ by Corollary 2.7. Applying Lemma 2.30 with $k := [G : H]$, $I := L^H$, $S := \mathbb{F}[R_{\leq s}]$ and noting that $\beta_k(S) \leq ks$ we obtain the above inequality. □

Lemma 2.32. *For a graded algebra I as in Definition 2.19 we have*

$$\beta_k(I) \leq (k - 1)\sigma(I) + \eta(I).$$

In particular, for any G-module V

$$\beta_k(G, V) \leq (k - 1)\sigma(G, V) + \eta(G, V).$$

Proof. Here we apply Lemma 2.30 for $r = 1$, $M := I_+$ and $S := \mathbb{F}[I_{\leq \sigma(I)}]$. Since $\beta(M, S) = \eta(I)$ we have $\beta_k(I) \leq (k-1)\sigma(I) + \max\{\beta(I), \eta(I) - \sigma(I)\}$, and this implies our claim using (2.16). □

In the present section we have generalized, in fact, some notions and results which were already known and much studied for abelian groups. E.g. $\eta(A)$ was originally defined as the smallest length of a sequence over A which guarantees the existence of a "short" zero-sum subsequence, i.e. one with length at most $\exp(A)$ (for some results on $\eta(A)$ see e.g. [21] ch. 5.7). The restriction of Lemma 2.32 to the abelian case appears in [21] as Lemma 6.1.3, and Theorem 2.25 was first proved for the abelian case in [18] Lemma 5.1.

Chapter 3

The semidirect product

The main question guiding our efforts in the present chapter is the following open conjecture reported in [48]:

Conjecture 3.1 (Pawale)**.** *If p, q are odd primes such that $q \mid p-1$ then we have $\beta(Z_p \rtimes Z_q) = p + q - 1$.*

The lower bound $\beta(Z_p \rtimes Z_q) \geq p + q - 1$ holds by Theorem 2.11. At present, however, we cannot prove or disprove that this upper bound holds, we were only able to improve the approximations given in [14] and [38].

3.1 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 identify them with the variables in the coordinate ring $L := \mathbb{F}[V]$. Goebel developed an algorithm for the case when V is a permutation representation (see [22], [33], [12]) 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 extend it to an action on $\mathcal{M}(\hat{A})$ by setting $U^g = (a_1^g, \ldots, a_l^g)$ for any sequence $U = (a_1, \ldots, a_l)$ and $g \in G$. 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 $(\mu_1(S), \ldots, \mu_h(S)) := (|R_1|, ..., |R_h|)$. By the *shape* $\lambda(S)$ of S we mean the l-tuple of such partitions

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

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 $\mathcal{V}$ is explicitly specified, it 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 3.2. 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 3.3. *$L_+ = \mathbb{F}[V]_+$ 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 divisor u of $m = uv$. Then we have

$$\sum_{b \in G/A} u^b v = \tau_A^G(u) v \in L_+^G L_+. \tag{3.1}$$

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 the concept of terminality is rather vacuous: e.g. 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. To exclude these irrelevant cases we assume in the rest of this chapter that

$$\text{no non-identity element of } G/A \text{ fixes any non-trivial element of } \hat{A} \quad (3.2)$$

Remark that (3.2) depends only on the structure of G; an obvious necessary condition for (3.2) 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 (3.2) is equivalent to the requirement that G is a Frobenius group with abelian Frobenius kernel A. In this thesis we will study in greater detail from this class of groups only 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 A_4.

Definition 3.4. 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 3.5. (i) If (3.2) 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 (3.2) 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 3.6. 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.

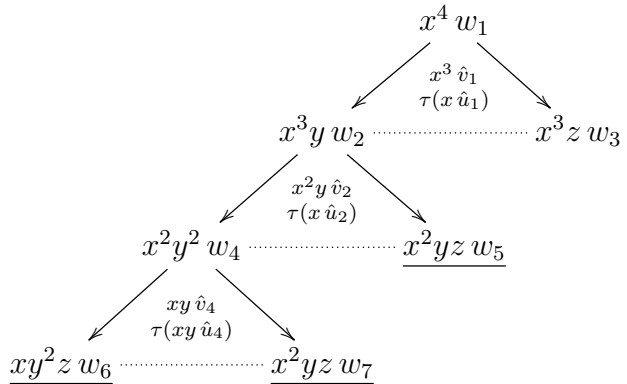
Note that if (3.2) holds, then for any non-trivial 1-dimensional A-module U the G-module $\mathrm{Ind}_A^G(U)$ is irreducible by Mackey's irreducibility criterion (cf. [44] ch. 7.4). Moreover, the set of A-characters occurring in $\mathrm{Ind}_A^G(U)$ coincides with the G/A-orbit of the character of 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.

Proposition 3.7. *Let G be a finite group satisfying* (3.2) *with $A \cong Z_p$ for some prime p. Let V be a G-module and $L := \mathbb{F}[V]$, $R := \mathbb{F}[V]^G$, and $\mathcal{V}$ a 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 $\mathcal{V}$ or b_i while $m_{\mathcal{V}}$ has a gapless divisor of degree at least*

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

Proof. By Lemma 3.3 it suffices to show that for any terminal monomial $m \in L_+$ not divisible by a brick belonging to $\mathcal{V}$ or by 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 $\Phi(m^*)^{O_i} = R_1R_2...R_h$ be the row decomposition of $\Phi(m^*)^{O_i}$, and denote by t the multiplicity of $\theta(x)$ in $\Phi(m_i^*)$. 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 $\Phi(ux) = R_t$. 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 1.15. 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 $\Phi((w^bv)_{\mathcal{V}})^{O_j} = \Phi(m_{\mathcal{V}})^{O_j}$. Moreover, $\mu_s(\Phi((w^bv)_{\mathcal{V}})^{O_i}) \geq \mu_s(\Phi(m_{\mathcal{V}})^{O_i})$ 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 $\sum_{s=1}^t \mu_s(\Phi((w^bv)_{\mathcal{V}})^{O_i}) > \sum_{s=1}^t \mu_s(\Phi((m^*/u)_{\mathcal{V}})^{O_i})$. This contradicts the assumption that m was terminal. □

Example 3.8. Let V be an irreducible representation of $Z_p \rtimes Z_3$ of dimension 3 and $\mathbb{F}[V] = \mathbb{F}[x, y, z]$. The monomials x^4, x^3y, x^2yz, x^2y^2 are representing all the possible shapes of the degree 4 monomials. The diagram below shows how the algorithm given in the proof of Proposition 3.7 rewrites the monomials using relations in R_+L_+ (represented here by triangles) in terms of monomials lower in the $\prec$ ordering (represented here by the arrows).



3.2 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 3.7, 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 3.9. *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. Then in the row decomposition $\Phi(m) = R_1 ... R_h$ we have $|R_{i+1}| < |R_i|$ for every $1 \leq i < h$, and $|R_1| \leq |O| - s$, so $\deg(m) \leq 1 + 2 + ... + (|O| - s) = \binom{|O|-s+1}{2}$. □

Corollary 3.10. *Let $A = Z_p$ and $G = A \rtimes Z_{q^n}$ where Z_{q^n} acts faithfully on A. Setting $r = \frac{p-1}{q^n}$ 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*

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

Proof. By Lemma 2.31 (applied with $s = q$ and $r = 1$) we have $\beta(L_+, R) \leq (q^n - 1)q + \max\{p, \beta(L_+/R_+L_+, S) - q\}$, where $S := \mathbb{F}[I_{\leq q}]$. Apart from $O_0 := \{0\}$, Z_p contains r different Z_{q^n}-orbits $O_1, \ldots, O_r$, each of cardinality q^n, and the bricks different from O_0 are all of size q. Thus $\beta(L_+/R_+L_+, S) \leq \beta(L_+/L_+R_+, \mathcal{B})$, and it is sufficient to show that for $e := \max\{rd + 1, p + d, p + q + 1\}$, $L_{\geq e} \subseteq L_+R_+ + \mathcal{B}$.

Denote by $M^{(i)}$ (resp. $M^{(0)}$) the subspace of $L_{\geq e}$ spanned by monomials u with $|\Phi(u)^{O_i}| > d$ (resp. $|\Phi(u)^{O_0}| \geq 1$). Clearly $L_{\geq e} \subseteq \sum_{i=0}^{r} M^{(i)}$. The A-invariant variables are bricks, so $M^{(0)} \subseteq \mathcal{B}$. Apply Proposition 3.7 with $\mathcal{V}$ the set of variables of weight in O_i for some fixed $i \in \{1, \ldots, r\}$. We obtain that the subspace $M^{(i)}$ is contained in $R_+L_+ + \mathcal{B} + \mathcal{G}_{d+1}(\mathcal{V})$. By Proposition 3.9, $\mathcal{G}_{d+1}(\mathcal{V}) \subseteq \mathcal{B}$, showing that $M^{(i)} \subseteq R_+L_+ + \mathcal{B}$. This holds for all i, hence $L_{\geq e} \subseteq L_+R_+ + \mathcal{B}$. □

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 3.7 all the b_i may be assumed to be A-invariant variables.

Corollary 3.11. *We have the inequality*

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

Proof. Applying Lemma 2.31 with $r = 1$ and $s := \binom{q}{2}$, and using $\beta(L_+, I) \le p$ we get

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

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

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

$$L_{\ge p+s} = N + \sum_{i=0}^{p-1/q} M^{(i)} \tag{3.3}$$

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

By Lemma 1.13 the weight sequence $\Phi(m)$ of a monomial $m \in N$ contains a non-empty zero-sum sequence of length at most $h(m) \le s$, hence $m \in \mathbb{F}[I_{\le s}]_+L_+$. Applying Proposition 3.7 with $\mathcal{V}$ the variables with weight in O_i for a fixed $i \in \{1, \dots, \frac{p-1}{q}\}$, we get $M^{(i)} \subseteq L_+R_+ + \mathcal{G}_{s+1}(\mathcal{V}) + M^{(0)}$, and by Proposition 3.9 we have $\mathcal{G}_{s+1}(\mathcal{V}) \subseteq \mathcal{B}$. Clearly $M^{(0)} \subseteq \mathcal{B}$. It follows by (3.3) that $L_{\ge p+s} \subseteq R_+L_+ + \mathcal{B} + L_+\,\mathbb{F}[I_{\le s}]_+$, and since bricks have degree at most $q \le s$, the inequality $\beta(L_+/R_+L_+, \mathbb{F}[I_{\le s}]) \le p+s$ is proven. □

Remark 3.12. The above results are getting close to the lower bound given in Theorem 2.11 only for small values of q. E.g. by Corollary 3.11 we have $p+2 \le \beta(Z_p \rtimes Z_3) \le p+6$ and $p+3 \le \beta(Z_p \rtimes Z_4) \le p+6$ by Corollary 3.10. For greater values of q the strategy to find a degree bound which guarantees the existence of a brick in a monomial seems to be insufficient.

Proposition 3.13.

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

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 $|S_i| \leq q-1$ for every i.

For each factor m_i we have $h(m_i) \leq |S_i| \leq q-1$, so if $\deg(m) \geq p$ then m contains an A-invariant divisor of degree at most $h(m) \leq q-1$ by Lemma 1.13, which is a contradiction, hence $\deg(m) \leq p-1$. On the other hand, as each factor m_i is gapless, $\deg(m_i) \leq \binom{|S_i|+1}{2} \leq \frac{|S_i|q}{2}$, and consequently

$$\deg(m) \leq \frac{|S|q}{2}. \tag{3.4}$$

We claim that $|S| \leq q + \frac{p-1}{q} - 2$. Write $q^{\wedge}T := \{t_1 + \cdots + t_q \mid t_i \neq t_j \in T\}$ for any subset $T \subseteq \hat{A}$. If our claim were false then we would get from the Dias da Silva - Hamidoune theorem (see Proposition 1.17) that

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

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 (3.4) and taking into account that q is odd we get $\deg(m) \leq \lfloor \frac{q^2-2q+p-1}{2} \rfloor = \frac{1}{2}(p+q(q-2))-1$. □

Proposition 3.14. *Suppose c, e are positive integers such that $c \leq q$ and $\binom{c}{2} < p \leq \binom{c+1}{2} - \binom{e+1}{2}$ (in particular, this forces that $p < \binom{q+1}{2}$). Then*

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

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 $|E| \leq p-1$, for otherwise by Lemma 1.13 we would get an A-invariant divisor of degree at most $c-e$. It follows that $|S_{c-e}| \leq e$, for otherwise the fact that m is gapless and $c \leq q$ would lead to the contradiction

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

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

To illustrate the use of Proposition 3.14 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 $I_{\geq 22} \subseteq I_+R_+ + (\mathcal{G}_{12} \cap I_{\geq 22}) \subseteq I_+R_+ + (I_+)_{\leq 3}I_{\geq 19}$ by Proposition 3.7, hence $I_{\geq 28} \subseteq I_+^3 I_{\geq 19} + I_+R_+$. Furthermore $I_{\geq 19} \subseteq I_+R_+ + (\mathcal{G}_9 \cap I_{\geq 19})$ by Proposition 3.7. A monomial $m \in \mathcal{G}_9 \cap I_{\geq 19}$ has a gapless divisor u of degree at least 9. It is easily seen that $h(u) \leq 3$, hence u can be completed to a monomial $v \mid m$ of degree 11 and height $h(v) \leq 5$, which will contain an A-invariant divisor of degree at most 5 by Lemma 1.13. We get that $I_{\geq 19} \subseteq (I_+)_{\leq 5}I_{\geq 14} + I_+R_+$. Finally $I_{\geq 14} \subseteq I_+^2$ and putting all these together yields $I_{\geq 28} \subseteq I_+^6 + I_+R_+ \subseteq I_+R_+$ by Proposition 2.5. As a result

$$\beta(Z_{11} \rtimes Z_5) \leq 27 \tag{3.5}$$

Proposition 3.15. *For any odd primes p, q such that $q \mid p-1$ we have*

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

Proof. Let d be a positive integer such that $\mathcal{G}_d \subseteq (I_+)_{\leq q}I$. Since $\mathcal{B} \subseteq (I_+)_{\leq q}I$, it follows that $\beta(L_+/R_+L_+, \mathbb{F}[I_{\leq q}]) \leq p + d - 2$ by Proposition 3.7. Using Lemma 2.31 we get that $\beta(L_+, R) \leq (q-2)q + p + d - 2$. Our first two estimates follow by substituting the value of d given in Proposition 3.13. The last one follows similarly by deducing form Proposition 3.14 that we have $\beta(L_+/R_+L_+, \mathbb{F}[I_{\leq c-1}]) \leq 2p - 2$, and then applying Lemma 2.31 again. □

Theorem 3.16. *We have $\gamma(Z_p \rtimes Z_q) < \frac{1}{2}$ where p, q are primes and $q \mid p-1$.*

Proof. By Corollary 3.11 we have $\beta(Z_p \rtimes Z_3) \leq p + 6$, hence $\gamma(G) < \frac{1}{2}$ for $p > 7$. The case $p = 7$ will be treated below, with the result $\beta(Z_7 \rtimes Z_3) = 9$ in Theorem 3.25. For the rest we may assume that $q \geq 5$. Suppose indirectly that $pq \leq 2\beta(Z_p \rtimes Z_q)$. Then by Lemma 1.4 (2) and by the first estimate in Proposition 3.15

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

Suppose first that $4q + 1 \leq p$. In this case $q^2 - 5q + 1 \leq 0$, whence $q < 5$, a contradiction. It remains that $p = 2q+1$. Since by (3.5) our statement is true for $q = 5, p = 11$, it remains that $q \geq 11$ (as $2q + 1$ is not prime for $q = 7$). Then $2p < q(q+1)$, so we can apply the third estimate in Proposition 3.15. 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 $c \geq 7$ as $p \geq 23$, but then by this inequality $q \leq 6$, a contradiction. □

3.3 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

$$W = V_+^{\oplus n_+} \oplus V_-^{\oplus n_-} \oplus V_0 \tag{3.6}$$

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 $\mathbb{F}[W] \cong \mathbb{F}[V_+^{\oplus n_1}] \otimes \mathbb{F}[V_-^{\oplus n_2}] \otimes \mathbb{F}[V_0]$; the degrees of these factors will be denoted by $d_+(m), d_-(m), d_0(m)$. Finally we set $I = \mathbb{F}[W]^{Z_7}, R = \mathbb{F}[W]^G$ and let $\tau = \tau_A^G : I \to R$ denote the transfer map.

Proposition 3.17. *Let $m \in \mathbb{F}[W]$ be a Z_7-invariant monomial such that $\deg(m) \geq 7$, $d_0(m) = 0$ and $d_+(m), d_-(m) \geq 1$. 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 $|S| \geq 2$ 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 $|S| \geq 4$ 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 $\nu_1 \leq 6$, $\nu_3 \leq 2$ and $\nu_5 \leq 4$. 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 $\deg(m) \geq 7$. 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 $|U| \geq 2$ or $|V| \geq 2$ 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 $i, j \geq 1$; but then an integer

$1 \leq n \leq 6$ exists such that $(ab^n)(a^{7i-1}b^{7j-n})$ is a Z_7-invariant factorization, and we are done as before. □

Corollary 3.18. *If $m \in \mathbb{F}[W]$ is a Z_7-invariant monomial of $\deg(m) \geq 10$ such that $d_0(m) \geq 2$ or $d_+(m), d_-(m) \geq 3 - d_0(m)$ then $m \in I_+R_+$.*

Proof. By Corollary 2.7 it is enough to prove that $m \in I_+^4$. This is immediate if $d_0(m) \geq 2$. If $d_0(m) = 1$ then applying Proposition 3.17 two times shows that $m \in I_1I_2^2I_+$. Finally, if $d_0(m) = 0$ then again after two applications of Proposition 3.17 we may suppose that $m = uv$ where $\deg(v) \geq 6$, $d_+(v), d_-(v) \geq 1$ and $u \in I_2^2$. It is easily checked (or deduced from Proposition 1.19) that any irreducible zero-sum sequence over Z_7 of length at least 6 is similar to (1^7) or (1^52), none of which can equal $\Phi(m)$ (for then $d_-(m) = d_-(u) = 2$, a contradiction). Therefore $v \in I_+^2$ follows and again $m \in I_+^4$. □

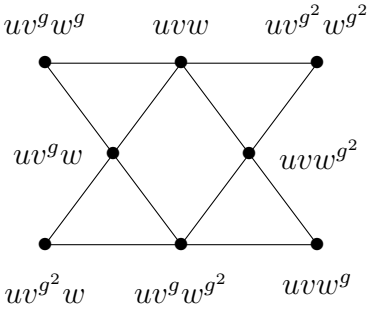
Lemma 3.19. *Let $G = A \rtimes \langle g \rangle$ where $\langle g \rangle \cong Z_3$ and A is an arbitrary abelian group. If $3 \in \mathbb{F}^\times$ then for any $u, v, w \in I_+$ the following relation holds:*

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

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

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

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



□

Proposition 3.20. *Let $m \in \mathbb{F}[W]$ be a Z_7-invariant monomial with the factorization $m_+ = m_1...m_n$ given by the isomorphism $\mathbb{F}[V_+^{\oplus n}] \cong \mathbb{F}[V_+]^{\otimes n}$. If $\deg(m) \geq 10$, $d_0(m) \leq 1$ and $\max_{i=1}^n \deg(m_i) \geq 3$ 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 $d_0(m) \leq 1$ by assumption, using Proposition 3.7 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 $|S| \geq 2$. 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 1.15 $|\Sigma(\Phi(m/tw))| = 7$. This gives an A-invariant factorization $m/w = uv$ such that $xy \mid u$ and $x \mid v$. By Lemma 3.19 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 3.7, 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 3.19. 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 this later monomial already belongs to I_+R_+ by the first part of this paragraph (since $xY^2Z^4 \in I_+^2$). □

Corollary 3.21. *If W is the regular representation V_{reg} of $Z_7 \rtimes Z_3$ then we have $\beta(I_+, R) \leq 9$.*

Proof. Here we have to deal with the case $n_+ = n_- = 3$. Let $m \in I_+$ be a monomial with $\deg(m) \geq 10$. If Corollary 3.18 can be applied then $m \in I_+R_+$ already holds. Otherwise $d_0(m) \leq 1$ and say $d_-(m) \leq 2 - d_0(m)$, whence $d_+(m) \geq 8$. 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 3.20. □

Remark 3.22. Pawale in [38] has proved, in fact for the whole non-modular case, that $\beta(G, W) = 9$ whenever $n_+, n_- = 2$. From this he concluded using Weyl's Theorem on polarization that $\beta(G) \leq 9$ holds in characteristic 0.

Proposition 3.23. *If* $\mathrm{char}(\mathbb{F}) \neq 2, 3, 7$ *then* $\beta(G) \leq 9$.

Proof. We already know that $\beta(G) \leq 13$ from Corollary 3.11. Therefore it is sufficient to show that $R_d \subseteq R_+^2$ whenever $10 \leq d \leq 13$. 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 1.7 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 $\beta(G) \leq \beta(G, V_{\mathrm{reg}}) \leq 9$ by Corollary 3.21.

Finally let $\mathrm{char}(\mathbb{F}) = 5$, so that $\max\{\dim(V_+), \dim(V_-), \frac{\beta(G)}{\mathrm{char}(\mathbb{F})-1}\} \leq 4$. By Proposition 1.7 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 [31] 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), provided that $d_+(f), d_-(f) \leq 3(\mathrm{char}(\mathbb{F}) - 1) = 12$. So for the rest we may suppose that say $d_+(f) \geq 13$. Then take the factorization $f_+ = f_1 f_2 f_3 f_4$ given by the isomorphism $\mathbb{F}[V_+^{\oplus 4}] \cong \mathbb{F}[V_+]^{\otimes 4}$, and observe that $\deg(f_i) \geq 4$ for some $i = 1, ..., 4$, so that $f \in I_+ R_+$ by Proposition 3.20. $\square$

3.4 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 usual $\mathbb{F}[V_+^{\oplus n}] = \otimes_{i=1}^n \mathbb{F}[x_i, y_i, z_i]$ 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:

$$\Delta_{i,j}(I_+ R_+) \subseteq I_+ R_+ \tag{3.7}$$

Proposition 3.24. *If* $\mathrm{char}(\mathbb{F}) = 2$ *then* $\beta(I_+, R) \leq 9$.

Proof. Let $m \in I$ be a monomial with $\deg(m) \geq 10$. It is sufficient to show that $m \in I_+ R_+$. We may suppose by symmetry that $d_+(m) \geq d_-(m)$. It suffices to deal with the cases not covered by Corollary 3.18 so we may suppose that $d_0(m) \leq 1$, $d_-(m) \leq 2 - d_0(m)$, whence $d_+(m) \geq 8$. By Proposition 3.7 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 $\deg(m_i) \geq 3$ for some $i \geq 1$ then $m \in I_+R_+$ by Proposition 3.20. So for the rest we may suppose that $\deg(m_i) \leq 2$ 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 (3.7) 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 3.19 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 1.15, suitable factors u, v must exist

(b) it remains that $d_0(m) = 0$. Again by Proposition 3.7 (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 $\deg(m/f) \geq 8$, the desired factorization of m is given by Lemma 1.15

(d) it remains that $d_0(m) = d_-(m) = 0$ and $\Phi(m/u)$ is an irreducible zero-sum sequence. Since $\deg(m/u) \geq 7$ 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 assure that $(124) \subseteq \Phi(m)$. If $d_0(m) = 0$ then this is achieved using Proposition 3.7. Otherwise, if there is

Z_7-invariant variable w in m then we may still suppose by Proposition 3.7 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 3.19. Now we may suppose that $m = x_1y_2z_3u$, say. We have:

$$\begin{aligned}\Delta_{1,2}z_1x_1y_3u + \Delta_{3,1}z_2x_3y_3u &= (z_1x_2y_3 + 2z_2x_1y_3 + z_2x_3y_1)u \\ &= (z_1x_2y_3 + y_1z_2x_3 + 2x_1y_2z_3)u = m + \tau(x_1y_2z_3)u\end{aligned}$$

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

Comparing Proposition 3.23 and Proposition 3.24 with the lower bound in Theorem 2.11, we have proved:

Theorem 3.25. *If* $\mathrm{char}(\mathbb{F}) \neq 3, 7$ *then* $\beta(Z_7 \rtimes Z_3) = 9$.

3.5 Calculating $\sigma(G)$

Lemma 3.26. *If* $S \cap -S = \emptyset$ *for a non-empty subset* $S \subseteq Z_p$ *and a prime* p *then a zero-sum sequence* T *exists with* $\mathrm{supp}(T) = S$ *and* $|T| \leq p$.

Proof. Write $p = (d+1)s+r$, where $s := |S|$ and $r < s$ while $r, d > 0$. Take an arbitrary subset $R \subseteq S$ with $|R| = r$ and consider the sequence $U := S^dR$. Its support is contained in S, and its length is $p - s$. By the Cauchy-Davenport Theorem we have $|\Sigma(U)| \geq \min\{p, 1 + d(|\Sigma(S)| - 1) + (|\Sigma(R)| - 1)\}$. On the other hand $|\Sigma(S)| \geq 1+s(s+1)/2$ and $\Sigma(R) \geq 1+r(r+1)/2$ by the theorem of Balandraud (see Proposition 1.18). Combining these two we conclude

$$|\Sigma(U)| \geq \min\left\{p, 1 + \frac{ds(s+1)}{2} + \frac{r(r+1)}{2}\right\} \geq \min\{p, (d+1)s + r\} = p$$

Consequently U has a subsequence V with $\theta(V) = -\theta(S)$ and $T := SV$ will be a sequence with the required properties. □

Proposition 3.27. *Let* $G = Z_p \rtimes Z_d$, *where* p *is a prime,* $d > 2$ *is a divisor of* $p - 1$, *and* Z_d *acts faithfully on* Z_p. *Then we have* $\sigma(G) = p$.

Proof. We know that $\sigma(G) \geq \sigma(A) = p$ by Corollary 2.28 and Corollary 2.21. By Lemma 2.20 it is enough to prove that $\sigma(G, U) \leq p$, where U is an irreducible representation of G. Denote by A the maximal normal subgroup Z_p of G. We have already seen in Section 3.1 that G has only two types of irreducible representations: if U is 1-dimensional with Z_p in its kernel, then $\sigma(G, U) \leq |G/A| = |Z_d| \leq p - 1$. Otherwise, the set of weights occurring in U forms a G/A-orbit $O \subseteq \hat{A}$. For every $k \leq |O|$ we choose representatives

$S_{k,1}, ..., S_{k,r_k}$ from each G/A-orbit of the k-element subsets of O. By Lemma 3.26 we can assign to each of them a monomial $m_{S_{k,i}}$ with support $S_{k,i}$ and degree at most p. Now consider the polynomials:

$$f_k = \sum_{i=1}^{r_k} \tau(m_{S_{k,i}}) \qquad \text{for } k = 1, ..., |O| \tag{3.8}$$

They are all G-invariants, moreover, it is easily checked that their common zero locus is $\{0\}$. Indeed, if the vector $u = (u_1, ..., u_{|O|}) \in U$ belongs to this common zero locus, and if the set $S = \{i : u_i \neq 0\}$ has cardinality $k > 0$ then $m_S(u) = f_k(u) = 0$, implying that $u_j = 0$ for an index $j \in S$, which is a contradiction. Consequently $\mathbb{F}[U]^G$ is finitely generated over $\mathbb{F}[f_1, ..., f_{|O|}]$ by Proposition 2.22, hence $\sigma(G, U) \leq \max_k \deg(f_k) \leq p$. □

If $d = 2$ then G is the dihedral group D_{2p} and in fact Proposition 3.27 holds for this case as well, as we shall see later from Corollary 5.5. Using Lemma 2.32 we could estimate $\beta_k(G)$ for $G = Z_p \rtimes Z_q$ if in addition to $\sigma(G)$ the value of $\eta(G)$ would also be know to us. Unfortunately, the approach in Proposition 3.7 is insufficient to achieve this latter goal because the rewriting procedure in its proof uses relations in I_+R_+ instead of relations in $I_+(R_+)_{\leq\sigma(G)}$. This additional combinatorial difficulty was solved only for the particular case studied in the next section.

3.6 The multiplicity free module of $Z_p \rtimes Z_3$

If a G-module V contains every irreducible G-module with multiplicity at most 1 then we say that V is multiplicity free.

Proposition 3.28. *Let $G = Z_p \rtimes Z_3$ where $p \neq 7$ is a prime such that $3 \mid p - 1$. If V is a multiplicity free representation of G not involving 1-dimensional subrepresentations and $I = \mathbb{F}[V]^{Z_p}$, $R = \mathbb{F}[V]^G$ then:*

$$\beta(I_+, R) \leq p.$$

Proof. Let $m \in I$ be a monomial with $\deg(m) \geq p + 1$ and $m = m_1...m_n$ the factorization corresponding to the decomposition $V = V_1 \oplus ... \oplus V_n$ into non-isomorphic irreducible components; here $n = \frac{p-1}{3}$. One of these factors, say m_1 must have degree at least 4. Let $w \mid m_1$ be a divisor such that $\deg(w) = 4$ and $\lambda(w)$ is minimal w.r.t. the ordering defined in Section 3.1. We have several cases:

(i) If $\lambda(w) = (3, 1)$ then w contains the brick $xyz \in R_3$ hence $m \in I_+R_3$

(ii) If $\lambda(w) = (2,2)$, say $w = x^2y^2$ and $-\theta(xy) \in \Sigma(\Phi(m/w))$ then we can find a Z_p-invariant monomial v such that $xy \mid v \mid m$ and the zero-sum sequence $(\theta(xy))\Phi(v/xy)$ is irreducible. We claim moreover that $\deg(v) \leq p$. For otherwise $\deg(v) = p+1$ and $\Phi(v/xy) = (c^{p-1})$ where $c = \theta(xy)$. By the maximality of $\deg(m_1)$ this weight c cannot belong to any irreducible component different from V_1. Moreover, by the minimality of $\lambda(w)$ the weight c must coincide with $\theta(x)$ or $\theta(y)$. But then either $\theta(y) = 0$ or $\theta(x) = 0$, respectively, which is a contradiction. Now set $u = m/v$ and observe that $u\tau(v) \in I_+(R_+)_{\leq p}$ while $m - u\tau(v) \in I_+R_3$ by case (i).

(iii) If $\lambda(w) = (2,2)$ as above, but $-\theta(xy) \notin \Sigma(\Phi(m/w))$ then necessarily $|\Sigma(\Phi(m/w))| \leq p-1$ and since $|\Phi(m/w)| \geq p-3$. Let S denote the support of $\Phi(m/w)$; If $S \cap -S \neq \emptyset$ then $\Phi(m/w)$ contains a subsequence $(s,-s)T$ where $s \in Z_p$ and $|T| = p-5$. Given that $|\Sigma(T)| \geq p-4$ by Lemma 1.15 and $-\theta(xy) \notin \Sigma(T)$, at least one of the weights $-\theta(x), -\theta(y), -\theta(x^2y), -\theta(xy^2)$ must occur in T. Therefore by symmetry in x and y we may assume that $m = uvw$, where u, v, w are Z_p-invariant, $\Phi(v) = (s,-s)$, $x \mid w$, and $xy^2 \mid u$. Here $\deg(vw) \leq 2 + |T| + 3 \leq p$ hence by Lemma 3.19 we conclude that m is congruent modulo $I_+(R_+)_{\leq p}$ to a monomial which falls under case (i).

It remains that $S \cap -S = \emptyset$ hence by a corollary of Balandraud's theorem (see Theorem 8 in [1]) we have $|\Sigma(\Phi(m/w))| \geq 1 + \nu_1 + 2\nu_2 + ... + k\nu_k$ where $\nu_1 \geq ... \geq \nu_k$ are the multiplicities of the different elements of Z_p occurring in $\Phi(m/w)$. Given that $|\Sigma(\Phi(m/w))| \leq p-1$ this forces that $\Phi(m/w)$ must have one the following three forms for some $a, b \in Z_p$:

$$(a^{p-2}) \qquad (a^{p-3}) \qquad (a^{p-4}, b).$$

Here again by the maximality of $\deg(m_1)$ and the minimality of $\lambda(w)$ we may suppose that $a = \theta(x)$ (using also that $p - 4 > 4$ by assumption).

(a) If $\Phi(m/w) = a^{p-2}$ then $\Phi(m) = (a^p, \theta(y)^2)$ and as $\Phi(m)$ is a zero-sum sequence it follows that $\theta(y) = 0$, a contradiction.

(b) If $\Phi(m/w) = a^{p-3}$ then $\Phi(m) = (a^{p-1}, (ra)^2)$ is a zero-sum sequence, where $r := \theta(y)/\theta(x) \in Z_p^\times$. Consequently $-a + 2ra = 0$ whence $2r = 1$. Given that $r^3 = 1 \in Z_p$ it follows that $p = 7$, but this was excluded.

(c) It remains that $\Phi(m/w) = (a^{p-4}, b)$. Here $a \neq \theta(xy)$ as $\theta(y) \neq 0$, thus the sequence $S := (a^{p-4}, b, \theta(xy))$ has height $h(S) = p-4$. Therefore a nonempty zero-sum sequence $T \subseteq S$ exists, for otherwise if S were zero-sum free then by the Freeze-Smith Lemma (see 1.16) we get that $\Sigma(S) \geq 2|S| - h(S) + 1 = p+1$, a contradiction. Moreover T cannot contain $\theta(xy)$ since we assumed that $-\theta(xy) \notin \Sigma(\Phi(m/w))$. It follows

that $T = (a^t, b)$ for some $0 \leq t \leq p-4$. Here $t \neq 0$ since $b \neq 0$. Similarly $t \neq p-4$, for otherwise $\theta(x^2y^2) = 0$ whence $\theta(x) = -\theta(y)$ follows, in contradiction with the fact that the variables x and y belong to the same representation V_1. This way we obtained a factorization $m = uv$ where $\Phi(v) = T$ and $u\tau(v) \in I_+(R_+)_{\leq p-4}$ while in the same time $m - u\tau(v) \in I_+R_3 + I_+(R_+)_{\leq p}$ by case (ii) or (i).

(iv) If $\lambda(w) = (2,1,1)$, say $w = x^3y$: Here $\theta(x^2y) \neq \theta(x)$, for otherwise $\theta(x) = -\theta(y)$, a contradiction as above. Moreover $\theta(xy)$ is different from both $\theta(x^2y)$ and $\theta(x)$, for otherwise we would get $\theta(x) = 0$ or $\theta(y) = 0$. Now we have two cases:

(a) If $\Sigma(\Phi(m/w))$ contains $-\theta(x^2y)$ or $-\theta(x)$ then we get a Z_p-invariant factorization $m = uv$ such that $x^2y \mid u$ and $x \mid v$. Here we can assure in addition that v is irreducible, so that $\deg(v) \leq p$. Then $u\tau(v) \in I_+(R_+)_{\leq p}$ while the monomials occurring in $m - u\tau(v)$ both fall under case (iii), (ii) or (i), and we are done.

(b) If however $\{-\theta(x), -\theta(x^2y)\} \notin \Sigma(\Phi(m/w))$ then $|\Sigma(\Phi(m/w))| \leq p-2$; as $|\Phi(m/w)| \geq p-3$ by assumption, this situation is only possible in view of Lemma 1.15 if $|\Phi(m/w)| = p-3$ while $|\Sigma(\Phi(m/w))| = p-2$. Using Vosper's Theorem (see Section 1.4) it follows that $\Sigma(\Phi(m/w))$ is an arithmetic progression and $\Phi(m/w) = (-a^i, a^{p-2-i})$ for some $a \in Z_p^\times$ and $0 \leq i \leq p-2$. It is also necessary that $-\theta(xy) \in \Sigma(\Phi(m/w))$, so a factorization $m = uv$ exists such that $xy \mid v$ and v is an irreducible Z_p-invariant monomial, whence $xy \neq v$ and $\deg(v) \leq \max\{i+2, p-i\} \leq p$. Therefore $u\tau(v) \in I_+(R+)_{\leq p}$ and the monomials occurring in $m - u\tau(v)$ both fall under case (iv/a), so we are done.

(v) $\lambda(w) = (1,1,1,1)$, say $w = x^4$: then $|\Sigma(\Phi(m/x^2))| = p$ by Lemma 1.15, so that $-\theta(x) \in \Phi(m/x^2)$ and this gives us then a Z_p-invariant factorization $m = uv$ such that $x \mid u$, $x \mid v$, and v is irreducible, hence $u\tau(v) \in I_+(R_+)_{\leq p}$ whereas the monomials in $m - u\tau(v)$ both fall under cases (i)–(iv). □

Theorem 3.29. *Let $G = Z_p \rtimes Z_3$ where $p \neq 7$ is a prime such that $3 \mid p-1$. If V is the multiplicity free representation of G then $\eta(G,V) \leq p+2$ and*

$$\beta_k(G,V) = kp + 2$$

Proof. We know from Theorem 2.11 that $\beta_k(G,V) \geq kp+2$ so it suffices to prove the converse. Let $m \in \mathbb{F}[V]^{Z_p}$ be a monomial with $\deg(m) \geq p+3$. Corresponding to the decomposition $V = V^A \oplus U$, where U contains no 1-dimensional irreducible representations of G, we have a factorization $m = vu$

where $v \in \mathbb{F}[V^A]$ and $u \in \mathbb{F}[U]$. If $\deg(v) \geq 3$ then $v \in I(R_+)_{\leq 3}$ whence $m \in I_+(R_+)_{\leq 3}$. Otherwise $\deg(u) \geq p+1$ hence by Proposition 3.28 we get $m \in I_+R_3 + I_+(R_+)_{\leq p}$. In both cases after applying the surjective R-homomorphism $\tau : I \to R$ we arrive to the conclusion that $\tau(m) \in R_+R_{\leq p}$. This shows that $\eta(G,V) \leq p+2$. Now taking into account that $\sigma(G) = p$ by Proposition 3.27 and using Lemma 2.32 we get that:

$$\beta_k(G,V) \leq (k-1)\sigma(G) + \eta(G,V) \leq (k-1)p + p + 2 = kp + 2 \qquad \square$$

Chapter 4

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 A, conjugation by g permutes them cyclically. Remark for future reference that the only irreducible zero-sum sequences over 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

$$(0)^q(a, a)^r(b, b)^s(c, c)^t(a, b, c)^e \qquad \text{where } e = 0 \text{ or } 1. \tag{4.1}$$

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 and it is generated over any field $\mathbb{F}$ with $\mathrm{char}(\mathbb{F}) \neq 2, 3$ by the matrices:

$$a \mapsto \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}, \quad b \mapsto \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}, \quad g \mapsto \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

Let x, y, z denote the corresponding basis in V^* and following our conventions introduced in Section 3.1 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. As usual, we write $I := \mathbb{F}[W]^A$, $R := \mathbb{F}[W]^G$ and $\tau := \tau_A^G : I \to R$ for the transfer map.

4.1 Calculating $\sigma(A_4)$ and $\eta(A_4)$

Proposition 4.1. *$\mathbb{F}[V]^G$ has an h.s.o.p. consisting of the invariants*

$$p_2 = \tau(x^2), \quad p_3 = xyz, \quad p_4 = \tau(x^2y^2)$$

Moreover $\mathbb{F}[V]^G = P \oplus sP$ where $P = \mathbb{F}[p_2, p_3, p_4]$ and $s = \tau(x^4y^2)$.

Proof. Consider a monomial $m \in \mathbb{F}[V]_+^A$ such that $\tau(m) \notin P$. In particular $p_3 \nmid m$, so we may suppose by (4.1) that $m = x^{2i}y^{2j}$. If $i, j \geq 2$ then $m = u^2v$ where $u = x^2y^2$ and the relation $\tau(m) = p_4\tau(uv) - p_3^2\tau(x^2v + y^2v) \in P$ leads to a contradiction. So we may suppose by symmetry that $j \leq 1$. Now if $i \geq 3$ then using the relation $\tau(m) + \tau(y^2m/x^2) + \tau(z^2m/x^2) = p_2\tau(m/x^2) \in P$ we reduce our case to the monomials my^2/x^2 and mz^2/x^2, for which $j - i$ is strictly smaller, and this way we get back to the case $i, j \geq 2$. So it remains that $i = 2$ and $\tau(m) = s$ hence $\mathbb{F}[V]^G$ is generated as P-module by 1 and s.

Finally, p_2, p_3, p_4 are algebraically independent since p_2, p_3^2, p_4 are the elementary symmetric polynomials in the ring $\mathbb{F}[x^2, y^2, z^2]$. □

Corollary 4.2. $\sigma(A_4) = 4$

Proof. We see from the explicit list of the primary invariants p_2, p_3, p_4 that $\sigma(A_4, V) = 4$. Moreover for any 1-dimensional representation U of A_4 we have $\sigma(A_4, U) = 3$ or 1. Hence our claim follows by Lemma 2.20. □

Proposition 4.3. $\beta_k(A_4, V) \geq 4k + 2$

Proof. Taking over the notations of Proposition 4.1 we claim that the invariant sp_4^{k-1} of degree $4k + 2$ does not belong to R_+^{k+1}. For suppose indirectly that this is false, i.e. that sp_4^{k-1} is the linear combination of some products $f_1 \cdots f_{k+1}$ where each $f_i \in R_+$ is homogeneous. Now observe that necessarily an index j exists such that $\deg(f_j) \leq 3$, for otherwise $\deg(f_1 \cdots f_{k+1}) \geq 4(k + 1)$ whereas $\deg(sp_4^{k-1}) = 4k + 2$. But it can be seen from Proposition 4.1 that any homogeneous element of degree at most 3 in R_+ must be a constant multiple of p_2 or p_3, which readily implies that:

$$sp_4^{k-1} \in p_2R + p_3R$$

By the uniqueness of the Hironaka-decomposition in Proposition 4.1 we conclude that $p_4^{k-1} \in p_2P + p_3P$, that is to say p_4^{k-1} belongs to the ideal of P generated by p_2 and p_3. This however contradicts the fact that p_2, p_3, p_4 are algebraically independent. This proves that $sp_4^{k-1} \notin R_+^{k+1}$. □

Proposition 4.4. *Suppose that* $\mathrm{char}(\mathbb{F}) \neq 2, 3$. *Then* $\eta(A_4, U \oplus V^{\oplus 3}) \leq 6$.

Proof. It is sufficient to show that $I_{\geq 7} \subseteq (R_+)_{\leq 4} I + (I_+)_{\leq 4} R$. Take a monomial $m \in I_{\geq 7}$ with $\deg(m_+) \geq 7$. We claim that in this case $m \in I_+(R_+)_{\leq 4}$. 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 $\deg(m_1) \geq 3$. If the G-invariant $x_1 y_1 z_1$ divides m then we are done. Using relation (3.1) 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 3.19 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 $\deg(m) \geq 8$ 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 3.19 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 $\deg(m_+) \leq 6$. If we have $\deg(m_0) \geq 3$ then $m_0 \in (R_+)_{\leq 3} I$ and we are done. So for the rest $\deg(m_0) \leq 2$. Given that $\mathsf{D}(A) = 3$ and $\mathsf{D}_2(A) = 5$ by Proposition 1.10, we have $m \in I_1 (I_+)^3_{\leq 3} I$ or $m \in I_1^2 (I_+)^2_{\leq 3} I$. In both cases $m \in I_+^4$ hence $m \in I_+ R_+$ by Proposition 2.5. Taking into account that $\deg(m) \leq 8$ we conclude that $m \in (R_+)_{\leq 4} I + (I_+)_{\leq 4} R$, as claimed. □

Theorem 4.5. *If* $\mathrm{char}(\mathbb{F}) \neq 2, 3$ *then* $\eta(A_4) = 6$ *and* $\beta_k(A_4) = 4k + 2$.

Proof. Consider the subalgebra $S := \mathbb{F}[U \oplus V^{\oplus 3}]^G$ in $R := \mathbb{F}[U \oplus V^{\oplus n}]^G$ (where $U = U^A$ and $n \geq 3$). By Corollary 2.7 we have $\beta(G) \leq \mathsf{D}_3(A) = 7$. Note that $\beta(S) \leq \eta(S) \leq 6$ by Proposition 4.4. 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. [49]) and in positive characteristic for $d \leq \dim(V)(\mathrm{char}(\mathbb{F}) - 1)$ by Theorem 5.1 and formula (6.3) in [31]; in our case $\dim(V)(\mathrm{char}(\mathbb{F}) - 1) \geq 12$. It follows that $R_7 = \mathbb{F}[\mathrm{GL}_n \cdot S_7] \subseteq \mathrm{GL}_n \cdot S_+^2 \subseteq R_+^2$, whence $\beta(A_4) \leq 6$.

Next we show that $\eta(R) \leq 6$, i.e. that $R_{\geq 7} \subseteq (R_+)_{\leq 4} R$. Given that R is generated by elements of degree at most 6, it is sufficient to prove that $\bigoplus_{d=7}^{12} R_d \subseteq (R_+)_{\leq 4} R$. Applying polarization as above and Proposition 4.4 we obtain $\bigoplus_{d=7}^{12} R_d \subseteq \mathbb{F}[\mathrm{GL}_n \cdot \bigoplus_{d=7}^{12} S_d] = \mathbb{F}[\mathrm{GL}_n \cdot (S_+)_{\leq 4} S] \subseteq (R_+)_{\leq 4} R$ as desired. Now the lower bound $\beta_k(A_4) \geq 4k + 2$ is given by Proposition 4.3, while $\beta_k(A_4) \leq (k-1)\sigma(A_4) + \eta(A_4) = 4k + 2$, by Lemma 2.32. □

Remark 4.6. Working over the field of complex numbers Schmid [43] already gave a computer assisted proof of the equality $\beta(A_4, U \oplus V^{\oplus 2}) = 6$.

Corollary 4.7. *Suppose that* $\mathrm{char}(\mathbb{F}) \neq 2, 3$. *Then* $\beta(\tilde{A}_4) = 12$.

Proof. We have $\beta(A_4) = 6$ by Theorem 4.5, and since $\tilde{A}_4$ has a two-element normal subgroup N with $\tilde{A}_4/N \cong A_4$, the inequality $\beta(\tilde{A}_4) \leq 12$ follows by

Lemma 1.8. It is sufficient to prove the reverse inequalities in characteristic zero (as $\beta(G,0) \leq \beta(G,p)$, see Section 1.2). Consider the ring of invariants of the 2-dimensional complex representation of $\tilde{A}_4$ realizing it as the binary tetrahedral group. It is well known (see for example the first row in the table of Lemma 4.1 in [28] or Section 0.13 in [39]) that this algebra is minimally generated by three elements of degree $6, 8, 12$, whence $\beta(\tilde{A}_4) \geq 12$. □

4.2 The group $(Z_2 \times Z_2) \rtimes Z_9$

Proposition 4.8. *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 $\beta(G) \leq 17$.*

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 abelian normal subgroup $A := K \times C$ where $C := \langle g^3 \rangle \cong Z_3$. For an arbitrary G-module W we set $J = \mathbb{F}[W]^C$, $I = \mathbb{F}[W]^A$, $R = \mathbb{F}[W]^G$; we use the transfer maps $\mu : J \to R$, $\tau : I \to R$. 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 1.8 we have $\beta(G) \leq 18$. Therefore by Lemma 3.3 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 2.2 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 1.10), and consequently $\tau(m) \in R_+^2$ again by Proposition 2.2.

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

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

Observe that the first factor has degree 6, hence it corresponds to a zero-sum sequence over A. By Definition 3.2 we get a good divisor which contradicts the assumption that m was terminal. □

Chapter 5

Extensions of Z_2 by an abelian group

In this chapter we present some techniques which are more efficient than the rewriting procedure in Proposition 3.7 for the particular case when $G/A \cong Z_2$ acts by an involution on the abelian normal subgroup $A \triangleleft G$.

5.1 Groups of dihedral type

Definition 5.1. A sequence C over an abelian group A is called a *zero-corner* if C has a factorization $C = EFH$ into non-empty subsequences E, F, H such that EF and EH are zero-sum sequences. We denote by $\rho(C)$ the minimal value of $\max\{|EF|, |EH|, |FH|\}$ over all factorizations $C = EFH$ satisfying the above properties, and we call it the *diameter* of C.

Lemma 5.2. *Let $S = (s_1, \ldots, s_l)$ be a sequence over A consisting of non-zero elements. Suppose that S contains a maximal zero-sum free subsequence of length $d \leq l - 3$. Then S contains a zero-corner C with $\rho(C) \leq d + 1$.*

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

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

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

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

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

We turn now to the group $G = A \rtimes_{-1} Z_2$ where A is a non-trivial abelian group and $Z_2 = \langle b \rangle$. Keeping conventions, notations and terminology introduced in Sections 1.3 and 3.1, let W be a G-module over $\mathbb{F}$, $I = \mathbb{F}[W]^A$, $R = \mathbb{F}[W]^G$ and $\tau : I \to R$ is the transfer map.

Proposition 5.3. *For any monomial $m \in I$ and integer $k \geq 0$ it holds that $m \in I_+ R_+^k$ provided that*

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

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

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

$$2m = \tau(ef)hr + \tau(eh)fr - \tau(fh^b)e^b r. \tag{5.1}$$

After division by $2 \in \mathbb{F}^\times$ we get from (5.1) that $m \in I_{\geq \deg(m)-d}(R_+)_{\leq d}$. Given that $\deg(m) - d \geq (k-1)\,\mathsf{D}(A) + 2$ by assumption, the induction hypothesis applies, whence $I_{\geq \deg(m)-d} \subseteq R_+^{k-1} I_+$ and $m \in I_+ R_+^k$ as claimed. Suppose next that condition (i) holds. If m contains three A-invariant variables, then $\Phi(m)$ contains the zero corner $(0, 0, 0)$ with diameter 2, hence we are back in case (ii). Otherwise $\Phi(m)$ contains a subsequence of length at least $k\,\mathsf{D}(A)$ of non-zero elements. If $k > 1$, then by Lemma 5.2 $\Phi(m)$ has a zero-corner of diameter at most $\mathsf{D}(A)$, so again we are back in case (ii). It remains that $k = 1$. If m contains one or two A-invariant variables, then $m \in I_+^3 \subseteq I_+ R_+$ by Corollary 2.7. Otherwise m contains a subsequence of length at least $\mathsf{D}(A) + 2$ of non-zero elements, hence by Lemma 5.2 $\Phi(m)$ contains a zero-corner of diameter at most $\mathsf{D}(A)$. We are done by case (ii). □

Theorem 5.4. *Let $G = A \rtimes_{-1} Z_2$ and suppose $|G| \in \mathbb{F}^\times$. Then*

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

Proof. Since $I_d \subseteq I_+ R_+^k$ for $d \ge k\,\mathsf{D}(A)+2$ by Proposition 5.3, it follows that $\beta_k(I_+, R) \le k\,\mathsf{D}(A) + 1$. The lower bound is given by Theorem 2.11 and by Lemma 1.4 (2). □

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

Corollary 5.5. *For the dihedral group D_{2n} of order $2n$ and an arbitrary positive integer k we have $\beta_k(D_{2n}) = nk + 1$, provided that $2n \in \mathbb{F}^\times$.*

The special case $k = 1$ of Corollary 5.5 is due to Schmid [43] when $\mathrm{char}(\mathbb{F}) = 0$ and to Sezer [45] in non-modular positive characteristic.

5.2 Extremal invariants

Definition 5.6. Let $R = \mathbb{F}[W]^G$; a monomial $u \in \mathbb{F}[W]^A$ will be called (k, ε)-*extremal with respect to* τ_A^G if $\deg(u) \ge \beta_k(G) - \varepsilon$ while $\tau_A^G(u) \notin R_+^{k+1}$. A sequence S over $\hat{A}$ is (k, ε)-extremal if there is a G-module V and a monomial $m \in \mathbb{F}[V]^A$ with $\Phi(m) = S$ such that m is (k, ε)-extremal with respect to τ_A^G. A $(k, 0)$-extremal monomial or weight sequence is also called k-*extremal*.

Proposition 5.7. *Let $G := D_{2n}$ be the dihedral group of order $2n$, $(n \ge 3)$. A sequence over $A := Z_n$ is k-extremal with respect to τ_A^G only if it has the form $(0, a^{kn})$ for some $\langle a \rangle = Z_n$.*

Proof. Let $m \in \mathbb{F}[W]^A$ be a monomial of $\deg(m) = \beta_k(D_{2n}) = kn + 1$ such that $\tau_A^G(m) \notin R_+^{k+1}$. If m is divisible by the product of two weight zero variables, then $m \in R_+ I_{\ge kn-1}$ by Proposition 2.5. Since $kn - 1 > \beta_{k-1}(D_{2n})$, we get $\tau_A^G(m) \in R_+ \tau_A^G(I_{>\beta_{k-1}(D_{2n})}) \subseteq R_+^{k+1}$, a contradiction. It remains that the multiplicity of 0 in $\Phi(m)$ is at most one. Let $H \subseteq Z_n$ be the set of nonzero values occurring in $\Phi(m)$. Suppose $|H| \ge 2$; if $\Phi(m)$ contains a zero-corner of the form $(w, w, -w)$ with diameter 2, then $\tau(m) \in R_+^{k+1}$ by Proposition 5.3 (ii), a contradiction. We are done if $n = 3$, so assume for the rest that $n \ge 4$. Then $\Phi(m)$ contains a zero-sum free subsequence of length 2, consisting of two distinct elements. By Lemma 1.16 this extends to a maximal zero-sum free subsequence of length at most $n - 2$. If $k > 1$ or $0 \notin \Phi(m)$, then $\tau(m) \in R_+^{k+1}$ by Lemma 5.2 and Proposition 5.3, a contradiction. If $k = 1$ and $0 \in \Phi(m)$, then $m \in I_+^3$, hence $\tau(m) \in R_+^2$ by Proposition 2.2, a contradiction again. Consequently $|H| = 1$ and $\Phi(m) = (0, a^{kn})$. Taking into account Proposition 2.2, a must have order n, whence our claim. □

We can even obtain some information on the case $\varepsilon > 0$, provided that $n = p$ is a prime:

Proposition 5.8. *Let $p \geq 5$ be a prime and $\varepsilon \leq \frac{p-3}{2}$. A (k, ε)-extremal weight sequence with respect to $\tau_{Z_p}^{D_{2p}}$ has row-decomposition $\Phi(m) = S_1...S_h$ where $h \geq kp - 2\varepsilon$, $|S_j| = 1$ for all $j \geq p - \varepsilon - 1$ and $\theta(S_i) \neq 0$ for all $i \geq 1$.*

Proof. The same argument as in the beginning of the proof of Proposition 5.7 shows that the multiplicity of 0 in $\Phi(m)$ is at most 1.

Let S_1^* be the sequence obtained form S_1 by deleting the occurrences of 0. Consider the truncated sequence $T := S_1^* S_2 ... S_{p-\varepsilon-1}$. If $|T| \geq p$, then T contains by Lemma 1.13 a zero-sum sequence $C = (s_1, ..., s_r)$ where $s_n \in S_{i_n}$ for each $n = 1, ..., r$ and some indices $1 \leq i_1 < ... < i_r \leq p - \varepsilon - 1$, so in particular $r \leq p - \varepsilon - 1$. Given that p is a prime, it is impossible that $s_1 = ... = s_n$, hence there is a smallest index t such that $s_t \neq s_1$. But as $s_t \in S_t \subseteq S_1^*$ the sequence $(s_t)C$ forms a zero-corner of diameter at most r. As a result $\tau(m) \in R_+^{k+1}$ by Proposition 5.3, a contradiction. Hence $|T| \leq p - 1$. It follows that $|S_{p-\varepsilon-1}| = 1$, for otherwise we would have $|T| \geq 2(p - \varepsilon - 1) = p + 1$, a contradiction. Hence each row S_i for $i \geq p - \varepsilon - 1$ must consist of the same non-zero element $a \in Z_p$. We get in addition that $h(S) \geq h(T) + (\deg(m) - 1 - |T|) \geq kp - 2\varepsilon$. We have also seen that $\theta(S_h) \neq 0$. Now suppose indirectly that $\theta(S_i) = 0$ for some $i \leq h - 1$. Let $S_i = S_{i1}...S_{in}$ be a decomposition into irreducible zero-sum sequences; by changing indices we may suppose that $S_h \subseteq S_{i1}$. Then the sequence $S_h S_{i1}$ is a zero-corner of diameter $\rho \leq |S_{i1}| \leq \frac{p-1}{2}$ (since $p \geq 5$), hence again $\tau(m) \in R_+^{k+1}$ by Proposition 5.3, a contradiction. □

5.3 The group $Z_p \rtimes Z_4$, where Z_4 acts faithfully

Proposition 5.9. *Let $G := A \rtimes Z_4$ where $Z_4 = \langle b \rangle$ and $A = Z_p$ for an odd prime p such that 4 divides $p - 1$, and conjugation by b is an order 4 automorphism of A. Suppose that* $\mathrm{char}(\mathbb{F}) \neq 2, p$. *Then $\beta(G) \leq \frac{3}{2}(p + 1)$.*

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

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

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

We need to show that $R_d \subseteq R_+^2$ for $d \geq p+4+\varepsilon$, where $\varepsilon = \frac{p-3}{2}$. We know that R_d is spanned by its elements of the form $\tau(m)$ where $m \in I_d$ is a monomial. Given that $\beta_2(D_{2p}) - d \leq 2p+1-(p+4+\varepsilon) = \varepsilon$, we may suppose that m is $(2,\varepsilon)$-extremal with respect to μ, for otherwise we have $\mu(m) \in J_+^3$, whence $\tau(m) = \nu(\mu(m)) \in R_+^2$ by Proposition 2.2 applied for G/D_{2p} acting on J. Proposition 5.8 describes the weight sequence of m and its row-decomposition $S_1...S_h$: we get first of all that $h \geq 2p - 2\varepsilon = p+3$ and that $|S_h| = |S_{h-1}| = 1$. Moreover as $\theta(S_i) \neq 0$ for every i, we get by Lemma 1.15 that the sequence $(\theta(S_1), ..., \theta(S_{h-2}))$ contains a subsequence of total weight equal to $-\theta(S_h)$. Note that $\mathrm{Stab}_{\langle b \rangle}(S_h) = \{1\}$ so we get a factorization $m = uv$, where u is a good divisor as in Definition 3.2. Hence by relation (3.1) we can express m modulo I_+R_+ as a linear combination of monomials $u^b v$ which are not $(2,\varepsilon)$-extremal with respect to μ by the above description, whence $\tau(m) \in R_+^2$ follows. □

Remark 5.10. We already knew from Remark 3.12 that $\beta(Z_p \rtimes Z_4) \leq p+6$. Proposition 5.9 is an improvement on this only for $p = 5$.

5.4 The contraction method

Let $C \leq A$ be a subgroup of an abelian group A. If $S = (s_1, ..., s_d)$ is a sequence over A, then $(s_1 + C, ..., s_d + C)$ is a sequence over A/C which will be denoted by S/C. Suppose that $\theta(S) \in C$; a *C-contraction* of S is a sequence over C of the form $(\theta(S_1), ..., \theta(S_l))$ where $S = S_1...S_l$ and each S_i/C is an irreducible zero-sum sequence over A/C; so indeed $\theta(S_i) \in C$. The relevance of this notion stems from the following observation:

Lemma 5.11. *Let $C \leq A \leq G$ be groups such that A is abelian and $C \lhd G$. Let V be a monomial representation of G in which A is mapped to diagonal matrices. Then a G/C-equivariant $\mathbb{F}$-algebra epimorphism $\pi : \mathbb{F}[U] \to \mathbb{F}[V]^C$ exists in which any monomial $m \in \mathbb{F}[V]^C$ has a preimage $\tilde{m} \in \pi^{-1}(m)$ with $\Phi(\tilde{m})$ equal to an arbitrarily prescribed $\widehat{A/C}$-contraction of $\Phi(m)$.*

Proof. By assumption V^* has a basis $x_1, ..., x_n$ consisting of A-eigenvectors which are permuted up to scalars by G. Let M be the set of C-invariant monomials in these variables, and $E \subset M$ the subset of the irreducibles among them, i.e. which cannot be factored into two non-trivial C-invariant monomials. $\mathbb{F}[V]^C$ is minimally generated as an algebra by E. Moreover the factor group G/C has an inherited action on $\mathrm{Span}_{\mathbb{F}}(M)$, which maps $\mathrm{Span}_{\mathbb{F}}(E)$ to itself. Define U as the dual of the G/C-invariant subspace $\mathrm{Span}_{\mathbb{F}}(E)$. E is a basis of this vector space, hence E is identified with the set

of variables in $\mathbb{F}[U]$. The $\mathbb{F}$-algebra epimorphism $\pi : \mathbb{F}[U] \to \mathbb{F}[V]^C$ taking a variable to the corresponding irreducible C-invariant monomial is G/C-equivariant. Now let $(\theta(S_1), ..., \theta(S_l))$ be an arbitrary $\widehat{A/C}$-contraction of $\Phi(m)$ for a monomial $m \in \mathbb{F}[V]^C$. By definition this means that $m = m_1...m_l$ where each m_i is an irreducible C-invariant monomial with $\Phi(m_i) = S_i$. Hence for each i there are variables $y_1, ..., y_l \in \mathbb{F}[U]$ such that $\pi(y_i) = m_i$ by construction, and the monomial $\tilde{m} := y_1...y_l$ has the required property. □

Using this map π we can derive information on the generators of $\mathbb{F}[V]^G$ from our preexisting knowledge about the generators of $\mathbb{F}[U]^{G/C}$. As an example of this principle, we will study here the group $G := Z_r \rtimes_{-1} Z_{2n}$ where r and $2n$ are coprime, and $r \geq 3$. The center of G is $C = Z_n$ and G/C is isomorphic to the dihedral group D_{2r} whose extremal monomials were described before. G also has an abelian normal subgroup $A = Z_{rn} \geq C$ such that $G/A \cong Z_2 = \langle b \rangle$. We will write $S \sim S'$ for two sequences over $\hat{A}$ if $S = EF$ and $S' = E^b F$ for a zero-sum sequence E of length at most n.

Proposition 5.12. *If S is a k-extremal sequence over $\hat{A}$ then any $\widehat{A/C}$-contraction of any sequence $S' \sim S$ is a k-extremal sequence over $\widehat{A/C}$.*

Proof. Since S is a k-extremal sequence, there is a G-module V and a monomial $m \in \mathbb{F}[V]^A$ such that $\Phi(m) = S$ and m is k-extremal with respect to τ_A^G. Let $\pi : \mathbb{F}[U]^{A/C} \to \mathbb{F}[V]^A$ denote the restriction of the map constructed in Lemma 5.11 to the A-invariants, and consider the transfer maps $\tilde{\tau} : \mathbb{F}[U]^{A/C} \to \mathbb{F}[U]^{G/C}$, $\tau : \mathbb{F}[V]^A \to \mathbb{F}[V]^G$. The G/C-equivariance of π implies that $\tau\pi = \pi\tilde{\tau}$. Suppose first that S has a non-k-extremal C-contraction $\tilde{S}$. Since $|\tilde{S}| \geq \frac{1}{n}|S|$ where we have $|S| = \beta_k(G) \geq knr + 1$ by Theorem 2.11, it follows that $|\tilde{S}| \geq kr + 1 = \beta_k(G/C)$. So for the monomial $\tilde{m} \in \mathbb{F}[U]$ with $\pi(\tilde{m}) = m$ and $\Phi(\tilde{m}) = \tilde{S}$, which exists by Lemma 5.11, we have $\tilde{\tau}(\tilde{m}) \in (\mathbb{F}[U]_+^{G/C})^{k+1}$. But then $\tau(m) = \pi(\tilde{\tau}(\tilde{m})) \in (\mathbb{F}[V]_+^G)^{k+1}$, a contradiction.

Now suppose that a sequence $S' = E^b F$ has a C-contraction $\tilde{S}$ which is not k-extremal, where $0 < |E| \leq n$. Then take a factorization $m = uv$ with $\Phi(u) = E$ and $\Phi(v) = F$. By the previous argument $\tau(u^b v) \in (\mathbb{F}[V]_+^G)^{k+1}$. By Lemma 2.3 and Corollary 5.5 we have $\beta_k(G) \leq \beta_{\beta_k(D_{2r})}(C) = nrk + n$, hence $\deg(v) = \deg(m) - |E| \geq \beta_k(G) - n \geq nrk + 1 - n > nr(k-1) + n \geq \beta_{k-1}(G)$. Consequently $\tau(v) \in (\mathbb{F}[V]_+^G)^k$ and $\tau(m) = \tau(u)\tau(v) - \tau(u^b v) \in (\mathbb{F}[V]_+^G)^{k+1}$, a contradiction again. □

Lemma 5.13. *Let S be a zero-sum sequence over $\hat{A} = Z_{rn}$ having length $l \geq nrk + 1$, where $k \geq 1$, and $n, r \geq 3$ are coprime. If any Z_r-contraction of any sequence $S' \sim S$ is similar to $(0, n^{rk})$ then S is similar to $(0, 1^{nrk})$.*

Proof. By assumption any Z_r-contraction of S must have length $l := rk+1$. By Lemma 1.22 then $S = T_1...T_l$ where $T_i/Z_r = (e^n)$ for every $i \leq l-2$ and some generator e of $Z_{rn}/Z_r \cong Z_n$, while $||T_{l-1}/Z_r||_e = ||T_l/Z_r||_e = n$. As $l \geq 4$ we may assume that $\theta(T_1) \neq 0$ and let $i \neq 1$ be any other index for which $\theta(T_i) \neq 0$. Take an arbitrary element $x \in T_i$ and let $U \subseteq T_1$ be an arbitrary subsequence of length $d := ||x + Z_r||_e < n$. After exchanging the proper subsequences U and (x) in T_1 and T_i the resulting $\tilde{T}_1$ and $\tilde{T}_i$ projects to zero-sum sequences over Z_n, so we get another Z_r-contraction of S:

$$(\theta(\tilde{T}_1), \theta(T_2), ..., \theta(\tilde{T}_i), ..., \theta(T_l)) = (0, n^{rk-2}, n-\delta, n+\delta)$$

where $\delta := \theta(U) - x$. By assumption this must be similar to $(0, n^{rk})$ which is only possible if they are actually equal (here we used that $l \geq 4$). Therefore $\delta = 0$ and $x = \theta(U)$. As this holds for any subsequence $U' \subseteq T_1$ of the same length $d < |T_1|$, necessarily $T_1 = (f^n)$ for some $f \in Z_{nr}$ such that $f + Z_r = e$. Moreover, as $x = \theta(U) = df$, we get by the definition of d and $||x||_f$ that

$$||x||_f = ||x + Z_r||_e \tag{5.2}$$

for every $x \in T_i$, where i differs from that unique index s for which $\theta(T_s) = 0$. Observe on the other hand that (5.2) cannot be true for every element $y \in T_s$, for otherwise $||T_s||_f = ||T_s/Z_r||_e = n$, which is impossible, as $||T_s||_f$ must be a multiple of nr. Now suppose that $|T_s| \geq 2$ and that (5.2) fails for $y \in T_s$. Then swapping y with a proper subsequence $U \subseteq T_1$ of length $||y + Z_r||_e$ we get as before that $\delta := \theta(U) - y = -nf$, whence $||y||_f = ||y + Z_r||_e + n(r-1)$. On the other hand if $z \in T_s$ is a second element besides y for which (5.2) fails, then in particular $(yz) \neq T_s$, as otherwise calculating $||z||_f$ by the same argument yields that $||T_s||_f = ||T_s/Z_r||_e + 2n(r-1) = n(2r-1)$, which is not a multiple of nr. Now swapping (yz) with a proper subsequence of T_1 of length $||yz + Z_r||_e$ gives a Z_r-contraction of S of the form $(2n, -n, n^{rk-2})$ which is not similar to $(0, n^{rk})$. This contradiction shows that y is unique with the property that $||y||_f \neq ||y + Z_r||_e$. So if $|T_s| \geq 3$ then the sequence S' obtained from S by replacing T_s with T_s^b will not satisfy this requirement, hence S' will have Z_r-contractions not similar to $(0, n^{rk})$, which is a contradiction as $S' \sim S$. It remains that $|T_s| = 2$ and $T_s = (-y, y)$. Then necessarily $s \in \{l-1, l\}$. If moreover $y \neq -f$ then $n(r-1) < ||y||_f < nr-1$ and consequently we have the factorization $T_s T_1 = (-y, y, f^n) = (y, f^{nr-||y||_f})(-y, f^{||y||_f - n(r-1)})$ which leads us back to the case when $|T_s| \geq 3$. Finally, if $y = -f$ then observe that $f^b \neq \pm f$, as we have $n > 2$; hence after replacing T_s with $T_s^b \neq (-f, f)$ we get back to the case when $y \neq -f$.

As a result of these contradictions we excluded that $|T_s| \geq 2$. Therefore $|T_s| = 1$ and $T_s = (0)$. Then we must have $|T_i| = n$ for every $i \neq s$ whence $|T_i/Z_r| = (e^n)$ follows. Using (5.2) this implies that $S = (0, f^{nrk})$. □

Theorem 5.14. *For the group $G = Z_s \times (Z_r \rtimes_{-1} Z_{2^{n+1}})$, where $r \geq 3$, $n \geq 1$ and r, s are coprime odd integers, we have $\beta_k(G) = 2^n srk + 1$, except if $s = n = 1$, in which case $\beta_k(G) = 2rk + 2$.*

Proof. $\beta_k(G)$ is the length of a sequence S over $A := Z_{2^n sr}$ which is k-extremal with respect to τ_A^G. By Proposition 5.12 any Z_r-contraction of any sequence equivalent to S must be k-extremal with respect to $\tau_{Z_r}^{D_{2r}}$, hence it is similar to $(0, (2^n s)^{rk})$ by Proposition 5.7. Therefore S is similar to $(0, 1^{2^n srk})$ by Lemma 5.13, provided that $2^n s \geq 3$; in particular $\beta_k(G) = |S| = 2^n srk+1$.

For the case $s = n = 1$ we have $\beta_k(Z_r \rtimes_{-1} Z_4) \leq 2\beta_k(D_{2r}) = 2r + 2$ by Lemma 2.3 and Corollary 5.5. To see the reverse inequality consider the representation on $V = \mathbb{F}^2$ of G given by the matrices:

$$A = \begin{pmatrix} \omega & 0 \\ 0 & \omega^{-1} \end{pmatrix} \qquad B = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \tag{5.3}$$

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

5.5 The quaternion group

The dicyclic group Dic_{4n} is defined for any $n > 1$ by the presentation

$$Dic_{4n} = \langle a, b : a^{2n} = 1, b^2 = a^n, a^b = a^{-1} \rangle$$

In particular for $n = 2$ we retrieve the quaternion group $Q = Dic_8$.

Proposition 5.15. *We have $\beta_k(Dic_{4n}) = 2nk+2$ for $n > 1$ even and $k \geq 1$. Moreover if $(r, 4n) = 1$ then $1 \leq \beta_k(Z_r \times Dic_{4n}) - 2nrk \leq 2$.*

Proof. Taking ω a primitive $2n$-th root of unity in (5.3), the same argument as in the proof of Theorem 5.14 shows that $\beta_k(Dic_{4n}) \geq 2nk + 2$. Moreover for $G := Z_r \times Dic_{4n}$ we have $\beta_k(G) \geq 2rnk + 1$ by Theorem 2.11. Observe that $G/Z(Dic_{4n})$ is isomorphic to $Z_r \times D_{2n}$, respectively to $Z_{2r} \times Z_2$ for $n = 2$. Combining Lemma 2.3 with Corollary 5.5, respectively with Proposition 1.10 leads to the inequality $\beta_k(G) \leq 2nrk + 2$. □

Proposition 5.16. *Let $Q = \langle a, b\rangle$ be the quaternion group where $A := \langle a\rangle$ is isomorphic to Z_4. If S is a zero-sum sequence over $\hat{A}$ of length $4k+2$ which is k-extremal with respect to τ_A^Q then $S = (1^t, 3^s)$ where $t \neq s$.*

Proof. Set $I = \mathbb{F}[V]^A$, $R = \mathbb{F}[V]^Q$ and let $S = (0^x, 2^y, 1^t, 3^s)$ be the weight sequence of a monomial $m \in I$ of degree $4k+2$ such that $\tau(m) \notin R_+^{k+1}$. By replacing m with m^b, if needed, we may suppose that $t \geq s$. We will use induction on $t-s$. Suppose first that $t-s \leq 4$ and consider the factorization $S = (22)^{\lfloor y/2\rfloor}(13)^s(0)^x T$. If y is odd then necessarily $T = (211)$ and $x \geq 1$, hence $m \in I_+^{2k+1}$, which is a contradiction by Corollary 2.7. If however y is even then either T is empty, and then $m \in I_+^{2k+1}$ again, or else $T = (1111)$; in this later case if $x \geq 2$ then again $m \in I_+^{2k+1}$ or otherwise, taking into account that $|S|$ is even, it remains that $x = 0$ and $S = (2^y, 1^{s+4}, 3^s)$. Now, if $y > 0$ then take a factorization $m = uv$ such that $\Phi(u) = (211)$ and observe that $\tau(m) = \tau(u)\tau(v) - \tau(u^b v) \in R_+^{k+1}$, because on the one hand $\deg(v) = 4k-1 > \beta_{k-1}(Q)$, while on the other hand $\Phi(u^b v) = (2^y)(13)^{s+2}$, hence $u^b v \in I_+^{2k+1}$ by what has been said before. From this contradiction we conclude that $y = 0$ and $S = (1^{s+4}, 3^s)$ whenever $t - s \leq 4$ holds.

Finally, if $t - s > 4$ we have a factorization $m = uv$ with $\Phi(u) = (1111)$, and since $\tau(m) = \tau(u)\tau(v) - \tau(u^b v) \notin R_+^{k+1}$ by assumption, it is necessary that either $\tau(v) \notin R_+^k$, when $\Phi(v) = (1^{t-4}, 3^s)$ by the induction hypothesis, or $\tau(u^b v) \notin R_+^k$, when similarly $\Phi(u^b v) = (1^{t-4}, 3^{s+4})$, and in both cases $\Phi(m) = (1^t, 3^s)$, as claimed. □

Theorem 5.17. *Let $G = Z_p \times Q$ for an odd prime p. Then $\beta_k(G) = 4pk+1$ for every $k \geq 1$.*

Proof. Here the distinguished abelian normal subgroup is $A := C \times B \cong Z_{4p}$, where $C := Z_p \lhd G$ and $B := \langle a\rangle$. Set $L := \mathbb{F}[V]$ and $R := L^G$. We write $\theta|_C$ and $\theta|_B$ for the restriction of the character $\theta \in \hat{A}$ to C or B, respectively, and we define accordingly $S|_C$ and $S|_B$ for any sequence S over $\hat{A}$; note that $\theta = (\theta|_C, \theta|_B)$ by the natural isomorphism $\hat{A} \cong \hat{C} \times \hat{B}$.

We already proved in Proposition 5.15 that $1 \leq \beta_k(G) - 4kp \leq 2$. Suppose for contradiction that there is a G-module V and a monomial $m \in \mathbb{F}[V]^A$ with $\deg(m) = 4pk+2$ and $\tau_A^G(m) \notin R_+^{k+1}$. Given that the restriction of τ_B^Q to L^A coincides with τ_A^G, the sequence $\Phi(m)|_B$ is kp-extremal: indeed, otherwise $\tau_B^Q(m) \in (L_+^Q)^{kp+1}$ as $\deg(m) = \beta_{kp}(Q)$, and since $(L_+^Q)^{kp+1} \subseteq R_+^k L_+^Q$ by Proposition 2.5, we get that $\tau_A^G(m) = \tau_B^Q(m) \in (R_+^k L_+^Q) \cap R_+$, but for any $f \in (R_+^k L_+^Q) \cap R_+$ we have $f = \frac{1}{[G:B]}\tau_A^G(\tau_B^A(f)) \in \tau_A^G(R_+^k \tau_B^A(L_+^Q)) \subseteq R_+^{k+1}$, a contradiction. As a result $\Phi(m)|_B = (1^t, 3^s)$ by Proposition 5.16, where $t > s$ can be assumed and $t + s = 4pk+2$. Accordingly m has a factorization

$$m = m_1 \cdots m_l \tag{5.4}$$

where $\Phi(m_i)|_B = (1,3)$ for $i \le s$ and $\Phi(m_i)|_B = (1^4)$ for $s < i \le l$, so that $l = s + \frac{t-s}{4}$. Consider the sequence $S := (\theta(m_1)|_C, ..., \theta(m_l)|_C)$; it contains at most one occurrence of 0, for otherwise $m \in (L_+^A)^2 L^A_{\ge 4pk-6} \subseteq R_+ L^A_{>\beta_{k-1}(G)}$ by Proposition 2.5, hence $\tau_A^G(m) \in R_+^{k+1}$, a contradiction. Moreover S cannot be factored into $2k+1$ zero-sum sequences over $\hat{C}$, for otherwise $\tau_A^G(m) \in R_+^{k+1}$ follows again as $m \in (L_+^A)^{2k+1} \in R_+^k L_+^A$.

We claim that $\{1, ..., l\}$ can be partitioned into two disjoint, non-empty subsets U, V such that the monomials $u = \prod_{i\in U} m_i$ and $v = \prod_{i\in V} m_i$ are A-invariant, $\tau_A^G(u^b v) \in R_+^{k+1}$ and $\deg(v) > 4p(k-1) + 2 \ge \beta_{k-1}(G)$. Under these assumptions $\tau_A^G(m) = \tau_A^G(u)\tau_A^G(v) - \tau_A^G(u^b v) \in R_+^{k+1}$, since $\tau_A^G(v) \in R_+^k$ and this will refute our indirect hypothesis.

We will prove our claim by induction on $\frac{t-s}{4}$. Suppose first that $\frac{t-s}{4} = 1$, i.e. $l = 2pk$. Then $\theta(m_1)|_C = ... = \theta(m_l)|_C$ for otherwise S could be factored into $2k+1$ zero-sum sequences. Observe that if x is a variable in m_i and y is a variable in m_j where $i \ne j$ and $\theta(x)|_B = \theta(y)|_B$, then $\theta(x) = \theta(y)$, since otherwise swapping the variables x and y yields another factorization as in (5.4) where $l = 2pk$ but not all $\theta(m_i)|_C$ are equal. We conclude that $\Phi(m) = (e^{2pk+3}, (3e)^{2pk-1})$ for some generator e of $\hat{A}$. Then $U := \{1, ..., p\}$, $V := \{p+1, ..., l\}$ is the required bipartition, since $\Phi(u^b v)$ is not similar to $\Phi(m)$ and consequently $\tau_A^G(u^b v) \in R_+^{k+1}$ by the above considerations.

For the rest it remains that $\frac{t-s}{4} > 1$, hence $\Phi(m_{l-1})|_B = \Phi(m_l)|_B = (1^4)$. If $\theta(m_i) = 0$ for some $i > s$, say $i = l$, then choosing $U = \{l\}$ gives the required factorization: indeed, $\Phi(u^b v)|_B = (1^r, 3^s)$ where $r - s < t - s$ and consequently $\tau_A^G(u^b v) \in R_+^{k+1}$ by induction on $\frac{t-s}{4}$. If however S contains at least $p+1$ non-zero elements then using Lemma 1.15 we get a subset $I \subset \{1, ..., l-2\}$ such that $|I| \le p-1$ and $\theta(\prod_{i\in I} m_i) = -\theta(m_l)$. Now set $U := I \cup \{l\}$, $V := \{1, ..., l-1\} \setminus I$ and observe that $\Phi(u^b v)|_B = (1^r, 3^s)$ where $r - s < t - s$. So we are done as before, provided that $|U| \le p-1$ or there is an index $i \in U$ such that $i \le s$, because this guarantees that $\deg(u) \le 4p-2$.

Otherwise it remains that $l = p+1$, $s = 1$ and $\theta(m_1) = 0$. Here $m_1 = xy$, where $\theta(x)|_B = 1$ and $\theta(y)|_B = 3$. If there is a variable z in $m_2 \dots m_l$ with $\theta_C(z) \ne \theta_C(x)$, then by swapping the variables x and z we get back to a case considered already. Thus $\Phi(m/y) = ((1,c)^{4p+1})$ for a non-zero element $c \in \hat{C} \cong Z_p$, and $\theta(y) = (3, -c)$. Here $U := \{1\}$, $V := \{2, ..., l\}$ is the required bipartition, because $\Phi(u^b v) = ((1,-c), (3,c), (1,c)^{4pk})$, and since $c \ne -c$ it follows by the above considerations that $\tau_A^G(u^b v) \in R_+^{k+1}$. □

5.6 Groups with a cyclic subgroup of index two

Proposition 5.18 (Burnside 1894, [4] Theorem 1.2, [5] ch. IV.4)**.** *If G is a finite p-group with a cyclic subgroup of index p then it is one of the following:*

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

Throughout this section let H be one of the 2-groups in the above list, $\langle a \rangle$ an index 2 subgroup in H, and $b \in H \setminus \langle a \rangle$, so that $H = \langle a, b \rangle$. If H is a 2-group as in case (3)–(6) of Proposition 5.18 then for any odd integer $r > 1$ it is customary to denote by M_{r2^n}, D_{r2^n}, SD_{r2^n}, Dic_{r2^n} the group $Z_r \rtimes_{-1} H$, where $b \in H$ acts on Z_r by inversion $x \mapsto x^{-1}$ and $\langle a \rangle$ centralizes Z_r.

Proposition 5.19. *Any finite group containing a cyclic subgroup of index two is isomorphic to*

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

where r, s are coprime odd integers, and H is a 2-group in Proposition 5.18.

Proof. Let G be a finite group with an index two cyclic subgroup C. Then C uniquely decomposes as $C = Z_m \times Z_{2^{n-1}}$ for some odd integer $m > 0$ and $n \geq 1$. As Z_m is a characteristic subgroup of C, it is normal in G. Thus by the Schur-Zassenhaus theorem $G = Z_m \rtimes H$ for a Sylow 2-subgroup H of G. Moreover, the characteristic direct factor $Z_{2^{n-1}}$ is also normal in G, hence we may suppose that it is identical to the index two cyclic subgroup $\langle a \rangle \leq H$ (as the automorphism group of H acts transitively on the set of index two subgroups of H). Now Z_m decomposes uniquely as a direct product $Z_m = P_1 \times \cdots \times P_l$ of its Sylow subgroups. After a possible renumbering we may assume that H centralizes $P_1, \ldots, P_t$, and $H/\langle a \rangle$ acts on $P_{t+1}, \ldots, P_l$ via the automorphism $x \mapsto x^{-1}$. Setting $Z_s := P_1 \times \cdots \times P_t$, $Z_r := P_{t+1} \times \cdots \times P_l$ we obtain the desired conclusion. □

Theorem 5.20. *If G is a non-cyclic group with a cyclic subgroup of index two then*

$$\beta_k(G) = \frac{1}{2}|G|k + \begin{cases} 2 & \text{if } G = Dic_{4n},\ n \text{ even} \\ & \text{or } G = Z_r \rtimes_{-1} Z_4,\ r \text{ odd} \\ 1 & \text{otherwise} \end{cases}$$

Proof. If G is any group with a cyclic subgroup $A = \langle a \rangle$ of index 2, then Theorem 2.11 gives us the following lower bound:

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

To establish the precise value of the generalized Noether number β_k for these groups, by Proposition 5.19 we will have to consider the groups of the form $G := Z_s \times (Z_r \rtimes_{-1} H)$ where H is one of the groups of order 2^n listed in Proposition 5.18. In all these cases $\beta_k(G) \leq \beta_{sk}(Z_r \rtimes_{-1} H)$ by Lemma 2.3.

(1) If $H = Z_{2^n}$ then by Theorem 5.14 we have $\beta_k(G) = 2^{n-1}rsk+1$ except if $n = 2$ and $s = 1$, in which case $\beta_k(G) = 2^{n-1}rsk + 2$

(2) If $H = Z_2 \times Z_{2^{n-1}}$ by the isomorphism $Z_r \rtimes_{-1} (Z_2 \times Z_{2^{n-1}}) \cong Z_{2^{n-1}} \times D_{2r}$ we get from the application of Lemma 2.3 and Corollary 5.5 that

$$\beta_k(G) \leq \beta_{sk}(Z_{2^{n-1}} \times D_{2r}) \leq \beta_{2^{n-1}sk}(D_{2r}) \leq 2^{n-1}rsk + 1 \tag{5.5}$$

(3) If $H = M_{2^n}$ then the group $Z_r \rtimes_{-1} M_{2^n} = M_{2^n r}$ will contain a subgroup $C = \langle a^2, b \rangle \cong Z_{2^{n-2}} \times D_{2r}$. The subgroup $N := Z_s \times C$ has index 2 in G and falls under case (2), hence by Lemma 2.3 and case (2) we heave

$$\beta_k(G) = \beta_{2k}(N) = 2^{n-1}krs + 1 \tag{5.6}$$

(4) If $H = D_{2^n}$ then $G = Z_s \times D_{2^n r}$ and we are done by Corollary 5.5

(5) If $H = SD_{2^n}$ then the group $Z_r \rtimes_{-1} SD_{2^n} = SD_{2^n r}$ contains a subgroup $B = \langle a^2, b \rangle \cong D_{2^{n-1}r}$. Observe that B is a normal subgroup, as it has index 2, hence by Lemma 2.3 and Corollary 5.5 we get that

$$\beta_k(G) \leq \beta_{sk}(SD_{2^n r}) \leq \beta_{2sk}(D_{2^{n-1}r}) \leq 2^{n-1}rsk + 1 \tag{5.7}$$

(6) If $H = Dic_{2^n}$ then for $n = 2$ we get back to case (2), as $Dic_4 = Z_2 \times Z_2$; if however $n \geq 3$ then the quaternion group Q is a subgroup of index $2^{n-3}r$ in $Z_r \rtimes_{-1} H$, therefore by Proposition 5.15 we have $\beta(G) = 2^n rsk + 2$ if $s = 1$ and for $s > 1$ we get using Corollary 2.7 combined with Theorem 5.17 that for any prime p dividing s:

$$\beta_k(G) \leq \beta_{k2^{n-3}r}(Z_s \times Q) \leq \beta_{k2^{n-3}rs/p}(Z_p \times Q) \leq 2^{n-1}rsk + 1 \tag{5.8}$$

With this all possibilities are accounted for and our claim is established. □

Chapter 6

Classification of the groups with large Noether number

6.1 A structure theorem

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

Theorem 6.1. *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 $\tilde{A}_4$ (the binary tetrahedral group);*
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 group $Z_p \rtimes Z_q$, where p, q are odd primes and $q \mid p-1$;*
   (c) *$Z_p \rtimes Z_4$, where 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 group $(Z_2 \times Z_2) \rtimes Z_9$.*

The proof of this theorem relies on some classic results due to Burnside and Zassenhaus which we shall reproduce here along with their proofs for the reader's convenience.

Lemma 6.2 (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.*

Proof. Suppose P is of order 2^n. If n = 0, there is nothing to prove. Consider the permutation action of G on itself by left multiplication. An element of order 2^n is a product of an odd number of 2^n-cycles, so is an odd permutation. Hence $H := G \cap A_{|G|} \neq G$ is a subgroup of index 2 in G. H has a cyclic Sylow 2-subgroup of order 2^{n-1}, so by induction $H = N \rtimes P_0$ for P_0 a cyclic subgroup of order 2^{n-1} and N a normal subgroup of H of odd order. Since N is the unique maximal subgroup of odd order in H, N is also normal in G. Taking P to be any Sylow 2-subgroup containing P_0, one has $G = N \rtimes P$. □

Proposition 6.3 (Zassenhaus, Satz 6 in [50])**.** *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.*

Proof. Let $\langle a \rangle \leq P$ be the cyclic subgroup of index 2. If $G = P$ then we can take $K = \langle a \rangle$. If P is cyclic then $G = N \rtimes P$ by Lemma 6.2 and we can take $K = N \rtimes \langle a \rangle$. So for the rest we may assume that $G \neq P$ and that P is non-cyclic. Let $M \lhd G$ be a minimal nontrivial normal subgroup. As G is solvable, M is an elementary abelian p-group. If p is odd then G/M has a Sylow 2-subgroup isomorphic to P, hence by induction on the group order we get a normal subgroup K/M in G/M such that $(G/M)/(K/M) = G/K$ is isomorphic to Z_2, A_4 or S_4, and the Sylow 2-subgroup of K/M, isomorphic to the Sylow 2-subgroup of K, is cyclic, so we are done. It remains that for any of its possible choices M is a 2-group, so that $M \leq P$. The order of $M/M \cap \langle a \rangle \cong M\langle a \rangle/\langle a \rangle$ is 1 or 2, hence M is either Z_2 or $Z_2 \times Z_2$:

(1) if $M = Z_2$ then $M \neq P$, since P was assumed to be non-cyclic. So we can apply again induction to the factor G/M and obtain a subgroup $K \lhd G$ as above. By Lemma 6.2 the odd order elements in K/M constitute a characteristic subgroup N/M which is then normal in G/M. Given that $\mathrm{Aut}(Z_2)$ is trivial, M is in the center of G, hence $N = M \times O$, where O consists of the odd order elements of K. But then O must be trivial, for otherwise it would contain a minimal normal subgroup of G of odd order, which is excluded at this point. Consequently $N = M$ and K/M is a 2-group, whence K is a 2-group, as well. Since we assumed that $G \neq P$, the factor G/K can only be A_4 or S_4. In both cases G/K has a non-cyclic Sylow 2-subgroup, which is only possible if the 2-group K is cyclic, and with this we are done.

(2) if $M = Z_2 \times Z_2$ then P/M must be cyclic, so we can apply Lemma 6.2 this time to the group G/M: as a result we get that P/M has a direct complement N/M consisting of the odd order elements of G/M. Since $G \neq P$ it is necessary that $N \neq M$. Again, M is self-centralizing in N, for otherwise we could find in G a non-trivial minimal normal subgroup of odd order, as before. Given that $N/C_N(M)$ is isomorphic to a subgroup of $\mathrm{Aut}(Z_2 \times Z_2) = S_3$ we conclude that $N/M = Z_3$ and $N = A_4$. Finally, consider the centralizer $C_G(N)$: it is disjoint from N since $C_G(N) \cap N \leq Z(A_4) = \{1\}$. Moreover $C_G(N)$ is trivial, for otherwise it would contain a nontrivial minimal normal subgroup of G which is not of odd order, hence G would contain a subgroup isomorphic to $M \times Z_2$, but this is excluded by the structure of the Sylow 2-subgroup P. Therefore $C_G(N) = \{1\}$, indeed, and since $G/C_G(N)$ is a subgroup of $\mathrm{Aut}(A_4) = S_4$, we get that G equals A_4 or S_4. □

Lemma 6.4 (Roquette [41], see also [4] Lemma 1.4 or III. 7. 6 in [29])**.** *If G is a finite p-group which does not contain a normal subgroup isomorphic to $Z_p \times Z_p$, 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 $Q = Dic_{2^3}$.*

Proof. Let $A \lhd G$ be a maximal cyclic normal subgroup and suppose that $A \neq G$. We claim first that $|A| \geq p^2$; for otherwise if $|A| \leq p$ then the center of G/A contains a cyclic subgroup of order p, whose inverse image at the surjection $G \to G/A$ is a normal subgroup of order $p|A|$, which is not isomorphic to $Z_p \times Z_p$ by assumption, hence it is cyclic, in contradiction with the maximality of A.

Secondly, we claim that A has index p in G. For suppose this is false and let H be the unique subgroup of A of order p^2. Then $G/C_G(H)$ is isomorphic to a subgroup of $\mathrm{Aut}(Z_{p^2}) = Z_{p(p-1)}$, hence $[G : C_G(H)] \leq p$. But since $[G : A] \geq p^2$ by our indirect hypothesis, it follows that A is a proper subgroup of $C_G(H)$. Again let B be the inverse image in $C_G(H)$ of a central subgroup of order p in $C_G(H)/A$. By maximality of A, the group B is not cyclic, but it contains the cyclic subgroup A of index p. Therefore B is isomorphic to one of the non-cyclic groups listed in Proposition 5.18 above. Moreover, H is central in B, hence the center of B has order at least p^2, which is only possible if B is isomorphic to M_{p^n} $(n \geq 4)$ or $Z_p \times Z_{p^{n-1}}$. In both cases B contains a characteristic subgroup isomorphic to $Z_p \times Z_p$, which is then normal in G, contrary to our assumption.

So we have proved that G contains a cyclic subgroup of index p, hence it is one of the groups listed in Proposition 5.18. However, the group M_{p^n} does contain a normal subgroup isomorphic to $Z_p \times Z_p$. It follows that G must be cyclic when $p > 2$, and if $p = 2$ and $n > 3$ then G can also be one of the groups D_{2^n}, SD_{2^n} or Dic_{2^n}. □

Corollary 6.5. *Any finite 2-group G falls under case (1), (2a) or (3a) of Theorem 6.1.*

Proof. Suppose that (1) does not hold for G. Then by Lemma 6.4, 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 6.4 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 noncylic 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 6.6. *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 6.1.*

Proof. By a theorem of Burnside (see p. 163 in [7]) 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 6.7. *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 6.1.*

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 6.6 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 $G/\Phi(C)$

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 6.1 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 6.4. As G does not fall under case (1) or (3b), its order is even by Proposition 6.6. Finally, as G does not fall under case (2a) or (3a), its Sylow 2-subgroup contains a cyclic subgroup of index 2 by Corollary 6.5. Therefore Proposition 6.3 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 6.2, $K = N \rtimes Q$, 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. 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 6.7.

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 $G = P \rtimes Z_3$. Take its presentation $P = \langle a, b \rangle$ given in Proposition 5.18: 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. 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 $M \leq N$ would exists 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 the 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 6.1 for non-solvable groups. Suppose to the contrary that Theorem 6.1 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 6.1 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 6.1, (2) or (3) holds for H, hence it holds also for G, a contradiction.

The minimal simple groups were determined by Thompson. According to Corollary 1 in [47], 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 one of (2a), (2b), (3) holds, hence G/N can not be isomorphic to any of them.

The group $L_2(2^p)$ contains as a subgroup the additive group of the field of 2^p elements. Hence when $p \geq 3$ 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. It turns out that the involutions plus the identity constitute the center, the center has order q, see for example [25], [8]. It follows that the Sylow 2-subgroup Q of $Sz(2^p)$ (p an odd prime) properly contains an elementary abelian 2-group of rank p in its Sylow 2-subgroup, hence (2a) holds for it. □

Remark 6.8. It is shown in [2] using the classification of finite simple groups that every non-abelian simple group contains a minimal simple group. Our proof however does not rely on this fact.

6.2 Proof of the classification theorem

Proof of Theorem 1.1. It suffices to consider the cases listed in Theorem 6.1:

1. if G contains a subgroup of index at most 2 then $\gamma(G) \geq \frac{1}{2}$ by Lemma 2.9
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 1.11 and Corollary 2.7
   $$\gamma(G) \leq \frac{1}{8k}\beta_k(Z_2 \times Z_2 \times Z_2) = \frac{1}{4} + \frac{3}{8k}$$
   (b) $H \cong Z_p \times Z_p$ then by Proposition 1.10 and Corollary 2.7
   $$\gamma(G) \leq \frac{1}{kp^2}\beta_k(Z_p \times Z_p) = \frac{1}{p} + \frac{p-1}{kp^2}$$
   (c) $H \cong A_4$ then by Theorem 4.5 and Corollary 2.7
   $$\gamma(G) \leq \frac{1}{12k}\beta_k(A_4) = \frac{1}{3} + \frac{1}{6k}$$

   It is easily checked that in all three cases the inequality $\gamma(G) \geq \frac{1}{2}$ 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 2.3 we have $\beta_k(\tilde{A}_4) \leq 2\beta_k(A_4)$ hence $\beta(G) \leq \beta_k(\tilde{A}_4) \leq 8k + 4$ by Corollary 2.7 and Theorem 4.5, so we get the same upper bound on $\gamma(G)$ as in the case when $H = A_4$.

3. For any subquotient K of G we have $\gamma(G) \leq \gamma(K)$ by Lemma 1.8;

   (a) if $K/N \cong Z_2 \times Z_2$ for some normal subgroup $N \cong Z_2 \times Z_2$ then by Lemma 2.3 and Proposition 1.10:

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

   (b) if $K \cong Z_p \rtimes Z_q$ then $\gamma(K) < \frac{1}{2}$ by Theorem 3.16

   (c) if $K \cong Z_p \rtimes Z_4$, where Z_4 acts faithfully, then by Proposition 5.9

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

   (d) if $K \cong D_{2p} \times D_{2q}$ where p, q are distinct odd primes then by Lemma 2.3 and Corollary 5.5:

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

   (e) if $K/N \cong D_{2p}$ for some normal subgroup $N \cong Z_2 \times Z_2$ then by Lemma 2.3 and Corollary 5.5:

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

   (f) if $K \cong (Z_2 \times Z_2) \rtimes Z_9$ then $\gamma(K) \leq \frac{17}{36}$ by Proposition 4.8

To sum up, $\gamma(G) < \frac{1}{2}$ when G falls under case (3) of Theorem 6.1. □

6.3 Some corollaries

Corollary 6.9. *Let $\mathcal{C}$ denote the set of isomorphism classes of non-cyclic finite groups of order not divisible by* $\mathrm{char}(\mathbb{F})$. *Then*

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

Proof. If G is a non-cyclic group with $\gamma(G) > \frac{1}{2}$, then either $G = Z_3 \times Z_3$ or by Theorem 1.1 it must be a group with a cyclic subgroup of index 2. Therefore by Theorem 5.20 we have

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

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

Proposition 6.10. *Let G be a finite non-cyclic group and $\mathbb{F}$ a field such that $|G| \in \mathbb{F}^\times$. If q is the smallest prime divisor of $|G|$, then*

$$\sigma(G) \leq \frac{1}{q}|G|$$

Proof. If G has a subgroup isomorphic to $Z_p \times Z_p$ for some prime $p \geq 2$ then by Remark 2.29 and Corollary 2.21 we get that:

$$\frac{\sigma(G)}{|G|} \leq \frac{\sigma(Z_p \times Z_p)}{p^2} = \frac{1}{p}$$

and we are done. Otherwise by Lemma 6.4 all Sylow subgroups of G are cyclic, hence G falls under case (3b), (3c) or (1) of Theorem 6.1. Given that $\sigma(Z_p \rtimes Z_q) = p$ and $\sigma(Z_p \rtimes Z_4) = p$ by Proposition 3.27, and that $\sigma(G) = |G|/2$ for any group containing a cyclic subgroup of index 2, as it is seen from Theorem 5.20 combined with Theorem 2.25 — our claim is verified for all three cases using Remark 2.29 as above. □

Conjecture 6.11. *Let $\mathcal{C}_q$ denote the set of isomorphism classes of non-cyclic finite groups of order not divisible by* $\mathrm{char}(\mathbb{F})$ *with smallest prime divisor q. Then*

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

Conjecture 6.12. *If $\sigma(G) = \beta(G)$ for a finite group G then G is cyclic.*

6.4 A remark on separating invariants

A *separating algebra* $A \subset \mathbb{F}[V]^G$ is defined in [30] by the property that for any $u, v \in V$ belonging to different G-orbits there is an element $f \in A$ such that $f(u) \neq f(v)$. Following [32] we write $\beta_{\mathrm{sep}}(G, V) = \sup \beta(A)$ where A runs through all the separating subalgebras of $\mathbb{F}[V]^G$. It is easily seen that:

$$\sigma(G) \leq \beta_{\mathrm{sep}}(G) \leq \beta(G) \tag{6.1}$$

Indeed, as $\mathbb{F}[V]^G$ itself is a separating algebra, $\sup \beta(A)$ is finite and bounded by $\beta(G)$. On the other hand, if $v \in V$ is an element of the common zero locus of A then $g(v) = 0 = g(0)$ for every homogeneous generator $g \in A$, but then by definition v is on the same G-orbit with 0, whence $v = 0$; this shows that $\sigma(G) \leq \beta_{\mathrm{sep}}(G)$. In the present section we will give an example where both inequalities in (6.1) are strict. (We are unaware of any such examples so far.) Recall that for the group $G = Z_p \rtimes Z_3$ we have $\sigma(G) = p$ by Proposition 3.27 and $\beta(G) \geq p+2$ by Theorem 2.11. This G will be such an example, because:

Theorem 6.13. *$\beta_{\mathrm{sep}}(Z_p \rtimes Z_3) = p + 1$ for any prime p different from 7.*

Proof. First we will prove the lower bound $\beta_{\mathrm{sep}}(G) \geq p + 1$. Recall that $G = \langle a, b : a^p = b^3 = 1, bab^{-1} = a^r \rangle$, where r has order 3 modulo p. Let U and V be irreducible representations of G of dimension 1 and 3, respectively. Then $\mathbb{F}[U \oplus V] = \mathbb{F}[y, x_1, x_2, x_3]$ where $y^a = y$ and $y^b = \omega y$ for a primitive third root of unity ω, while the x_i are a-eigenvectors of eigenvalues $\varepsilon, \varepsilon^r, \varepsilon^{r^2}$ for some primitive p-th root of unity, which are cyclically permuted by b. Now, the point $(0, 1, 0, 0)$ has trivial stabilizer in G, hence the points $(1, 1, 0, 0)$ and $(\omega, 1, 0, 0)$ do not belong to the same G-orbit. We claim that they cannot be separated by invariants of degree at most p. Indeed, suppose to the contrary that they can be separated. Then there exists an $\langle a \rangle$-invariant monomial u with $\deg(u) \leq p$ and $\tau(u)(1, 1, 0, 0) \neq \tau(u)(\omega, 1, 0, 0)$. If an $\langle a \rangle$-invariant monomial v involves at least two variables from $\{x_1, x_2, x_3\}$, then $\tau(v)$ vanishes on both of $(1, 1, 0, 0)$ and $(\omega, 1, 0, 0)$. If u involves only y, then $\tau(u) = 0$ unless $u = y^{3k}$ for some positive integer k, when $\tau(u)$ takes the value 1 both on $(1, 1, 0, 0)$ and $(\omega, 1, 0, 0)$. So u involves exactly one variable from $\{x_1, x_2, x_3\}$, forcing that $u = x_i^p$, and then $\tau(u)$ agrees on the two given points, a contradiction.

Next we prove the inequality $\beta_{\mathrm{sep}}(G) \leq p + 1$. Let W be a multiplicity free representation of G which contains every irreducible representation of G with multiplicity 1. An arbitrary representation of G is contained in W^n for a sufficiently great integer n. According to the Draisma-Kemper-Wehlau theorem (see [15]) a separating set of $\mathbb{F}[W^{\oplus n}]^G$ can be obtained by "cheap" polarization from a separating set of $\mathbb{F}[W]^G$, which is a degree-preserving procedure, whence $\beta_{\mathrm{sep}}(G, W^{\oplus n}) \leq \beta_{\mathrm{sep}}(G, W)$ and

$$\beta_{\mathrm{sep}}(G) \leq \beta_{\mathrm{sep}}(G, W) \tag{6.2}$$

Now let $W = U \oplus V$ where U is the sum of 1-dimensional irreducibles, and V is the sum of 3-dimensional irreducibles. Suppose that (u_1, v_1) and (u_2, v_2) belong to different G-orbits in $U \oplus V$. We need to show that they can be separated by a polynomial invariant of degree at most $p + 1$. If u_1 and u_2 belong to different G-orbits, then they can be separated by a polynomial invariant of degree at most $q = |G/G'|$ (recall that G' acts trivially on U), and we are done. From now on we assume that u_1 and u_2 have the same G/G'-orbits. If v_1 and v_2 belong to different G-orbits in V, then they can be separated by a G-invariant on V of degree at most $p + 1$ by Theorem 3.29 and we are done. It remains that $v_1 = v_2^g$ for some $g \in G$; after replacing (u_2, v_2) with an appropriate element $v_1 = v_2 = v$ might be assumed, and then u_1 and u_2 are not on the same orbit under $\mathrm{Stab}_G(v)$. Consequently $\mathrm{Stab}_G(v)$ is contained in G' (for otherwise $\mathrm{Stab}_G(v)$ is mapped surjectively

onto G/G'). Let U_0 be a 1-dimensional summand in $U = U_0 \oplus U_1$ such that $\pi(u_1, v) \neq \pi(u_2, v)$, where $\pi : U \oplus V \to U_0$ is the projection onto U_0 with kernel $U_1 \oplus V$. Denote by y the coordinate function on U_0, viewed as an element of $\mathbb{F}[U \oplus V]$ by composing it with π. If G acts trivially on U_0, then y is a G-invariant of degree 1 that separates (u_1, v) and (u_2, v). Otherwise y is a relative invariant of some non-trivial weight χ. By Lemma 6.14 below, there is an $f \in \mathbb{F}[V]^{G,\chi^{-1}}$ such that $f(v) \neq 0$. Moreover, $\mathbb{F}[V]^{G,\chi^{-1}}$ is generated as an $\mathbb{F}[V]^G$-module by its elements of degree at most p by Proposition 3.28, hence we may assume that f has degree at most p. Now yf is a G-invariant of degree at most $p+1$ which separates (u_1, v) and (u_2, v) by construction. □

Lemma 6.14. *Let G be a finite group and V a G-module over a field $\mathbb{F}$ in which $|G|$ is invertible. Given any character $\chi : G \to \mathbb{F}^\times$ and any point $v \in V$ such that $\mathrm{Stab}_G(v) \leq \ker(\chi)$, a relative invariant $f \in \mathbb{F}[V]^{G,\chi}$ exists for which $f(v) \neq 0$.*

Proof. Let $g_1, ..., g_n \in G$ be a system of representatives of the left cosets of the subgroup $\mathrm{Stab}_G(v)$. Then by definition the points $g_1 \cdot v, ..., g_n \cdot v \in V$ are all different from each other. Therefore we can construct, e.g. using multivariate Lagrange interpolation a polynomial $p \in \mathbb{F}[V]$ such that

$$p(g_i \cdot v) = \chi(g_i) \qquad \text{for each } i = 1, ..., n$$

Now set $f := \tau_\chi(p)$ where $\tau_\chi : \mathbb{F}[V] \to \mathbb{F}[V]^{G,\chi}$ is the twisted transfer map defined as $\tau_\chi(p) := \sum_{g \in G} \chi^{-1}(g) p^g$. Then f is a relative invariant of character χ by construction. Moreover, since χ factors through a unique character $\tilde{\chi} : G/G' \to \mathbb{F}^\times$, and since $\mathrm{Stab}_G(v) \leq \ker(\chi)$ by assumption, we have:

$$f(v) = \sum_{g \in G} \chi^{-1}(g) p(g \cdot v) = |\operatorname{Stab}_G(v)| \sum_{i=1}^{n} \chi^{-1}(g_i) p(g_i \cdot v) = |G|$$

which is indeed non-zero in $\mathbb{F}$ by our assumption. □

Bibliography

[1] E. Balandraud. An addition theorem and maximal zero-sum free sets in $\mathbb{Z}/p\mathbb{Z}$. *Israel Journal of Mathematics*, 188:405–429, 2012.

[2] M. J. J. Barry and M. B. Ward. Simple groups contain minimal simple groups. *Publications Matématiques*, 41:411–415, 1997.

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

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

[5] K. Brown. *Cohomology of Groups*, volume 87 of *GTM*. Springer, 1982.

[6] R. M. Bryant and G. Kemper. Global degree bounds and the transfer principle. *J. Algebra*, 284(1):80–90, 2005.

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

[8] M. J. Collins. The characterization of the Suzuki groups by their Sylow 2-subgroups. *Math. Z.*, 123:32–48, 1971.

[9] J. A. Dias da Silva and Y. O. Hamidoune. Cyclic spaces for Grassmann derivatives and additive theory. *Bull. London Math. Soc.*, 26(2):140–146, 1994.

[10] Ch. Delorme, O. Ordaz, and D. Quiroz. Some remarks on Davenport constant. *Discrete Mathematics*, 237:119–128, 2001.

[11] H. Derksen. Polynomial bounds for rings of invariants. *Proceedings of the American Mathematical Society*, 129(4):955–963, 2000.

[12] H. Derksen and G. Kemper. *Computational Invariant Theory*, volume 130 of *Encyclopedia of Mathematical Sciences*. Springer-Verlag, 2002.

[13] H. Derksen and G. Kemper. On global degree bounds for invariants. *CRM Proceedings and Lecture Notes*, 35:37–41, 2003.

[14] M. Domokos and P. Hegedűs. Noether's bound for polynomial invariants of finite groups. *Arch. Math. (Basel)*, 74(3):161–167, 2000.

[15] J. Draisma, G. Kemper, and D. L. Wehlau. Polarization of separating invariants. *Canad. J. Math*, 60(3):556–571, 2008.

[16] P. Fleishmann. The Noether bound in invariant theory of finite groups. *Adv. Math.*, 156(1):23–32, 2000.

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

[18] M. Freeze and W. A. Schmid. Remarks on a generalization of the Davenport constant. *Discrete Math.*, 310:3373–3389, 2010.

[19] M. Freeze and W.W. Smith. Sumsets of zerofree sequences. *Arab J. Sci. Eng. Section C: Theme Issues*, 26:97–105, 2001.

[20] W. Gao and A. Geroldinger. Zero-sum problems in finite abelian groups: a survey. *Expo. Math.*, 24:337–369, 2006.

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

[22] M. Göbel. Computing bases of permutation-invariant polynomials. *J. Symbolic Computation*, 19:285–291, 1995.

[23] F.D. Grosshans. Vector invariants in arbitrary characteristic. *Transformation Groups*, 12:499–514, 2007.

[24] F. Halter-Koch. A generalization of Davenport's constant and its arithmetical applications. *Colloquium Mathematicum*, LXIII:203–210, 1992.

[25] G. Higman. Suzuki 2-groups. *Illinois Journal of Mathematics*, 7:79–95, 1963.

[26] D. Hilbert. Über die Theorie der algebraischen Formen. *Math. Ann.*, 36:473–531, 1890.

[27] D. Hilbert. Über die vollen Invariantensysteme. *Math. Ann.*, 42:313–370, 1893.

[28] W. C. Huffman. Polynomial invariants of finite linear groups of degree two. *Canad. J. Math*, 32:317–330, 1980.

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

[30] G. Kemper. Separating invariants. *Journal of Symbolic Computation*, 44(9):1212–1222, 2009.

[31] F. Knop. On Noether's and Weyl's bound in positive characteristic. In H. E. A. Eddy Campbell and D. L. Wehlau, editors, *Invariant Theory in All Characteristics*, volume 35 of *CRM Proceedings and Lecture Notes*. Amer. Math. Soc., Providence, Rhode Island, 2004.

[32] M. Kohls and H. Kraft. Degree bounds for separating invariants. *Math. Res. Lett.*, 17:10001–10012, 2010.

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

[34] E. Noether. Der Endlichkeitssatz der Invarianten endlicher Gruppen. *Math. Ann.*, 77:89–92, 1916.

[35] E. Noether. Der Endlichkeitssatz der Invarianten endlicher linearer Gruppen der Charakteristik p. *Nachr. Ges. Wiss. Göttingen*, pages 28–36, 1926.

[36] J. E. Olson. A combinatorial problem on finite Abelian groups I. *Journal of Number Theory*, 1:8–10, 195–199, 1969.

[37] J. E. Olson. A combinatorial problem on finite Abelian groups II. *Journal of Number Theory*, 1:195–199, 1969.

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

[39] V. L. Popov and E.B. Vinberg. Invariant theory. In *Algebraic Geometry IV*, volume 55 of *Encyclopedia of Mathematical Sciences*. Springer-Verlag, Berlin-Heidelberg, 1994.

[40] D. R. Richman. Invariants of finite groups over fields of characteristic p. *Adv. Math.*, 124:25–48, 1996.

[41] P. Roquette. Realisierung von Darstellungen endlicher nilpotenten Gruppen. *Arch. Math.*, 9:241–250, 1958.

[42] S. Savchev and F. Chen. Long zero-free sequences in finite cyclic groups. *Discrete Mathematics*, 307:2671–2679, 2007.

[43] B. J. Schmid. Finite groups and invariant theory. In Malliavin M. P., editor, *Topics in invariant theory*, number 1478 in Lecture notes in mathematics. Springer, 1989-90.

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

[45] M. Sezer. Sharpening the generalized Noether bound in the invariant theory of finite groups. *J. Algebra*, 254(2):252–263, 2002.

[46] T. Tao and V. Vu. *Additive Combinatorics*. Number 105 in Cambridge studies in advanced mathematics. Cambride University Press, 2006.

[47] J. G. Thompson. Nonsolvable finite groups all of whose local subgroups are solvable. *Bull. Amer. Math. Soc.*, 74:383–437, 1968.

[48] D. Wehlau. The Noether number in invariant theory. *Comptes Rendus Math. Rep. Acad. Sci. Canada*, 28(2):39 – 62, 2006.

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

[50] H. Zassenhaus. Über endliche Fastkörper. *Abhandlungen aus dem Mathematischen Seminar der Hamburgische Universität*, 11:pp. 187–220, 1935.