The Interplay of Invariant Theory with Multiplicative Ideal Theory and with Arithmetic Combinatorics

Kálmán Cziszter, Mátyás Domokos and Alfred Geroldinger

Dedicated to Franz Halter-Koch on the occasion of his 70th birthday

Abstract This paper surveys and develops links between polynomial invariants of finite groups, factorization theory of Krull domains, and product-one sequences over finite groups. The goal is to gain a better understanding of the multiplicative ideal theory of invariant rings, and connections between the Noether number and the Davenport constants of finite groups.

Keywords Invariant rings · Krull monoids · Noether number · Davenport constant · Zero-sum sequences · Product-one sequences

1 Introduction

The goal of this paper is to deepen the links between the areas in the title. Invariant theory is concerned with the study of group actions on algebras, and in the present article we entirely concentrate on actions of finite groups on polynomial algebras via linear substitution of the variables.

K. Cziszter · M. Domokos (✉)
MTA Alfréd Rényi Institute of Mathematics, Reáltanoda u. 13–15, Budapest 1053, Hungary
e-mail: domokos.matyas@renyi.mta.hu

K. Cziszter
e-mail: cziszter.kalman@gmail.com

A. Geroldinger
Institute for Mathematics and Scientific Computing, University of Graz, NAWI Graz,
Heinrichstraße 36, 8010 Graz, Austria
e-mail: alfred.geroldinger@uni-graz.at

To begin with, let us briefly sketch the already existing links between the mentioned areas. For a finite-dimensional vector space V over a field $\mathbb{F}$ and a finite group $G \leq \mathrm{GL}(V)$, let $\mathbb{F}[V]^G \subset \mathbb{F}[V]$ denote the ring of invariants. Since E. Noether we know that $\mathbb{F}[V]^G \subset \mathbb{F}[V]$ is an integral ring extension and that $\mathbb{F}[V]^G$ is a finitely generated $\mathbb{F}$-algebra. In particular, $\mathbb{F}[V]^G$ is an integrally closed noetherian domain and hence a Krull domain. Benson [4] and Nakajima [58] determined its class group. Krull domains (their ideal theory and their class groups) are a central topic in multiplicative ideal theory (see the monographs [46, 51] and the recent survey [52]). B. Schmid [73] observed that the Noether number of a finite abelian group G equals the Davenport constant of G (a constant of central importance in zero-sum theory) and this established a first link between invariant theory and arithmetic combinatorics. Moreover, ideal and factorization theory of Krull domains are most closely linked with zero-sum theory via transfer homomorphisms (see [37, 40] and Sect. 3.2).

These links serve as our starting point. It is well known that a domain R is a Krull domain if and only if its monoid $R^\bullet$ of nonzero elements is a Krull monoid if and only if R (resp. $R^\bullet$) has a divisor theory. To start with Krull monoids, a monoid H is Krull if and only if its associated reduced monoid $H/H^\times$ is Krull, and every Krull monoid H is a direct product $H^\times \times H_0$ where H_0 is isomorphic to $H/H^\times$. A reduced Krull monoid is uniquely determined (up to isomorphism) by its characteristic (roughly speaking by its class group $\mathscr{C}(H)$ and the distribution of the prime divisors in its classes; see the end of Sect. 4.2). By definition of the class group, a Krull monoid H is factorial if and only if $\mathscr{C}(H)$ is trivial. Information on the subset $\mathscr{C}(H)^* \subset \mathscr{C}(H)$ of classes containing prime divisors is the crucial ingredient to understand the arithmetic of H, and hence in order to study the arithmetic of Krull monoids the first and most important issue is to determine $\mathscr{C}(H)^*$. By far the best understood setting in factorization theory are Krull monoids with finite class groups where every class contains a prime divisor. Indeed, there has been an abundance of work on them and we refer the reader to the survey by W.A. Schmid in this proceedings [77]. A canonical method to obtain information on $\mathscr{C}(H)^*$ is to identify explicitly a divisor theory for H. A divisor theory of a monoid (or a domain) H is a divisibility preserving homomorphism from H to a free abelian monoid which satisfies a certain minimality property (Sect. 2.1). The concept of a divisor theory stems from algebraic number theory and it has found far-reaching generalizations in multiplicative ideal theory [51]. Indeed, divisor-theoretic tools, together with ideal-theoretic and valuation-theoretic ones, constitute a highly developed machinery for the structural description of monoids and domains.

All the above-mentioned concepts and problems from multiplicative ideal theory are studied for the ring of invariants. Theorem 4.5 (in Sect. 4.2) provides an explicit divisor theory of the ring of invariants $R = \mathbb{F}[V]^G$. The divisibility preserving homomorphism from $R^\bullet$ goes into a free abelian monoid which can be naturally described in the language of invariant theory, and the associated canonical transfer homomorphism $\theta \colon R^\bullet \to \mathscr{B}(\mathscr{C}(R)^*)$ from the multiplicative monoid of the ring R onto the monoid of zero-sum sequences over the class group of R also has a natural invariant

theoretic interpretation. In addition to recovering the result of Benson and Nakajima on the class group $\mathscr{C}(\mathbb{F}[V]^G)$ (our treatment is essentially self-contained), we gain further information on the multiplicative structure of R, and we pose the problem to determine its characteristic (Problem 1). In particular, whenever we can show—for a given ring of invariants—that every class contains at least one prime divisor, then all results of factorization theory (obtained for Krull monoids with finite class group and prime divisors in all classes) apply to the ring of invariants.

In Sect. 4.3 we specialize to abelian groups whose order is not divisible by the characteristic of $\mathbb{F}$. The Noether number $\beta(G)$ is the supremum over all finite dimensional G-modules V of the maximal degree of an element in a minimal homogeneous generating system of $\mathbb{F}[V]^G$, and the Davenport constant $\mathsf{D}(G)$ is the maximal length of a minimal zero-sum sequence over G. We start with a result on the structural connection between $\mathbb{F}[V]^G$ and the monoid of zero-sum sequences over G, that lies behind the equality $\beta(G) = \mathsf{D}(G)$. Clearly, the idea here is well known (as far as we know, it was first used by B. Schmid [73], see also [24]). The benefit of the detailed presentation as given in Proposition 4.7 is twofold. First, the past 20 years have seen great progress in zero-sum theory (see Sect. 3.4 for a sample of results) and Proposition 4.7 allows to carry over all results on the structure of (long) minimal zero-sum sequences to the structure of G-invariant monomials. Second, we observe that the submonoid M^G of $R^\bullet$ consisting of the invariant monomials is again a Krull monoid, and restricting the transfer homomorphism $\theta\colon R^\bullet \to \mathscr{B}(\mathscr{C}(R)^*)$ (mentioned in the above paragraph) to M^G we obtain essentially the canonical transfer homomorphism $M^G \to \mathscr{B}(\mathscr{C}(M^G)^*)$. This turns out to be rather close to the transfer homomorphism $\psi\colon M^G \to \mathscr{B}(\widehat{G})$ into the monoid of zero-sum sequences over the character group of G (see Proposition 4.7), which is responsible for the equality $\beta(G) = \mathsf{D}(G)$. The precise statement is given in Proposition 4.9, which explains how the transfer homomorphism ψ (existing only for abelian groups) relates to the more general transfer homomorphism θ from the above paragraph which exists for an arbitrary finite group. In Proposition 4.9 we point out that every class of $\mathscr{C}(\mathbb{F}[V]^G)$ contains a prime divisor which contributes to Problem 1.

Let now G be a finite non-abelian group. Until recently, the precise value of the Noether number $\beta(G)$ was known only for the dihedral groups and very few small groups (such as A_4). In the last couple of years the first two authors have determined the precise value of the Noether number for groups having a cyclic subgroup of index two and for non-abelian groups of order $3p$ [10, 12, 13]. In this work results on zero-sum sequences over finite abelian groups (for example, information on the structure of long minimal zero-sum sequences and on the kth Davenport constants) were successfully applied. Moreover, a decisive step was the introduction of the kth Noether numbers, a concept inspired by the kth Davenport constants of abelian groups. The significance of this concept is that it furnishes some reduction lemmas (listed in Sect. 5.1) by which the ordinary Noether number of a group can be bounded via structural reduction in the group.

The concept of the kth Davenport constants $\mathsf{D}_k(G)$ has been introduced by Halter-Koch [50] for abelian groups in order to study the asymptotic behavior of arithmetical counting functions in rings of integers of algebraic number fields

(see [40, Theorem 9.1.8], [67, Theorem 1]). They have been further studied in [15, 30]. In the last years the third author and Grynkiewicz [39, 48] studied the (small and the large) Davenport constant of non-abelian groups, and among others determined their precise values for groups having a cyclic subgroup of index two. It can be observed that for these groups the Noether number is between the small and the large Davenport constant.

This motivated a new and more abstract view at the Davenport constants, namely kth Davenport constants of BF-monoids (Sect. 2.5). The goal is to relate the Noether number with Davenport constants of suitable monoids as a generalization of the equation $\beta(G) = \mathsf{D}(G)$ in the abelian case. Indeed, the kth Davenport constant $\mathsf{D}_k(G)$ of an abelian group G is recovered as our kth Davenport constant of the monoid $\mathscr{B}(G)$ of zero-sum sequences over G.

We apply the new concept of the kth Davenport constants to two classes of BF-monoids. First, to the monoid $\mathscr{B}(G, V)$ associated to a G-module V in Sect. 4.4 (when G is abelian we recover the monoid M^G of G-invariant monomials from Sect. 4.3), whose Davenport constants provide a lower bound for the corresponding Noether numbers (see Proposition 4.12). Second, we study the monoid of product-one sequences over finite groups (Sects. 3.1 and 3.3). We derive a variety of features of the kth Davenport constants of the monoid of product-one sequences over G and observe that they are strikingly similar to the corresponding features of the kth Noether numbers (see Sect. 5.1 for a comparison).

We pose a problem on the relationship between Noether numbers and Davenport constants of non-abelian groups (Problem 2) and we illustrate the efficiency of the above methods by Examples 5.2–5.4 (appearing for the first time), where the explicit value of Noether numbers and Davenport constants of some non-abelian groups are determined.

Throughout this paper, let G be a finite group, $\mathbb{F}$ be a field, and V be a finite dimensional $\mathbb{F}$-vector space endowed with a linear action of G.

2 Multiplicative Ideal Theory: Krull Monoids, C-Monoids, and Class Groups

We denote by $\mathbb{N}$ the set of positive integers, and we put $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$. For every $n \in \mathbb{N}$, we denote by C_n a cyclic group with n elements. For real numbers $a, b \in \mathbb{R}$, we set $[a, b] = \{x \in \mathbb{Z} : a \le x \le b\}$. If A, B are sets, we write $A \subset B$ to mean that A is contained in B but may be equal to B. In Sects. 2.1–2.4 we gather basic material on Krull monoids and C-monoids. In Sect. 2.5 we introduce a new concept, namely Davenport constants of BF-monoids.

2.1 Monoids and Domains: Ideal Theoretic and Divisor Theoretic Concepts

Our notation and terminology follows [40, 51] (note that the monoids in [51] do contain a zero-element, whereas the monoids in [40] and in the present manuscript do not contain a zero-element). By a *monoid*, we mean a commutative, cancellative semigroup with unit element. Then the multiplicative semigroup $R^{\bullet} = R \setminus \{0\}$ of nonzero elements of a domain is a monoid. Following the philosophy of multiplicative ideal theory we describe the arithmetic and the theory of divisorial ideals of domains by means of their multiplicative monoids. Thus we start with monoids.

Let H be a multiplicatively written monoid. An element $u \in H$ is called

- *invertible* if there is an element $v \in H$ with $uv = 1$.
- *irreducible* (or an *atom*) if u is not invertible and, for all $a, b \in H$, $u = ab$ implies a is invertible or b is invertible.
- *prime* if u is not invertible and, for all $a, b \in H$, $u \mid ab$ implies $u \mid a$ or $u \mid b$.

We denote by $\mathscr{A}(H)$ the set of atoms of H, by $H^{\times}$ the group of invertible elements, and by $H_{\mathrm{red}} = \{aH^{\times} : a \in H\}$ the associated reduced monoid of H. We say that H is reduced if $|H^{\times}| = 1$. We denote by $\mathsf{q}(H)$ a quotient group of H with $H \subset \mathsf{q}(H)$, and for a prime element $p \in H$, let $\mathsf{v}_p \colon \mathsf{q}(H) \to \mathbb{Z}$ be the p-adic valuation. Each monoid homomorphism $\varphi \colon H \to D$ induces a group homomorphism $\mathsf{q}(H) \colon \mathsf{q}(H) \to \mathsf{q}(D)$. For a subset $H_0 \subset H$, we denote by $[H_0] \subset H$ the submonoid generated by H_0, and by $\langle H_0 \rangle \leq \mathsf{q}(H)$ the subgroup generated by H_0. We denote by $\widetilde{H} = \{x \in \mathsf{q}(H) : x^n \in H \text{ for some } n \in \mathbb{N}\}$ the *root closure* of H, and by $\widehat{H} = \{x \in \mathsf{q}(H) : \text{ there exists } c \in H \text{ such that } cx^n \in H \text{ for all } n \in \mathbb{N}\}$ the *complete integral closure* of H. Both $\widetilde{H}$ and $\widehat{H}$ are monoids, and we have $H \subset \widetilde{H} \subset \widehat{H} \subset \mathsf{q}(H)$. We say that H is root closed (completely integrally closed resp.) if $H = \widetilde{H}$ ($H = \widehat{H}$ resp.). For a set P, we denote by $\mathscr{F}(P)$ the free abelian monoid with basis P. Then every $a \in \mathscr{F}(P)$ has a unique representation in the form

$$a = \prod_{p \in P} p^{\mathsf{v}_p(a)}, \text{ where } \mathsf{v}_p(a) \in \mathbb{N}_0 \text{ and } \mathsf{v}_p(a) = 0 \text{ for almost all } p \in P.$$

The monoid H is said to be

- *atomic* if every $a \in H \setminus H^{\times}$ is a product of finitely many atoms of H.
- *factorial* if every $a \in H \setminus H^{\times}$ is a product of finitely many primes of H (equivalently, $H = H^{\times} \times \mathscr{F}(P)$ where P is a set of representatives of primes of F).
- *finitely generated* if $H = [E]$ for some finite subset $E \subset H$.

If $H = H^{\times} \times \mathscr{F}(P)$ is factorial and $a \in H$, then $|a| = \sum_{p \in P} \mathsf{v}_p(a) \in \mathbb{N}_0$ is called the length of a. If H is reduced, then it is finitely generated if and only if it is atomic and $\mathscr{A}(H)$ is finite. Since every prime is an atom, every factorial monoid is atomic. For every non-unit $a \in H$,

$$\mathsf{L}_H(a) = \mathsf{L}(a) = \{k \in \mathbb{N} \colon a \text{ may be written as a product of } k \text{ atoms}\} \subset \mathbb{N}$$

denotes the *set of lengths* of a. For convenience, we set $\mathsf{L}(a) = \{0\}$ for $a \in H^\times$. We say that H is a BF-monoid if it is atomic and all sets of lengths are finite. A monoid homomorphism $\varphi \colon H \to D$ is said to be

- a *divisor homomorphism* if $\varphi(a) \mid \varphi(b)$ implies that $a \mid b$ for all $a, b \in H$.
- *cofinal* if for every $\alpha \in D$ there is an $a \in H$ such that $\alpha \mid \varphi(a)$.
- a *divisor theory* (for H) if $D = \mathscr{F}(P)$ for some set P, φ is a divisor homomorphism, and for every $p \in P$, there exists a finite nonempty subset $X \subset H$ satisfying $p = \gcd\big(\varphi(X)\big)$.

Obviously, every divisor theory is cofinal. Let $H \subset D$ be a submonoid. Then $H \subset D$ is called

- *saturated* if the embedding $H \hookrightarrow D$ is a divisor homomorphism.
- *divisor closed* if $a \in H$, $b \in D$ and $b \mid a$ implies $b \in H$.
- *cofinal* if the embedding $H \hookrightarrow D$ is cofinal.

It is easy to verify that $H \hookrightarrow D$ is a divisor homomorphism if and only if $H = \mathsf{q}(H) \cap D$, and if this holds, then $H^\times = D^\times \cap H$. If $H \subset D$ is divisor closed, then $H \subset D$ is saturated.

For subsets $A, B \subset \mathsf{q}(H)$, we denote by $(A \colon B) = \{x \in \mathsf{q}(H) \colon xB \subset A\}$, by $A^{-1} = (H \colon A)$, and by $A_v = (A^{-1})^{-1}$. A subset $\mathfrak{a} \subset H$ is called an s-ideal of H if $\mathfrak{a}H = \mathfrak{a}$. A subset $X \subset \mathsf{q}(H)$ is called a fractional v-ideal (or a *fractional divisorial ideal*) if there is a $c \in H$ such that $cX \subset H$ and $X_v = X$. We denote by $\mathscr{F}_v(H)$ the set of all fractional v-ideals and by $\mathscr{I}_v(H)$ the set of all v-ideals of H. Furthermore, $\mathscr{I}_v^*(H)$ is the monoid of v-invertible v-ideals (with v-multiplication) and $\mathscr{F}_v(H)^\times = \mathsf{q}\big(\mathscr{I}_v^*(H)\big)$ is its quotient group of fractional invertible v-ideals. The monoid H is completely integrally closed if and only if every nonempty v-ideal of H is v-invertible, and H is called v-noetherian if it satisfies the ACC (ascending chain condition) on v-ideals. If H is v-noetherian, then H is a BF-monoid. We denote by $\mathfrak{X}(H)$ the set of all minimal nonempty prime s-ideals of H.

The map $\partial \colon H \to \mathscr{I}_v^*(H)$, defined by $\partial(a) = aH$ for each $a \in H$, is a cofinal divisor homomorphism. Thus, if $\mathscr{H} = \{aH \colon a \in H\}$ is the monoid of principal ideals of H, then $\mathscr{H} \subset \mathscr{I}_v^*(H)$ is saturated and cofinal.

2.2 Class Groups and Class Semigroups

Let $\varphi \colon H \to D$ be a monoid homomorphism. The group $\mathscr{C}(\varphi) = \mathsf{q}(D)/\mathsf{q}(\varphi(H))$ is called the *class group* of φ. For $a \in \mathsf{q}(D)$, we denote by $[a]_\varphi = a\mathsf{q}(\varphi(H)) \in \mathscr{C}(\varphi)$ the class containing a. We use additive notation for $\mathscr{C}(\varphi)$ and so $[1]_\varphi$ is the zero element of $\mathscr{C}(\varphi)$.

Suppose that $H \subset D$ and that $\varphi = (H \hookrightarrow D)$. Then $\mathscr{C}(\varphi) = \mathsf{q}(D)/\mathsf{q}(H)$, and for $a \in D$ we set $[a]_\varphi = [a]_{D/H} = a\mathsf{q}(H)$. Then

$$D/H = \{[a]_{D/H} : a \in D\} \subset \mathscr{C}(\varphi)$$

is a submonoid with quotient group $\mathsf{q}(D/H) = \mathscr{C}(\varphi)$. It is easy to check that D/H is a group if and only if $H \subset D$ is cofinal. In particular, if D/H is finite or if $\mathsf{q}(D)/\mathsf{q}(H)$ is a torsion group, then $D/H = \mathsf{q}(D)/\mathsf{q}(H)$. Let H be a monoid. Then $\mathscr{H} \subset \mathscr{I}_v^*(H)$ is saturated and cofinal, and

$$\mathscr{C}_v(H) = \mathscr{I}_v^*(H)/\mathscr{H} = \mathscr{F}_v(H)^\times/\mathsf{q}(\mathscr{H})$$

is the *v-class group* of H.

We will also need the concept of class semigroups which are a refinement of ordinary class groups in commutative algebra. Let D be a monoid and $H \subset D$ a submonoid. Two elements $y, y' \in D$ are called H-equivalent, if $y^{-1}H \cap D = y'^{-1}H \cap D$. H-equivalence is a congruence relation on D. For $y \in D$, let $[y]_H^D$ denote the congruence class of y, and let

$$\mathscr{C}(H, D) = \{[y]_H^D : y \in D\} \quad \text{and} \quad \mathscr{C}^*(H, D) = \{[y]_H^D : y \in (D \backslash D^\times) \cup \{1\}\}.$$

Then $\mathscr{C}(H, D)$ is a semigroup with unit element $[1]_H^D$ (called the *class semigroup of H in D*) and $\mathscr{C}^*(H, D) \subset \mathscr{C}(H, D)$ is a subsemigroup (called the *reduced class semigroup of H in D*). The map

$$\theta: \mathscr{C}(H, D) \to D/H, \quad \text{defined by} \quad \theta([a]_H^D) = [a]_{D/H} \quad \text{for all } a \in D,$$

is an epimorphism, and it is an isomorphism if and only if $H \subset D$ is saturated.

2.3 Krull Monoids and Krull Domains

Theorem 2.1 *Let H be a monoid. Then, the following statements are equivalent:*

(a) H is v-noetherian and completely integrally closed,
(b) $\partial: H \to \mathscr{I}_v^*(H)$ is a divisor theory.
(c) H has a divisor theory.
(d) There is a divisor homomorphism $\varphi: H \to D$ into a factorial monoid D.
(e) H_{red} is a saturated submonoid of a free abelian monoid.

If H satisfies these conditions, then H is called a Krull monoid.

Proof See [40, Theorem 2.4.8] or [51, Chap. 22].

Let H be a Krull monoid. Then $\mathscr{I}_v^*(H)$ is free abelian with basis $\mathfrak{X}(H)$. Let $\mathfrak{p} \in \mathfrak{X}(H)$. Then $\mathsf{v}_\mathfrak{p}$ denotes the $\mathfrak{p}$-adic valuation of $\mathscr{F}_v(H)^\times$. For $x \in \mathsf{q}(H)$, we

set $v_{\mathfrak{p}}(x) = v_{\mathfrak{p}}(xH)$ and we call $v_{\mathfrak{p}}$ the $\mathfrak{p}$-adic valuation of H. Then $v\colon H \to \mathbb{N}_0^{(\mathfrak{X}(H))}$, defined by $v(a) = \big(v_{\mathfrak{p}}(a)\big)_{\mathfrak{p}\in\mathfrak{X}(H)}$ is a divisor theory and $H = \{x \in q(H)\colon v_{\mathfrak{p}}(x) \geq 0$ for all $\mathfrak{p} \in \mathfrak{X}(H)\}$.

If $\varphi\colon H \to D = \mathscr{F}(P)$ is a divisor theory, then there is an isomorphism $\Phi\colon \mathscr{I}_v^*(H) \to D$ such that $\Phi \circ \partial = \varphi$, and it induces an isomorphism $\overline{\Phi}\colon \mathscr{C}_v(H) \to \mathscr{C}(\varphi)$. Let $D = \mathscr{F}(P)$ be such that $H_{\mathrm{red}} \hookrightarrow D$ is a divisor theory. Then D and P are uniquely determined by H,

$$\mathscr{C}(H) = \mathscr{C}(H_{\mathrm{red}}) = D/H_{\mathrm{red}}$$

is called the (*divisor*) *class group* of H, and its elements are called the classes of H. By definition, every class $g \in \mathscr{C}(H)$ is a subset of $q(D)$ and $P \cap g$ is the set of prime divisors lying in g. We denote by $\mathscr{C}(H)^* = \{[p]_{D/H_{\mathrm{red}}}\colon p \in P\} \subset \mathscr{C}(H)$ the subset of classes containing prime divisors (for more details we refer to the discussion after Definition 2.4.9 in [40]).

Proposition 2.2 *Let H be a Krull monoid, and let $\varphi\colon H \to D = \mathscr{F}(P)$ be a divisor homomorphism.*

1. *There is a submonoid $C_0 \subset \mathscr{C}(\varphi)$ and an epimorphism $C_0 \to \mathscr{C}_v(H)$.*
2. *Suppose that $H \subset D$ is saturated and that $q(D)/q(H)$ is a torsion group. We set $D_0 = \{\gcd_D(X)\colon X \subset H \text{ finite}\}$, and for $p \in P$ define $e(p) = \min\{v_p(h)\colon h \in H \text{ with } v_p(h) > 0\}$.*

   (a) *D_0 is a free abelian monoid with basis $\{p^{e(p)}\colon p \in P\}$.*
   (b) *The embedding $H \hookrightarrow D_0$ is a divisor theory for H.*

Proof 1. follows from [40, Theorem 2.4.8], and 2. from [74, Lemma 3.2]. $\qquad\square$

Let R be a domain with quotient field K. Then $R^\bullet = R\setminus\{0\}$ is a monoid, and all notions defined for monoids so far will be applied for domains. To mention a couple of explicit examples, we denote by $q(R)$ the quotient field of R and we have $q(R) = q(R^\bullet) \cup \{0\}$, and for the complete integral closure we have $\widehat{R} = \widehat{R^\bullet} \cup \{0\}$ (where $\widehat{R}$ is the integral closure of R in its quotient field). We denote by $\mathfrak{X}(R)$ the set of all minimal nonzero prime ideals of R, by $\mathscr{I}_v(R)$ the set of divisorial ideals of R, by $\mathscr{I}_v^*(R)$ the set of v-invertible divisorial ideals of R, and by $\mathscr{F}_v(R)$ the set of fractional divisorial ideals of R. Equipped with v-multiplication, $\mathscr{F}_v(R)$ is a semigroup, and the map

$$\iota^\bullet\colon \mathscr{F}_v(R) \to \mathscr{F}_v(R^\bullet), \quad \text{defined by} \quad \mathfrak{a} \mapsto \mathfrak{a}\setminus\{0\},$$

is a semigroup isomorphism mapping $\mathscr{I}_v(R)$ onto $\mathscr{I}_v(R^\bullet)$ and fractional principal ideals of R onto fractional principal ideals of $R^\bullet$. Thus R satisfies the ACC on divisorial ideals of R if and only if $R^\bullet$ satisfies the ACC on divisorial ideals of $R^\bullet$. Furthermore, R is completely integrally closed if and only if $R^\bullet$ is completely integrally closed. A domain R is a Krull domain if it is completely integrally closed and satisfies the ACC on divisorial ideals of R, and thus R is a Krull domain if and only if $R^\bullet$ is a Krull

monoid. If R is a Krull domain, we set $\mathscr{C}(R) = \mathscr{C}(R^\bullet)$. The group $\mathscr{F}_v(R)^\times$ is the group of v-invertible fractional ideals and the set $\mathscr{I}_v^*(R) = \mathscr{F}_v(R)^\times \cap \mathscr{I}_v(R)$ of all v-invertible v-ideals of R is a monoid with quotient group $\mathscr{F}_v(R)^\times$. The embedding of the nonzero principal ideals $\mathscr{H}(R) \hookrightarrow \mathscr{I}_v^*(R)$ is a cofinal divisor homomorphism, and the factor group

$$\mathscr{C}_v(R) = \mathscr{F}_v(R)^\times / \{aR \colon a \in K^\times\} = \mathscr{I}_v^*(R)/\mathscr{H}(R)$$

is called the *v-class group* of R. The map $\iota^\bullet$ induces isomorphisms $\mathscr{F}_v(R)^\times \xrightarrow{\sim} \mathscr{F}_v(R^\bullet)^\times$, $\mathscr{I}_v^*(R) \xrightarrow{\sim} \mathscr{I}_v^*(R^\bullet)$, and $\mathscr{C}_v(R) \xrightarrow{\sim} \mathscr{C}_v(R^\bullet)$, and in the sequel we shall identify these monoids and groups.

The above correspondence between domains and their monoids of non-zero elements can be extended to commutative rings with zero-divisors and their monoids of regular elements [45, Theorem 3.5], and there is an analogue for prime Goldie rings [38, Proposition 5.1].

Examples 2.3 1. (Domains) As mentioned above, the multiplicative monoid $R^\bullet$ of a domain R is a Krull monoid if and only if R is a Krull domain. Thus Property (a) in Theorem 2.1 implies that a noetherian domain is Krull if and only if it is normal (i.e. integrally closed in its field of fractions). In particular, rings of invariants are Krull, as we shall see in Theorem 4.1.

2. (Submonoids of domains) Regular congruence submonoids of Krull domains are Krull [40, Proposition 2.11.6].

3. (Monoids of modules) Let R be a (possibly noncommutative) ring and let $\mathscr{C}$ be a class of finitely generated (right) R-modules which is closed under finite direct-sums, direct summands, and isomorphisms. Then the set $\mathscr{V}(\mathscr{C})$ of isomorphism classes of modules is a commutative semigroup with operation induced by the direct sum. If the endomorphism ring of each module in $\mathscr{C}$ is semilocal, then $\mathscr{V}(\mathscr{C})$ is a Krull monoid [19, Theorem 3.4]. For more information we refer to [1, 20, 21].

4. (Monoids of product-one sequences) In Theorem 3.2 we will characterize the monoids of product-one sequences which are Krull.

2.4 C-Monoids and C-Domains

A monoid H is called a C-*monoid* if it is a submonoid of a factorial monoid F such that $H \cap F^\times = H^\times$ and the reduced class semigroup $\mathscr{C}^*(H, F)$ is finite. A domain is called a C-*domain* if $R^\bullet$ is a C-monoid.

Proposition 2.4 *Let F be a factorial monoid and $H \subset F$ a submonoid such that $H \cap F^\times = H^\times$.*

1. *If H is a C-monoid, then H is v-noetherian with $(H : \widehat{H}) \neq \emptyset$, and the complete integral closure $\widehat{H}$ is a Krull monoid with finite class group $\mathscr{C}(\widehat{H})$.*

2. *Suppose that $F/F^\times$ is finitely generated, say $F = F^\times \times [p_1, \ldots, p_s]$ with pairwise nonassociated prime elements $p_1, \ldots, p_s$. Then, the following statements are equivalent:*

   (a) *H is a C-monoid defined in F.*
   (b) *There exist some $\alpha \in \mathbb{N}$ and a subgroup $W \le F^\times$ such that $(F^\times : W) \mid \alpha$, $W(H \backslash H^\times) \subset H$, and for all $j \in [1, s]$ and $a \in p_j^\alpha F$ we have $a \in H$ if and only if $p_j^\alpha a \in H$.*

Proof For 1., see [40, Theorems 2.9.11 and 2.9.13] and for 2. see [40, Theorems 2.9.7].

Examples 2.5 1. (Krull monoids) A Krull monoid is a C-monoid if and only if the class group is finite [40, Theorem 2.9.12].

2. (Domains) Let R be a domain. Necessary conditions for R being a C-domain are given in Proposition 2.4. Thus suppose that R is a Mori domain (i.e., a *v*-noetherian domain) with nonzero conductor $\mathfrak{f} = (R : \widehat{R})$ and suppose that $\mathscr{C}(\widehat{R})$ is finite. If $R/\mathfrak{f}$ is finite, then R is a C-domain by [40, Theorem 2.11.9]. This result generalizes to rings with zero-divisors [45], and in special cases we know that R is a C-domain if and only if $R/\mathfrak{f}$ is finite [69].

3. (Congruence monoids) Let R be Krull domain with finite class group $\mathscr{C}(R)$ and $H \subset R$ a congruence monoid such that $R/\mathfrak{f}$ is finite where $\mathfrak{f}$ is an ideal of definition for H. If R is noetherian or $\mathfrak{f}$ is divisorial, then H is a C-monoid [40, Theorem 2.11.8]. For a survey on arithmetical congruence monoids see [2].

4. In Sect. 3.1 we shall prove that monoids of product-one sequences are C-monoids (Theorem 3.2), and we will meet C-monoids again in Proposition 4.11 dealing with the monoid $\mathscr{B}(G, V)$.

Finitely generated monoids allow simple characterizations when they are Krull or when they are C-monoids. We summarize these characterizations in the next lemma.

Proposition 2.6 *Let H be a monoid such that H_{red} is finitely generated.*

1. *Then H is v-noetherian with $(H : \widehat{H}) \neq \emptyset$, $\widetilde{H} = \widehat{H}$, $\widetilde{H}/H^\times$ is finitely generated, and $\widehat{H}$ is a Krull monoid. In particular, H is a Krull monoid if and only if $H = \widehat{H}$.*
2. *H is a C-monoid if and only if $\mathscr{C}(\widehat{H})$ is finite.*
3. *Suppose that H is a submonoid of a factorial monoid $F = F^\times \times \mathscr{F}(P)$. Then, the following statements are equivalent:*

   a. *H is a C-monoid defined in F, $F^\times/H^\times$ is a torsion group, and for every $p \in P$ there is an $a \in H$ such that $\mathsf{v}_p(a) > 0$.*
   b. *For every $a \in F$, there is an $n_a \in \mathbb{N}$ with $a^{n_a} \in H$.*

   If (a) and (b) hold, then P is finite and $\widetilde{H} = \widehat{H} = \mathsf{q}(H) \cap F \subset F$ is saturated and cofinal.

Proof 1. follows from [40, 2.7.9–2.7.13], and 2. follows from [41, Proposition 4.8].

3. (a) $\Rightarrow$ (b) For every $p \in P$, we set $d_p = \gcd\left(\mathsf{v}_p(H)\right)$, and by assumption we have $d_p > 0$. We set $P_0 = \{p^{d_p} : p \in P\}$ and $F_0 = F^\times \times \mathscr{F}(P_0)$. By [40, Theorem 2.9.11], H is a C-monoid defined in F_0 and there is a divisor theory $\partial \colon \widehat{H} \to \mathscr{F}(P_0)$. By construction of F_0, it is sufficient to prove the assertion for all $a \in F_0$. Since $F^\times/H^\times$ is a torsion group, it is sufficient to prove the assertion for all $a \in \mathscr{F}(P_0)$. Let $a \in \mathscr{F}(P_0)$. Since $\mathscr{C}(\widehat{H})$ is finite, there is an $n'_a \in \mathbb{N}$ such that $a^{n'_a} \in \widehat{H}$. Since $\widehat{H} = \widetilde{H}$, there is an $n''_a \in \mathbb{N}$ such that $(a^{n'_a})^{n''_a} \in H$.

(b) $\Rightarrow$ (a) For every $p \in P$ there is an $n_p \in \mathbb{N}$ such that $p^{n_p} \in H$ whence $\mathsf{v}_p(p^{n_p}) = n_p > 0$. Clearly, we have $\widehat{H} \subset \widehat{F} = F$, and hence $\widehat{H} \subset \mathsf{q}(\widehat{H}) \cap F = \mathsf{q}(H) \cap F$. Since for each $a \in F$ there is an $n_a \in \mathbb{N}_0$ with $a^{n_a} \in H$, we infer that $\mathsf{q}(H) \cap F \subset \widetilde{H} = \widehat{H}$ and hence $\widehat{H} = \mathsf{q}(H) \cap F$. Furthermore, $H \subset F$ and $\widehat{H} \subset F$ are cofinal, and $\mathsf{q}(F)/\mathsf{q}(H) = F/H$ is a torsion group. Clearly, $\mathsf{q}(H) \cap F \subset F$ is saturated, and thus $\widehat{H}$ is Krull. Since $\widehat{H}^\times = \widehat{H} \cap F^\times$ and $H^\times = \widehat{H}^\times \cap H$, it follows that $H^\times = H \cap F^\times$ and then we obtain that $F^\times/H^\times$ is a torsion group.

By 1., $\widehat{H}/H^\times$ is finitely generated, say $\widehat{H}/H^\times = \{u_1 H^\times, \ldots, u_n H^\times\}$, and set $P_0 = \{p \in P \colon p$ divides $u_1 \cdot \cdots \cdot u_n$ in $F\}$. Then P_0 is finite, and we assert that $P_0 = P$. If there would exist some $p \in P \backslash P_0$, then there is an $n_p \in \mathbb{N}$ such that $p^{n_p} \in H$, and hence $p^{n_p} H^\times$ is a product of $u_1 H^\times, \ldots, u_n H^\times$, a contradiction. Therefore P is finite, $F/F^\times$ is a finitely generated monoid, $\mathsf{q}(F)/F^\times$ is a finitely generated group, and therefore $\mathsf{q}(F)/\mathsf{q}(H)F^\times$ is a finitely generated torsion group and thus finite. Since $\varphi \colon \widehat{H} \to F \to F/F^\times$ is a divisor homomorphism and $\mathscr{C}(\varphi) = \mathsf{q}(F)/\mathsf{q}(H)F^\times$, Proposition 2.2.1 implies that $\mathscr{C}(\widehat{H})$ is an epimorphic image of a submonoid of $\mathsf{q}(F)/\mathsf{q}(H)F^\times$ and thus $\mathscr{C}(\widehat{H})$ is finite. Thus 2. implies that H is a C-monoid (indeed, Property 2.(b) of Proposition 2.4 holds and hence H is a C-monoid defined in F).

2.5 Davenport Constants of BF-Monoids

Let H be a BF-monoid. For every $k \in \mathbb{N}$, we study the sets

$$\mathscr{M}_k(H) = \{a \in H \colon \max \mathsf{L}(a) \leq k\} \quad \text{and} \quad \overline{\mathscr{M}}_k(H) = \{a \in H \colon \max \mathsf{L}(a) = k\}.$$

A monoid homomorphism $|\cdot| \colon H \to (\mathbb{N}_0, +)$ will be called a *degree function* on H. In this section, we study abstract monoids having a degree function. The results will be applied in particular to monoids of product-one sequences and to monoids $\mathscr{B}(G, V)$ (see Sects. 3.3 and 4.4). In all our applications the monoid H will be a submonoid of a factorial monoid F and if not stated otherwise the degree function on H will be the restriction of the length function on F.

If $\theta \colon H \to B$ is a homomorphism and H and B have degree functions, then we say that θ is *degree preserving* if $|a|_H = |\theta(a)|_B$ for all $a \in H$. Suppose we are given a degree function on H and $k \in \mathbb{N}$, then

$$\mathsf{D}_k(H) = \sup\{|a| \colon a \in \mathscr{M}_k(H)\} \in \mathbb{N}_0 \cup \{\infty\}$$

is called the *large kth Davenport constant* of H (with respect to $|\cdot|_H$). Clearly, $\mathscr{M}_1(H) = \mathscr{A}(H) \cup H^\times$. We call $\mathsf{D}(H) = \mathsf{D}_1(H) = \sup\{|a| \colon a \in \mathscr{A}(H)\} \in \mathbb{N}_0 \cup \{\infty\}$ the *Davenport constant* of H. For every $k \in \mathbb{N}$, we have $\mathscr{M}_k(H) \subset \mathscr{M}_{k+1}(H)$, $\mathsf{D}_k(H) \leq \mathsf{D}_{k+1}(H)$, and $\mathsf{D}_k(H) \leq k\mathsf{D}(H)$. Furthermore, we have $|u| = 0$ for every unit $u \in H^\times$. Therefore, the degree function on H induces automatically a degree function $|\cdot| \colon H_{\mathrm{red}} \to (\mathbb{N}_0, +)$, and so the kth Davenport constant of H_{red} is defined. Obviously we have $\mathsf{D}_k(H) = \mathsf{D}_k(H_{\mathrm{red}})$. Let $\mathsf{e}(H)$ denote the smallest $\ell \in \mathbb{N}_0 \cup \{\infty\}$ with the following property:

> There is a $K \in \mathbb{N}_0$ such that every $a \in H$ with $|a| \geq K$ is divisible by an element $b \in H \backslash H^\times$ with $|b| \leq \ell$.

Clearly, $\mathsf{e}(H) \leq \mathsf{D}(H)$.

Proposition 2.7 *Let H be a* BF*-monoid and* $|\cdot| \colon H \to (\mathbb{N}_0, +)$ *be a degree function.*

1. *If H_{red} is finitely generated, then the sets $\mathscr{M}_k(H_{\mathrm{red}})$ are finite and $\mathsf{D}_k(H) < \infty$ for every $k \in \mathbb{N}$.*
2. *If $\mathsf{D}(H) < \infty$, then there exist constants $D_H, K_H \in \mathbb{N}_0$ such that $\mathsf{D}_k(H) = k\mathsf{e}(H) + D_H$ for all $k \geq K_H$.*
3. *If $\mathsf{D}(H) < \infty$, then the map $\mathbb{N} \to \mathbb{Q}$, $k \mapsto \frac{\mathsf{D}_k(H)}{k}$ is nonincreasing.*
4. *Suppose that H has a prime element. Then*

$$\mathsf{D}_k(H) = \max\{|a| \colon a \in \overline{\mathscr{M}}_k(H)\} \leq k\mathsf{D}(H)$$

and

$$k\mathsf{D}(H) = \max\{|a| \colon a \in H,\ \min\mathsf{L}(a) \leq k\} = \max\{|a| \colon a \in H,\ k \in \mathsf{L}(a)\}.$$

Proof 1. Suppose that H_{red} is finitely generated. Then $\mathscr{A}(H_{\mathrm{red}})$ is finite whence $\mathscr{M}_k(H)$ is finite for every $k \in \mathbb{N}$. It follows that $\mathsf{D}(H) < \infty$ and $\mathsf{D}_k(H) \leq k\mathsf{D}(H) < \infty$ for all $k \in \mathbb{N}$.

2. Suppose that $\mathsf{D}(H) < \infty$ and note that $\mathsf{e}(H) \leq \mathsf{D}(H)$. Let $\mathsf{f}(H) \in \mathbb{N}_0$ be the smallest $K \in \mathbb{N}_0$ such that every $a \in H$ with $|a| \geq K$ is divisible by an element $b \in H$ with $|b| \leq \mathsf{e}(H)$. We define $A = \{a \in \mathscr{A}(H) \colon |a| = \mathsf{e}(H)\}$. Let $k \in \mathbb{N}$ and continue with the following assertion.

A. There exist $a_1, \ldots, a_k \in A$ such that $a_1 \ldots a_k \in \mathscr{M}_k(H)$. In particular, $\mathsf{D}_k(H) \geq |a_1 \ldots a_k| = k\mathsf{e}(H)$.

Proof of **A.** Assume to the contrary that for all $a_1, \ldots, a_k \in A$ the product $a_1 \ldots a_k$ is divisible by an atom $u \in \mathscr{A}(H)$ with $|u| < \mathsf{e}(H)$. We set $K = \mathsf{f}(H) + (k-1)\mathsf{e}(H)$ and choose $a \in H$ with $|a| \geq K$. Then a can be written in the form $a = a_1 \ldots a_k b$ where $a_1, \ldots, a_k, b \in H$ and $|a_i| \leq \mathsf{e}(H)$ for all $i \in [1, k]$. If there is some $i \in [1, k]$ with $|a_i| < \mathsf{e}(H)$, then a_i is a divisor of a with $|a_i| < \mathsf{e}(H)$. Otherwise, $a_1, \ldots, a_k \in A$ and by our assumption the product $a_1 \ldots a_k$ and hence a has a divisor of degree strictly smaller than $\mathsf{e}(H)$. This is a contradiction to the definition of $\mathsf{e}(H)$. $\square$(Proof of **A**)

Now let $k \geq \mathsf{f}(H)/\mathsf{e}(H) - 1$. Then **A** implies that $\mathsf{D}_k(H) + \mathsf{e}(H) \geq (k+1)\mathsf{e}(H) \geq \mathsf{f}(H)$. Let $a \in H$ with $|a| > \mathsf{D}_k(H) + \mathsf{e}(H)$. Then, by definition of $\mathsf{f}(H)$, there are $b, c \in H$ such that $a = bc$ with $|c| \leq \mathsf{e}(H)$ and hence $|b| > \mathsf{D}_k(H)$. This implies that $\max \mathsf{L}(b) > k$, whence $\max \mathsf{L}(a) > k+1$ and $a \notin \mathscr{M}_{k+1}(H)$. Therefore, we obtain that $\mathsf{D}_{k+1}(H) \leq \mathsf{D}_k(H) + \mathsf{e}(H)$ and thus

$$0 \leq \mathsf{D}_{k+1}(H) - (k+1)\mathsf{e}(H) \leq \mathsf{D}_k(H) - k\mathsf{e}(H).$$

Since a non-increasing sequence of nonnegative integers stabilizes, the assertion follows.

3. Suppose that $\mathsf{D}(H) < \infty$. Let $k \in \mathbb{N}$, $a \in \mathscr{M}_{k+1}(H)$ with $|a| = \mathsf{D}_{k+1}(H)$, and set $l = \max \mathsf{L}(a)$. Then $l \leq k+1$. If $l \leq k$, then $a \in \mathscr{M}_k(H)$ and $\mathsf{D}_{k+1}(H) \geq \mathsf{D}_k(H) \geq |a| = \mathsf{D}_{k+1}(H)$ whence $\mathsf{D}_k(H) = \mathsf{D}_{k+1}(H)$. Suppose that $l = k+1$. We set $a = a_1 \ldots a_{k+1}$ with $a_1, \ldots, a_{k+1} \in \mathscr{A}(H)$ and $|a_1| \geq \cdots \geq |a_{k+1}|$ whence $|a_{k+1}| \leq (|a_1| + \cdots + |a_k|)/k$. It follows that

$$\frac{\mathsf{D}_{k+1}(H)}{k+1} = \frac{|a_1| + \cdots + |a_{k+1}|}{k+1} \leq \frac{|a_1| + \cdots + |a_k|}{k} \leq \frac{\mathsf{D}_k(H)}{k},$$

where the last inequality holds because $a_1 \ldots a_k \in \mathscr{M}_k(H)$.

4. Let $p \in H$ be a prime element. We assert that

$$\mathsf{D}_k(H) \leq \max\{|a| : a \in H, \ \max \mathsf{L}(a) = k\}. \tag{$*$}$$

Indeed, if $a \in \mathscr{M}_k(H)$ and $\max \mathsf{L}(a) = l \leq k$, then $ap^{k-l} \in \mathscr{M}_k(H)$ and

$$|a| \leq |ap^{k-l}| \leq \max\{|a| : a \in H, \ \max \mathsf{L}(a) = k\},$$

and hence $(*)$ follows. Next, we assert that

$$\max\{|a| : a \in H, \ \min \mathsf{L}(a) \leq k\} \leq k\mathsf{D}(H). \tag{$**$}$$

Let $a \in H$ with $\min \mathsf{L}(a) = l \leq k$, say $a = u_1 \ldots u_l$, where $u_1, \ldots, u_l \in \mathscr{A}(H)$. Then $|a| = |u_1| + \cdots + |u_l| \leq l\mathsf{D}(H) \leq k\mathsf{D}(H)$, and thus $(**)$ follows. Using $(*)$ and $(**)$ we infer that

$$\mathsf{D}_k(H) \leq \max\{|a| : a \in H, \ \max \mathsf{L}(a) = k\} \leq \max\{|a| : a \in H, \ \max \mathsf{L}(a) \leq k\}$$
$$= \mathsf{D}_k(H) \leq \max\{|a| : a \in H, \ \min \mathsf{L}(a) \leq k\}$$

and that

$$k\mathsf{D}(H) = \max\{|a| : a \in H, \ k \in \mathsf{L}(a)\} \leq \max\{|a| : a \in H, \ \min \mathsf{L}(a) \leq k\} \leq k\mathsf{D}(H).$$

Let F be a factorial monoid and $H \subset F$ a submonoid such that $H^\times = H \cap F^\times$. Then H is a BF-monoid by [40, Corollary 1.3.3]. For $k \in \mathbb{N}$, let $\mathscr{M}_k^*(H)$ denote the

set of all $a \in F$ such that a is not divisible by a product of k non-units of H. The restriction of the usual length function $|\cdot|\colon F \to \mathbb{N}_0$ on F (introduced in Sect. 2.1) gives a degree function on H. We define the *small kth Davenport constant* $\mathsf{d}_k(H)$ as

$$\mathsf{d}_k(H) = \sup\{|a|\colon a \in \mathscr{M}_k^*(H)\} \in \mathbb{N}_0 \cup \{\infty\}. \tag{1}$$

In other words, $1 + \mathsf{d}_k(H)$ is the smallest integer $\ell \in \mathbb{N}$ such that every $a \in F$ of length $|a| \geq \ell$ is divisible by a product of k non-units of H. We call $\mathsf{d}(H) = \mathsf{d}_1(H)$ the *small Davenport constant* of H. Clearly we have $\mathscr{M}_k^*(H) \subset \mathscr{M}_{k+1}^*(H)$ hence $\mathsf{d}_k(H) \leq \mathsf{d}_{k+1}(H)$.

Furthermore, let $\eta(H)$ denote the smallest integer $\ell \in \mathbb{N} \cup \{\infty\}$ such that every $a \in F$ with $|a| \geq \ell$ has a divisor $b \in H \backslash H^\times$ with $|b| \in [1, \mathsf{e}(H)]$. For $p \in \mathscr{A}(F)$ denote by o_p the smallest integer $\ell \in \mathbb{N} \cup \{\infty\}$ such that $p^{o_p} \in H$. Clearly, we have $o_p \leq \eta(H)$ for all $p \in \mathscr{A}(F)$.

Proposition 2.8 *Let $F = F^\times \times \mathscr{F}(P)$ be a factorial monoid and $H \subset F$ a submonoid such that $H^\times = H \cap F^\times$, and let $k \in \mathbb{N}$.*

1. *If for every $a \in F$ there is a prime $p \in F$ such that $ap \in H$, then $1 + \mathsf{d}_k(H) \leq \mathsf{D}_k(H)$.*
2. *Suppose that H_{red} is finitely generated and that for every $a \in F$ there is an $n_a \in H$ such that $a^{n_a} \in H$. Then H is a C-monoid and we have*

   (a) *$\mathsf{e}(H) = \max\{o_p\colon p \in P\}$ and $\eta(H) < \infty$.*
   (b) *$\mathsf{d}_k(H) + 1 \geq k\mathsf{e}(H)$ and there exist constants $d_H \in \mathbb{Z}_{\geq -1}, k_H \in \mathbb{N}_0$ such that $\mathsf{d}_k(H) = k\mathsf{e}(H) + d_H$ for all $k \geq k_H$.*

Proof 1. Let $a \in \mathscr{M}_k^*(H)$ such that $|a| = \mathsf{d}_k(H)$. We choose a prime $p \in F$ such that $ap \in H$. Take any factorization $ap = u_1 \ldots u_\ell$ where $u_i \in \mathscr{A}(H)$. We may assume that $p \mid u_1$ in F. Then $u_2 \ldots u_\ell \mid a$ in F, and hence, $\ell - 1 < k$. Thus, it follows that $ap \in \mathscr{M}_k(H)$ and $\mathsf{D}_k(H) \geq |ap| = |a| + 1 \geq \mathsf{d}_k(H) + 1$.

2.(a) By Proposition 2.6.3, H is a C-monoid, P is finite and hence $\mathsf{e}(H) < \infty$. If $p \in P$, then $p^{o_p} \in \mathscr{A}(H)$ and by the minimality of o_p, p^{o_p} does not have a divisor $b \in H \backslash H^\times$ such that $|b| < o_p$. Thus, it follows that $\mathsf{e}(H) \geq \max\{o_p\colon p \in P\}$. For the reverse inequality, note that by Proposition 2.4.2 there exists an $\alpha \in \mathbb{N}$ such that for all $p \in P$ and all $a \in p^\alpha F$ we have $a \in H$ if and only if $p^\alpha a \in H$. Since any multiple of α has the same property, we may assume that α is divisible by o_p for all $p \in P$. Let $b \in H$ with $|b| > |P|(2\alpha - 1)$. Then, there exists a $p \in P$ such that $b \in p^{2\alpha} F \cap H$. Hence b is divisible in H by p^α, implying in turn that $p^{o_p} \in \mathscr{A}(H)$ divides b in H. Therefore, we obtain that $\mathsf{e}(H) \leq \max\{o_p\colon p \in P\}$.

If $a \in F$ with $|a| \geq \sum_{p \in P}(o_p - 1)$, then there is a $p \in P$ such that p^{o_p} divides a in F, and thus $\eta(H) \leq 1 + \sum_{p \in P}(o_p - 1)$.

2.(b) Let $p \in P$ with $o(p) = \mathsf{e}(H)$. Then $p^{ko_p - 1} \in \mathscr{M}_k^*(H)$ and $|p^{ko_p - 1}| = k\mathsf{e}(H) - 1$, showing the inequality $\mathsf{d}_k(H) + 1 \geq k\mathsf{e}(H)$ for all $k \in \mathbb{N}$. Now let $k \in \mathbb{N}$ be such that $1 + \mathsf{d}_k(H) + \mathsf{e}(H) \geq \eta(H)$, and let $a \in F$ with $|a| \geq \mathsf{d}_k(H) + \mathsf{e}(H) + 1$. Then, by definition of $\eta(H)$, there are $b \in F$ and $c \in H \backslash H^\times$ such that $a = bc$ with $|c| \leq$

$e(H)$ and $|b| > d_k(H)$. This implies that b is divisible by a product of k non-units of H whence a is divisible by a product of $k + 1$ non-units of H. Therefore, it follows that $1 + d_{k+1}(H) \leq d_k(H) + e(H) + 1$ and hence

$$0 \leq d_{k+1}(H) - ke(H) \leq d_k(H) - (k - 1)e(H) \quad \text{for all sufficiently large} \quad k.$$

Since a nonincreasing sequence of nonnegative integers stabilizes, the assertion follows.

3 Arithmetic Combinatorics: Zero-Sum Results with a Focus on Davenport Constants

This section is devoted to Zero-Sum Theory, a vivid subfield of Arithmetic Combinatorics (see [32, 37, 49]). In Sect. 3.1 we give an algebraic study of the monoid of product-one sequences over finite but not necessarily abelian groups. In Sect. 3.2 we put together well-known material on transfer homomorphisms used in Sects. 4.2 and 4.3. In Sects. 3.3 and 3.4 we consider the kth Davenport constants of finite groups. In particular, we gather results which will be needed in Sect. 5.2 and results having relevance in invariant theory by Proposition 4.7.

3.1 The Monoid of Product-One Sequences

Let $G_0 \subset G$ be a subset and let $G' = [G, G] = \langle g^{-1}h^{-1}gh \colon g, h \in G \rangle$ denote the commutator subgroup of G. A *sequence* over G_0 means a finite sequence of terms from G_0 which is unordered and repetition of terms is allowed, and it will be considered as an element of the free abelian monoid $\mathscr{F}(G_0)$. In order to distinguish between the group operation in G and the operation in $\mathscr{F}(G_0)$, we use the symbol $\cdot$ for the multiplication in $\mathscr{F}(G_0)$, hence $\mathscr{F}(G_0) = (\mathscr{F}(G_0), \cdot)$—this coincides with the convention in the monographs [40, 49]—and we denote multiplication in G by juxtaposition of elements. To clarify this, if $S_1, S_2 \in \mathscr{F}(G_0)$ and $g_1, g_2 \in G_0$, then $S_1 \cdot S_2 \in \mathscr{F}(G_0)$ has length $|S_1| + |S_2|$, $S_1 \cdot g_1 \in \mathscr{F}(G_0)$ has length $|S_1| + 1$, $g_1 \cdot g_2 \in \mathscr{F}(G_0)$ is a sequence of length 2, but g_1g_2 is an element of G. Furthermore, in order to avoid confusion between exponentiation in G and exponentiation in $\mathscr{F}(G_0)$, we use brackets for the exponentiation in $\mathscr{F}(G_0)$. So for $g \in G_0$, $S \in \mathscr{F}(G_0)$, and $k \in \mathbb{N}_0$, we have

$$g^{[k]} = \underbrace{g \cdot \dots \cdot g}_{k} \in \mathscr{F}(G) \quad \text{with} \quad |g^{[k]}| = k, \quad \text{and} \quad S^{[k]} = \underbrace{S \cdot \dots \cdot S}_{k} \in \mathscr{F}(G).$$

Now let

$$S = g_1 \cdot \ldots \cdot g_\ell = \prod_{g \in G_0} g^{\mathsf{v}_g(S)},$$

be a sequence over G_0 (in this notation, we tacitly assume that $\ell \in \mathbb{N}_0$ and $g_1, \ldots, g_\ell \in G_0$). Then $|S| = \ell = 0$ if and only if $S = 1_{\mathscr{F}(G_0)}$ is the identity element in $\mathscr{F}(G_0)$, and then S will also be called the *trivial sequence*. The elements in $\mathscr{F}(G_0) \setminus \{1_{\mathscr{F}(G_0)}\}$ are called *nontrivial sequences*. We use all notions of divisibility theory in general free abelian monoids. Thus, for an element $g \in G_0$, we refer to $\mathsf{v}_g(S)$ as the *multiplicity* of g in S. A divisor T of S will also be called a subsequence of S. We call $\mathrm{supp}(S) = \{g_1, \ldots, g_\ell\} \subset G_0$ the *support* of S. When G is written multiplicatively (with unit element $1_G \in G$), we use

$$\pi(S) = \{g_{\tau(1)} \ldots g_{\tau(\ell)} \in G \colon \tau \text{ a permutation of } [1, \ell]\} \subset G$$

to denote the *set of products* of S (if $|S| = 0$, we use the convention that $\pi(S) = \{1_G\}$). Clearly, $\pi(S)$ is contained in a G'-coset. When G is written additively with commutative operation, we likewise let

$$\sigma(S) = g_1 + \cdots + g_\ell \in G$$

denote the *sum* of S. Furthermore, we denote by

$$\Sigma(S) = \{\sigma(T) \colon T \mid S \text{ and } 1 \neq T\} \subset G \quad \text{and} \quad \Pi(S) = \bigcup_{\substack{T \mid S \\ 1 \neq T}} \pi(T) \subset G,$$

the *subsequence sums* and *subsequence products* of S. The sequence S is called

- a *product-one sequence* if $1_G \in \pi(S)$,
- *product-one free* if $1_G \notin \Pi(S)$.

Every map of finite groups $\varphi \colon G_1 \to G_2$ extends to a homomorphism $\varphi \colon \mathscr{F}(G_1) \to \mathscr{F}(G_2)$ where $\varphi(S) = \varphi(g_1) \cdot \ldots \cdot \varphi(g_\ell)$. If φ is a group homomorphism, then $\varphi(S)$ is a product-one sequence if and only if $\pi(S) \cap \mathrm{Ker}(\varphi) \neq \emptyset$. We denote by

$$\mathscr{B}(G_0) = \{S \in \mathscr{F}(G_0) \colon 1_G \in \pi(S)\}$$

the set of all product-one sequences over G_0, and clearly $\mathscr{B}(G_0) \subset \mathscr{F}(G_0)$ is a submonoid. We will use all concepts introduced in Sect. 2.5 for the monoid $\mathscr{B}(G_0)$ with the degree function stemming from the length function on the free abelian monoid $\mathscr{F}(G_0)$. For all notations $*(H)$ introduced for a monoid H we write—as usual—$*(G_0)$ instead of $*(\mathscr{B}(G_0))$. In particular, for $k \in \mathbb{N}$, we set $\mathscr{M}_k(G_0) = \mathscr{M}_k(\mathscr{B}(G_0))$, $\mathsf{D}_k(G_0) = \mathsf{D}_k(\mathscr{B}(G_0))$, $\eta(G_0) = \eta(\mathscr{B}(G_0))$, $\mathsf{e}(G_0) = \mathsf{e}(\mathscr{B}(G_0))$, and so on. By Proposition 2.8.2(a), $\mathsf{e}(G_0) = \max\{\mathrm{ord}(g) \colon g \in G_0\}$. Note that $\mathscr{M}_1^*(G_0)$ is the set of all product-one free sequences over G_0. In particular,

$$\mathsf{D}(G_0) = \sup\{|S|: S \in \mathscr{A}(G_0)\} \in \mathbb{N} \cup \{\infty\}$$

is the *large Davenport constant* of G_0, and

$$\mathsf{d}(G_0) = \sup\{|S|: S \in \mathscr{F}(G_0) \text{ is product-one free}\} \in \mathbb{N}_0 \cup \{\infty\}$$

is the *small Davenport constant* of G_0. Their study will be the focus of the Sects. 3.3 and 3.4.

Lemma 3.1 *Let $G_0 \subset G$ be a subset.*

1. $\mathscr{B}(G_0) \subset \mathscr{F}(G_0)$ *is a reduced finitely generated submonoid, $\mathscr{A}(G_0)$ is finite, and $\mathsf{D}(G_0) \leq |G|$. Furthermore, $\mathscr{M}_k(G_0)$ is finite and $\mathsf{D}_k(G_0) < \infty$ for all $k \in \mathbb{N}$.*
2. *Let $S \in \mathscr{F}(G)$ be product-one free.*

   a. *If $g_0 \in \pi(S)$, then $g_0^{-1} \cdot S \in \mathscr{A}(G)$. In particular, $\mathsf{d}(G) + 1 \leq \mathsf{D}(G)$.*
   b. *If $|S| = \mathsf{d}(G)$, then $\Pi(S) = G\backslash\{1_G\}$ and hence $\mathsf{d}(G) = \max\{|S|: S \in \mathscr{F}(G) \text{ with } \Pi(S) = G\backslash\{1_G\}\}$.*

3. *If G is cyclic, then $\mathsf{d}(G) + 1 = \mathsf{D}(G) = |G|$.*

Proof 1. We assert that for every $U \in \mathscr{A}(G)$ we have $|U| \leq |G|$. Then $\mathscr{A}(G_0) \subset \mathscr{A}(G)$ is finite and $\mathsf{D}(G_0) \leq \mathsf{D}(G) \leq |G|$. As already mentioned, $\mathscr{B}(G_0) \subset \mathscr{F}(G_0)$ is a submonoid, and clearly $\mathscr{B}(G_0)^{\times} = \{1_{\mathscr{F}(G_0)}\}$. Since $\mathscr{F}(G_0)$ is factorial and $\mathscr{B}(G_0)^{\times} = \mathscr{B}(G_0) \cap \mathscr{F}(G_0)^{\times}$, $\mathscr{B}(G_0)$ is atomic by [40, Corollary 1.3.3]. This means that $\mathscr{B}(G_0) = [\mathscr{A}(G_0) \cup \mathscr{B}(G_0)^{\times}]$, and thus, $\mathscr{B}(G_0)$ is finitely generated. Since $\mathscr{B}(G_0)$ is reduced and finitely generated, the sets $\mathscr{M}_k(G_0)$ are finite by Proposition 2.7.

Now let $U \in \mathscr{B}(G)$, say $U = g_1 \cdot \ldots \cdot g_\ell$ with $g_1 g_2 \ldots g_\ell = 1_G$. We suppose that $\ell > |G|$ and show that $U \notin \mathscr{A}(G)$. Consider the set

$$M = \{g_1 g_2 \ldots g_i: i \in [1, \ell]\}.$$

Since $\ell > |G|$, there are $i, j \in [1, \ell]$ with $i < j$ and $g_1 \ldots g_i = g_1 \ldots g_j$. Then $g_{i+1} \ldots g_j = 1_G$ and thus $g_1 \ldots g_i g_{j+1} \ldots g_\ell = 1_G$ which implies that U is the product of two nontrivial product-one subsequences.

2.(a) If $g_0 \in \pi(S)$, then S can be written as $S = g_1 \cdot \ldots \cdot g_\ell$ such that $g_0 = g_1 \ldots g_\ell$, which implies that $g_0^{-1} \cdot g_1 \cdot \ldots \cdot g_\ell \in \mathscr{A}(G)$.

2.(b) If S is product-one free with $|S| = \mathsf{d}(G)$, and if there would be an $h \in G\backslash\{\Pi(S) \cup \{1_G\}\}$, then $T = h^{-1} \cdot S$ would be product-one free of length $|T| = |S| + 1 > \mathsf{d}(G)$, a contradiction. Thus every product-one free sequence S of length $|S| = \mathsf{d}(G)$ satisfies $\Pi(S) = G\backslash\{1_G\}$. If S is a sequence with $\Pi(S) = G\backslash\{1_G\}$, then S is product-one free and hence $|S| \leq \mathsf{d}(G)$.

3. Clearly, the assertion holds for $|G| = 1$. Suppose that G is cyclic of order $n \geq 2$, and let $g \in G$ with $\text{ord}(g) = n$. Then $g^{[n-1]}$ is product-one free, and thus 1. and 2. imply that $n \leq 1 + \mathsf{d}(G) \leq \mathsf{D}(G) \leq n$.

The next result gathers the algebraic properties of monoids of product-one sequences and highlights the difference between the abelian and the non-abelian case.

Theorem 3.2 *Let $G_0 \subset G$ be a subset and let G' denote the commutator subgroup of $\langle G_0 \rangle$.*

1. *$\mathcal{B}(G_0) \subset \mathcal{F}(G_0)$ is cofinal and $\mathcal{B}(G_0)$ is a finitely generated C-monoid. $\widehat{\mathcal{B}(G_0)} = \overline{\mathcal{B}(G_0)}$ is a finitely generated Krull monoid, the embedding $\widehat{\mathcal{B}(G_0)} \hookrightarrow \mathcal{F}(G_0)$ is a cofinal divisor homomorphism with class group $\mathcal{F}(G_0)/\mathcal{B}(G_0)$, and the map*

$$\Phi : \mathcal{F}(G_0)/\mathcal{B}(G_0) \longrightarrow \langle G_0 \rangle / G'$$
$$[S]_{\mathcal{F}(G_0)/\mathcal{B}(G_0)} \longmapsto gG' \text{ for any } g \in \pi(S)$$

   is a group epimorphism. Suppose that $G_0 = G$. Then Φ is an isomorphism, every class of $\mathcal{C}(\widehat{\mathcal{B}(G)})$ contains a prime divisor, and if $|G| \neq 2$, then $\widehat{\mathcal{B}(G)} \hookrightarrow \mathcal{F}(G)$ is a divisor theory.

2. *The following statements are equivalent:*

   (a) *$\mathcal{B}(G_0)$ is a Krull monoid.*
   (b) *$\mathcal{B}(G_0)$ is root closed.*
   (c) *$\mathcal{B}(G_0) \subset \mathcal{F}(G_0)$ is saturated.*

3. *$\mathcal{B}(G)$ is a Krull monoid if and only if G is abelian.*
4. *$\mathcal{B}(G)$ is factorial if and only if $|G| \leq 2$.*

Proof 1. $\mathcal{B}(G_0)$ is finitely generated by Lemma 3.1. If $n = \text{lcm}\{\text{ord}(g) : g \in G_0\}$, then $S^{[n]} \in \mathcal{B}(G_0)$ for each $S \in \mathcal{F}(G_0)$. Thus $\mathcal{B}(G_0) \subset \mathcal{F}(G_0)$ and $\widehat{\mathcal{B}(G_0)} \hookrightarrow \mathcal{F}(G_0)$ are cofinal, $\mathcal{F}(G_0)/\mathcal{B}(G_0)$ is a group and

$$\mathcal{F}(G_0)/\mathcal{B}(G_0) = \mathsf{q}(\mathcal{F}(G_0))/\mathsf{q}(\mathcal{B}(G_0)) = \mathsf{q}(\mathcal{F}(G_0))/\mathsf{q}(\widehat{\mathcal{B}(G_0)})$$

is the class group of the embedding $\widehat{\mathcal{B}(G_0)} \hookrightarrow \mathcal{F}(G_0)$. All statements on the structure of $\mathcal{B}(G_0)$ and $\widehat{\mathcal{B}(G_0)}$ follow from Proposition 2.6.3, and it remains to show the assertions on Φ.

Let $S, S' \in \mathcal{F}(G_0)$, $g \in \pi(S), g' \in \pi(S')$, and $B \in \mathcal{B}(G_0)$. Then $\pi(S) \subset gG'$, $\pi(S') \subset g'G'$, $\pi(B) \subset G'$, and $\pi(S \cdot B) \subset gG'$. We use the abbreviation $[S] = [S]_{\mathcal{F}(G_0)/\mathcal{B}(G_0)}$, and note that $[S] = [S']$ if and only if there are $C, C' \in \mathcal{B}(G_0)$ such that $S \cdot C = S' \cdot C'$.

In order to show that Φ is well-defined, suppose that $[S] = [S']$ and that $S \cdot C = S' \cdot C'$ with $C, C' \in \mathcal{B}(G_0)$. Then $\pi(S \cdot C) = \pi(S' \cdot C') \subset gG' \cap g'G'$, and hence $gG' = g'G'$. In order to show that Φ is surjective, let $g \in \langle G_0 \rangle$ be given. Clearly, there is an $S \in \mathcal{F}(G_0)$ such that $g \in \pi(S)$ whence $\Phi([S]) = gG'$.

Suppose that $G_0 = G$. First, we show that Φ is injective. Let $S, S' \in \mathscr{F}(G)$ with $g \in \pi(S), g' \in \pi(S')$ such that $gG' = g'G'$. Then there are $k \in \mathbb{N}, a_1, b_1, \ldots, a_k, b_k \in G$ such that

$$gg'^{-1} = \prod_{i=1}^{k} (a_i^{-1} b_i^{-1} a_i b_i).$$

We define $T = \prod_{i=1}^{k} (a_i^{-1} \cdot b_i^{-1} \cdot a_i \cdot b_i)$ and obtain that

$$S \cdot (S' \cdot g^{-1} \cdot T) = S' \cdot (S \cdot g^{-1} \cdot T) \in \mathscr{F}(G).$$

Since $1 \in \pi(T)$ and $gg'^{-1} \in \pi(T)$, it follows that $1 \in \pi(S' \cdot g^{-1} \cdot T)$ and $1 \in \pi(S \cdot g^{-1} \cdot T)$ which implies that $[S] = [S']$.

If $|G| \le 2$, then 4. will show that $\mathscr{B}(G)$ is factorial and clearly the trivial class contains a prime divisor. Suppose that $|G| \ge 3$. In order to show that $\widehat{\mathscr{B}(G)} \hookrightarrow \mathscr{F}(G)$ is a divisor theory, let $g \in G\backslash\{1_G\}$ be given. Then there is an $h \in G\backslash\{g^{-1}, 1_G\}$, $U = g \cdot g^{-1} \in \mathscr{A}(G) \subset \widehat{\mathscr{B}(G)}$, $U' = g \cdot h \cdot (h^{-1}g^{-1}) \in \mathscr{A}(G) \subset \widehat{\mathscr{B}(G)}$, and $g = \gcd_{\mathscr{F}(G)}(U, U')$. Thus $\widehat{\mathscr{B}(G)} \hookrightarrow \mathscr{F}(G)$ is a divisor theory.

Let $S \in \mathscr{F}(G)$ with $g \in \pi(S)$. Then $g \in \mathscr{F}(G)$ is a prime divisor and we show that $[g] = [S]$. Indeed, if $g = 1_G$, then $S \in \mathscr{B}(G), 1_G \in \mathscr{B}(G), S \cdot 1_G = g \cdot S$ whence $[g] = [S]$. If $\mathrm{ord}(g) = n \ge 2$, then $g^{[n]} \in \mathscr{B}(G), S \cdot g^{[n-1]} \in \mathscr{B}(G), S \cdot g^{[n]} = g \cdot S \cdot g^{[n-1]}$ whence $[S] = [g]$.

2. (a) $\Rightarrow$ (b) Every Krull monoid is completely integrally closed and hence root closed.

(b) $\Rightarrow$ (c) Let $S, T \in \mathscr{B}(G_0)$ with $T \mid S$ in $\mathscr{F}(G_0)$, say $S = T \cdot U$ where $U = g_1 \cdot \ldots \cdot g_\ell \in \mathscr{F}(G_0)$. If $n = \mathrm{lcm}(\mathrm{ord}(g_1), \ldots, \mathrm{ord}(g_\ell))$, then $(T^{[-1]} \cdot S)^{[n]} = U^{[n]} \in \mathscr{B}(G_0)$. Since $\mathscr{B}(G_0)$ is root closed, this implies that $U = T^{[-1]} \cdot S \in \mathscr{B}(G_0)$ and hence $T \mid S$ in $\mathscr{B}(G_0)$.

(c) $\Rightarrow$ (a) Since $\mathscr{F}(G_0)$ is free abelian, $\mathscr{B}(G_0)$ is Krull by Theorem 2.1.

3. If G is a abelian, then it is obvious that $\mathscr{B}(G) \subset \mathscr{F}(G)$ is saturated, and thus $\mathscr{B}(G)$ is a Krull monoid by 2. Suppose that G is not abelian. Then there are $g, h \in G$ with $gh \ne hg$. Then $ghg^{-1} \ne h, S = g \cdot h \cdot g^{-1} \cdot (ghg^{-1})^{-1} \in \mathscr{B}(G), T = g \cdot g^{-1} \in \mathscr{B}(G)$ divides S in $\mathscr{F}(G)$ but $T^{[-1]} \cdot S = h \cdot (ghg^{-1})^{-1}$ does not have product-one. Thus $\mathscr{B}(G) \subset \mathscr{F}(G)$ is not saturated and hence $\mathscr{B}(G)$ is not Krull by 2.

4. If $G = \{0\}$, then $\mathscr{B}(G) = \mathscr{F}(G)$ is factorial. If $G = \{0, g\}$, then $\mathscr{A}(G) = \{0, g^{[2]}\}$, each atom is a prime, and $\mathscr{B}(G)$ is factorial. Conversely, suppose that $\mathscr{B}(G)$ is factorial. Then $\mathscr{B}(G)$ is a Krull monoid by [40, Corollary 2.3.13], and hence G is abelian by 3. Suppose that $|G| \ge 3$. We show that $\mathscr{B}(G)$ is not factorial. If there is an element $g \in G$ with $\mathrm{ord}(g) = n \ge 3$, then $U = g^{[n]}, -U = (-g)^{[n]}, W = (-g) \cdot g \in \mathscr{A}(G)$, and $U \cdot (-U) = W^{[n]}$. Suppose there is no $g \in G$ with $\mathrm{ord}(g) \ge 3$. Then there are $e_1, e_2 \in G$ with $\mathrm{ord}(e_1) = \mathrm{ord}(e_2) = 2$ and $e_1 + e_2 \ne 0$. Then $U = e_1 \cdot e_2 \cdot (e_1 + e_2), W_1 = e_1^{[2]}, W_2 = e_2^{[2]}, W_0 = (e_1 + e_2)^{[2]} \in \mathscr{A}(G)$, and $U^{[2]} = W_0 \cdot W_1 \cdot W_2$.

For a subset $G_0 \subset G$, the monoid $\mathscr{B}(G_0)$ may be Krull or just seminormal but it need not be Krull. We provide examples for both situations.

Proposition 3.3 *Let $G_0 \subset G$ be a subset satisfying the following property* **P***:*

P.   *For each two elements $g, h \in G_0$, $\langle h \rangle \subset \langle g, h \rangle$ is normal or $\langle g \rangle \subset \langle g, h \rangle$ is normal.*

Then $\mathscr{B}(G_0)$ is a Krull monoid if and only if $\langle G_0 \rangle$ is abelian.

Proof If $\langle G_0 \rangle$ is a abelian, then it is obvious that $\mathscr{B}(G_0) \subset \mathscr{F}(G_0)$ is saturated, and thus $\mathscr{B}(G_0)$ is Krull by Theorem 3.2.2.

Conversely, suppose that $\mathscr{B}(G_0)$ is Krull and that G_0 satisfies Property **P**. In order to show that $\langle G_0 \rangle$ is abelian, it is sufficient to prove that $gh = hg$ for each two elements $g, h \in G_0$. Let $g, h \in G_0$ be given such that $\langle h \rangle \subset \langle g, h \rangle$ is normal, $\mathrm{ord}(g) = m$, $\mathrm{ord}(h) = n$, and assume to the contrary that $ghg^{-1} \neq h$. Since $g\langle h \rangle g^{-1} = \langle h \rangle$, it follows that $ghg^{-1} = h^{\nu}$ for some $\nu \in [2, n-1]$. Thus $ghg^{m-1}h^{n-\nu} = 1$ and $S = g \cdot h \cdot g^{[m-1]} \cdot h^{[n-\nu]} \in \mathscr{B}(G_0)$. Clearly, $T = g^{[m]} \in \mathscr{B}(G_0)$ but $S \cdot T^{[-1]} = h^{[n-\nu+1]} \notin \mathscr{B}(G_0)$. Thus $\mathscr{B}(G_0) \subset \mathscr{F}(G_0)$ is not saturated, a contradiction.

Proposition 3.4 *Let $G = D_{2n}$ be the dihedral group, say $G = \langle a, b \rangle = \{1, a, \ldots, a^{n-1}, b, ab, \ldots, a^{n-1}b\}$, where $\mathrm{ord}(a) = n \geq 2$, $\mathrm{ord}(b) = 2$, and set $G_0 = \{ab, b\}$. Then, $\mathscr{B}(G_0)$ is a Krull monoid if and only if n is even.*

Proof Clearly, we have $\mathrm{ord}(ab) = \mathrm{ord}(b) = 2$ and $\langle G_0 \rangle = G$. Suppose that n is odd and consider the sequence $S = (ab)^{[n]} \cdot b^{[n]}$. Since $\big((ab)b\big)^n = 1$, it follows that S is a product-one sequence. Obviously, $S_1 = (ab)^{[n-1]} \cdot b^{[n-1]} \in \mathscr{B}(G_0)$ and $S_2 = (ab) \cdot b \notin \mathscr{B}(G_0)$. Since $S = S_1 \cdot S_2$, it follows that $\mathscr{B}(G_0) \subset \mathscr{F}(G_0)$ is not saturated, and hence $\mathscr{B}(G_0)$ is not Krull by Theorem 3.2.2.

Suppose that n is even. Then $\mathscr{A}(G_0) = \{(ab)^{[2]}, b^{[2]}\}$ and $\mathscr{B}(G_0) = \{(ab)^{[\ell]} \cdot b^{[m]} : \ell, m \in \mathbb{N}_0 \text{ even}\}$. This description of $\mathscr{B}(G_0)$ implies immediately that $\mathscr{B}(G_0) \subset \mathscr{F}(G_0)$ is saturated, and hence $\mathscr{B}(G_0)$ is Krull by Theorem 3.2.2.

Remark (*Seminormality of $\mathscr{B}(G_0)$*) A monoid H is called seminormal if for all $x \in \mathsf{q}(H)$ with $x^2, x^3 \in H$ it follows that $x \in H$. Thus, by definition, every root closed monoid is seminormal.

1. Let $n \equiv 3 \mod 4$ and $G = D_{2n}$ the dihedral group, say $G = \langle a, b \rangle = \{1, a, \ldots, a^{n-1}, b, ab, \ldots, a^{n-1}b\}$, where $\mathrm{ord}(a) = n$, $\mathrm{ord}(b) = 2$, and

$$a^k b a^l b = a^{k-l} \quad \text{for all } k, l \in \mathbb{Z}.$$

We consider the sequence

$$S = a^{\left[\frac{n-1}{2}\right]} \cdot b^{[2]} \in \mathscr{F}(G).$$

Then

$$S^{[2]} = \left(a^{\left[\frac{n-1}{2}\right]} \cdot b \cdot a^{\left[\frac{n-1}{2}\right]} \cdot b\right) \cdot (b \cdot b) \text{ and } S^{[3]} = a^{[n]} \cdot \left(a^{\left[\frac{n-3}{4}\right]} \cdot b \cdot a^{\left[\frac{n-3}{4}\right]} \cdot b\right) \cdot b^{[4]}$$

are both in $\mathscr{B}(G)$ whence $S \in \mathsf{q}\big(\mathscr{B}(G)\big)$, but obviously $S \notin \mathscr{B}(G)$. Thus $\mathscr{B}(\{a, b\})$ and $\mathscr{B}(G)$ are not seminormal.

2. Let $G = H_8 = \{E, I, J, K, -E, -I, -J, -K\}$ be the quaternion group with the relations

$$IJ = -JI = K, \ JK = -KJ = I, \quad \text{and} \quad KI = -IK = J,$$

and set $G_0 = \{I, J\}$. By Theorem 3.2, $\mathscr{B}(G)$ is not Krull and by Proposition 3.3, $\mathscr{B}(G_0)$ is not Krull. However, we assert that $\mathscr{B}(G_0)$ is seminormal.

First, we are going to derive an explicit description of $\mathscr{B}(G_0)$. Since $E = (-E)(-E) = (KK)(II) = (IJ)(IJ)(II)$, it follows that $U = I^{[4]} \cdot J^{[2]} \in \mathscr{B}(G_0)$. Assume that $U = U_1 \cdot U_2$ with $U_1, U_2 \in \mathscr{A}(G_0)$ and $|U_1| \leq |U_2|$. Then $|U_1| \in \{2, 3\}$, but U does not have a subsequence with product one and length two or three. Thus $U \in \mathscr{A}(G_0)$ and similarly we obtain that $I^{[2]} \cdot J^{[4]} \in \mathscr{A}(G_0)$. Since $\mathsf{D}(G_0) \leq \mathsf{D}(G) = 6$, it is easy to check that

$$\mathscr{A}(G_0) = \{I^{[4]}, J^{[4]}, I^{[2]} \cdot J^{[2]}, I^{[4]} \cdot J^{[2]}, I^{[2]} \cdot J^{[4]}\}.$$

This implies that

$$\mathscr{B}(G_0) = \{I^{[k]} \cdot J^{[l]} : k = l = 0 \text{ or } k, l \in \mathbb{N}_0 \text{ are both even with } k + l \geq 4\}.$$

In order to show that $\mathscr{B}(G_0)$ is seminormal, let $x \in \mathsf{q}\big(\mathscr{B}(G_0)\big)$ be given such that $x^{[2]}, x^{[3]} \in \mathscr{B}(G_0)$. We have to show that $x \in \mathscr{B}(G_0)$. Since $x^{[2]}, x^{[3]} \in \mathscr{B}(G_0) \subset \mathscr{F}(G_0)$ and $\mathscr{F}(G_0)$ is seminormal, it follows that $x \in \mathscr{F}(G_0)$. If $x = I^{[k]}$ with $k \in \mathbb{N}_0$, then $I^{[3k]} \in \mathscr{B}(G_0)$ implies that $4 \mid 3k$, hence $4 \mid k$, and thus $x \in \mathscr{B}(G_0)$. Similarly, if $x = J^{[l]} \in \mathscr{B}(G_0)$ with $l \in \mathbb{N}_0$, then $x \in \mathscr{B}(G_0)$. It remains to consider the case $x = I^{[k]} \cdot J^{[l]}$ with $k, l \in \mathbb{N}$. Since $x^{[3]} = I^{[3k]} \cdot J^{[3l]} \in \mathscr{B}(G_0)$, it follows that k, l are both even, and thus $x \in \mathscr{B}(G_0)$. Therefore, $\mathscr{B}(G_0)$ is seminormal.

3.2 Transfer Homomorphisms

A well-established strategy for investigating the arithmetic of a given monoid H is to construct a transfer homomorphism $\theta \colon H \to B$, where B is a simpler monoid than H and the transfer homomorphism θ allows to shift arithmetical results from B back to the (original, more complicated) monoid H. We will use transfer homomorphisms in Sect. 4 in order to show that properties of the monoid of G-invariant monomials can be studied in a monoid of zero-sum sequences (see Propositions 4.7 and 4.9).

Definition 3.5 A monoid homomorphism $\theta \colon H \to B$ is called a *transfer homomorphism* if it has the following properties:

(**T 1**) $B = \theta(H)B^{\times}$ and $\theta^{-1}(B^{\times}) = H^{\times}$.

(**T 2**) If $u \in H$, $b, c \in B$ and $\theta(u) = bc$, then there exist $v, w \in H$ such that $u = vw$, $\theta(v)B^{\times} = bB^{\times}$ and $\theta(w)B^{\times} = cB^{\times}$.

We will use the simple fact that, if $\theta\colon H \to B$ and $\theta'\colon B \to B'$ are transfer homomorphisms, then their composition $\theta' \circ \theta\colon H \to B'$ is a transfer homomorphism too. The next proposition summarizes key properties of transfer homomorphisms.

Proposition 3.6 *Let $\theta\colon H \to B$ be a transfer homomorphism and $a \in H$.*

1. *a is an atom of H if and only if $\theta(a)$ is an atom of B.*
2. *$\mathsf{L}_H(a) = \mathsf{L}_B\big(\theta(a)\big)$, whence $\theta\big(\mathscr{M}_k(H)\big) = \mathscr{M}_k(B)$ and $\theta^{-1}\big(\mathscr{M}_k(B)\big) = \mathscr{M}_k(H)$.*
3. *If θ is degree preserving, then $\mathsf{D}_k(H) = \mathsf{D}_k(B)$ for all $k \in \mathbb{N}$.*

Proof 1. and 2. follow from [40, Proposition 3.2.3]. In order to prove 3., note that for all $k \in \mathbb{N}$ we have

$$\mathsf{D}_k(H) = \sup\{|a|_H : a \in \mathscr{M}_k(H)\} = \sup\{|\theta(a)|_B : \theta(a) \in \mathscr{M}_k(B)\}$$
$$= \sup\{|b|_B : b \in \mathscr{M}_k(B)\} = \mathsf{D}_k(B).$$

The first examples of transfer homomorphisms in the literature start from a Krull monoid to its associated monoid of zero-sum sequences which is a Krull monoid having a combinatorial flavor. These ideas were generalized widely, and there are transfer homomorphisms from weakly Krull monoids to (simpler) weakly Krull monoids (having a combinatorial flavor) and the same is true for C-monoids.

Proposition 3.7 *Let H be a Krull monoid, $\varphi\colon H \to \mathscr{F}(P)$ be a cofinal divisor homomorphism with class group $G = \mathscr{C}(\varphi)$, and let $G^* \subset G$ denote the set of classes containing prime divisors. Let $\widetilde{\theta}\colon \mathscr{F}(P) \to \mathscr{F}(G^*)$ denote the unique homomorphism defined by $\widetilde{\theta}(p) = [p]$ for all $p \in P$, and set $\theta = \widetilde{\theta} \circ \varphi\colon H \to \mathscr{B}(G^*)$.*

1. *θ is a transfer homomorphism.*
2. *For $a \in H$, we set $|a| = |\varphi(a)|$ and for $S \in \mathscr{B}(G^*)$ we set $|S| = |S|_{\mathscr{F}(G^*)}$. Then $|a| = |\theta(a)|$ for all $a \in H$, $\theta(\mathscr{M}_k^*(H)) = \mathscr{M}_k^*(G^*)$ and $\theta^{-1}(\mathscr{M}_k^*(G^*)) = \mathscr{M}_k^*(H)$ for all $k \in \mathbb{N}$. Furthermore, $\mathsf{e}(H) = \mathsf{e}(G^*)$, $\eta(H) = \eta(G^*)$, and $\mathsf{D}_k(H) = \mathsf{D}_k(G^*)$ for all $k \in \mathbb{N}$.*

Proof 1. follows from [40, Sect. 3.4]. By definition, we have $|a| = |\theta(a)|$ for all $a \in H$. Thus, the assertions on $\mathsf{D}_k(H)$ follow from Proposition 2.7, and the remaining statements can be derived in a similar way.

The above transfer homomorphism $\theta\colon H \to \mathscr{B}(G^*)$ constitutes the link between the arithmetic of Krull monoids on the one side and zero-sum theory on the other side. In this way, methods from Arithmetic Combinatorics can be used to obtain precise results for arithmetical invariants describing the arithmetic of H. For an overview of this interplay see [37].

There is a variety of transfer homomorphisms from monoids of zero-sum sequences to monoids of zero-sum sequences in order to simplify specific structural features of the involved subsets of groups. Below we present a simple example of such a transfer homomorphism which we will meet again in Proposition 4.9

(for more of this nature we refer to [74] and to [40, Theorem 6.7.11]). Let G be abelian and let $G_0 \subset G$ be a subset. For $g \in G_0$ we define

$$e(G_0, g) = \gcd\left(\{\mathsf{v}_g(B) \colon B \in \mathscr{B}(G_0)\}\right),$$

and it is easy to check that (for details see [43, Lemma 3.4])

$$
\begin{aligned}
e(G_0, g) &= \gcd\left(\{\mathsf{v}_g(A) \colon A \in \mathscr{A}(G_0)\}\right) \\
&= \min\left(\{\mathsf{v}_g(A) \colon \mathsf{v}_g(A) > 0, A \in \mathscr{A}(G_0)\}\right) \\
&= \min\left(\{\mathsf{v}_g(B) \colon \mathsf{v}_g(B) > 0, B \in \mathscr{B}(G_0)\}\right) \\
&= \min\left(\{k \in \mathbb{N} \colon kg \in \langle G_0\setminus\{g\}\rangle\}\right) = \gcd\left(\{k \in \mathbb{N} \colon kg \in \langle G_0\setminus\{g\}\rangle\}\right).
\end{aligned}
$$

Proposition 3.8 *Let G be abelian and $G_0, G_1, G_2 \subset G$ be subsets such that $G_0 = G_1 \uplus G_2$. For $g \in G_0$ we set $e(g) = e(G_0, g)$ and we define $G_0^* = \{e(g)g \colon g \in G_1\} \cup G_2$. Then, the map*

$$
\begin{aligned}
\theta \colon \mathscr{B}(G_0) &\longrightarrow \mathscr{B}(G_0^*) \\
B = \prod_{g \in G_0} g^{[\mathsf{v}_g(B)]} &\longmapsto \prod_{g \in G_1} (e(g)g)^{[\mathsf{v}_g(B)/e(g)]} \prod_{g \in G_2} g^{[\mathsf{v}_g(B)]}
\end{aligned}
$$

is a transfer homomorphism.

Proof Clearly, θ is a surjective homomorphism satisfying $\theta^{-1}(1_{\mathscr{F}(G_0)}) = \{1_{\mathscr{F}(G_0)}\}$. In order to verify property (**T2**) of Definition 3.5, let $B \in \mathscr{B}(G_0)$ and $C_1, C_2 \in \mathscr{B}(G_0^*)$ be such that $\theta(B) = C_1 \cdot C_2$. We have to show that there are $B_1, B_2 \in \mathscr{B}(G_0)$ such that $B = B_1 \cdot B_2$, $\theta(B_1) = C_1$, and $\theta(B_2) = C_2$. This can be checked easily.

3.3 The kth Davenport Constants: The General Case

Let $G_0 \subset G$ be a subset, and $k \in \mathbb{N}$. Recall that $\mathsf{e}(G) = \max\{\text{ord}(g) \colon g \in G\}$. If G is nilpotent, then G is the direct sum of its p-Sylow subgroups and hence $\mathsf{e}(G) = \text{lcm}\{\text{ord}(g) \colon g \in G\} = \exp(G)$. Let

- $\mathsf{E}(G_0)$ be the smallest integer $\ell \in \mathbb{N}$ such that every sequence $S \in \mathscr{F}(G_0)$ of length $|S| \geq \ell$ has a product-one subsequence of length $|G|$.
- $\mathsf{s}(G_0)$ denote the smallest integer $\ell \in \mathbb{N}$ such that every sequence $S \in \mathscr{F}(G_0)$ of length $|S| \geq \ell$ has a product-one subsequence of length $\mathsf{e}(G)$.

The Davenport constants, together with the Erdős–Ginzburg–Ziv constant $\mathsf{s}(G)$, the constants $\eta(G)$ and $\mathsf{E}(G)$, are the most classical zero-sum invariants whose study (in the abelian setting) goes back to the early 1960s. The kth Davenport constants $\mathsf{D}_k(G)$ were introduced by Halter-Koch [50] and further studied in [40, Sect. 6.1]

and [30] (all this work is done in the abelian setting). First results in the non-abelian setting were achieved in [15].

If G is abelian, then W. Gao proved that $\mathsf{E}(G) = |G| + \mathsf{d}(G)$. For cyclic groups this is the Theorem of Erdős–Ginzburg–Ziv which dates back to 1961 [40, Proposition 5.7.9]. W. Gao and J. Zhuang conjectured that the above equality holds true for all finite groups [82, Conjecture 2], and their conjecture has been verified in a variety of special cases [3, 33, 34, 53]. For more in the non-abelian setting see [79, 80].

We verify two simple properties occurring in the assumptions of Propositions 2.7 and 2.8.

- If $S \in \mathscr{F}(G)$ and $g_0 \in \pi(S)$, then $h = g_0^{-1} \in G$ is a prime in $\mathscr{F}(G)$ and $h \cdot S \in \mathscr{B}(G)$.
- Clearly, $1_G \in \mathscr{B}(G)$ is a prime element of $\mathscr{B}(G)$.

Therefore, all properties proved in Propositions 2.7 and 2.8 for $\mathsf{D}_k(H)$ and $\mathsf{d}_k(H)$ hold for the constants $\mathsf{D}_k(G)$ and $\mathsf{d}_k(G)$ (the linearity properties as given in Propositions 2.7.2 and 2.8.2.(b) were first proved by Freeze and W.A. Schmid in case of abelian groups G [30]). We continue with properties which are more specific.

Proposition 3.9 *Let $H \leq G$ be a subgroup, $N \lhd G$ be a normal subgroup, and $k, \ell \in \mathbb{N}$.*

1. $\mathsf{d}_k(N) + \mathsf{d}_\ell(G/N) \leq \mathsf{d}_{k+\ell-1}(G)$.

2. $\mathsf{d}_k(G) \leq \mathsf{d}_{\mathsf{d}_k(N)+1}(G/N)$.

3. $\mathsf{d}_k(G) + 1 \leq [G{:}H](\mathsf{d}_k(H) + 1)$.

4. $\mathsf{d}_k(G) + 1 \leq k(\mathsf{d}(G) + 1)$.

5. $\mathsf{D}_k(G) \leq [G{:}H]\mathsf{D}_k(H)$.

Proof 1. Let $\overline{S} = (g_1 N) \cdot \cdots \cdot (g_s N) \in \mathscr{M}_\ell^*(G/N)$ with $|\overline{S}| = s = \mathsf{d}_\ell(G/N)$ and let $T = h_1 \cdot \cdots \cdot h_t \in \mathscr{M}_k^*(N)$ with $t = \mathsf{d}_k(N)$. We consider the sequence $W = g_1 \cdot \cdots \cdot g_s \cdot h_1 \cdot \cdots \cdot h_t \in \mathscr{F}(G)$ and suppose that it is divisible by $S_1 \cdot \cdots \cdot S_a \cdot T_1 \cdot \cdots \cdot T_b$ where $S_i, T_j \in \mathscr{B}(G) \backslash \{1_{\mathscr{F}(G)}\}$, $\operatorname{supp}(S_i) \cap \{g_1, \ldots, g_s\} \neq \emptyset$ and $T_1 \cdot \cdots \cdot T_b \mid h_1 \cdot \cdots \cdot h_t$ for all $i \in [1, a]$ and all $j \in [1, b]$. For $i \in [1, a]$, let $\overline{S_i} \in \mathscr{F}(G/N)$ denote the sequence obtained from S_i by replacing each g_ν by $g_\nu N$ and by omitting the elements of S_i which lie in $\{h_1, \ldots, h_t\}$. Then $\overline{S_1}, \ldots, \overline{S_a} \in \mathscr{B}(G/N) \backslash \{1_{\mathscr{F}(G)}\}$ and $\overline{S_1} \cdot \cdots \cdot \overline{S_a} \mid \overline{S}$ whence $a \leq \ell - 1$. By construction, we have $b \leq k - 1$ whence $a + b < k + \ell - 1$, $W \in \mathscr{M}_{k+\ell-1}^*(G)$, and $|W| = s + t = \mathsf{d}_k(N) + \mathsf{d}_\ell(G/N) \leq \mathsf{d}_{k+\ell-1}(G)$.

2. We set $m = \mathsf{d}_{\mathsf{d}_k(N)+1}(G/N) + 1$. By (1), we have to show that every sequence S over G of length $|S| \geq m$ is divisible by a product of k nontrivial product-one sequences. Let $f \colon G \to G/N$ denote the canonical epimorphism and let $S \in \mathscr{F}(G)$ be a sequence of length $|S| \geq m$. By definition of m, there exist sequences $S_1, \ldots, S_{\mathsf{d}_k(N)+1}$ such that $S_1 \cdot \cdots \cdot S_{\mathsf{d}_k(N)+1} \mid S$ and $f(S_1), \ldots, f(S_{\mathsf{d}_k(N)+1})$ are product-one sequences over G/N. Thus, for each $\nu \in [1, \mathsf{d}_k(N) + 1]$, there are elements $h_\nu \in N$ such that $h_\nu \in \pi(S_\nu)$. Then $T = h_1 \cdot \cdots \cdot h_{\mathsf{d}_k(N)+1}$ is a sequence

over N, and it has k nontrivial product-one subsequences $T_1, \ldots, T_k$ whose product $T_1 \cdot \cdots \cdot T_k$ divides T. Therefore we obtain k nontrivial product-one sequences whose product divides S.

3. We set $m = [G : H]$ and start with the following assertion.

A. If $S \in \mathscr{F}(G)$ with $|S| \geq m$, then $\Pi(S) \cap H \neq \emptyset$.

Proof of **A**. Let $S = g_1 \cdot \cdots \cdot g_n \in \mathscr{F}(G)$ with $|S| = n \geq m$. We consider the left cosets $g_1 H, g_1 g_2 H, \ldots, g_1 \ldots g_m H$. If one of these cosets equals H, then we are done. If this is not the case, then there are $k, \ell \in [1, m]$ with $k < \ell$ such that $g_1 \ldots g_k H = g_1 \ldots g_k g_{k+1} \ldots g_\ell H$ which implies that $g_{k+1} \ldots g_\ell \in H$. $\square$(Proof of **A**)

Now let $S \in \mathscr{F}(G)$ be a sequence of length $|S| = [G : H](\mathsf{d}_k(H) + 1)$. We have to show that S is divisible by a product of k nontrivial product-one sequences. By **A**, there are $\mathsf{d}_k(H) + 1$ sequences $S_1, \ldots, S_{\mathsf{d}_k(H)+1}$ and elements $h_1, \ldots, h_{\mathsf{d}_k(H)+1} \in H$ such that $S_1 \cdot \cdots \cdot S_{\mathsf{d}_k(H)+1} \mid S$ and $h_\nu \in \pi(S_\nu)$ for each $\nu \in [1, \mathsf{d}_k(H) + 1]$. By definition, the sequence $h_1 \cdot \cdots \cdot h_{\mathsf{d}_k(H)+1} \in \mathscr{F}(H)$ is divisible by a product of k nontrivial product-one sequences. Therefore S is divisible by a product of k nontrivial product-one sequences.

4. Let $S \in \mathscr{F}(G)$ be a sequence of length $|S| = k(\mathsf{d}(G) + 1)$. Then S may be written as a product $S = S_1 \cdot \cdots \cdot S_k$ where $S_1, \ldots, S_k \in \mathscr{F}(G)$ with $|S_\nu| = \mathsf{d}(G) + 1$ for every $\nu \in [1, k]$. Then each S_ν is divisible by a nontrivial product-one sequence T_ν, and hence, S is divisible by $T_1 \cdot \cdots \cdot T_k$. Thus by (1) we infer that $\mathsf{d}_k(G) + 1 \leq k(\mathsf{d}(G) + 1)$.

5. Let $A = g_1 \cdot \cdots \cdot g_\ell \in \mathscr{B}(G)$ with $g_1 \ldots g_\ell = 1$ and $\ell > [G : H]\mathsf{D}_k(H)$. We show that $\ell > \mathsf{D}_k(G)$. We set $d = \mathsf{D}_k(H)$ and consider the left H-cosets $C_j = g_1 \ldots g_j H$ for each $j \in [1, \ell]$. By the pigeonhole principle there exist $1 \leq i_1 < \cdots < i_{d+1} \leq \ell$ such that $C_{i_1} = \cdots = C_{i_{d+1}}$. We set $h_s = g_{i_s+1} \ldots g_{i_{s+1}}$ for each $s \in [1, d]$ and $h_{d+1} = g_{i_{d+1}+1} \ldots g_\ell g_1 \ldots g_{i_1-1}$. Clearly $h_1, \ldots, h_{d+1} \in H$, and $g_1 \cdots g_\ell = 1$ implies $h_1 \cdots h_{d+1} = 1$ whence $h_1 \cdot \cdots \cdot h_{d+1} \in \mathscr{B}(H)$. The inequality $d + 1 > \mathsf{D}_k(H)$ implies that $h_1 \cdot \cdots \cdot h_{d+1} = S_1 \cdot \cdots \cdot S_{k+1}$, where $1_{\mathscr{F}(H)} \neq S_i \in \mathscr{B}(H)$ for $i \in [1, k + 1]$. Let $T_i \in \mathscr{F}(G)$ denote the sequence obtained from S_i by replacing each occurrence of h_s by $g_{i_s+1} \cdot \cdots \cdot g_{i_{s+1}}$ for $s \in [1, d]$ and h_{d+1} by $g_{i_{d+1}+1} \cdot \cdots \cdot g_\ell \cdot g_1 \cdot \cdots \cdot g_{i_1-1}$. Then $T_1, \ldots, T_{k+1} \in \mathscr{B}(G)$ and $A = g_1 \cdot \cdots \cdot g_\ell = T_1 \cdot \cdots \cdot T_{k+1}$, which implies that $\ell > \mathsf{D}_k(G)$.

Much more is known for the classical Davenport constants $\mathsf{D}_1(G) = \mathsf{D}(G)$ and $\mathsf{d}_1(G) = \mathsf{d}(G)$. We start with metacyclic groups of index two. The following result was proved in [39, Theorem 1.1].

Theorem 3.10 *Suppose that G has a cyclic, index 2 subgroup. Then*

$$\mathsf{D}(G) = \mathsf{d}(G) + |G'| \quad and \quad \mathsf{d}(G) = \begin{cases} |G| - 1 & \text{if } G \text{ is cyclic} \\ \frac{1}{2}|G| & \text{if } G \text{ is noncyclic,} \end{cases}$$

where $G' = [G, G]$ is the commutator subgroup of G.

The next result gathers upper bounds for the large Davenport constant (for $\mathsf{d}(G)$ see [36]).

Theorem 3.11 *Let $G' = [G, G]$ denote the commutator subgroup of G.*

1. $\mathsf{D}(G) \leq \mathsf{d}(G) + 2|G'| - 1$, *and equality holds if and only if G is abelian.*
2. *If G is a non-abelian p-group, then* $\mathsf{D}(G) \leq \frac{p^2+2p-2}{p^3}|G|$.
3. *If G is non-abelian of order pq, where p, q are primes with $p < q$, then* $\mathsf{D}(G) = 2q$ *and* $\mathsf{d}(G) = q + p - 2$.
4. *If $N \lhd G$ is a normal subgroup with $G/N \cong C_p \oplus C_p$ for some prime p, then*

$$\mathsf{d}(G) \leq (\mathsf{d}(N) + 2)p - 2 \leq \frac{1}{p}|G| + p - 2.$$

5. *If G is noncyclic and p is the smallest prime dividing $|G|$, then* $\mathsf{D}(G) \leq \frac{2}{p}|G|$.
6. *If G is neither cyclic nor isomorphic to a dihedral group of order 2n with odd n, then* $\mathsf{D}(G) \leq \frac{3}{4}|G|$.

Proof All results can be found in [48]: see Lemma 4.2, Theorems 3.1, 4.1, 5.1, 7.1, 7.2, and Corollary 5.7.

Corollary 3.12 *The following statements are equivalent:*

(a) G is cyclic or isomorphic to a dihedral group of order 2n for some odd $n \geq 3$.
(b) $\mathsf{D}(G) = |G|$.

Proof If G is not as in (a), then $\mathsf{D}(G) \leq \frac{3}{4}|G|$ by Theorem 3.11.6. If G is cyclic, then $\mathsf{D}(G) = |G|$ by Lemma 3.1.3. If G is dihedral of order 2n for some odd $n \geq 3$, then the commutator subgroup G' of G has order n and hence $\mathsf{D}(G) = |G|$ by Theorem 3.10.

3.4   The kth Davenport Constants: The Abelian Case

Throughout this subsection, all groups are abelian and will be written additively.

We have $G \cong C_{n_1} \oplus \cdots \oplus C_{n_r}$, with $r \in \mathbb{N}_0$ and $1 < n_1 \mid \ldots \mid n_r$, $\mathsf{r}(G) = r$ is the *rank* of G and $n_r = \exp(G)$ is the *exponent* of G. We define

$$\mathsf{d}^*(G) = \sum_{i=1}^{r}(n_i - 1).$$

If $G = \{0\}$, then $r = 0 = \mathsf{d}^*(G)$. An s-tuple $(e_1, \ldots, e_s)$ of elements of $G \setminus \{0\}$ is said to be a *basis* of G if $G = \langle e_1 \rangle \oplus \cdots \oplus \langle e_s \rangle$. First, we provide a lower bound for the Davenport constants.

Lemma 3.13 *Let G be abelian.*

1. $\mathsf{D}_k(G) = 1 + \mathsf{d}_k(G)$ *for every* $k \in \mathbb{N}$.
2. $\mathsf{d}^*(G) + (k-1)\exp(G) \leq \mathsf{d}_k(G)$.

Proof 1. Let $k \in \mathbb{N}$. By Proposition 2.8.1, we have $1 + \mathsf{d}_k(G) \leq \mathsf{D}_k(G)$. Obviously, the map

$$\psi : \mathscr{M}_k^*(G) \to \mathscr{M}_k(G)\backslash\{1\}, \quad \text{given by} \quad \psi(S) = (-\sigma(S)) \cdot S,$$

is surjective and we have $|\psi(S)| = 1 + |S|$ for every $S \in \mathscr{M}_k^*(G)$. Therefore, we have $1 + \mathsf{d}_k(G) = \mathsf{D}_k(G)$.

2. Suppose that $G \cong C_{n_1} \oplus \cdots \oplus C_{n_r}$, with $r \in \mathbb{N}_0$ and $1 < n_1 \mid \ldots \mid n_r$. If $(e_1, \ldots, e_r)$ is a basis of G with $\mathrm{ord}(e_i) = n_i$ for all $i \in [1, r]$, then

$$S = e_r^{[n_r(k-1)]} \prod_{i=1}^r e_i^{[n_i-1]}$$

is not divisible by a product of k nontrivial zero-sum sequences whence $\mathsf{d}^*(G) + (k-1)\exp(G) = |S| \leq \mathsf{d}_k(G)$.

We continue with a result on the kth Davenport constant which refines the more general results in Sect. 2.5. It provides an explicit formula for $\mathsf{d}_k(G)$ in terms of $\mathsf{d}(G)$ (see [40, Theorem 6.1.5]).

Theorem 3.14 *Let G be abelian,* $\exp(G) = n$, *and* $k \in \mathbb{N}$.

1. *Let* $H \leq G$ *be a subgroup such that* $G = H \oplus C_n$. *Then*

$$\mathsf{d}(H) + kn - 1 \leq \mathsf{d}_k(G) \leq (k-1)n + \max\{\mathsf{d}(G), \eta(G) - n - 1\}.$$

   In particular, if $\mathsf{d}(G) = \mathsf{d}(H) + n - 1$ *and* $\eta(G) \leq \mathsf{d}(G) + n + 1$, *then* $\mathsf{d}_k(G) = \mathsf{d}(G) + (k-1)n$.
2. *If* $\mathsf{r}(G) \leq 2$, *then* $\mathsf{d}_k(G) = \mathsf{d}(G) + (k-1)n$.
3. *If* G *is a p-group and* $\mathsf{D}(G) \leq 2n - 1$, *then* $\mathsf{d}_k(G) = \mathsf{d}(G) + (k-1)n$.

For the rest of this section, we focus on the classical Davenport constant $\mathsf{D}(G)$. By Lemma 3.13.2, there is the crucial inequality

$$\mathsf{d}^*(G) \leq \mathsf{d}(G).$$

We continue with a list of groups for which equality holds. The list is incomplete but the remaining groups for which $\mathsf{d}^*(G) = \mathsf{d}(G)$ is known are of a similar special nature as those listed in Theorem 3.15.3 (see [76] for a more detailed discussion). In particular, it is still open whether equality holds for all groups of rank three (see [76, Sect. 4.1]) or for all groups of the form $G = C_n^r$ (see [47]).

Theorem 3.15 *We have* $\mathsf{d}^*(G) = \mathsf{d}(G)$ *in each of the following cases:*

1. *G is a p-group or has rank $\mathsf{r}(G) \leq 2$.*
2. *$G = K \oplus C_{km}$ where $k, m \in \mathbb{N}$, $p \in \mathbb{P}$ a prime, m a power of p and $K \leq G$ is a p-subgroup with $\mathsf{d}(K) \leq m - 1$.*
3. *$G = C_m^2 \oplus C_{mn}$ where $m \in \{2, 3, 4, 6\}$ and $n \in \mathbb{N}$.*

Proof For 1. see [40] (in particular, Theorems 5.5.9 and 5.8.3) for proofs and historical comments. For 2. see [37, Corollary 4.2.13], and 3. can be found in [5] and [76, Theorem 4.1].

There are infinite series of groups G with $\mathsf{d}^*(G) < \mathsf{d}(G)$. However, the true reason for the phenomenon $\mathsf{d}^*(G) < \mathsf{d}(G)$ is not understood. Here is a simple observation. Suppose that $G = C_{n_1} \oplus \cdots \oplus C_{n_r}$ with $1 < n_1 \mid \ldots \mid n_r$, $I \subset [1, r]$, and let $G' = \oplus_{i \in I} C_{n_i}$. If $\mathsf{d}^*(G') < \mathsf{d}(G')$, then $\mathsf{d}^*(G) < \mathsf{d}(G)$. For series of groups G which have rank four and five and satisfy $\mathsf{d}^*(G) < \mathsf{d}(G)$ we refer to [42, 44]. A standing conjecture for an upper bound on $\mathsf{D}(G)$ states that $\mathsf{d}(G) \leq \mathsf{d}^*(G) + \mathsf{r}(G)$. However, the available results are much weaker [6], [40, Theorem 5.5.5].

The remainder of this subsection is devoted to inverse problems with respect to the Davenport constant. Thus the objective is to study the structure of zero-sum free sequences S whose lengths $|S|$ are close to the maximal possible value $\mathsf{d}(G)$.

If G is cyclic of order $n \geq 2$, then an easy exercise shows that S is zero-sum free of length $|S| = \mathsf{d}(G)$ if and only if $S = g^{[n-1]}$ for some $g \in G$ with $\mathrm{ord}(g) = n$. After many contributions since the 1980s, S. Savchev and F. Chen could finally prove a (sharp) structural result. In order to formulate it we need some more terminology. If $g \in G$ is a nonzero element of order $\mathrm{ord}(g) = n$ and

$$S = (n_1 g) \cdot \cdots \cdot (n_\ell g), \quad \text{where} \quad \ell \in \mathbb{N}_0 \quad \text{and} \quad n_1, \ldots, n_\ell \in [1, n],$$

we define

$$\|S\|_g = \frac{n_1 + \cdots + n_\ell}{n}.$$

Obviously, S has sum zero if and only if $\|S\|_g \in \mathbb{N}_0$, and the *index of S* is defined as

$$\mathrm{ind}(S) = \min\{\|S\|_g \colon g \in G \text{ with } G = \langle g \rangle\} \in \mathbb{Q}_{\geq 0}.$$

Theorem 3.16 *Let G be cyclic of order $|G| = n \geq 3$.*

1. *If S is a zero-sum free sequence over G of length $|S| \geq (n + 1)/2$, then there exist $g \in G$ with $\mathrm{ord}(g) = n$ and integers $1 = m_1, \ldots, m_{|S|} \in [1, n - 1]$ such that*
   - *$S = (m_1 g) \cdot \cdots \cdot (m_{|S|} g)$*
   - *$m_1 + \cdots + m_{|S|} < n$ and $\Sigma(S) = \{vg \colon v \in [1, m_1 + \cdots + m_{|S|}]\}$.*

2. *If $U \in \mathscr{A}(G)$ has length $|U| \geq \lfloor \frac{n}{2} \rfloor + 2$, then $\mathrm{ind}(U) = 1$.*

Proof 1. See [71] for the original paper. For the history of the problem and a proof in the present terminology see [37, Chap. 5.1] or [49, Chap. 11].

2. This is a simple consequence of the first part (see [37, Theorem 5.1.8]).

The above result was generalized to groups of the form $G = C_2 \oplus C_{2n}$ by S. Savchev and F. Chen [72]. Not much is known about the number of all minimal zero-sum sequences of a given group. However, the above result allows to give a formula for the number of minimal zero-sum sequences of length $\ell \geq \lfloor \frac{n}{2} \rfloor + 2$ (this formula was first proved by Ponomarenko [66] for $\ell > 2n/3$).

Corollary 3.17 *Let G be cyclic of order* $|G| = n \geq 3$, *and let* $\ell \in \left[\lfloor \frac{n}{2} \rfloor + 2, n \right]$. *Then the number of minimal zero-sum sequences* $U \in \mathscr{A}(G)$ *of length* ℓ *equals* $\Phi(n)\mathsf{p}_\ell(n)$, *where* $\Phi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$ *is Euler's Phi function and* $\mathsf{p}_\ell(n)$ *is the number of integer partitions of n into* ℓ *summands.*

Proof Clearly, every generating element $g \in G$ and every integer partition $n = m_1 + \cdots + m_\ell$ gives rise to a minimal zero-sum sequence $U = (m_1 g) \cdot \cdots \cdot (m_\ell g)$. Conversely, if $U \in \mathscr{A}(G)$ is of length $|U| = \ell$, then Theorem 3.16.2 implies that there is an element $g \in G$ with $\mathrm{ord}(g) = n$ such that

$$U = (m_1 g) \cdot \cdots \cdot (m_\ell g) \quad \text{where} \quad m_1, \ldots, m_\ell \in [1, n-1] \text{ with } n = m_1 + \cdots + m_\ell. \tag{$*$}$$

Since G has precisely $\Phi(n)$ generating elements, it remains to show that for every $U \in \mathscr{A}(G)$ of length $|U| = \ell$ there is precisely one generating element $g \in G$ with $\|U\|_g = 1$. Let U be as in $(*)$, and assume to the contrary that there are $a \in [2, n-1]$ with $\gcd(a, n) = 1$ and $m'_1, \ldots, m'_\ell \in [1, n]$ such that $m'_1 + \cdots + m'_\ell = n$ and

$$U = \left(m'_1(ag) \right) \cdot \cdots \cdot \left(m'_\ell(ag) \right).$$

Let $a' \in [2, n-1]$ be such that $aa' \equiv 1 \pmod{n}$. Since

$$n = m_1 + \cdots + m_\ell \geq \mathsf{v}_g(U) + a\mathsf{v}_{ag}(U) + 2(\ell - \mathsf{v}_g(U) - \mathsf{v}_{ag}(U))$$
$$= 2\ell - \mathsf{v}_g(U) + (a - 2)\mathsf{v}_{ag}(U) \quad \text{and}$$
$$n = m'_1 + \cdots + m'_\ell \geq a'\mathsf{v}_g(U) + \mathsf{v}_{ag}(U) + 2(\ell - \mathsf{v}_g(U) - \mathsf{v}_{ag}(U))$$
$$= 2\ell + (a' - 2)\mathsf{v}_g(U) - \mathsf{v}_{ag}(U),$$

it follows that

$$(a-1)n = n + (a-2)n$$
$$\geq 2\ell - \mathsf{v}_g(U) + (a-2)\mathsf{v}_{ag}(U) + (a-2)(2\ell + (a'-2)\mathsf{v}_g(U) - \mathsf{v}_{ag}(U))$$
$$= (a-1)2\ell + ((a-2)(a'-2) - 1)\mathsf{v}_g(U),$$

whence $a = 2, a' = \frac{n+1}{2}$ or $a' = 2, a = \frac{n+1}{2}$ because $\ell \geq \lfloor \frac{n}{2} \rfloor + 2$. By symmetry, we may assume that $a = 2$. Then $\mathsf{v}_g(U) \geq 2\ell - n \geq 2\lfloor \frac{n}{2} \rfloor + 4 - n \geq 3$, and thus $n \geq a'\mathsf{v}_g(U) \geq 3\frac{n+1}{2}$, a contradiction.

The structure of all minimal zero-sum sequences of maximal length $\mathsf{D}(G)$ has been completely determined for rank two groups [31, 35, 68, 75], for groups of the form $G = C_2 \oplus C_2 \oplus C_{2n}$ with $n \geq 2$ [76, Theorem 3.13], and for groups of the form $G = C_2^4 \oplus C_{2n}$ with $n \geq 70$ [8, Theorems 5.8 and 5.9].

4 Multiplicative Ideal Theory of Invariant Rings

After gathering basic material from invariant theory in Sect. 4.1 we construct an explicit divisor theory for the algebra of polynomial invariants of a finite group (see Sect. 4.2). In Sect. 4.3 we present a detailed study of the abelian case as outlined in the Introduction. In Sect. 4.4 we associate a BF-monoid to a G-module whose kth Davenport constant is a lower bound for the kth Noether number.

4.1 Basics of Invariant Theory

Let $n = \dim_{\mathbb{F}}(V)$ and let $\rho \colon G \to \mathrm{GL}(n, \mathbb{F})$ be a group homomorphism. Consider the action of G on the polynomial ring $\mathbb{F}[x_1, \ldots, x_n]$ via $\mathbb{F}$-algebra automorphisms induced by $g \cdot x_j = \sum_{i=1}^{n} \rho(g^{-1})_{ji} x_i$. Taking a slightly more abstract point of departure, we suppose that V is a G-module (i.e., we suppose that V is endowed with an action of G via linear transformations). Choosing a basis of V, V is identified with $\mathbb{F}^n$, the group $\mathrm{GL}(n, \mathbb{F})$ is identified with the group $\mathrm{GL}(V)$ of invertible linear transformations of V, and $\mathbb{F}[V] = \mathbb{F}[x_1, \ldots, x_n]$ can be thought of as the symmetric algebra of V^*, the dual G-module of V, in which $(x_1, \ldots, x_n)$ is a basis dual to the standard basis in V. The action on V^* is given by $(g \cdot x)(v) = x(\rho(g^{-1})v)$, where $g \in G$, $x \in V^*$, $v \in V$. Note that, if $\mathbb{F}$ is infinite, then $\mathbb{F}[V]$ is the algebra of polynomial functions $V \to \mathbb{F}$, and the action of G on $\mathbb{F}[V]$ is the usual action on functions $V \to F$ induced by the action of G on V via ρ. Denote by $\mathbb{F}(V)$ the quotient field of $\mathbb{F}[V]$, and extend the G-action on $\mathbb{F}[V]$ to $\mathbb{F}(V)$ by

$$g \cdot \frac{f_1}{f_2} = \frac{g \cdot f_1}{g \cdot f_2} \quad \text{for } f_1, f_2 \in \mathbb{F}[V] \quad \text{and } g \in G.$$

We define

$$\mathbb{F}(V)^G = \{f \in \mathbb{F}(V) \colon g \cdot f = f \text{ for all } g \in G\} \subset \mathbb{F}(V) \quad \text{and} \quad \mathbb{F}[V]^G = \mathbb{F}(V)^G \cap \mathbb{F}[V].$$

Then $\mathbb{F}(V)^G \subset \mathbb{F}(V)$ is a subfield and $\mathbb{F}[V]^G \subset \mathbb{F}[V]$ is an $\mathbb{F}$-subalgebra of $\mathbb{F}[V]$, called the *ring of polynomial invariants* of G (the group homomorphism $\rho \colon G \to \mathrm{GL}(V)$ giving the G-action on V is usually suppressed from the notation). Since every element of $\mathbb{F}(V)$ can be written in the form $f_1 f_2^{-1}$ with $f_1 \in \mathbb{F}[V]$ and $f_2 \in \mathbb{F}[V]^G$,

it follows that $\mathbb{F}(V)^G$ is the quotient field of $\mathbb{F}[V]^G$. Next, we summarize some well-known ring theoretical properties of $\mathbb{F}[V]^G$ going back to E. Noether [64].

Theorem 4.1 *Let all notations be as above.*

1. $\mathbb{F}[V]^G \subset \mathbb{F}[V]$ *is an integral ring extension and* $\mathbb{F}[V]^G$ *is normal.*
2. $\mathbb{F}[V]$ *is a finitely generated* $\mathbb{F}[V]^G$-*module, and* $\mathbb{F}[V]^G$ *is a finitely generated* $\mathbb{F}$-*algebra* (*hence in particular a noetherian domain*).
3. $\mathbb{F}[V]^G$ *is a Krull domain with Krull dimension* $\dim_{\mathbb{F}}(V)$.

Proof 1. To show that $\mathbb{F}[V]^G$ is normal, consider an element $f \in \mathbb{F}(V)^G$ which is integral over $\mathbb{F}[V]^G$. Then f is integral over $\mathbb{F}[V]$ as well, and since $\mathbb{F}[V]$ is normal, it follows that $f \in \mathbb{F}[V] \cap \mathbb{F}(V)^G = \mathbb{F}[V]^G$.

To show that $\mathbb{F}[V]^G \subset \mathbb{F}[V]$ is an integral ring extension, consider an element $f \in \mathbb{F}[V]$ and the polynomial

$$\Phi_f = \prod_{g \in G}(X - gf) \in \mathbb{F}[V][X]. \tag{2}$$

The coefficients of Φ_f are the elementary symmetric functions (up to sign) evaluated at $(gf)_{g \in G}$, and hence, they are in $\mathbb{F}[V]^G$. Thus f is a root of a monic polynomial with coefficients in $\mathbb{F}[V]^G$.

2. For $i \in [1, n]$, we consider the polynomials $\Phi_{x_i}(X)$ (cf. (2)), and denote by $A \subset \mathbb{F}[V]^G \subset \mathbb{F}[V]$ the $\mathbb{F}$-algebra generated by the coefficients of $\Phi_{x_1}, \ldots, \Phi_{x_n}$. By definition, A is a finitely generated $\mathbb{F}$-algebra, and hence, a noetherian domain. Since $x_1, \ldots, x_n$ are integral over A, $\mathbb{F}[V] = A[x_1, \ldots, x_n]$ is a finitely generated (and hence noetherian) A-module. Therefore, the A-submodule $\mathbb{F}[V]^G$ is a finitely generated A-module, and hence, a finitely generated $\mathbb{F}$-algebra.

3. By 1. and 2., $\mathbb{F}[V]^G$ is a normal noetherian domain, and hence a Krull domain by Theorem 2.1.2. Since $\mathbb{F}[V]^G \subset \mathbb{F}[V]$ is an integral ring extension, the Theorem of Cohen–Seidenberg implies that their Krull dimensions coincide, and hence $\dim(\mathbb{F}[V]^G) = \dim(\mathbb{F}[V]) = \dim_{\mathbb{F}}(V)$.

The algebra $\mathbb{F}[V]$ is graded in the standard way (namely, $\deg(x_1) = \cdots = \deg(x_n) = 1$), and the subalgebra $\mathbb{F}[V]^G$ is generated by homogeneous elements. For $\mathbb{F}$-subspaces $S, T \subset \mathbb{F}[V]$ we write ST for the $\mathbb{F}$-subspace in $\mathbb{F}[V]$ spanned by all the products st ($s \in S, t \in T$), and write $S^k = S \ldots S$ (with k factors). The factor algebra of $\mathbb{F}[V]$ by the ideal generated by $\mathbb{F}[V]_+^G$ is usually called the *algebra of coinvariants*. It inherits the grading of $\mathbb{F}[V]$ and is finite dimensional.

Definition 4.2 Let $k \in \mathbb{N}$.

1. Let $\beta_k(G, V)$ be the top degree of the factor space $\mathbb{F}[V]_+^G/(\mathbb{F}[V]_+^G)^{k+1}$, where $\mathbb{F}[V]_+^G$ is the maximal ideal of $\mathbb{F}[V]^G$ spanned by the positive degree homogeneous elements. We call

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

the kth *Noether number* of G.

2. Let $b_k(G, V)$ denote the top degree of the factor algebra $\mathbb{F}[V]/(\mathbb{F}[V]_+^G)^k\mathbb{F}[V]$ and set

$$b_k(G) = \sup\{b_k(G, W) : W \text{ is a } G\text{-module over } \mathbb{F}\}.$$

In the special case $k = 1$ we set

$$\beta(G, V) = \beta_1(G, V), \beta(G) = \beta_1(G), \ b(G, V) = b_1(G, V), \text{ and } b(G) = b_1(G),$$

and $\beta(G)$ is the *Noether number* of G. If $\{f_1, \ldots, f_m\}$ and $\{h_1, \ldots, h_l\}$ are two minimal homogeneous generating sets of $\mathbb{F}[V]^G$, then $m = l$ and, after renumbering if necessary, $\deg(f_i) = \deg(h_i)$ for all $i \in [1, m]$ [61, Proposition 6.19]. Therefore by the Graded Nakayama Lemma [61, Proposition 8.31] we have

$$\beta(G, V) = \max\{\deg(f_i) : i \in [1, m]\},$$

where $\{f_1, \ldots, f_m\}$ is a minimal homogeneous generating set of $\mathbb{F}[V]^G$. Again by the Graded Nakayama Lemma, $b(G, V)$ is the maximal degree of a generator in a minimal system of homogeneous generators of $\mathbb{F}[V]$ as an $\mathbb{F}[V]^G$-module. If $\text{char}(\mathbb{F}) \nmid |G|$, then by [11, Corollary 3.2] we have

$$\beta_k(G) = b_k(G) + 1 \quad \text{and} \quad \beta(G, V) \le b(G, V) + 1, \tag{3}$$

where the second inequality can be strict. If G is abelian, then $\beta_k(G, V)$ and $b_k(G, V)$ will be interpreted as kth Davenport constants (see Proposition 4.7).

The *regular G-module* V_{reg} has a basis $\{e_g : g \in G\}$ labeled by the group elements, and the group action is given by $g \cdot e_h = e_{gh}$ for $g, h \in G$. More conceptually, one can identify V_{reg} with the space of $\mathbb{F}$-valued functions on G, on which G acts linearly via the action induced by the left multiplication action of G on itself. In this interpretation, the basis element e_g is the characteristic function of the set $\{g\} \subset G$. It was proved in [73] that, if $\text{char}(\mathbb{F}) = 0$, then $\beta(G) = \beta(G, V_{\text{reg}})$. If $\mathbb{F}$ is algebraically closed, each irreducible G-module occurs in V_{reg} as a direct summand with multiplicity equal to its dimension.

Theorem 4.3 *1. If $\text{char}(\mathbb{F}) \nmid |G|$, then $\beta(G) \le |G|$.*
2. If $\text{char}(\mathbb{F}) \mid |G|$, then $\beta(G) = \infty$.

Proof 1. The case $\text{char}(\mathbb{F}) = 0$ was proved by E. Noether [63] in 1916, and her argument works as well when the characteristic of $\mathbb{F}$ is greater than $|G|$. The general case was shown independently by P. Fleischmann [25] and J. Fogarty [28] (see also [62, Theorem 2.3.3] and [56]). For 2. see [70]. $\blacksquare$

Bounding the Noether number has always been an objective of invariant theory (for recent surveys we refer to [60, 81]; degree bounds are discussed in [10, 17, 26,

54, 78]; see [16] for algorithmic aspects). Moreover, the main motivation to introduce the kth Noether numbers $\beta_k(G)$ [11–13] was to bound the ordinary Noether number $\beta(G)$ via structural reduction (see Sect. 5.1).

4.2 The Divisor Theory of Invariant Rings

Let $G \subset \mathrm{GL}(V)$ and $\chi \in \mathrm{Hom}(G, \mathbb{F}^\bullet)$. Then

$$\mathbb{F}[V]^{G,\chi} = \{f \in \mathbb{F}[V] \colon g \cdot f = \chi(g)f \text{ for all } g \in G\}$$

denotes the space of *relative invariants of weight* χ, and we set

$$\mathbb{F}[V]^{G,\mathrm{rel}} = \bigcup_{\chi \in \mathrm{Hom}(G,\mathbb{F}^\bullet)} \mathbb{F}[V]^{G,\chi}.$$

Clearly, we have $\mathbb{F}[V]^G \subset \mathbb{F}[V]^{G,\mathrm{rel}} \subset \mathbb{F}[V]$, and to simplify notation, we set

$$H = (\mathbb{F}[V]^G \setminus \{0\})_{\mathrm{red}}, \quad D = (\mathbb{F}[V]^{G,\mathrm{rel}} \setminus \{0\})_{\mathrm{red}}, \quad \text{and} \quad E = (\mathbb{F}[V] \setminus \{0\})_{\mathrm{red}}.$$

Since $\mathbb{F}[V]$ is a factorial domain with $\mathbb{F}^\bullet$ as its set of units, $E = \mathscr{F}(P)$ is the free abelian monoid generated by $P = \{\mathbb{F}^\bullet f \colon f \in \mathbb{F}[V] \text{ is irreducible}\}$. The action of G on $\mathbb{F}[V]$ is via $\mathbb{F}$-algebra automorphisms, so it induces a permutation action of G on E and P. Denote by P/G the set of G-orbits in P. We shall identify P/G with a subset of E as follows: assign to the G-orbit $\{f_1, \ldots, f_r\}$ the element $f_1 \ldots f_r \in E$ (here $f_1, \ldots, f_r \in P$ are distinct).

We say that a nonidentity element $g \in G \subset \mathrm{GL}(V)$ is a *pseudoreflection* if a hyperplane in V is fixed pointwise by g, and g is not unipotent (this latter condition holds automatically if $\mathrm{char}(\mathbb{F})$ does not divide $|G|$, since then a nonidentity unipotent transformation cannot have finite order). We denote by $\mathrm{Hom}^0(G, \mathbb{F}^\bullet) \le \mathrm{Hom}(G, \mathbb{F}^\bullet)$ the subgroup of the character group consisting of the characters that contain all pseudoreflections in their kernels. For each $p \in P$, choose a representative $\tilde{p} \in \mathbb{F}[V]$ in the associate class $p = \mathbb{F}^\bullet \tilde{p}$. We have $\mathfrak{X}(\mathbb{F}[V]) = \{\tilde{p}\mathbb{F}[V] \colon p \in P\}$ because $\mathbb{F}[V]$ is factorial. We set $\mathsf{v}_{\tilde{p}} = \mathsf{v}_p \colon \mathsf{q}(\mathbb{F}[V]^\bullet) = \mathbb{F}(V)^\bullet \to \mathbb{Z}$, and for a subset $X \subset \mathbb{F}(V)$ we write $\mathsf{v}_p(X) = \inf\{\mathsf{v}_p(f) \colon f \in X \setminus \{0\}\}$. The *ramification index* of the prime ideal $\tilde{p}\mathbb{F}[V]$ over $\mathbb{F}[V]^G$ is $e(p) = \mathsf{v}_p(\tilde{p}\mathbb{F}[V] \cap \mathbb{F}[V]^G)$. The ramification index $e(p)$ can be expressed in terms of the *inertia subgroup*

$$I_p = \{g \in G \colon g \cdot f - f \in \tilde{p}\mathbb{F}[V] \text{ for all } f \in \mathbb{F}[V]\}.$$

Since $V^\star$ is a G-stable subspace in $\mathbb{F}[V]$, the inertia subgroup I_p acts trivially on $V^\star/(V^\star \cap \tilde{p}\mathbb{F}[V])$. On the other hand I_p acts faithfully on $V^\star$. So if I_p is nontrivial, then $V^\star \cap \tilde{p}\mathbb{F}[V] \ne 0$, implying $\tilde{p} \in V^\star$. Clearly I_p must act trivially on the

hyperplane $\mathscr{V}(\tilde{p}) = \{v \in V : \tilde{p}(v) = 0\}$, and hence acts via multiplication by a character $\delta_p \in \mathrm{Hom}(I_p, \mathbb{F}^{\bullet})$ on the *one*-dimensional factor space $V/\mathscr{V}(\tilde{p})$. So $\ker(\delta_p)$ is a normal subgroup of I_p (necessarily unipotent hence trivial if $\mathrm{char}(\mathbb{F}) \nmid |G|$) and $I_p = \ker(\delta_p)Z$ decomposes as a semi-direct product of $\ker(\delta_p)$ and a cyclic subgroup Z consisting of pseudoreflections fixing pointwise $\mathscr{V}(\tilde{p})$. So $Z \cong I_p/\ker(\delta_p)$ is isomorphic to a finite subgroup of $\mathbb{F}^{\bullet}$.

The next Lemma 4.4 is extracted from Nakajima's paper [58].

Lemma 4.4

1. *We have the equality $e(p) = |Z|$.*
2. $\mathsf{v}_p(\mathbb{F}[V]^{G,\chi}) < e(p)$ *for all* $\chi \in \mathrm{Hom}(G, \mathbb{F}^{\bullet})$.
3. $\mathsf{v}_p(\mathbb{F}[V]^{G,\chi}) = 0$ *for all* $\chi \in \mathrm{Hom}^0(G, \mathbb{F}^{\bullet})$.

Proof 1. By [59, 9.6, Proposition (i)], we have that $e(p) = \mathsf{v}_p(\tilde{p}\mathbb{F}[V] \cap \mathbb{F}[V]^{I_p})$, the ramification index of the prime ideal $\tilde{p}\mathbb{F}[V]$ over the subring of I_p-invariants. Thus, if I_p is trivial, then $e(p) = 1$, and of course $|Z| = 1$. If I_p is nontrivial, then as it was explained above, $\tilde{p}$ is a linear form, which is a relative I_p-invariant with weight δ_p^{-1}, hence $\tilde{p}^{|Z|}$ is an I_p-invariant, implying $\mathsf{v}_p(\tilde{p}\mathbb{F}[V] \cap \mathbb{F}[V]^{I_p}) \leq |Z|$. On the other hand $\mathbb{F}[V]^{I_p}$ is contained in $\mathbb{F}[V]^Z$, and the algebra of invariants of the cyclic group Z fixing pointwise the hyperplane $\mathscr{V}(\tilde{p})$ is generated by $\tilde{p}^{|Z|}$ and a subspace of V^* complementary to $\mathbb{F}\tilde{p}$. Thus $\mathsf{v}_p(\tilde{p}\mathbb{F}[V] \cap \mathbb{F}[V]^{I_p}) \geq \mathsf{v}_p(\tilde{p}\mathbb{F}[V] \cap \mathbb{F}[V]^Z) = |Z|$, implying in turn that $e(p) = |Z|$.

2. Take an $h \in \mathbb{F}[V]^G$ with $e(p) = \mathsf{v}_p(h)$. Note that $\mathsf{v}_q(h) = \mathsf{v}_p(h)$ and $\mathsf{v}_q(\mathbb{F}[V]^{G,\chi}) = \mathsf{v}_p(\mathbb{F}[V]^{G,\chi})$ holds for all $q \in G \cdot p$, since $\mathbb{F}[V]^{G,\chi}$ is a G-stable subset in $\mathbb{F}[V]$. Set $S = \{\frac{f}{t} : f \in \mathbb{F}[V], \quad t \in \mathbb{F}[V]^G \backslash \tilde{p}\mathbb{F}[V]\}$. This is a G-stable subring in $\mathsf{q}(\mathbb{F}[V])$ containing $\mathbb{F}[V]$. Consider $S^{\chi} = S \cap \mathsf{q}(\mathbb{F}[V])^{\chi}$, where $\mathsf{q}(\mathbb{F}[V])^{\chi} = \{s \in \mathsf{q}(\mathbb{F}[V]) : g \cdot s = \chi(g)s \text{ for all } g \in G\}$. Then $\mathsf{v}_q(S^{\chi}) = \mathsf{v}_q(\mathbb{F}[V]^{G,\chi})$ for all $q \in G \cdot p$, since for any denominator t of an element $\frac{f}{t}$ of S we have $\mathsf{v}_q(t) = 0$. Now suppose that contrary to our statement we have $e(p) \leq \mathsf{v}_p(\mathbb{F}[V]^{G,\chi})$, and hence $\mathsf{v}_q(h) \leq \mathsf{v}_q(S^{\chi})$ for all $q \in G \cdot p$. In particular this means that $\mathbb{F}[V]^{G,\chi} \neq \{0\}$. Then $\mathsf{v}_q(h^{-1}S^{\chi}) \geq 0$ holds for all $q \in G \cdot p$. Now S is a Krull domain with $\mathfrak{X}(S) = \{\tilde{q}S : q \in G \cdot p\}$, thus $h^{-1}S^{\chi} \subset S$ (see the discussion after Theorem 2.1), implying that $S^{\chi} \subset hS$. Clearly $hS \cap S^{\chi} = hS^{\chi}$, so we conclude in turn that $S^{\chi} \subset hS^{\chi}$. Iterating this we deduce $\{0\} \neq S^{\chi} \subset \cap_{n=1}^{\infty}h^nS$, a contradiction.

3. It is well known that $\mathbb{F}[V]^{G,\chi} \neq \{0\}$ (see the proof of **A4.** below). Write $v = \mathsf{v}_p(\mathbb{F}[V]^{G,\chi})$. Take $f \in \mathbb{F}[V]^{G,\chi}$ with $\mathsf{v}_p(f) = v$, say $f = \tilde{p}^vh$, where $h \in \mathbb{F}[V]$. Note that both f and $\tilde{p}$ are relative invariants of I_p, hence so is h. Therefore $g \cdot h \in \mathbb{F}^{\bullet}h$, and $\tilde{p} \mid_{\mathbb{F}[V]} (g \cdot h - h)$ for all $g \in I_p$, implying that h is an I_p-invariant. Any $\chi \in \mathrm{Hom}^0(G, \mathbb{F}^{\bullet})$ contains I_p in its kernel (the unipotent normal subgroup $\ker(\delta_p)$ of I_p has no non-trivial characters at all, and $Z = I_p/\ker(\delta_p)$ consists of pseudoreflections). Thus f is I_p-invariant as well. Therefore $\tilde{p}^v$ is I_p-invariant, so its weight δ_p^v is trivial. Consequently, the order $|Z|$ of δ_p in $\mathrm{Hom}(I_p, \mathbb{F}^{\bullet})$ divides v. We have $e(p) = |Z|$ by 1., and on the other hand $v < e(p)$ by 2., forcing $v = 0$.

For a relative invariant f, we denote by $w(f)$ the weight of f. This induces a homomorphism $w\colon D \to \mathrm{Hom}(G, \mathbb{F}^\bullet)$ assigning to $\mathbb{F}^\bullet f \in D$ the weight $w(f)$ of the relative invariant f. Clearly, w extends to a group homomorphism $w\colon \mathsf{q}(D) \to \mathrm{Hom}(G, \mathbb{F}^\bullet)$. The kernel of w consists of elements of the form $(\mathbb{F}^\bullet h)^{-1}\mathbb{F}^\bullet f$, where $f, h \in \mathbb{F}[V]^{G,\chi}$ for some character χ. Now f/h belongs to $\mathbb{F}(V)^G$, which is the field of fractions of $\mathbb{F}[V]^G$, so there exist $f_1, h_1 \in \mathbb{F}[V]^G$ with $f/h = f_1/h_1$, implying $(\mathbb{F}^\bullet h)^{-1}\mathbb{F}^\bullet f = (\mathbb{F}^\bullet h_1)^{-1}\mathbb{F}^\bullet f_1 \in \mathsf{q}(H)$. Thus $\ker(w) = \mathsf{q}(H)$. Therefore, w induces a monomorphism $\overline{w}\colon \mathsf{q}(D)/\mathsf{q}(H) \to \mathrm{Hom}(G, \mathbb{F}^\bullet)$.

Theorem 4.5 *Let $G \subset \mathrm{GL}(V)$, $H = (\mathbb{F}[V]^G\backslash\{0\})_{\mathrm{red}}$, and $D = (\mathbb{F}[V]^{G,\mathrm{rel}}\backslash\{0\})_{\mathrm{red}}$.*

1. *The embeddings $\mathbb{F}[V]^G\backslash\{0\} \overset{\varphi}{\hookrightarrow} \mathbb{F}[V]^{G,\mathrm{rel}}\backslash\{0\} \overset{\psi}{\hookrightarrow} \mathbb{F}[V]^\bullet$ are cofinal divisor homomorphisms.*
2. *D is factorial, $P/G \subset E$ is the set of prime elements in D, and $\mathscr{C}(\varphi)$ is a torsion group.*
3. *The monoid $D_0 = \{\gcd_D(X)\colon X \subset H \text{ finite}\} \subset D$ is free abelian with basis $\{q^{e(q)}\colon q \in P/G\}$, where $e(q) = \min\{\mathsf{v}_q(h)\colon q \mid_D h \in H\}$, and the embedding $H \hookrightarrow D_0$ is a divisor theory.*
4. *We have $D_0 = \{f \in D\colon w(f) \in \mathrm{Hom}^0(G, \mathbb{F}^\bullet)\}$ and $\overline{w}\mid_{\mathsf{q}(D_0)/\mathsf{q}(H)}\colon \mathscr{C}(\mathbb{F}[V]^G) = \mathsf{q}(D_0)/\mathsf{q}(H) \to \mathrm{Hom}^0(G, \mathbb{F}^\bullet)$ is an isomorphism.*

Theorem 4.5 immediately implies the following corollary which can be found in Benson's book [4, Theorem 3.9.2] and which goes back to Nakajima [58] (see also [27] for a discussion of this theorem).

Corollary 4.6 (Benson–Nakajima) *The class group of $\mathbb{F}[V]^G$ is isomorphic to $\mathrm{Hom}^0(G, \mathbb{F}^\bullet)$, the subgroup of the character group consisting of the characters that contain all pseudoreflections in their kernels.*

Proof (of Theorem 4.5) 1. Since $\mathbb{F}[V]^G = \mathbb{F}(V)^G \cap \mathbb{F}[V]$, the embedding $\psi \circ \varphi\colon \mathbb{F}[V]^G \hookrightarrow \mathbb{F}[V]$ is a divisor homomorphism, and hence φ is a divisor homomorphism. Furthermore, if the quotient of two relative invariants lies in $\mathbb{F}[V]$, then it is a relative invariant whence ψ is a divisor homomorphism. In order to show that the embeddings are cofinal, let $0 \neq f \in \mathbb{F}[V]$ be given. Then $f^* = \prod_{g\in G} gf \in \mathbb{F}[V]^G$ and $f \mid f^*$, so the embedding $\psi \circ \varphi$ is cofinal and hence φ and ψ are cofinal.

2. Suppose that $\{f_1, \ldots, f_r\} \subset \mathbb{F}[V]$ represents a G-orbit in P. Then $g \cdot (f_1 \ldots f_r)$ is a non-zero scalar multiple of $f_1 \ldots f_r$, hence $f_1 \ldots f_r \in \mathbb{F}[V]^{G,\mathrm{rel}}$. This shows that $P/G \subset E$ is in fact contained in D. Conversely, take an irreducible element $\mathbb{F}^\bullet f$ in the monoid D (so f is a relative invariant). Take any irreducible divisor f_1 of f in $\mathbb{F}[V]$. Since $g \cdot f \in \mathbb{F}^\bullet f$, the polynomial $g \cdot f_1$ is also the divisor of f. Denoting by $f_1, \ldots, f_r$ polynomials representing the G-orbit of $\mathbb{F}^\bullet f_1$ in P, we conclude that $f_1 \ldots f_r$ divides f in $\mathbb{F}[V]$, hence $\mathbb{F}^\bullet f_1 \ldots f_r$ divides $\mathbb{F}^\bullet f$ in D as well, so $\mathbb{F}^\bullet f_1 \ldots f_r = \mathbb{F}^\bullet f$. This implies that D is the submonoid of $E = \mathscr{F}(P)$ generated by P/G.

In order to show that $\mathscr{C}(\varphi)$ is a torsion group, let $f \in D$ be given. We have to find an $m \in \mathbb{N}$ such that $f^m \in H$. Clearly, this holds with m being the order in $\mathrm{Hom}(G, F^\bullet)$ of the weight of the relative invariant corresponding to f.

3. Since $\mathscr{C}(\varphi)$ is a torsion group, Proposition 2.2 implies that the embedding $H \hookrightarrow D_0$ is a divisor theory, and that D_0 is free abelian with basis $\{q^{e(q)} : q \in P/G\}$, where $e(q) = \min\{\mathsf{v}_q(h) : q \mid_D h \in H\}$ (note that if $q \in P/G$ is the G-orbit of $p \in P$, then $\mathsf{v}_q(h) = \mathsf{v}_p(h)$, where the latter is the exponent of p in $h \in E = \mathscr{F}(P)$).

4. It remains to prove the following three assertions.

A1. $D_0 = \{f \in D : w(f) \in \mathrm{Hom}^0(G, \mathbb{F}^\bullet)\}$.

A2. $w(D_0) = \mathrm{Hom}^0(G, \mathbb{F}^\bullet)$.

A3. $\overline{w} \mid_{\mathsf{q}(D_0)/\mathsf{q}(H)} : \mathsf{q}(D_0)/\mathsf{q}(H) \to w(D_0)$ is an isomorphism.

Proof of **A1**. Set $D^0 = \{f \in D : w(f) \in \mathrm{Hom}^0(G, \mathbb{F}^\bullet)\}$. We show first $D_0 \subset D^0$. Let χ be a character of G, and assume that $\chi(g) \neq 1$ for some pseudoreflection $g \in G$. Let f be a relative invariant with $w(f) = \chi$. Then for any v with $gv = v$ we have $f(v) = f(g^{-1}v) = (gf)(v) = \chi(g)f(v)$, hence $f(v) = 0$. So $l \mid_{\mathbb{F}[V]} f$, where l is a nonzero linear form on V that vanishes on the reflecting hyperplane of g. Denoting by $l = l_1, \ldots, l_r$ representatives of the G-orbit of $\mathbb{F}^\bullet l$, we find that the relative invariant $q = l_1 \ldots l_r$ divides f. Thus $\gcd_D\{f \in D \mid w(f) = \chi\} \neq 1$. Now suppose that for some $\mathbb{F}^\bullet k \in D_0$ we have that $w(k)$ does not belong to $\mathrm{Hom}^0(G, \mathbb{F}^\bullet)$. By definition of D_0 there exist $h_1, \ldots, h_n \in D$ with $\gcd_D(h_1, \ldots, h_n) = 1$ and $kh_1, \ldots, kh_n \in H$. Clearly $w(h_i) = w(k)^{-1} \notin \mathrm{Hom}^0(G, \mathbb{F}^\bullet)$, hence by the above considerations $\gcd_D(h_1, \ldots, h_n) \neq 1$, a contradiction.

Next we show $D^0 \subset D_0$. Let d be an element in the monoid D^0. By Lemma 4.4.3 for any prime divisor $p \in P$ of d there exists an $h_p \in D$ such that $w(h_p) = w(d)^{-1}$ and $p \nmid_E h_p$. Denote by $m > 1$ the order of $w(d)$ in the group of characters. Clearly $d^m \in H$ and $dh_p \in H$. Moreover, $\gcd_E(d^m, dh_p : p \in P, \quad p \mid_E d) = d$.

Proof of **A2**. The statement follows from **A1**, as soon as we show that $\mathbb{F}[V]^{G,\chi} \neq 0$ for all $\chi \in \mathrm{Hom}(G, \mathbb{F}^\bullet)$. For any character $\chi \in \mathrm{Hom}(G, \mathbb{F}^\bullet)$ the group $\bar{G} = G/\ker(\chi)$ is isomorphic to a cyclic subgroup of $\mathbb{F}^\bullet$, hence its order is not divisible by $\mathrm{char}(\mathbb{F})$. Moreover, $\bar{G}$ acts faithfully on the field $T = \mathbb{F}(V)^{\ker(\chi)}$, with $T^{\bar{G}} = \mathbb{F}(V)^G$. By the Normal Basis Theorem, T as a $\bar{G}$-module over $T^{\bar{G}}$ is isomorphic to the regular representation of $\bar{G}$, hence contains the representation χ as a summand with multiplicity 1. This shows in particular that $T^{\bar{G}}$ contains a relative invariant of weight χ. Multiplying this by an appropriate element of $T^{\bar{G}} \cap \mathbb{F}[V] = \mathbb{F}[V]^G$ we get an element of $\mathbb{F}[V]^{G,\chi}$. So all characters of G occur as the weight of a relative invariant in $\mathbb{F}[V]$.

Proof of **A3**. Since $\overline{w} : \mathsf{q}(D)/\mathsf{q}(H) \to \mathrm{Hom}(G, \mathbb{F}^\bullet)$ is a monomorphism, the map $\overline{w} \mid_{\mathsf{q}(D_0)/\mathsf{q}(H)} : \mathsf{q}(D_0)/\mathsf{q}(H) \to w(\mathsf{q}(D_0))$ is an isomorphism. Note finally that $w(\mathsf{q}(D_0)) = \mathsf{q}(w(D_0)) = w(D_0)$.

As already mentioned, not only the class group but also the distribution of prime divisors in the classes is crucial for the arithmetic of the domain. Moreover, the class group together with the distribution of prime divisors in the classes are characteristic (up to units) for the domain. For a precise formulation we need one more definition.

Let H be a Krull monoid, $H_{\mathrm{red}} \hookrightarrow \mathscr{F}(\mathscr{P})$ a divisor theory, and let G be an abelian group and $(m_g)_{g \in G}$ be a family of cardinal numbers. We say that H has *characteristic*

$(G, (m_g)_{g \in G})$ if there is a group isomorphism $\Phi : G \to \mathscr{C}(H)$ such that $m_g = |\mathscr{P} \cap \Phi(g)|$. Two reduced Krull monoids are isomorphic if and only if they have the same characteristic [40, Theorem 2.5.4]. We pose the following problem.

Problem 1 Let G be a finite group, $\mathbb{F}$ be a field, and V be a finite dimensional $\mathbb{F}$-vector space endowed with a linear action of G. Determine the characteristic of $\mathbb{F}[V]^G$.

Let all assumptions be as in Problem 1 and suppose further that G acts trivially on one variable. Then $\mathbb{F}[V]^G$ is a polynomial ring in this variable and hence every class contains a prime divisor by [29, Theorem 14.3].

4.3 The Abelian Case

Throughout this subsection, suppose that G is abelian, $\mathbb{F}$ is algebraically closed, and char$(\mathbb{F}) \nmid |G|$.

The assumption on algebraic closedness is not too restrictive, since for any field $\mathbb{F}$ the set $\mathbb{F}[V]^G$ spans the ring of invariants over the algebraic closure $\overline{\mathbb{F}}$ as a vector space over $\overline{\mathbb{F}}$. The assumption on the characteristic guarantees that every G-module is completely reducible (i.e., is the direct sum of irreducible G-modules). The dual space V^* has a basis $\{x_1, \ldots, x_n\}$ consisting of G-eigenvectors whence $g \cdot x_i = \chi_i(g)x_i$ for all $i \in [1, n]$ where $\chi_1, \ldots, \chi_n \in \text{Hom}(G, \mathbb{F}^\bullet)$. We set $\widehat{G} = \text{Hom}(G, \mathbb{F}^\bullet)$, $\widehat{G}_V = \{\chi_1, \ldots, \chi_n\} \subset \widehat{G}$, and note that $G \cong \widehat{G}$. Recall that a completely reducible H-module W (for a not necessarily abelian group H) is called *multiplicity free* if it is the direct sum of pairwise non-isomorphic irreducible H-modules. In our case V is multiplicity free if and only if the characters $\chi_1, \ldots, \chi_n$ are pairwise distinct.

It was B. Schmid [73, Sect. 2] who first formulated a correspondence between a minimal generating system of $\mathbb{F}[V]^G$ and minimal product-one sequences over the character group (see also [24]). The next proposition describes in detail the structural interplay. In particular, Proposition 4.7.2 shows that all (direct and inverse) results on minimal zero-sum sequences over $\widehat{G}_V$ (see Sects. 3.3 and 3.4) carry over to $\mathscr{A}(M^G)$.

Proposition 4.7 *Let $M \subset \mathbb{F}[x_1, \ldots, x_n]$ be the multiplicative monoid of monomials, $\psi : M \to \mathscr{F}(\widehat{G}_V)$ be the unique monoid homomorphism defined by $\psi(x_i) = \chi_i$ for all $i \in [1, n]$, and let $M^G \subset M$ denote the submonoid of G-invariant monomials.*

1. *$\mathbb{F}[V]^G$ has M^G as an $\mathbb{F}$-vector space basis, and $\mathbb{F}[V]^G$ is minimally generated as an $\mathbb{F}$-algebra by $\mathscr{A}(M^G)$.*
2. *The homomorphism $\psi : M \to \mathscr{F}(\widehat{G}_V)$ and its restriction $\psi \mid_{M^G} : M^G \to \mathscr{B}(\widehat{G}_V)$ are degree-preserving transfer homomorphisms. Moreover, M^G is a reduced finitely generated Krull monoid, and $\mathscr{A}(M^G) = \psi^{-1}(\mathscr{A}(\widehat{G}_V))$.*
3. *$\psi \mid_{M^G}$ is an isomorphism if and only if V is a multiplicity free G-module.*
4. *$\beta_k(G, V) = \mathsf{D}_k(M^G) = \mathsf{D}_k(\widehat{G}_V)$ and $\beta_k(G) = \mathsf{D}_k(G)$ for all $k \in \mathbb{N}$.*

Proof 1. Each monomial spans a G-stable subspace in $\mathbb{F}[V]$, hence a polynomial is G-invariant if and only if all its monomials are G-invariant, so M^G spans $\mathbb{F}[V]^G$. The elements of M^G are linearly independent, therefore $\mathbb{F}[V]^G$ can be identified with the monoid algebra of M^G over $\mathbb{F}$, which shows the second statement.

2. M and $\mathscr{F}(\widehat{G}_V)$ are free abelian monoids and ψ maps primes onto primes. Thus $\psi: M \to \mathscr{F}(\widehat{G}_V)$ is a surjective degree-preserving monoid homomorphism and it is a transfer homomorphism. Let $\pi: \mathscr{F}(\widehat{G}) \to \widehat{G}$ be the monoid homomorphism defined by $\pi(\chi) = \chi$ for all $\chi \in \widehat{G}$. Then $\ker(\pi) = \mathscr{B}(\widehat{G})$. Taking into account that for a monomial $m \in M$ G acts on the space $\mathbb{F}m$ via the character $\pi(\psi(m))$, we conclude that for a monomial $m \in M$ we have that $m \in M^G$ if and only if $\psi(m) \in \mathscr{B}(\widehat{G}_V)$. This implies that the restriction $\psi|_{M^G}$ of the transfer homomorphism ψ is also a transfer homomorphism. Therefore M^G is generated by $\mathscr{A}(M^G) = \psi^{-1}\big(\mathscr{A}(\widehat{G}_V)\big)$. Since $\mathscr{A}(\widehat{G}_V)$ is finite, and ψ has finite fibers, we conclude that the monoid M^G is finitely generated. Since M is factorial and $\mathbb{F}[V]^G \subset \mathbb{F}[V]$ is saturated by Theorem 4.5, it follows that

$$M \cap \mathsf{q}(M^G) \subset M \cap \mathbb{F}[V] \cap \mathsf{q}(\mathbb{F}[V]^G) \subset M \cap \mathbb{F}[V]^G = M^G$$

whence $M^G \subset M$ is saturated and thus M^G is a Krull monoid.

3. V is a multiplicity free G-module if and only if $\chi_1, \ldots, \chi_n$ are pairwise distinct. Since $\psi: M \to \mathscr{F}(\widehat{G}_V)$ maps the primes $x_1, \ldots, x_n$ of M onto the primes $\chi_1, \ldots, \chi_n$ of $\mathscr{F}(\widehat{G}_V)$, ψ is an isomorphism if and only if $\chi_1, \ldots, \chi_n$ are pairwise distinct.

4. Let $k \in \mathbb{N}$ and $M_+^G = M^G \backslash \{1\}$. Then $M^G \backslash (M_+^G)^{k+1} = \mathscr{M}_k(M^G)$. Since $\psi|_{M^G}: M^G \to \mathscr{B}(\widehat{G}_V)$ is degree-preserving transfer homomorphism, Proposition 3.6.3 implies that $\mathsf{D}_k(M^G) = \mathsf{D}_k(\widehat{G}_V)$. Since $\mathbb{F}[V]^G$ is spanned by M^G, $(\mathbb{F}[V]_+^G)^{k+1}$ is spanned by $(M_+^G)^{k+1}$. Therefore, the top degree of a homogeneous G-invariant not contained in $(\mathbb{F}[V]_+^G)^{k+1}$ coincides with the maximal degree of a monomial in $M_+^G \backslash (M_+^G)^{k+1} = \mathscr{M}_k(M^G)$. Thus $\beta_k(G, V) = \mathsf{D}_k(M^G)$. For the kth Noether number $\beta_k(G)$ we have

$$\beta_k(G) = \sup\{\beta_k(G, W) : W \text{ is a } G\text{-module over } \mathbb{F}\}$$
$$= \sup\{\mathsf{D}_k(\widehat{G}_W) : W \text{ is a } G\text{-module over } \mathbb{F}\} = \mathsf{D}_k(\widehat{G})$$

because for the regular representation V_{reg} we have $\widehat{G}_{V_{\mathrm{reg}}} = \widehat{G}$.

Recalling the notation of Theorem 4.5, we have

$$H = (\mathbb{F}[V]^G \backslash \{0\})_{\mathrm{red}} \quad \text{and} \quad D_0 = \{\underset{D}{\gcd}(X) : X \subset H \text{ finite}\} \subset D = (\mathbb{F}[V]^{G,\mathrm{rel}} \backslash \{0\})_{\mathrm{red}}.$$

Furthermore, $M \subset \mathbb{F}[V] = \mathbb{F}[x_1, \ldots, x_n]$ is the monoid of monomials, $M^G = M \cap \mathbb{F}[V]^G$, and we can view M as a submonoid of H and then $M^G = M \cap H$. Since $M \subset H$ is saturated, $M = \mathsf{q}(M) \cap H$, and

$$q(M)/q(M^G) = q(M)/q(M \cap H) = q(M)/(q(M) \cap q(H))$$
$$\cong q(M)q(H)/q(H) \subset q(D)/q(H),$$

we consider $q(M)/q(M^G)$ as a subset of $q(D)/q(H)$.

Proposition 4.8 *Let all notation be as above and set $M_0 = M \cap D_0$.*

1. *$M_0 \subset D_0$ is divisor closed whence M_0 is free abelian, and $\mathscr{A}(M_0) = M \cap \mathscr{A}(D_0) = \{x_1^{e(x_1)}, \ldots, x_n^{e(x_n)}\}$.*
2. *We have $e(x_i) = \min\{k \in \mathbb{N} : \chi_i^k \in \langle \chi_j \mid j \neq i \rangle\}$.*
3. *$\mathrm{Hom}^0(\rho(G), \mathbb{F}^\bullet)$ is generated by $\{\chi_1^{e(x_1)}, \ldots, \chi_n^{e(x_n)}\}$ and $\mathbb{F}[x_1^{e(x_1)}, \ldots, x_n^{e(x_n)}] = \mathbb{F}[V]^{G_1}$, where G_1 denotes the subgroup of $\rho(G)$ generated by the pseudoreflections in $\rho(G)$.*
4. *The embedding $M^G \hookrightarrow M_0$ is a divisor theory,*

$$\overline{w} \mid_{q(M_0)/q(M^G)} : \mathscr{C}(M^G) = q(M_0)/q(M^G) \to \mathrm{Hom}^0(\rho(G), \mathbb{F}^\bullet)$$

is an isomorphism, and $\overline{w}(\mathscr{C}(M^G)^*) = \{\chi_1^{e(x_1)}, \ldots, \chi_n^{e(x_n)}\}$.

Proof 1. If the product of two polynomials in $\mathbb{F}[V]$ has a single non-zero term, then both polynomials must have only one non-zero term. Thus, if $ab \in M$ for some $a, b \in D$, then both a and b belong to M. Hence $M \subset D$ is divisor closed implying that $M_0 \subset D_0$ is divisor-closed. Therefore $\mathscr{A}(M_0) = M \cap \mathscr{A}(D_0)$.

By Theorem 4.5.3, $\mathscr{A}(D_0) = \{q^{e(q)} : q \in \mathscr{A}(D)\}$. The divisor closedness of M in D implies that if $q^{e(q)} \in M$, then $q \in M \cap \mathscr{A}(D) = \mathscr{A}(M) = \{x_1, \ldots, x_n\}$. Thus $M \cap \mathscr{A}(D_0) = \{x_1^{e(x_1)}, \ldots, x_n^{e(x_n)}\}$.

2. For $i \in [1, n]$, we have

$$e(x_i) = \min\{v_{x_i}(h) : x_i \mid_D h, h \in H\} = \min\{v_{x_i}(m) : x_i \mid_D m, m \in M^G\},$$

where the second equality holds because for all $h \in H$ we have $v_{x_i}(h) = \min\{v_{x_i}(m) : m \text{ ranges over the monomials of } h\}$. Note that a monomial $m = \prod_{i=1}^n x_i^{a_i}$ lies in M^G if and only if $\prod_{i=1}^n \chi_i^{[a_i]}$ is a product-one sequence over $\widehat{G}$ if and only if $\chi_i^{a_i} = \prod_{j \neq i} \chi_j^{-a_j}$. Thus $\min\{v_{x_i}(m) : x_i \mid_D m, m \in M^G\} = \min\{k \in \mathbb{N} : \chi_i^k \in \langle \chi_j \mid j \neq i \rangle\}$.

3. By Theorem 4.5.4, $\mathrm{Hom}^0(\rho(G), \mathbb{F}^\bullet) = w(D_0)$ and hence $\mathrm{Hom}^0(\rho(G), \mathbb{F}^\bullet)$ is generated by $w(\mathscr{A}(D_0))$. Thus by 1., it remains to show that $\langle w(\mathscr{A}(D_0)) \rangle = \langle w(\mathscr{A}(M_0)) \rangle$. Since $\mathscr{A}(M_0) \subset \mathscr{A}(D_0)$, it follows that $\langle w(\mathscr{A}(D_0)) \rangle \supset \langle w(\mathscr{A}(M_0)) \rangle$. To show the reverse inclusion, let $a \in \mathscr{A}(D_0)$. For any monomial m occurring in a, we have $w(m) = w(a)$. By Theorem 4.5.4, $D_0 = \{f \in D : w(f) \in \mathrm{Hom}^0(\rho(G), \mathbb{F}^\bullet)\}$ whence $m \in M \cap D_0 = M_0$ and clearly $w(m) \in \langle w(\mathscr{A}(M_0)) \rangle$.

Recall that each monomial in $\mathbb{F}[V]$ spans a G-invariant subspace. Thus $f \in \mathbb{F}[V]$ is G_1-invariant if and only if all monomials of f are G_1-invariant. Furthermore, a monomial m is G_1-invariant if and only if $w(m)$ contains G_1 in its kernel; equivalently (by the characterization of D_0) $m \in M \cap D_0 = M_0$. Thus $\mathbb{F}[V]^{G_1}$ is generated by $\mathscr{A}(M_0)$ and hence the assertion follows from 1.

4. Since $M \subset D$, $M_0 \subset D_0$ and $M^G \subset H$ are divisor closed and since the embedding $H \subset D_0$ is a divisor theory (Theorem 4.5.4), $M^G \hookrightarrow M_0$ is a divisor homomorphism into a free abelian monoid. Let $m \in M_0$. Then $m \in D_0$ and there is a finite subset $Y \subset H$ such that $m = \gcd_{D_0}(Y)$. Let $X \subset D_0 \cap M = M_0$ be the set of all monomials occurring in some $y \in Y$. Then $m = \gcd_{D_0}(X) = \gcd_{M_0}(X)$, where the last equality holds because $M_0 \subset D_0$ is divisor closed.

Restricting the isomorphism

$$\overline{w} \mid_{\mathsf{q}(D_0)/\mathsf{q}(H)} \colon \mathscr{C}(\mathbb{F}[V]^G) = \mathsf{q}(D_0)/\mathsf{q}(H) \to \mathrm{Hom}^0(\rho(G), \mathbb{F}^\bullet)$$

from Theorem 4.5, we obtain a monomorphism

$$\overline{w} \mid_{\mathsf{q}(M_0)/\mathsf{q}(M^G)} \colon \mathscr{C}(M^G) = \mathsf{q}(M_0)/\mathsf{q}(M^G) \to \mathrm{Hom}^0(\rho(G), \mathbb{F}^\bullet).$$

By 1. and 3., the image contains the generating set $\{\chi_1^{e(x_1)}, \dots, \chi_n^{e(x_n)}\}$ of the group $\mathrm{Hom}^0(\rho(G), \mathbb{F}^\bullet)$ and hence the above monomorphism is an isomorphism. The last statement follows from 1. by $\overline{w}(\mathscr{C}(M^G)^*) = \overline{w}(\mathscr{A}(M_0))$.

Proposition 4.9 *Let $M \subset \mathbb{F}[x_1, \dots, x_n]$ be the multiplicative monoid of monomials, and $M^G \subset M$ the submonoid of G-invariant monomials.*

1. *Every class of $\mathscr{C}(\mathbb{F}[V]^G)$ contains a prime divisor.*
2. *We have the following commutative diagram of monoid homomorphisms*
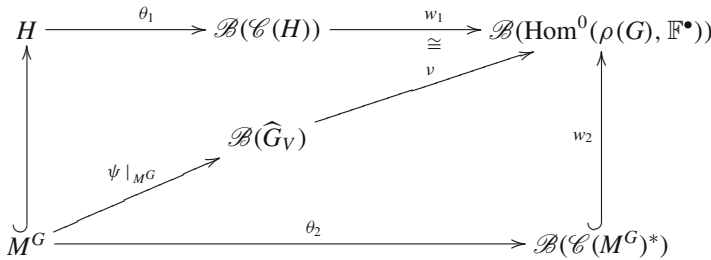
where

- *θ_1 and θ_2 are transfer homomorphisms of Krull monoids as given in Proposition 3.7.*
- *w_1 is the extension to the monoid of product-one sequences of the group isomorphism $\overline{w} \mid_{\mathsf{q}(D_0)/\mathsf{q}(H)}$ given in Theorem 4.5.4*
- *w_2 is the extension to the monoid of product-one sequences of the restriction to $\mathscr{C}(M^G)^*$ of the group isomorphism $\overline{w} \mid_{\mathsf{q}(M_0)/\mathsf{q}(M^G)}$ given in Proposition 4.8*
- *ψ is given in Proposition 4.7.*
- *v will be defined below (indeed, v is a transfer homomorphism as given in Proposition 3.8).*

3. *If $\widehat{G}_V = \widehat{G}$, then every class of $\mathscr{C}(M^G)$ contains a prime divisor.*

Proof 1. By Proposition 4.7.1, $\mathbb{F}[V]^G$ is the monoid algebra of M^G over $\mathbb{F}$. Thus, by [7, Theorem 8], every class of $\mathbb{F}[V]^G$ contains a prime divisor.

2. In order to show that the diagram is commutative, we fix an $m \in M^G$. We consider the divisor theory $M^G \hookrightarrow M_0$ from Proposition 4.8 and factorize m in M_0, say $m = \prod_{i=1}^{n} \left(x_i^{e(x_i)} \right)^{a_i}$ where $a_1, \ldots, a_n \in \mathbb{N}_0$. Since $\overline{w}(x_i^{e(x_i)}) = \chi_i^{e(x_i)}$ for all $i \in [1, n]$, it follows that

$$(w_2 \circ \theta_2)(m) = (\chi_1^{e(x_1)})^{[a_1]} \cdot \cdots \cdot (\chi_n^{e(x_n)})^{[a_n]} \in \mathscr{B}(\mathrm{Hom}^0(\rho(G), \mathbb{F}^\bullet)).$$

Next we view m as an element in H and consider the divisor theory $H \hookrightarrow D_0$. Since $M_0 \subset D_0$ is divisor closed, $m = \prod_{i=1}^{n} \left(x_i^{e(x_i)} \right)^{a_i}$ is a factorization of m in D_0. Therefore $(w_1 \circ \theta_1)(m) = (w_2 \circ \theta_2)(m)$.

By definition of ψ, we infer that

$$\psi(m) = \chi_1^{[e(x_1)a_1]} \cdot \cdots \cdot \chi_n^{[e(x_n)a_n]}.$$

We define a partition of $\widehat{G}_V = G_1 \cup G_2$, where $G_2 = \{\chi_i \colon \chi_i = \chi_j$ for some distinct $i, j \in [1, n]\}$ and $G_1 = \widehat{G}_V \backslash G_2$. Let $\nu \colon \mathscr{B}(\widehat{G}_V) \to \mathscr{B}(\mathrm{Hom}^0(\rho(G), \mathbb{F}^\bullet))$ be defined as in Proposition 3.8 (with respect to the partition $G_0 = G_1 \uplus G_2$). By Proposition 4.8.2, $e(x_i) = 1$ if $\chi_i \in G_2$, and $e(x_i)$ equals the number $e(\chi_i)$ in Proposition 3.8 if $\chi_i \in G_1$. Therefore it follows that

$$\nu(\psi(m)) = (\chi_1^{e(x_1)})^{[a_1]} \cdot \cdots \cdot (\chi_n^{e(x_n)})^{[a_n]},$$

and hence the diagram commutes.

3. In a finite abelian group all elements are contained in the subgroup generated by the other elements, with the only exception of the generator of a 2-element group. Therefore unless G is the 2-element group and the non-trivial character occurs with multiplicity one in the sequence $\chi_1 \cdot \cdots \cdot \chi_n$, all the $e(x_i) = 1$ by Proposition 4.8.3, and the elements x_i are all prime in M_0, so they represent all the divisor classes, as i varies in $[1, n]$. In the missing case we have $\mathbb{F}[V]^G = \mathbb{F}[x_1, \ldots, x_{n-1}, x_n^2]$ (after a renumbering of the variables if necessary), hence both class groups are trivial, and x_1 and x_2^2 are prime elements in the unique class.

Thus Proposition 4.9.1 gives a partial answer to Problem 1. Using that notation it states that $m_g \geq 1$ for all $g \in \mathscr{C}(\mathbb{F}[V]^G)$.

Example 4.10 The set $\mathscr{C}(M^G)^*$ may be a proper subset of $\mathscr{C}(M^G)$, and consequently the monoid homomorphism $\nu \colon \mathscr{B}(\widehat{G}_V) \to \mathscr{B}(\mathrm{Hom}^0(\rho(G), \mathbb{F}^\bullet))$ is not surjective in general.

1. Indeed, let G be cyclic of order 3, $g \in G$ with $\mathrm{ord}(g) = 3$, and the action on $\mathbb{F}[x_1, x_2, x_3]$ is given by $g \cdot x_i = \omega x_i$, where ω is a primitive cubic root of 1. Then $\chi_1 = \chi_2 = \chi_3 = \chi$, so $e(x_1) = e(x_2) = e(x_3) = 1$, implying $\overline{w}(\mathscr{C}(M^G)^*) = \{\chi\}$ (each of the x_i is a prime element in the class χ), whereas $\overline{w}(\mathscr{C}(M^G)) = \{\chi, \chi^2, \chi^3 = 1\}$, the 3-element group. Thus $\mathscr{B}(\widehat{G}_V) = \{\chi^{[3k]} \colon k \in \mathbb{N}_0\}$, and $\nu(\mathscr{B}(\widehat{G}_V))$ is the free

abelian monoid $\mathscr{F}(\{\chi^3\})$ generated by $\chi^3 = 1 \in \widehat{G}$. The polynomials $x_1^2 + x_2 x_3$ and $x_1^3 + x_2^2 x_3$ are irreducible, they are relative invariants of weight χ^2 and χ^3, so they represent prime elements of D_0 in the remaining classes χ^2 and $\chi^3 = 1$.

2. To provide an example with a multiplicity free module, let G be cyclic of order 5, $g \in G$ with $\mathrm{ord}(g) = 5$, and the action on $\mathbb{F}[x_1, x_2, x_3]$ is given by $g \cdot x_1 = \omega x_1$, $g \cdot x_2 = \omega^2 x_2$, $g \cdot x_3 = \omega^3 x_3$, where ω is a primitive fifth root of 1. Then setting $\chi = \chi_1$, we have $\chi_2 = \chi^2$, $\chi_3 = \chi^3$ and $\overline{w}(\mathscr{C}(M^G)) = \langle \chi \rangle$ is the 5-element group, so V is multiplicity free. Still we have $e(x_1) = e(x_2) = e(x_3) = 1$, so $\overline{w}(\mathscr{C}(M^G)^*) = \{\chi, \chi^2, \chi^3\}$ (and x_1, x_2, x_3 are the prime elements of M_0 in these classes). The remaining classes χ^4 and $\chi^5 = 1$ contain the prime elements of D_0 represented by $x_2^2 + x_1 x_3$ and $x_1^5 + x_2 x_3$.

4.4 A Monoid Associated with G-Modules

Throughout this subsection, suppose that $\mathrm{char}(\mathbb{F}) \nmid |G|$.

In this subsection, we discuss a monoid associated with representations of not necessarily abelian groups which in the case of abelian groups recovers the monoid of G-invariant monomials. Decompose V into the direct sum of G-modules:

$$V = V_1 \oplus \cdots \oplus V_r \tag{4}$$

and denote by $\rho_i \colon G \to \mathrm{GL}(V_i)$ the corresponding group homomorphisms. Then (4) induces a decomposition of $\mathbb{F}[V]$ into multihomogeneous components as follows. The coordinate ring $\mathbb{F}[V]$ is the symmetric algebra $\mathrm{Sym}(V^*) = \bigoplus_{n=0}^{\infty} \mathrm{Sym}^n(V^*)$. Writing $\mathbb{F}[V]_a = \mathrm{Sym}^{a_1}(V_1^*) \otimes \ldots \otimes \mathrm{Sym}^{a_r}(V_r^*)$ we have $\mathrm{Sym}^n(V^*) = \oplus_{|a|=n} \mathbb{F}[V]_a$, and hence $\mathbb{F}[V] = \oplus_{a \in \mathbb{N}_0^r} \mathbb{F}[V]_a$. The summands $\mathbb{F}[V]_a$ are G-submodules in $\mathbb{F}[V]$, and $\mathbb{F}[V]_a \mathbb{F}[V]_b \subset \mathbb{F}[V]_{a+b}$, so $\mathbb{F}[V]$ is a $\mathbb{N}_0^r$-graded algebra. Moreover, $\mathbb{F}[V]^G$ is spanned by its multihomogeneous components $\mathbb{F}[V]_a^G = \mathbb{F}[V]^G \cap \mathbb{F}[V]_a$. For $f \in \mathbb{F}[V]_a$ we call a the *multidegree* of f. We are in the position to define

$$\mathscr{B}(G, V) = \{a \in \mathbb{N}_0^r \colon \mathbb{F}[V]_a^G \neq \{0\}\} \tag{5}$$

the set of multidegrees of multihomogeneous G-invariants. We give precise information on $\mathscr{B}(G, V)$ in terms of quantities associated to the direct summands V_i of V. For $i \in [1, r]$ denote by c_i the greatest common divisor of the elements of $\mathscr{B}(G, V_i)$, and F_i the Frobenius number of the numerical semigroup $\mathscr{B}(G, V_i) \subset \mathbb{N}_0$, so F_i is the minimal positive integer N such that $\mathscr{B}(G, V_i)$ contains $N + k c_i$ for all $k \in \mathbb{N}_0$.

Proposition 4.11

1. $\mathscr{B}(G, V) \subset \mathbb{N}_0^r$ is a reduced finitely generated C-monoid.
2. For each $i \in [1, r]$ and all $a \in \mathbb{N}_0^r$ satisfying $a_i \geq b(G, V_i) + F_i$ we have

$$a \in \mathscr{B}(G, V) \quad \textit{if and only if} \quad c_i e_i + a \in \mathscr{B}(G, V). \tag{6}$$

3. *For each $i \in [1, r]$ we have $c_i = |\rho_i(G) \cap \mathbb{F}^\bullet \mathrm{id}_{V_i}|$.*

Proof 1. Take $a, b \in \mathscr{B}(G, V)$, so there exist non-zero $f \in \mathbb{F}[V]_a^G$ and $h \in \mathbb{F}[V]_b^G$. Now $0 \neq fh \in \mathbb{F}[V]_{a+b}^G$, hence $a + b \in \mathscr{B}(G, V)$. This shows that $\mathscr{B}(G, V)$ is a submonoid of $\mathbb{N}_0$. Moreover, the multidegrees of a multihomogeneous $\mathbb{F}$-algebra generating system of $\mathbb{F}[V]^G$ clearly generate the monoid $\mathscr{B}(G, V)$. Thus $\mathscr{B}(G, V)$ is finitely generated by Theorem 4.1.

To show that $\mathscr{B}(G, V)$ is also a C-monoid, recall that by Proposition 2.6.3 a finitely generated submonoid H of $\mathbb{N}_0^r$ is a C-monoid if and only if each standard basis element $e_i \in \mathbb{N}_0^r$ has a multiple in H. Now this condition holds for $\mathscr{B}(G, V)$, since by Theorem 4.1.2 $\mathbb{F}[V_i]^G \subset \mathbb{F}[V]^G$ contains a homogeneous element of positive degree for each $i \in [1, r]$.

2. By symmetry it is sufficient to verify (6) in the case $i = 1$. Suppose $a \in \mathscr{B}(G, V)$, so there is a non-zero G-invariant $f \in \mathrm{Sym}^{a_1}(V_1^*) \otimes \cdots \otimes \mathrm{Sym}^{a_r}(V_r^*)$. Decompose $\mathrm{Sym}^{a_1}(V_1^*) = \bigoplus_j W_j$ into a direct sum of irreducible G-modules. This gives a direct sum decomposition $\mathrm{Sym}^{a_1}(V_1^*) \otimes \cdots \otimes \mathrm{Sym}^{a_r}(V_r^*) = \bigoplus_j (W_j \otimes \mathrm{Sym}^{a_2}(V_2^*) \otimes \cdots \otimes \mathrm{Sym}^{a_r}(V_r^*))$. It follows that $\mathrm{Sym}^{a_1}(V_1^*)$ contains an irreducible G-module direct summand W such that $W \otimes \mathrm{Sym}^{a_2}(V_2^*) \otimes \cdots \otimes \mathrm{Sym}^{a_r}(V_r^*)$ contains a non-zero G-invariant. By definition of $b(G, V_1)$ we know that $\mathbb{F}[V_1]$ is generated as an $\mathbb{F}[V_1]^G$ module by its homogeneous components of degree $\leq b(G, V_1)$. Therefore, there exists a $d \leq b(G, V_1)$ such that the degree d homogeneous component of $\mathbb{F}[V]$ contains a G-submodule $U \cong W$, and $a_1 \in d + \mathscr{B}(G, V_1)$. Now for any homogeneous $h \in \mathbb{F}[V_1]^G$ we have $hU \otimes \mathrm{Sym}^{a_2}(V_2^*) \otimes \cdots \otimes \mathrm{Sym}^{a_r}(V_r^*)) \subset \mathbb{F}[V]_{(d+\deg(h), a_2, \ldots, a_r)}$ contains a non-zero G-invariant, since it is isomorphic to $W \otimes \mathrm{Sym}^{a_2}(V_2^*) \otimes \cdots \otimes \mathrm{Sym}^{a_r}(V_r^*))$. It follows that $(k, a_2, \ldots, a_r) \in \mathscr{B}(G, V)$ for all $k \in d + \mathscr{B}(G, V_1)$, in particular, for all $k \in \{d + F_1, d + F_1 + c_1, d + F_1 + 2c_1, \ldots\}$.

3. Let $i \in [1, r]$, and to simplify notation set $W = V_i$, $c = c_i$, and $\phi = \rho_i$. Recall that $\mathbb{F}[W]^A = \mathbb{F}[W]^B$ for some finite subgroups $A, B \subset \mathrm{GL}(W)$ implies that $A = B$. Indeed, the condition implies equality $\mathbb{F}(W)^A = \mathbb{F}(W)^B$ of the corresponding quotient fields, and so both A and B are the Galois groups of the field extension $\mathbb{F}(W)$ over $\mathbb{F}(W)^A = \mathbb{F}(W)^B$, implying $A = B$. Now denote by $Z \subset \mathrm{GL}(W)$ the subgroup of scalar transformations $Z = \{\omega \mathrm{id}_W : \omega^c = 1\}$, so Z is a central cyclic subgroup of $\mathrm{GL}(W)$ of order c. Clearly every homogeneous element of $\mathbb{F}[W]$ whose degree is a multiple of c is invariant under Z. It follows that $\mathbb{F}[W]^G \subset \mathbb{F}[W]^Z$, hence denoting by $\tilde{G}$ the subgroup $\phi(G)Z$ of $\mathrm{GL}(W)$, we have $\mathbb{F}[W]^G = \mathbb{F}[W]^{\tilde{G}}$. It follows that $\phi(G) = \tilde{G}$, i.e. $Z \subset \phi(G)$, and so $c = |Z|$ divides the order of $\phi(G) \cap \mathbb{F}^\bullet \mathrm{id}_W$. Conversely, if $\lambda \mathrm{id}_W$ belongs to $\rho(G)$, then every element of $\mathbb{F}[W]^G$ must be invariant under the scalar transformation $\lambda \mathrm{id}_W$, whence all homogeneous components of $\mathbb{F}[W]^G$ have degree divisible by the order of λ, so the order of the cyclic group $\phi(G) \cap \mathbb{F}^\bullet \mathrm{id}_W$ must divide c.

In general $\mathscr{B}(G, V)$ is not a Krull monoid. To provide an example, consider the two-dimensional irreducible representation V of the symmetric group $S_3 = D_6$. Its

ring of polynomial invariants is generated by an element of degree 2 and 3, hence $\mathscr{B}(G, V) = \langle 2, 3 \rangle \subset (\mathbb{N}_0, +)$, which is not Krull.

Proposition 4.12 *For every $k \in \mathbb{N}$ we have $\mathsf{D}_k(\mathscr{B}(G, V)) \leq \beta_k(G, V)$.*

Proof Let $k \in \mathbb{N}$. Take $a \in \mathscr{B}(G, V)$ such that $|a| > \beta_k(G, V)$. By (5) a multi-homogeneous invariant $f \in \mathbb{F}[V]_a^G$ exists. As $\deg(f) = |a| > \beta_k(G, V)$ it follows that $f = \sum_{i=1}^N f_{i,1} \ldots f_{i,k+1}$ for some non-zero multihomogeneous invariants $f_{i,j}$ of positive degree. Denoting by $a_{i,j} \in \mathbb{N}_0^r$ the multidegree of $f_{i,j}$, we have that $a = a_{i,1} + \cdots + a_{i,k+1}$, where $0 \neq a_{i,j} \in \mathscr{B}(G, V)$. This shows that all $a \in \mathscr{B}(G, V)$ with $|a| > \beta_k(G, V)$ factor into the product of more than k atoms, implying the desired inequality.

Remarks 1. Let G be abelian and suppose that $\mathbb{F}$ is algebraically closed. Then we may take in (4) a decomposition of V into the direct sum of 1-dimensional submodules and so V_i^*, is spanned by a variable x_i as in Sect. 4.3. Then $\mathbb{F}[V]_a$ is spanned by the monomial $x_1^{a_1} \cdots x_r^{a_r}$ and $a \in \mathscr{B}(G, V)$ holds if and only if the corresponding monomial is G-invariant. So in this case $\mathscr{B}(G, V)$ can be naturally identified with M^G and the transfer homomorphism $\psi \mid_{M^G}$ of Proposition 4.7 can be thought of as a transfer homomorphism $\mathscr{B}(G, V) \to \mathscr{B}(\widehat{G}_V)$, which is an isomorphism if V is multiplicity free. However, this transfer homomorphism does not seem to have an analogues for non-abelian G (i.e., the study of $\mathscr{B}(G, V)$ can not be reduced to the multiplicity free case), as it is shown by the example below.

2. The binary tetrahedral group $G = \widetilde{A}_4 \cong SL_2(\mathbb{F}_3)$ of order 24 has a two-dimensional complex irreducible representation V such that $\mathbb{F}[V]^G$ is minimally generated by elements of degree 6, 8, 12 (see for example [4, Appendix A]), hence $\mathscr{B}(G, V) = \{0, 6, 8, 12, 14, 16, 18, \ldots\}$. On the other hand under this representation G is mapped into the special linear group of V, so on $V \oplus V$ the function mapping $((x_1, x_2), (y_1, y_2)) \mapsto \det \begin{pmatrix} x_1 & y_1 \\ x_2 & y_2 \end{pmatrix}$ is a G-invariant of multidegree $(1, 1)$, implying that $(1, 1) \in \mathscr{B}(G, V \oplus V)$. This shows that the transfer homomorphism $\tau : \mathbb{N}_0^2 \to \mathbb{N}_0$, $(a_1, a_2) \mapsto a_1 + a_2$ does not map $\mathscr{B}(G, V \oplus V)$ into $\mathscr{B}(G, V)$, as $\tau(1, 1) = 2 \notin \mathscr{B}(G, V)$.

Recall that the multigraded Hilbert series of $\mathbb{F}[V]^G$ in r indeterminates $T = (T_1, ..., T_r)$ is

$$H(\mathbb{F}[V]^G, T) = \sum_{a \in \mathbb{N}_0^r} \dim_{\mathbb{F}}(\mathbb{F}[V]_a^G) T_1^{a_1} \cdots T_r^{a_r}, \quad \text{and hence}$$

$$\mathscr{B}(G, V) = \{a \in \mathbb{N}_0^r \colon \text{ the coefficient of } T^a \text{ in } H(\mathbb{F}[V]^G, T) \text{ is nonzero}\}.$$

By this observation Proposition 4.12 can be used for finding lower bounds on the Noether number $\beta(G, V)$, thanks to the following classical result of Molien (see for example [4, Theorem 2.5.2]):

Proposition 4.13 *Given a G-module $V = V_1 \oplus \dots \oplus V_r$ over $\mathbb{C}$, let $\rho_i(g) \in \mathrm{GL}(V_i)$ be the linear transformation defining the action of $g \in G$ on V_i. Then we have*

$$H(\mathbb{C}[V]^G, T) = \frac{1}{|G|} \sum_{g \in G} \prod_{i=1}^{r} \frac{1}{\det(\mathrm{id}_{V_i} - \rho_i(g) \cdot T_i)}.$$

Example 4.14 (*see pp. 54–55 in* [62]) Consider the alternating group A_5 and its 3-dimensional representation over $\mathbb{C}^3$ as the group of symmetries of an icosahedron. The Hilbert series then equals

$$\frac{1 + T^{15}}{(1 - T^2)(1 - T^6)(1 - T^{10})}$$

whence it is easily seen that $\mathscr{B}(A_5, \mathbb{C}^3) = \langle 2, 6, 10, 15 \rangle$ and consequently $\beta(A_5) \geq \mathsf{D}(\mathscr{B}(A_5, \mathbb{C}^3)) = 15$. Note that this lower bound is stronger than what we could get from $\beta(G) \geq \max_{H \subsetneq G} \beta(H)$, since $\beta(H) \leq |H| \leq 12$ for any proper subgroup H of A_5.

5 Constants from Invariant Theory and Their Counterparts in Arithmetic Combinatorics

In Sect. 5.1 we compare known reduction lemmas for the Noether number with reduction lemmas for the Davenport constants achieved in previous sections. We demonstrate how to use them to determine the precise value of Noether numbers and Davenport constants in new examples. In Sect. 5.2 we consider an invariant theoretic analogue of the constant $\eta(G)$ (for the definition of $\eta(G)$ see the discussions before Proposition 2.8 and Lemma 3.1).

Throughout this section, suppose that $\mathrm{char}(\mathbb{F}) \nmid |G|$.

5.1 The Noether Number Versus the Davenport Constant

In the non-abelian case no structural connection (like Proposition 4.7) is known between the G-invariant polynomials and the product-one sequences over G. Nevertheless, a variety of features of the kth Noether numbers and the kth Davenport constants are strikingly similar, and we offer a detailed comparison.

Recall that $\beta_k(G) = b_k(G) + 1$ ((3)) and that $\mathsf{d}_k(G) + 1 \leq \mathsf{D}_k(G)$ (Proposition 2.8.1).

1. The inequalities

$$(a) \quad \beta_k(G) \le k\beta(G) \quad (b) \quad \mathsf{d}_k(G) + 1 \le k(\mathsf{d}(G) + 1) \quad (c) \quad \mathsf{D}_k(G) \le k\mathsf{D}(G) \tag{7}$$

2. Reduction lemma for normal subgroups $N \triangleleft G$:

$$(a) \quad \beta_k(G) \le \beta_{\beta_k(G/N)}(N) \qquad (b) \quad \mathsf{d}_k(G) \le \mathsf{d}_{\mathsf{d}_k(N)+1}(G/N) \tag{8}$$

3. Reduction lemma for arbitrary subgroups $H \le G$ with index $l = [G : H]$:

$$(a)\, \beta_k(G) \le \beta_{kl}(H) \le l\beta_k(H) \quad (b)\, \mathsf{d}_k(G) + 1 \le l(\mathsf{d}_k(H) + 1) \quad (c)\, \mathsf{D}_k(G) \le l\mathsf{D}_k(H) \tag{9}$$

4. Supra-additivity: for a normal subgroup $N \triangleleft G$ we have

$$(a) \quad b_{k+r-1}(G) \ge b_k(N) + b_r(G/N) \text{ if } G/N \text{ is abelian} \tag{10}$$

$$(b) \quad \mathsf{d}_{k+r-1}(G) \ge \mathsf{d}_k(N) + \mathsf{d}_r(G/N)$$

5. Monotonicity: for an arbitrary subgroup $H \le G$ we have

$$(a) \quad \beta_k(G) \ge \beta_k(H) \quad (b) \quad \mathsf{d}_k(G) \ge \mathsf{d}_k(H) \quad (c) \quad \mathsf{D}_k(G) \ge \mathsf{D}_k(H) \tag{11}$$

6. Almost linearity in k: there are positive constants $C, C', C'', k_0, k_0', k_0''$ depending only on G such that

$$(a)\, \beta_k(G) = k\sigma(G) + C \text{ for all } k > k_0 \text{ if } \operatorname{char}(\mathbb{F}) = 0 \quad (b)\, \mathsf{d}_k(G) = k\mathsf{e}(G) + C' \tag{12}$$

for all $k > k_0'$ and $(c)\, \mathsf{D}_k(G) = k\mathsf{e}(G) + C''$ for all $k > k_0''$

7. The following functions are nonincreasing in k:

$$(a) \quad \beta_k(G)/k \text{ if } \operatorname{char}(\mathbb{F}) = 0 \qquad (b) \quad \mathsf{D}_k(G)/k \tag{13}$$

The inequality (7) (a) is observed in [12], (b) is shown in Proposition 3.9.4, whereas (c) is observed in the beginning of Sect. 2.5.

For the proof of (8) (a) see [12, Lemma 1.5] and for part (b) see Proposition 3.9.2. Note that the roles of N and G/N are swapped in the formulas (a) respectively (b), but in the abelian case they amount to the same.

The first inequality in part (a) of (9) is proved in [12, Corollary 1.11] for cases when (i) $\operatorname{char}(\mathbb{F}) = 0$ or $\operatorname{char}(\mathbb{F}) > [G : H]$; (ii) H is normal in G and $\operatorname{char}(\mathbb{F}) \nmid [G : H]$; (iii) $\operatorname{char}(\mathbb{F})$ does not divide $|G|$. It is conjectured, however that it holds in fact whenever $\operatorname{char}(F) \nmid [G : H]$ (see [55]). By [11, Lemma 4.3], we have $\beta_{kl}(H) \le$

$l\beta_k(H)$ for all positive integers k, l, implying the second inequality in part (a). Parts (b) and (c) of (9) appear in Proposition 3.9 (3. and 5.).

Part (a) of (10) appears in [13, Theorem 4.3 and Remark 4.4] while part (b) is proved in Proposition 3.9.1.

Parts (b) and (c) of (11) are immediate from the definitions, while part (a) follows from an argument of B. Schmid [73, Proposition 5.1] which also shows that $\beta_k(G, \mathrm{Ind}_H^G V) \geq \beta_k(H, V)$ for all $k \geq 1$ (see [13, Lemma 4.1]).

Part (a) of (12) is proved in [11, Proposition 4.5] (the constant $\sigma(G)$ will be discussed in Sect. 5.2, and for (12) (b) and (c) we refer to Proposition 2.7.2 and Proposition 2.8.2.

Part (a) of (13) is proved in [11, Sect. 4] and for (13) (b) we refer to Proposition 2.7.3.

Furthermore, for a normal subgroup $N \lhd G$ we have

$$(a) \quad \beta(G) \leq \beta(G/N)\beta(N) \qquad (b) \quad \mathsf{D}(G) \leq \mathsf{D}(N)\mathsf{D}(G/N), \qquad (14)$$

where in (b) we assume that $N \cap G' = \{1\}$. Here part (a) is originally due to B. Schmid [73, Lemma 3.1] and it is an immediate consequence of (7) (a) and (8) (a) while part (b) is proven in [39, Theorem 3.3].

The above reduction lemmas on the Noether numbers are key tools in the proof of the following theorem.

Theorem 5.1 *Let $k \in \mathbb{N}$.*

1. *$\beta_k(A_4) = 4k + 2$ and $\beta(\tilde{A}_4) = 12$, where A_4 is the alternating group of degree 4 and $\tilde{A}_4$ is the binary tetrahedral group.*

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

$$\beta_k(G) = \frac{1}{2}|G|k + \begin{cases} 2 & \text{if } G = Dic_{4m}, \ m > 1; \\ 1 & \text{otherwise.} \end{cases}$$

   where $Dic_{4m} = \langle a, b : a^{2m} = 1, b^2 = a^m, bab^{-1} = a^{-1}\rangle$ is the dicyclic group.

3.

$$\beta(G) \geq \frac{1}{2}|G| \quad \text{if and only if} \quad G \text{ has a cyclic subgroup of index at most two or}$$

$$G \text{ is isomorphic to } C_3 \oplus C_3, \ C_2 \oplus C_2 \oplus C_2, \ A_4 \text{ or } \tilde{A}_4$$

Proof For 1. see [12, Theorem 3.4 and Corollary 3.6], for 2. see [13, Theorem 10.3], and 3. can be found in [12, Theorem 1.1]. $\square$

It is worthwhile to compare Theorem 5.1.3 with the statement from [65] asserting that $\mathsf{d}(G) < \frac{1}{2}|G|$ unless G has a cyclic subgroup of index at most two. If G is abelian, then Lemma 3.13 and Proposition 4.7 imply $\mathsf{d}(G) + 1 = \beta(G) = \mathsf{D}(G)$. Combining Theorems 3.10 and 5.1 we obtain that all groups G having a cyclic subgroup of index

at most two satisfy the inequality $\mathsf{d}(G) + 1 \leq \beta(G) \leq \mathsf{D}(G)$. Moreover, for these groups $\beta(G) = \mathsf{d}(G) + 1$, except for the dicyclic groups, where $\beta(G) = \mathsf{d}(G) + 2$. On the other hand, it was shown in [14] that for the Heisenberg group H_{27} of order 27 we have $\mathsf{D}(H_{27}) < \beta(H_{27})$.

Problem 2 Study the relationship between the invariants $\mathsf{d}(G)$, $\beta(G)$, and $\mathsf{D}(G)$. In particular,

- Characterize the groups G satisfying $\mathsf{d}(G) + 1 \leq \beta(G)$.
- Characterize the groups G satisfying $\beta(G) \leq \mathsf{D}(G)$.

In the following examples we demonstrate how the reduction results presented at the beginning of this section do work. This allows us to determine Noether numbers and Davenport constants of non-abelian groups, for which they were not known before.

Example 5.2 Let p, q be primes such that $q \mid p - 1$.

1. Consider the non-abelian semi-direct product $G = C_p \rtimes C_q$. A conjecture attributed to Pawale [81] states that $\beta(C_p \rtimes C_q) = p + q - 1$ and many subsequent research was done in this direction [12, 17]. Currently it is fully proved only for the cases $q = 2$ in [73] and $q = 3$ in [10] whereas for arbitrary q we have only upper bounds in [12], proved using known results related to the Olson constant of the cyclic group of order p. Theorem 3.11.3 implies that $\mathsf{d}(G) + 1 = p + q - 1$ and hence $\mathsf{d}(G) + 1$ coincides with the conjectured value for $\beta(G)$.

2. In view of the great difficulties related to Pawale's conjecture it is quite remarkable that we can determine the exact value of the Noether number for the non-abelian semi-direct product $C_{pq} \rtimes C_q$. Indeed, this group contains an index p subgroup isomorphic to $C_q \oplus C_q$, hence $\beta(C_{pq} \rtimes C_q) \leq \beta_p(C_q \oplus C_q)$ by (9). By Proposition 4.7 4. we have $\beta_p(C_q \oplus C_q) = \mathsf{D}_p(C_q \oplus C_q)$, and finally, $\mathsf{D}_p(C_q \oplus C_q) = pq + q - 1$ by Theorem 3.14. Thus we have $\beta(C_{pq} \rtimes C_q) \leq pq + q - 1$. The reverse inequality also holds, since $\beta(C_{pq} \rtimes C_q)$ contains a normal subgroup $N \cong C_{pq}$ with $G/N \cong C_q$, so by (10) and (3) we have $\beta(C_{pq} \rtimes C_q) \geq \beta(C_{pq}) + \beta(C_q) - 1 = pq + q - 1$. So we have $\beta(C_{pq} \rtimes C_q) = pq + q - 1$.

Next we determine the small Davenport constant of this group. Since C_{pq} is a normal subgroup and the corresponding factor group is C_q, we have by Proposition 3.9.1 that $\mathsf{d}(C_{pq} \rtimes C_q) \geq \mathsf{d}(C_{pq}) + \mathsf{d}(C_q) = p + q - 2$. The reverse inequality $\mathsf{d}(C_{pq} \rtimes C_q) \leq p + q - 2$ follows from Theorem 3.11.4, since $C_{pq} \rtimes C_q$ contains also a normal subgroup $N \cong C_p$ such that $G/N \cong C_q \oplus C_q$. Consequently, by Lemma 3.1.2.(a) we have

$$\mathsf{D}(C_{pq} \rtimes C_q) \geq \mathsf{d}(C_{pq} \rtimes C_q) + 1 = pq + q - 1.$$

Example 5.3 The symmetric group S_4 has a normal subgroup $N \cong C_2 \oplus C_2$ such that $S_4/N \cong D_6$. We know that $\beta(D_6) = 4$ (say by Theorem 5.1 2.). Thus by (8) and Theorem 3.14 we have $\beta(S_4) \leq \beta_{\beta(D_6)}(C_2 \oplus C_2) = \mathsf{D}_4(C_2 \oplus C_2) = 2 \cdot 4 + 1 = 9$.

Now let V be the standard 4-dimensional permutation representation of S_4 and sign : $S_4 \to \{\pm 1\}$ the sign character. It is not difficult to prove the algebra isomorphism $\mathbb{F}[V \otimes \text{sign}]^{S_4} \cong \mathbb{F}[V]^{S_4}_{even} \oplus \Delta_4 \mathbb{F}[V]^{S_4}_{odd}$ where Δ_4 is the Vandermonde determinant in 4 variables, $\mathbb{F}[V]^{S_4}_{even}$ is the span of the even degree homogeneous components of $\mathbb{F}[V]^{S_4}$, and $\mathbb{F}[V]^{S_4}_{odd}$ is the span of the odd degree homogeneous components of $\mathbb{F}[V]^{S_4}$. Moreover, the algebra $\mathbb{F}[V]^{S_4}_{even} \oplus \Delta_4 \mathbb{F}[V]^{S_4}_{odd}$ is easily seen to be minimally generated by $\sigma_2, \sigma_1^2, \sigma_1\sigma_3, \sigma_4, \sigma_3^2, \sigma_1\Delta_4, \sigma_3\Delta_4$, where σ_i is the ith elementary symmetric polynomial. As a result $\beta(S_4, V \otimes \text{sign}) = \deg(\sigma_3\Delta_4) = 3 + \binom{4}{2} = 9$. So we conclude that $\beta(S_4) = 9$ (and not 10, as it is claimed on p. 14 of [57]).

Example 5.4 Let G be the group generated by the complex Pauli matrices

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

This is a pseudoreflection group, hence the ring of invariants on $V = \mathbb{C}^2$ is generated by two elements, namely $\mathbb{C}[x, y]^G = \mathbb{C}[x^4 + y^4, x^2y^2]$. Moreover, $b(G, V)$ is the sum of the degrees of the generators minus $\dim(V)$ (again because G is a pseudoreflection group, see [9]), so $b(G, V) = 6$. It follows by (3) that $\beta(G) = b(G) + 1 \geq b(G, V) + 1 = 7$.

On the other hand, G is a non-abelian semi-direct product $(C_4 \oplus C_2) \rtimes C_2$. Therefore G has a normal subgroup N such that $N \cong G/N \cong C_2 \oplus C_2$ and thus

$$\beta(G) \leq \beta_{\beta(C_2\oplus C_2)}(C_2 \oplus C_2) = \mathsf{D}_3(C_2 \oplus C_2) = 7.$$

So we conclude that $\beta(G) = 7$.

5.2 The Constants $\sigma(G, V)$ and $\eta(G, V)$

Definition 5.5 1. Let $\sigma(G, V)$ denote the smallest $d \in \mathbb{N}_0 \cup \{\infty\}$ such that $\mathbb{F}[V]^G$ is a finitely generated module over a subring $\mathbb{F}[f_1, \dots, f_r]$ such that $\max\{\deg(f_i) : i \in [1, r]\} = d$. We define $\sigma(G) = \sup\{\sigma(G, W) : W \text{ is a } G\text{-module}\}$.

2. Let $S \subset \mathbb{F}[V]^G$ be the F-subalgebra of $\mathbb{F}[V]^G$ generated by its elements of degree at most $\sigma(G, V)$. Then $\eta(G, V)$ denotes the maximal degree of generators of $\mathbb{F}[V]^G_+$ as an S-module.

One motivation to study $\sigma(G, V)$ and $\eta(G, V)$ is that by a straightforward induction argument [11, Sect. 4] we have

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

By [11, Proposition 6.2], $\sigma(C_p \rtimes C_q) = p$ (this is also true in characteristic q, see [18, Proposition 4.5]).

If $\mathbb{F}$ is algebraically closed, then, by Hilbert's Nullstellensatz, $\sigma(G, V)$ is the smallest d such that there exist homogeneous invariants of degree at most d whose common zero locus is the origin. It is shown in Lemmas 5.1, 5.4 and 5.6 of [11] (some extensions to the modular case and for linear algebraic groups are given in [18]) that

- $\sigma(G) \leq \sigma(G/N)\sigma(N)$ if $N \lhd G$;
- $\sigma(H) \leq \sigma(G) \leq [G : H]\sigma(H)$ if $H \leq G$;
- $\sigma(G) = \max\{\sigma(G, V) \colon V \text{ is an irreducible } G\text{-module}\}$.

Proposition 5.6 *Let G be abelian.*

1. $\sigma(G) = \exp(G) = \mathsf{e}(G)$.
2. $\eta(G) = \sup\{\eta(G, W) \colon W \text{ is a } G\text{-module}\}$.

Proof For 1. see [11, Corollary 5.3]. To prove 2., let $T \in \mathcal{F}(\widehat{G})$ with $|T| = \eta(G) - 1$ such that T has no product-one subsequence U with $|U| \in [1, \mathsf{e}(G)]$. Let V be the regular representation of G, and denote by S the subalgebra of $\mathbb{F}[V]^G$ generated by its elements of degree at most $\sigma(G) = \mathsf{e}(G)$. Now $\psi \colon M \to \mathcal{F}(\widehat{G})$ is an isomorphism (see the proof of Proposition 4.7.3.). Thus $\psi^{-1}(T) \in M$ is not divisible by a G-invariant monomial of degree smaller than $\mathsf{e}(G)$. Since both S and $\mathbb{F}[V]$ are spanned by monomials, it follows that $\psi^{-1}(T) \in M$ is not contained in the S-submodule of $\mathbb{F}[V]_+^G$ generated by elements of degree less than $\deg(\psi^{-1}(T))$. This shows that for the regular representation V of G we have $\eta(G, V) \geq \eta(\widehat{G})$.

On the other hand let W be an arbitrary G-module, and $m \in M$ a monomial with $\deg(m) > \eta(G)$. Then $\psi(m)$ has a product-one subsequence with length at most $\mathsf{e}(G) = \sigma(G)$, hence m is divisible by a G-invariant monomial of length at most $\sigma(G)$ (see the beginning of the proof of Proposition 4.7.2). This shows the inequality $\eta(G, W) \leq \eta(\widehat{G})$. Taking into account the isomorphism $\widehat{G} \cong G$ we are done. $\square$

For the state of the art on $\eta(G)$ (in the abelian case) we refer to [22, 23], [40, Theorem 5.8.3]. Proposition 5.6 inspires the following problem.

Problem 3 Let G be a finite non-abelian group. Is $\sup\{\eta(G, W) \colon W \text{ is a } G\text{-module}\}$ finite? Is it related to $\eta(\mathscr{B}(G))$ (see Sects. 2.5 and 3.1)?

References

1. N.R. Baeth, A. Geroldinger, Monoids of modules and arithmetic of direct-sum decompositions. Pacific J. Math. **271**, 257–319 (2014)
2. P. Baginski, S.T. Chapman, Arithmetic congruence, monoids: a survey, *Combinatorial and Additive Number Theory: CANT, and 2012*, Springer Proceedings in Mathematics and Statistics (Springer, Berlin, 2014), pp. 15–38

3. J. Bass, Improving the Erdős-Ginzburg-Ziv theorem for some non-abelian groups. J. Number Theor. **126**, 217 (2007)
4. D.J. Benson, *Polynomial Invariants of Finite Groups*, vol. 190, London Mathematical Society Lecture Notes Series (Cambridge University Press, Cambridge, 1993)
5. G. Bhowmik, J.-C. Schlage-Puchta, Davenport's constant for groups of the form $\mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{3d}$, in *Additive Combinatorics*, vol. 43, CRM Proceedings and Lecture Notes, ed. by A. Granville, M.B. Nathanson, J. Solymosi (American Mathematical Society, 2007), pp. 307–326
6. G. Bhowmik, J.-C. Schlage-Puchta, Davenport's constant for groups with large exponent, *Theory and Applications of Finite Fields*, Contemporary Mathematics (AMS, 2013), pp. 21–31
7. G.W. Chang, Every divisor class of Krull monoid domains contains a prime ideal. J. Algebra **336**, 370–377 (2011)
8. F. Chen, S. Savchev, Long minimal zero-sum sequences in the groups $C_2^{r-1} \oplus C_{2k}$. Integers **14**, Paper A23 (2014)
9. C. Chevalley, Invariants of finite groups generated by reflections. Amer. J. Math. **77**, 778–782 (1955)
10. K. Cziszter, The Noether number of the non-abelian group of order $3p$. Per. Math. Hungarica **68**, 150–159 (2014)
11. K. Cziszter, M. Domokos, On the generalized Davenport constant and the Noether number. Central Eur. J. Math. **11**, 1605–1615 (2013)
12. K. Cziszter, M. Domokos, Groups with large Noether bound. Ann. Inst. Fourier (Grenoble) **64**, 909–944 (2014)
13. K. Cziszter, M. Domokos, The Noether number for the groups with a cyclic subgroup of index two. J. Algebra **399**, 546–560 (2014)
14. K. Cziszter, M. Domokos, I. Szöllősi, The Noether number and the Davenport constants of the groups of order less than 32, manuscript in preparation
15. C. Delorme, O. Ordaz, D. Quiroz, Some remarks on Davenport constant. Discrete Math. **237**, 119–128 (2001)
16. H. Derksen, G. Kemper, Computational invariant theory, *Encyclopedia of Mathematical Sciences*, vol. 130 (Springer, Berlin, 2002)
17. M. Domokos, P. Hegedűs, Noether's bound for polynomial invariants of finite groups. Arch. Math. **74**, 161–167 (2000)
18. J. Elmer, M. Kohls, Zero-separating invariants for finite groups. J. Algebra **411**, 92–113 (2014)
19. A. Facchini, Direct sum decomposition of modules, semilocal endomorphism rings, and Krull monoids. J. Algebra **256**, 280–307 (2002)
20. A. Facchini, Krull monoids and their application in module theory, in *Algebras, Rings and their Representations*, ed. by A. Facchini, K. Fuller, C.M. Ringel, C. Santa-Clara (World Scientific, 2006), pp. 53–71
21. A. Facchini, Direct-sum decompositions of modules with semilocal endomorphism rings. Bull. Math. Sci. **2**, 225–279 (2012)
22. Y. Fan, W. Gao, Q. Zhong, On the Erdős-Ginzburg-Ziv constant of finite abelian groups of high rank. J. Number Theory **131**, 1864–1874 (2011)
23. Y. Fan, W. Gao, L. Wang, Q. Zhong, Two zero-sum invariants on finite abelian groups. Europ. J. Comb. **34**, 1331–1337 (2013)
24. B.W. Finklea, T. Moore, V. Ponomarenko, Z.J. Turner, Invariant polynomials and minimal zero sequences. Involve **1**, 159–165 (2008)
25. P. Fleischmann, The Noether bound in invariant theory of finite groups. Adv. Math. **156**, 23–32 (2000)
26. P. Fleischmann, M. Sezer, R.J. Shank, C.F. Woodcock, The Noether numbers for cyclic groups of prime order. Adv. Math. **207**, 149–155 (2006)
27. P. Fleischmann, C.F. Woodcock, Relative invariants, ideal classes, and quasi-canonical modules of modular rings of invariants. J. Algebra **348**, 110–134 (2011)
28. J. Fogarty, On Noether's bound for polynomial invariants of a finite group. Electron. Res. Announc. Amer. Math. Soc. **7**, 5–7 (2001). (electronic)

29. R.M. Fossum, *The Divisor Class Group of a Krull Domain* (Springer, Berlin, 1973)
30. M. Freeze, W.A. Schmid, Remarks on a generalization of the Davenport constant. Discrete Math. **310**, 3373–3389 (2010)
31. W. Gao, A. Geroldinger, On zero-sum sequences in $\mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$. Integers **3**, Paper A08, 45 p (2003)
32. W. Gao, A. Geroldinger, Zero-sum problems in finite abelian groups : a survey. Expo. Math. **24**, 337–369 (2006)
33. W. Gao, Z. Lu, The Erdős-Ginzburg-Ziv theorem for dihedral groups. J. Pure Appl. Algebra **212**, 311–319 (2008)
34. W. Gao, Y. Li, The Erdős-Ginzburg-Ziv theorem for finite solvable groups. J. Pure Appl. Algebra **214**, 898–909 (2010)
35. W. Gao, A. Geroldinger, D.J. Grynkiewicz, Inverse zero-sum problems III. Acta Arith. **141**, 103–152 (2010)
36. W. Gao, Y. Li, J. Peng, An upper bound for the Davenport constant of finite groups. J. Pure Appl. Algebra **218**, 1838–1844 (2014)
37. A. Geroldinger, Additive group theory and non-unique factorizations, in *Combinatorial Number Theory and Additive Group Theory*, Advanced Courses in Mathematics CRM Barcelona, ed. by A. Geroldinger, I. Ruzsa (Birkhäuser, 2009), pp. 1–86
38. A. Geroldinger, Non-commutative Krull monoids: a divisor theoretic approach and their arithmetic. Osaka J. Math. **50**, 503–539 (2013)
39. A. Geroldinger, D.J. Grynkiewicz, The large Davenport constant I: groups with a cyclic index 2 subgroup. J. Pure Appl. Algebra **217**, 863–885 (2013)
40. A. Geroldinger, F. Halter-Koch, *Non-Unique Factorizations. Algebraic, Combinatorial and Analytic Theory*, vol. 278, Pure and Applied Mathematics (Chapman & Hall/CRC, 2006)
41. A. Geroldinger, W. Hassler, Arithmetic of Mori domains and monoids. J. Algebra **319**, 3419–3463 (2008)
42. A. Geroldinger, R. Schneider, On Davenport's constant, J. Comb. Theory, Ser. A **61**, 147–152 (1992)
43. A. Geroldinger, Q. Zhong, *The set of minimal distances in Krull monoids*. Acta Arithmetica **173**, 97–120 (2016)
44. A. Geroldinger, M. Liebmann, A. Philipp, On the Davenport constant and on the structure of extremal sequences. Period. Math. Hung. **64**, 213–225 (2012)
45. A. Geroldinger, S. Ramacher, A. Reinhart, On v-Marot Mori rings and C-rings. J. Korean Math. Soc. **52**, 1–21 (2015)
46. R. Gilmer, Multiplicative Ideal Theory. Queen's Papers **90** (1992)
47. B. Girard, Inverse zero-sum problems and algebraic invariants. Acta Arith. **135**, 231–246 (2008)
48. D.J. Grynkiewicz, The large Davenport constant II: general upper bounds. J. Pure Appl. Algebra **217**, 2221–2246 (2013)
49. D.J. Grynkiewicz, *Structural Additive Theory*, Developments in Mathematics (Springer, Berlin, 2013)
50. F. Halter-Koch, A generalization of Davenport's constant and its arithmetical applications. Colloq. Math. **63**, 203–210 (1992)
51. F. Halter-Koch, *Ideal Systems. An Introduction to Multiplicative Ideal Theory* (Marcel Dekker, 1998)
52. F. Halter-Koch, Multiplicative ideal theory in the context of commutative monoids, in *Commutative Algebra: Noetherian and Non-Noetherian Perspectives*, ed. by M. Fontana, S.-E. Kabbaj, B. Olberding, I. Swanson (Springer, 2011), pp. 203–231
53. D. Han, The Erdős-Ginzburg-Ziv Theorem for finite nilpotent groups. Archiv Math. **104**, 325–332 (2015)
54. P. Hegedűs, L. Pyber, *Bounding the Noether Number of Finite Groups*. In preparation
55. G. Kemper, Separating invariants. J. Symbolic Comput. **44**(9), 1212–1222 (2009)
56. F. Knop, On Noether's and Weyl's bound in positive characteristic, *Invariant Theory in All Characteristics*, vol. 35, CRM Proceedings of Lecture Notes (American Mathematical Society, Providence, 2004), pp. 175–188

57. H. Kraft, C. Procesi, *Classical Invariant Theory, A Primer* Website of H. Kraft (1996)
58. H. Nakajima, Relative invariants of finite groups. J. Algebra **79**, 218–234 (1982)
59. J. Neukirch, *Algebraic Number Theory* (Springer, Berlin, 1999)
60. M.D. Neusel, Degree bounds—an invitation to postmodern invariant theory. Topology Appl. **154**, 792–814 (2007)
61. M.D. Neusel, Invariant Theory, *Student Mathematical Library*, vol. 36 (AMS, 2007)
62. M.D. Neusel, L. Smith, Invariant theory of finite groups, *Mathematical Surveys and Monographs*, vol. 94 (AMS, 2002)
63. E. Noether, Der Endlichkeitssatz der Invarianten endlicher Gruppen. Math. Ann. **77**, 89–92 (1916)
64. E. Noether, Der Endlichkeitssatz der Invarianten endlicher Gruppen der Charakteristik p. Nachr. Ges. Wiss. Göttingen, Math.-Phys. Kl. **1926**, 28–35 (1926)
65. J.E. Olson, E.T. White, Sums from a sequence of group elements, in *Number Theory and Algebra*, ed. by H. Zassenhaus (Academic Press, 1977), pp. 215–222
66. V. Ponomarenko, Minimal zero sequences of finite cyclic groups. Integers **4**, A24, 6 p (2004)
67. M. Radziejewski, On the distribution of algebraic numbers with prescribed factorization properties. Acta Arith. **116**, 153–171 (2005)
68. C. Reiher, A proof of the theorem according to which every prime number possesses property B, Ph.D. thesis, Rostock, 2010
69. A. Reinhart, On integral domains that are C-monoids. Houston J. Math. **39**, 1095–1116 (2013)
70. D.R. Richman, Invariants of finite groups over fields of characteristic p. Adv. Math. **124**, 25–48 (1996)
71. S. Savchev, F. Chen, Long zero-free sequences in finite cyclic groups. Discrete Math. **307**, 2671–2679 (2007)
72. S. Savchev, F. Chen, *Long minimal zero-sum sequences in the group $C_2 \oplus C_{2k}$*. Integers **12**, Paper A51, 18 p (2012)
73. B.J. Schmid, Finite groups and invariant theory, *Topics in Invariant Theory*, vol. 1478, Lecture Notes in Mathematics (Springer, Berlin, 1991), pp. 35–66
74. W.A. Schmid, Higher-order class groups and block monoids of Krull monoids with torsion class group. J. Algebra Appl. **9**, 433–464 (2010)
75. W.A. Schmid, Inverse zero-sum problems II. Acta Arith. **143**, 333–343 (2010)
76. W.A. Schmid, The inverse problem associated to the Davenport constant for $C_2 \oplus C_2 \oplus C_{2n}$, and applications to the arithmetical characterization of class groups. Electron. J. Comb. **18**(1) (2011). Research Paper 33
77. W.A. Schmid, Some recent results and open problems on sets of lengths of Krull monoids with finite class group, in *Multiplicative Ideal Theory and Factorization Theory*, ed. by S.T. Chapman, M. Fontana, A. Geroldinger, B. Olberding (Springer, Berlin, 2016)
78. M. Sezer, Sharpening the generalized Noether bound in the invariant theory of finite groups. J. Algebra **254**, 252–263 (2002)
79. Q. Wang, Y. Qu, On the critical number of finite groups II. Ars Comb. **113**, 321–330 (2014)
80. Q. Wang, J.J. Zhuang, On the critical number of finite groups of order pq. Int. J. Number Theor. **8**, 1271–1279 (2012)
81. D.L. Wehlau, The Noether number in invariant theory. C. R. Math. Acad. Sci. Soc. R. Can. **28**(2), 39–62 (2006)
82. K. Cziszter, M. Domokos, I. Szöllősi, The Noether number and the Davenport constants of the groups of order less than 32, manuscript in preparation