ADDITIVE GROUP THEORY AND NON-UNIQUE FACTORIZATIONS

ALFRED GEROLDINGER

1. Introduction

This article is the extended and revised version of notes written for the Advanced Course in Combinatorics and Geometry: Additive Combinatorics. The course took place at the Centre de Recerca Matemàtica (CRM) at Barcelona in spring 2008. It gives a survey on the interaction between two, at first glance very disparate areas of mathematics: Non-Unique Factorization Theory (see [71, 70, 13, 88, 124]) and Additive Group Theory (see [103, 36, 104, 107, 23, 130, 51]). The main objective of factorization theory is a systematic treatment of phenomena related to the non-uniqueness of factorizations in monoids and integral domains. In the setting of Krull monoids (the main examples we have in mind are the multiplicative monoids of rings of integers of algebraic number fields) most problems can be translated into zero-sum problems over the class group. It will be a main aim of this course to highlight this relationship.

In Section 3 we introduce the basic concepts of factorization theory, point out that arithmetical questions in arbitrary Krull monoids can be translated into combinatorial questions on zero-sum sequences over the class group and formulate some main problems (Section 3.D). In Section 4 we study the Davenport constant, and using group algebras we derive its precise value for p-groups (Theorem 4.10). In Section 5 we discuss the structure of sets of lengths (see Theorems 5.3, 5.9, 5.10 and 5.11). The characterization problem (Section 5.C) is a central topic. We give a proof in the case of cyclic groups and elementary 2-groups (Corollary 7.28), and this proof requires most of the results from additive group theory discussed in the previous parts. Section 6 starts with addition theorems, and then the Erdős-Ginzburg-Ziv constant and some of its variants are studied. We outline the power of the inductive method and determine the Davenport and the Erdős-Ginzburg-Ziv constant for groups of rank at most two (Theorem 6.13). Section 7 deals with inverse zero-sum problems. The focus is on cyclic groups and on groups of rank two.

2. Notations

Our notation and terminology is consistent with [71]. We briefly gather some key notions. We denote by $\mathbb{N}$ the set of positive integers, and we put $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$. For real numbers $a, b \in \mathbb{R}$ we set $[a, b] = \{x \in \mathbb{Z} \mid a \le x \le b\}$, and we define $\sup \emptyset = \max \emptyset = \min \emptyset = 0$.

Let $A, B \subset \mathbb{Z}$ be finite nonempty subsets. Then $A + B = \{a + b \mid a \in A, b \in B\}$ is their *sumset*. We denote by $\Delta(A)$ the *set of* (*successive*) *distances* of A, that is if $A = \{a_1, \ldots, a_t\}$ with $t \in \mathbb{N}$ and $a_1 < \ldots < a_t$, then $\Delta(A) = \{a_{\nu+1} - a_\nu \mid \nu \in [1, t-1]\}$). Moreover, we set $\Delta(\emptyset) = \emptyset$. A subset $P \subset \mathbb{Z}$ is called an *arithmetical progression* with *difference* $d \in \mathbb{N}$ if P is finite nonempty and $\Delta(P) \subset \{d\}$. If $A \subset \mathbb{N}$, we call

$$\rho(A) = \frac{\max A}{\min A} \in \mathbb{Q}_{\ge 1}$$

the *elasticity* of A, and we set $\rho(\{0\}) = 1$.

2000 *Mathematics Subject Classification.* 11P70,11B50, 11B75, 13F05, 13A05, 20M14.

Key words and phrases. non-unique factorizations, Krull monoids, zero-sum problems.

By a *monoid* we always mean a commutative semigroup with identity which satisfies the cancellation law (that is, if a, b, c are elements of the monoid with $ab = ac$, then $b = c$ follows). If R is an integral domain and $R^\bullet = R \setminus \{0\}$ its multiplicative semigroup of non-zero elements, then $R^\bullet$ is a monoid.

Throughout this paper, let H be a multiplicative monoid and G an additive finite abelian group.

3. Basic concepts of non-unique factorizations

We denote by $H^\times$ the set of invertible elements of H, and we say that H is *reduced* if $H^\times = \{1\}$. Let $H_{\text{red}} = H/H^\times = \{aH^\times \mid a \in H\}$ be the associated reduced monoid, and $\mathsf q(H)$ a quotient group of H.

Let $a, b \in H$. We say that *a divides b* (and we write $a \,|\, b$) if there is an element $c \in H$ such that $b = ac$. We say that a and b are *associated* (and we write $a \simeq b$) if $a \,|\, b$ and $b \,|\, a$ (equivalently, $aH^\times = bH^\times$).

A monoid F is called *free* (*abelian, with basis $P \subset F$*) if every $a \in F$ has a unique representation in the form

$$a = \prod_{p \in P} p^{\mathsf v_p(a)} \quad \text{with} \quad \mathsf v_p(a) \in \mathbb N_0 \ \text{ and } \ \mathsf v_p(a) = 0 \ \text{ for almost all } \ p \in P\,.$$

In this case, F is (up to canonical isomorphism) uniquely determined by P, and conversely P is uniquely determined by F.

We set $F = \mathcal F(P)$ and call

$$|a|_F = |a| = \sum_{p \in P} \mathsf v_p(a) \quad \text{the } \textit{length} \text{ of } a\,.$$

An element $a \in H$ is called

- an *atom* (or an irreducible element) if $a \notin H^\times$ and, for all $b,\, c \in H$, $a = bc$ implies $b \in H^\times$ or $c \in H^\times$. We denote by $\mathcal A(H)$ the set of all atoms of H.
- a *prime* (or a prime element) if $a \notin H^\times$ and, for all $b,\, c \in H$, $a \,|\, bc$ implies $a \,|\, b$ or $a \,|\, c$.

The monoid H is called

- *atomic* if every $a \in H \setminus H^\times$ is a product of atoms.
- *factorial* if it satisfies one of the following equivalent conditions:
  (a) Every $a \in H \setminus H^\times$ is a product of primes.
  (b) H is atomic, and every atom is a prime.
  (c) Every $a \in H \setminus H^\times$ is a product of atoms, and this factorization is unique up to associates and the order of the factors.
  (d) H_{red} is free (in that case H_{red} is free with basis $\{pH^\times \mid p \in P\}$ where P denotes the set of primes of H).
  (e) $H = H^\times \times \mathcal F(P)$ for some subset $P \subset H$ (in that case P is a maximal set of pairwise non-associated primes of H).

Every prime is an atom, and every factorial monoid is atomic. An element $a \in H$ is an atom [a prime] of H if and only if $aH^\times$ is an atom [a prime] of H_{red}. Thus H_{red} is atomic [factorial] if and only if H has this property.

By a *factorization* z of an element $a \in H$ we mean an equation of the form

$$z : a = u_1 \cdot \ldots \cdot u_l \text{ with } l \in \mathbb N_0 \text{ and } u_1, \ldots, u_l \text{ are atoms}\,.$$

The number of atoms l is called the length of the factorization, and two factorizations which differ only in the order of their factors and up to associates are considered as being equal. This concept can be formalized as follows.

The free monoid $\mathsf Z(H) = \mathcal F\big(\mathcal A(H_{\text{red}})\big)$, whose basis is the set of atoms in H_{red}, is called the *factorization monoid* of H. The homomorphism

$$\pi_H = \pi\colon \mathsf Z(H) \to H_{\text{red}}, \quad \text{defined by} \quad \pi(z) = \prod_{u \in \mathcal A(H_{\text{red}})} u^{\mathsf v_u(z)},$$

is called the *factorization homomorphism* of H. For $a \in H$, we set

$$\mathsf Z_H(a) = \mathsf Z(a) = \pi^{-1}(aH^\times) \subset \mathsf Z(H),$$

and we call the elements $z \in \mathsf Z(a)$ the *factorizations* of a. We say that a has *unique factorization* if $|\mathsf Z(a)| = 1$. For a factorization $z \in \mathsf Z(a)$, we call $|z|$ the *length* of z (clearly, this coincides with the above informal definition), and the set

$$\mathsf L_H(a) = \mathsf L(a) = \big\{|z| \ \big| \ z \in \mathsf Z(a)\big\} \subset \mathbb N_0$$

is called the *set of lengths* of a.

Note that $0 \in \mathsf L(a)$ if and only if $a \in H^\times$ and then $\mathsf L(a) = \{0\}$. We have $1 \in \mathsf L(a)$ if and only if a is an atom and then $\mathsf L(a) = \{1\}$. The monoid H is atomic if and only if $\mathsf Z(a) \ne \emptyset$ for all $a \in H$, and it is factorial if and only if $|\mathsf Z(a)| = 1$ for all $a \in H$. For every $b \in H$ we have

$$\mathsf Z(a)\mathsf Z(b) \subset \mathsf Z(ab) \quad \text{and} \quad \mathsf L(a) + \mathsf L(b) \subset \mathsf L(ab).$$

Furthermore, the monoid H is called

- *half-factorial* if $|\mathsf L(a)| = 1$ for all $a \in H$.
- an FF-*monoid* (a finite factorization monoid) if $\mathsf Z(a)$ is finite and nonempty for all $a \in H$.
- a BF-*monoid* (a bounded factorization monoid) if $\mathsf L(a)$ is finite and nonempty for all $a \in H$.

Half-factorial monoids and domains have received a lot of attention in the literature (see [14], [20], [123] for recent surveys). Here is a first, very simple but important observation.

Lemma 3.1. *Let H be atomic but not half-factorial. Then for every $N \in \mathbb N$ there exists some $a \in H$ such that $|\mathsf L(a)| \ge N+1$.*

Proof. If $a = u_1 \cdot \ldots \cdot u_k = v_1 \cdot \ldots \cdot v_l$ with $k < l$ and $u_1, \ldots, u_k, v_1, \ldots, v_l \in \mathcal A(H)$, then

$$c = a^N = (u_1 \cdot \ldots \cdot u_k)^\nu (v_1 \cdot \ldots \cdot v_l)^{N-\nu} \quad \text{for all} \quad \nu \in [0, N]$$

whence $\{\nu k + l(N-\nu) \mid \nu \in [0,N]\} \subset \mathsf L(c)$. □

3.A Arithmetical invariants

Most monoids studied so far in factorization theory are BF-monoids. In particular the multiplicative monoids of noetherian domains are BF-monoids ([71, Theorem 2.2.9]). We call

$$\mathcal L(H) = \{\mathsf L(a) \mid a \in H\}$$

the *system of sets of lengths* of H. If H is a BF-monoid, then $\mathcal L(H)$ is a set of finite nonempty subsets of the non-negative integers, and apart from the trivial case of half-factoriality, for every $N \in \mathbb N$ there is an $L \in \mathcal L(H)$ such that $|L| > N$. In order to describe the structure of sets of lengths we introduce the following arithmetical invariants.

Definition 3.2. Let H be a BF-monoid.

1. For $a \in H$, we call $\rho(a) = \rho\big(\mathsf L(a)\big)$ the *elasticity* of a and

$$\rho(H) = \sup\{\rho(a) \mid a \in H\} = \sup\{\rho(L) \mid L \in \mathcal L(H)\} \in \mathbb R_{\ge 1} \cup \{\infty\}$$

the *elasticity* of H.

2. Let $k \in \mathbb{N}$. If $H = H^\times$, we set $\rho_k(H) = \lambda_k(H) = k$, and if $H \ne H^\times$, then we define
$$\rho_k(H) = \sup\{\max L \mid L \in \mathcal{L}(H),\ k \in L\} \in \mathbb{N} \cup \{\infty\} \quad \text{and}$$
$$\lambda_k(H) = \min\{\min L \mid L \in \mathcal{L}(H),\ k \in L\} \in [1, k]\,.$$

3. We call
$$\Delta(H) = \bigcup_{L \in \mathcal{L}(H)} \Delta(L) \ \subset \ \mathbb{N}$$
the *set of distances* of H .

Clearly, H is half-factorial if and only if $\Delta(H) = \emptyset$ if and only if $\rho_k(H) = k$ for all $k \in \mathbb{N}$. Furthermore, $|\Delta(H)| = 1$ if and only if all sets of lengths are arithmetical progressions with the same difference. Whereas the elasticity may be infinite in non-principal orders of algebraic number fields ([71, Corollary 3.7.2]), we shall prove that it is finite in all Krull monoids with finite class group (thus in particular in all principal orders; see Theorems 3.17 and 4.11).

Lemma 3.3. *If H is a* BF*-monoid and $\Delta(H)$ is nonempty, then* $\min \Delta(H) = \gcd \Delta(H)$.

Proof. We set $d = \gcd \Delta(H)$. Clearly, it suffices to show that $d \in \Delta(H)$. There are $t \in \mathbb{N}, d_1, \ldots, d_t \in \Delta(H)$ and $m_1, \ldots, m_t \in \mathbb{Z} \setminus \{0\}$ such that $d = m_1 d_1 + \ldots + m_t d_t$. After renumbering if necessary there is some $s \in [1, t]$ such that $m_1, \ldots, m_s, -m_{s+1}, \ldots, -m_t$ are positive. For every $i \in [1, t]$, there are $x_i \in \mathbb{N}$ and $a_i \in H$ such that
$$\{x_i, x_i + d_i\} \subset \mathsf{L}(a_i) \quad \text{for every} \quad i \in [1, s]$$
and
$$\{x_i - d_i, x_i\} \subset \mathsf{L}(a_i) \quad \text{for every} \quad i \in [s+1, t]\,.$$
Then we get
$$\begin{aligned} \Big\{k = \sum_{i=1}^{s} m_i x_i - \sum_{i=s+1}^{t} m_i x_i,\ l = \sum_{i=1}^{s} m_i(x_i + d_i) - \sum_{i=s+1}^{t} m_i(x_i - d_i)\Big\} \\ \subset \sum_{i=1}^{s} \{m_i x_i,\ m_i(x_i + d_i)\} - \sum_{i=s+1}^{t} \{m_i(x_i - d_i),\ m_i x_i\} \\ \subset \mathsf{L}\big(a_1^{|m_1|} \cdot \ldots \cdot a_t^{|m_t|}\big) = L\,. \end{aligned}$$
Since $d \le \min \Delta(H)$, it follows that $d = l - k$ is a successive distance of L and hence $d \in \Delta(L) \subset \Delta(H)$. $\square$

The structure of sets of lengths will be studied in detail in Section 5. We continue with concepts which consider factorizations in a more direct way and not only their lengths.

Definition 3.4. Let H be atomic and $z,\, z' \in \mathsf{Z}(H)$, say
$$z = u_1 \cdot \ldots \cdot u_l v_1 \cdot \ldots \cdot v_m \quad \text{and} \quad z' = u_1 \cdot \ldots \cdot u_l w_1 \cdot \ldots \cdot w_n\,,$$
where $l,\, m,\, n \in \mathbb{N}_0,\ u_1, \ldots, u_l,\ v_1, \ldots, v_m,\ w_1, \ldots, w_n \in \mathcal{A}(H_{\text{red}})$ and
$$\{v_1, \ldots, v_m\} \cap \{w_1, \ldots, w_n\} = \emptyset\,.$$
Then we call $\mathsf{d}(z, z') = \max\{m,\, n\} \in \mathbb{N}_0$ the *distance* between z and z'.

The distance function $\mathsf{d}\colon \mathsf{Z}(H) \times \mathsf{Z}(H) \to \mathbb{N}_0$ is a metric. The following observation is analogue to Lemma 3.1.

Lemma 3.5. *Let H be atomic but not factorial. Then for every $N \in \mathbb{N}$ there exists some $a \in H$ such that $|\mathsf{Z}(a)| \ge N + 1$, and there exist factorizations $z,\, z' \in \mathsf{Z}(a)$ such that $\mathsf{d}(z, z') \ge 2N$.*

This phenomenon motivates the following definition.

Definition 3.6. Let H be atomic.

1. We define the *catenary degree* $\mathsf c(a)$ for $a \in H$ to be the smallest $N \in \mathbb N_0 \cup \{\infty\}$ such that, for any two factorizations z, z' of a, there exists a finite sequence $z = z_0, z_1, \ldots, z_k = z'$ of factorizations of a satisfying that $\mathsf d(z_{i-1}, z_i) \le N$ for all $i \in [1,k]$.
2. Globally, we define
$$\mathsf c(H) = \sup\{\mathsf c(a) \mid a \in H\} \in \mathbb N_0 \cup \{\infty\}\,,$$
and we call $\mathsf c(H)$ the *catenary degree* of H.

The next lemma gathers some elementary properties. In particular, Lemma 3.7.1 shows that H is factorial if and only if the catenary degree $\mathsf c(H) = 0$.

Lemma 3.7. *Let H be atomic and $a \in H$.*

1. $\mathsf c(a) \le \sup \mathsf L(a)$*, and* $\mathsf c(a) = 0$ *if and only if* $|\mathsf Z(a)| = 1$.
2. *If* $z, z' \in \mathsf Z(a)$ *and* $z \ne z'$*, then* $2 + \big||z| - |z'|\big| \le \mathsf d(z,z')$.
3. *If* $|\mathsf Z(a)| \ge 2$*, then* $2 + \sup \Delta\big(\mathsf L(a)\big) \le \mathsf c(a)$*. In particular,* $2 + \sup\Delta(H) \le \mathsf c(H)$.
4. *If* $\mathsf c(a) \le 2$*, then* $|\mathsf L(a)| = 1$*, and if* $\mathsf c(a) \le 3$*, then* $\mathsf L(a)$ *is an arithmetical progression with difference* 1.

Proof. 1. If $z, z' \in \mathsf Z(a)$, then $\mathsf d(z,z') \le \max\{|z|, |z'|\} \le \sup \mathsf L(a)$. Hence $\mathsf c(a) \le \sup \mathsf L(a)$. The second assertion follows by the very definition of $\mathsf c(a)$.

2. Let $z, z' \in \mathsf Z(a)$ be distinct, $x = \gcd(z,z')$ and $z = xy$, $z' = xy'$, where $y, y' \in \mathsf Z(H)$. Then $|y| \ge 2$, $|y'| \ge 2$ and $\mathsf d(z,z') = \max\{|y|, |y'|\}$. Thus it follows that $2 + \big||z| - |z'|\big| = 2 + \big||y| - |y'|\big| \le \max\{|y|, |y'|\} = \mathsf d(z,z')$.

3. We may assume that $\Delta\big(\mathsf L(a)\big) \ne \emptyset$, and we must prove that $2 + s \le \mathsf c(a)$ for every $s \in \Delta\big(\mathsf L(a)\big)$. If $s \in \Delta\big(\mathsf L(a)\big)$, then there exist factorizations $z, z' \in \mathsf Z(a)$ such that $|z'| = |z| + s$, and there is no factorization $z'' \in \mathsf Z(a)$ with $|z| < |z''| < |z'|$. By definition of $\mathsf c(a)$, there exist factorizations $z = z_0, z_1 \ldots, z_k = z' \in \mathsf Z(a)$ such that $\mathsf d(z_{i-1}, z_i) \le \mathsf c(a)$ for all $i \in [1,k]$. Thus there exists some $i \in [1,k]$ such that $|z_{i-1}| \le |z|$ and $|z_i| \ge |z'|$. Hence $2 + s \le 2 + |z_i| - |z_{i-1}| \le \mathsf d(z_{i-1}, z_i) \le \mathsf c(a)$.

4. Obvious by 3. □

Next we consider local tameness. We start with the formal definition, and then we discuss the meaning of this concept in some detail.

Definition 3.8. Suppose that H is atomic.

1. For $a, b \in H$ let $\omega(a,b)$ denote the smallest $N \in \mathbb N_0 \cup \{\infty\}$ with the following property:
   For all $n \in \mathbb N$ and $a_1, \ldots, a_n \in H$, if $a = a_1 \cdot \ldots \cdot a_n$ and $b \,|\, a$, then there exists a subset $\Omega \subset [1,n]$ such that $|\Omega| \le N$ and
$$b \,\Big|\, \prod_{\nu \in \Omega} a_\nu\,.$$
   In particular, if $b \nmid a$, then $\omega(a,b) = 0$. For $b \in H$ we define
$$\omega(H,b) = \sup\big\{\omega(a,b) \,\big|\, a \in H\big\} \in \mathbb N_0 \cup \{\infty\}\,.$$
2. For $a \in H$ and $x \in \mathsf Z(H)$ let $\mathsf t(a,x) \in \mathbb N_0 \cup \{\infty\}$ denote the smallest $N \in \mathbb N_0 \cup \{\infty\}$ with the following property:
   If $\mathsf Z(a) \cap x\mathsf Z(H) \ne \emptyset$ and $z \in \mathsf Z(a)$, then there exists $z' \in \mathsf Z(a) \cap x\mathsf Z(H)$ such that $\mathsf d(z,z') \le N$.

For subsets $H' \subset H$ and $X \subset \mathsf Z(H)$, we define

$$\mathsf t(H', X) = \sup \bigl\{ \mathsf t(a, x) \bigm| a \in H', x \in X \bigr\} \in \mathbb N_0 \cup \{\infty\}\,.$$

H is called *locally tame* if $\mathsf t(H, u) < \infty$ for all $u \in \mathcal A(H_{\text{red}})$.

Local tameness is a basic finiteness property in the theory of non-unique factorizations, in the sense that in many situations where the finiteness of an arithmetical invariant such as the catenary degree or the set of distances is studied, local tameness has to be proved first (see also the sketch of the proof of Theorem 5.9). The closely related $\omega(H, \cdot)$-invariants, introduced in [68], are further well-established invariants in the theory of non-unique factorizations, which appear also in the context of direct-sum decompositions of modules [26, Remark 1.6].

For simplicity of notation suppose that H is atomic and reduced, and let $u \in \mathcal A(H)$. Then u is a prime if and only if $\omega(H, u) = 1$. Thus $\omega(H, u)$ measures how far away is u from being a prime. Let $a \in H$. If $u \nmid a$, then $\mathsf t(a, u) = 0$ by definition. Suppose that $u \,|\, a$. Then $\mathsf t(a, u)$ is the smallest $N \in \mathbb N_0 \cup \{\infty\}$ with the following property: if $z = a_1 \cdot \ldots \cdot a_n$ is any factorization of a where $a_1, \ldots, a_n$ are atoms, then there exist a subset $\Omega \subset [1, n]$, say $\Omega = [1, k]$, and a factorization $z' = u u_2 \cdot \ldots u_l a_{k+1} \cdot \ldots \cdot a_n \in \mathsf Z(a)$, with atoms $u_2, \ldots, u_l$, such that $\max\{k, l\} \le N$. Thus $\mathsf t(a, u)$ measures how far away from any given factorization z of a there is a factorization z' of a which contains u, and if u is not a prime then $\omega(H, u) \le \mathsf t(H, u)$. Suppose that u is a prime. Then every factorization of a contains u, we can choose $z' = z$ in the above definition, obtain that $\mathsf d(z, z') = \mathsf d(z, z) = 0$ and hence $\mathsf t(H, u) = 0$. Whereas in monoids, which satisfy the ascending chain condition for v-ideals, we have $\omega(H, u) < \infty$ for all atoms $u \in \mathcal A(H)$, this does not hold for the $\mathsf t(H, u)$ values (see [74, Theorems 3.6 and 4.4]).

3.B Krull monoids

Krull monoids play a central role in factorization theory. We briefly summarize some of their main properties without giving any proofs. Then we discuss two main examples of Krull monoids: those stemming from domains and the monoid of zero-sum sequences over an abelian group. For more on the theory of Krull monoids we refer to the monographs [87, 79, 71]. A detailed discussion of further examples may be found in [71, Examples 2.3.2 and 7.4.2].

Definition 3.9. (Krull monoids and class groups)

1. Let D be a monoid and $H \subset D$ a submonoid with $\mathsf q(H) \subset \mathsf q(D)$.
   (a) Then $H \subset D$ is called *saturated* if $\mathsf q(H) \cap D = H$ (that is, if $a, b \in H$ and a divides b in D, then a divides b in H).
   (b) For $a \in \mathsf q(D)$ we denote by $[a] = [a]_{D/H} = a\,\mathsf q(H) \in \mathsf q(D)/\mathsf q(H)$ the class containing a. We call $D/H = \{[a] \mid a \in D\} \subset \mathsf q(D)/\mathsf q(H)$ the *class group* of D modulo H.
2. H is called a *Krull monoid* if H_{red} is a saturated submonoid of a free monoid.
3. Let H be a Krull monoid and suppose that $H_{\text{red}} \subset D = \mathcal F(P)$ is a saturated submonoid of a free monoid such that every $p \in P$ is the greatest common divisor of finitely many elements of H_{red}. Then we call D a monoid of *divisors* and P a set of *prime divisors* of H (for short, we refer to them as primes).

Let $H \subset D$ be as above. If $\mathsf q(D)/\mathsf q(H)$ is finite (this condition is fulfilled throughout the present article), then $D/H = \mathsf q(D)/\mathsf q(H)$. Class groups will be written additively whence $[1]$ is the zero element of D/H. Moreover, $H \subset D$ is saturated if and only if

$$H = \{a \in D \mid [a] = [1]\}\,.$$

Every Krull monoid possesses a monoid of divisors, and if D and D' are monoids of divisors of H, then there is a unique isomorphism $\Phi\colon D \to D'$ with $\Phi \mid H_{\text{red}} = \text{id}$. Hence the class group

$$\mathcal{C}(H) = D/H_{\text{red}} \quad \text{and the subset} \quad \{[p] \in \mathcal{C}(H) \mid p \in P\}$$

of all classes containing primes are uniquely determined by H (up to canonical isomorphism) and hence $\mathcal{C}(H)$ will be called the *class group* of the Krull monoid H.

Now we consider domains and outline when the multiplicative monoid of a domain is a Krull monoid (more details and proofs can be found in [71, Section 2.10]). Let R be a domain,

$$\mathcal{H}(R) = \{aR \mid a \in R^\bullet\}$$

the monoid of non-zero principal ideals and

$$\mathcal{I}^*(R) = \{I \lhd R \mid I \text{ is invertible}\}$$

the monoid of invertible ideals (recall, that a non-zero ideal I of R is invertible if there is a non-zero ideal J of R such that their product IJ is a principal ideal). Then $(R^\bullet)_{\text{red}} \cong \mathcal{H}(R)$, the prime elements of the monoid $\mathcal{I}^*(R)$ are precisely the non-zero prime ideals of R, and $\mathcal{H}(R) \subset \mathcal{I}^*(R)$ is saturated.

Theorem 3.10. *Let R be an integral domain.*

1. *The following statements are equivalent*:
   - (a) *$R^\bullet$ is a Krull monoid.*
   - (b) *R is completely integrally closed and satisfies the ascending chain condition for v-ideals* (*also called divisorial ideals*).
   - (c) *R satisfies the ascending chain condition for v-ideals and $R_{\mathfrak{m}}$ is a discrete valuation domain for all v-maximal v-ideals of R.*
2. *The following statements are equivalent*:
   - (a) *R is integrally closed, noetherian and every non-zero prime ideal of R is maximal.*
   - (b) *R is a one-dimensional Krull domain.*
   - (c) *Every non-zero ideal is a product of prime ideals.*

A domain R is called a *Krull domain* if it satisfies the equivalent conditions of Theorem 3.10.1. In particular, every integrally closed noetherian domain is a Krull domain.

A domain R is called a *Dedekind domain* if it satisfies the equivalent conditions of Theorem 3.10.2. Suppose R is a Dedekind domain. Then $\mathcal{I}^*(R)$ is a monoid of divisors of $\mathcal{H}(R)$, the set of non-zero prime ideals is a set of prime divisors of $\mathcal{H}(R)$, and the class group of $\mathcal{H}(R) \subset \mathcal{I}^*(R)$ is the usual ideal class group of R. If K is an algebraic number field and $\mathfrak{o}_K$ the ring of integers of K, then $\mathfrak{o}_K$ is a Dedekind domain with finite class group and every class contains infinitely many primes.

Next we discuss the monoid of zero-sum sequences over an abelian group, which will turn out to be a Krull monoid. It connects the theory of non-unique factorizations with additive group theory and combinatorial number theory.

Definition 3.11. Let $G_0 \subset G$ be a subset.

1. Let $\mathcal{F}(G_0)$ be the free (multiplicative) monoid with basis G_0. The elements of $\mathcal{F}(G_0)$ are called *sequences* over G_0. We write sequences $S \in \mathcal{F}(G_0)$ in the form

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

   where $\mathsf{v}_g(S) \in \mathbb{N}_0$.

2. If S is as above, then

$$\sigma(S) = \sum_{i=1}^{l} g_i = \sum_{g \in G} \mathsf{v}_g(S) g \in G \qquad \text{is called the } \textit{sum} \text{ of } S,$$

and we denote by $\mathcal{B}(G_0) = \{S \in \mathcal{F}(G_0) \mid \sigma(S) = 0\}$ the *monoid of zero-sum sequences* (*block monoid*) over G_0. The elements of $\mathcal{B}(G_0)$ are called *zero-sum sequences*, and the atoms of $\mathcal{B}(G_0)$ are called *minimal zero-sum sequences*.

For every arithmetical invariant $*(H)$ defined for the monoid H, we write $*(G_0)$ instead of $*\big(\mathcal{B}(G_0)\big)$ whenever the precise meaning is clear from the context. For example, we set $\mathcal{A}(G_0) = \mathcal{A}\big(\mathcal{B}(G_0)\big)$, $\mathcal{L}(G_0) = \mathcal{L}\big(\mathcal{B}(G_0)\big)$, $\Delta(G_0) = \Delta\big(\mathcal{B}(G_0)\big)$ and so on.

Proposition 3.12. *Let* $G_0 \subset G$ *be a nonempty subset.*

1. $\mathcal{B}(G_0) \subset \mathcal{F}(G_0)$ *is saturated and thus* $\mathcal{B}(G_0)$ *is a Krull monoid.*
2. $\mathcal{A}(G_0)$ *is finite and thus* $\mathcal{B}(G_0)$ *is finitely generated.*
3. *If* $|G| \ne 2$*, then* $\mathcal{F}(G)$ *is a monoid of divisors for* $\mathcal{B}(G)$, $\mathcal{C}\big(\mathcal{B}(G)\big) \cong G$*, and every class of* $\mathcal{B}(G)$ *contains exactly one prime.*
4. *The following statements are equivalent*:
   (a) $|G| \le 2$.
   (b) $\mathcal{B}(G)$ *is factorial.*
   (c) $\mathcal{B}(G)$ *is half-factorial.*

Proof. 1. This follows immediately from the definitions.

2. Every atom of $\mathcal{B}(G_0)$ divides the zero-sum sequence

$$B = \prod_{g \in G_0} g^{\operatorname{ord}(g)}$$

and hence there are only finitely many atoms.

3. Let $|G| \ne 2$. To verify that $\mathcal{F}(G)$ is a monoid of divisors for $\mathcal{B}(G)$, let $g \in G$ be given. If $\operatorname{ord}(g) = n \ge 3$, then $g = \gcd\big(g^n, g(-g)\big)$. If $\operatorname{ord}(g) = 2$, then there is an element $h \in G \setminus \{0, g\}$ and $g = \gcd\big(g^2, gh(g-h)\big)$.

The map $\sigma \colon \mathcal{F}(G) \to G$ is a monoid epimorphism. If $S, S' \in \mathcal{F}(G)$, then $\sigma(S) = \sigma(S')$ if and only if $S' \in [S] = S\mathsf{q}\big(\mathcal{B}(G)\big)$. Thus σ induces a group isomorphism $\Phi \colon \mathcal{F}(G)/\mathcal{B}(G) \to G$, defined by $\Phi([S]) = \sigma(S)$, and we have $[S] \cap G = \{g\}$. Thus the class $[S]$ contains exactly one prime.

4. (a) $\Rightarrow$ (b) If $G = \{0\}$, then $\mathcal{B}(G) = \mathcal{F}(G) \cong (\mathbb{N}_0, +)$ is factorial. Suppose that $G = \{0, e\}$. Then $\mathcal{A}(G) = \{0, e^2\}$, every atom is a prime and hence $\mathcal{B}(G)$ is factorial (indeed, $\mathcal{B}(G) \cong (\mathbb{N}_0^2, +)$).

(b) $\Rightarrow$ (c) Obvious.

(c) $\Rightarrow$ (a) Suppose there is some $g \in G$ with $\operatorname{ord}(g) = n \ge 3$. Then $U = g^n$, $-U = (-g)^n$, $V = (-g)g$ are atoms of $\mathcal{B}(G)$ and $(-U)U = V^n$, a contradiction to half-factoriality. Thus $\operatorname{ord}(g) \le 2$ for all $g \in G$. Assume to the contrary, that there are two distinct non-zero elements $e_1, e_2 \in G$ and set $e_0 = e_1 + e_2$. Then $U = e_0 e_1 e_2$ and $V_i = e_i^2$ are atoms of $\mathcal{B}(G)$ for $i \in [0, 2]$. But $U^2 = V_0 V_1 V_2$ is again a contradiction to half-factoriality. Thus G has no elements of order greater than or equal to 3, and at most one element of order 2 which implies $|G| \le 2$. □

3.C Transfer principles

A central method in factorization theory is to study the arithmetic in auxiliary monoids and to shift the results to monoids and domains of arithmetical interest. We start with the crucial definition.

Definition 3.13. 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 $u = vw$, $\theta(v) \simeq b$ and $\theta(w) \simeq c$.

Thus the strategy is to find, for a given monoid H, a simpler monoid B, to study the arithmetic in B, and then to shift the arithmetical results from B back to H. The next proposition shows that a shift back is possible.

Proposition 3.14. *Let $\theta\colon H \to B$ be a transfer homomorphism of atomic monoids and $u \in H$.*

1. *If $n \in \mathbb{N}$, $b_1, \ldots, b_n \in B$ and $\theta(u) \simeq b_1 \cdot \ldots \cdot b_n$, then there exist $u_1, \ldots, u_n \in H$ such that $u \simeq u_1 \cdot \ldots \cdot u_n$ and $\theta(u_\nu) \simeq b_\nu$ for all $\nu \in [1, n]$.*
2. *u is an atom of H if and only if $\theta(u)$ is an atom of B.*
3. *$\mathsf{L}_H(u) = \mathsf{L}_B\big(\theta(u)\big)$.*
4. *$\mathcal{L}(H) = \mathcal{L}(B)$. In particular, H is a* BF*-monoid if and only if B is a* BF*-monoid, and then we have $\rho(H) = \rho(B)$ and $\Delta(H) = \Delta(B)$.*

Proof. We suppose that H and B are reduced.

1. This follows by induction on n.

2. If $u \in \mathcal{A}(H)$ and $\theta(u) = bc$ for some $b, c \in B$, then there exist $v, w \in H$ such that $u = vw$, $\theta(v) = b$ and $\theta(w) = c$. Hence $v = 1$ or $w = 1$ and thus $b = 1$ or $c = 1$. If $\theta(u) \in \mathcal{A}(B)$ and $u = vw$ for some $v, w \in H$, then $\theta(u) = \theta(v)\theta(w)$ implies $\theta(v) = 1$ or $\theta(w) = 1$ and thus $v = 1$ or $w = 1$.

3. By **(T 1)** , we have $u = 1$ if and only if $\theta(u) = 1$, and by definition we have $\mathsf{L}_H(1) = \{0\} = \mathsf{L}_B\big(\theta(u)\big)$. Suppose that $u \ne 1$. If $k \in \mathsf{L}_H(u)$, then there are atoms $u_1, \ldots, u_k$ of H such that $u = u_1 \cdot \ldots \cdot u_k$. Then $\theta(u) = \theta(u_1) \cdot \ldots \cdot \theta(u_k)$. By 2., $\theta(u_1), \ldots, \theta(u_k)$ are atoms of B, and hence $k \in \mathsf{L}_B\big(\theta(u)\big)$. Conversely, we pick $k \in \mathsf{L}_B\big(\theta(u)\big)$. Then there are atoms $b_1, \ldots, b_k$ of B such that $\theta(u) = b_1 \cdot \ldots \cdot b_k$. By 1., there are $u_1, \ldots, u_k \in H$ such that $u = u_1 \cdot \ldots \cdot u_k$ and $\theta(u_\nu) = b_\nu$ for all $\nu \in [1, k]$. Thus by 2., $u_1, \ldots, u_k$ are atoms of H and hence $k \in \mathsf{L}_H(u)$.

4. This follows immediately from 3. □

We introduce the Davenport constant which will be investigated in detail in Section 4. Recall that $\mathcal{A}(G_0)$ is finite by Proposition 3.12.

Definition 3.15. Let $G_0 \subset G$ be a nonempty subset. Then

$$\mathsf{D}(G_0) = \max\big\{|U| \bigm| U \in \mathcal{A}(G_0)\big\} \in \mathbb{N}_0$$

is called the *Davenport constant* of G_0.

The next result gives the required link between factorization theory on the one side and additive group theory and combinatorial number theory on the other side.

Theorem 3.16. *Let H be a reduced Krull monoid with finite class group, $H \subset D = \mathcal{F}(P)$ a monoid of divisors and $G_0 = \{[p] \mid p \in P\} \subset G = D/H$ the set of classes containing primes. Let $\widetilde{\boldsymbol{\beta}}\colon D \to \mathcal{F}(G_0)$ be the unique homomorphism satisfying $\widetilde{\boldsymbol{\beta}}(p) = [p]$ for all $p \in P$.*

1. *For $a \in D$ we have $\widetilde{\boldsymbol{\beta}}(a) \in \mathcal{B}(G_0)$ if and only if $a \in H$. Thus $\widetilde{\boldsymbol{\beta}}(H) = \mathcal{B}(G_0)$ and $\widetilde{\boldsymbol{\beta}}^{-1}\big(\mathcal{B}(G_0)\big) = H$.*

2. *The restriction* $\beta = \widetilde{\beta}|H \colon H \to \mathcal{B}(G_0)$ *is a transfer homomorphism. In particular, we have* $\mathcal{L}(H) = \mathcal{L}(G_0)$.
3. $\mathsf{D}(G_0)$ *is the maximum of all* $l \in \mathbb{N}_0$ *with the following property: There exists an atom* $u \in H$ *such that* u *is the product of* l *primes of* D.
4. *We have* $\mathsf{c}(G_0) \le \mathsf{c}(H) \le \max\{\mathsf{c}(G_0), 2\}$.

Proof. 1. Let $a = p_1 \cdot \ldots \cdot p_l \in D$ where $l \in \mathbb{N}$ and $p_1, \ldots, p_l \in P$. Then

$$\widetilde{\beta}(a) = [p_1] \cdot \ldots \cdot [p_l] \in \mathcal{F}(G_0) \quad \text{and} \quad \sigma\big([p_1] \cdot \ldots \cdot [p_l]\big) = [p_1] + \ldots + [p_l] = [a] \,.$$

Since $H \subset D$ is saturated, we have $[a] = 0 \in G$ if and only if $a \in H$, and thus all assertions follow.

2. By 1., $\beta \colon H \to \mathcal{B}(G_0)$ is surjective and $\beta^{-1}(1) = \{1\}$. Let $a = p_1 \cdot \ldots \cdot p_l \in H$, with $l \in \mathbb{N}$ and $p_1, \ldots, p_l \in P$, and suppose that $\beta(a) = BC$, say $B = [p_1] \cdot \ldots \cdot [p_k]$ and $C = [p_{k+1}] \cdot \ldots \cdot [p_l]$. By 1., $b = p_1 \cdot \ldots \cdot p_k \in H$, $c = p_{k+1} \cdot \ldots \cdot p_l \in H$ and clearly we have $a = bc$. Therefore β is a transfer homomorphism, and thus Proposition 3.14 implies $\mathcal{L}(H) = \mathcal{L}(G_0)$.

3. Let $l \in \mathbb{N}_0$, $p_1, \ldots, p_l$ primes of D and $u = p_1 \cdot \ldots \cdot p_l$ be an atom of H. Since β is a transfer homomorphism, $\beta(u) = [p_1] \cdot \ldots \cdot [p_l] \in \mathcal{A}(G_0)$, and hence $\mathsf{D}(G_0) \ge |\beta(u)| = l$. Conversely, let $U = g_1 \cdot \ldots \cdot g_l \in \mathcal{A}(G_0)$ with $\mathsf{D}(G_0) = |U| = l$. If $p_i \in G_0$ with $g_i = [p_i]$ for $i \in [1, l]$, then $u = p_1 \cdot \ldots \cdot p_l$ is an atom of H which is a product of l primes of D.

4. The proof is not difficult but requires concepts not introduced here (see [71, Theorem 3.4.10]). □

The homomorphism $\beta \colon H \to \mathcal{B}(G_0)$ is called the *block homomorphism* of H. It transports arithmetical problems in H to zero-sum problems over G. In particular, if $a = p_1 \cdot \ldots \cdot p_l \in D$ is as above, then a is an atom of H if and only if $\beta(a)$ is a minimal zero-sum sequence.

The next result states that in a Krull monoid with finite class group all arithmetical invariants introduced so far are finite. The proof of finiteness is fairly simple. However, establishing the precise values of the invariants is a completely different task. It can be tackled with methods from additive group theory, and the remaining sections of this article will be devoted to that.

Theorem 3.17. *Let* H *be a Krull monoid with finite class group. Then* H *is a locally tame* FF*-monoid with finite catenary degree* $\mathsf{c}(H)$*, finite set of distances* $\Delta(H)$*, finite elasticity* $\rho(H)$ *and with* $\rho_k(H) < \infty$ *for all* $k \in \mathbb{N}$.

Proof. We may suppose that H is reduced. Let $D = \mathcal{F}(P)$ be a monoid of divisors of H, $G = D/H$ its class group and $G_0 \subset G$ the set of classes containing primes. We proceed in several steps.

H is an FF*-monoid.* If $a \in H$, then there are primes $p_1, \ldots, p_l \in P$ such that $a = p_1 \cdot \ldots \cdot p_l$, and this is the only factorization of a in D. Therefore every factorization $a = u_1 \cdot \ldots \cdot u_k$ of a into atoms of H corresponds uniquely to a partition

$$[1, l] = \bigcup_{\nu=1}^{k} I_\nu \,, \quad \text{where} \quad \sum_{j \in I_\nu} [p_j] = 0 \in G \quad \text{but} \quad \sum_{j \in I'_\nu} [p_j] \ne 0 \in G \,,$$

for all nonempty proper subsets $I'_\nu \subset I_\nu$ and all $\nu \in [1, k]$. Thus a has only finitely many factorizations in H.

H is locally tame. Let $u = p_1 \cdot \ldots \cdot p_l \in \mathcal{A}(H)$ with $l \in \mathbb{N}$ and $p_1, \ldots, p_l \in P$. We assert that

$$\mathsf{t}(H, u) \le 1 + \frac{l(\mathsf{D}(G_0) - 1)}{2} \le 1 + \frac{\mathsf{D}(G_0)(\mathsf{D}(G_0) - 1)}{2} \,.$$

The second inequality follows from Theorem 3.16.3 and provides a global bound for all local tame degrees $\mathsf{t}(H, v)$ with $v \in \mathcal{A}(H)$. So we have to verify the first inequality. If u is a prime in H, then $\mathsf{t}(H, u) = 0$ by definition. Suppose that u is not a prime in H, that is $u \notin P$. Then $\mathsf{D}(G_0) \ge l \ge 2$. We recall two notations. If $c \in D = \mathcal{F}(P)$, then $c = q_1 \cdot \ldots \cdot q_s$, where $s \in \mathbb{N}_0$ and $q_1, \ldots, q_s \in P$, and $|c|_D = s$. If $w \in \mathsf{Z}(H) = \mathcal{F}(\mathcal{A}(H))$, then $w = v_1 \cdot \ldots \cdot v_t$, where $t \in \mathbb{N}_0$ and $v_1, \ldots, v_t \in \mathcal{A}(H)$, and $|w| = t$.

Let $a \in H$, with $u \,|\, a$ and $z = u_1 \cdot \ldots \cdot u_r \in \mathsf{Z}(a)$, where $r \in \mathbb{N}$ and $u_1, \ldots, u_r \in \mathcal{A}(H)$. We must prove that there exists some $z' \in \mathsf{Z}(a) \cap u\mathsf{Z}(H)$ such that

$$\mathsf{d}(z, z') \le 1 + \frac{l(\mathsf{D}(G_0) - 1)}{2}\,.$$

After renumbering if necessary we may assume that there exists some $k \in [1, r]$ such that $k \le l$, $u \,|\, u_1 \cdot \ldots \cdot u_k$, but u does not divide any proper subproduct of $u_1 \cdot \ldots \cdot u_k$ (in D and hence in H). Since $u \notin P$, it follows that $u_1, \ldots, u_k \notin P$, and thus $u_1 \cdot \ldots \cdot u_k$ is not divisible by any $p \in P \cap H$. If $u_1 \cdot \ldots \cdot u_k = uc$, where $c \in H$, and if $w \in \mathsf{Z}(c)$, then $|c|_D \ge 2|w|$ and

$$|w| \le \frac{|c|_D}{2} = \frac{|u_1|_D + \ldots + |u_k|_D - |u|_D}{2} \le \frac{k\mathsf{D}(G_0) - l}{2} \le \frac{l(\mathsf{D}(G_0) - 1)}{2}\,.$$

Now it follows that $z' = uwu_{k+1} \cdot \ldots \cdot u_r \in \mathsf{Z}(a)$, and

$$\mathsf{d}(z, z') \le \max\{k, |w| + 1\} \le \max\{l, |w| + 1\} \le 1 + \frac{l\,(\mathsf{D}(G_0) - 1)}{2}\,.$$

On the remaining invariants. By Theorem 3.16, we have $\Delta(H) = \Delta(G_0)$, $\mathsf{c}(H) \le \max\{\mathsf{c}(G_0), 2\}$, $\rho(H) = \rho(G_0)$ and $\rho_k(H) = \rho_k(G_0)$ for all $k \in \mathbb{N}$, and hence it suffices to consider $\mathcal{B}(G_0)$. Clearly, we have $\Delta(G_0) \subset \Delta(G)$, $\mathsf{c}(G_0) \le \mathsf{c}(G)$, $\rho(G_0) \le \rho(G)$ and $\rho_k(G_0) \le \rho_k(G)$ for all $k \in \mathbb{N}$. For these latter invariants we shall derive explicit upper bounds and in some cases even precise values in Section 4.C. □

3.D Main problems in factorization theory

1. Which noetherian domains satisfy the main finiteness properties of factorization theory: local tameness, finiteness of the catenary degree and the Structure Theorem for Sets of Lengths? (see Definition 5.8 and the subsequent results).

The goal is to derive explicit characterizations in terms of ring invariants. A prototype of such a result may be found in [96, Theorem 6.1]. It provides an explicit ring theoretical characterization of those finitely generated domains having finite elasticity.

2. If R is a ring of integers of an algebraic number field, then almost all elements of R have catenary degree at most 3 (see Corollary 5.13).

Which other domains have such a property? Of course, "almost all" has to be interpreted in a suitable way: i.e., for orders in global fields in the sense of Dirichlet density and for $\mathbb{Q}$-algebras in the sense of Zariski density.

3. Let H be a Krull monoid with finite class group G such that every class contains a prime (the multiplicative monoid of non-zero elements of a ring of integers of an algebraic number field is such a Krull monoid).

Find the precise values of arithmetical invariants of H (such as of $\mathsf{c}(H)$, $\Delta(H)$ and $\rho_k(H)$ for $k \in \mathbb{N}$) in terms of the group invariants of G (see [71, Chapter 6], and note that by the simple Theorem 3.17 all the invariants are finite). Results of this type are substantial for making progress on the Characterization Problem described in **5.C**.

Let R be a noetherian domain. If R is integrally closed, then its multiplicative monoid $R^\bullet$ is a Krull monoid. Suppose that R is not integrally closed. If the integral closure $\overline{R}$ is a finitely generated R-module and some further natural finiteness conditions hold, then the arithmetic of R is studied via C-monoids and weakly C-monoids. These monoids play a similar role as the monoid of zero-sum sequences does for Krull monoids (see [71, Theorems 2.11.9 and 3.3.4] and [73]).

However, in the present article we restrict to Krull monoids and focus on Problem **3.** with respect to the invariants $\Delta(H)$, $\mathsf c(H)$ and $\rho_k(H)$ for all $k \in \mathbb N$.

4. The Davenport constant and first precise arithmetical results

In this section we study the Davenport constant, a classical combinatorial invariant which has been investigated since the 1960s (see [115], [105], [31], [108] and [103]). From the very beginning the investigation of this invariant was related also to arithmetical problems (it is reported in [108] that in 1966 H. Davenport asked for $\mathsf D(G)$, since it is the largest number of prime ideals occurring in the prime ideal decomposition of an irreducible integer in an algebraic number field with ideal class group G). However, it has turned out that this and related invariants occur in many branches of combinatorics, number theory and geometry (see [51] for a recent survey, and [99], [33] for the relationship to invariant theory).

We shall determine the precise value of the Davenport constant among others for p-groups and for groups of rank at most two (see Theorems 4.10 and 6.13 and Corollary 6.16). For general finite abelian groups the precise value is still unknown. After that we put the Davenport constant in connection to the arithmetical invariants introduced in Section 3.

4.A The Davenport constant

We set $G^\bullet = G \setminus \{0\}$. Let $G_0 \subset G$ be a subset and

$$S = \prod_{g \in G_0} g^{\mathsf v_g(S)} = g_1 \cdot \ldots \cdot g_l \in \mathcal F(G_0)$$

a sequence over G_0. We call $\mathsf v_g(S)$ the *multiplicity* of g in S, and we say that S *contains* g if $\mathsf v_g(S) > 0$. S is called *squarefree* (in $\mathcal F(G)$) if $\mathsf v_g(S) \le 1$ for all $g \in G$. A sequence S_1 is called a *subsequence* of S if $S_1 \,|\, S$ in $\mathcal F(G)$ (equivalently, $\mathsf v_g(S_1) \le \mathsf v_g(S)$ for all $g \in G$), and it is called a *proper subsequence* of S if it is a subsequence with $1 \ne S_1 \ne S$. We call

$$|S| = l = \sum_{g \in G_0} \mathsf v_g(S) \in \mathbb N_0 \qquad \text{the } \textit{length} \text{ of } S\,,$$

$$\mathsf h(S) = \max\{\mathsf v_g(S) \mid g \in G\} \in [0, |S|]$$

$$\text{the } \textit{maximum of the multiplicities} \text{ of } S\,,$$

$$\operatorname{supp}(S) = \{g \in G \mid \mathsf v_g(S) > 0\} \subset G \qquad \text{the } \textit{support} \text{ of } S\,,$$

$$\Sigma_k(S) = \Big\{ \sum_{i \in I} g_i \;\Big|\; I \subset [1,l] \text{ with } |I| = k \Big\} \text{ the } \textit{set of k-term subsums} \text{ of } S\,, \text{ for all } k \in \mathbb N\,,$$

$$\Sigma_{\le k}(S) = \bigcup_{j \in [1,k]} \Sigma_j(S)\,, \qquad \Sigma_{\ge k}(S) = \bigcup_{j \ge k} \Sigma_j(S)\,,$$

and

$$\Sigma(S) = \Sigma_{\ge 1}(S) \text{ the } \textit{set of (all) subsums} \text{ of } S\,.$$

We set $-S = (-g_1) \cdot \ldots \cdot (-g_l)$, and for every $g \in G$ we set $g + S = (g+g_1) \cdot \ldots \cdot (g+g_l)$.

A sequence S is called *zero-sum free* if $0 \notin \Sigma(S)$, and we denote by $\mathcal A^*(G_0)$ the set of all zero-sum free sequences. Since every zero-sum free sequence S is a subsequence of

$$\prod_{g \in G_0} g^{\operatorname{ord}(g)-1}\,,$$

$\mathcal A^*(G_0)$ is finite. For convenience we introduce the following technical variant of the Davenport constant $\mathsf D(G_0)$ (introduced in Definition 3.15), and in Lemma 4.2.3 we give a straightforward characterization.

Definition 4.1. Let $G_0 \subset G$ be a nonempty subset. Then

$$\mathsf{d}(G_0) = \max\bigl\{|S| \bigm| S \in \mathcal{F}(G_0) \text{ is zero-sum free } \bigr\} \in \mathbb{N}_0$$

is called the *little Davenport constant* of G_0.

Obviously, the map $\psi \colon \mathcal{A}^*(G_0) \to \mathcal{A}(G)$, defined by $S \mapsto (-\sigma(S))S$, is well-defined, and $\mathsf{D}(G_0) \le 1 + \mathsf{d}(G_0)$. If $G_0 = G$, then ψ is surjective and $\mathsf{D}(G) = 1 + \mathsf{d}(G)$. The following two lemmas gather some elementary properties of the Davenport constant.

Lemma 4.2.

1. *If* $S \in \mathcal{A}^*(G)$ *has length* $|S| = \mathsf{d}(G)$, *then* $\Sigma(S) = G^\bullet$ *and* $G = \langle \mathrm{supp}(S) \rangle$.
2. $\mathsf{d}(G) = \max\bigl\{|S| \bigm| S \in \mathcal{F}(G)\,,\ \Sigma(S) = G^\bullet\bigr\}$.
3. $\mathsf{D}(G)$ *is the smallest integer* $l \in \mathbb{N}$ *such that every sequence* $S \in \mathcal{F}(G)$ *of length* $|S| \ge l$ *has a nontrivial zero-sum subsequence* (*that is,* $S \notin \mathcal{A}^*(G)$).
4. *If* $S \in \mathcal{A}^*(G)$, *then* $|S| \le |\Sigma(S)| \le |G| - 1$. *In particular,* $\mathsf{d}(G) \le |G| - 1$ *and* $\mathsf{D}(G) \le |G|$.

Proof. 1. Let $S \in \mathcal{A}^*(G)$ with $|S| = \mathsf{d}(G)$, and assume that there is some $h \in G^\bullet \setminus \Sigma(S)$. Then $T = (-h)S \in \mathcal{A}^*(G)$ and $|T| = 1 + |S|$, which contradicts the maximal choice of S. Clearly, $\Sigma(S) = G^\bullet$ implies $G = \langle \mathrm{supp}(S) \rangle$.

2. If $S \in \mathcal{F}(G)$ and $\Sigma(S) = G^\bullet$, then $S \in \mathcal{A}^*(G)$, and thus $|S| \le \mathsf{d}(G)$. Conversely, if $S \in \mathcal{A}^*(G)$ and $|S| = \mathsf{d}(G)$, then $\Sigma(S) = G^\bullet$ by 1.

3. By definition we have $\mathsf{d}(G) = \max\bigl\{|S| \bigm| S \in \mathcal{A}^*(G)\bigr\}$. Hence $\mathsf{D}(G) = \mathsf{d}(G) + 1$ is the smallest integer $l \in \mathbb{N}$ such that every sequence $S \in \mathcal{F}(G)$ with $|S| \ge l$ does not lie in $\mathcal{A}^*(G)$.

4. If $S = g_1 \cdot \ldots \cdot g_l \in \mathcal{A}^*(G)$, then $C = \{g_1 + \ldots + g_k \mid k \in [1, l]\} \subset \Sigma(S) \subset G^\bullet$, and therefore $|S| = |C| \le |\Sigma(S)| \le |G| - 1$. Hence $\mathsf{d}(G) \le |G| - 1$, and thus $\mathsf{D}(G) \le |G|$. □

Let $r \in \mathbb{N}$. An r-tuple $(e_1, \ldots, e_r)$ of elements of $G^\bullet$ (resp. the elements $e_1, \ldots, e_r$) is said to be *independent* if for every $(m_i)_{i \in [1,r]} \in \mathbb{Z}^r$

$$\sum_{i=1}^r m_i e_i = 0 \quad \text{implies that} \quad m_1 e_1 = \ldots = m_r e_r = 0$$

(equivalently, $\langle e_1, \ldots, e_r \rangle = \langle e_1 \rangle \oplus \ldots \oplus \langle e_r \rangle$). Moreover, $(e_1, \ldots, e_r)$ is called a *basis* of G if $(e_1, \ldots, e_r)$ is independent and $\{e_1, \ldots, e_r\}$ generates G.

Suppose that $|G| > 1$. Then by the Structure Theorem of Finite Abelian Groups, we have

$$G \cong C_{n_1} \oplus \ldots \oplus C_{n_r}$$

where $1 < n_1 \mid \ldots \mid n_r$, $r = \mathsf{r}(G)$ is the *rank* of G and $n_r = \exp(G) = \mathrm{lcm}\{\mathrm{ord}(g) \mid g \in G\}$ is the *exponent* of G. We define

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

and we set $\mathsf{d}^*(\{0\}) = 0$. G is called an (*elementary*) *p-group* if $\exp(G)$ is a power of p (resp. $\exp(G) \mid p$).

Lemma 4.3. *Let* $\exp(G) = n \ge 2$.

1. *If* $e_1, \ldots, e_r \in G$ *are independent elements, then*
$$S = \prod_{i=1}^r e_i^{\mathrm{ord}(e_i) - 1} \in \mathcal{A}^*(G)\,.$$
2. *There exists a sequence* $S \in \mathcal{A}^*(G)$ *such that* $|S| = \mathsf{d}^*(G)$. *In particular,* $\mathsf{d}^*(G) \le \mathsf{d}(G)$.

Proof. 1. If $1 \ne T$ is a a subsequence of S, then $T = e_1^{k_1} \cdot \ldots \cdot e_r^{k_r}$ where $k_i \in [0, \operatorname{ord}(e_i) - 1]$ for all $i \in [1, r]$ and $k_i > 0$ for at least one $i \in [1, r]$. Hence $\sigma(T) = k_1 e_1 + \ldots + k_r e_r \ne 0$, and thus S is zero-sum free.

2. If $G \cong C_{n_1} \oplus \ldots \oplus C_{n_r}$ where $1 < n_1 \mid \ldots \mid n_r$ and $(e_1, \ldots, e_r)$ is a basis of G such that $\operatorname{ord}(e_i) = n_i$ for all $i \in [1, r]$, then $S = e_1^{n_1 - 1} \cdot \ldots \cdot e_r^{n_r - 1} \in \mathcal{A}^*(G)$ by 1., and hence $\mathsf{d}^*(G) = |S| \le \mathsf{d}(G)$. □

Corollary 4.4.

1. *Let G be cyclic of order $n \ge 2$. A sequence $S \in \mathcal{F}(G)$ is zero-sum free of length $|S| = \mathsf{d}(G)$ if and only if $S = g^{n-1}$ for some $g \in G$ with $\operatorname{ord}(g) = n$. In particular, $\mathsf{d}(G) = \mathsf{d}^*(G) = n - 1$ and $\mathsf{D}(G) = n$.*
2. *Let G be an elementary 2-group. A sequence $S \in \mathcal{F}(G)$ is zero-sum free if and only if S is squarefree and $\operatorname{supp}(S)$ is an independent set. In particular, $\mathsf{d}(G) = \mathsf{d}^*(G) = \mathsf{r}(G)$.*

Proof. 1. By Lemmas 4.2 and 4.3, we have $n - 1 = \mathsf{d}^*(G) \le \mathsf{d}(G) \le |G| - 1 = n - 1$ and thus $\mathsf{d}(G) = n - 1$ and $\mathsf{D}(G) = n$. Obviously, if $g \in G$ with $\operatorname{ord}(g) = n$, then $S = g^{n-1} \in \mathcal{A}^*(G)$. Conversely, assume to the contrary that $S = g_1 \cdot \ldots \cdot g_{n-1} \in \mathcal{A}^*(G)$ and $g_1 \ne g_2$. If $\Sigma = \{g_1 + \ldots + g_k \mid k \in [1, n-1]\}$, then $|\Sigma| = n - 1$ and $g_2 \notin \Sigma$, a contradiction.

2. If S is squarefree and $\operatorname{supp}(S)$ is independent, then S is zero-sum free by Lemma 4.3.1. Conversely, if $S \in \mathcal{A}^*(G)$, then $\mathsf{v}_g(S) < \operatorname{ord}(g) \le 2$ for all $g \in \operatorname{supp}(S)$. Hence S is squarefree, and $0 \notin \Sigma(S)$ implies that $\operatorname{supp}(S)$ is independent.

Thus we get $\mathsf{d}(G) = \mathsf{r}(G)$, and by the very definitions, it follows that $\mathsf{d}^*(G) = \mathsf{r}(G)$. □

There is a weighted version of the Davenport constant, called the cross number, which plays a crucial role in factorization theory (in particular, in the investigations of half-factorial and minimal non-half-factorial subsets, see [71, Chapter 5], [110, 111] and [76, 77] for recent progress).

4.B Group algebras

Group algebras $R[G]$ - over suitable commutative rings R - have turned out to be powerful tools for a growing variety of questions from combinatorics and number theory. We discuss the classical application of group algebras to the investigation of zero-sum free sequences over p-groups, which is due to P. van Emde Boas, D. Kruyswijk and J.E. Olson. Theorem 4.10 provides the classical result that for a p-group G we have $\mathsf{d}(G) = \mathsf{d}^*(G)$.

Let R be a commutative ring (throughout, we assume that R has a unit element $1 \ne 0$). The *group algebra* $R[G]$ of G over R is a free R-module with basis $\{X^g \mid g \in G\}$, where multiplication is defined by

$$\Big(\sum_{g \in G} a_g X^g\Big)\Big(\sum_{g \in G} b_g X^g\Big) = \sum_{g \in G}\Big(\sum_{h \in G} a_h b_{g-h}\Big) X^g .$$

In particular, $X^g X^h = X^{g+h}$ for all $g, h \in G$. Thus we can think of this as a generalization of a polynomial ring, where the exponents come from the group G rather than from $\mathbb{N}_0$. Moreover, we view R as a subset of $R[G]$ by means of $a = aX^0$ for all $a \in R$. The *augmentation map*

$$\varepsilon \colon R[G] \to R, \quad \text{defined by} \quad \varepsilon\Big(\sum_{g \in G} a_g X^g\Big) = \sum_{g \in G} a_g$$

is an epimorphism of R-algebras, and its kernel $\operatorname{Ker}(\varepsilon) = I_G$ is called the *augmentation ideal.*

Definition 4.5. For a commutative ring R, let $\mathsf{d}(G, R)$ denote the largest integer $l \in \mathbb{N}$ having the following property:

There is some sequence $S = g_1 \cdot \ldots \cdot g_l$ of length l over G such that

$$(a_1 - X^{g_1}) \cdot \ldots \cdot (a_l - X^{g_l}) \ne 0 \in R[G] \quad \text{for all} \quad a_1, \ldots, a_l \in R^\bullet .$$

Lemma 4.6. *Let R be an integral domain, $S = g_1 \cdot \ldots \cdot g_l \in \mathcal{F}(G)$ a zero-sum free sequence and $a_1, \ldots, a_l \in R^\bullet$. If*

$$f = \prod_{i=1}^{l} (a_i - X^{g_i}) = \sum_{g \in G} c_g X^g \in R[G] \quad \textit{with} \quad c_g \in R \ \textit{ for all } g \in G\,,$$

then $c_0 \ne 0$, and hence $f \ne 0$. In particular, we have $\mathsf{d}(G) \le \mathsf{d}(G, R)$.

Proof. Since R is an integral domain and $0 \notin \Sigma(S)$, it follows that $c_0 = a_1 \cdot \ldots \cdot a_l \ne 0$. □

Definition 4.7. Let $S = g_1 \cdot \ldots \cdot g_l \in \mathcal{F}(G)$ be a sequence of length $|S| = l \in \mathbb{N}_0$ and let $g \in G$.

1. For every $k \in \mathbb{N}_0$ let
$$\mathsf{N}_g^k(S) = \Big| \Big\{ I \subset [1, l] \ \Big| \ \sum_{i \in I} g_i = g \text{ and } |I| = k \Big\} \Big|$$
denote the number of subsequences T of S having sum $\sigma(T) = g$ and length $|T| = k$ (counted with the multiplicity of their appearance in S).
2. We define
$$\mathsf{N}_g(S) = \sum_{k \ge 0} \mathsf{N}_g^k(S)\,, \quad \mathsf{N}_g^+(S) = \sum_{k \ge 0} \mathsf{N}_g^{2k}(S) \quad \text{and} \quad \mathsf{N}_g^-(S) = \sum_{k \ge 0} \mathsf{N}_g^{2k+1}(S)\,.$$
Thus $\mathsf{N}_g(S)$ denotes the number of subsequences T of S having sum $\sigma(T) = g$, $\mathsf{N}_g^+(S)$ denotes the number of all such subsequences of even length, and $\mathsf{N}_g^-(S)$ denotes the number of all such subsequences of odd length (each counted with the multiplicity of its appearance in S).

Lemma 4.8. *Let p be a prime and G a p-group. Then the following identities hold in $\mathbb{F}_p[G]$.*

1. *If $g \in G$ and $\operatorname{ord}(g) = m \ge 2$, then*
$$(1 - X^g)^m = 0 \in \mathbb{F}_p[G]\,, \quad (1 - X^g)^{m-1} = \sum_{j=0}^{m-1} X^{jg} \in \mathbb{F}_p[G]$$
and
$$(1 - X^g)^{m-2} = \sum_{j=0}^{m-1} (j+1) X^{jg} \in \mathbb{F}_p[G]\,.$$
2. *Let $(e_1, \ldots, e_r)$ be a basis of G and $\operatorname{ord}(e_i) = n_i \ge 2$ for all $i \in [1, r]$. Then*
$$\prod_{i=1}^{r} (1 - X^{e_i})^{n_i - 1} = \sum_{g \in G} X^g \in \mathbb{F}_p[G]\,,$$
and if $m \in \mathbb{N}$ and $g_1, \ldots, g_m \in G$, then
$$\prod_{\mu=1}^{m} (1 - X^{g_\mu}) \ = \ \sum_{j=1}^{t} c_j \prod_{i=1}^{r} (1 - X^{e_i})^{l_{j,i}} \ \in \mathbb{F}_p[G]\,,$$
where $t \in \mathbb{N}_0$, $c_j \in \mathbb{F}_p$, $l_{j,1}, \ldots, l_{j,r} \in \mathbb{N}_0$ and $l_{j,1} + \ldots + l_{j,r} \ge m$ for all $j \in [1, t]$.

Proof. 1. Since m is a power of p, we obtain $(1 - X^g)^m = 1 - X^{mg} = 0 \in \mathbb{F}_p[G]$. For $k \in \{1, 2\}$, we have

$$(1 - X^g)^{m-k} = \sum_{j=0}^{m-k} \binom{m-k}{j} (-1)^j X^{jg}\,.$$

We assert that, for every $j \in [0, m-1]$,

$$\binom{m-1}{j}(-1)^j \equiv 1 \mod p \quad \text{and} \quad \binom{m-2}{j}(-1)^j \equiv (j+1) \mod p\,.$$

Indeed, in the polynomial ring $\mathbb{F}_p[T]$ we have

$$\sum_{j=0}^{m-1} \binom{m-1}{j}(-1)^j T^j = (1-T)^{m-1} = \frac{(1-T)^m}{1-T} = \frac{1-T^m}{1-T} = \sum_{j=0}^{m-1} T^j\,,$$

whence the first assertion follows. Since

$$\binom{m-2}{j} = \binom{m-1}{j}\frac{m-j-1}{m-1} \equiv (j+1)\binom{m-1}{j} \mod p\,,$$

the second assertion follows.

2. Every $g \in G$ has a unique representation of the form $g = \nu_1 e_1 + \ldots + \nu_r e_r$, where $\nu_i \in [0, n_i - 1]$ for all $i \in [1, r]$. Therefore 1. implies that

$$\prod_{i=1}^{r}(1 - X^{e_i})^{n_i - 1} = \prod_{i=1}^{r}\sum_{\nu_i=0}^{n_i-1} X^{\nu_i e_i} = \sum_{g \in G} X^g\,.$$

For the proof of the second identity we define, for every $\boldsymbol{l} = (l_1, \ldots, l_r) \in \mathbb{N}_0^r$,

$$g_{\boldsymbol{l}} = \prod_{i=1}^{r}(1 - X^{e_i})^{l_i}\,.$$

The augmentation ideal I_G is generated by $\{g_{\boldsymbol{l}} \mid \boldsymbol{0} \ne \boldsymbol{l} \in \mathbb{N}_0^r\}$. For $\mu \in [1, m]$ we have $1 - X^{g_\mu} \in I_G$ and therefore

$$1 - X^{g_\mu} = \sum_{\boldsymbol{0} \ne \boldsymbol{l} \in \mathbb{N}_0^r} c_{\mu, \boldsymbol{l}}\, g_{\boldsymbol{l}}$$

with coefficients $c_{\mu,\boldsymbol{l}} \in \mathbb{F}_p$. Hence

$$\prod_{\mu=1}^{m}(1 - X^{g_\mu}) \;=\; \sum_{\boldsymbol{0} \ne \boldsymbol{l}_1, \ldots, \boldsymbol{l}_m \in \mathbb{N}_0^r} c_{1,\boldsymbol{l}_1} \cdot \ldots \cdot c_{m,\boldsymbol{l}_m}\, g_{\boldsymbol{l}_1 + \ldots + \boldsymbol{l}_m}\,,$$

and $|\boldsymbol{l}_1 + \ldots + \boldsymbol{l}_m| \ge m$ for all $\boldsymbol{l}_1, \ldots, \boldsymbol{l}_m \in \mathbb{N}_0^r \setminus \{\boldsymbol{0}\}$. □

Lemma 4.9. *Let p be a prime, G a p-group, $S = g_1 \cdot \ldots \cdot g_l \in \mathcal{F}(G)$, and*

$$f \;=\; \prod_{i=1}^{l}(1 - X^{g_i}) = \sum_{g \in G} c_g(S) X^g \in \mathbb{F}_p[G]\,.$$

1. *For every $g \in G$, we have $c_g(S) = \mathsf{N}_g^+(S) - \mathsf{N}_g^-(S) + p\mathbb{Z} \in \mathbb{F}_p$. In particular, if $c_0(S) = 0$, then $0 \in \Sigma(S)$, and if $g \in G^\bullet$ and $c_g(S) \ne 0$, then $g \in \Sigma(S)$.*
2. *For $i \in [1, l]$, let $g_i = p^{m_i} g_i'$ with $g_i' \in G$ and $m_i \in \mathbb{N}_0$, and define*

$$m = \sum_{i=1}^{l} p^{m_i}\,.$$

If $m > \mathsf{d}^*(G)$, then $c_g(S) = 0$ for all $g \in G$, $0 \in \Sigma(S)$, and in particular $\mathsf{N}_g^+(S) \equiv \mathsf{N}_g^-(S) \mod p$ for all $g \in G$.

Proof. 1. For $g \in G$, we set

$$\Omega_g = \Big\{ I \subset [1,l] \ \Big| \ \sum_{i \in I} g_i = g \Big\} \,.$$

Then $\emptyset \in \Omega_0$ and

$$c_g(S) = \sum_{J \in \Omega_g} (-1)^{|J|} + p\mathbb{Z} \ = \ \mathsf{N}_g^+(S) - \mathsf{N}_g^-(S) + p\mathbb{Z} \in \mathbb{F}_p \,.$$

Hence $c_0(S) = 0$ implies $0 \in \Sigma(S)$, and if $g \in G^\bullet$ is such that $c_g(S) \ne 0$, then $g \in \Sigma(S)$.

2. We shall repeatedly make use of Lemma 4.8. Let $(e_1, \ldots, e_r)$ be a basis of G, $\operatorname{ord}(e_i) = n_i$ for all $i \in [1,r]$, and $1 < n_1 \,|\, \ldots \,|\, n_r$. Then

$$\mathsf{d}^*(G) = (n_1 - 1) + \ldots + (n_r - 1) \,.$$

For $i \in [1,r]$ we have $(1 - X^{g_i'})^{p^{m_i}} = 1 - X^{p^{m_i} g_i'} = 1 - X^{g_i}$, and therefore

$$f \ = \ \prod_{i=1}^{l} (1 - X^{g_i'})^{p^{m_i}} = \sum_{j=1}^{t} c_j \prod_{i=1}^{r} (1 - X^{e_i})^{l_{j,i}}$$

for some $t \in \mathbb{N}_0$, $c_1, \ldots, c_t \in \mathbb{F}_p$, $l_{j,i} \in \mathbb{N}_0$ and $l_{j,1} + \ldots + l_{j,r} \ge m$ for all $j \in [1,t]$. If $j \in [1,t]$ and $l_{j,i} \ge n_i$ for some $i \in [1,r]$, then

$$\prod_{i=1}^{r} \big(1 - X^{e_i}\big)^{l_{j,i}} = 0 \in \mathbb{F}_p[G] \,.$$

Hence we may assume that $l_{j,i} < n_i$ for all $i \in [1,r]$ and $j \in [1,t]$, and then either $t = 0$ or $m \le l_{j,1} + \ldots + l_{j,r} \le \mathsf{d}^*(G)$ for all $j \in [1,t]$.

If $m > \mathsf{d}^*(G)$, then $t = 0$, hence $f = 0$, and thus $c_g(S) = 0$ for all $g \in G$. The remaining assertions follow by 1. □

Theorem 4.10. *If G is a p-group, then* $\mathsf{d}^*(G) = \mathsf{d}(G) = \mathsf{d}(G, \mathbb{F}_p)$.

Proof. Suppose that G is a p-group. Lemmas 4.3.2 and 4.6 imply that $\mathsf{d}^*(G) \le \mathsf{d}(G) \le \mathsf{d}(G, \mathbb{F}_p)$. If $S = g_1 \cdot \ldots \cdot g_l \in \mathcal{F}(G)$ with $|S| = l > \mathsf{d}^*(G)$, then Lemma 4.9.2 (with $m_1 = \ldots = m_l = 0$) implies that

$$(1 - X^{g_1}) \cdot \ldots \cdot (1 - X^{g_l}) = 0 \,,$$

and thus $\mathsf{d}(G, \mathbb{F}_p) \le \mathsf{d}^*(G)$. □

An alternate proof of Theorem 4.10 was given by Zhi-Wei Sun who used covers of the integers (see [128, Corollary 2.1]). Here we briefly discuss some extensions of the classical approach via group algebras.

Let G' be a finite abelian group. Then, by G. Higman's Theorem, $\mathbb{Z}[G] \cong \mathbb{Z}[G']$ implies that $G \cong G'$ (see [106, Corollary 3.5.6 and Theorem 9.1.4]). Therefore any combinatorial problem in G can, at least in principle, be tackled via the group algebra $\mathbb{Z}[G]$. Indeed, working over $\mathbb{Z}[G]$ allows to refine the congruences involving $\mathsf{N}_g^+(S)$ and $\mathsf{N}_g^-(S)$, as obtained in Lemma 4.9.2 (see [52]).

Let $\exp(G) = n$ and let K be a splitting field of G (that is $|\{\zeta \in K \mid \zeta^n = 1\}| = n$). Following the ideas of P. van Emde Boas and using character theory, one obtains that

$$\mathsf{d}(G, K) \le (n-1) + n \log \frac{|G|}{n}$$

(see [71, Theorem 5.5.5]). In particular, for cyclic group this implies that $\mathsf{d}(G) = \mathsf{d}(G, K) = n - 1$. W. Gao conjectures that for every G there is a splitting field F such that $\mathsf{d}(G) = \mathsf{d}(G, F)$, and in [59] W. Gao and Y. Li showed that, for every splitting field K of $G = C_2 \oplus C_{2n}$ we have $\mathsf{d}(C_2 \oplus C_{2n}) = \mathsf{d}(C_2 \oplus C_{2n}, K)$ (see also [55]).

4.C Arithmetical invariants again

Theorem 4.11. *Let H be a Krull monoid with class group G such that every class contains a prime and suppose that $|G|>1$. Let $k \in \mathbb{N}$.*

1. *If $A = 0^m B \in \mathcal{B}(G)$, with $m \in \mathbb{N}_0$ and $B \in \mathcal{B}(G^\bullet)$, then*
$$2\max \mathsf{L}(A) - m \le |A| \le \mathsf{D}(G)\min \mathsf{L}(A) - m(\mathsf{D}(G)-1) \quad \textit{and} \quad \rho(A) \le \frac{\mathsf{D}(G)}{2}\,.$$
2. *We have $k \le \rho_k(H) \le k\frac{\mathsf{D}(G)}{2}$ and $\rho(H)^{-1}k \le \lambda_k(H) \le k$.*
3. *$\rho_{2k}(H) = k\mathsf{D}(G)$ and $\rho(H) = \frac{\mathsf{D}(G)}{2}$.*
4. *If $j,l \in \mathbb{N}_0$ such that $l\mathsf{D}(G)+j \ge 1$, then*
$$2l + \frac{2j}{\mathsf{D}(G)} \le \lambda_{l\mathsf{D}(G)+j}(G) \le 2l+j\,.$$
In particular, $\lambda_{l\mathsf{D}(G)}(G) = 2l$ for every $l \in \mathbb{N}$.

Proof. By Theorem 3.16 it suffices to consider the block monoid $\mathcal{B}(G)$.

1. Let $A = 0^m U_1 \cdot \ldots \cdot U_l$ where $l,m \in \mathbb{N}_0$ and $U_1,\ldots,U_l \in \mathcal{A}(G^\bullet)$. Then $2 \le |U_\nu| \le \mathsf{D}(G)$ for all $\nu \in [1,l]$ and hence
$$m + 2l \le |A| \le m + l\mathsf{D}(G)\,.$$
Choosing $l = \min \mathsf{L}(B)$ and $l = \max \mathsf{L}(B)$ we obtain the first inequalities, and then we get
$$\rho(A) = \frac{\max \mathsf{L}(A)}{\min \mathsf{L}(A)} = \frac{m+\max \mathsf{L}(B)}{m+\min \mathsf{L}(B)} \le \frac{\max \mathsf{L}(B)}{\min \mathsf{L}(B)} \le \frac{\mathsf{D}(G)}{2}\,.$$

2. By definition, we have $k \le \rho_k(G)$. If $A \in \mathcal{B}(G)$ with $k \in \mathsf{L}(A)$ and $\max \mathsf{L}(A) = \rho_k(G)$, then 1. implies that
$$\frac{\rho_k(G)}{k} \le \frac{\max \mathsf{L}(A)}{\min \mathsf{L}(A)} = \rho(A) \le \frac{\mathsf{D}(G)}{2}\,.$$
There is some $L \in \mathcal{L}(G)$ with $k, \lambda_k(G) \in L$, and hence it follows that
$$k \le \max L \le \rho(G)\min L = \rho(G)\lambda_k(G)\,.$$

3. By 1. and 2. it follows that $\rho_{2k}(G) \le k\mathsf{D}(G)$ and $\rho(G) \le \frac{\mathsf{D}(G)}{2}$. If $U = g_1 \cdot \ldots \cdot g_l \in \mathcal{A}(G)$ with $|U| = l = \mathsf{D}(G)$, then
$$(-U)^k U^k = \prod_{\nu=1}^{l} \big((-g_\nu)g_\nu\big)^k\,,$$
shows that in both inequalities we actually have equality.

4. Let $j,l \in \mathbb{N}_0$ such that $l\mathsf{D}(G)+j \ge 1$. Then 2. and 3. imply that
$$2l + \frac{2j}{\mathsf{D}(G)} = \rho(G)^{-1}\big(l\mathsf{D}(G)+j\big) \le \lambda_{l\mathsf{D}(G)+j}(G) \le l\mathsf{D}(G)+j\,.$$
If $j=0$, it follows that $\lambda_{l\mathsf{D}(G)}(G) = 2l$. □

Lemma 4.12.

1. *For $j \in \mathbb{N}_{\ge 2}$, the following statements are equivalent:*
   (a) *There exists some $L \in \mathcal{L}(G)$ with $\{2,j\} \subset L$.*
   (b) *$j \le \mathsf{D}(G)$.*
2. *Let $|G| \ge 3$ and $A \in \mathcal{B}(G)$. Then $\{2, \mathsf{D}(G)\} \subset \mathsf{L}(A)$ if and only if $A = U(-U)$ for some $U \in \mathcal{A}(G)$ with $|U| = \mathsf{D}(G)$.*

Proof. 1. (a) $\Rightarrow$ (b) If $L \in \mathcal{L}(G)$ and $\{2, j\} \subset L$, then Theorem 4.11.3 implies that $j \le \sup L \le \rho_2(G) = \mathsf{D}(G)$.

(b) $\Rightarrow$ (a) If $j \le \mathsf{D}(G)$, then there exists some $U \in \mathcal{A}(G)$ with $|U| = l \ge j$, say $U = g_1 \cdot \ldots \cdot g_l$. Then $V = g_1 \cdot \ldots \cdot g_{j-1}(g_j + \ldots + g_l) \in \mathcal{A}(G)$, and $\{2, j\} \subset \mathsf{L}\big(V(-V)\big)$.

2. If $\{2,\, \mathsf{D}(G)\} \subset \mathsf{L}(A)$, then there exist $U_1, U_2, V_1, \ldots, V_{\mathsf{D}(G)} \in \mathcal{A}(G)$ such that $A = U_1U_2 = V_1 \cdot \ldots \cdot V_{\mathsf{D}(G)}$, and clearly $0 \nmid A$, since otherwise $U_1 = 0$ or $U_2 = 0$ and $\mathsf{D}(G) = 2$. Theorem 4.11.1 implies that $\max \mathsf{L}(A) = \mathsf{D}(G)$ and $|A| = 2\mathsf{D}(G)$. Hence $|V_i| = 2$ for all $i \in [1, \mathsf{D}(G)]$, and $|U_1| = |U_2| = \mathsf{D}(G)$, which implies $U_2 = -U_1$. The converse is obvious. □

Lemma 4.13. *Suppose that $d \in \mathbb{N}$ has the following property:*

> *For all U, $V \in \mathcal{A}(G)$ with $\min\{|U|, |V|\} > d$ there exists a factorization $UV = W_1 \cdot \ldots \cdot W_k$ with $k \in [2, d]$ and $|W_1| \le d$.*

Then $\mathsf{c}(G) \le d$.

Proof. We must prove that $\mathsf{c}(A) \le d$ for all $A \in \mathcal{B}(G)$. We proceed by induction on $|A|$, and we must prove that any two factorizations of A can be concatenated by a d-chain. Let z, z' be two factorizations of A, say

$$z = U_1 \cdot \ldots \cdot U_r \quad \text{and} \quad z' = V_1 \cdot \ldots \cdot V_s\,, \quad \text{where} \quad U_1, \ldots, U_r, V_1, \ldots, V_s \in \mathcal{A}(G)\,.$$

If $\max\{r,\, s\} \le d$, then $\mathsf{d}(z, z') \le d$ and we are done. Assume that $r > d$.

CASE 1: $|V_i| \le d$ for some $i \in [1, s]$, say $|V_1| \le d$.

We may assume that $V_1 \,|\, U_1 \cdot \ldots \cdot U_{r-1}$, say $U_1 \cdot \ldots \cdot U_{r-1} = V_1 W_1 \cdot \ldots \cdot W_t$ with $t \in \mathbb{N}$ and $W_1, \ldots, W_t \in \mathcal{A}(G)$. By the induction hypothesis there is a d-chain of factorizations $y_0, \ldots, y_k$ concatenating $U_1 \cdot \ldots \cdot U_{r-1}$ and $V_1 W_1 \cdot \ldots \cdot W_t$, and there is a d-chain of factorizations $z_0, \ldots, z_l$ concatenating $W_1 \cdot \ldots \cdot W_t U_r$ and $V_2 \cdot \ldots \cdot V_s$. Then $z = y_0 U_r, \ldots, y_k U_r = z_0 V_1, \ldots, z_l V_1 = z'$ is a d-chain concatenating z and z'.

CASE 2: $|V_i| > d$ for all $i \in [1, s]$.

By assumption there is a factorization $V_1 V_2 = W_1 \cdot \ldots \cdot W_k$, where $k \in [2, d]$ and $|W_1| \le d$. Then the factorization $z'' = W_1 \cdot \ldots \cdot W_k V_3 \cdot \ldots \cdot V_s$ of A satisfies $\mathsf{d}(z', z'') = \max\{2, k\} \le d$, and by CASE 1 there is a d-chain of factorizations concatenating z and z''. □

Theorem 4.14. *Let H be a Krull monoid with class group G.*

1. $\mathsf{c}(H) \le \mathsf{D}(G)$.
2. *Suppose that $|G| \ge 3$. Then $\mathsf{c}(G) = \mathsf{D}(G)$ if and only if G is either cyclic or an elementary 2-group.*

Proof. 1. By Theorem 3.16 it suffices to show that $\mathsf{c}(G) \le \mathsf{D}(G)$. This follows immediately from Lemma 4.13 with $d = \mathsf{D}(G)$.

2. If G is cyclic, $g \in G$ with $\mathrm{ord}(g) = n = |G|$ and $U = g^n$, then $\mathsf{c}\big((-U)U\big) = n$ and hence $\mathsf{c}(G) = \mathsf{D}(G)$. If G is an elementary 2-group with basis $(e_1, \ldots, e_r)$, $e_0 = e_1 + \ldots + e_r$ and $U = e_0 \cdot \ldots \cdot e_r$, then $\mathsf{c}\big(U^2\big) = r + 1 = \mathsf{D}(G)$ and hence $\mathsf{c}(G) = \mathsf{D}(G)$.

Assume now that G is neither cyclic nor an elementary 2-group. We shall prove that for all U, $V \in \mathcal{A}(G)$ with $|U| = |V| = \mathsf{D}(G)$ there exists some factorization $UV = W_1 \cdot \ldots \cdot W_k$ with $k \in [2, \mathsf{d}(G)]$ and $|W_1| \le \mathsf{d}(G)$. Then $\mathsf{c}(G) \le \mathsf{d}(G)$ by Lemma 4.13.

Let U, $V \in \mathcal{A}(G)$ with $|U| = |V| = \mathsf{D}(G)$. Then $\max \mathsf{L}(UV) \le \mathsf{D}(G)$, and equality holds if and only if $V = -U$ (cf. Lemma 4.12). Now we distinguish two cases.

CASE 1: $V \ne -U$.

It is sufficient to prove that there exists some $W \in \mathcal{A}(G)$ such that $W \,|\, UV$ and $|W| < \mathsf{D}(G)$. Assume the contrary. Let $g \in \mathrm{supp}(U)$ and $V = h_1 \cdot \ldots \cdot h_l$ with $l = \mathsf{D}(G)$. For every $i \in [1, l]$, we consider the sequence $S_i = gh_i^{-1}V \in \mathcal{F}(G)$. Since $|S_i| = \mathsf{D}(G)$, there exists some $S_i' \in \mathcal{A}(G)$ such that $S_i' \,|\, S_i \,|\, UV$. By assumption, this implies $|S_i'| = \mathsf{D}(G)$, hence $S_i' = S_i$ and therefore $0 = \sigma(S_i) = g - h_i$. Thus $V = g^l$, and Lemma 4.2.1 implies $G = \langle \mathrm{supp}(V) \rangle = \langle g \rangle$, a contradiction.

CASE 2: $V = -U$.

It is sufficient to prove that there exists some $W \in \mathcal{A}(G)$ such that $W \,|\, U(-U)$ and $2 < |W| < \mathsf{D}(G)$. Then we consider any factorization $U(-U) = WW_2 \cdot \ldots \cdot W_k$ with $W_2, \ldots, W_k \in \mathcal{A}(G)$, and obtain that $k < \mathsf{D}(G)$.

By Lemma 4.2.1 we have $\langle \mathrm{supp}(U) \rangle = G$, and since G is not an elementary 2-group, there exists some $g_0 \in \mathrm{supp}(U)$ with $\mathrm{ord}(g_0) > 2$. We set $U = g_0^m g_1 \cdot \ldots \cdot g_l$ with $g_0 \notin \{g_1, \ldots, g_l\}$. Since $G = \langle \mathrm{supp}(U) \rangle$ is not cyclic, it follows that $l \ge 2$. If $W' = (-g_0)^m g_1 \cdot \ldots \cdot g_l$, then $W' \,|\, U(-U)$ and $|W'| = \mathsf{D}(G)$. Hence there exists some $W \in \mathcal{A}(G)$ with $W \,|\, W'$, and we shall prove that $2 < |W| < \mathsf{D}(G)$. Since $U \in \mathcal{A}(G)$, we have $W \nmid g_1 \cdot \ldots \cdot g_l$ and thus $-g_0 \,|\, W$. Since $g_0 \notin \{g_1, \ldots, g_l\}$ and $g_0 \ne -g_0$, it follows that $W \ne g_0(-g_0)$ and thus $|W| > 2$.

Assume to the contrary that $|W| = \mathsf{D}(G)$. Then $W = W'$, and $\sigma(U) = \sigma(W) = 0$ implies $2mg_0 = 0$ and thus $m > 1$. We consider the sequence $S = g_0^m g_1 \cdot \ldots \cdot g_{l-1}$. Since $S \in \mathcal{A}^*(G)$ and $|S| = \mathsf{d}(G)$, Lemma 4.2.1 implies $\Sigma(S) = G^\bullet$ and thus $(m+1)g_0 \in \Sigma(S)$, say

$$(m+1)g_0 = sg_0 + \sum_{i \in I} g_i \quad \text{with} \quad s \in [0, m] \quad \text{and} \quad I \subset [1, l-1]\,.$$

If $s = 0$, then

$$0 = 2mg_0 = (m-1)g_0 + \sum_{i \in I} g_i \ \in \Sigma(S),$$

a contradiction. If $s \ge 1$, then it follows that

$$T = (-g_0)^{m+1-s} \prod_{i \in I} g_i$$

is a proper zero-sum subsequence of W, a contradiction to $W \in \mathcal{A}(G)$. □

Corollary 4.15. *Let H be a Krull monoid with class group G such that every class contains a prime. Suppose that $|G| \ge 3$ and that $\exp(G) = n \ge 2$. Then*

$$[1, n-2] \subset \Delta(H) \subset [1, \mathsf{c}(G) - 2] \subset [1, \mathsf{D}(G) - 2]\,.$$

In particular, if G is cyclic, then $\Delta(H) = [1, n-2]$.

Proof. By Theorem 3.16, it suffices to consider the block monoid $\mathcal{B}(G)$. Lemma 3.7.3 implies that $\Delta(G) \subset [1, \mathsf{c}(G) - 2]$ and Theorem 4.14 that $\mathsf{c}(G) \le \mathsf{D}(G)$.

Suppose that $n \ge 3$, pick $i \in [3, n]$ and $g \in G$ with $\mathrm{ord}(g) = n$. Then $T = g^n, U = (-g)^{i-1}\big((i-1)g\big), V = (-g)g$ and $W = g^{n-i+1}\big((i-1)g\big)$ are minimal zero-sum sequences. Then

$$TU = V^{i-1}W$$

shows that $\mathsf{L}(TU) = \{2, i\}$ whence $i - 2 \in \Delta\big(\mathsf{L}(TU)\big) \subset \Delta(G)$.

If G is cyclic, then Corollary 4.4 implies that $\mathsf{D}(G) = n$ and thus $\Delta(G) = [1, n-2]$. □

For all groups known so far it always holds $\Delta(G) = [1, \mathsf{c}(G) - 2]$.

Corollary 4.16. *The following statements are equivalent*:

(a) *Every $L \in \mathcal{L}(G)$ with $\{2, \mathsf{D}(G)\} \subset L$ satisfies $L = \{2, \mathsf{D}(G)\}$.*

(b) $\{2, \mathsf{D}(G)\} \in \mathcal{L}(G)$.

(c) *G is either cyclic or an elementary 2-group.*

Proof. (a) $\Rightarrow$ (b) By Lemma 4.12.1 there exists some $L \in \mathcal{L}(G)$ with $\{2, \mathsf{D}(G)\} \subset L$.

(b) $\Rightarrow$ (c) If $L = \{2, \mathsf{D}(G)\} \in \mathcal{L}(G)$, then, by Lemma 3.7.3 and Theorem 4.14.1 we have $\mathsf{D}(G) \le 2 + \sup \Delta(G) \le \mathsf{c}(G) \le \mathsf{D}(G)$, hence $\mathsf{c}(G) = \mathsf{D}(G)$, and the assertion follows by Theorem 4.14.2.

(c) $\Rightarrow$ (a) Let $L \in \mathcal{L}(G)$ with $\{2, \mathsf{D}(G)\} \subset L$. By Lemma 4.12.2 we have $L = \mathsf{L}\big(U(-U)\big)$ for some $U \in \mathcal{A}(G)$ with $|U| = \mathsf{D}(G)$.

If G is cyclic of order $n \ge 3$, then Corollary 4.4 implies that $U = g^n$ for some $g \in G$ with $\operatorname{ord}(g) = n$. Since $\mathcal{A}(\{-g, g\}) = \{(-g)^n,\, g^n,\, g(-g)\}$, it follows that $\mathsf{L}\big(U(-U)\big) = \{2, \mathsf{D}(G)\}$.

If G is an elementary 2-group of rank $r \ge 2$ and $(e_1, \ldots, e_r)$ is a basis of G, then $U = e_1 \cdot \ldots \cdot e_r(e_1 + \ldots + e_r)$ by Corollary 4.4 and $\mathsf{L}\big(U(-U)\big) = \{2, r+1\} = \{2, \mathsf{D}(G)\}$. □

5. The structure of sets of lengths

Sets of lengths in Krull monoids and in noetherian domains are finite and nonempty. Furthermore, either all sets of lengths are singletons or sets of lengths may become arbitrarily large (see Lemma 3.1).

5.A Unions of sets of lengths

Definition 5.1. Let H be a BF-monoid and $k \in \mathbb{N}$. Let $\mathcal{V}_k(H)$ denote the set of all $m \in \mathbb{N}$ for which there exist $u_1, \ldots, u_k, v_1, \ldots, v_m \in \mathcal{A}(H)$ with $u_1 \cdot \ldots \cdot u_k = v_1 \cdot \ldots \cdot v_m$.

Lemma 5.2. *Let H be a* BF*-monoid with $H \ne H^\times$ and $k, l \in \mathbb{N}$.*

1. *$\mathcal{V}_1(H) = \{1\}$, $k \in \mathcal{V}_k(H)$ and*
$$\mathcal{V}_k(H) \;=\; \bigcup_{k \in L, L \in \mathcal{L}(H)} L\,.$$
In particular, $\rho_k(H) = \sup \mathcal{V}_k(H)$ and $\lambda_k(H) = \min \mathcal{V}_k(H)$.
2. *$\mathcal{V}_k(H) + \mathcal{V}_l(H) \;\subset\; \mathcal{V}_{k+l}(H)$ and*
$$\lambda_{k+l}(H) \le \lambda_k(H) + \lambda_l(H) \le k + l \le \rho_k(H) + \rho_l(H) \le \rho_{k+l}(H)\,.$$
3. *We have $l \in \mathcal{V}_k(H)$ if and only if $k \in \mathcal{V}_l(H)$.*

Proof. This follows immediately from the definitions. □

Thus the sets $\mathcal{V}_k(H)$ are unions of sets of lengths. They were introduced by S.T. Chapman and W.W. Smith in 1990 (see [17]). The following result reveals that, in Krull monoids where every class contains a prime, the $\mathcal{V}_k(H)$ sets are intervals. This was first shown in [35]. The following simple proof is due to F. Halter-Koch.

Theorem 5.3. *Let H be a Krull monoid with finite class group G such that every class contains a prime. Then for every $k \in \mathbb{N}$ the set $\mathcal{V}_k(H)$ is an arithmetical progression with difference* 1*, and hence $\mathcal{V}_k(H) = [\lambda_k(H), \rho_k(H)]$.*

Proof. By Theorem 3.16, it suffices to consider the block monoid $\mathcal{B}(G)$.

If $|G| \le 2$, then $\mathcal{B}(G)$ is half-factorial by Proposition 3.12 whence the sets $\mathcal{V}_k(G)$ are singletons for all $k \in \mathbb{N}$. Let $|G| \ge 3$ and $k \in \mathbb{N}$. First, we point out that it suffices to prove that $[k, \rho_k(G)] \subset \mathcal{V}_k(G)$. Indeed, suppose that this is done, and let $l \in [\lambda_k(G), k]$. Then $l \le k \le \rho_l(G)$, hence $k \in \mathcal{V}_l(G)$ and consequently $l \in \mathcal{V}_k(G)$.

Thus let $l \in [k, \rho_k(G)]$ be minimal such that $[l, \rho_k(G)] \subset \mathcal{V}_k(G)$ and assume to the contrary that $l > k$. Let Ω be the set of all $A \in \mathcal{B}(G)$ such that $\{k, j\} \subset \mathsf{L}(A)$ for some $j \ge l$, and let $B \in \Omega$ be such that $|B|$

is minimal. Then $B = U_1 \cdot \ldots \cdot U_k = V_1 \cdot \ldots \cdot V_j$, where $j \ge l$ and $U_1, \ldots, U_k, V_1, \ldots, V_j \in \mathcal{A}(G)$. Since $j > k$, we have $B \ne 0^{|B|}$, and (after renumbering if necessary) we may assume that $U_k = g_1 g_2 U'$ and $V_{j-1} V_j = g_1 g_2 V'$, where $g_1, g_2 \in G$ and $U', V' \in \mathcal{F}(G)$. Then $U_k' = (g_1 + g_2) U' \in \mathcal{A}(G)$, and we suppose that $V_{j-1}' = (g_1 + g_2) V' = W_1 \cdot \ldots \cdot W_t$, where $t \in \mathbb{N}$ and $W_1, \ldots, W_t \in \mathcal{A}(G)$. If $B' = U_1 \cdot \ldots \cdot U_{k-1} U_k'$, then $|B'| < |B|$ and $B' = V_1 \cdot \ldots \cdot V_{j-2} W_1 \cdot \ldots \cdot W_t$. By the minimal choice of $|B|$, it follows that $j - 2 + t < l$, hence $t = 1$, $j = l$ and $l - 1 \in \mathcal{V}_k(G)$, a contradiction. □

The structure of unions of sets of lengths in much more general settings is studied in [53]. Here we stick to Krull monoids and determine the $\lambda_k(H)$-invariants with respect to the $\rho_k(H)$-invariants.

Corollary 5.4. *Let H be a Krull monoid with class group G such that every class contains a prime, and suppose that $|G| > 1$. Then for every $l \in \mathbb{N}_0$ we have*

$$\lambda_{l\mathsf{D}(G)+j}(H) = \begin{cases} 2l & \text{for } \ j = 0 \\ 2l+1 & \text{for } \ j \in [1, \rho_{2l+1}(G) - l\mathsf{D}(G)] \\ 2l+2 & \text{for } \ j \in [\rho_{2l+1}(G) - l\mathsf{D}(G) + 1, \mathsf{D}(G) - 1]\,, \end{cases}$$

provided that $l\mathsf{D}(G) + j \ge 1$.

Proof. By Theorem 3.16, it suffices to consider the block monoid $\mathcal{B}(G)$. If $|G| = 2$, then $\mathcal{B}(G)$ is half-factorial, $\mathsf{D}(G) = 2$ and hence the assertion follows. Suppose that $|G| \ge 3$, and thus we get $\mathsf{D}(G) \ge 3$.

Let $l \in \mathbb{N}_0$ and $j \in [0, \mathsf{D}(G) - 1]$ such that $l\mathsf{D}(G) + j \ge 1$. For $j = 0$ the assertion follows from Theorem 4.11.4. Let $j \in [1, \mathsf{D}(G) - 1]$. By Theorem 4.11.4 we obtain that

$$2l + \frac{2j}{\mathsf{D}(G)} = \frac{l\mathsf{D}(G) + j}{\rho(G)} \le \lambda_{l\mathsf{D}(G)+j}(G) \le 2l + j\,.$$

Thus the assertion follows for $j = 1$, and hence from now on we may suppose that $j \ge 2$. Lemma 4.12.1 implies that $\{2, j\} \subset \mathsf{L}(B)$ for some $B \in \mathcal{B}(G)$ and thus $\lambda_j(G) = 2$. Hence we obtain

$$\lambda_{l\mathsf{D}(G)+j}(G) \le \lambda_{l\mathsf{D}(G)}(G) + \lambda_j(G) = 2l + 2\,,$$

and therefore $\lambda_{l\mathsf{D}(G)+j}(G) \in \{2l+1, 2l+2\}$.

If $j \in [2, \rho_{2l+1}(G) - l\mathsf{D}(G)]$, then $l \ge 1$ and $l\mathsf{D}(G) + j \in \mathcal{V}_{2l+1}(G)$ by Theorem 5.3. Thus $\lambda_{l\mathsf{D}(G)+j}(G) \le 2l + 1$ and hence $\lambda_{l\mathsf{D}(G)+j}(G) = 2l + 1$.

If $j > \rho_{2l+1}(G) - l\mathsf{D}(G)$, then $l\mathsf{D}(G) + j > \rho_{2l+1}(G)$ and $l\mathsf{D}(G) + j \notin \mathcal{V}_{2l+1}(G)$. Thus $\lambda_{l\mathsf{D}(G)+j}(G) > 2l + 1$ and hence $\lambda_{l\mathsf{D}(G)+j}(G) = 2l + 2$. □

Corollary 5.5. *Let H be a Krull monoid whose class group G is an elementary 2-group and suppose that every class contains a prime. Then for every $k \in \mathbb{N}_{\ge 2}$ and every $l \in \mathbb{N}_0$ we have $\mathcal{V}_k(H) = [\lambda_k(H), \rho_k(H)]$,*

$$\rho_k(H) = \lfloor \frac{k\mathsf{D}(G)}{2} \rfloor \quad \text{and} \quad \lambda_{l\mathsf{D}(G)+j}(H) = \begin{cases} 2l + j & \text{for } j \in [0,1] \\ 2l+1 & \text{for } j \in [2, \mathsf{D}(G)/2] \text{ and } l \ge 1\,, \\ 2l+2 & \text{for } j \in [2, \mathsf{D}(G) - 1] \text{ and } (\text{either } j > \mathsf{D}(G)/2 \text{ or } l = 0)\,, \end{cases}$$

provided that $l\mathsf{D}(G) + j \ge 1$.

Proof. By Theorem 3.16 it suffices to consider the block monoid $\mathcal{B}(G)$. By Theorem 5.3 we obtain that $\mathcal{V}_k(H) = [\lambda_k(G), \rho_k(G)]$. If $|G| = 2$, then $\mathcal{B}(G)$ is half-factorial by Proposition 3.12 whence for all $k \in \mathbb{N}$ we have $\lambda_k(G) = k = \rho_k(G)$.

Now suppose that $|G| \ge 4$ and hence $\mathsf{D}(G) > 2$. We first prove the assertion on $\rho_k(G)$ and then the assertion on $\lambda_{l\mathsf{D}(G)+j}(G)$.

1. Let $k \in \mathbb{N}$. If k is even, then the assertion follows from Theorem 4.11.3. Suppose we know that

$$(*) \qquad \rho_3(G) \ge \lfloor \frac{3\mathsf D(G)}{2} \rfloor\,.$$

Then Theorem 4.11 and Lemma 5.2 imply that

$$\lfloor \frac{3\mathsf D(G)}{2} \rfloor + k\mathsf D(G) \le \rho_3(G) + \rho_{2k}(G) \le \rho_{2k+3}(G) \le \lfloor \frac{(2k+3)\mathsf D(G)}{2} \rfloor = \lfloor \frac{3\mathsf D(G)}{2} \rfloor + k\mathsf D(G)\,,$$

and hence the assertion follows. Thus it remains to prove $(*)$. We pick a basis $(e_1, \ldots, e_{\mathsf r(G)})$ of G and set $e_0 = e_1 + \ldots e_{\mathsf r(G)}$.

First suppose that $\mathsf r(G) = 2s+1$ with $s \in \mathbb{N}$. Then

$$\begin{aligned} U &= e_1 \cdot \ldots \cdot e_{s+1} e_{s+2} \cdot \ldots \cdot e_{2s+1} e_0\,, \\ V &= e_1 \cdot \ldots \cdot e_{s+1} (e_1 + e_{s+2}) \cdot \ldots \cdot (e_s + e_{2s+1})(e_{s+1} + \ldots + e_{2s+1}) \quad \text{and} \\ W &= e_{s+2} \cdot \ldots \cdot e_{2s+1} e_0 (e_1 + e_{s+2}) \cdot \ldots \cdot (e_s + e_{2s+1})(e_{s+1} + \ldots + e_{2s+1}) \end{aligned}$$

are minimal zero-sum sequences of length $\mathsf D(G) = 2s+2$. By construction, UVW may be written as a product of $3\mathsf D(G)/2$ minimal zero-sum sequences, and hence $(*)$ follows.

Second suppose that $\mathsf r(G) = 2s$ with $s \in \mathbb{N}$. Then

$$\begin{aligned} U &= e_1 \cdot \ldots \cdot e_s e_{s+1} \cdot \ldots \cdot e_{2s} e_0\,, \\ V &= e_1 \cdot \ldots \cdot e_s (e_1 + e_{s+1}) \cdot \ldots \cdot (e_s + e_{2s})(e_{s+1} + \ldots + e_{2s}) \quad \text{and} \\ W &= e_{s+1} \cdot \ldots \cdot e_{2s} (e_1 + e_{s+1}) \cdot \ldots \cdot (e_s + e_{2s})(e_1 + \ldots + e_s) \end{aligned}$$

are minimal zero-sum sequences of length $\mathsf D(G) = 2s+1$. By construction, UVW may be written as a product of $\lfloor 3\mathsf D(G)/2 \rfloor = 3s+1$ minimal zero-sum sequences, and hence $(*)$ follows.

2. Since $\rho_k(G) = \lfloor \frac{k\mathsf D(G)}{2} \rfloor$, the assertion on $\lambda_{l\mathsf D(G)+j}(G)$ follows from Corollary 5.4. □

5.B Almost arithmetical multiprogressions and the structure of sets of lengths

We start with four simple examples which show the variety of possible structures for sets of lengths.

Examples 5.6.

1. *Arithmetical progressions.* Let $d \in \mathbb{N}$. Let $g \in G$ with $\operatorname{ord}(g) = d+2$, and set $B = (-g)^{d+2} g^{d+2}$. Then for every $l \in \mathbb{N}$ we obviously have

$$\mathsf L(B^l) = 2l + \{\nu d \mid \nu \in [0, l]\} \in \mathcal L(G)\,,$$

whence $\mathcal L(G)$ contains arithmetical progressions with difference d and any length l.

2. *Multidimensional arithmetical progressions.* Let $r \in \mathbb{N}$, $d_1, \ldots, d_r \in \mathbb{N}$ and $l_1, \ldots, l_r \in \mathbb{N}$. For every $i \in [1, r]$, let G_i be a finite abelian group and $B_i^{l_i} \in \mathcal B(G_i)$ as in 1., such that $\mathsf L(B_i^{l_i})$ is an arithmetical progression with difference d_i and length l_i. If $G_1 \oplus \ldots \oplus G_r \subset G$ and $B = B_1^{l_1} \cdot \ldots \cdot B_r^{l_r}$, then

$$\mathsf L(B) = \sum_{i=1}^{r} \mathsf L(B_i) \in \mathcal L(G)$$

is an r-dimensional arithmetical progression.

3. *Arithmetical progressions with gaps at their end.* Let $n \ge 2$, $e_1, e_2 \in G$ independent elements with $\operatorname{ord}(e_1) = 2$, $\operatorname{ord}(e_2) = 2n$ and set $e_0 = e_1 + n e_2$. If $G_0 = \{e_0, e_1, e_2, -e_2\}$ and $U = e_0 e_1 e_2^n$, then

$$\mathcal A(G_0) = \{g^{\operatorname{ord}(g)} \mid g \in G_0\} \cup \big\{\big((-e_2)e_2\big), U, -U\big\}\,.$$

For every $l \in \mathbb{N}$ we consider

$$B_l = e_0^2 e_1^2 \big((-e_2)e_2\big)^{n+2nl}\,.$$

Let $B_l = A_1 \cdot \ldots \cdot A_k$ with $A_1, \ldots, A_k \in \mathcal{A}(G_0)$, and let $I \subset [1,k]$ be the set of all $i \in [1,k]$ such that $\operatorname{supp}(A_i) \cap \{e_0, e_1\} \ne \emptyset$. Then $|I| = 2$, say $I = \{1,2\}$, and we set $C_l = \prod_{i=3}^k A_i$. There are the following four possibilities:

- $\{A_1, A_2\} = \{e_0^2, e_1^2\}$. Then $C_l = \big((-e_2)e_2\big)^{n+2nl}$ and
$$\mathsf L(C_l) = n + 2l + \{\nu(2n-2) \mid \nu \in [0,l]\}\,.$$
- $\{A_1, A_2\} = \{-U, U\}$. Then $C_l = \big((-e_2)e_2\big)^{2nl}$ and
$$\mathsf L(C_l) = 2l + \{\nu(2n-2) \mid \nu \in [0,l]\}\,.$$
- $\{A_1, A_2\} = \{U\}$. Then $C_l = (-e_2)^{2n}\big((-e_2)e_2\big)^{n+2n(l-1)}$ and
$$\mathsf L(C_l) = 1 + n + 2(l-1) + \{\nu(2n-2) \mid \nu \in [0,l-1]\}\,.$$
- $\{A_1, A_2\} = \{-U\}$. Then $C_l = e_2^{2n}\big((-e_2)e_2\big)^{n+2n(l-1)}$ and
$$\mathsf L(C_l) = 1 + n + 2(l-1) + \{\nu(2n-2) \mid \nu \in [0,l-1]\}\,.$$

Thus we obtain that
$$\mathsf L(B_l) = 2 + 2l + \Big(\big((\mathcal D + (2n-2)\mathbb Z) \cap [0,(2n-2)l]\big) \cup \{n + (2n-2)l\}\Big)\ ,$$
where $\mathcal D = \{0, n-1, n, 2n-2\}$. In terms of the following definition, $\mathsf L(B_l)$ is an AAMP with difference $2n-2$, period $\mathcal D$, length l and bound n. If in particular $n = 2$, then $\mathsf L(B_l)$ is an arithmetical progression with difference 2 and a gap at its end.

4. *Arithmetical multiprogressions.* It can be shown that for every finite subset $L \subset \mathbb N_{\ge 2}$ there is a finite abelian group G_1 such that $L \in \mathcal L(G_1)$ ([71, Proposition 4.8.3]), say $L = \mathsf L(B_1) = x + \mathcal D$ where $x = \min L, \min \mathcal D = 0, \max \mathcal D = d$ and $B_1 \in \mathcal B(G_1)$. By 1., there is a group G_2 and a $B_2 \in \mathcal B(G_2)$ such that, for every $l \in \mathbb N$, $\mathsf L(B_2^l) = 2l + \{\nu d \mid \nu \in [0,l]\}$ is an arithmetical progression with difference d and length l. Thus for every $l \in \mathbb N$ we have
$$\begin{aligned}\mathsf L(B_1B_2^l) &= \mathsf L(B_1) + \mathsf L(B_2^l)\\ &= (x+2l) + \mathcal D + \{\nu d \mid \nu \in [0,l]\}\\ &= \min \mathsf L(B_1B_2^l) + \Big(\mathcal D + d\mathbb Z \cap [0, \max \mathsf L(B_1B_2^l) - \min \mathsf L(B_1B_2^l)]\Big)\,.\end{aligned}$$

Definition 5.7. Let $d \in \mathbb N$, l, $M \in \mathbb N_0$ and $\{0,d\} \subset \mathcal D \subset [0,d]$. A subset $L \subset \mathbb Z$ is called an

- *arithmetical multiprogression* (AMP for short) with *difference* d, *period* $\mathcal D$ and *length* l, if L is an interval of $\min L + \mathcal D + d\mathbb Z$ (this means that L is finite nonempty and $L = (\min L + \mathcal D + d\mathbb Z) \cap [\min L, \max L]$), and l is maximal such that $\min L + ld \in L$.
- *almost arithmetical multiprogression* (AAMP for short) with *difference* d, *period* $\mathcal D$, *length* l and *bound* M, if
$$L = y + (L' \cup L^* \cup L'') \subset y + \mathcal D + d\mathbb Z$$
where L^* is an AMP with difference d (whence $L^* \ne \emptyset$), period $\mathcal D$ and length l such that $\min L^* = 0$, $L' \subset [-M,-1]$, $L'' \subset \max L^* + [1,M]$ and $y \in \mathbb Z$.

  We call $y + L'$ the *initial part*, $y + L^*$ the *central part* and $y + L''$ the *end part* of L.
- *almost arithmetical progression* (AAP for short) with *difference* d, *bound* M and *length* l, if it is an AAMP with difference d, period $\{0,d\}$, bound M and length l.

Note that

- AMPs, AAMPs and AAPs are finite nonempty subsets of $\mathbb Z$.

- A set L is an AMP if and only if it is an AAMP with bound 0, and it is an arithmetical progression with difference d if and only if it is an AAP with difference d and bound 0.
- A set L is an AAMP if and only if the shifted set $y+L$ is an AAMP for any $y \in \mathbb{Z}$.
- $L^* = \big(\mathcal{D} + d\mathbb{Z}\big) \cap [0, \max L^*]$.

AAMPs, as defined above, were introduced in [38], and a slightly less restrictive notion was first defined in [67].

Definition 5.8. We say that *the Structure Theorem for Sets of Lengths holds for the monoid* H if H is atomic and there exist some $M^* \in \mathbb{N}_0$ and a finite nonempty set $\Delta^* \subset \mathbb{N}$ such that every $L \in \mathcal{L}(H)$ is an AAMP with some difference $d \in \Delta^*$ and bound M^*.

If the Structure Theorem for Sets of Lengths holds for the monoid H, then H is a BF-monoid with finite set of distances $\Delta(H)$ (note that the formulation in [71, Definition 4.7.1] is slightly different and erronous, since it was forgotten to require $\Delta^*(H)$ to be finite). We cite three key results on the structure of sets of lengths in Krull monoids (proofs can be found in [71, Section 4.7], [121] and [71, Theorem 7.6.9]).

Theorem 5.9. *Let* H *be a Krull monoid with finite class group* G*. Then the Structure Theorem for Sets of Lengths holds. Moreover, if* $|G| \ge 3$ *and every class contains a prime, then it holds with the set* $\Delta^* = \{\min \Delta(G_0) \mid G_0 \subset G \text{ with } \Delta(G_0) \ne \emptyset\} \subset \Delta(G)$*.*

Idea of the Proof. The proof splits into an abstract additive part and an ideal-theoretic part. Both steps are based on the concepts of *Pattern ideals* and of *Tamely generated ideals* which are defined as follows:

- For a finite nonempty set $A \subset \mathbb{Z}$ the pattern ideal $\Phi(A)$ is the set of all $a \in H$ for which there is some $y \in \mathbb{Z}$ such that $y + A \subset \mathsf{L}(a)$.
- A subset $\mathfrak{a} \subset H$ is called tamely generated if there exist a subset $E \subset \mathfrak{a}$ and a bound $N \in \mathbb{N}$ with the following property:
  For every $a \in \mathfrak{a}$ there exists some $e \in E$ such that $e \,|\, a$, $\sup \mathsf{L}(e) \le N$ and $\mathsf{t}(a, \mathsf{Z}(e)) \le N$.

In the additive part one proves that the Structure Theorem for Sets of Lengths holds for every BF-monoid H with finite set $\Delta(H)$ in which all pattern ideals are tamely generated. This is done in the spirit of additive number theory. To apply this additive result to a BF-monoid H, it must be proved that $\Delta(H)$ is finite and that all pattern ideals are tamely generated. This is fairly simple for finitely generated monoids (but far from being simple for C-monoids).

Let H be a Krull monoid as above and let $G_0 \subset G$ denote the set of classes containing primes. By Theorem 3.16 it suffices to prove the Structure Theorem for the monoid $\mathcal{B}(G_0)$ of zero-sum sequences over G_0. Since $\mathcal{B}(G_0)$ is finitely generated by Proposition 3.12, the assertion follows. □

Theorem 5.9 was recently generalized to Krull monoids with finite Davenport constant ([69]). More classes of monoids and domains where the Structure Theorem for Sets of Lengths holds can be found in [71, Section 4.7]. The next theorem is a realization result stating that Theorem 5.9 is sharp.

Theorem 5.10. *Let* $M \in \mathbb{N}_0$ *and* $\Delta^* \subset \mathbb{N}$ *be a finite nonempty set. Then there exists a Krull monoid* H *with finite class group such that the following holds: for every* AAMP L *with difference* $d \in \Delta^*$ *and bound* M *there is some* $y_{H,L} \in \mathbb{N}$ *such that*

$$y + L \in \mathcal{L}(H) \quad \text{for all} \quad y \ge y_{H,L}.$$

Indeed, there exists an algebraic number field such that its ring of integers has this property.

The next result is in a certain contrast to the previous two. In terms of zero-sum sequences it states that whenever the underlying set $\operatorname{supp}(S)$ of a given zero-sum sequence S is a group, then the factorizations of S are as nice as possible. Indeed, its catenary degree $\mathsf{c}(S)$ is bounded above by 3, and its set of lengths $\mathsf{L}(S)$ is an arithmetical progression with difference 1.

Theorem 5.11. *Let H be a Krull monoid with class group G and $a \in H$ such that*

$$\operatorname{supp}(\beta(a)) \cup \{0\} \subset G \quad \textit{is a subgroup}.$$

Then $\mathsf{c}(a) \le 3$ and hence the set of lengths $\mathsf{L}(a)$ is an arithmetical progression with difference 1.

The main tool in the proof of Theorem 5.11 is the following result on the structure of additively closed sequences (see [50] and [71, Theorem 7.5.2]).

Proposition 5.12. *Let $S, B, C \in \mathcal{F}(G^\bullet)$ be sequences such that $S = BC$, $|S| \ge 4$ and $|B| \ge |C|$. Suppose that, for all $g_1, g_2 \in G$,*

$$\textit{if} \quad g_1g_2 \,|\, B \quad \textit{or} \quad g_1g_2 \,|\, C \quad , \textit{then} \quad (g_1+g_2) \,|\, S\,.$$

Then S has a proper zero-sum subsequence, apart from the following exceptions:

1. *$|C| = 1$, and we are in one of the following cases:*
   - *$B = g^k$ and $C = 2g$ for some $k \ge 3$ and $g \in G$ with $\operatorname{ord}(g) \ge k+2$.*
   - *$B = g^k(2g)$ and $C = 3g$ for some $k \ge 2$ and $g \in G$ with $\operatorname{ord}(g) \ge k+5$.*
   - *$B = g_1g_2(g_1+g_2)$ and $C = g_1+2g_2$ for some $g_1, g_2 \in G$ with $\operatorname{ord}(g_1) = 2$ and $\operatorname{ord}(g_2) \ge 5$.*
2. *$\{B, C\} = \{\, g(9g)(10g)\,, (11g)(3g)(14g)\,\}$ for some $g \in G$ with $\operatorname{ord}(g) = 16$.*

Theorem 5.11 and some analytic machinery are the main ingredients to obtain the following density result (see [71, Theorem 9.4.11]). It states that the factorizations and hence the sets of lengths of "almost all" elements in a ring of integers are "as nice as possible".

Corollary 5.13. *Let K be an algebraic number field with ring of integers R and ideal class group G, and let $H = \{aR \mid a \in R^\bullet\}$ denote the monoid of non-zero principal ideals. For a principal ideal $a \in H$ let $|a| = (R\colon a)$ denote its norm. Then for every $x \ge 2$ we have*

$$\frac{\big|\{a \in H \mid \mathsf{c}(a) \le 3\,, |a| \le x\}\big|}{\big|\{a \in H \mid |a| \le x\}\big|} = 1 + O\big((\log x)^{-1/|G|}\big)\,.$$

5.C The characterization problem

Two reduced Krull monoids H and H' are isomorphic if and only if there is a group isomorphism $\Phi\colon \mathcal{C}(H) \to \mathcal{C}(H')$ such that for every class $g \in \mathcal{C}(H)$ the number of primes in g equals the number of primes in the class $\Phi(g) \in \mathcal{C}(H')$ (see [71, Theorem 2.5.4]). If H is the multiplicative monoid of the ring of integers of an algebraic number field, then the class group is finite and the set of primes in each class is denumerable. Thus the traditional idea in algebraic number theory, that the class group determines the arithmetic, is justified. Initiated by a problem of W. Narkiewicz in the 1970s, a huge variety of explicit results in this direction was derived.

If the class group of a Krull monoid H is finite and every class contains a prime, then, roughly speaking, the system of sets of factorizations $\mathcal{Z}(H) = \{\mathsf{Z}(a) \mid a \in H\}$ determines the class group (see [71, Sections 7.1 and 7.2]). The question arose, which is still wide open, whether the same is true for the system of sets of lengths. Clearly, if H and H' are reduced Krull monoids with isomorphic class groups G, G' and primes in all classes, then

$$\mathcal{L}(H) = \mathcal{L}(G) = \mathcal{L}(H')$$

but H and H' need not be isomorphic. By Proposition 3.12.4 it follows that

$$\mathcal{L}(C_1) = \{\{k\} \mid k \in \mathbb{N}_0\} = \mathcal{L}(C_2)\,,$$

and it is easy to check (details may be found in [71, Theorem 7.3.2]) that

$$\mathcal{L}(C_3) = \{y + 2k + [0,k] \mid y, k \in \mathbb{N}_0\} = \mathcal{L}(C_2 \oplus C_2)\,.$$

Note that $\mathsf{D}(C_3) = \mathsf{D}(C_2 \oplus C_2) = 3$, and $C_1, C_2, C_2 \oplus C_2$ and C_3 are the only finite abelian groups G' with $\mathsf{D}(G') \le 3$. So the best we can hope for is a positive answer to the following question:

> Given two finite abelian groups G and G' with $\mathsf{D}(G) \ge 4$ such that $\mathcal{L}(G) = \mathcal{L}(G')$. Does it follow that $G \cong G'$?

Up to now there is known no pair of non-isomorphic groups (G, G') with $\mathsf{D}(G) \ge 4$ and $\mathcal{L}(G) = \mathcal{L}(G')$. We start with some simple observations and then we gather the results known so far.

Proposition 5.14.

1. $\mathcal{L}(G) = \{y + L \mid y \in \mathbb{N}_0,\ L \in \mathcal{L}(G^\bullet)\} \supset \big\{\{y\} \bigm| y \in \mathbb{N}_0\big\}$, *and equality holds if and only if* $|G| \le 2$.
2. *If* $G_0 \subset G$ *is a subset, then* $\mathcal{L}(G_0) \subset \mathcal{L}(G)$.
3. *Let* G' *be an abelian group with* $|G'| \ge 3$ *such that* $\mathcal{L}(G) = \mathcal{L}(G')$. *Then we have* $\rho_k(G) = \rho_k(G')$ *and* $\lambda_k(G) = \lambda_k(G')$ *for every* $k \in \mathbb{N}$, $\mathsf{D}(G) = \mathsf{D}(G')$ *and* $\Delta(G) = \Delta(G')$.
4. *There exist (up to isomorphisms) only finitely many finite abelian groups* G' *such that* $\mathcal{L}(G) = \mathcal{L}(G')$.

Proof. 1. Observe that $\mathcal{B}(G) = \{0^y B \mid B \in \mathcal{B}(G^\bullet),\ y \in \mathbb{N}_0\}$, and if $B \in \mathcal{B}(G^\bullet)$ and $y \in \mathbb{N}_0$, then $\mathsf{L}(0^y B) = y + \mathsf{L}(B)$. By definition, we have $|L| = 1$ for every $L \in \mathcal{L}(G)$ if and only if $\mathcal{B}(G)$ is half-factorial, and by Proposition 3.12 this is equivalent to $|G| \le 2$.

2. Obvious.

3. By 1. we obtain $|G| \ge 3$. By the very definition we have $\Delta(G) = \Delta(G')$, $\lambda_k(G) = \lambda_k(G')$ and $\rho_k(G) = \rho_k(G')$ for every $k \in \mathbb{N}$, and hence $\mathsf{D}(G) = \rho_2(G) = \rho_2(G') = \mathsf{D}(G')$ by Theorem 4.11.3.

4. If G' is an abelian group with $\mathcal{L}(G) = \mathcal{L}(G')$ and $|G'| \ge 3$, then it follows that $\mathsf{D}(G) = \mathsf{D}(G') \ge 1 + \mathsf{d}^*(G')$ (see Lemma 4.3.2). By the very definition of $\mathsf{d}^*(\cdot)$, there are up to isomorphisms only finitely many finite abelian groups G' with $\mathsf{d}^*(G') < \mathsf{D}(G)$. □

Proposition 5.15. *Let* G' *be a finite abelian group with* $\mathsf{D}(G') \in [4, 10]$.
If $\mathcal{L}(G) = \mathcal{L}(G')$, *then* $G \cong G'$.

Theorem 5.16. *Let* G *be a finite elementary* p*-group and let* G' *be a finite elementary* q*-group with* $\mathsf{D}(G') \ge 4$ *and with primes* $p, q \in \mathbb{P}$. *If* $\mathcal{L}(G) = \mathcal{L}(G')$, *then* $G \cong G'$.

Theorem 5.17. *Let* G' *be a finite abelian group with* $\mathsf{D}(G') \ge 4$ *and suppose that one of the following statements hold*:

1. G *is cyclic.*
2. G *is an elementary* 2*-group.*
3. $G \cong C_2 \oplus C_{2n}$ *with* $n \ge 2$.
4. $G \cong C_n \oplus C_n$ *with* $n \ge 3$.

If $\mathcal{L}(G) = \mathcal{L}(G')$, *then* $G \cong G'$.

The results given in 5.15, 5.16 and 5.17 are mainly due to Wolfgang A. Schmid (see [122, 124, 119] and [71, Section 7.3]). They are based on solid investigations of the set $\Delta^*(G) = \{\min \Delta(G_0) \mid G_0 \subset G \text{ with } \Delta(G_0) \ne \emptyset\}$, which occurs in Theorem 5.9. We do not discuss these topics here, but using results on the $\rho_k(G)$-invariants we will be able prove Theorem 5.17 for cyclic groups and for elementary 2-groups (see Corollary 7.28).

6. Addition theorems and direct zero-sum problems

We start with the classical theorems of Kneser and Kemperman-Scherk which are fundamental in additive group theory. Having these results at our disposal we continue the investigation of the Davenport constant, of the Erdős-Ginzburg-Ziv constant and of related invariants in zero-sum theory.

6.A The Theorems of Kneser and of Kemperman-Scherk

Let $k \in \mathbb N$ and $A, B, A_1, \ldots, A_k \subset G$ be nonempty subsets. Then

$$\operatorname{Stab}(A) = \{g \in G \mid g + A = A\}$$

denotes the *stabilizer* of A, which is a subgroup of A. For $g \in G$, let

$$\mathsf r_{A_1,\ldots,A_k}(g) = \Big| \Big\{(a_1, \ldots, a_k) \in A_1 \times \ldots \times A_k \mid g = a_1 + \ldots + a_k\Big\} \Big|$$

denote the number of representations of g as a sum of elements of $A_1, \ldots, A_k$. In particular, we have

$$r_{A,B}(g) = |\{(a, b) \in A \times B \mid g = a + b\}| = |A \cap (g - B)|\,.$$

In the 1950s M. Kneser proved the following addition theorem formulated in Theorem 6.1. Since a proof is given in the Part "Sumsets and Structure" by Imre Z. Ruzsa, we do not give a proof here. Moreover, a variety of proofs and historical references may be found in each of the following monographs [104, Chapter 1], [107, Chapter 4], [71, Section 5.2], and [130, Theorem 5.5]. For some recent development around Kneser's Theorem, and in particular on the isoperimetric approach, we refer to [22, 83, 126, 97, 19, 81, 25, 24, 3, 89, 90, 93, 91, 80].

Theorem 6.2 was first proved by J.H.B. Kemperman ([98]; the special case $\min\{\, r_{A,B}(g) \mid g \in A{+}B\} = 1$ was settled before by P. Scherk answering a question of L.Moser [118]; a short proof of Scherk's Theorem, which is not based on Kneser's Theorem, may be found in [90]). Corollary 6.3 is crucial in many investigations on the structure of zero-sum free sequences (as for example in the proofs of Proposition 6.9 and Corollary 7.10).

Theorem 6.1 (Kneser). *Let $K = \operatorname{Stab}(A + B)$ be the stabilizer of $A + B$.*

1. *There exists a subgroup $K' \subset K$ such that $|A + B| \ge |A| + |B| - |K'|$.*
2. *There exists a subgroup $K' \subset K$ such that $|A + B| \ge |A + K'| + |B + K'| - |K'|$.*
3. $|A + B| \ge |A + K| + |B + K| - |K|$.
4. *Either $|A + B| \ge |A| + |B|$ or $|A + B| = |A + K| + |B + K| - |K|$.*

Theorem 6.2 (Kemperman-Scherk). *Let $K = \operatorname{Stab}(A + B)$ be the stabilizer of $A + B$. Then*

$$\begin{aligned} |A + B| &\ge |A| + |B| - \min\{\, r_{(a+K)\cap A,(b+K)\cap B}\,(g) \mid a \in A,\ b \in B,\ g \in a + b + K\} \\ &\ge |A| + |B| - \min\{\, r_{A,B}(g) \mid g \in A + B\}\,. \end{aligned}$$

Proof. If $a \in A,\ b \in B$ and $g \in a+b+K$, then $r_{(a+K)\cap A,(b+K)\cap B}\,(g) \le r_{A,B}(g)$, and therefore

$$\begin{aligned}&\min\{r_{(a+K)\cap A,(b+K)\cap B}\,(g) \mid a \in A,\ b \in B,\ g \in a+b+K\}\\ &\quad\le \min\{r_{A,B}(g) \mid a \in A,\, b \in B,\, g \in a+b+K\}\\ &\quad= \min\{r_{A,B}(g) \mid g \in A+B+K\} = \min\{r_{A,B}(g) \mid g \in A+B\}\,.\end{aligned}$$

Thus it suffices to prove the first inequality. We may assume that $|A+B| < |A|+|B|$, and then $|A+B| = |A+K|+|B+K|-|K|$ by Theorem 6.1.4.

Suppose that $a \in A,\ b \in B$ and $g \in a+b+K$. By definition, we have

$$r_{(a+K)\cap A,(b+K)\cap B}\,(g) = |C_1 \cap C_2|\,,$$

where $C_1 = (a+K)\cap A$ and $C_2 = g - [(b+K)\cap B]$, and thus we must prove that $|C_1 \cap C_2| \ge |A|+|B|-|A+B|$. Since $C_1 \cup C_2 \subset a+K$, we obtain

$$\begin{aligned}|C_1 \cap C_2| &= |C_1|+|C_2|-|C_1 \cup C_2| \ge |C_1|+|C_2|-|a+K|\\ &= |(a+K)\cap A| + |(b+K)\cap B| - |K|\\ &= |a+K| - |(a+K)\setminus A| + |b+K| - |(b+K)\setminus B| - |K|\\ &\ge |K| - |(A+K)\setminus A| - |(B+K)\setminus B|\\ &= |K| - |A+K| + |A| - |B+K| + |B| = |A|+|B|-|A+B|\,. \quad \square\end{aligned}$$

Corollary 6.3. *Let* $k \in \mathbb{N}$.

1. *Let* $A_1, \ldots, A_k \subset G$ *be nonempty subsets. Then*
$$|A_1+\ldots+A_k| \ge |A_1|+\ldots+|A_k| - (k-2) - \min\{r_{A_1,\ldots,A_k}(g) \mid g \in A_1+\ldots+A_k\}\,.$$
2. *If* $S = S_1 \cdot \ldots \cdot S_k \in \mathcal{A}^*(G)$, *then*
$$|\Sigma(S)| \ge |\Sigma(S_1)| + \ldots + |\Sigma(S_k)|\,.$$

Proof. 1. We proceed by induction on k. For $k=1$ the assertion is clear. Suppose that $k \ge 2$. We start with the following assertion.

A. For every $g \in A_1+\ldots+A_k$ we have

$$r_{A_1,\ldots,A_k}(g) \ge \min\{r_{A_1,\ldots,A_{k-1}}(a) \mid a \in A_1+\ldots+A_{k-1}\} + \min\{r_{A_1+\ldots+A_{k-1},A_k}(b) \mid b \in A_1+\ldots+A_k\} - 1\,.$$

Proof of **A**. If $g \in A_1+\ldots+A_k$, then we get

$$\begin{aligned}r_{A_1,\ldots,A_k}(g) &\ge \min\{r_{A_1,\ldots,A_{k-1}}(a) \mid a \in A_1+\ldots+A_{k-1}\} \cdot r_{A_1+\ldots+A_{k-1},A_k}(g)\\ &\ge \min\{r_{A_1,\ldots,A_{k-1}}(a) \mid a \in A_1+\ldots+A_{k-1}\} \min\{r_{A_1+\ldots+A_{k-1},A_k}(b) \mid b \in A_1+\ldots+A_k\}\\ &\ge \min\{r_{A_1,\ldots,A_{k-1}}(a) \mid a \in A_1+\ldots+A_{k-1}\} + \min\{r_{A_1+\ldots+A_{k-1},A_k}(b) \mid b \in A_1+\ldots+A_k\} - 1\,.\end{aligned}$$

Now the induction hypothesis, Theorem 6.2 and **A** imply that

$$\begin{aligned}|A_1+\ldots+A_k| &\ge |A_1+\ldots+A_{k-1}| + |A_k| - \min\{r_{A_1+\ldots+A_{k-1},A_k}(b) \mid b \in A_1+\ldots+A_k\}\\ &\ge |A_1|+\ldots+|A_{k-1}| - (k-3) - \min\{r_{A_1,\ldots,A_{k-1}}(a) \mid a \in A_1+\ldots+A_{k-1}\}\\ &\qquad + |A_k| - \min\{r_{A_1+\ldots+A_{k-1},A_k}(b) \mid b \in A_1+\ldots+A_k\}\\ &\ge |A_1|+\ldots+|A_k| - (k-2) - \min\{r_{A_1,\ldots,A_k}(g) \mid g \in A_1+\ldots+A_k\}\,.\end{aligned}$$

2. For $i \in [1,k]$ we set $A_i = \Sigma(S_i) \cup \{0\}$. Then $r_{A_1,\ldots,A_k}(0) = 1$, and hence 1. implies that

$$|\Sigma(S)| \ge |A_1+\ldots+A_k| - 1 \ge |A_1|+\ldots+|A_k| - k = |\Sigma(S_1)|+\ldots+|\Sigma(S_k)|\,. \qquad \square$$

6.B On the Erdős-Ginzburg-Ziv constant $\mathsf{s}(G)$ and on some of its variants

Definition 6.4. Let $\exp(G) = n$.

1. A sequence $S \in \mathcal{F}(G)$ is called *short* (in G) if $|S| \in [1, n]$.
2. We denote by $\eta(G)$ the smallest integer $l \in \mathbb{N}$ with the following property:
   - Every sequence $S \in \mathcal{F}(G)$ of length $|S| \ge l$ has a short zero-sum subsequence.
3. We denote by $\mathsf{s}(G)$ the smallest integer $l \in \mathbb{N}$ with the following property:
   - Every sequence $S \in \mathcal{F}(G)$ of length $|S| \ge l$ has a zero-sum subsequence T of length $|T| = n$.

   The invariant $\mathsf{s}(G)$ will be called the *Erdős-Ginzburg-Ziv constant* (EGZ constant for short).
4. We denote by $\mathsf{s}_{n\mathbb{N}}(G)$ the smallest integer $l \in \mathbb{N}$ with the following property:
   - Every sequence $S \in \mathcal{F}(G)$ of length $|S| \ge l$ has a nontrivial zero-sum subsequence T of length $|T| \equiv 0 \mod n$.

The investigation of these invariants has a long tradition in combinatorial number theory as well as in finite geometry. Indeed, the Erdős-Ginzburg-Ziv Theorem, first proved in 1961 ([32]) and stating that $\mathsf{s}(C_n) = 2n - 1$ (see Corollary 6.11), is considered as a starting point in zero-sum theory. As already pointed out by H. Harborth ([94]), $\mathsf{s}(C_n^r)$ is the smallest integer $l \in \mathbb{N}$ such that every set of l lattice point in an r-dimensional euclidean space contains n elements which have a centroid with integral coordinates. Moreover, if φ is the maximal size of a cap in $\mathrm{AG}(r, 3)$, then $\mathsf{s}(C_3^r) = 2\varphi + 1$ (see [28, Section 5] for the connection to finite geometry).

The invariant $\eta(G)$ is a crucial tool in the inductive method which roughly works as follows: for the investigation of a given sequence $S \in \mathcal{F}(G)$ proceed in the following three steps:

- Find a suitable subgroup $K \subset G$ and consider the natural epimorphism $\varphi \colon G \to G/K$.
- Consider a factorization $S = S_0 S_1 \cdot \ldots \cdot S_k$ such that $|S_i|$ is small and $\varphi(S_i) \in \mathcal{B}(G/K)$ for all $i \in [1, k]$.
- Investigate the sequences $T = \sigma(S_1) \cdot \ldots \cdot \sigma(S_k) \in \mathcal{F}(K)$ and $S_0 T \in \mathcal{F}(G)$. Clearly, if S is zero-sum free, then $S_0 T$ is zero-sum free too.

The inductive method was already used successfully by J.E. Olson and P. van Emde Boas in the 1960s, and then it was more and more refined by W. Gao and many other authors. After having done the necessary preparations in Lemmas 6.7 and 6.8 we will demonstrate the power of this method in 6.13 and 6.15 (the polynomial method - see the article "The polynomial method in additive combinatorics" by G. Károlyi in Part III - and coverings by cosets - see [71, Chapter 5.6], [128, 102] - are further important methods, which however cannot be discussed here).

Our main result in this subsection is Theorem 6.13 which gives, for groups G of rank $\mathsf{r}(G) \le 2$, the precise values of $\mathsf{d}(G)$, $\eta(G)$ and $\mathsf{s}(G)$. For $\mathsf{d}(G)$ this was shown independently by J.E. Olson and D. Kruyswijk in the late 1960s. The result on $\mathsf{s}(G)$ is based on C. Reiher's work ([114]). The proof of 6.13, as presented here, follows the lines from [71, Theorem 5.8.3]. On our way we show the Theorem of Erdős-Ginzburg-Ziv (Corollary 6.11; for some recent development in the flavor of Erdős-Ginzburg-Ziv see [40, 39, 82, 84, 86]).

Lemma 6.5.

1. *We have* $\mathsf{D}(G) \le \eta(G) \le \mathsf{s}(G) - \exp(G) + 1$.
2. *Let* $G = C_{n_1} \oplus \cdots \oplus C_{n_r}$ *with* $r = \mathsf{r}(G)$ *and* $1 < n_1 \mid \ldots \mid n_r$. *If* $r \ge 2$, *then* $\eta(G) \ge \mathsf{d}^*(G) + n_1$.

Proof. 1. The inequality $\mathsf{D}(G) \le \eta(G)$ follows by Lemma 4.2.3 and the very definition of $\eta(G)$. For the proof of the second inequality let $n = \exp(G)$, and consider a sequence $S \in \mathcal{F}(G)$ of length $|S| \ge \mathsf{s}(G) - n + 1$. We must prove that S has a short zero-sum subsequence. The sequence $T = 0^{n-1} S \in \mathcal{F}(G)$ satisfies $|T| \ge \mathsf{s}(G)$, and therefore there exists a zero-sum subsequence $T' = 0^k S'$ of T, where $k \in [0, n-1]$, $S' \mid S$ and $|T'| = |S'| + k = n$. Hence S' is a short zero-sum subsequence of S.

2. Let $r \ge 2$ and $(e_1, \ldots, e_r)$ be a basis of G such that $\operatorname{ord}(e_i) = n_i$ for all $i \in [1, r]$,

$$e_0 = \sum_{i=1}^{r} e_i \quad \text{and} \quad S = e_0^{n_1-1} \prod_{i=1}^{r} e_i^{n_i-1} \in \mathcal{F}(G)\,.$$

We assert that S has no short zero-sum subsequence. Let

$$T = e_0^{n_0} \prod_{i=1}^{r} e_i^{n_i'}\,, \quad \text{where} \quad n_0 \in [0, n_1-1] \ \text{and} \ n_i' \in [0, n_i-1] \ \text{for all} \ i \in [1, r],$$

be a nontrivial zero-sum subsequence of S. Then $n_0 \ge 1$ by Lemma 4.3. Since $0 = \sigma(T) = (n_1' + n_0)e_1 + \ldots + (n_r' + n_0)e_r$, it follows that $n_i' + n_0 \equiv 0 \mod n_i$ for all $i \in [1, r]$, and $1 \le n_i' + n_0 \le 2n_i - 2$ implies $n_i' = n_i - n_0$ for all $i \in [1, r]$. Hence

$$|T| = n_0 + \sum_{i=1}^{r} (n_i - n_0) = n_r + \sum_{i=1}^{r-1} (n_i - n_0) > n_r = \exp(G)\,,$$

and thus T is not a short zero-sum sequence of S over G. □

Lemma 6.6. *Let $S \in \mathcal{F}(G)$ and $n \ge 2$.*

1. *If $|S| \ge \mathsf{D}(G \oplus C_n)$ and $\mathsf{D}(G \oplus C_n) \le 3n - 1$, then S has a zero-sum subsequence $T \in \mathcal{B}(G)$ of length $|T| \in \{n, 2n\}$.*
2. *Suppose that $\mathsf{D}(G) \le 2n - 1$, $\mathsf{D}(G \oplus C_n) \le 3n - 1$ and $|S| \ge \mathsf{D}(G \oplus C_n)$. Then S has a zero-sum subsequence $T \in \mathcal{B}(G)$ of length $|T| \in [1, n]$. In particular, if $n \le \exp(G)$, then $\eta(G) \le \mathsf{D}(G \oplus C_n)$.*
3. *If $\exp(G) = n$, then*
$$\mathsf{D}(G) + n - 1 \le \mathsf{s}_{n\mathbb{N}}(G) \le \min\{\mathsf{s}(G), \mathsf{D}(G \oplus C_n)\}.$$

Proof. Let $G \oplus C_n = G \oplus \langle e \rangle$ with $\operatorname{ord}(e) = n$, so that every $h \in G \oplus C_n$ has a unique representation $h = g + je$, where $g \in G$ and $j \in [0, n-1]$. We define $\varphi\colon G \to G \oplus C_n$ by $\varphi(g) = g + e$ for every $g \in G$.

1. Since $\varphi(S) \in \mathcal{F}(G \oplus C_n)$ and $|\varphi(S)| = |S| \ge \mathsf{D}(G \oplus C_n)$, S has a subsequence T with $1 \le |T| \le \mathsf{D}(G \oplus C_n) \le 3n - 1$ such that $\varphi(T)$ has sum zero. Because $0 = \sigma\big(\varphi(T)\big) = \sigma(T) + |T|e \in G \oplus C_n$, we obtain that $\sigma(T) = 0$, $|T| \equiv 0 \mod n$, and $|T| \le 3n - 1$ implies $|T| \in \{n, 2n\}$.

2. If $|S| \ge \mathsf{D}(G \oplus C_n)$, then by 1. there exists a zero-sum subsequence T of S such that $|T| \in \{n, 2n\}$. If $|T| \le n$, we are done. If $|T| = 2n$, then $|T| > \mathsf{D}(G)$ implies $T = T_1T_2$ for some zero-sum subsequences T_1, T_2 with $1 \le |T_1| \le |T_2|$, and T_1 is the desired subsequence of S.

3. If $S \in \mathcal{F}(G)$ is a zero-sum free sequence of length $|S| = \mathsf{D}(G) - 1$, then the sequence $0^{n-1}S$ has no zero-sum subsequence of length divisible by n. Thus $\mathsf{D}(G) + n - 2 = |0^{n-1} \cdot S| < \mathsf{s}_{n\mathbb{N}}(G)$. By definition we have $\mathsf{s}_{n\mathbb{N}}(G) \le \mathsf{s}(G)$.

In order to verify that $\mathsf{s}_{n\mathbb{N}}(G) \le \mathsf{D}(G \oplus C_n)$, let $S = \prod_{i=1}^{l} g_i \in \mathcal{F}(G)$ with $l = \mathsf{D}(G \oplus C_n)$. Then the sequence $\prod_{i=1}^{l} (g_i + e) \in \mathcal{F}(G \oplus C_n)$ has a zero-sum subsequence T of length $|T| \equiv 0 \mod n$, and whence the same is true for S. □

Lemma 6.7. *Let $\varphi\colon G \to \overline{G}$ be a group homomorphism and $k \in \mathbb{N}$.*

1. *If $S \in \mathcal{F}(G)$ and $|S| \ge (k-1)\exp(\overline{G}) + \mathsf{s}(\overline{G})$, then S admits a product decomposition $S = S_1 \cdot \ldots \cdot S_k S'$, where $S_1, \ldots, S_k, S' \in \mathcal{F}(G)$ and, for every $i \in [1, k]$, $\varphi(S_i)$ has sum zero and length $|S_i| = \exp(\overline{G})$.*
2. *If $S \in \mathcal{F}(G)$ and $|S| \ge (k-1)\exp(\overline{G}) + \eta(\overline{G})$, then S admits a product decomposition $S = S_1 \cdot \ldots \cdot S_k S'$, where $S_1, \ldots, S_k, S' \in \mathcal{F}(G)$ and, for every $i \in [1, k]$, $\varphi(S_i)$ has sum zero and length $|S_i| \in [1, \exp(\overline{G})]$.*

Proof. 1. Suppose that for some $j \in [0, k-1]$ we have found a product decomposition $S = S_1 \cdot \ldots \cdot S_j S'$ where $S_1, \ldots, S_j, S' \in \mathcal{F}(G)$ and, for every $i \in [1, j]$, $\varphi(S_i)$ has sum zero and length $|S_i| = \exp(\overline{G})$. Then

$$|\varphi(S')| = |S'| = |S| - j \exp(\overline{G}) \ge \big(k - 1 - j\big) \exp(\overline{G}) + \mathsf{s}(\overline{G}) \ge \mathsf{s}(\overline{G}) ,$$

and therefore S' has a subsequence S_{j+1} such that $\varphi(S_{j+1})$ has sum zero and length $|S_{j+1}| = \exp(\overline{G})$. Now the assertion follows by induction on j.

2. This is proved in precisely the same way as 1. □

Lemma 6.8. *Let $K \subset G$ be a subgroup.*

1. *If $S \in \mathcal{F}(G)$ and $|S| \ge (\mathsf{s}(K) - 1) \exp(G/K) + \mathsf{s}(G/K)$, then S has a zero-sum subsequence T of length $|T| = \exp(K) \exp(G/K)$. In particular, if $\exp(G) = \exp(K) \exp(G/K)$, then*
$$\mathsf{s}(G) \le (\mathsf{s}(K) - 1) \exp(G/K) + \mathsf{s}(G/K) .$$
2. *If $S \in \mathcal{F}(G)$ and $|S| \ge (\eta(K) - 1) \exp(G/K) + \eta(G/K)$, then S has a zero-sum subsequence T of length $1 \le |T| \le \exp(K) \exp(G/K)$. In particular, if $\exp(G) = \exp(K) \exp(G/K)$, then*
$$\eta(G) \le (\eta(K) - 1) \exp(G/K) + \eta(G/K) .$$
3. $\mathsf{d}(G) \le \mathsf{d}(K) \exp(G/K) + \max\big\{\mathsf{d}(G/K), \eta(G/K) - \exp(G/K) - 1\big\}$.

Proof. Let $\varphi \colon G \to G/K$ denote the canonical epimorphism. If $K = \{0\}$, then all assertions are obvious. Suppose that $K \ne \{0\}$.

1. Let $S \in \mathcal{F}(G)$ be a sequence with $|S| \ge (\mathsf{s}(K) - 1) \exp(G/K) + \mathsf{s}(G/K)$. By Lemma 6.7.1, S has a product decomposition $S = S_1 \cdot \ldots \cdot S_{\mathsf{s}(K)} S'$, where $S_1, \ldots, S_{\mathsf{s}(K)}, S' \in \mathcal{F}(G)$ and, for every $i \in [1, \mathsf{s}(K)]$, $\varphi(S_i)$ has sum zero and length $|S_i| = \exp(G/K)$. Then the sequence $\sigma(S_1) \cdot \ldots \cdot \sigma(S_{\mathsf{s}(K)}) \in \mathcal{F}(K)$ has a zero-sum subsequence V of length $|V| = \exp(K)$, say

$$V = \prod_{i \in I} \sigma(S_i) , \quad \text{where} \quad I \subset [1, \mathsf{s}(K)] \quad \text{and} \quad |I| = \exp(K) .$$

Thus the sequence

$$T = \prod_{i \in I} S_i$$

is a zero-sum subsequence of S of length $|T| = |I| \exp(G/K) = \exp(K) \exp(G/K)$.

2. This is proved in precisely the same way as 1.

3. Let $S \in \mathcal{F}(G)$ be a sequence of length

$$|S| > \mathsf{d}(K) \exp(G/K) + \max\big\{\mathsf{d}(G/K), \eta(G/K) - \exp(G/K) - 1\big\} .$$

We must prove that S is not zero-sum free. Since $|S| \ge (\mathsf{d}(K) - 1) \exp(G/K) + \eta(G/K)$, Lemma 6.7.2 provides us with a product decomposition $S = S_1 \cdot \ldots \cdot S_{\mathsf{d}(K)} S'$, where $S_1, \ldots, S_{\mathsf{d}(K)}, S' \in \mathcal{F}(G)$ and, for every $i \in [1, \mathsf{d}(K)]$, $\varphi(S_i)$ has sum zero and length $|S_i| \in [1, \exp(G/K)]$. Now we obtain $|S'| \ge |S| - \exp(G/K)\mathsf{d}(K) > \mathsf{d}(G/K)$, and therefore S' has a nontrivial subsequence S_0 such that $\varphi(S_0)$ has sum zero. Hence $V = \sigma(S_0)\sigma(S_1) \cdot \ldots \cdot \sigma(S_{\mathsf{d}(K)}) \in \mathcal{F}(K)$, and $|V| > \mathsf{d}(K)$ implies that V is not zero-sum free. Hence $T = S_0 S_1 \cdot \ldots \cdot S_{\mathsf{d}(K)}$ is a subsequence of S which is not zero-sum free. □

The following result was found independently by several authors. Its history is described in [92].

Proposition 6.9. *Let $S \in \mathcal{F}(G)$ be a sequence of length $|S| \ge |G|$ and $k' = \max\{\operatorname{ord}(g) \mid g \in \operatorname{supp}(S)\}$. Then S has a nontrivial zero-sum subsequence T of length $|T| \le \min\{\mathsf{h}(S), k'\}$.*

Proof. We set $k = \mathsf{h}(S)$. If $k' \le k$, let $g \in G$ be such that $\mathsf{v}_g(S) = k$. Then $T = g^{\operatorname{ord}(g)}$ has the desired property. Hence it is sufficient to prove that S has a zero-sum subsequence of T of length $|T| \in [1, k]$. If $0 \in \operatorname{supp}(S)$, we set $T = 0$. Thus suppose that $0 \notin \operatorname{supp}(S)$. There exists a decomposition $S = S_1 \cdot \ldots \cdot S_k$, where $S_1, \ldots, S_k \in \mathcal{F}(G)$ are squarefree. For $i \in [1, k]$, let $B_i = \operatorname{supp}(S_i)$, $A_i = B_i \cup \{0\}$, and assume that S has no zero-sum subsequence as required. This implies that $r_{A_1, \ldots, A_k}(0) = 1$, and thus Corollary 6.3 implies that

$$|A_1 + \ldots + A_k| \ge |A_1| + \ldots + |A_k| - k + 1 = |B_1| + \ldots + |B_k| + 1 = |G| + 1\,,$$

a contradiction. □

Theorem 6.10 (Gao)**.** *We have* $\eta(G) \le |G|$ *and* $\mathsf{s}(G) \le |G| + \exp(G) - 1$.

Proof. The first inequality is an immediate consequence of Proposition 6.9. In order to verify the upper bound for $\mathsf{s}(G)$, we set $n = \exp(G)$ and must prove that every sequence $S \in \mathcal{F}(G)$ of length $|S| \ge |G| + n - 1$ has a zero-sum subsequence of length n. Thus assume that

$$S = g_1^{k_1} \cdot \ldots \cdot g_l^{k_l} \in \mathcal{F}(G)\,,$$

where $|S| \ge |G| + n - 1$, $k = k_1 \ge \cdots \ge k_l \ge 1$ and $g_1, \ldots, g_l \in G$ are distinct. If $k \ge n$, then g_1^n is a zero-sum subsequence of length n. Therefore we assume that $k \le n - 1$ and $l \ge 2$, and we consider the sequence

$$U = (g_2 - g_1)^{k_2} \cdot \ldots \cdot (g_l - g_1)^{k_l} \in \mathcal{F}(G)\,.$$

It is sufficient to prove that U has a zero-sum subsequence V such that $n - k \le |V| \le n$. Indeed, if $V = (g_2 - g_1)^{k_2'} \cdot \ldots \cdot (g_l - g_1)^{k_l'}$ is such a zero-sum subsequence, where $k_i' \in [0, k_i]$ for all $i \in [2, l]$ and $n - k \le k_2' + \ldots + k_l' \le n$, then $0 \le n - (k_2' + \ldots + k_l') \le k$, and the sequence

$$T = g_1^{n - (k_2' + \ldots + k_l')} g_2^{k_2'} \cdot \ldots \cdot g_l^{k_l'}$$

is a zero-sum subsequence of S of length n.

Since $|U| = |S| - k \ge |G| + n - 1 - k \ge |G|$ and $\eta(G) \le |G|$, it follows that U has a short zero-sum subsequence. Let V be a short zero-sum subsequence of U of maximal length and assume, contrary to our requirement, that $|V| \le n - k - 1$. If $U = VV'$, then $|V'| = |U| - |V| \ge (|G| + n - 1 - k) - (n - k - 1) = |G|$, and by Proposition 6.9 it follows that V' has a zero-sum subsequence V'' of length

$$1 \le |V''| \le \max\{\mathsf{v}_g(V') \mid g \in G\} \le \max\{\mathsf{v}_g(U) \mid g \in G\} \le k\,.$$

Then VV'' is a zero-sum subsequence of U of length

$$|V| < |VV''| = |V| + |V''| \le (n - k - 1) + k = n - 1,$$

a contradiction to the maximality of $|V|$. □

In the same spirits (using 6.9 and 6.10) W. Gao proved that $|G| + \mathsf{d}(G)$ is the smallest integer $l \in \mathbb{N}$ such that every sequence $T \in \mathcal{F}(G)$ of length $|T| \ge l$ has a zero-sum subsequence of length $|G|$ (see ([42] and [71, Proposition 5.7.9]). There is a weighted generalization of this theorem by Y. ould Hamidoune [92] and for more of this flavor see [66, 1, 84, 78, 85]). For cyclic groups Gao's Theorem 6.10 reduces to the classical result of Erdős-Ginzburg-Ziv.

Corollary 6.11 (Erdős-Ginzburg-Ziv)**.** *For every* $n \in \mathbb{N}$ *we have*

$$\eta(C_n) = n \quad \textit{and} \quad \mathsf{s}(C_n) = 2n - 1\,.$$

Proof. By Lemma 6.5 and Theorem 6.10, we obtain

$$n = \mathsf{D}(C_n) \le \eta(C_n) \le |C_n| = n$$

and thus $\eta(C_n) = n$. Again by Lemma 6.5 and by Theorem 6.10 we get

$$2n-1 = \eta(C_n) + \exp(C_n) - 1 \le \mathsf{s}(C_n) \le |C_n| + \exp(C_n) - 1 = 2n-1$$

and thus $\mathsf{s}(C_n) = 2n-1$. □

Proposition 6.12 (Reiher). *For every prime $p \in \mathbb{P}$ we have $\mathsf{s}(C_p \oplus C_p) \le 4p-3$.*

Proof. The original proof by C. Reiher (see [114]) is based on the Theorem of Chevalley-Warning (see [130, Theorem 9.24]). A proof using group algebras may be found in [71, Proposition 5.8.1], and for a generalization see [125]. □

Theorem 6.13. *Let $G = C_{n_1} \oplus C_{n_2}$ with $1 \le n_1 \,|\, n_2$. Then*

$$\mathsf{s}(G) = 2n_1 + 2n_2 - 3\,, \quad \eta(G) = 2n_1 + n_2 - 2 \quad \textit{and} \quad \mathsf{d}(G) = n_1 + n_2 - 2 = \mathsf{d}^*(G)\,.$$

Proof. By Corollaries 6.11 and 4.4, the result holds for $n_1 = 1$. Suppose that $n_1 > 1$ and note that $\exp(G) = n_2$. By Lemma 4.3 we have $\mathsf{d}^*(G) \le \mathsf{d}(G)$. Now Lemma 6.5 implies that

$$\eta(G) \ge 2n_1 + n_2 - 2 \quad \text{and} \quad \mathsf{s}(G) \ge \eta(G) + n_2 - 1 \ge 2n_1 + 2n_2 - 3\,.$$

Thus it remains to show that $\mathsf{s}(G) \le 2n_1 + 2n_2 - 3$ and $\mathsf{d}(G) \le n_1 + n_2 - 2$.

We use induction on $\exp(G)$. If $p \in \mathbb{P}$ and $G = C_p \oplus C_p$, then $\mathsf{d}(G) = 2p-2$ by Theorem 4.10, and Proposition 6.12 implies $\mathsf{s}(G) \le 4p-3$.

Assume now that $p \in \mathbb{P}$, $p \,|\, n_1$, $p < n_2$ and set $m_i = p^{-1} n_i$ for $i \in \{1,2\}$. Then the assertions are true for the groups $pG \cong C_{m_1} \oplus C_{m_2}$ and $G/pG \cong C_p \oplus C_p$. By Lemma 6.8.1 we obtain

$$\mathsf{s}(G) \le \big(\mathsf{s}(pG) - 1\big)p + \mathsf{s}(G/pG) \le (2m_1 + 2m_2 - 4)p + (4p-3) = 2n_1 + 2n_2 - 3\,,$$

and Lemma 6.8.3 implies

$$\begin{aligned} \mathsf{d}(G) \le\ & \mathsf{d}(pG)p + \max\big\{\mathsf{d}(G/pG),\, \eta(G/pG) - p - 1\big\} \\ =\ & (m_1 + m_2 - 2)p + \max\big\{2p-2,\, (3p-2) - p - 1\big\} = n_1 + n_2 - 2\,. \quad \square \end{aligned}$$

The next corollary was first proved in [51, Theorem 6.7].

Corollary 6.14. *Let $\exp(G) = n$. If G is either a p-group or $\mathsf{r}(G) \le 2$, then $\mathsf{s}_{n\mathbb{N}}(G) = \mathsf{d}(G) + n$.*

Proof. If G is a p-group, then the assertion follows from Theorem 4.10 and from Lemma 6.6.3.

Suppose that $G = C_{n_1} \oplus C_{n_2}$ with $1 \le n_1 \mid n_2$. Then Lemma 6.6.3 implies that $\mathsf{d}(G) + n_2 \le \mathsf{s}_{n\mathbb{N}}(G)$ whence it remains to prove that $\mathsf{s}_{n\mathbb{N}}(G) \le \mathsf{d}(G) + n_2 = n_1 + 2n_2 - 2$. If $n_1 = 1$, this follows from Theorem 6.13 and again from Lemma 6.6.3. Suppose that $n_1 > 1$, and let $S \in \mathcal{F}(G)$ be a sequence of length $|S| = n_1 + 2n_2 - 2$. We have to show that S has a zero-sum subsequence of length n_2 or $2n_2$.

Let $K = G \oplus C_{n_2} = G \oplus \langle e \rangle$ with $\operatorname{ord}(e) = n_2$, so that every $h \in G \oplus C_{n_2}$ has a unique representation $h = g + je$, where $g \in G$ and $j \in [0, n_2 - 1]$. We define $\psi \colon G \to K$ by $\psi(g) = g + e$ for every $g \in G$. Thus it suffices to show that $\psi(S)$ has a nontrivial zero-sum subsequence. We distinguish two cases.

CASE 1: $n_1 = n_2$.

We set $n = n_1$ and proceed by induction on n. If n is prime, then G is a p-group and the assertion holds. Suppose that n is composite, p a prime divisor of n and $\varphi \colon K \to K$ the multiplication by p. Then $pG \cong C_{n/p} \oplus C_{n/p}$ and $\operatorname{Ker}(\varphi) \cong C_p^3$. Since by Theorem 6.13, $\mathsf{s}(pG) = 4(n/p) - 3$ and $|S| = 3n - 2 \ge (3p-4)(n/p) + 4n/p - 3$, S admits a product decomposition $S = S_1 \cdot \ldots \cdot S_{3p-3} S'$ such that, for all $i \in [1, 3p-3]$, $\varphi(S_i)$ has sum zero and length $|S_i| = n/p$ (see Lemma 6.7.1). Then

$|S'| = 3n/p - 2 = \mathsf s_{(n/p)\mathbb N}(C_{n/p} \oplus C_{n/p})$, and thus S' has a subsequence S_{3p-2} such that $\varphi(S_{3p-2})$ has sum zero and length $|S_{3p-2}| \in \{n/p, 2n/p\}$. This implies that

$$\prod_{i=1}^{3p-2} \sigma\bigl(\psi(S_i)\bigr) \in \mathcal F\bigl(\mathrm{Ker}(\varphi)\bigr)\,.$$

Since $\mathsf D(\mathrm{Ker}(\varphi)) = 3p-2$, there exists a nonempty subset $I \subset [1, 3p-2]$ such that

$$\sum_{i\in I} \sigma\bigl(\psi(S_i)\bigr) = 0 \quad \text{whence} \quad \prod_{i\in I} \psi(S_i)$$

is a nontrivial zero-sum subsequence of $\psi(S)$.

CASE 2: $n_2 > n_1$.

Let $m = n_1^{-1}n_2$ and let $\varphi\colon K = C_{n_1} \oplus C_{n_2}^2 \to C_{n_1} \oplus mC_{n_2}^2$ be a map which is the identity on the first component and the multiplication by m on the second and on the third component whence $\mathrm{Ker}(\varphi) \cong C_m \oplus C_m$ and $\varphi(G) \cong C_{n_1} \oplus C_{n_1}$. Since $\mathsf s(C_{n_1} \oplus C_{n_1}) = 4n_1 - 3$ and $|S| = n_1 + 2n_2 - 2 \ge (2m-3)n_1 + (4n_1 - 3)$, S admits a product decomposition $S = S_1 \cdot \ldots \cdot S_{2m-2}S'$, where for all $i \in [1, 2m-2]$, $\varphi(S_i)$ has sum zero and length $|S_i| = n_1$. Then $|S'| = 3n_1 - 2$, and since by CASE 1, $\mathsf s_{n_1\mathbb N}(C_{n_1} \oplus C_{n_1}) = 3n_1 - 2$, the sequence S' has a subsequence S_{2m-1} such that $\varphi(S_{2m-1})$ has sum zero and length $|S_{2m-1}| \in \{n_1, 2n_1\}$. This implies that

$$\prod_{i=1}^{2m-1} \sigma\bigl(\psi(S_i)\bigr) \in \mathcal F\bigl(\mathrm{Ker}(\varphi)\bigr)\,.$$

Since $\mathsf D(\mathrm{Ker}(\varphi)) = 2m-1$, there exists a nonempty subset $I \subset [1, 2m-1]$ such that

$$\sum_{i\in I} \sigma\bigl(\psi(S_i)\bigr) = 0 \quad \text{whence} \quad \prod_{i\in I} \psi(S_i)$$

is a nontrivial zero-sum subsequence of $\psi(S)$. □

We briefly discuss the state of the art concerning groups of higher rank (more detailed information can be found in [51]). A conjecture by W. Gao states that we always have $\eta(G) = \mathsf s(G) - \exp(G) + 1$. This was recently proved for p-groups G, where p is odd and $\mathsf D(G) = 2\exp(G) - 1$ ([125]). C. Elsholtz et al. showed that, for all odd $n \ge 3$,

$$\eta(C_n^3) \ge 8n - 7,\quad \mathsf s(C_n^3) \ge 9n - 8,\quad \eta(C_n^4) \ge 19n - 18 \quad \text{and} \quad \mathsf s(C_n^4) \ge 20n - 19\,,$$

and it is conjectured that all bounds are sharp (see [29, 28, 27, 113] for recent results).

It is conjectured that, if $\mathsf r(G) = 3$ or $G = C_n^r$ with $n, r \ge 3$, then $\mathsf d(G) = \mathsf d^*(G)$. On the other hand, for every $r \ge 4$ there are infinitely many groups G of rank $\mathsf r(G) = r$ such that $\mathsf d(G) > \mathsf d^*(G)$ (see [75] and [48, Theorem 3.3]). We end with a result (see [15]) providing more groups G with $\mathsf d(G) = \mathsf d^*(G)$ and whose proof demonstrates once more the power of the inductive method (for recent results see [6, 4]).

Theorem 6.15. *Let* $G = K \oplus C_{km}$ *where* $k, m \in \mathbb N$ *and* $K \subset G$ *is a subgroup with* $\exp(K) | m$. *If* $\mathsf d(K \oplus C_m) = \mathsf d(K) + m - 1$ *and* $\eta(K \oplus C_m) \le \mathsf d(K) + 2m$, *then* $\mathsf d(G) = \mathsf d(K) + km - 1$.

Proof. Clearly, we have $\mathsf d(G) \ge \mathsf d(K) + \mathsf d(C_{km}) = \mathsf d(K) + km - 1$. Now let $S \in \mathcal F(G)$ be a sequence of length $|S| = \mathsf d(K) + km$. We have to show that S has a nontrivial zero-sum subsequence.

We consider the map $\varphi\colon G \to G$ which maps an element $g = h + a$, with $h \in K$ and $a \in C_{km}$, to $h + ka$ for all $g \in G$. Then $\mathrm{Ker}(\varphi) \cong C_k$ and $\varphi(G) \cong K \oplus C_m$. Since

$$|\varphi(S)| = |S| = (k-2)m + \bigl(\mathsf d(K) + 2m\bigr) \quad \text{and} \quad \eta(K \oplus C_m) \le \mathsf d(K) + 2m\,,$$

Lemma 6.7 provides us with a product decomposition

$$S = S_1 \cdot \ldots \cdot S_{k-1}S'$$

where $S_1, \ldots, S_{k-1}, S' \in \mathcal{F}(G)$ and, for every $i \in [1, k]$, $\varphi(S_i)$ has sum zero and length $|S_i| \in [1, \exp(K \oplus C_m)] = [1, m]$. Thus we get

$$|S'| = |S| - \sum_{i=1}^{k-1} |S_i| \geq |S| - (k-1)m = \mathsf{d}(K) + m = \mathsf{D}(K \oplus C_m)\,,$$

and hence S' has a subsequence S_k such that $\varphi(S_k)$ has sum zero. Thus

$$\prod_{i=1}^{k} \sigma(S_i) \in \mathcal{F}\big(\mathrm{Ker}(\varphi)\big)\,,$$

and there is a nonempty subset $I \subset [1, k]$ such that $\prod_{i \in I} \sigma(S_i)$ has sum zero. Hence $\prod_{i \in I} S_i$ is a nontrivial zero-sum subsequence of S. □

Corollary 6.16. *Let* $G = K \oplus C_{km}$ *where* $k, m \in \mathbb{N}$*,* $p \in \mathbb{P}$ *a prime,* m *a power of* p *and* $K \subset G$ *is a* p*-subgroup with* $\mathsf{d}(K) \leq m - 1$*. Then* $\mathsf{d}(G) = \mathsf{d}^*(G)$*.*

Proof. Since $K \oplus C_m$ is a p-group, Theorem 4.10 implies that

$$\mathsf{d}(K \oplus C_m) = \mathsf{d}^*(K \oplus C_m) = \mathsf{d}^*(K) + m - 1 = \mathsf{d}(K) + m - 1\,.$$

Since $\exp(K)$ is a p-power and $\exp(K) - 1 \leq \mathsf{d}(K) \leq m - 1$, it follows that $\exp(K)$ divides m. By Lemma 6.6 we infer that

$$\eta(K \oplus C_m) \leq \mathsf{d}(K \oplus C_m^2) + 1 = \mathsf{d}(K) + 2m - 1\,.$$

Thus all assumptions of Theorem 6.15 are satisfied and we obtain that

$$\mathsf{d}(G) = \mathsf{d}(K) + km - 1 = \mathsf{d}^*(K) + km - 1 = \mathsf{d}^*(G)\,.$$ □

7. Inverse zero-sum problems and arithmetical consequences

The investigation of inverse problems has a long tradition in combinatorial number theory (see [107, 37]), and more recently it has been promoted by applications in the theory of non-unique factorizations. In this section we discuss the inverse problems associated to the invariants $\mathsf{D}(G)$, $\eta(G)$ and $\mathsf{s}(G)$. More precisely, we investigate the structure of sequences of length $\mathsf{D}(G) - 1$ ($\eta(G) - 1$ or $\mathsf{s}(G) - 1$, respectively) that do not have a zero-sum subsequence (of the required length). Recent results on the structure of $\Sigma(S)$ for (long) zero-sum free sequences may be found in [9, 58, 127, 133, 60].

We start with cyclic groups, then we deal with groups of the form $G = C_n^r$, and finally we outline some consequences in factorization theory.

7.A Cyclic groups

Clearly, we can rephrase Corollary 4.4.1 as follows: let G be cyclic of order $n \geq 2$ and $S \in \mathcal{F}(G)$ a sequence of length $\mathsf{D}(G) - 1 = \eta(G) - 1$. Then S has no (short) zero-sum subsequence if and only if $S = g^{n-1}$ for some $g \in G$ with $\mathrm{ord}(g) = n$.

We present a strong structural result on long zero-sum free sequences recently achieved by S. Savchev and Fang Chen ([116]). Among others their result settles a problem on the index of zero-sum sequences (studied in [16, 46, 112, 18], see Corollary 7.9) and provides information on multiplicities of elements, a topic studied by many authors before (Corollary 7.10).

Definition 7.1.

1. Let $g \in G$ be a non-zero element with $\operatorname{ord}(g) = n < \infty$. For a sequence
$$S = (n_1 g) \cdot \ldots \cdot (n_l g), \quad \text{where } l \in \mathbb{N}_0 \quad \text{and} \quad n_1, \ldots, n_l \in [1, n],$$
we define
$$\|S\|_g = \frac{n_1 + \ldots + n_l}{n}.$$
Obviously, S has sum zero if and only if $\|S\|_g \in \mathbb{N}_0$.
2. Let $S \in \mathcal{F}(G)$ be a sequence for which $\langle \operatorname{supp}(S) \rangle \subset G$ is cyclic. Then we call
$$\operatorname{ind}(S) = \min\{\|S\|_g \mid g \in G \text{ with } \langle \operatorname{supp}(S) \rangle = \langle g \rangle\} \in \mathbb{Q}_{\ge 0}$$
the *index of* S.
3. If G is cyclic, then let $\mathsf{I}(G)$ denote the smallest integer $l \in \mathbb{N}$ such that every minimal zero-sum sequence $S \in \mathcal{F}(G)$ of length $|S| \ge l$ satisfies $\operatorname{ind}(S) = 1$.

Lemma 7.2. *Let G be cyclic and $S \in \mathcal{F}(G)$. Then*
$$\begin{aligned} \operatorname{ind}(S) &= \min\{\|S\|_g \mid g \in G \textit{ with } \operatorname{supp}(S) \subset \langle g \rangle\} \\ &= \min\{\|S\|_g \mid g \in G \textit{ with } G = \langle g \rangle\}. \end{aligned}$$

Proof. We set $|G| = n$,
$$I_1 = \min\{\|S\|_g \mid g \in G \text{ with } \operatorname{supp}(S) \subset \langle g \rangle\} \quad \text{and} \quad I_2 = \min\{\|S\|_g \mid g \in G \text{ with } G = \langle g \rangle\}.$$
Let $|S| = l$, $g \in G$ with $\operatorname{ord}(g) = m$ and $S = (a_1 g) \cdot \ldots \cdot (a_l g)$ with $a_1, \ldots, a_l \in [1, m]$ such that $\|S\|_g = I_1$. First we verify that $I_1 = I_2$ and then we show that $I_1 = \operatorname{ind}(S)$.

1. Obviously, we have $I_1 \le I_2$, and it remains to verify the reverse inequality. There is an element $h \in G$ with $\langle h \rangle = G$ and $\frac{n}{m} h = g$. Thus we obtain
$$S = (a_1 \frac{n}{m} h) \cdot \ldots \cdot (a_l \frac{n}{m} h) \quad \text{with} \quad a_1 \frac{n}{m}, \ldots, a_l \frac{n}{m} \in [1, n],$$
$$\|S\|_h = \frac{\frac{n}{m} a_1 + \ldots + \frac{n}{m} a_l}{n} = \frac{a_1 + \ldots + a_l}{m} = \|S\|_g$$
and hence $I_2 \le \|S\|_h = \|S\|_g = I_1$.

2. Obviously, we have $I_1 \le \operatorname{ind}(S)$, and it remains to verify the reverse inequality. We set $\langle a_1 g, \ldots, a_l g \rangle = K$ and pick an $a \in [1, m]$ with $a \,|\, m$ and $K = \langle a g \rangle$. Then $\operatorname{ord}(ag) = a^{-1} m$. For every $i \in [1, l]$ we have $a_i g \in \langle a g \rangle = \{ag, 2ag, \ldots, (a^{-1} m) ag\}$ and hence $a_i = a a_i'$ with $a_i' \in [1, a^{-1} m]$. Thus we obtain
$$S = (a_1' a g) \cdot \ldots \cdot (a_l' a g),$$
$$\|S\|_g = \frac{a(a_1' + \ldots + a_l')}{m} = \frac{a_1' + \ldots + a_l'}{a^{-1} m} = \|S\|_{ag}$$
and hence $I_1 = \|S\|_g = \|S\|_{ag} \ge \operatorname{ind}(S)$. □

Definition 7.3. A sequence $S \in \mathcal{F}(G)$ is called

- *smooth* if $S = (n_1 g) \cdot \ldots \cdot (n_l g)$, where $l = |S| \in \mathbb{N}$, $g \in G$, $1 = n_1 \le \ldots \le n_l$, $n = n_1 + \ldots + n_l < \operatorname{ord}(g)$ and $\Sigma(S) = \{g, 2g, \ldots, ng\}$ (in this case we say more precisely that S is g-smooth).
- *a splittable atom* if $S = (g_1 + g_2) T$ for some $g_1, g_2 \in G$ and $T \in \mathcal{F}(G)$ such that $S \in \mathcal{A}(G)$ and $g_1 g_2 T \in \mathcal{A}(G)$.

Lemma 7.4. *Let $g \in G$ and $k, l, n_1, \ldots, n_l \in \mathbb{N}$ such that $l \ge k/2$ and $n = n_1 + \ldots + n_l < k \le \operatorname{ord}(g)$. If $1 \le n_1 \le \ldots \le n_l$ and $S = (n_1 g) \cdot \ldots \cdot (n_l g)$, then $\Sigma(S) = \{g, 2g, \ldots, ng\}$, and S is g-smooth.*

Proof. We start with the following assertion.

A. For every $i \in [0, l-1]$ we have $n_{i+1} \le 1 + n_1 + \ldots + n_i$, and in particular we have $n_1 = 1$.

Proof of **A**. Assume to the contrary that there is an $i \in [0, l-1]$ such that $n_{i+1} \ge 2 + n_1 + \ldots + n_i$. Then for all $j \in [i+1, l]$ we have $n_j \ge n_{i+1} \ge 2 + i$ and therefore

$$k > n_1 + \ldots + n_l \ge i + (l-i)(2+i) = 2l + i(l-i-1) \ge k\,,$$

a contradiction.

For every $i \in [1, l]$ we set $S_i = (n_1 g) \cdot \ldots \cdot (n_i g)$ and assert that $\Sigma(S_i) = \{jg \mid j \in [1, n_1 + \ldots + n_i]\}$. We proceed by induction on i. For $i = 1$, this hold since $n_1 = 1$. If $i \in [1, l-1]$, then **A** and the induction hypothesis imply that

$$\begin{aligned}\Sigma(S_{i+1}) &= \Sigma(S_i) \cup \Big(n_{i+1}g + \big(\Sigma(S_i) \cup \{0\}\big)\Big)\\ &= \{jg \mid j \in [1, n_1 + \ldots + n_i]\} \cup \{jg \mid j \in [n_{i+1}, n_1 + \ldots + n_i + n_{i+1}]\}\\ &= \{jg \mid j \in [1, n_1 + \ldots + n_{i+1}]\}\,.\end{aligned}$$

□

Lemma 7.5. *Let $S \in \mathcal{F}(G)$ and $b \in G$ such that $Sb \in \mathcal{A}^*(G)$ and $|\Sigma(Sb)| = |\Sigma(S)| + 1$.*

1. *We have $\Sigma(S) = \{b, 2b, \ldots, sb\} \cup P_1 \cup \ldots \cup P_m$, where $s \in [1, \mathrm{ord}(b) - 2]$, $m \in \mathbb{N}_0$ and $P_1, \ldots, P_m \in G/\langle b\rangle$ are distinct cosets different from $\langle b\rangle$. Moreover, $sb = \sigma(S)$ and $|\Sigma(Sb^j)| = |\Sigma(Sb^{j-1})| + 1$ for all $j \in [1, \mathrm{ord}(b) - s]$.*
2. *If $c \in G$ is such that $Sc \in \mathcal{A}^*(G)$ and $|\Sigma(Sc)| = |\Sigma(S)| + 1$, then $c = b$.*

Proof. 1. Since $Sb \in \mathcal{A}^*(G)$, $|\Sigma(Sb)| = |\Sigma(S)| + 1$ and $\sigma(S) + b \in \Sigma(Sb)$, it follows that $\Sigma(Sb) \setminus \Sigma(S) = \{\sigma(S) + b\}$, and since $b \in \Sigma(Sb)$ and $\sigma(S) \ne 0$, we obtain that $b \in \Sigma(S)$. Let $s \in \mathbb{N}$ be maximal such that $\{b, 2b, \ldots, sb\} \subset \Sigma(S)$. Then $(s+1)b \in \Sigma(Sb)$, hence $(s+1)b = \sigma(S) + b$ and $sb = \sigma(S)$. Moreover, $Sb \in \mathcal{A}^*(G)$ implies that $s + 1 < \mathrm{ord}(b)$.

In order to prove that $\Sigma(S) \setminus \{b, 2b, \ldots, sb\}$ is the union of proper cosets of $\langle b\rangle$ in G, we have to verify that $c \in \Sigma(S) \setminus \{b, 2b, \ldots, sb\}$ implies that $c + b \in \Sigma(S) \setminus \{b, 2b, \ldots, sb\}$. Indeed, if $c \in \Sigma(S) \setminus \{b, 2b, \ldots, sb\}$, then $c + b \in \Sigma(Sb)$. If $c + b \notin \Sigma(S) \setminus \{b, 2b, \ldots, sb\}$, then $c + b = tb$ for some $t \in [1, s+1]$, and thus $c = (t-1)b \in \{0, b, 2b, \ldots, sb\}$, a contradiction. Hence it follows that $c + b \in \Sigma(S) \setminus \{b, 2b, \ldots, sb\}$.

If $j \in [1, \mathrm{ord}(b) - s]$, then

$$\Sigma(Sb^j) = \{b, 2b, \ldots, (s+j)b\} \cup P_1 \cup \ldots \cup P_m = \Sigma(Sb^{j-1}) \cup \{(s+j)b\}\,,$$

and since $s + j \le \mathrm{ord}(b)$, we obtain $|\Sigma(Sb^j)| = |\Sigma(Sb^{j-1})| + 1$.

2. Let $c \in G$ be such that $Sc \in \mathcal{A}^*(G)$ and $|\Sigma(Sc)| = |\Sigma(S)| + 1$. Then $R = \{c, b+c, 2b+c, \ldots, sb+c\} \subset \Sigma(Sc)$, and since $|R| \ge 2$ we have $R \cap \Sigma(S) \ne \emptyset$. Suppose there is some $j \in [1, m]$ such that $R \cap P_j \ne \emptyset$. Then $R \subset P_j$, but $sb + c = \sigma(S) + c \in \Sigma(Sc) \setminus \Sigma(S)$ and thus $sb + c \notin P_j$, a contradiction. Hence it follows that $R \cap \{b, 2b, \ldots, sb\} \ne \emptyset$, say $rb + c = tb$ for some $r \in [0, s]$ and $t \in [1, s]$. Thus we obtain $c = (t-r)b$ and $R = \{(t - r + j)b \mid j \in [0, s]\}$. If $t \le r$, this implies $0 \in R$, a contradiction. If $t \ge r + 2$, then we obtain $\{(s+1)b, (s+2)b\} \subset R \setminus \Sigma(S) \subset \Sigma(Sc) \setminus \Sigma(S)$, contradicting $|\Sigma(Sc)| = |\Sigma(S)| + 1$. Therefore we get $t = r + 1$ and $c = b$. □

Lemma 7.6. *Let G be cyclic of order $n \ge 3$, $S = S_1S_2 \in \mathcal{A}^*(G)$ where $|S| = l \ge \frac{n+1}{2}$, $2 \le |S_1| = k + 1 \le l$ and $|\Sigma(S_1)| \ge 2k + 1$. Then there is a decomposition $S_2 = S_2'c$ with $S_2' \in \mathcal{F}(G)$ and $c \in G$ such that $|\Sigma(S)| = |\Sigma(S_1S_2')| + 1$.*

Proof. Let $t \in \mathbb{N}_0$ be maximal such that there is a decomposition $S_2 = g_1 \cdot \ldots \cdot g_tT$, where $g_1, \ldots, g_t \in G$ and $T \in \mathcal{F}(G)$ are such that

$$|\Sigma(S_1g_1 \cdot \ldots \cdot g_j)| \ge |\Sigma(S_1g_1 \cdot \ldots \cdot g_{j-1})| + 2 \quad \text{for all} \quad j \in [1, t]\,.$$

Then we have

$$n-1 \ge |\Sigma(S)| \ge |\Sigma(S_1 g_1 \cdot \ldots \cdot g_t)| \ge |\Sigma(S_1)| + 2t \ge 2k+1+2t\,.$$

Therefore it follows that $2t+2 \le n-2k$, whence $t+1 \le n/2 - k < l-k$ and $|T| = |S| - |S_1| - t = l-(k+1)-t > 0$. Let $c \in \mathrm{supp}(T)$. Since $|\Sigma(S_1 g_1 \cdot \ldots \cdot g_t c)| = |\Sigma(S_1 g_1 \cdot \ldots \cdot g_t)| + 1$ (by the maximality of t), Lemma 7.5 implies that

$$\Sigma(S_1 g_1 \cdot \ldots \cdot g_t) = \{c, 2c, \ldots, sc\} \cup P_1 \cup \ldots \cup P_m\,,$$

where $s \in [1, \mathrm{ord}(c)-2]$, $m \in \mathbb{N}_0$ and $P_1, \ldots, P_m \in G/\langle c\rangle$ are proper cosets. If $d \in \mathrm{supp}(c^{-1}T)$, then (again by the maximality of t) $|\Sigma(S_1 g_1 \cdot \ldots \cdot g_t d)| = |\Sigma(S_1 g_1 \cdot \ldots \cdot g_t)| + 1$, and Lemma 7.5 implies $d = c$. Hence $T = c^j$ for some $j \in [1, \mathrm{ord}(c) - s]$ and $S_2' = g_1 \cdot \ldots \cdot g_t c^{j-1}$ fulfills our requirements. □

Lemma 7.7. *Let G be cyclic of order $n \ge 3$, $S \in \mathcal{A}^*(G)$ with $\Sigma(S) = G^\bullet$, $|S| = l \ge \frac{n+1}{2}$, $a \in \mathrm{supp}(S)$ and S_a a maximal a-smooth subsequence of S. If $S_a \ne S$, then $(-\sigma(S)) \,|\, S_a^{-1}S$.*

Proof. Let $S_a = (s_1 a) \cdot \ldots \cdot (s_k a)$, where $k, s_1, \ldots, s_k \in \mathbb{N}$, $1 = s_1 \le s_2 \le \ldots \le s_k$, $s = s_1 + \ldots + s_k < \mathrm{ord}(a)$, and assume that $S_a \ne S$. Then $S = S_a b S_2$, where $b \in G$ and $S_2 \in \mathcal{F}(G)$, and we have $\Sigma(S_a b) = P_1 \cup P_2$ where $P_1 = \Sigma(S_a) = \{a, 2a, \ldots, sa\}$ and $P_2 = b + \big(\Sigma(S_a) \cup \{0\}\big) = \{b, b+a, \ldots, b+sa\}$. We shall prove that

A. $P_1 \cap P_2 = \emptyset$.

Proof of **A**. The assertion is obvious if $b \notin \langle a\rangle$. Thus assume that $b = ta$ for some $t \in [1, \mathrm{ord}(a)-1]$. Then $\Sigma(S_a b) = \{a, 2a, \ldots, sa, ta, (t+1)a, \ldots, (t+s)a\}$. If $t \le s$, then $t + s \ge s+1$ and $S_a b$ is a-smooth, contradicting the maximality of S_a. If $t+s \ge \mathrm{ord}(a)$, then $0 \in \Sigma(S_a b)$, a contradiction. Hence $s < t < \mathrm{ord}(a) - s$ and $P_1 \cap P_2 = \emptyset$.

We apply Lemma 7.6 with $S_1 = S_a b$. Note that $2 \le k+1 = |S_a b| \le |S| = l$ and

$$n-1 \ge |\Sigma(S_a b)| = |P_1| + |P_2| = 2s+1 \ge 2k+1\,.$$

Thus we arrive at a decomposition $S_2 = S_2' c$ for some $S_2' \in \mathcal{F}(G)$ and $c \in G$ such that $|\Sigma(S)| = |\Sigma(S_1 S_2')| + 1 = |G| - 1$. Since $\Sigma(S) = \Sigma(S_1 S_2') \cup \{\sigma(S)\}$ and $-c \notin \Sigma(S_1 S_2')$, it follows that $c = -\sigma(S)$, whence $-\sigma(S) \,|\, S_2 \,|\, S_a^{-1} S$. □

Theorem 7.8 (Savchev-Chen). *Let G be cyclic of order $n \ge 3$.*

1. *If $S \in \mathcal{A}^*(G)$ and $|S| \ge \frac{n+1}{2}$, then S is g-smooth for some $g \in G$ with* $\mathrm{ord}(g) = n$.
2. *Let $U \in \mathcal{A}(G)$ be of length $|U| \ge \lfloor \frac{n}{2} \rfloor + 2$. Then* $\mathrm{ind}(U) = 1$, *and if U is not splittable, then $U = g^n$ for some $g \in G$.*

Proof. We may suppose that $U = g_0 S$ with $|S| = l \ge \frac{n+1}{2}$. First we show that S is g-smooth for some $g \in G$. Then we show $\mathrm{ind}(U) = 1$ and $\mathrm{ord}(g) = n$.

1. Pick a sequence $S' \in \mathcal{A}^*(G)$ such that $S \,|\, S'$ and $|S'|$ is maximal. Then $\Sigma(S') = G^\bullet$ and $m = |S'| \ge |S| \ge \frac{n+1}{2}$. Let $a \in \mathrm{supp}(S')$ and S_a be a maximal a-smooth subsequence of S'. If $S_a \ne S'$ and $h = -\sigma(S')$, then $h \,|\, S_a^{-1} S'$ by Lemma 7.7. Now let S_h be a maximal h-smooth subsequence of S'. Then $h \nmid S_h^{-1} S'$, since otherwise $h S_h$ would be a longer h-smooth subsequence of S'. Hence again Lemma 7.7 implies that $S_h = S'$.

In any case S' is smooth, and thus we may assume that $S' = (n_1 g) \cdot \ldots \cdot (n_m g)$ and $S = (n_1 g) \cdot \ldots \cdot (n_l g)$, where $g \in G$, $m \in \mathbb{N}$, $n_1, \ldots, n_m \in \mathbb{N}$, $l \le m \le n_1 + \ldots + n_m < \mathrm{ord}(g) \le n < 2l$ and $1 \le n_1 \le \ldots \le n_l$. Thus Lemma 7.4 (with $k = \mathrm{ord}(g)$) implies that S is g-smooth.

2. By 1., $S = (n_1 g) \cdot \ldots \cdot (n_l g)$ is g-smooth,whence $n_1, \ldots, n_l \in \mathbb{N}$ and $s = n_1 + \ldots + n_l < \mathrm{ord}(g)$. Then $-g_0 = \sigma(S) = sg$ and $U = (n_0 g)(n_1 g) \cdot \ldots \cdot (n_l g)$ with $n_0 = \mathrm{ord}(g) - s \in \mathbb{N}$ and hence $n_0 + \ldots + n_l = \mathrm{ord}(g)$. Let $m \in \mathbb{N}$ with $\mathrm{ord}(g) = n/m$ and $g' \in G$ with $mg' = g$. Then $U = (mn_0 g') \cdot \ldots \cdot (mn_l g')$ and

$mn_0 + \ldots + mn_l = n$ whence $\operatorname{ind}(U) = 1$. Since $n = mn_0 + \ldots + mn_l \ge m(l+1) \ge m\frac{n+3}{2}$, it follows that $m = 1$ and $g = g'$.

If there is some $i \in [0, l]$ with $n_i \ge 2$, say $i = 0$, then $\big((n_0 - 1)g\big)g(n_1 g) \cdot \ldots \cdot (n_l g) \in \mathcal{A}(G)$, and hence U is splittable. □

Corollary 7.9 was achieved independently by S. Savchev and F. Chen, and by P. Yuan (see [132, Theorem 3.1] and [116, Proposition 10]).

Corollary 7.9. *Let G be cyclic of order $n \ge 1$. If $n \in \{1,2,3,4,5,7\}$, then $\mathsf{l}(G) = 1$, and otherwise we have $\mathsf{l}(G) = \lfloor \frac{n}{2} \rfloor + 2$.*

Proof. If $n \le 4$, it can be seen immediately that $\mathsf{l}(G) = 1$. If $n \in \{5, 7\}$, a longer (but straightforward) case distinction shows that again $\mathsf{l}(G) = 1$ holds. Suppose that $n \in \mathbb{N}_{\ge 6} \setminus \{7\}$, and let $g \in G$ with $\operatorname{ord}(g) = n$. Since the sequence

$$S = \begin{cases} g^{\frac{n-4}{2}}(\frac{n}{2}g)(\frac{n+2}{2}g)^2 & \text{if} \quad n \quad \text{is even,} \\ g^{\frac{n-5}{2}}(\frac{n+3}{2}g)^2(\frac{n-1}{2}g) & \text{if} \quad n \quad \text{is odd.} \end{cases}$$

is a minimal zero-sum sequence with $\operatorname{ind}(S) = 2$, it follows that $\mathsf{l}(G) \ge \lfloor \frac{n}{2} \rfloor + 2$, and hence equality holds by Theorem 7.8.2. □

The second statement of Corollary 7.10 was first proved by J.D. Bovey, P. Erdős and I. Niven ([10]) and the fourth statement by A. Geroldinger and Y. ould Hamidoune ([72]). Note that the bounds given in 7.10.4 are attained ([71, Example 5.4.7]).

Corollary 7.10. *Let G be cyclic of order $n \ge 3$, $S \in \mathcal{F}(G)$ a zero-sum free sequence of length*

$$|S| \ge \frac{n+1}{2}.$$

1. *For all $g \in \operatorname{supp}(S)$ we have $\operatorname{ord}(g) \ge 3$.*
2. *There exists some $g \in \operatorname{supp}(S)$ with $\mathsf{v}_g(S) \ge 2|S| - n + 1$.*
3. *There exists some $g \in \operatorname{supp}(S)$ with $\mathsf{v}_g(S) \ge |S| - \frac{n-1}{3}$.*
4. *There exists some $g \in \operatorname{supp}(S)$ with $\operatorname{ord}(g) = n$ such that*

$$\mathsf{v}_g(S) \ge \frac{n+5}{6} \quad \textit{if} \;\; n \;\; \textit{is odd}, \qquad \textit{and} \qquad \mathsf{v}_g(S) \ge 3 \quad \textit{if} \;\; n \;\; \textit{is even}.$$

Proof. 1. The assertion is clear for odd n. Thus suppose that $n = 2m$ for some $m \ge 2$. By Theorem 7.8, $S = (n_1 g) \cdot \ldots \cdot (n_l g)$ for some $g \in G$ with $\operatorname{ord}(g) = n$, $1 = n_1 \le \ldots \le n_l$ and $\Sigma(S) = \{g, 2g, \ldots, sg\}$ where $s = n_1 + \ldots + n_l$. Assume to the contrary that S contains some element of order 2. Then there is an $i \in [1, l]$ with $n_i = m$ and hence $s = n_1 + \ldots + n_l \ge l - 1 + m \ge 2m$, a contradiction to S zero-sum free.

2. We write S in the form $S = S_1 \cdot \ldots \cdot S_k\,(gh)^l g^{m-l}$, where $k,\, m \in \mathbb{N}_0$, $l \in [0, m]$, $g \ne h$, $S_1, \ldots, S_k$ are squarefree, and $|S_i| = 3$ for all $i \in [1, k]$. Clearly, we have $|\Sigma(gh)| = 3$, and using 1. we obtain that $|\Sigma(S_i)| \ge 6$ for all $i \in [1, k]$. By Corollary 6.3 it follows that

$$n - 1 \ge |\Sigma(S)| \ge 6k + 3l + (m - l) \ge 6k + 2l + 2m - \mathsf{v}_g(S) = 2|S| - \mathsf{v}_g(S)$$

and therefore $\mathsf{v}_g(S) \ge 2|S| - n + 1$.

3. and 4. The sequence $S_1 = \big(-\sigma(S)\big)S$ is a minimal zero-sum sequence of length $|S_1| \ge (n+3)/2$. Thus Corollary 7.9 implies that $\operatorname{ind}(S_1) = 1$. Thus there is an element $h \in G$ with $\operatorname{ord}(h) = n$ such that

$$S_1 = (xh)h^u(2h)^v(x_1 h) \cdot \ldots \cdot (x_t h),$$

where $x \in [1, n-1], xh = -\sigma(S)$, $u, v, t \in \mathbb{N}_0$, $x_1, \ldots, x_t \in [3, n-1]$ and $x + u + 2v + (x_1 + \ldots + x_t) = n$. Clearly, we have

$$|S| = u + v + t \quad \text{and} \quad u + 2v + 3t = n - r \text{ for some } r \in \mathbb{N}\,,$$

which implies that $2u + v = 3|S| - (n - r)$ and hence

$$\max\{u, v\} \ge |S| - \frac{n-r}{3} \ge |S| - \frac{n-1}{3}\,.$$

If n is odd, then $\operatorname{ord}(h) = \operatorname{ord}(2h) = n$ and

$$\max\{\mathsf{v}_h(S), \mathsf{v}_{2h}(S)\} = \max\{u, v\} \ge |S| - \frac{n-1}{3} \ge \frac{n+5}{6}\,.$$

If n is even, then $|S| \ge (n/2) + 1$ and

$$\mathsf{v}_h(S) = u = 2|S| - n + r + t \ge 2 + r + t \ge 3\,. \qquad \square$$

Without proof we cite a most recent result by W. Gao et. al. (see [61]).

Theorem 7.11. *Let G be cyclic of order $n \ge 3$. If $S \in \mathcal{F}(G)$ is a zero-sum free sequence of length*

$$|S| \ge \frac{6n+28}{19}\,, \quad \textit{then} \quad \mathsf{h}(S) \ge \frac{6|S| - n + 1}{17}\,.$$

Next we consider the inverse problem with respect to the $\mathsf{s}(G)$-invariant. The first result in this direction was achieved independently by B. Peterson and T. Yuster ([109, Theorem 1]), and by A. Bialostocki and P. Dierker ([7, Lemma 4]). It runs as follows.

Proposition 7.12. *Let G be cyclic of order $n \ge 2$ and $S \in \mathcal{F}(G)$ a sequence of length $|S| = \mathsf{s}(G) - 1$. Then the following statements are equivalent:*

(a) *S has no zero-sum subsequence of length n.*

(b) *$S = (gh)^{n-1}$ where $g, h \in G$ with $\operatorname{ord}(g - h) = n$.*

Proposition 7.12 was the starting point for a huge variety of investigations (see [11, 34, 12, 43, 62, 8, 131, 63, 95, 65]). We present a recent result, achieved by S. Savchev and F. Chen in [117], which characterizes all sequences of length greater than or equal to $(3n-1)/2$ that have no zero-sum subsequence of length n (Theorem 7.16). This easily implies Proposition 7.12, and moreover the lower bound is, in a certain sense, best possible (see Remark 7.17). We start with the following result of W. Gao (see [41, Theorem 1]).

Proposition 7.13 (Gao)**.** *Let $S \in \mathcal{F}(G)$ be a sequence of length $|S| = |G| + k$ with $k \in \mathbb{N}_0$, and suppose that for every $g \in G$ and every subsequence T of S of length $|T| = k+1$ the sequence $g+T$ has a zero-sum subsequence. Then*

$$\Sigma_{|G|}(S) = \bigcap_{g \in G} \Sigma(g + S)\,.$$

In particular, if $\mathsf{h}(S) = \mathsf{v}_0(S)$, then $\Sigma_{\ge |G|}(S) = \Sigma_{|G|}(S)$.

Proof. We set $|G| = n$. Let $S = a^h T$ with $h = \mathsf{h}(S)$ and $|S| = n + k$. Without restriction we may suppose that $a = 0$. Obviously, we have

$$\Sigma_n(S) \subset \bigcap_{g \in G} \Sigma(g + S) \subset \Sigma(S)\,.$$

Hence, for the main statement, it suffices to show that $\Sigma(S) \subset \Sigma_n(S)$. But this inclusion clearly implies the "In particular" statement too. We pick $b \in \Sigma(S)$ and distinguish two cases.

CASE 1: $h \ge n$.

If $b = 0$, then $0^n \,|\, S$ and $0 = \sigma(0^n) \subset \Sigma_n(S)$. Suppose that $b \ne 0$. Since $b \in \Sigma(S)$, there is a subsequence T' of T with $b = \sigma(T')$. Since $\mathsf D(G) \le n$, we may assume that $|T'| \le n$. This implies that $T'0^{n-|T'|} \,|\, S$ and $b = \sigma(T'0^{n-|T'|}) \subset \Sigma_n(S)$.

CASE 2: $h \le n-1$.

If $b \ne 0$, then $b \in \Sigma(T)$. If $b = 0$, then $n+k-h \ge k+1$, and thus the assumption implies that $b \in \Sigma(T)$. Therefore in both cases we have $b \in \Sigma(T)$, and we assert that there is a subsequence U of T with $b = \sigma(U)$ and $|U| \in [n-h, n]$. If this holds, then $U0^{n-|U|} \,|\, S$ and $b = \sigma(U0^{n-|U|}) \in \Sigma_n(S)$.

Let U be a subsequence of T of maximal length such that $b = \sigma(U)$. By the maximality of $|U|$ it follows that $0 \notin \Sigma(U^{-1}T)$ and hence $|U^{-1}T| \le k$ by assumption. This implies that $|U| \ge |T| - k = n - h$. If $|U| \le n$, then we are done. Suppose that $|U| > n$. By Proposition 6.9, U admits a product decomposition $U = U_1 \cdot \ldots \cdot U_\varphi U'$ where all $U_i \in \mathcal B(G)$ are of length $|U_i| \le h$ for $i \in [1,\varphi]$ and $U' \in \mathcal F(G)$ with $n - h \le |U'| \le n$. Since $b = \sigma(U) = \sigma(U')$, the sequence U' has the required property. □

Although Proposition 7.12 is a straightforward consequence of the main result 7.16, we give a simple independent proof based on Proposition 7.13.

Proof of Proposition 7.12. (a) $\Rightarrow$ (b) Let $S \in \mathcal F(G)$ be a sequence of length $2n-2$ which has no zero-sum subsequence of length n, that is $0 \notin \Sigma_n(S)$. For every $g \in G$ we have $|g+S| = 2n-2 \ge n$, hence $0 \in \Sigma(g+S)$ and consequently $\Sigma_n(S) \ne \bigcap_{g \in G} \Sigma(g+S)$. By Proposition 7.13, there is some $g \in G$ and some subsequence T of S such that $|T| = n-1$ and $g+T$ is zero-sum free. Then Corollary 4.4 implies that $g+T = a^{n-1}$ and thus $T = (a-g)^{n-1}$. Let $c = a-g$ and $S = c^{n-1}U$ for some sequence $U \in \mathcal F(G)$. Then $-c+S = 0^{n-1}(-c+U)$. Since $-c+S$ has no zero-sum subsequence of length n, it follows that $-c+U$ is zero-sum free whence $-c+U = d^{n-1}$ for some $d \in G$ with $\operatorname{ord}(d) = n$. Thus it follows that $S = c^{n-1}(c+d)^{n-1}$.

(b) $\Rightarrow$ (a) Since $\operatorname{ord}(g-h) = n$, the shifted sequence $-h+S = 0^{n-1}(g-h)^{n-1}$ has no zero-sum subsequence of length n, and hence S has no zero-sum subsequence of length n. □

We continue with a simple observation which will be need frequently in the sequel. Let $g \in G$ with $\operatorname{ord}(g) = n$ and $S = (n_1g) \cdot \ldots \cdot (n_lg)$ where $l \in \mathbb N_0$ and $n_1, \ldots, n_l \in [1,n]$. Then $n\|S\|_g = n_1 + \ldots + n_l$,

$$g - S = \big((n-n_1+1)g\big) \cdot \ldots \cdot \big((n-n_l+1)g\big)$$

and

$$n\|g-S\|_g = \sum_{i=1}^{l}(n-n_i+1) = \sum_{\substack{i=1\\ n_i \ne n}}^{l}(n-n_i) + |S|\,.$$

Proposition 7.14. *Let G be cyclic of order $n \ge 3$, $k \in [1,n-1]$, $g \in G$ with $\operatorname{ord}(g) = n$ and $S, S_1, S_2 \in \mathcal F(G)$ such that $S = S_1S_2$, $|S| = n+k-1$, $\|S_1\|_g < 1$ and $\|g-S_2\|_g < 1$.*

1. *S has no zero-sum subsequence of length n.*
2. *$k \le |S_1| < n$, $k \le |S_2| < n$ and $b - a \ge k$ where $a, b \in [1,n]$, $(ag) \,|\, S_1$ and $(bg) \,|\, S_2$. In particular, $\gcd(S_1, S_2) = 1$.*
3. (i) *We have*

$$\mathsf v_g(S) + \mathsf v_0(S) \ge 2k, \ \max\{\mathsf v_g(S), \mathsf v_0(S)\} \ge k \quad \text{and} \quad \min\{\mathsf v_g(S), \mathsf v_0(S)\} \ge 2k-n+1\,.$$

   (ii) *The following statements are equivalent:*
      (a) *$\mathsf v_g(S) + \mathsf v_0(S) = 2k$.*
      (b) *$S_1 = g^{2p-n+1}(2g)^{n-1-p}$ and $S_2 = 0^{2q-n+1}(-g)^{n-1-q}$ where $p, q \in [(n-1)/2, n-1]$ and $p+q = n+k-1$.*

   (iii) *The following statements are equivalent:*

(a) *$\max\{\mathsf{v}_g(S), \mathsf{v}_0(S)\} = k$.*

(b) *$n+k$ is odd, $S_1 = g^k (2g)^{(n-k-1)/2}$ and $S_2 = 0^k(-g)^{(n-k-1)/2}$.*

4. *If $k \ge \frac{n-1}{2}$, then $\mathsf{h}(S) = \max\{\mathsf{v}_g(S), \mathsf{v}_0(S)\}$.*

Proof. 1. Let $S' = S_1' S_2'$ be a zero-sum subsequence of S where $S_1' \mid S_1$ and $S_2' \mid S_2$. We set

$$S_1' = (a_1 g) \cdot \ldots \cdot (a_r g) \quad \text{and} \quad S_2' = (b_1 g) \cdot \ldots \cdot (b_s g)$$

where $r, s \in \mathbb{N}_0$ and $a_1, \ldots, a_r, b_1, \ldots, b_s \in [1, n]$. Since S' has sum zero, we infer that $\sum_{i=1}^r a_i \equiv \sum_{j=1}^s (n - b_j) \mod n$. Since $0 \le \sum_{i=1}^r a_i \le n \|S_1\|_g < n$ and

$$0 \le \sum_{j=1}^{s} (n - b_j) \le n \|g - S_2\|_g - |S_2| < n - |S_2| \le n \,,$$

we infer that $r \le \sum_{i=1}^r a_i = \sum_{j=1}^s (n - b_j) < n - |S_2|$ and hence $|S'| = |S_1' S_2'| \le r + |S_2| < n$.

2. Since $|S_1 S_2| = n + k - 1$, $|S_1| \le n \|S_1\|_g < n$ and $|S_2| = |g - S_2| \le n \|g - S_2\|_g < n$, we obtain the first two inequalities. We set

$$M = \max\{a \in [1,n] \mid (ag) \mid S_1\} + \max\{n - b + 1 \mid b \in [1,n], (bg) \mid S_2\} \,.$$

Then

$$2(n-1) \ge n\|S_1\|_g + n\|g - S_2\|_g \ge M + (|S_1| - 1) + (|S_2| - 1) \ge M + n + k - 3 \,,$$

and hence $M \le n - k + 1$. If $a, b \in [1, n]$ such that $(ag) \mid S_1$ and $(bg) \mid S_2$, then $a + n - b + 1 \le M \le n - k + 1$ and hence $b - a \ge k$.

3.(i) Since $\|S_1\|_g < 1$, we get $0 \nmid S_1$ and thus $\mathsf{v}_0(S) = \mathsf{v}_0(S_2)$. Similarly, we get $\mathsf{v}_g(S) = \mathsf{v}_g(S_1)$. We have

$$n - 1 \ge n \|S_1\|_g \ge \mathsf{v}_g(S_1) + 2(|S_1| - \mathsf{v}_g(S_1)) = 2|S_1| - \mathsf{v}_g(S)$$

and

$$n - 1 \ge n\|g - S_2\|_g \ge \mathsf{v}_0(S_2) + 2(|S_2| - \mathsf{v}_0(S_2)) = 2|S_2| - \mathsf{v}_0(S) \,.$$

Adding these two inequalities we obtain

$$(*) \qquad 2(n-1) \ge 2|S| - (\mathsf{v}_g(S) + \mathsf{v}_0(S)) = 2(n + k - 1) - (\mathsf{v}_g(S) + \mathsf{v}_0(S))$$

and hence $\mathsf{v}_g(S) + \mathsf{v}_0(S) \ge 2k$. Using 2., we get $k \le \max\{\mathsf{v}_g(S), \mathsf{v}_0(S)\} \le n - 1$ and thus $\min\{\mathsf{v}_g(S), \mathsf{v}_0(S)\} \ge 2k - n + 1$.

3.(ii) The implication (b) $\Rightarrow$ (a) is obvious, and hence it suffices to show that (a) $\Rightarrow$ (b).

The equality $\mathsf{v}_g(S) + \mathsf{v}_0(S) = 2k$ holds if and only if $n - 1 = 2|S_1| - \mathsf{v}_g(S)$ and $n - 1 = 2|S_2| - \mathsf{v}_0(S)$. These conditions imply that $S_1 = g^{\mathsf{v}_g(S_1)} (2g)^{\mathsf{v}_{2g}(S_1)}$, $S_2 = 0^{\mathsf{v}_0(S_2)} (-g)^{\mathsf{v}_{-g}(S_2)}$, $\mathsf{v}_g(S_1) = 2|S_1| - n + 1 \ge 0$ and $\mathsf{v}_0(S_2) = 2|S_2| - n + 1 \ge 0$. Using 2. we infer that $|S_i| \in [n-1)/2, n-1]$ for $i \in \{1, 2\}$. Now setting $p = |S_1|$ and $q = |S_2|$ we obtain the assertion.

3.(iii) Again it suffices to show that (a) $\Rightarrow$ (b). Suppose that $\max\{\mathsf{v}_g(S), \mathsf{v}_0(S)\} = k$. Since $\mathsf{v}_g(S) + \mathsf{v}_0(S) \ge 2k$, it follows that $\mathsf{v}_g(S) = \mathsf{v}_0(S) = k$. Thus we have again equality in $(*)$ and in the two previous inequalities, which implies the assertion.

4. Since $\mathsf{v}_g(S) + \mathsf{v}_0(S) \ge 2k$ and $k \ge \frac{n-1}{2}$, it follows that

$$|g^{-\mathsf{v}_g(S)} 0^{-\mathsf{v}_0(S)} S| \le |S| - 2k = n - 1 - k \le k \,.$$

By 3. we have $\max\{\mathsf{v}_g(S), \mathsf{v}_0(S)\} \ge k$, and thus the assertion follows. □

Lemma 7.15. *Let $g \in G$ with $\operatorname{ord}(g) = n \ge 2$ and $S \in \mathcal{F}(\langle g \rangle)$ with $2|S| > n\|S\|_g$.*

1. *$\mathsf{v}_g(S) \ge 2|S| - n\|S\|_g$.*
2. *For every $x \in [2|S| - n\|S\|_g, n\|S\|_g]$ there is a subsequence S' of S with $|S'| \ge 2|S| - n\|S\|_g$ and $\sigma(S') = xg$.*

Proof. 1. We set $S = g^{\mathsf{v}_g(S)}(a_1 g) \cdot \ldots \cdot (a_k g)$ where $k \in \mathbb{N}_0$ and $a_1, \ldots, a_k \in [2, n]$. Since $2(\mathsf{v}_g(S) + k) = 2|S| > n\|S\|_g = \mathsf{v}_g(S) + a_1 + \ldots + a_k$, it follows that

$$0 < 2|S| - n\|S\|_g = 2|S| - (\mathsf{v}_g(S) + a_1 + \ldots + a_k) = \mathsf{v}_g(S) - \sum_{i=1}^{k} (a_i - 2) \le \mathsf{v}_g(S) .$$

2. We start with the following assertion.

A. Let $k \in \mathbb{N}$ and $1 = a_0, a_1, \ldots, a_k \in \mathbb{N}$ such that $a_1 + \ldots + a_i \le 2i$ for all $i \in [1, k]$. Then

$$\Big\{ \sum_{i \in I} a_i \mid \emptyset \ne I \subset [0, k] \Big\} = \Big[1, \sum_{\nu=0}^{k} a_\nu \Big] .$$

Proof of **A**. We proceed by induction on k. If $k = 1$, then $a_1 \le 2$, and hence the assertion follows. Suppose that $k \ge 2$ and that the assertion holds for $k - 1$. Then

$$\begin{aligned} \Big\{ \sum_{i \in I} a_i \mid \emptyset \ne I \subset [0, k] \Big\} &= \Big\{ \sum_{i \in I} a_i \mid \emptyset \ne I \subset [0, k-1] \Big\} \cup \{a_k\} \cup \Big\{ a_k + \sum_{i \in I} a_i \mid \emptyset \ne I \subset [0, k-1] \Big\} \\ &= \Big[1, \sum_{\nu=0}^{k-1} a_\nu \Big] \cup \{a_k\} \cup \Big[1 + a_k, \sum_{\nu=0}^{k} a_\nu \Big] . \end{aligned}$$

Since $2 \sum_{\nu=0}^{k-1} a_\nu \ge 2k \ge a_1 + \ldots + a_k$, we infer that $a_k \le 1 + \sum_{\nu=0}^{k-1} a_\nu$, and thus **A** follows.

We set $m = 2|S| - n\|S\|_g$ and $S = g^m (a_1 g) \cdot \ldots \cdot (a_{|S|-m} g)$ where $1 \le a_1 \le \ldots \le a_{|S|-m} \le n$. Then $a_1 + \ldots + a_{|S|-m} = n\|S\|_g - m = 2(|S| - m)$ and hence

$$a_1 \le \frac{a_1 + a_2}{2} \le \frac{a_1 + a_2 + a_3}{3} \le \ldots \le \frac{a_1 + \ldots + a_{|S|-m}}{|S| - m} = 2 ,$$

which implies that $a_1 + \ldots + a_i \le 2i$ for all $i \in [1, |S| - m]$. Pick $x \in [2|S| - n\|S\|_g, n\|S\|_g] = [m, 2|S| - m]$ and set $y = x - (m - 1) \in [1, 2(|S| - m) + 1]$. Then **A** implies that the sequence $g(a_1 g) \cdot \ldots \cdot (a_{|S|-m} g)$ has a subsequence S'' with $\sigma(S'') = yg$. Then $S' = g^{m-1} S''$ is a subsequence of S with $|S'| \ge m$ such that $\sigma(S') = xg$. □

Let $\exp(G) = n$ and $S \in \mathcal{F}(G)$. Obviously, S has no zero-sum subsequence of length n if and only if $-g + S$ has no zero-sum subsequence of length n for any $g \in G$. Thus the investigation of sequences, that have no zero-sum subsequences of length n, can be restricted to those sequences T with $\mathsf{h}(T) = \mathsf{v}_0(T)$.

Theorem 7.16 (Savchev-Chen). *Let G be cyclic of order $n \ge 3$ and $S \in \mathcal{F}(G)$ a sequence of length $|S| \ge \frac{3n-1}{2}$. Then the following statements are equivalent*:

(a) *S has no zero-sum subsequence of length n and $\mathsf{h}(S) = \mathsf{v}_0(S)$.*

(b) *$S = S_1 S_2$ where $S_1, S_2 \in \mathcal{F}(G)$ with $\|S_1\|_g < 1$ and $\|g - S_2\|_g < 1$ for some $g \in G$ with $\operatorname{ord}(g) = n$.*

Proof. (a) $\Rightarrow$ (b) We set $S = 0^{\mathsf{h}(S)} S'$ with $S' \in \mathcal{F}(G)$. Then (a) and the in particular statement of Proposition 7.13 imply that for every zero-sum subsequence T of S we have $|T| < n$. In particular, $\mathsf{v}_0(S) < n$.

Let T be a zero-sum subsequence of S' of maximal length. Thus $U = T^{-1} S'$ is zero-sum free, $|T| + \mathsf{h}(S) < n$ and $|U| \ge \frac{3n-1}{2} - (n - 1) = \frac{n+1}{2}$. By Theorem 7.8.1, there is some $g \in G$ with $\operatorname{ord}(g) = n$ such that U is g-smooth. We set

$$T = g^{\mathsf{v}_g(T)} (b_1 g) \cdot \ldots \cdot (b_q g)$$

where $q \in \mathbb{N}_0$ and $b_1, \ldots, b_q \in [2, n-1]$. We continue with the following two assertions.

A1. Let $I \subset [1,q]$ such that $\varphi = n - \sum_{i \in I}(n-b_i) \in [2, n\|U\|_g]$. Then

$$|I| \ge \begin{cases} 2|U| - n\|U\|_g & \text{if} \quad \varphi \in [2|U| - n\|U\|_g, n\|U\|_g]\,, \\ \varphi & \text{if} \quad \varphi \in [2, 2|U| - n\|U\|_g - 1]\,, \end{cases}$$

and $b_i > n\|U\|_g$ for all $i \in [1,q]$.

A2. $n\|U\|_g + \sum_{j=1}^q (n-b_j) < n$.

Suppose that **A2** holds. We set

$$S_1 = g^{\mathsf v_g(T)} U \quad \text{and} \quad S_2 = 0^{\mathsf v_0(S)}(b_1 g) \cdot \ldots \cdot (b_q g)\,,$$

and then clearly $S = S_1 S_2$. Since T has sum zero, we get $\mathsf v_g(T) \equiv \sum_{j=1}^q (n-b_j) \mod n$. Because S has no zero-sum subsequence of length n, we have $\mathsf v_g(T) \in [0, n-1]$, and by **A2** we have $\sum_{j=1}^q (n-b_j) < n$. Thus $\mathsf v_g(T) = \sum_{j=1}^q (n-b_j)$, and again by **A2** we infer that $n\|S_1\|_g = \mathsf v_g(T) + n\|U\|_g < n$. Furthermore, it follows that

$$n\|g - S_2\|_g = \sum_{j=1}^q (n-b_j) + \big(\mathsf v_0(S) + q\big) = \mathsf v_g(T) + \mathsf h(S) + q = |T| + \mathsf h(S) < n\,.$$

Proof of **A1**. Note that $2|U| - n\|U\|_g \ge 2|U| - (n-1) \ge 2$.

Let $\varphi \in [2|U| - n\|U\|_g, n\|U\|_g] \subset [2, n-1]$. By Lemma 7.15.2 there is a subsequence U' of U with $|U'| \ge 2|U| - n\|U\|_g$ and $\sigma(U') = \varphi g = \big(\sum_{i \in I} b_i\big) g$. This implies that $|I| \ge |U'| \ge 2|U| - n\|U\|_g$, because $|I| < |U'|$ and replacing $\prod_{i \in I}(b_i g)$ by U' would yield a zero-sum subsequence T' of S with $|T'| > |T|$, a contradiction to the maximality of $|T|$.

Let $\varphi \in [2, 2|U| - n\|U\|_g - 1]$. By Lemma 7.15.1 there is a subsequence $U' = g^\varphi$ of U with $\sigma(U') = \varphi g = \big(\sum_{i \in I} b_i\big) g$. As above it follows that $|I| \ge |U'| = \varphi$.

Let $i \in [1,q]$ and assume to the contrary that $b_i \le n\|U\|_g$. Then $2 \le b_i = n - (n-b_i) \le n\|U\|_g$, which yields a contradiction to the lower bound of $|I|$ for $I = \{i\}$.

Proof of **A2**. If $q = 0$, then the assertion follows because U is g-smooth. Assume to the contrary that $q \ge 1$ and $n\|U\|_g + \sum_{j=1}^q (n-b_j) \ge n$. Thus there is some minimal $I \subset [1,q]$, say $I = [1,m]$, such that $\varphi = n - \sum_{j=1}^m (n-b_j) \le n\|U\|_g$, and hence $\varphi + (n-b_j) > n\|U\|_g$ for all $j \in [1,m]$. Since $b_m > n\|U\|_g$ by **A1**, we get

$$\varphi > n\|U\|_g - (n-b_m) > n\|U\|_g - (n - n\|U\|_g) = 2n\|U\|_g - n \ge 2|U| - n \ge 1\,.$$

If $\varphi \in [2|U| - n\|U\|_g, n\|U\|_g]$, then **A1** implies $m \ge 2|U| - n\|U\|_g$ and hence

$$n\|U\|_g + 1 \le n - \sum_{j=1}^{m-1}(n-b_j) \le n - (m-1) \le n - (2|U| - n\|U\|_g - 1) = (n - 2|U|) + n\|U\|_g + 1\,,$$

a contradiction to $2|U| \ge n+1$.

Suppose that $\varphi \in [2, 2|U| - n\|U\|_g - 1]$. Then **A1** implies $m \ge \varphi$, and since $n - b_j \ge n\|U\|_g + 1 - \varphi > 0$ for all $j \in [1,m]$, we infer that

$$n = \varphi + \sum_{j=1}^m (n-b_j) \ge \varphi + m\big(n\|U\|_g + 1 - \varphi\big) \ge \varphi + \varphi\big(n\|U\|_g + 1 - \varphi\big) = \varphi\big(n\|U\|_g + 2 - \varphi\big)\,.$$

Consider the quadratic function $f\colon \mathbb R \to \mathbb R$, defined by $f(x) = x^2 - (n\|U\|_g + 2)x + n$ for all $x \in \mathbb R$, and observe that the above inequality states that $f(\varphi) \ge 0$. However, the maximum value of f in the interval between 2 and $2|U| - n\|U\|_g - 1$ equals $f(2) = n - 2n\|U\|_g \le n - 2|U| < 0$, a contradiction.

(b) $\Rightarrow$ (a) This follows from Proposition 7.14. □

Remarks 7.17. Let G be cyclic of order $n \ge 3$.

1. Let $S \in \mathcal{F}(G)$ be a sequence of length $n+k-1$, with $k \in [(n+1)/2, n-1]$, that has no zero-sum subsequence of length n, and suppose that $\mathsf{h}(S) = \mathsf{v}_0(S)$. Then Theorem 7.16 and Proposition 7.14 give structural information on S. In particular, we get $\mathsf{v}_g(S) + \mathsf{v}_0(S) \ge 2k$. Thus if $k = n-1$, we obtain the description of S given in Proposition 7.12.

2. We give an example of a sequence S of length $|S| = \lfloor (3n-2)/2 \rfloor$, that has no zero-sum subsequence of length n, but that does not satisfy the structural description given in Theorem 7.16.(b). For an element $h \in G$ with $\operatorname{ord}(h) = n$, where $n \ge 9$ for odd n and $n \ge 6$ for even n, we set

$$S = \begin{cases} 0^{n-1}(2h)^{\frac{n}{2}-1}(3h) & \text{if} \quad n \quad \text{is even,} \\ 0^{n-1}(2h)^{\frac{n-5}{2}}(3h)^2 & \text{if} \quad n \quad \text{is odd.} \end{cases}$$

Obviously, S has the asserted length and no zero-sum subsequence of length n. Assume to the contrary that there exists an element $g \in G$ with $\operatorname{ord}(g) = n$ such that the condition in Theorem 7.16.(b) holds. Then Proposition 7.14.4 implies that $n-1 = \mathsf{h}(S) = \max\{\mathsf{v}_g(S), \mathsf{v}_0(S)\}$, and hence $S_2 = 0^{n-1}$. Then $S_1 = S^{-1}S$ and $\|S_1\|_g \ge 1$, a contradiction.

7.B Groups of higher rank

We focus on groups of the form $G = C_n^r$, with $n, r \in \mathbb{N}$ and $n \ge 2$, and start our discussion with the following two properties.

Property C. Every sequence S over G of length $|S| = \eta(G) - 1$ that has no zero-sum subsequence of length in $[1, n]$ has the form $S = T^{n-1}$ for some sequence T over G.

Property D. Every sequence S over G of length $|S| = \mathsf{s}(G) - 1$ that has no zero-sum subsequence of length n has the form $S = T^{n-1}$ for some sequence T over G.

For groups of rank two, Property **C** was first considered by P. van Emde Boas and Property **D** by W. Gao (see [30, 45], [44, Lemma 4.7]).

If $r = 1$, then G has Property **D** by Proposition 7.12. It follows from the very definition that C_2^r satisfies Property **D**, and a straightforward argument shows that C_3^r satisfies Property **D** (see [28, Lemma 2.3.3] and the subsequent discussion). In [51, Conjecture 7.2] it is conjectured that every group $G = C_n^r$, where $r \in \mathbb{N}$ and $n \in \mathbb{N}_{\ge 2}$, has Property **D** (see [129, 57]. Groups of rank two will be considered in some detail below.

Following [47, Proposition 2.7] and [64], we work out the relationship between Property **C** and Property **D**. We need the technical Property **D1** for an (arbitrary group G) with $\exp(G) = n$.

Property D1. Every sequence S over G of length $|S| = \mathsf{s}(G) - 1$ that has no zero-sum subsequence of length n satisfies $\mathsf{h}(S) \ge \lfloor \frac{n-1}{2} \rfloor$.

Lemma 7.18. *Let* $\exp(G) = n$ *and* $S \in \mathcal{F}(G)$.

1. *If* $g \in G$ *with* $\mathsf{v}_g(S) \ge \lfloor \frac{n-1}{2} \rfloor$ *and* S *has no zero-sum subsequence of length* n*, then* S *has a subsequence* T *of length* $|T| \ge |S| - n + 1$ *such that* $-g + T$ *has no short zero-sum subsequence.*
2. *If* $i \in [1, (n+2)/2]$ *and* $|S| = \eta(G) + i - 1$*, then* S *has a zero-sum subsequence* T *of length* $|T| \in [i, n]$.
3. *If* $|S| = \eta(G) + n - 1$ *and* $\mathsf{h}(S) \ge \lfloor \frac{n-1}{2} \rfloor$*, then* S *has a zero-sum subsequence of length* n.
4. *If* G *has Property* **D1***, then* $\mathsf{s}(G) = \eta(G) + n - 1$.

Proof. 1. Without restriction we may suppose that $g = 0$, say $S = 0^v R$ with $v \ge \lfloor \frac{n-1}{2} \rfloor$ and $R \in \mathcal{F}(G)$. Let U be a zero-sum subsequence of R such that $|U| \le n$ is maximal. Then, by the maximality of $|U|$, either $|U| > n/2$ or $U^{-1}R$ has no short zero-sum subsequence. Since S has no zero-sum subsequence of length n, it follows that $|U|+v<n$. Thus $|U| \le n/2$ and $T=U^{-1}R$ has no short zero-sum subsequence. Since $|S|=|T|+|U|+v$ and $|U|+v<n$, we obtain that $|T|>|S|-n$.

2. We proceed by induction on i. For $i=1$, the assertion is clear. Now suppose the assertion holds for $i \in [1,n/2]$, and we have to show it for $i+1$. Then S has a zero-sum subsequence T_1 of length $|T_1| \in [i,n]$. If $|T_1| \ge i+1$, then we are done. Otherwise, $|T_1|=i$ and $|T_1^{-1}S| \ge \eta(G)$. Thus $T_1^{-1}S$ has a short zero-sum subsequence T_2. If $|T_2| \ge i+1$, then we are done. Otherwise, $|T_2| \in [1,i]$ and T_1T_2 is a zero-sum subsequence of S of length $1+i \le |T_1T_2| \le 2i \le n$.

3. We may suppose that $S=0^vR$ with $v \ge \lfloor \frac{n-1}{2} \rfloor$ and $R \in \mathcal{F}(G)$. If $v \ge n$, then we are done. Suppose that $v \le n-1$. Since $|R|=\eta(G)+n-1-v$ and $1 \le n-v \le (n+2)/2$, 2. implies that R has a zero-sum subsequence T of length $|T| \in [n-v,n]$. Thus $0^{n-|T|}|T|$ is a zero-sum subsequence of S of length n.

4. Lemma 6.5.1 implies that $\mathsf{s}(G) \ge \eta(G)+n-1$. Let $S \in \mathcal{F}(G)$ be a sequence of length $|S|=\mathsf{s}(G)-1$ that has no zero-sum subsequence of length n. By Property **D1** we have $\mathsf{h}(S) \ge \lfloor \frac{n-1}{2} \rfloor$, and hence 3. implies that $\mathsf{s}(G)-1=|S| \le \eta(G)+n-2$. □

Proposition 7.19. *Let $G=C_n^r$ with $r,n \ge 2$. Then the following statements are equivalent:*

(a) *G has Property* **D**.

(b) *G has Properties* **C** *and* **D1**.

Proof. (a) ⇒ (b) By definition, G has Property **D1**. To show that G satisfies Property **C** as well, let $S \in \mathcal{F}(G)$ be a sequence of length $\eta(G)-1$ which has no short zero-sum subsequence. We consider the sequence

$$T=0^{n-1}S\,.$$

If T has a zero-sum subsequence T' of length $|T'|=n$, then $T'=0^kS'$ with $k' \in [0,n-1]$ whence S' is a short zero-sum subsequence of S. Since Property **D** holds, Lemma 7.18.4 implies that $|T|=\eta(G)-1+(n-1)=\mathsf{s}(G)-1$. Therefore Property **D** implies that S has the required form.

(b) ⇒ (a) Let $S \in \mathcal{F}(G)$ be a sequence of length $|S|=\mathsf{s}(G)-1$ that has no zero-sum subsequence of length n. By Property **D1**, S may be written in the form $S=g^{\mathsf{h}(S)}S'$ where $g \in$G, $S' \in \mathcal{F}(G)$ and $\mathsf{h}(S) \ge \lfloor \frac{n-1}{2} \rfloor$. By Lemma 7.18.1, S has a subsequence T of length $|T| \ge |S|-n+1 \ge \eta(G)-1$ such that $-g+T$ has no short zero-sum subsequence. Clearly, we may suppose that $|T|=\eta(G)-1$. Since G has Property **C**, it follows that there are $a_1,\ldots,a_k \in G$ such that $-g+T=(a_1\cdot\ldots\cdot a_k)^{n-1}$. Since $0 \notin \{a_1,\ldots,a_k\}$, it follows that $T \,|\, S'$. This implies that $\mathsf{h}(S)=n-1$ and hence $S=\big(g(g+a_1)\cdot\ldots\cdot(g+a_k)\big)^{n-1}$. □

Suppose that Property **D** holds. Then, by definition, there exists some $c(G) \in \mathbb{N}$ such that $\mathsf{s}(G)=c(G)(n-1)+1$. For $r=1$ we have $\mathsf{c}(G)=2$ and for $r=2$ we have $c(G)=4$ (see Theorem 6.13). In case of higher ranks bounds for $c(G)$ are given by N. Alon and M. Dubiner ([2]) and then in [100, 29, 28, 27]).

Property **C** and Property **D** are both multiplicative, provided that the $c(\cdot)$-invariants of all involved groups coincide (see [56, Theorem 3.2]).

Theorem 7.20. *Let $G=C_{mn}^r$ with $m,n,r \in \mathbb{N}$.*

1. *If both C_m^r and C_n^r have Property* **D** *and*

$$\frac{\mathsf{s}(C_m^r)-1}{m-1}=\frac{\mathsf{s}(C_n^r)-1}{n-1}=\frac{\mathsf{s}(C_{mn}^r)-1}{mn-1}\,,$$

then G has Property **D**.

2. *If both C_m^r and C_n^r have Property* **C** *and*

$$\frac{\eta(C_m^r)-1}{m-1}=\frac{\eta(C_n^r)-1}{n-1}=\frac{\eta(C_{mn}^r)-1}{mn-1}\,,$$

then G has Property **C**.

From now on we restrict our discussion on groups of rank two. For $G = C_n \oplus C_n$ with $n \ge 2$ the following property was first addressed in [48].

Property B. Every minimal zero-sum sequence S over G of length $|S| = \mathsf{D}(G) = 2n-1$ contains some element with multiplicity $n-1$.

It is conjectured that every group of the above form satisfies Property **B**. Several equivalent conditions to Property **B** may be found in [71, Section 5.8]. Proposition 7.23 shows that if G satisfies one of the Properties **B**, **C** or **D**, then the structure of the extremal sequences is completely determined. In order to work this out we need some preparations.

Lemma 7.21. *Let $G = C_n \oplus C_n$ with $n \ge 2$ and $S \in \mathcal{F}(G)$. If $|S| = 3n-3$ and S has no short zero-sum subsequence, then S has a minimal zero-sum subsequence T of length $|T| = 2n-1$.*

Proof. Suppose that $|S| = 3n-3$, that S has no short zero-sum subsequence and set $W = 0S \in \mathcal{F}(G)$. Then Corollary 6.14 implies that W has a zero-sum subsequence U of length $|U| \in \{n, 2n\}$, and by our assumption on S we get $|U| = 2n$. If U is a subsequence of S, then $\mathsf{D}(G) = 2n-1$ implies that $U = U_1U_2$, where both U_1 and U_2 are nontrivial zero-sum sequences. Therefore, either U_1 or U_2 is a short zero-sum subsequence of S, a contradiction. Therefore, $U = 0T$ with $|T| = 2n-1$, and since S has no short zero-sum subsequence, it follows that T is a minimal zero-sum sequence. □

Theorem 7.22. *Let $G = C_n \oplus C_n$ with $n \ge 2$ and let $S \in \mathcal{A}(G)$ be a minimal zero-sum sequence of length $|S| = 2n-1$.*

1. *For every $g \in \operatorname{supp}(S)$ we have $\operatorname{ord}(g) = n$.*
2. *If $|\operatorname{supp}(S)| = 3$, then S contains some element with multiplicity $n-1$.*
3. *If G has Property **B**, then G has Property **C**.*

Proof. 1. See [71, Theorem 5.8.4]. The proof is done by the inductive method.

2. See [101, Theorem 1]. The proof uses the theory of continued fractions.

3. By Corollary 6.14 this follows from [49, Theorem 6.2]. □

Proposition 7.23. *Let $G = C_n \oplus C_n$ with $n \ge 2$ and let $S \in \mathcal{F}(G)$.*

1. *If S has length $\mathsf{D}(G)$, then the following statements are equivalent:*
   (a) *S is a minimal zero-sum sequence and contains some element with multiplicity $n-1$.*
   (b) *There exists a basis (e_1, e_2) of G and integers $x_1, \ldots, x_n \in [0, n-1]$ with $x_1 + \ldots + x_n \equiv 1 \mod n$ such that*
   $$S = e_1^{n-1} \prod_{\nu=1}^{n} (x_\nu e_1 + e_2)\,.$$
2. *If S has length $\eta(G) - 1$, then the following statements are equivalent:*
   (a) *$S = T^{n-1}$ for some $T \in \mathcal{F}(G)$ and S has no short zero-sum subsequence.*
   (b) *There exists a basis (e_1, e_2) of G and some $x \in [1, n-1]$ with $\gcd(x, n) = 1$ such that*
   $$S = \big(e_1 e_2 (x e_1 + e_2)\big)^{n-1}\,.$$
3. *If S has length $\mathsf{s}(G) - 1$, then the following statements are equivalent:*
   (a) *$S = T^{n-1}$ for some $T \in \mathcal{F}(G)$ and S no zero-sum subsequence of length n.*
   (b) *For every $g \in \operatorname{supp}(S)$ there exists a basis (e_1, e_2) of G and some $x \in [1, n-1]$ with $\gcd(x, n) = 1$ such that*
   $$-g + S = \big(0 e_1 e_2 (x e_1 + e_2)\big)^{n-1}\,.$$

Proof. In all three items, the implications (b) $\Rightarrow$ (a) are obvious. Thus it remains to verify the converse.

1. Let $S = {e_1}^{n-1} g_1 \cdot \ldots \cdot g_n$, where $g_1, \ldots, g_n \in G$. Then $\operatorname{ord}(e_1) = n$, and there exists some $\widetilde{e} \in G$ such that $(e_1, \widetilde{e})$ is a basis of G. For $i \in [1,n]$ let $x_i,\ y_i \in [0, n-1]$ be such that $g_i = x_i e_1 + y_i \widetilde{e}$. Since

$$\sigma(S) = (n-1+x_1+\ldots+x_n)e_1 + (y_1+\ldots+y_n)\widetilde{e} = 0\,,$$

we obtain that $x_1+\ldots+x_n \equiv 1 \mod n$, and that $B = (y_1\widetilde{e}) \cdot \ldots \cdot (y_n \widetilde{e})$ has sum zero. We assert that B is even a minimal zero-sum sequence. Indeed, otherwise there exists some $\emptyset \ne I \subsetneq [1,n]$ such that

$$\sum_{i \in I} y_i \equiv 0 \mod n\,.$$

If $k \in [0, n-1]$ is such that

$$\sum_{i \in I} x_i \equiv n-k \mod n\,, \quad \text{then} \quad {e_1}^k \prod_{i \in I} (x_i e_1 + y_i \widetilde{e})$$

has sum zero, a contradiction to $S \in \mathcal{A}(G)$. Now Corollary 4.4.1 implies that $y_1 = \ldots = y_n = y$, where $\gcd(y,n) = 1$, and we set $e_2 = y\widetilde{e}$ to complete the proof.

2. Let $S = T^{n-1}$ be as in 2.(a). By Lemma 7.21, S has a minimal zero-sum subsequence U of length $|U| = 2n-1$. Since $3 = |\operatorname{supp}(S)| = |\operatorname{supp}(U)|$, Theorem 7.22.2 and item 1. imply that U has a form as given in 1.(b). Thus there exists a basis (e_1, e_2) of G such that $T = e_1(x_1e_1+e_2)(x_2e_1+e_2)$ with $0 \le x_1 < x_2 \le n-1$. Clearly, $(f_1, f_2) = (e_1, x_1e_1+e_2)$ is a basis of G and hence $T = f_1 f_2 (x f_1 + f_2)$ with $x \in [1, n-1]$. Assume to the contrary, that $\gcd(x,n) = a > 1$ and set $n' = n/a$. Then $(xf_1+f_2)^{n'} f_2^{n-n'}$ is a short zero-sum subsequence of S, a contradiction.

3. Let $S = T^{n-1}$ be as in 3.(a) and let $g \in \operatorname{supp}(S)$. Then $T = gU$ for some $U \in \mathcal{F}(G)$. Since $-g + U^{n-1}$ has no short zero-sum subsequence, 2. implies that $-g + S$ has the required form. □

The argument in Proposition 7.23.2 stems from [120]. Moreover, in that paper Wolfgang A. Schmid established a characterization of the structure of all minimal zero-sum sequences over $C_{n_1} \oplus C_{n_2}$, where $1 < n_1 \mid n_2$, of length $\mathsf{D}(C_{n_1} \oplus C_{n_2}) = n_1 + n_2 - 1$, under the hypothesis that $C_{n_1} \oplus C_{n_1}$ has Property **B**. Analogous results were derived for Properties **C** and **D**.

The next theorem reduces the question whether Property **B** holds for all groups under discussion to groups $C_p \oplus C_p$ where p is a prime (see [54]). Property **B** is verified for some small primes in [49, 5].

Theorem 7.24. *Let* $G = C_n \oplus C_n$ *with* $n \ge 2$. *If for every prime divisor p of n the group* $C_p \oplus C_p$ *has Property* **B**, *then* G *has Property* **B**.

Theorem 7.25. *Let* $G = C_p \oplus C_p$ *for some odd prime p and let* $S \in \mathcal{F}(G)$.

1. *If S is a minimal zero-sum sequence of length* $|S| = \mathsf{D}(G)$, *then* $|\operatorname{supp}(S)| \in [3, p]$.
2. *If S is zero-sum free of length* $\mathsf{D}(G) - 1$, *then each two distinct elements of* $\operatorname{supp}(S)$ *are independent.*
3. *If S is zero-sum free of length* $\mathsf{D}(G) - 1$, $\varepsilon > 0$ *and p sufficiently large, then S contains some element g with multiplicity* $\mathsf{v}_g(S) > p^{1/4 - \varepsilon}$.

Proof. 1. See [71, Proposition 5.8.5]. Note that for every $j \in [3,p]$ there is an $S_j \in \mathcal{A}(G)$ of length $|S_j| = \mathsf{D}(G)$ and with $|\operatorname{supp}(S_j)| = j$.

2. See [71, Corollary 5.6.9]. The proof is based on a covering result.

3. See [56, Theorem 4.1]. The proof is based on a Theorem of J.A. Dias da Silva and Y. ould Hamidoune ([21]) which runs as follows: if $A \in \mathcal{F}(G)$ is a squarefree sequence and $k \in [1, |A|]$, then

$$|\Sigma_k(A)| \ge \min\{p, k(|A| - k) + 1\}\,. \qquad \square$$

7.C Arithmetical consequences

Some simple arithmetical consequences of Property **B** can be found in [71, Chapter 6]. In this subsection we restrict to cyclic groups and start with a result, first proved in [53] and based on Theorem 7.8.

Theorem 7.26. *Let H be a Krull monoid with cyclic class group G of order $n \ge 2$ such that every class contains a prime. Then for every $k \in \mathbb{N}$ we have $\rho_{2k+1}(H) = kn + 1$.*

Proof. By Theorem 3.16 it suffices to consider $\mathcal{B}(G)$. Assume to the contrary that there is some $k \in \mathbb{N}$ such that $\rho_{2k+1}(G) \ge kn + 2$. Let $k \in \mathbb{N}$ be minimal with this property whence $\rho_{2k-1}(G) = (k-1)n + 1$. Thus there are $B \in \mathcal{B}(G)$ and $U_1, \ldots, U_{2k+1}, V_1, \ldots, V_\rho \in \mathcal{A}(G)$ with $\rho = \rho_{2k+1}(G)$, $|U_1| \ge \ldots \ge |U_{2k+1}|$, $|V_1| \le \ldots \le |V_\rho|$ and

$$(*) \qquad B = U_1 \cdot \ldots \cdot U_{2k+1} = V_1 \cdot \ldots \cdot V_\rho \,.$$

We may suppose that $|B|$ is maximal such that an equation $(*)$ holds. Since $\rho_{2k}(G) = kn$, it follows that $0 \nmid B$ whence $|U_{2k+1}| \ge 2$.

Let $\ell \in [0, \rho]$ such that $|V_\ell| = 2$ and $3 \le |V_{\ell+1}|$, and assume that $(*)$ is a representation with maximal ℓ. Then $h(-h) \nmid V_{\ell+1} \cdot \ldots \cdot V_\rho$ for any $h \in G$. Indeed, assume to the contrary that there are $h \in G$ and distinct $i, j \in [\ell+1, \rho]$ such that $h \,|\, V_i$ and $-h \,|\, V_j$. Then $V_i V_j = h(-h)V'$ with $V' \in \mathcal{B}(G)$, and by the maximality of ρ it follows that $V' \in \mathcal{A}(G)$. But this contradicts the maximal choice of ℓ.

Next we prove that $\ell \ge 1$. If $\ell = 0$, then $3\rho \le |B| \le (2k+1)n$ implies $\rho \le \frac{n}{3}(2k+1) < kn + 1$, a contradiction.

By the maximality of $|B|$ it follows that, for all $i \in [1, 2k+1]$, U_i is not splittable, and we assert that $|U_{2k}| \ge \lfloor \frac{n}{2} \rfloor + 2$. Indeed, assume to the contrary that $|U_{2k}| \le \lfloor \frac{n}{2} \rfloor + 1$. Then

$$2\rho \le |B| \le \Big((2k-1)n + 2\big(\frac{n}{2} + 1\big)\Big) = 2kn + 2\,,$$

and hence $\rho \le kn + 1$, a contradiction. Thus Theorem 7.8 implies that $U_i = g_i^n$ for all $i \in [1, 2k]$.

Assume to the contrary that there are $i, j \in [1, 2k+1]$ such that $U_i = g^n$ and $U_j = (-g)^n$. Then $\ell \ge n$, and after renumbering if necessary we may suppose that $V_1 = \ldots = V_n = (-g)g$. Since $(U_iU_j)^{-1}B = V_{n+1} \cdot \ldots \cdot V_\rho$, it follows that $(k-1)n + 1 = \rho_{2k-1}(G) \ge \rho - n \ge (k-1)n + 2$, a contradiction. Thus there are no two U_i, U_j of such a form and hence $\ell \le |U_{2k+1}|$.

If $|U_{2k+1}| \ge \lfloor \frac{n}{2} \rfloor + 2$, then Theorem 7.8 implies that $U_{2k+1} = g_{2k+1}^n$ for some $g_{2k+1} \in G$. Since $\ell \ge 1$, it follows that $g_{2k+1} \in \{-g_1, \ldots, -g_{2k}\}$, a contradiction. Thus

$$|U_{2k+1}| \le \lfloor \frac{n}{2} \rfloor + 1\,,$$

and therefore we obtain that

$$\rho \le \ell + \frac{|B| - 2\ell}{3} = \frac{|B| + \ell}{3} = \frac{2kn + |U_{2k+1}| + \ell}{3} \le \frac{2kn + 2|U_{2k+1}|}{3} \le \frac{2kn + n + 2}{3} \le kn + \frac{2}{3}\,,$$

a contradiction. □

Corollary 7.27. *Let H be a Krull monoid with cyclic class group G of order $n \ge 2$ such that every class contains a prime. Then for every $k \in \mathbb{N}$ and every $l \in \mathbb{N}_0$ we have $\mathcal{V}_k(H) = [\lambda_k(H), \rho_k(H)]$,*

$$\rho_{2k+j}(H) = kn + j \quad \text{for} \quad j \in [0,1] \quad \text{and} \quad \lambda_{ln+j}(H) = \begin{cases} 2l + j & \text{for} \quad j \in [0,1] \\ 2l + 2 & \text{for} \quad j \in [2, n-1] \end{cases}$$

provided that $ln + j \ge 1$.

Proof. As in the proof of Theorem 5.3 it suffices to consider the block monoid $\mathcal{B}(G)$. If $n = 2$, then $\mathcal{B}(G)$ is half-factorial whence for all $k \in \mathbb{N}$ we have $\lambda_k(G) = k = \rho_k(G)$. Suppose that $n \ge 3$, and let $k \in \mathbb{N}$. By Theorem 5.3 we obtain that $\mathcal{V}_k(H) = [\lambda_k(G), \rho_k(G)]$. The assertion on $\rho_{2k+j}(G)$ follows from Theorem 7.26, and the assertion on $\lambda_{ln+j}(G)$ follows from Corollary 5.4. □

Corollary 7.28. *Let G be either cyclic or an elementary 2-group with Davenport constant $\mathsf{D}(G) = n \ge 4$. If G' is a finite abelian group with $\mathcal{L}(G) = \mathcal{L}(G')$, then $G \cong G'$.*

Proof. Suppose that $\mathcal{L}(G) = \mathcal{L}(G')$. Then Proposition 5.14 implies that $\Delta(G) = \Delta(G')$ and $\rho_k(G) = \rho_k(G')$ for all $k \in \mathbb{N}$. By Corollary 4.16 it follows that G' is either cyclic or an elementary 2-group. Corollary 5.5 and Theorem 7.26 imply that

$$\rho_3(C_n) = n + 1 < \lfloor \frac{3n}{2} \rfloor = \rho_3(C_2^{n-1}),$$

and thus we obtain that $G \cong G'$. □

Acknowledgements. This work was supported by the Centre de Recerca Matemàtica (CRM) at Barcelona and by the Austrian Science Fund FWF, Project No. M1014-N13.

I would like to thank the co-ordinators of the DocCourse, Combinatorics and Geometry 2008, J. Cilleruelo, M. Noy and O. Serra, for their invitation and all their hospitality, and the CRM for providing an excellent working atmosphere.

A special thanks goes to W. Gao, D. Grynkiewicz, F. Halter-Koch, Y. ould Hamidoune and Wolfgang A. Schmid for all their suggestions and helpful comments on previous versions of this manuscript.

References

[1] S.D. Adhikari and P. Rath, *Davenport constants with weights and some related questions*, Integers **6** (2006), Paper A30, 6p.

[2] N. Alon and M. Dubiner, *A lattice point problem and additive number theory*, Combinatorica **15** (1995), 301 – 309.

[3] E. Balandraud, *Une variante de la méthode isopérimétrique de Hamidoune, appliquée au théorème de Kneser*, Ann. Inst. Fourier **58** (2008), 915 – 943.

[4] G. Bhowmik, I. Halupczok, and J.-C. Schlage-Puchta, *Inductive methods and zero-sum free sequences*, manuscript.

[5] ———, *The structure of maximal zero-sum free sequences II*, manuscript.

[6] G. Bhowmik and J.-C. Schlage-Puchta, *Davenport's constant for groups of the form $\mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{3d}$*, Additive Combinatorics, CRM Proceedings and Lecture Notes, vol. 43, Am. Math. Soc., 2008.

[7] A. Bialostocki and P. Dierker, *On the Erdős-Ginzburg-Ziv theorem and the Ramsey numbers for stars and matchings*, Discrete Math. **110** (1992), 1 – 8.

[8] A. Bialostocki, P. Dierker, D. Grynkiewicz, and M. Lotspeich, *On some developments of the Erdős-Ginzburg-Ziv Theorem II*, Acta Arith. **110** (2003), 173 – 184.

[9] B. Bollobás and I. Leader, *The number of k-sums modulo k*, J. Number Theory **78** (1999), 27 – 35.

[10] J.D. Bovey, P. Erdős, and I. Niven, *Conditions for zero sum modulo n*, Can. Math. Bull. **18** (1975), 27 – 29.

[11] Y. Caro, *Zero-sum Ramsey numbers-stars*, Discrete Math. **104** (1992), 1 – 6.

[12] ———, *Zero-sum problems - a survey*, Discrete Math. **152** (1996), 93 – 113.

[13] S.T. Chapman (ed.), *Arithmetical Properties of Commutative Rings and Monoids*, Lect. Notes Pure Appl. Math., vol. 241, Chapman & Hall/CRC, 2005.

[14] S.T. Chapman and J. Coykendall, *Half-factorial domains, a survey*, Non-Noetherian Commutative Ring Theory, Mathematics and Its Applications, vol. 520, Kluwer Academic Publishers, 2000, pp. 97 – 115.

[15] S.T. Chapman, M. Freeze, W. Gao, and W.W. Smith, *On Davenport's constant of finite abelian groups*, Far East J. Math. Sci. **5** (2002), 47 – 54.

[16] S.T. Chapman, M. Freeze, and W.W. Smith, *Minimal zero sequences and the strong Davenport constant*, Discrete Math. **203** (1999), 271 – 277.

[17] S.T. Chapman and W.W. Smith, *Factorization in Dedekind domains with finite class group*, Isr. J. Math. **71** (1990), 65 – 95.

[18] ———, *A characterization of minimal zero-sequences of index one in finite cyclic groups*, Integers **5(1)** (2005), Paper A27, 5p.

[19] X. Chen and P. Yuan, *A note on Kneser's theorem*, JP J. Algebra Number Theory Appl. **6** (2006), 77 – 83.

[20] J. Coykendall, *Extensions of half-factorial domains: a survey*, Arithmetical Properties of Commutative Rings and Monoids, Lect. Notes Pure Appl. Math., vol. 241, Chapman & Hall/CRC, 2005, pp. 46 – 70.

[21] J.A. Dias da Silva and Y. ould Hamidoune, *Cyclic spaces for Grassmann derivatives and additive theory*, Bull. Lond. Math. Soc. **26** (1994), 140 – 146.

[22] J.M. Deshouillers and G.A. Freiman, *A step beyond Kneser's theorem for abelian finite groups*, Proc. Lond. Math. Soc. **86** (2003), 1 – 28.

[23] J.M. Deshouillers, B. Landreau, and A.A. Yudin, *Structure Theory of Set Addition*, vol. 258, Astérisque, 1999.

[24] M. DeVos, *A short proof of Kneser's addition theorem for abelian groups*, manuscript.

[25] M. DeVos, L. Goddyn, and B. Mohar, *A generalization of Kneser's addition theorem*, Adv. Math., to appear.

[26] L. Diracca, *On a generalization of the exchange property to modules with semilocal endomorphism rings*, J. Algebra **313** (2007), 972 – 987.

[27] Y. Edel, *Sequences in abelian groups G of odd order without zero-sum subsequences of length* $\exp(G)$, Des. Codes Cryptography **47** (2008), 125 – 134.

[28] Y. Edel, C. Elsholtz, A. Geroldinger, S. Kubertin, and L. Rackham, *Zero-sum problems in finite abelian groups and affine caps*, Quarterly. J. Math., Oxford II. Ser. **58** (2007), 159 – 186.

[29] C. Elsholtz, *Lower bounds for multidimensional zero sums*, Combinatorica **24** (2004), 351 – 358.

[30] P. van Emde Boas, *A combinatorial problem on finite abelian groups II*, Reports ZW-1969-007, Math. Centre, Amsterdam, 1969.

[31] P. van Emde Boas and D. Kruyswijk, *A combinatorial problem on finite abelian groups*, Reports ZW-1967-009, Math. Centre, Amsterdam, 1967.

[32] P. Erdős, A. Ginzburg, and A. Ziv, *Theorem in the additive number theory*, Bull. Research Council Israel **10** (1961), 41 – 43.

[33] B.W. Finklea, T. Moore, V. Ponomarenko, and Z.J. Turner, *Invariant polynomials and minimal zero sequences*, Involve **1** (2008), 159 – 165.

[34] C. Flores and O. Ordaz, *On the Erdős-Ginzburg-Ziv theorem*, Discrete Math. **152** (1996), 321 – 324.

[35] M. Freeze and A. Geroldinger, *Unions of sets of lengths*, Funct. Approximatio, Comment. Math. **39** (2008), 149 – 162.

[36] G.A. Freiman, *Foundations of a Structural Theory of Set Addition*, Translations of Mathematical Monographs, vol. 37, American Mathematical Society, 1973.

[37] ———, *Structure theory of set addition*, Structure Theory of Set Addition, vol. 258, Astérisque, 1999, pp. 1 – 33.

[38] G.A. Freiman and A. Geroldinger, *An addition theorem and its arithmetical application*, J. Number Theory **85** (2000), 59 – 73.

[39] L. Gallardo, G. Grekos, L. Habsieger, F. Hennecart, B. Landreau, and A. Plagne, *Restricted addition in* $\mathbb{Z}/n\mathbb{Z}$ *and an application to the Erdős-Ginzburg-Ziv problem*, J. Lond. Math. Soc. **65** (2002), 513 – 523.

[40] L. Gallardo, G. Grekos, and J. Pihko, *On a variant of the Erdős-Ginzburg-Ziv problem*, Acta Arith. **89** (1999), 331 – 336.

[41] W. Gao, *Addition theorems for finite abelian groups*, J. Number Theory **53** (1995), 241 – 246.

[42] ———, *A combinatorial problem on finite abelian groups*, J. Number Theory **58** (1995), 100 – 103.

[43] ———, *An addition theorem for finite cyclic groups*, Discrete Math. **163** (1997), 257 – 265.

[44] ———, *On Davenport's constant of finite abelian groups with rank three*, Discrete Math. **222** (2000), 111 – 124.

[45] ———, *Two zero sum problems and multiple properties*, J. Number Theory **81** (2000), 254 – 265.

[46] ———, *Zero sums in finite cyclic groups*, Integers **0** (2000), Paper A14, 9p.

[47] ———, *On zero sum subsequences of restricted size II*, Discrete Math. **271** (2003), 51 – 59.

[48] W. Gao and A. Geroldinger, *On long minimal zero sequences in finite abelian groups*, Period. Math. Hung. **38** (1999), 179 – 211.

[49] ———, *On zero-sum sequences in* $\mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$, Integers **3** (2003), Paper A08, 45p.

[50] ———, *On a property of minimal zero-sum sequences and restricted sumsets*, Bull. Lond. Math. Soc. **37** (2005), 321 – 334.

[51] ———, *Zero-sum problems in finite abelian groups: a survey*, Expo. Math. **24** (2006), 337 – 369.

[52] ———, *On the number of subsequences with given sum of sequences over finite abelian p-groups*, Rocky Mt. J. Math. **37** (2007), 1541 – 1550.

[53] ———, *On products of k atoms*, Monatsh. Math. **156** (2009), 141 – 157.

[54] W. Gao, A. Geroldinger, and D.J. Grynkiewicz, *Inverse zero-sum problems III*, submitted.

[55] W. Gao, A. Geroldinger, and F. Halter-Koch, *Group algebras of finite abelian groups and their applications to combinatorial problems*, Rocky Mt. J. Math., to appear.

[56] W. Gao, A. Geroldinger, and W.A. Schmid, *Inverse zero-sum problems*, Acta Arith. **128** (2007), 245 – 279.

[57] W. Gao, Q.H. Hou, W.A. Schmid, and R. Thangadurai, *On short zero-sum subsequences II*, Integers **7** (2007), Paper A21, 22p.

[58] W. Gao and I. Leader, *Sums and k-sums in abelian groups of order k*, J. Number Theory **120** (2006), 26 – 32.

[59] W. Gao and Y. Li, *Remarks on group rings and the Davenport constant*, Ars Comb., to appear.

[60] W. Gao, Y. Li, J. Peng, and F. Sun, *On subsequence sums of a zero-sum free sequence II*, Electron. J. Comb. **15** (2008), Research paper 117.

[61] ———, *Subsums of a zero-sum free subset of an abelian group*, Electron. J. Comb. **15** (2008), Research Paper 116.

[62] W. Gao and Y. ould Hamidoune, *Zero sums in abelian groups*, Combin. Probab. Comput. **7** (1998), 261 – 263.

[63] W. Gao, A. Panigrahi, and R. Thangadurai, *On the structure of p-zero-sum free sequences and its application to a variant of Erdős-Ginzburg-Ziv theorem*, Proc. Indian Acad. Sci., Math. Sci. **115** (2005), 67 – 77.

[64] W. Gao and R. Thangadurai, *On the structure of sequences with forbidden zero-sum subsequences*, Colloq. Math. **98** (2003), 213 – 222.

[65] W. Gao, R. Thangadurai, and J. Zhuang, *Addition theorems on the cyclic groups of order p^l*, Discrete Math. **308** (2008), 2030 – 2033.

[66] W. Gao and J. Zhuang, *Sequences not containing long zero-sum subsequences*, Eur. J. Comb. **27** (2006), 777 – 787.

[67] A. Geroldinger, *Über nicht-eindeutige Zerlegungen in irreduzible Elemente*, Math. Z. **197** (1988), 505 – 529.

[68] ———, *Chains of factorizations in weakly Krull domains*, Colloq. Math. **72** (1997), 53 – 81.

[69] A. Geroldinger and D.J. Grynkiewicz, *On the arithmetic of Krull monoids with finite Davenport constant*, J. Algebra **321** (2009), 1256 – 1284.

[70] A. Geroldinger and F. Halter-Koch, *Non-unique factorizations: a survey*, Multiplicative Ideal Theory in Commutative Algebra (J.W. Brewer, S. Glaz, W. Heinzer, and B. Olberding, eds.), Springer, 2006, pp. 217 – 226.

[71] ———, *Non-Unique Factorizations. Algebraic, Combinatorial and Analytic Theory*, Pure and Applied Mathematics, vol. 278, Chapman & Hall/CRC, 2006.

[72] A. Geroldinger and Y. ould Hamidoune, *Zero-sumfree sequences in cyclic groups and some arithmetical application*, J. Théor. Nombres Bordx. **14** (2002), 221 – 239.

[73] A. Geroldinger and W. Hassler, *Arithmetic of Mori domains and monoids*, J. Algebra **319** (2008), 3419 – 3463.

[74] ———, *Local tameness of v-noetherian monoids*, J. Pure Appl. Algebra **212** (2008), 1509 – 1524.

[75] A. Geroldinger and R. Schneider, *On Davenport's constant*, J. Comb. Theory, Ser. A **61** (1992), 147 – 152.

[76] B. Girard, *A new upper bound for the cross number of finite abelian groups*, Isr. J. Math., to appear.

[77] ———, *Inverse zero-sum problems and algebraic invariants*, Acta Arith. **135** (2008), 231 – 246.

[78] S. Griffiths, *The Erdős-Ginzburg-Ziv theorem with units*, Discrete Math. **308** (2008), 5473 – 5484.

[79] P.A. Grillet, *Commutative Semigroups*, Kluwer Academic Publishers, 2001.

[80] D.J. Grynkiewicz, *On extending Pollard's theorem for t-representable sums*, Isr. J. Math., to appear.

[81] ———, *A step beyond Kemperman's structure theorem*, Mathematika, to appear.

[82] ———, *On an extension of the Erdős-Ginzburg-Ziv Theorem to hypergraphs*, Eur. J. Comb. **26** (2005), 1154 – 1176.

[83] ———, *Quasi-periodic decompositions and the Kemperman structure theorem*, Eur. J. Comb. **26** (2005), 559 – 575.

[84] ———, *A weighted Erdős-Ginzburg-Ziv Theorem*, Combinatorica **26** (2006), 445 – 453.

[85] D.J. Grynkiewicz, E. Marchan, and O. Ordaz, *Representation of finite abelian group elements by subsequence sums*, J. Théor. Nombres Bordx., to appear.

[86] D.J. Grynkiewicz, O. Ordaz, M.T. Varela, and F. Villarroel, *On Erdős-Ginzburg-Ziv inverse theorems*, Acta Arith. **129** (2007), 307 – 318.

[87] F. Halter-Koch, *Ideal Systems. An Introduction to Multiplicative Ideal Theory*, Marcel Dekker, 1998.

[88] ———, *Non-unique factorizations of algebraic integers*, Funct. Approximatio, Comment. Math. **39** (2008), 49 – 60.

[89] Y. ould Hamidoune, *The global isoperimetric methodology applied to Kneser's theorem*, manuscript, –.

[90] ———, *Hyper-atoms and the Kemperman's critical pair theory*, manuscript, –.

[91] ———, *Some additive applications of the isoperimetric approach*, Ann. Inst. Fourier **58** (2008), 2007 – 2036.

[92] ———, *A weighted generalization of Gao's $n + D - 1$ theorem*, Comb. Probab. Comput. **17** (2008), 793 – 798.

[93] Y. ould Hamidoune, O. Serra, and G. Zémor, *On some subgroup chains related to Kneser's theorem*, J. Théor. Nombres Bordx. **20** (2008), 125 – 130.

[94] H. Harborth, *Ein Extremalproblem für Gitterpunkte*, J. Reine Angew. Math. **262** (1973), 356 – 360.

[95] F. Hennecart, *La fonction de Brakemeier dans le problème d'Erdős-Ginzburg-Ziv*, Acta Arith. **117** (2005), 35 – 50.

[96] F. Kainrath, *Elasticity of finitely generated domains*, Houston J. Math. **31** (2005), 43 – 64.

[97] ———, *On local half-factorial orders*, Arithmetical Properties of Commutative Rings and Monoids, Lect. Notes Pure Appl. Math., vol. 241, Chapman & Hall/CRC, 2005, pp. 316 – 324.

[98] J.H.B. Kemperman, *On small sumsets in an abelian group*, Acta Math. **103** (1960), 63 – 88.

[99] H. Kraft and C. Procesi, *Classical invariant theory, a primer*, http://www.math.unibas.ch/∼kraft/, 2000.

[100] S. Kubertin, *Nullsummen in $\mathbb{Z}_p^d$*, Master's thesis, Technical University Clausthal, 2002.

[101] G. Lettl and W.A. Schmid, *Minimal zero-sum sequences in $C_n \oplus C_n$*, Eur. J. Comb. **28** (2007), 742 – 753.

[102] G. Lettl and Zhi-Wei Sun, *On covers of abelian groups by cosets*, Acta Arith. **131** (2008), 341 – 350.

[103] H.B. Mann, *Additive group theory - a progress report*, Bull. Am. Math. Soc. **79** (1973), 1069 – 1075.

[104] ———, *Addition Theorems: The Addition Theorems of Group Theory and Number Theory*, R.E. Krieger, 1976.

[105] H.B. Mann and J.E. Olson, *Sums of sets in the elementary abelian group of type* (p, p), J. Comb. Theory, Ser. A **2** (1967), 275 – 284.

[106] C.P. Milies and S.K. Sehgal, *An Introduction to Group Rings*, Kluwer Academic Publishers, 2002.

[107] M.B. Nathanson, *Additive Number Theory: Inverse Problems and the Geometry of Sumsets*, Springer, 1996.

[108] J.E. Olson, *A combinatorial problem on finite abelian groups I*, J. Number Theory **1** (1969), 8 – 10.

[109] B. Peterson and T. Yuster, *A generalization of an addition theorem for solvable groups*, Can. J. Math. **36** (1984), 529 – 536.

[110] A. Plagne and W.A. Schmid, *On large half-factorial sets in elementary p-groups: maximal cardinality and structural characterization*, Isr. J. Math. **145** (2005), 285 – 310.

[111] ______, *On the maximal cardinality of half-factorial sets in cyclic groups*, Math. Ann. **333** (2005), 759 – 785.

[112] V. Ponomarenko, *Minimal zero sequences of finite cyclic groups*, Integers **4** (2004), Paper A24, 6p.

[113] A. Potechin, *Maximal caps in* $AG(6, 3)$, Des. Codes Cryptography **46** (2008), 243 – 259.

[114] C. Reiher, *On Kemnitz' conjecture concerning lattice points in the plane*, Ramanujan J. **13** (2007), 333 – 337.

[115] K. Rogers, *A combinatorial problem in abelian groups*, Proc. Camb. Philos. Soc. **59** (1963), 559 – 562.

[116] S. Savchev and F. Chen, *Long zero-free sequences in finite cyclic groups*, Discrete Math. **307** (2007), 2671 – 2679.

[117] ______, *Long n-zero-free sequences in finite cyclic groups*, Discrete Math. **308** (2008), 1 – 8.

[118] P. Scherk, *Distinct elements in a set of sums*, Am. Math. Mon. **62** (1955), 46 – 47.

[119] W.A. Schmid, *Arithmetical characterization of class groups of the form* $\mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$ *via the system of sets of lengths*, Abh. Math. Semin. Univ. Hamb., to appear.

[120] ______, *Inverse zero-sum problems II*, submitted, posted on arxiv.

[121] ______, *A realization theorem for sets of lengths*, J. Number Theory, to appear.

[122] ______, *Differences in sets of lengths of Krull monoids with finite class group*, J. Théor. Nombres Bordx. **17** (2005), 323 – 345.

[123] ______, *Half-factorial sets in finite abelian groups: a survey*, Grazer Math. Ber. **348** (2005), 41 – 64.

[124] ______, *Characterization of class groups of Krull monoids via their systems of sets of lengths: a status report*, HRI Conference Proceedings (S.D. Adhikari and B. Ramakrishnan, eds.), 2008.

[125] W.A. Schmid and J.J. Zhuang, *On short zero-sum subsequences over p-groups*, Ars Comb., to appear.

[126] O. Serra, *An isoperimetric method for the small sumset problem*, Surveys in Combinatorics 2005, London Mathematical Society Lecture Note Series, vol. 327, Cambridge University Press, 2005, pp. 119 – 152.

[127] Fang Sun, *On subsequence sums of a zero-sumfree sequence*, Electron. J. Comb. **14** (2007), Paper R52, 9p.

[128] Zhi-Wei Sun, *Zero-sum problems for abelian p-groups and covers of the integers by residue classes*, Isr. J. Math., to appear.

[129] B. Sury and R. Thangadurai, *Gao's conjecture on zero-sum sequences*, Proc. Indian Acad. Sci., Math. Sci. **112** (2002), 399 – 414.

[130] T. Tao and Van H. Vu, *Additive Combinatorics*, Cambridge University Press, 2006.

[131] C. Wang, *Note on a variant of the Erdős-Ginzburg-Ziv Theorem*, Acta Arith. **108** (2003), 53 – 59.

[132] P. Yuan, *On the index of minimal zero-sum sequences over finite cyclic groups*, J. Comb. Theory, Ser. A **114** (2007), 1545 – 1551.

[133] ______, *Subsequence sums of a zero-sumfree sequence*, Eur. J. Comb. **30** (2009), 439 – 446.

Institut für Mathematik und Wissenschaftliches Rechnen, Karl–Franzens–Universität Graz, Heinrichstrasse 36, 8010 Graz, Austria

E-mail address: alfred.geroldinger@uni-graz.at