

**DocCourse**  
**in**  
**Combinatorics and Geometry:**  
**Additive Combinatorics**

**Notes of the Course**

January to March, 2008  
Centre de Recerca Matemàtica  
Bellaterra (Spain)



# Contents

**Foreword** ..... v

**Alfred Geroldinger**

Additive group theory and the theory of non-unique factorizations ..... 1

The notes contained in this booklet were printed directly from files supplied by the authors before the course.

# Foreword

These notes correspond to the course ‘Additive group theory and the theory of non-unique factorizations’ by Prof. Alfred Geroldinger, which is part of the DocCourse in Additive Combinatorics held in the Centre de Recerca Matemàtica (CRM) in Bellaterra (Barcelona) from January to March 2008.

The course focusses on the interplay between zero-sum problems, arising from the Erdős-Ginzburg-Ziv theorem, and non-uniqueness of factorizations in monoids and integral domains, an area where Prof. Geroldinger is acknowledged as a leading researcher.

The motivation for the study of non-unique factorizations arises from the fact that the ring of integers of an algebraic number field may fail to have unique factorization. This led to a systematic combinatorial and analytic investigation of phenomena of non-unique factorizations in rings of integers of algebraic number fields carried over by W. Narkiewicz in the late 20th century. This investigation evolved to the study of non-unique factorizations in commutative cancellative monoids. Geroldinger’s fundamental characterization of sets of lengths in certain Krull monoids paved the way for many authors to analyze more deeply the arithmetic constants associated with factorization theory. In this setting the connection with zero-sum problems in Abelian groups has been most fruitful and it gives the opportunity to see the most fundamental results of Additive Group Theory in action.

This notes will be complemented with a second set devoted to the course ‘Sumsets and structure’ by I. Z. Ruzsa.

We wish to express our gratitude to the director and the staff of the CRM who helped us in the organization of this course. We thank the I-Math project of the Spanish government for providing generous financial support for the organization of this DocCourse. We also thank Prof. Geroldinger for his effort in preparing this set of notes.

Javier Cilleruelo  
Marc Noy  
Oriol Serra

Co-ordinators



# Additive group theory and non-unique factorizations

Alfred Geroldinger



# Contents

1	Basic concepts of non-unique factorizations	9
2	The Davenport constant and first precise arithmetical results	21
3	The structure of sets of lengths	35
4	Addition theorems and direct zero-sum problems	45
5	Inverse zero-sum problems and arithmetical consequences	55



# Introduction

The course centers on the interaction between two, at first glance very disparate areas of mathematics: Non-Unique Factorization Theory (see [58, 57, 12, 68, 91, 13]) and Additive Group Theory (see [79, 35, 80, 83, 23, 99, 47]). 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 1 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 a main problem (Section 3.D). In Section 2 we introduce the Davenport constant, and using group algebras we derive its precise value for  $p$ -groups (Theorem 2.10). In Section 3 we discuss the structure of sets of lengths (see Theorems 3.3, 3.8, 3.9 and 3.10). The characterization problem (Section 5.C) is a central topic. We give a proof in the case of cyclic groups (Corollary 5.12), and this proof requires most of the results from additive group theory discussed in this course. Section 4 starts with addition theorems, and then the invariants  $\eta(G)$  and  $\mathfrak{s}(G)$  - occurring in the Theorem of Erdős-Ginzburg-Ziv - are studied. We outline the power of the inductive method and determine the invariants  $D(G)$ ,  $\eta(G)$  and  $\mathfrak{s}(G)$  for groups of rank two (Theorem 4.13). Section 5 deals with inverse zero-sum problems. The focus is on cyclic groups and on groups of rank two.



# Notations

Our notation and terminology is consistent with [58]. 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  $[a, b] = \{x \in \mathbb{Z} \mid a \leq x \leq b\}$ , and we define  $\sup \emptyset = \max \emptyset = \min \emptyset = 0$ .

Let  $A, B \subset \mathbb{Z}$  be finite non-empty 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  $A = \{a_1, \dots, a_t\}$  with  $t \in \mathbb{N}$  and  $a_1 < \dots < a_t$ , 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* (AP for short) with *difference*  $d \in \mathbb{N}$  if  $P$  is finite nonempty and  $\Delta(P) \subset \{d\}$ . If  $A \subset \mathbb{N}$ , we call

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

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

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.*



# Chapter 1

## 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  $\mathfrak{q}(H)$  a quotient group of  $H$ .

Let  $a, b \in H$ . We say that  $a$  *divides*  $b$  (and we write  $a \mid b$ ) 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  $a \mid b$  and  $b \mid a$  (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

$$a = \prod_{p \in P} p^{v_p(a)} \quad \text{with } v_p(a) \in \mathbb{N}_0 \text{ and } v_p(a) = 0 \text{ for almost all } p \in P.$$

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

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

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  $b, c \in H$ ,  $a \mid bc$  implies  $a \mid b$  or  $a \mid c$ .

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)  $H_{\text{red}}$  is free (in that case  $H_{\text{red}}$  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  $H_{\text{red}}$ . Thus  $H_{\text{red}}$  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

$$z : a = u_1 \cdot \dots \cdot u_l \text{ with } l \in \mathbb{N}_0 \text{ and } u_1, \dots, u_l \text{ are atoms.}$$

We call  $l = |z|$  the *length* of the factorization  $z$ . Two factorizations which differ only in the order of their factors and up to associates are considered as being equal. Let  $Z_H(a) = Z(a)$  be the *set of factorizations* of  $a$  (in  $H$ ) and

$$L_H(a) = L(a) = \{|z| \mid z \in Z(a)\} \subset \mathbb{N}_0$$

the *set of lengths* of all factorization of  $a$  (in  $H$ ). The concept of factorizations can be formalized by considering the set of factorizations of  $a$  as a subset of the free monoid with basis  $\mathcal{A}(H_{\text{red}})$ , but we suppress this formal point of view. Note that  $0 \in L(a)$  if and only if  $a \in H^\times$  and then  $L(a) = \{0\}$ . We have  $1 \in L(a)$  if and only if  $a$  is an atom and then  $L(a) = \{1\}$ . The monoid  $H$  is atomic if and only if  $Z(a) \neq \emptyset$  for all  $a \in H$ , and it is factorial if and only if  $|Z(a)| = 1$ . For every  $b \in H$  we have

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

Furthermore, the monoid  $H$  is called

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

- a *BF-monoid* ( a bounded factorization monoid) if  $\mathsf{L}(a)$  is finite and non-empty for all  $a \in H$ .

Half-factorial monoids and domains have received a lot of attention in the literature (see [14], [20], [96] for recent surveys). Here is a first, very simple but important observation.

**Lemma 1.1.** *Let  $H$  be atomic but not half-factorial. Then for every  $N \in \mathbb{N}$  there exists some  $a \in H$  such that  $|\mathsf{L}(a)| \geq N + 1$ .*

*Proof.* If  $a = u_1 \cdots u_k = v_1 \cdots v_l$  with  $k < l$  and  $u_1, \dots, u_k, v_1, \dots, v_l \in \mathcal{A}(H)$ , then

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

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

### 1.A Arithmetical invariants

More or less all monoids studied so far in factorization theory are BF-monoids. In particular the multiplicative monoids of noetherian domains are BF-monoids. 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 system of finite non-empty 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 1.2.** Let  $H$  be a BF-monoid.

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

$$\rho(H) = \sup\{\rho(a) \mid a \in H\} = \sup\{\rho(L) \mid L \in \mathcal{L}(H)\} \in \mathbb{R}_{\geq 1} \cup \{\infty\}$$

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  $H \neq H^\times$ , then we define

$$\begin{aligned} \rho_k(H) &= \sup\{\max L \mid L \in \mathcal{L}(H), k \in L\} \in \mathbb{N} \cup \{\infty\} \quad \text{and} \\ \lambda_k(H) &= \min\{\min L \mid L \in \mathcal{L}(H), k \in L\} \in [1, k]. \end{aligned}$$

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 APs with the same difference.

**Lemma 1.3.** *If  $H$  is a BF-monoid and  $\Delta(H)$  is non-empty, 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  $t \in \mathbb{N}, d_1, \dots, d_t \in \Delta(H)$  and  $m_1, \dots, m_t \in \mathbb{Z} \setminus \{0\}$  such that  $d = m_1 d_1 + \dots + m_t d_t$ . After renumbering there is some  $s \in [1, t]$  such that  $m_1, \dots, m_s, -m_{s+1}, \dots, -m_t$  are positive. For every  $i \in [1, s]$ , there are  $x_i \in \mathbb{N}$  and  $a_i \in H$  such that

$$\{x_i, x_i + d_i\} \subset \mathcal{L}(a_i) \quad \text{for every } i \in [1, s]$$

and

$$\{x_i - d_i, x_i\} \subset \mathcal{L}(a_i) \quad \text{for every } i \in [s+1, t].$$

Then we get

$$\begin{aligned} \{k = \sum_{i=1}^s m_i x_i + \sum_{i=s+1}^t m_i (x_i - d_i), l = \sum_{i=1}^s m_i (x_i + d_i) + \sum_{i=s+1}^t m_i x_i\} \\ \subset \sum_{i=1}^s \{m_i x_i, m_i (x_i + d_i)\} + \sum_{i=s+1}^t \{m_i (x_i - d_i), m_i x_i\} \\ \subset \mathcal{L}(a_1^{m_1} \cdot \dots \cdot a_t^{m_t}) = L. \end{aligned}$$

Since  $d \leq \min \Delta(H)$ , it follows that  $d = l - k$  is a successive distance of  $L$  hence  $d \in \Delta(L) \subset \Delta(H)$ .  $\square$

Next we consider factorizations in a more direct way and not only their lengths.

**Definition 1.4.** Let  $H$  be atomic and  $a \in H$ . Let

$$z: a = u_1 \cdot \dots \cdot u_n v_1 \cdot \dots \cdot v_r \quad \text{and} \quad z': u_1 \cdot \dots \cdot u_n w_1 \cdot \dots \cdot w_s$$

be factorizations of  $a$  into atoms such that  $\{v_1 H^\times, \dots, v_r H^\times\} \cap \{w_1 H^\times, \dots, w_s H^\times\} = \emptyset$ . Then we call

$$d(z, z') = \max\{r, s\}$$

the *distance* between  $z$  and  $z'$ .

The distance is a metric on the set of all factorizations, and the following observation is analogue to Lemma 1.1.

**Lemma 1.5.** *Let  $H$  be atomic but not factorial. Then for every  $N \in \mathbb{N}$  there exists some  $a \in H$  such that  $|Z(a)| \geq N + 1$ , and there exist factorizations  $z, z' \in Z(a)$  such that  $d(z, z') \geq 2N$ .*

This phenomenon motivates the following definition.

**Definition 1.6.** Let  $H$  be atomic.

1. We define the *catenary degree*  $c(a)$  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  $z = z_0, z_1, \dots, z_k = z'$  of factorizations of  $a$  satisfying that  $d(z_{i-1}, z_i) \leq N$  for all  $i \in [1, k]$ .
2. Globally, we define

$$c(H) = \sup\{c(a) \mid a \in H\} \in \mathbb{N}_0 \cup \{\infty\},$$

and we call  $c(H)$  the *catenary degree* of  $H$ .

The next lemma gathers some elementary properties.

**Lemma 1.7.** *Let  $H$  be atomic and  $a \in H$ .*

1.  $c(a) \leq \sup L(a)$ , and  $c(a) = 0$  if and only if  $|Z(a)| = 1$ .
2. If  $z, z' \in Z(a)$  and  $z \neq z'$ , then  $2 + ||z| - |z'|| \leq d(z, z')$ .
3. If  $|Z(a)| \geq 2$ , then  $2 + \sup \Delta(L(a)) \leq c(a)$ . In particular,  $2 + \sup \Delta(H) \leq c(H)$ .
4. If  $c(a) \leq 2$ , then  $|L(a)| = 1$ , and if  $c(a) \leq 3$ , then  $L(a)$  is an AP with difference 1.

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

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

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

4. Obvious by 3. □

### 1.B Krull monoids

**Definition 1.8.** (Krull monoids and class groups)

1. Let  $D$  be a monoid and  $H \subset D$  a submonoid.
  - (a) Then  $H \subset D$  is called *saturated* if  $\mathfrak{q}(H) \cap D = H$  (that is, if  $a, b \in H$  and  $a$  divides  $b$  in  $D$ , then  $a$  divides  $b$  in  $H$ ).
  - (b) For  $a \in \mathfrak{q}(D)$  we denote by  $[a] = [a]_{D/H} = a \mathfrak{q}(H) \in \mathfrak{q}(D)/\mathfrak{q}(H)$  the class containing  $a$ . We call  $D/H = \{[a] \mid a \in D\} \subset \mathfrak{q}(D)/\mathfrak{q}(H)$  the *class group* of  $D$  modulo  $H$ .
2.  $H$  is called a *Krull monoid* if  $H_{\text{red}}$  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  $H_{\text{red}}$ . Then we call  $D$  a monoid of *divisors* and  $P$  a set of *prime divisors* of  $H$ .

Let  $H \subset D$  be as above. If  $\mathfrak{q}(D)/\mathfrak{q}(H)$  is finite (this condition is fulfilled throughout the present article), then  $D/H = \mathfrak{q}(D)/\mathfrak{q}(H)$ . 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  $\Phi: D \rightarrow D'$  with  $\Phi|_{H_{\text{red}}} = \text{id}$ . 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  $H$ .

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 Krull monoids we refer to [69, 62, 58]).

We start with ring theory. Let  $R$  be a domain,

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

the monoid of non-zero principal ideals and

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

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 1.9.** *Let  $R$  be an integral domain.*

1.  *$R$  is a Krull domain if and only if  $R^\bullet$  is a Krull monoid.*
2. *Every integrally closed noetherian domain is a Krull domain.*
3. *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 *Dedekind domain* if it satisfies the equivalent conditions of Theorem 1.9.3. 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. It connects the theory of non-unique factorizations with additive group theory and combinatorial number theory.

**Definition 1.10.** 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

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

where  $v_g(S) \in \mathbb{N}_0$ .

2. If  $S$  is as above, then

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

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*.

**Proposition 1.11.** *Let  $G_0 \subset G$  be a non-empty 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  $|G| \neq 2$ , then  $\mathcal{F}(G)$  is a monoid of divisors for  $\mathcal{B}(G)$ ,  $\mathcal{C}(\mathcal{B}(G)) \cong G$ , and every class of  $\mathcal{B}(G)$  contains exactly one prime.
4. The following statements are equivalent:
  - (a)  $|G| \leq 2$ .
  - (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

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

and hence there are only finitely many atoms.

3. and 4. We skip the proof of 3, but verify in detail the equivalence of all the conditions in 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  $\text{ord}(g) = n \geq 3$ . 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  $\text{ord}(g) \leq 2$  for all  $g \in G$ . Assume to the contrary, that there are two distinct non-zero elements  $e_1, \dots, e_2 \in G$  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  $|G| \leq 2$ .  $\square$

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

### 1.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 1.12.** A monoid homomorphism  $\theta: H \rightarrow B$  is called a *transfer homomorphism* if it has the following properties:

$$\text{(T1)} \quad B = \theta(H)B^\times \quad \text{and} \quad \theta^{-1}(B^\times) = H^\times.$$

**(T2)** 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 1.13.** Let  $\theta: H \rightarrow B$  be a transfer homomorphism of atomic monoids and  $u \in H$ .

1. If  $n \in \mathbb{N}$ ,  $b_1, \dots, b_n \in B$  and  $\theta(u) \simeq b_1 \cdot \dots \cdot b_n$ , then there exist  $u_1, \dots, u_n \in H$  such that  $u \simeq u_1 \cdot \dots \cdot u_n$  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.  $\mathsf{L}_H(u) = \mathsf{L}_B(\theta(u))$ .
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 **(T1)**, we have  $u = 1$  if and only if  $\theta(u) = 1$ , and by definition we have  $\mathsf{L}_H(1) = \{0\} = \mathsf{L}_B(\theta(u))$ . Suppose that  $u \neq 1$ . If  $k \in \mathsf{L}_H(u)$ , then there are

atoms  $u_1, \dots, u_k$  of  $H$  such that  $u = u_1 \cdot \dots \cdot u_k$ . Then  $\theta(u) = \theta(u_1) \cdot \dots \cdot \theta(u_k)$ . By 2.,  $\theta(u_1), \dots, \theta(u_k)$  are atoms of  $B$ , and hence  $k \in \mathbf{L}_B(\theta(u))$ . Conversely, we pick  $k \in \mathbf{L}_B(\theta(u))$ . Then there are atoms  $b_1, \dots, b_k$  of  $B$  such that  $\theta(u) = b_1 \cdot \dots \cdot b_k$ . By 1., there are  $u_1, \dots, u_k \in H$  such that  $u = u_1 \cdot \dots \cdot u_k$  and  $\theta(u_\nu) = b_\nu$  for all  $\nu \in [1, k]$ . Thus by 2.,  $u_1, \dots, u_k$  are atoms of  $H$  and hence  $k \in \mathbf{L}_H(u)$ .

4. This follows immediately from 3.  $\square$

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 1.14.** *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  $\tilde{\beta}: D \rightarrow \mathcal{F}(G_0)$  be the unique homomorphism satisfying  $\tilde{\beta}(p) = [p]$  for all  $p \in P$ .*

1. *For  $a \in D$  we have  $\tilde{\beta}(a) \in \mathcal{B}(G_0)$  if and only if  $a \in H$ . Thus  $\tilde{\beta}(H) = \mathcal{B}(G_0)$  and  $\tilde{\beta}^{-1}(\mathcal{B}(G_0)) = H$ .*
2. *The restriction  $\beta = \tilde{\beta}|_H: H \rightarrow \mathcal{B}(G_0)$  is a transfer homomorphism. In particular, we have  $\mathcal{L}(H) = \mathcal{L}(G_0)$ .*
3. *We have  $\mathbf{c}(G_0) \leq \mathbf{c}(H) \leq \max\{\mathbf{c}(G_0), 2\}$ .*

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

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

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.,  $\beta: H \rightarrow \mathcal{B}(G_0)$  is surjective and  $\beta^{-1}(1) = \{1\}$ . Let  $a = p_1 \cdot \dots \cdot p_l \in H$ , with  $l \in \mathbb{N}$  and  $p_1, \dots, p_l \in P$ , and suppose that  $\beta(a) = BC$ , say  $B = [p_1] \cdot \dots \cdot [p_k]$  and  $C = [p_{k+1}] \cdot \dots \cdot [p_l]$ . By 1.,  $b = p_1 \cdot \dots \cdot p_k \in H$ ,  $c = p_{k+1} \cdot \dots \cdot p_l \in H$  and clearly we have  $a = bc$ . Therefore  $\beta$  is a transfer homomorphism, and thus Proposition 1.13 implies  $\mathcal{L}(H) = \mathcal{L}(G_0)$ .

3. The proof is not difficult but requires concepts not introduced here.  $\square$

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

**Theorem 1.15.** *Let  $H$  be a Krull monoid with finite class group. Then  $H$  is an FF-monoid,  $\Delta(H)$  is finite,  $\rho(H) < \infty$  and  $\rho_k(H) < \infty$  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. If  $a \in H$ , then there are primes  $p_1, \dots, p_l \in P$  such that  $a = p_1 \cdot \dots \cdot p_l$ , and this is the only factorization of  $a$  in  $H$ . Thus every factorization  $a = u_1 \cdot \dots \cdot u_k$  of  $a$  into atoms of  $H$  corresponds uniquely to a partition

$$[1, l] = \bigcup_{\nu=1}^k I_\nu \quad \text{where} \quad \sum_{j \in I_\nu} [p_j] = 0 \quad \text{for all} \quad \nu \in [1, k],$$

and thus  $a$  has only finitely many factorizations in  $H$ .

Since by Theorem 1.14,  $\Delta(H) = \Delta(G_0)$ ,  $\rho(H) = \rho(G_0)$  and  $\rho_k(H) = \rho_k(G_0)$  for all  $k \in \mathbb{N}$ , it suffices to consider  $\mathcal{B}(G_0)$ . Since  $\mathcal{B}(G_0)$  is finitely generated by Proposition 1.11, the finiteness of all the invariants is a simple consequence of Dickson's Finiteness Theorem which we formulate for convenience.

*Dickson's Theorem.* If  $M \subset \mathbb{N}_0^s$ , then the set  $\text{Min}(M)$  of its minimal points is finite, and for every  $\mathbf{c} \in M$  there exists some  $\mathbf{a} \in \text{Min}(M)$  satisfying  $\mathbf{a} \leq \mathbf{c}$ .  $\square$

### 1.D A main problem

Let  $H$  be a Krull monoid with finite class group  $G$  such that every class contains a prime, say  $G = C_{n_1} \oplus \dots \oplus C_{n_r}$  where  $1 < n_1 \mid \dots \mid n_r$ . Find the precise values of the arithmetical invariants of  $H$  (such as of  $\mathfrak{c}(H)$ ,  $\Delta(H)$  and  $\rho_k(H)$  for  $k \in \mathbb{N}$ ) in terms of the group invariants  $n_1, \dots, n_r$  of  $G$  (by the simple Theorem 1.15 all the invariants are finite).



## Chapter 2

# The Davenport constant and first precise arithmetical results

### 2.A The Davenport constant

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

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

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

$$|S| = l = \sum_{g \in G_0} v_g(S) \in \mathbb{N}_0 \quad \text{the length of } S,$$

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

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

$$\Sigma_{\leq k}(S) = \bigcup_{j \in [1, k]} \Sigma_j(S), \quad \Sigma_{\geq k}(S) = \bigcup_{j \geq k} \Sigma_j(S),$$

and

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

A sequence  $S$  is called *zero-sumfree* if  $0 \notin \Sigma(S)$ , and we denote by  $\mathcal{A}^*(G_0)$  the set of zero-sumfree sequences. We set  $-S = (-g_1) \cdot \dots \cdot (-g_l)$ , and for every  $g \in G$  we set  $g + S = (g + g_1) \cdot \dots \cdot (g + g_l)$ .

**Definition 2.1.** Let  $G_0 \subset G$  be a non-empty subset. Then

$$D(G_0) = \sup\{|U| \mid U \in \mathcal{A}(G_0)\} \in \mathbb{N}_0$$

is said to be the *Davenport constant* of  $G_0$  and

$$d(G_0) = \sup\{|S| \mid S \in \mathcal{F}(G_0) \text{ is zero-sumfree}\} \in \mathbb{N}_0$$

is called the *little Davenport constant* of  $G_0$ .

The Davenport constant has been studied since the 1960s (see [88], [81], [30], [84] and [79]), and its precise value is still unknown in general. Obviously,  $\psi: \mathcal{A}^*(G_0) \rightarrow \mathcal{A}(G)$ ,  $S \mapsto (-\sigma(S))S$ , is a well-defined and  $D(G_0) \leq 1 + d(G_0)$ . If  $G_0 = G$ , then  $\psi$  is surjective and  $D(G) = 1 + d(G)$ . The following two lemmas gather some elementary properties of the Davenport constant.

**Lemma 2.2.**

1. If  $S \in \mathcal{A}^*(G)$  has length  $|S| = d(G)$ , then  $\Sigma(S) = G^\bullet$  and  $G = \langle \text{supp}(S) \rangle$ .
2.  $d(G) = \max\{|S| \mid S \in \mathcal{F}(G), \Sigma(S) = G^\bullet\}$ .
3.  $D(G)$  is the smallest integer  $l \in \mathbb{N}$  such that every sequence  $S \in \mathcal{F}(G)$  of length  $|S| \geq l$  has a non-empty zero-sum subsequence (that is,  $S \notin \mathcal{A}^*(G)$ ).
4. If  $S \in \mathcal{A}^*(G)$ , then  $|S| \leq |\Sigma(S)| \leq |G| - 1$ . In particular,  $d(G) \leq |G| - 1$  and  $D(G) \leq |G|$ .

*Proof.* 1. Let  $S \in \mathcal{A}^*(G)$  with  $|S| = d(G)$ , 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  $G = \langle \text{supp}(S) \rangle$ .

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

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

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

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

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

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

By the Structure Theorem of Finite Abelian Groups, we have

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

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

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

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

**Lemma 2.3.** *Let  $\exp(G) = n \geq 2$ .*

1. *If  $e_1, \dots, e_r \in G$  are independent elements, then*

$$S = \prod_{i=1}^r e_i^{\text{ord}(e_i)-1} \in \mathcal{A}^*(G).$$

2. *There exists a sequence  $S \in \mathcal{A}^*(G)$  such that  $|S| = d^*(G)$ . In particular,  $d^*(G) \leq d(G)$ .*

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

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

**Corollary 2.4.**

1. *Let  $G$  be cyclic of order  $n \geq 2$ . A sequence  $S \in \mathcal{F}(G)$  is zero-sumfree of length  $|S| = d(G)$  if and only if  $S = g^{n-1}$  for some  $g \in G$  with  $\text{ord}(g) = n$ . In particular,  $d(G) = d^*(G) = n - 1$  and  $D(G) = n$ .*

2. Let  $G$  be an elementary 2-group. A sequence  $S \in \mathcal{F}(G)$  is zero-sumfree if and only if  $S$  is squarefree and  $\text{supp}(S)$  is an independent set. In particular,  $d(G) = d^*(G) = r(G)$ .

*Proof.* 1. By Lemmas 2.2 and 2.3, we have  $n-1 = d^*(G) \leq d(G) \leq |G|-1 = n-1$  and thus  $d(G) = n-1$  and  $D(G) = n$ . Obviously, if  $g \in G$  with  $\text{ord}(g) = n$ , then  $S = g^{n-1} \in \mathcal{A}^*(G)$ . Conversely, assume to the contrary that  $S = g_1 \cdots g_{n-1} \in \mathcal{A}^*(G)$  and  $g_1 \neq g_2$ . If  $\Sigma = \{g_1 + \dots + g_k \mid k \in [1, n-1]\}$ , then  $|\Sigma| = n-1$  and  $g_2 \notin \Sigma$ , a contradiction.

2. If  $S$  is squarefree and  $\text{supp}(S)$  is independent, then  $S$  is zero-sumfree by Lemma 2.3.1. Conversely, if  $S \in \mathcal{A}^*(G)$ , then  $v_g(S) < \text{ord}(g) \leq 2$  for all  $g \in \text{supp}(S)$ . Hence  $S$  is squarefree, and  $0 \notin \Sigma(S)$  implies that  $\text{supp}(S)$  is independent.

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

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 [58, Chapter 5], [85, 86] and [61] for recent progress).

## 2.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-sumfree sequences over  $p$ -groups, which is due to P. van Emde Boas, D. Kruswijk and J.E. Olson. Theorem 2.10 provides the classical result that for a  $p$ -group  $G$  we have  $d(G) = d^*(G)$ .

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

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

We view  $R$  as a subset of  $R[G]$  by means of  $a = aX^0$  for all  $a \in R$ . The *augmentation map*

$$\varepsilon: R[G] \rightarrow R, \quad \text{defined by} \quad \varepsilon\left(\sum_{g \in G} a_g X^g\right) = \sum_{g \in G} a_g$$

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

**Definition 2.5.** For a commutative ring  $R$ , let  $d(G, R)$  denote the largest integer  $l \in \mathbb{N}$  having the following property:

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

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

**Lemma 2.6.** Let  $R$  be an integral domain,  $S = g_1 \cdot \dots \cdot g_l \in \mathcal{F}(G)$  a zero-sumfree sequence,  $k \in [1, l]$  and  $a_1, \dots, a_k \in K^\times$ . If

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

then  $c_0 \neq 0$ , and hence  $f \neq 0$ . In particular, we have  $d(G) \leq d(G, R)$ .

*Proof.* Since  $R$  is an integral domain and  $0 \notin \Sigma(S)$ , it follows that  $c_0 = a_1 \cdot \dots \cdot a_k \neq 0$ .  $\square$

**Definition 2.7.** Let  $S = g_1 \cdot \dots \cdot g_l \in \mathcal{F}(G)$  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

$$\mathbf{N}_g^k(S) = \left| \left\{ I \subset [1, l] \mid \sum_{i \in I} g_i = g \text{ and } |I| = k \right\} \right|$$

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

$$\mathbf{N}_g(S) = \sum_{k \geq 0} \mathbf{N}_g^k(S), \quad \mathbf{N}_g^+(S) = \sum_{k \geq 0} \mathbf{N}_g^{2k}(S) \quad \text{and} \quad \mathbf{N}_g^-(S) = \sum_{k \geq 0} \mathbf{N}_g^{2k+1}(S).$$

Thus  $\mathbf{N}_g(S)$  denotes the number of subsequences  $T$  of  $S$  having sum  $\sigma(T) = g$ ,  $\mathbf{N}_g^+(S)$  denotes the number of all such subsequences of even length, and  $\mathbf{N}_g^-(S)$  denotes the number of all such subsequences of odd length (each counted with the multiplicity of its appearance in  $S$ ).

**Lemma 2.8.** 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  $\text{ord}(g) = m \geq 2$ , 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  $(e_1, \dots, e_r)$  be a basis of  $G$  and  $\text{ord}(e_i) = n_i \geq 2$  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  $g_1, \dots, g_m \in G$ , 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  $t \in \mathbb{N}_0$ ,  $c_j \in \mathbb{F}_p$ ,  $l_{j,1}, \dots, l_{j,r} \in \mathbb{N}_0$  and  $l_{j,1} + \dots + l_{j,r} \geq m$  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  $j \in [0, m-1]$ ,

$$\binom{m-1}{j} (-1)^j \equiv 1 \pmod{p}.$$

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 assertion follows.

2. Every  $g \in G$  has a unique representation of the form  $g = \nu_1 e_1 + \dots + \nu_r e_r$ , 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  $\mathbf{l} = (l_1, \dots, l_r) \in \mathbb{N}_0^r$ ,

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

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

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

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

$$\prod_{\mu=1}^m (1 - X^{g_\mu}) = \sum_{\mathbf{0} \neq \mathbf{l}_1, \dots, \mathbf{l}_m \in \mathbb{N}_0^r} c_{1, \mathbf{l}_1} \cdots c_{m, \mathbf{l}_m} g_{\mathbf{l}_1 + \dots + \mathbf{l}_m},$$

and  $|\mathbf{l}_1 + \dots + \mathbf{l}_m| \geq m$  for all  $\mathbf{l}_1, \dots, \mathbf{l}_m \in \mathbb{N}_0^r \setminus \{\mathbf{0}\}$ .  $\square$

**Lemma 2.9.** *Let  $p$  be a prime,  $G$  a  $p$ -group,  $S = g_1 \cdots g_l \in \mathcal{F}(G)$ , 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  $c_g(S) = \mathbf{N}_g^+(S) - \mathbf{N}_g^-(S) + p\mathbb{Z} \in \mathbb{F}_p$ . In particular, if  $c_{\mathbf{0}}(S) = 0$ , then  $0 \in \Sigma(S)$ , and if  $g \in G^\bullet$  and  $c_g(S) \neq 0$ , 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  $m > \mathbf{d}^*(G)$ , then  $c_g(S) = 0$  for all  $g \in G$ ,  $0 \in \Sigma(S)$ , and in particular  $\mathbf{N}_g^+(S) \equiv \mathbf{N}_g^-(S) \pmod{p}$  for all  $g \in G$ .*

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

$$\Omega_g = \left\{ I \subset [1, l] \mid \sum_{i \in I} g_i = g \right\}.$$

Then  $\emptyset \in \Omega_{\mathbf{0}}$  and

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

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

2. We shall repeatedly make use of Lemma 2.7. Let  $(e_1, \dots, e_r)$  be a basis of  $G$ ,  $\text{ord}(e_i) = n_i$  for all  $i \in [1, r]$ , and  $1 < n_1 \mid \dots \mid n_r$ . Then

$$\mathbf{d}^*(G) = (n_1 - 1) + \dots + (n_r - 1).$$

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

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

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  $m \leq l_{j,1} + \dots + l_{j,r} \leq \mathbf{d}^*(G)$  for all  $j \in [1, t]$ .

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

**Theorem 2.10.** *If  $G$  is a  $p$ -group, then  $\mathbf{d}^*(G) = \mathbf{d}(G) = \mathbf{d}(G, \mathbb{F}_p)$ .*

*Proof.* Suppose that  $G$  is a  $p$ -group. Lemmas 2.3.2 and 2.6 imply that  $\mathbf{d}^*(G) \leq \mathbf{d}(G) \leq \mathbf{d}(G, \mathbb{F}_p)$ . If  $S = g_1 \cdot \dots \cdot g_l \in \mathcal{F}(G)$  with  $|S| = l > \mathbf{d}^*(G)$ , then Lemma 2.9.2 (with  $m_1 = \dots = m_l = 0$ ) implies that

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

and thus  $\mathbf{d}(G, \mathbb{F}_p) \leq \mathbf{d}^*(G)$ .  $\square$

An alternate proof of Theorem 2.10 was given by Zhi-Wei Sun who used covers of the integers (see [98, 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 [82, 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  $\mathbf{N}_g^+(S)$  and  $\mathbf{N}_g^-(S)$ , as obtained in Lemma 2.9.2 (see [48]).

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

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

(see [58, Theorem 5.5.5]). In particular, for cyclic group this implies that  $d(G) = d(G, K) = n-1$ . W. Gao conjectures that for every  $G$  there is a splitting field  $F$  such that  $d(G) = d(G, F)$ , and in [52]) W. Gao and Y. Li showed that, for every splitting field  $K$  of  $G = C_2 \oplus C_{2n}$  we have  $d(C_2 \oplus C_{2n}) = d(C_2 \oplus C_{2n}, K)$  (see also [49]).

## 2.C Arithmetical invariants again

**Theorem 2.11.** *Let  $H$  be a Krull monoid with class group  $G$  such that every class contains a prime and suppose that  $|G| \geq 3$ . 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*

$$2 \max \mathsf{L}(A) - m \leq |A| \leq \mathsf{D}(G) \min \mathsf{L}(A) - m(\mathsf{D}(G) - 1) \quad \text{and} \quad \rho(A) \leq \frac{\mathsf{D}(G)}{2}.$$

2. *We have  $k \leq \rho_k(H) \leq k \frac{\mathsf{D}(G)}{2}$  and  $\lambda_k(H) \geq \rho(H)^{-1} k$ .*

3.  *$\rho_{2k}(H) = k \mathsf{D}(G)$  and  $\rho(H) = \frac{\mathsf{D}(G)}{2}$ .*

4. *If  $l \in \mathbb{N}_0$  and  $j \in [0, 1]$  such that  $l \mathsf{D}(G) + j \geq 1$ , then  $\lambda_{l \mathsf{D}(G) + j}(H) = 2l + j$ .*

*Proof.* 1. Let  $A = 0^m U_1 \cdots U_l$  where  $l, m \in \mathbb{N}_0$  and  $U_1, \dots, U_l \in \mathcal{A}(G^\bullet)$ . Then  $2 \leq |U_\nu| \leq \mathsf{D}(G)$  for all  $\nu \in [1, l]$  and hence

$$m + 2l \leq |A| \leq m + l \mathsf{D}(G).$$

Choosing  $l = \min \mathsf{L}(A)$  and  $l = \max \mathsf{L}(A)$  we obtain the first inequalities, and then we get

$$\rho(A) = \frac{\max \mathsf{L}(A)}{\min \mathsf{L}(A)} = \frac{m + \max \mathsf{L}(B)}{m + \min \mathsf{L}(B)} \leq \frac{\max \mathsf{L}(B)}{\min \mathsf{L}(B)} \leq \frac{\mathsf{D}(G)}{2}.$$

2. By definition, we have  $k \leq \rho_k(H)$ . If  $A \in \mathcal{B}(G)$  with  $k \in \mathsf{L}(A)$  and  $\max \mathsf{L}(A) = \rho_k(H)$ , then 1. implies that

$$\frac{\rho_k(H)}{k} \leq \frac{\max \mathsf{L}(A)}{\min \mathsf{L}(A)} = \rho(A) \leq \frac{\mathsf{D}(G)}{2}.$$

There is some  $L \in \mathcal{L}(H)$  with  $k, \lambda_k(H) \in L$ , and hence it follows that

$$k \leq \max L \leq \rho(H) \min L = \rho(H) \lambda_k(H).$$

3. By 1. and 2. it follows that  $\rho_{2k}(H) \leq kD(G)$  and  $\rho(H) \leq \frac{D(G)}{2}$ . If  $U = g_1 \cdot \dots \cdot g_l \in \mathcal{A}(G)$  with  $|U| = l = D(G)$ , then

$$(-U)^k U^k = \prod_{\nu=1}^l ((-g_\nu)g_\nu)^k,$$

shows that in both inequalities we actually have equality.

4. Let  $l \in \mathbb{N}_0$  and  $j \in [0, 1]$  such that  $lD(G) + j \geq 1$ . Then 2. and 3. imply that

$$2l + \frac{2j}{D(G)} = \rho(H)^{-1}(lD(G) + j) \leq \lambda_{lD(G)+j}(G).$$

Since  $\rho_{2l}(G) = lD(G)$ , we get  $\rho_{2l+j}(G) \geq lD(G) + j$ ,  $\lambda_{lD(G)+j}(G) \leq 2l + j$  and hence  $\lambda_{lD(G)+j}(G) = 2l + j$ .  $\square$

**Lemma 2.12.**

1. For  $j \in \mathbb{N}_{\geq 3}$ , the following statements are equivalent:

- (a) There exists some  $L \in \mathcal{L}(G)$  with  $\{2, j\} \subset L$ .
- (b)  $j \leq D(G)$ .

2. Let  $A \in \mathcal{B}(G)$ . Then  $\{2, D(G)\} \subset L(A)$  if and only if  $A = U(-U)$  for some  $U \in \mathcal{A}(G)$  with  $|U| = D(G)$ .

*Proof.* 1. (a)  $\Rightarrow$  (b) If  $L \in \mathcal{L}(G)$  and  $\{2, j\} \subset L$ , then Theorem 2.11.3 implies that  $j \leq \sup L \leq \rho_2(G) = D(G)$ .

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

2. If  $\{2, D(G)\} \subset L(A)$ , then there exist  $U_1, U_2, V_1, \dots, V_{D(G)} \in \mathcal{A}(G)$  such that  $A = U_1 U_2 = V_1 \cdot \dots \cdot V_{D(G)}$ , and clearly  $0 \nmid A$ , since otherwise  $U_1 = 0$  or  $U_2 = 0$  and  $D(G) = 2$ . Theorem 2.11.1 implies that  $\max L(A) = D(G)$  and  $|A| = 2D(G)$ . Hence  $|V_i| = 2$  for all  $i \in [1, D(G)]$ , and  $|U_1| = |U_2| = D(G)$ , which implies  $U_2 = -U_1$ . The converse is obvious.  $\square$

**Lemma 2.13.** 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  $UV = W_1 \cdot \dots \cdot W_k$  with  $k \in [2, d]$  and  $|W_1| \leq d$ .

Then  $c(G) \leq d$ .

*Proof.* We must prove that  $c(A) \leq d$  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

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

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

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

We may assume that  $V_1 | U_1 \cdot \dots \cdot U_{r-1}$ , say  $U_1 \cdot \dots \cdot U_{r-1} = V_1 W_1 \cdot \dots \cdot W_t$  with  $t \in \mathbb{N}$  and  $W_1, \dots, W_t \in \mathcal{A}(G)$ . By the induction hypothesis there is a  $d$ -chain of factorizations  $y_0, \dots, y_k$  concatenating  $U_1 \cdot \dots \cdot U_{r-1}$  and  $V_1 W_1 \cdot \dots \cdot W_t$ , and there is a  $d$ -chain of factorizations  $z_0, \dots, z_l$  concatenating  $W_1 \cdot \dots \cdot W_t U_r$  and  $V_2 \cdot \dots \cdot V_s$ . Then  $z = y_0 U_r, \dots, y_k U_r = z_0 V_1, \dots, z_l V_1 = z'$  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  $V_1 V_2 = W_1 \cdot \dots \cdot W_k$ , where  $k \in [2, d]$  and  $|W_1| \leq d$ . Then the factorization  $z'' = W_1 \cdot \dots \cdot W_k V_3 \cdot \dots \cdot V_s$  of  $A$  satisfies  $d(z', z'') = \max\{2, k\} \leq d$ , and by CASE 1 there is a  $d$ -chain of factorizations concatenating  $z$  and  $z''$ .  $\square$

**Theorem 2.14.** *Let  $H$  be a Krull monoid with class group  $G$ .*

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

*Proof.* 1. By Theorem 1.14 it suffices to show that  $c(G) \leq D(G)$ . This follows immediately from Lemma 2.13 with  $d = D(G)$ .

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

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  $|U| = |V| = D(G)$  there exists some factorization  $UV = W_1 \cdot \dots \cdot W_k$  with  $k \in [2, d(G)]$  and  $|W_1| \leq d(G)$ . Then  $c(G) \leq d(G)$  by Lemma 2.13.

Let  $U, V \in \mathcal{A}(G)$  with  $|U| = |V| = D(G)$ . Then  $\max L(UV) \leq D(G)$ , and equality holds if and only if  $V = -U$  (cf. Lemma 2.12). Now we distinguish two cases.

CASE 1:  $V \neq -U$ .

It is sufficient to prove that there exists some  $W \in \mathcal{A}(G)$  such that  $W \mid UV$  and  $|W| < D(G)$ . Assume the contrary. Let  $g \in \text{supp}(U)$  and  $V = h_1 \cdot \dots \cdot h_l$  with  $l = D(G)$ . For every  $i \in [1, l]$ , we consider the sequence  $S_i = gh_i^{-1}V \in \mathcal{F}(G)$ . Since  $|S_i| = D(G)$ , there exists some  $S'_i \in \mathcal{A}(G)$  such that  $S'_i \mid S_i \mid UV$ . By assumption, this implies  $|S'_i| = D(G)$ , hence  $S'_i = S_i$  and therefore  $0 = \sigma(S_i) = g - h_i$ . Thus  $V = g^l$ , and Lemma 2.2.1 implies  $G = \langle \text{supp}(V) \rangle = \langle g \rangle$ , a contradiction.

CASE 2:  $V = -U$ .

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

By Lemma 2.2.1 we have  $\langle \text{supp}(U) \rangle = G$ , and since  $G$  is not an elementary 2-group, there exists some  $g_0 \in \text{supp}(U)$  with  $\text{ord}(g_0) > 2$ . We set  $U = g_0^m g_1 \dots g_l$  with  $g_0 \notin \{g_1, \dots, g_l\}$ . Since  $G = \langle \text{supp}(U) \rangle$  is not cyclic, it follows that  $l \geq 2$ . If  $W' = (-g_0)^m g_1 \dots g_l$ , then  $W' \mid U(-U)$  and  $|W'| = D(G)$ . Hence there exists some  $W \in \mathcal{A}(G)$  with  $W \mid W'$ , and we shall prove that  $2 < |W| < D(G)$ . Since  $U \in \mathcal{A}(G)$ , we have  $W \nmid g_1 \dots g_l$  and thus  $-g_0 \mid W$ . Since  $g_0 \notin \{g_1, \dots, g_l\}$  and  $g_0 \neq -g_0$ , it follows that  $W \neq g_0(-g_0)$  and thus  $|W| > 2$ .

Assume to the contrary that  $|W| = D(G)$ . Then  $W = W'$ , and  $\sigma(U) = \sigma(W) = 0$  implies  $2mg_0 = 0$  and thus  $m > 1$ . We consider the sequence  $S = g_0^m g_1 \dots g_{l-1}$ . Since  $S \in \mathcal{A}^*(G)$  and  $|S| = d(G)$ , Lemma 2.2.1 implies  $\Sigma(S) = G^\bullet$  and thus  $(m+1)g_0 \in \Sigma(S)$ , say

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

If  $s = 0$ , then

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

a contradiction. If  $s \geq 1$ , 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  $W \in \mathcal{A}(G)$ .  $\square$

**Corollary 2.15.** *Let  $H$  be a Krull monoid with class group  $G$  such that every class contains a prime. Suppose that  $|G| \geq 3$  and that  $\text{exp}(G) = n \geq 2$ . Then*

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

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

*Proof.* By Theorem 1.14, we have  $\Delta(H) = \Delta(G)$ . Lemma 1.7.3 implies that  $\Delta(H) \subset [1, c(G)-2]$  and Theorem 2.14 that  $c(G) \leq D(G)$ .

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

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

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

If  $G$  is cyclic, then Corollary 2.4 implies that  $\mathbf{D}(G) = n$  and thus  $\Delta(G) = [1, n - 2]$ .  $\square$

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

**Corollary 2.16.** *The following statements are equivalent:*

- (a) Every  $L \in \mathcal{L}(G)$  with  $\{2, \mathbf{D}(G)\} \subset L$  satisfies  $L = \{2, \mathbf{D}(G)\}$ .
- (b)  $\{2, \mathbf{D}(G)\} \in \mathcal{L}(G)$ .
- (c)  $G$  is either cyclic or an elementary 2-group.

*Proof.* (a)  $\Rightarrow$  (b) By Lemma 2.12.1 there exists some  $L \in \mathcal{L}(G)$  with  $\{2, \mathbf{D}(G)\} \subset L$ .

(b)  $\Rightarrow$  (c) If  $L = \{2, \mathbf{D}(G)\} \in \mathcal{L}(G)$ , then, by Lemma 1.7.3 and Theorem 2.14.1 we have  $\mathbf{D}(G) \leq 2 + \sup \Delta(G) \leq \mathbf{c}(G) \leq \mathbf{D}(G)$ , hence  $\mathbf{c}(G) = \mathbf{D}(G)$ , and the assertion follows by Theorem 2.14.2.

(c)  $\Rightarrow$  (a) Let  $L \in \mathcal{L}(G)$  with  $\{2, \mathbf{D}(G)\} \subset L$ . By Lemma 2.12.2 we have  $L = \mathbf{L}(U(-U))$  for some  $U \in \mathcal{A}(G)$  with  $|U| = \mathbf{D}(G)$ .

If  $G$  is cyclic of order  $n \geq 3$ , then Corollary 2.4 implies that  $U = g^n$  for some  $g \in G$  with  $\text{ord}(g) = n$ . Since  $\mathcal{A}(\{-g, g\}) = \{(-g)^n, g^n, g(-g)\}$ , it follows that  $\mathbf{L}(U(-U)) = \{2, \mathbf{D}(G)\}$ .

If  $G$  is an elementary 2-group of rank  $r \geq 2$  and  $(e_1, \dots, e_r)$  is a basis of  $G$ , then  $U = e_1 \cdots e_r(e_1 + \dots + e_r)$  by Corollary 2.4 and  $\mathbf{L}(U(-U)) = \{2, r + 1\} = \{2, \mathbf{D}(G)\}$ .  $\square$



## Chapter 3

# The structure of sets of lengths

Recall, that if  $H$  is not half-factorial then for every  $N \in \mathbb{N}$  there is a  $c \in H$  such that  $|\mathcal{L}(c)| > N$ .

### 3.A Unions of sets of lengths

**Definition 3.1.** 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  $u_1, \dots, u_k, v_1, \dots, v_m \in \mathcal{A}(H)$  with  $u_1 \cdot \dots \cdot u_k = v_1 \cdot \dots \cdot v_m$ .

**Lemma 3.2.** Let  $H$  be a BF-monoid with  $H \neq H^\times$  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

$$\lambda_{k+l}(H) \leq \lambda_k(H) + \lambda_l(H) \leq k + l \leq \rho_k(H) + \rho_l(H) \leq \rho_{k+l}(H).$$

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.  $\square$

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 is due to M. Freeze and A. Geroldinger ([34]).

**Theorem 3.3.** *Let  $H$  be a Krull monoid with 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 AP with difference 1.*

*Proof.* By Theorem 1.14, we have  $\mathcal{V}_k(H) = \mathcal{V}_k(G)$  and hence  $\lambda_k(H) = \lambda_k(G)$  and  $\rho_k(H) = \rho_k(G)$  for all  $k \in \mathbb{N}$ . Thus it suffices to prove the assertion for the block monoid  $\mathcal{B}(G)$ .

If  $|G| \leq 2$ , then  $\mathcal{B}(G)$  is half-factorial by Proposition 1.11 whence the sets  $\mathcal{V}_k(G)$  are singletons for all  $k \in \mathbb{N}$ . Let  $|G| \geq 3$  and  $k \in \mathbb{N}$ . Obviously, it suffices to prove the following three assertions.

**A1.**  $\mathcal{V}_{2k}(G) \cap [2k, kD(G)]$  is an AP with difference 1.

**A2.**  $\mathcal{V}_k(G) \cap [0, k]$  is an AP with difference 1.

**A3.**  $\mathcal{V}_k(G) \cap \mathbb{N}_{\geq k}$  is an AP with difference 1.

*Proof of A1.* Lemma 2.12.1 implies that

$$\mathcal{V}_2(G) = \bigcup_{2 \in L, L \in \mathcal{L}(G)} L = [2, D(G)].$$

Now suppose that  $k \geq 2$ . Then

$$2k \in \mathcal{V}_2(G) + \mathcal{V}_{2(k-1)}(G) \subset \mathcal{V}_{2k}(G).$$

Since  $\mathcal{V}_2(G) = [2, D(G)]$  and, by Lemma 1.6.2,  $\max \Delta(\mathcal{V}_{2(k-1)}(G)) \leq \max \Delta(G) \leq D(G) - 2$ , it follows that  $\mathcal{V}_2(G) + \mathcal{V}_{2(k-1)}(G)$  is an AP with difference 1. Since the maxima of  $\mathcal{V}_2(G) + \mathcal{V}_{2(k-1)}(G)$  and of  $\mathcal{V}_{2k}(G)$  coincide, it follows that  $\mathcal{V}_{2k} \cap [2k, kD(G)]$  is an AP with difference 1.

*Proof of A2.* We set  $l = \lambda_k(G)$  and have to show that  $\mathcal{V}_k(G) \cap [l, k]$  is an AP with difference 1. Pick  $m \in [l, k]$ . In order to show that  $m \in \mathcal{V}_k(G)$ , we verify that  $k \in \mathcal{V}_m(G)$ .

CASE 1:  $m$  is even.

Since  $l \leq m \leq k \leq \rho_l(G) \leq \rho_m(G)$ , we get that  $k \in [m, \rho_m(G)]$ , and thus 1. implies that  $k \in \mathcal{V}_m(G)$ .

CASE 2:  $m$  is odd.

If  $m = l$ , then there is nothing to show. Suppose that  $l + 1 \leq m$ . Since  $l \leq m - 1 \leq k - 1 \leq \rho_l(G) \leq \rho_{m-1}(G)$ , it follows that  $k - 1 \in [m - 1, \rho_{m-1}(G)]$ . Since  $m - 1$  is even, 1. implies that  $k - 1 \in \mathcal{V}_{m-1}(G)$  and hence  $k \in \mathcal{V}_m(G)$ .

*Proof of A3.* For  $l \in [k, \rho_k(G)]$  let

$$m_l(G) = \min\{|B| \mid B \in \mathcal{B}(G) \text{ with } k, l \in L(B)\}.$$

We assert that every  $l \in [k+1, \rho_k(G)]$  lies in  $\mathcal{V}_k(G)$  and that

$$m_l(G) < m_{l+1}(G) < \dots < m_{\rho_k(G)}(G).$$

We proceed by induction on  $l$ . For  $l = \rho_k(G)$  the assertion is clear. Suppose that  $l \leq \rho_k(G)$  and that the assertions hold for all  $s \in [l, \rho_k(G)]$ .

Let  $B \in \mathcal{B}(G)$  such that  $k, l \in \mathcal{L}(B)$  and  $|B| = m_l(G)$ . Then there are  $U_1, \dots, U_k, V_1, \dots, V_l \in \mathcal{A}(G)$  such that

$$B = U_1 \cdot \dots \cdot U_k = V_1 \cdot \dots \cdot V_l.$$

After renumbering if necessary there is some  $i \in [0, k-1]$  such that  $U_1 = V_1, \dots, U_i = V_i$  and  $\{U_{i+1}, \dots, U_k\} \cap \{V_{i+1}, \dots, V_l\} = \emptyset$ . Since  $|B| = m_l(G)$ , it follows that  $|U_1| = \dots = |U_i| = 1$  and that  $|U_r| \geq 2$  and  $|V_s| \geq 2$  for all  $r \in [i+1, k]$  and all  $s \in [i+1, l]$ .

Since  $U_k \nmid V_j$  for any  $j \in [i+1, l]$  and  $|U_k| \geq 2$  there are  $g_1, g_2 \in G$  such that  $g_1 g_2 \mid U_k$  and, after renumbering  $V_{i+1}, \dots, V_l$  if necessary,  $g_1 \mid V_{l-1}$  and  $g_2 \mid V_l$ . We set

$$\widetilde{U}_k = (g_1 + g_2)(g_1 g_2)^{-1} U_k \quad \text{and} \quad \widetilde{V}_{l-1} = (g_1 + g_2)(g_1 g_2)^{-1} V_{l-1} V_l.$$

Then  $\widetilde{U}_k \in \mathcal{A}(G)$ ,  $\widetilde{V}_{l-1} \in \mathcal{B}(G)$  and

$$U_1 \cdot \dots \cdot U_{k-1} \widetilde{U}_k = V_1 \cdot \dots \cdot V_{l-2} \widetilde{V}_{l-1}.$$

Suppose that  $\widetilde{V}_{l-1}$  is a product of  $t$  atoms. Then  $t \in [1, \rho_k(G) - (l-2)]$ .

Assume to the contrary that  $t \geq 2$ . Then

$$m_l(G) = |B| > |U_1 \cdot \dots \cdot U_{k-1} \widetilde{U}_k| \geq m_{l-2+t}(G) \geq m_l(G),$$

a contradiction.

Thus it follows that  $t = 1$ ,  $\widetilde{V}_{l-1} \in \mathcal{A}(G)$ ,  $l-1 \in \mathcal{V}_k(G)$  and

$$m_{l-1}(G) \leq |U_1 \cdot \dots \cdot U_{k-1} \widetilde{U}_k| < |U_1 \cdot \dots \cdot U_k| = m_l(G). \quad \square$$

**Corollary 3.4.** *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*

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

provided that  $\text{lD}(G) + j \geq 1$ .

*Proof.* If  $|G| = 2$ , then  $H$  is half-factorial,  $D(G) = 2$  and hence the assertion follows. Suppose that  $|G| \geq 3$ , and thus we get  $D(G) \geq 3$ .

Let  $l \in \mathbb{N}_0$  and  $j \in [0, D(G) - 1]$  such that  $lD(G) + j \geq 1$ . For  $j \in [0, 1]$  the assertion follows from Theorem 2.11.4.

Let  $j \in [2, D(G) - 1]$ . By Theorem 2.11 (items 2. and 3.) we obtain that

$$2l + \frac{2j}{D(G)} = \frac{lD(G) + j}{\rho(G)} \leq \lambda_{lD(G)+j}(G).$$

By Lemma 2.12.1 there are  $U_1, U_2, V_1, \dots, V_j \in \mathcal{A}(G)$  such that  $U_1 U_2 = V_1 \dots V_j$  whence  $\lambda_j(G) = 2$ . If  $l \in \mathbb{N}$ , then  $\lambda_{lD(G)}(G) = 2l$  and hence

$$\lambda_{lD(G)+j}(G) \leq \lambda_{lD(G)}(G) + \lambda_j(G) = 2l + 2.$$

Thus it follows that  $\lambda_{lD(G)+j}(G) \in \{2l + 1, 2l + 2\}$ .

Suppose that  $j \in [2, \rho_{2l+1}(G) - lD(G)]$ . Then  $l \geq 1$ , and by Theorem 3.3 we have

$$\mathcal{V}_{2l+1}(G) = [\lambda_{2l+1}(G), \rho_{2l+1}(G)].$$

Thus there are  $U_1, \dots, U_{2l+1}, V_1, \dots, V_{lD(G)+j} \in \mathcal{A}(G)$  such that  $U_1 \dots U_{2l+1} = V_1 \dots V_{lD(G)+j}$ . This implies that  $\lambda_{lD(G)+j}(G) \leq 2l + 1$  and hence equality holds.

Suppose that  $j > \rho_{2l+1}(G) - lD(G)$ , and assume to the contrary that  $\lambda_{lD(G)+j}(G) = 2l + 1$ . But this implies that  $\rho_{2l+1}(G) \geq lD(G) + j$ , a contradiction and hence we get  $\lambda_{lD(G)+j}(G) = 2l + 2$ .  $\square$

**Corollary 3.5.** *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  $k \in \mathbb{N}_{\geq 2}$  and every  $l \in \mathbb{N}_0$  we have  $\mathcal{V}_k(H) = [\lambda_k(H), \rho_k(H)]$ ,*

$$\rho_k(H) = \lfloor \frac{kD(G)}{2} \rfloor \quad \text{and}$$

$$\lambda_{lD(G)+j}(H) = \begin{cases} 2l + j & \text{for } j \in [0, 1] \\ 2l + 1 & \text{for } j \in [2, D(G)/2] \text{ and } l \geq 1, \\ 2l + 2 & \text{for } j \in [2, D(G) - 1] \text{ and (either } j > D(G)/2 \text{ or } l = 0), \end{cases}$$

provided that  $lD(G) + j \geq 1$ .

*Proof.* As in the proof of Theorem 3.3 it suffices to consider the block monoid  $\mathcal{B}(G)$ . By Theorem 3.3 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 1.11 whence for all  $k \in \mathbb{N}$  we have  $\lambda_k(G) = k = \rho_k(G)$ .

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

1. Let  $k \in \mathbb{N}$ . If  $k$  is even, then the assertion follows from Theorem 2.11.3. Suppose we know that

$$\rho_3(G) \geq \lfloor \frac{3D(G)}{2} \rfloor. \quad (*)$$

Then Theorem 2.11 and Lemma 3.2.4 imply that

$$\lfloor \frac{3D(G)}{2} \rfloor + kD(G) \leq \rho_3(G) + \rho_{2k}(G) \leq \rho_{2k+3}(G) \leq \lfloor \frac{(2k+3)D(G)}{2} \rfloor,$$

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

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

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

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

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

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

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

2. Since  $\rho_k(G) = \lfloor \frac{kD(G)}{2} \rfloor$ , the assertion on  $\lambda_{|D(G)+j}(G)$  follows from Corollary 3.4.  $\square$

### 3.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 3.6.

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

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

whence  $\mathcal{L}(G)$  contains APs with difference  $d$  and any length  $l$ .

**2. Multidimensional arithmetical progressions.** Let  $r \in \mathbb{N}$ ,  $d_1, \dots, d_r \in \mathbb{N}$  and  $l_1, \dots, l_r \in \mathbb{N}$ . 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 AP with difference  $d_i$  and length  $l_i$ . If  $G_1 \oplus \dots \oplus G_r \subset G$  and  $B = B_1^{l_1} \cdot \dots \cdot B_r^{l_r}$ , 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 beginning and end parts.** Let  $n \geq 3$ ,  $l \in \mathbb{N}$ ,  $g \in G$  with  $\text{ord}(g) = n$ ,  $B = (-g)^n g^n$ ,  $U = (2g)g^{n-2}$  and consider

$$\mathsf{L}(B^l U (-g)^n)$$

It is easy to check that  $\mathsf{L}(B^l U (-g)^n)$  is (almost) an arithmetical progression with difference 1, but has gaps at the beginning part.

**4. Arithmetical multiprogressions.** It is not difficult to show that for every finite subset  $L \subset \mathbb{N}_{\geq 2}$  there is a finite abelian group  $G_1$  such that  $L \in \mathcal{L}(G_1)$  ([58, 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 AP with difference  $d$  and length  $l$ . Thus for every  $l \in \mathbb{N}$  we have

$$\begin{aligned} \mathsf{L}(B_1 B_2^l) &= \mathsf{L}(B_1) + \mathsf{L}(B_2) \\ &= (x + 2l) + \mathcal{D} + \{\nu d \mid \nu \in [0, l]\} \\ &= \min \mathsf{L}(B_1 B_2^l) + \left( \mathcal{D} + d\mathbb{Z} \cap [0, \max \mathsf{L}(B_1 B_2^l) - \min \mathsf{L}(B_1 B_2^l)] \right). \end{aligned}$$

**Definition 3.7.** 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  $\min L + \mathcal{D} + d\mathbb{Z}$  (in part.,  $L \neq \emptyset$ ), 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  $L^* \neq \emptyset$ ), 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 non-empty 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 AP 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  $y \in \mathbb{Z}$ .
- $L^* = (\mathcal{D} + d\mathbb{Z}) \cap [0, \max L^*]$ .

AAMPs, as defined above, were introduced in [36] (a slightly less restrictive notion was defined in [56]). We cite three key results on the structure of sets of lengths in Krull monoids (proofs can be found in [58, Section 4.7], [94] and [58, Theorem 7.6.9]).

**Theorem 3.8.** *Let  $H$  be a Krull monoid with finite class group. Then there exist  $M \in \mathbb{N}_0$  and a finite set  $\Delta^* \subset \mathbb{N}$  such that the following holds: every  $L \in \mathcal{L}(H)$  is an AAMP with difference  $d \in \Delta^*$  and bound  $M$ .*

**Theorem 3.9.** *Let  $M \in \mathbb{N}_0$  and  $\Delta^* \subset \mathbb{N}$  be a finite non-empty 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*

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

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

**Theorem 3.10.** *Let  $H$  be a Krull monoid with class group  $G$  and  $a \in H$  such that*

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

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

### 3.C The characterization problem

Two reduced Krull monoids  $H$  and  $H'$  are isomorphic if and only if there is a group isomorphism  $\Phi: \mathcal{C}(H) \rightarrow \mathcal{C}(H')$  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 [58, 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 the system of sets of factorizations  $\mathcal{Z}(H) = \{\mathbf{Z}(a) \mid a \in H\}$  determines the class group (see [58, 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 1.11 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 [58, 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  $D(C_3) = D(C_2 \oplus C_2) = 3$ , and  $C_1, C_2, C_2 \oplus C_2$  and  $C_3$  are the only finite abelian groups  $G'$  with  $D(G') \leq 3$ . So the best we can hope for is a positive answer to the following question:

Given two finite abelian groups  $G$  and  $G'$  with  $D(G) \geq 4$  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  $D(G) \geq 4$  and  $\mathcal{L}(G) = \mathcal{L}(G')$ . We start with some simple observations and then we gather the results known so far.

**Proposition 3.11.**

1.  $\mathcal{L}(G) = \{y + L \mid y \in \mathbb{N}_0, L \in \mathcal{L}(G^\bullet)\} \supset \{\{y\} \mid y \in \mathbb{N}_0\}$ , and equality holds if and only if  $|G| \leq 2$ .
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  $|G'| \geq 3$  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  $k \in \mathbb{N}$ ,  $D(G) = D(G')$  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  $L(0^y B) = y + L(B)$ . 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 1.11 this is equivalent to  $|G| \leq 2$ .

2. If  $G_0 \subset G$  is a subset, then  $\mathcal{B}(G_0)$  is a divisor-closed submonoid of  $\mathcal{B}(G)$ , and thus the assertion follows.

3. By 1. we obtain  $|G| \geq 3$ . 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  $D(G) = \rho_2(G) = \rho_2(G') = D(G')$  by Theorem 2.11.3.

4. If  $G'$  is an abelian group with  $\mathcal{L}(G) = \mathcal{L}(G')$  and  $|G'| \geq 3$ , then it follows that  $D(G) = D(G') \geq 1 + d^*(G')$  (see Lemma 2.3.2). By the very definition of  $d^*(\cdot)$ , there are up to isomorphisms only finitely many finite abelian groups  $G'$  with  $d^*(G') < D(G)$ .  $\square$

**Proposition 3.12.** *Let  $G'$  be a finite abelian group with  $D(G') \in [4, 10]$ . If  $\mathcal{L}(G) = \mathcal{L}(G')$ , then  $G \cong G'$ .*

**Theorem 3.13.** *Let  $G$  be a finite elementary  $p$ -group and let  $G'$  be a finite elementary  $q$ -group with  $D(G') \geq 4$  and with primes  $p, q \in \mathbb{P}$ . If  $\mathcal{L}(G) = \mathcal{L}(G')$ , then  $G \cong G'$ .*

**Theorem 3.14.** *Let  $G'$  be a finite abelian group with  $D(G') \geq 4$  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  $n \geq 2$ .
4.  $G \cong C_n \oplus C_n$  with  $n \geq 3$ .

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

The results given in 3.12, 3.13 and 3.14 are mainly due to Wolfgang A. Schmid (see [95, 91, 92] and [58, Section 7.3]). In Section 5 we prove Theorem 3.14 for cyclic groups and for elementary 2-groups.



## Chapter 4

# Addition theorems and direct zero-sum problems

### 4.A The Theorems of Kneser and of Kemperman-Scherk

Let  $A, B \subset G$  be non-empty subsets. Then

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

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

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

denote the number of representations of  $g$  as a sum of an element of  $A$  and an element of  $B$ . In the 1950s M. Kneser proved the following addition theorem which is a basic result in additive group theory (a proof may be found in each of the following monographs [80, Chapter 1], [83, Chapter 4], [58, Section 5.2], and [99, Theorem 5.5]; for some recent development see [22, 65, 19, 63, 25, 24, 4, 70, 71, 73]). Corollary 4.3 is crucial in many investigations on the structure of zero-sumfree sequences (as for example in the proofs of Theorem 5.5 and Corollary 5.6).

**Theorem 4.1** (Kneser). *Let  $K = \text{Stab}(A + B)$  be the stabilizer of  $A + B$ .*

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

**Theorem 4.2** (Kemperman-Scherk). *Let  $K = \text{Stab}(A + B)$  be the stabilizer of  $A + B$ . Then*

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

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

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

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 4.1.4.

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  $|C_1 \cap C_2| \geq |A| + |B| - |A + B|$ . Since  $C_1 \cup C_2 \subset a + K$ , we obtain

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

**Corollary 4.3.** *If  $l \in \mathbb{N}$  and  $S = S_1 \cdots S_l \in \mathcal{A}^*(G)$ , then*

$$|\Sigma(S)| \geq |\Sigma(S_1)| + \dots + |\Sigma(S_l)|.$$

*Proof.* We proceed by induction on  $l$ , and it is clearly sufficient to consider the case  $S = S_1 S_2$ , where  $1 \neq S_1$  and  $1 \neq S_2$ . If  $A = \Sigma(S_1) \cup \{0\}$  and  $B = \Sigma(S_2) \cup \{0\}$ , then  $A + B \setminus \{0\} \subset \Sigma(S_1 S_2) = \Sigma(S)$ , and  $r_{A,B}(0) = 1$ , since  $S$  is zero-sumfree. Hence Theorem 4.2 implies  $|\Sigma(S)| \geq |A + B| - 1 \geq |A| + |B| - 2 = |\Sigma(S_1)| + |\Sigma(S_2)|$ .  $\square$

#### 4.B On the invariants $\eta(G)$ and $s(G)$

**Definition 4.4.**

1. A sequence  $S \in \mathcal{F}(G)$  is called *short* (in  $G$ ) if  $1 \leq |S| \leq \exp(G)$ .

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  $|S| \geq l$  has a short zero-sum subsequence.
3. We denote by  $\mathfrak{s}(G)$  the smallest integer  $l \in \mathbb{N}$  with the following property:
  - Every sequence  $S \in \mathcal{F}(G)$  of length  $|S| \geq l$  has a zero-sum subsequence  $T$  of length  $|T| = \exp(G)$ .

The investigation of these invariants has a long tradition in combinatorial number theory as well as in finite geometry. As already pointed out by H. Harborth ([74]),  $\mathfrak{s}(C_n^r)$  is the smallest integer  $l \in \mathbb{N}$  such that every set of  $l$  lattice point in  $r$ -dimensional euclidean space contains  $n$  elements which have a centroid with integral coordinates. For more information on geometric aspects of  $\mathfrak{s}(G)$  we refer to [27, Section 5].

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  $\varphi: G \rightarrow G/K$ .
- Consider a factorization  $S = S_0 S_1 \cdot \dots \cdot S_k$  such that  $|S_i|$  is small and  $\varphi(S_i) \in \mathcal{B}(G/K)$  for all  $i \in [1, k]$ .
- Investigate the sequences  $T = \sigma(S_1) \cdot \dots \cdot \sigma(S_k) \in \mathcal{F}(K)$  and  $S_0 T \in \mathcal{F}(G)$ . Clearly, if  $S$  is zero-sumfree, then  $S_0 T$  is zero-sumfree 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 4.7 and 4.8 we will demonstrate the power of this method in 4.13 and 4.14 (the polynomial method - recall the lecture by G. Karolyi - and coverings by cosets - see [58, Chapter 5.6], [98, 78] - are central methods which cannot be discussed here).

Our main result in this subsection is Theorem 4.13 which gives, for groups  $G$  of rank  $r(G) \leq 2$ , the precise values of  $\mathfrak{d}(G)$ ,  $\eta(G)$  and  $\mathfrak{s}(G)$ . For  $\mathfrak{d}(G)$  this was shown independently by J.E. Olson and D. Kruyswijk in the late 1960s. The result on  $\mathfrak{s}(G)$  is based on C. Reiher's work ([87]). The proof of 4.13, as presented here, follows the lines from [58, Theorem 5.8.3]. On our way we show the Theorem of Erdős-Ginzburg-Ziv, which was first proved in 1961 ([31]) and which is considered as a starting point in zero-sum theory (for some recent development of that flavor see [64, 66, 67]).

**Lemma 4.5.**

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

*Proof.* 1. The inequality  $D(G) \leq \eta(G)$  follows by Lemma 2.2.3 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  $|S| \geq s(G) - n + 1$ . We must prove that  $S$  has a short zero-sum subsequence. The sequence  $T = 0^{n-1}S \in \mathcal{F}(G)$  satisfies  $|T| \geq s(G)$ , 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. If  $r = 1$ , then  $\exp(G) = n_1 = D(C_{n_1}) \leq \eta(C_{n_1})$ , and thus  $\eta(C_{n_1}) = n_1$ . Let  $r \geq 2$  and  $(e_1, \dots, e_r)$  be a basis of  $G$  such that  $\text{ord}(e_i) = n_i$  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

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

be a non-empty zero-sum subsequence of  $S$ . Then  $n_0 \geq 1$  by Lemma 2.3. Since  $0 = \sigma(T) = (n'_1 + n_0)e_1 + \cdots + (n'_r + n_0)e_r$ , it follows that  $n'_i + n_0 \equiv 0 \pmod{n_i}$  for all  $i \in [1, r]$ , and  $1 \leq n'_i + n_0 \leq 2n_i - 2$  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 4.6.** *Let  $S \in \mathcal{F}(G)$ ,  $n \in \mathbb{N}$  and  $D(G \oplus C_n) \leq 3n - 1$ .*

1. *If  $|S| \geq D(G \oplus C_n)$ , then  $S$  has a zero-sum subsequence  $T \in \mathcal{B}(G)$  of length  $|T| \in \{n, 2n\}$ .*
2. *Suppose that  $D(G) \leq 2n - 1$  and  $|S| \geq D(G \oplus C_n)$ . Then  $S$  has a zero-sum subsequence  $T \in \mathcal{B}(G)$  of length  $|T| \in [1, n]$ . In particular, if  $n \leq \exp(G)$  and  $D(G) \leq 2n - 1$ , then  $\eta(G) \leq D(G \oplus C_n)$ .*

*Proof.* Let  $G \oplus C_n = G \oplus \langle e \rangle$  with  $\text{ord}(e) = n$ , 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  $\varphi: G \oplus C_n \rightarrow G \oplus C_n$  by  $\varphi(g) = g + e$  for every  $g \in G$ .

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

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

**Lemma 4.7.** *Let  $\varphi: G \rightarrow \overline{G}$  be a group epimorphism and  $k \in \mathbb{N}$ .*

1. *If  $S \in \mathcal{F}(G)$  and  $|S| \geq (k-1) \exp(\overline{G}) + \mathbf{s}(\overline{G})$ , then  $S$  admits a product decomposition  $S = S_1 \cdots S_k S'$ , where  $S_1, \dots, S_k, S' \in \mathcal{F}(G)$  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  $|S| \geq (k-1) \exp(\overline{G}) + \eta(\overline{G})$ , then  $S$  admits a product decomposition  $S = S_1 \cdots S_k S'$ , where  $S_1, \dots, S_k, S' \in \mathcal{F}(G)$  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  $S = S_1 \cdots S_j S'$  where  $S_1, \dots, S_j, S' \in \mathcal{F}(G)$  and, for every  $i \in [1, j]$ ,  $\varphi(S_i)$  has sum zero and length  $|S_i| = \exp(\overline{G})$ . Then

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

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.  $\square$

**Lemma 4.8.** *Let  $K \subset G$  be a subgroup.*

1. *If  $S \in \mathcal{F}(G)$  and  $|S| \geq (\mathbf{s}(K) - 1) \exp(G/K) + \mathbf{s}(G/K)$ , 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*

$$\mathbf{s}(G) \leq (\mathbf{s}(K) - 1) \exp(G/K) + \mathbf{s}(G/K).$$

2. If  $S \in \mathcal{F}(G)$  and  $|S| \geq (\eta(K) - 1) \exp(G/K) + \eta(G/K)$ , then  $S$  has a zero-sum subsequence  $T$  of length  $1 \leq |T| \leq \exp(K) \exp(G/K)$ . In particular, if  $\exp(G) = \exp(K) \exp(G/K)$ , then

$$\eta(G) \leq (\eta(K) - 1) \exp(G/K) + \eta(G/K).$$

3.  $d(G) \leq d(K) \exp(G/K) + \max\{d(G/K), \eta(G/K) - \exp(G/K) - 1\}$ .

*Proof.* Let  $\varphi: G \rightarrow G/K$  denote the canonical epimorphism. If  $K = \{0\}$ , then all assertions are obvious. Suppose that  $K \neq \{0\}$ .

1. Let  $S \in \mathcal{F}(G)$  be a sequence with  $|S| \geq (s(K) - 1) \exp(G/K) + s(G/K)$ . By Lemma 4.7.1,  $S$  has a product decomposition  $S = S_1 \cdots S_{s(K)} S'$ , where  $S_1, \dots, S_{s(K)}, S' \in \mathcal{F}(G)$  and, for every  $i \in [1, s(K)]$ ,  $\varphi(S_i)$  has sum zero and length  $|S_i| = \exp(G/K)$ . Then the sequence  $\sigma(S_1) \cdots \sigma(S_{s(K)}) \in \mathcal{F}(K)$  has a zero-sum subsequence  $V$  of length  $|V| = \exp(K)$ , say

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

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

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

We must prove that  $S$  is not zero-sumfree. Since  $|S| \geq (d(K) - 1) \exp(G/K) + \eta(G/K)$ , Lemma 4.7.2 provides us with a product decomposition  $S = S_1 \cdots S_{d(K)} S'$ , where  $S_1, \dots, S_{d(K)}, S' \in \mathcal{F}(G)$  and, for every  $i \in [1, d(K)]$ ,  $\varphi(S_i)$  has sum zero and length  $|S_i| \in [1, \exp(G/K)]$ . Now we obtain  $|S'| \geq |S| - \exp(G/K)d(K) > d(G/K)$ , and therefore  $S'$  has a non-empty subsequence  $S_0$  such that  $\varphi(S_0)$  has sum zero. Hence  $V = \sigma(S_0)\sigma(S_1) \cdots \sigma(S_{d(K)}) \in \mathcal{F}(K)$ , and  $|V| > d(K)$  implies that  $V$  is not zero-sumfree. Hence  $T = S_0 S_1 \cdots S_{d(K)}$  is a subsequence of  $S$  which is not zero-sumfree.  $\square$

The following two results are due to W. Gao and the presented simple proof of 4.9 may be found in [54].

**Proposition 4.9** (Gao). *Let  $S \in \mathcal{F}(G)$  be a sequence of length  $|S| \geq |G|$ ,*

$$k = \max\{v_g(S) \mid g \in G\} \quad \text{and} \quad k' = \max\{\text{ord}(g) \mid g \in \text{supp}(S)\}.$$

*Then  $S$  has a non-empty zero-sum subsequence  $T$  of length  $|T| \leq \min\{k, k'\}$ .*

*Proof.* If  $k' \leq k$ , let  $g \in G$  be such that  $v_g(S) = k$ . Then  $T = g^{\text{ord}(g)}$  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  $0 \in \text{supp}(S)$ , we set  $T = 0$ . Thus suppose that  $0 \notin \text{supp}(S)$ . Since  $k = \max\{v_g(S) \mid g \in G\}$ , there exists a decomposition  $S = S_1 \cdots S_k$ , where  $S_1, \dots, S_k \in \mathcal{F}(G)$  are squarefree, and we set  $\text{supp}(S_i) = B_i$  for  $i \in [1, k]$ .

Let  $A, B, C \subset G$  be non-empty subsets. We set

$$A \oplus B = A \cup B \cup (A + B),$$

and clearly we have  $A \oplus B = B \oplus A$  and  $A \oplus (B \oplus C) = (A \oplus B) \oplus C$ . Assume to the contrary that  $S$  has no zero-sum subsequence  $T$  as required, which implies that  $0 \notin B_1 \oplus \dots \oplus B_k$ . For  $i \in [1, k]$  we set  $A_i = B_i \cup \{0\}$ , and assert that for every  $i \in [1, k]$ ,

$$|A_1 + \dots + A_i| \geq |B_1| + \dots + |B_i| + 1.$$

We proceed by induction on  $i$ . For  $i = 1$  this is clear. Suppose that  $i \in [2, k]$  and that the assertion holds for  $i - 1$ . Then we apply Theorem 4.2 to

$$A_1 + \dots + A_{i-1} = B_1 \oplus \dots \oplus B_{i-1} \cup \{0\} \quad \text{and to} \quad A_i$$

and obtain

$$\begin{aligned} |A_1 + \dots + A_i| &\geq |A_1 + \dots + A_{i-1}| + |A_i| - 1 \\ &\geq (|B_1| + \dots + |B_{i-1}| + 1) + (|B_i| + 1) - 1 \\ &= |B_1| + \dots + |B_i| + 1. \end{aligned}$$

Thus for  $i = k$  we get

$$|A_1 + \dots + A_k| \geq |B_1| + \dots + |B_k| + 1 = |G| + 1,$$

a contradiction.  $\square$

**Theorem 4.10** (Gao). *We have  $\eta(G) \leq |G|$  and  $s(G) \leq |G| + \exp(G) - 1$ .*

*Proof.* By Lemma 4.5.1 it suffices to verify the upper bound for  $s(G)$ . We set  $n = \exp(G)$  and must prove that every sequence  $S \in \mathcal{F}(G)$  of length  $|S| \geq |G| + n - 1$  has a zero-sum subsequence of length  $n$ . Thus assume that

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

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

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

It is sufficient to prove that  $U$  has a zero-sum subsequence  $V$  such that  $n - k \leq |V| \leq n$ . Indeed, if  $V = (g_2 - g_1)^{k'_2} \cdot \dots \cdot (g_l - g_1)^{k'_l}$  is such a zero-sum subsequence, where  $k'_i \in [0, k_i]$  for all  $i \in [2, l]$  and  $n - k \leq k'_2 + \dots + k'_l \leq n$ , then  $0 \leq n - (k'_2 + \dots + k'_l) \leq k$ , and the sequence

$$T = g_1^{n-(k'_2+\dots+k'_l)} g_2^{k'_2} \cdot \dots \cdot g_l^{k'_l}$$

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

Since  $|U| = |S| - k \geq |G| + n - 1 - k \geq |G|$  and  $\eta(G) \leq |G|$ , 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  $|V| \leq n - k - 1$ . If  $U = VV'$ , then  $|V'| = |U| - |V| \geq (|G| + n - 1 - k) - (n - k - 1) = |G|$ , and by Proposition 4.9 it follows that  $V'$  has a zero-sum subsequence  $V''$  of length

$$1 \leq |V''| \leq \max\{v_g(V') \mid g \in G\} \leq \max\{v_g(U) \mid g \in G\} \leq k.$$

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

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

a contradiction to the maximality of  $|V|$ .  $\square$

In the same spirits (using 4.9 and 4.10) W. Gao ([38]) proved that  $|G| + d(G)$  is the smallest integer  $l \in \mathbb{N}$  such that every sequence  $T \in \mathcal{F}(G)$  of length  $|T| \geq l$  has a zero-sum subsequence of length  $|G|$  (there is a weighted generalization of this theorem by Y.ould Hamidoune [72] and for more of this flavor see [55, 2, 1]). For cyclic groups Gao's Theorem reduces to the classical result of Erdős-Ginzburg-Ziv.

**Corollary 4.11** (Erdős-Ginzburg-Ziv). *For every  $n \in \mathbb{N}$  we have*

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

*Proof.* By Lemma 4.5 and Theorem 4.10, we obtain

$$n = D(C_n) \leq \eta(C_n) \leq |C_n| = n$$

and thus  $\eta(C_n) = n$ . Again by Lemma 4.5 and by Theorem 4.10 we get

$$2n - 1 = \eta(C_n) + \exp(C_n) - 1 \leq s(C_n) \leq |C_n| + \exp(C_n) - 1 = 2n - 1$$

and thus  $s(C_n) = 2n - 1$ .  $\square$

**Proposition 4.12** (Reiher). *For every prime  $p \in \mathbb{P}$  we have  $s(G) \leq 4p - 3$ .*

*Proof.* The original proof by C. Reiher (see [87]) is based on the Theorem of Chevalley-Waring (see [99, Theorem 9.24]). A proof using group algebras may be found in [58, Proposition 5.8.1].  $\square$

**Theorem 4.13.** *Let  $G = C_{n_1} \oplus C_{n_2}$  with  $1 \leq n_1 | n_2$ . Then*

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

*Proof.* By Corollaries 4.11 and 2.4, the result holds for  $n_1 = 1$ . Suppose that  $n_1 > 1$  and note that  $\exp(G) = n_2$ . By Lemma 2.3 we have  $d^*(G) \leq d(G)$ . Now Lemma 4.5 implies that

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

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

We use induction on  $\exp(G)$ . If  $p \in \mathbb{P}$  and  $G = C_p \oplus C_p$ , then  $d(G) = 2p - 2$  by Theorem 2.10, and Proposition 4.12 implies  $s(G) \leq 4p - 3$ .

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 4.8.1 we obtain

$$s(G) \leq (s(pG) - 1)p + s(G/pG) \leq (2m_1 + 2m_2 - 4)p + (4p - 3) = 2n_1 + 2n_2 - 3,$$

and Lemma 4.8.3 implies

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

We briefly discuss the state of the art concerning groups of higher rank (more detailed information can be found in [47]). A conjecture by W. Gao states that we always have  $\eta(G) = s(G) - \exp(G) + 1$ . This was recently proved for  $p$ -groups  $G$  with  $D(G) = 2\exp(G) - 1$  ([97]). C. Elsholtz et. al. showed that, for all odd  $n \geq 3$ ,

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

and it is conjectured that all bounds are sharp ([28, 27, 26]).

It is conjectured that, if  $r(G) = 3$  or  $G = C_n^r$  with  $n, r \geq 3$ , then  $d(G) = d^*(G)$ . On the other hand, for every  $r \geq 4$  there are infinitely many groups  $G$  of rank  $r(G) = r$  such that  $d(G) > d^*(G)$  (see [60] and [32]). We end with a result (see [15]) providing more groups  $G$  with  $d(G) = d^*(G)$  and whose proof demonstrates once more the power of the inductive method (for recent results see [6, 5]).

**Theorem 4.14.** *Let  $G = K \oplus C_{km}$  where  $k, m \in \mathbb{N}$  and  $K \subset G$  is a subgroup with  $\exp(K) | m$ . If  $d(K \oplus C_m) = d(K) + m - 1$  and  $\eta(K \oplus C_m) \leq d(K) + 2m$ , then  $d(G) = d(K) + km - 1$ .*

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

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

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

Lemma 4.7 provides us with a product decomposition

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

where  $S_1, \dots, S_{k-1}, S' \in \mathcal{F}(G)$  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

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

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

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

and there is a non-empty 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 zero-sum subsequence of  $S$ .  $\square$

**Corollary 4.15.** *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  $d(K) \leq m - 1$ . Then  $d(G) = d^*(G)$ .*

*Proof.* Since  $K \oplus C_m$  is a  $p$ -group, Theorem 2.10 implies that

$$d(G \oplus C_m) = d^*(K \oplus C_m) = d^*(K) + m - 1 = d(K) + m - 1.$$

Since  $\exp(K)$  is a  $p$ -power and  $\exp(K) - 1 \leq d(K) \leq m - 1$ , it follows that  $\exp(K)$  divides  $m$ . By Lemma 4.6 we infer that

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

Thus all assumptions of Theorem 4.14 are satisfied and we obtain that

$$d(G) = d(K) + km - 1 = d^*(K) + km - 1 = d^*(G).$$

$\square$

## Chapter 5

# Inverse zero-sum problems and arithmetical consequences

The investigation of inverse problems has a long tradition in combinatorial number theory (see [83]), 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  $D(G)$ ,  $\eta(G)$  and  $s(G)$ . More precisely, we investigate the structure of sequences of length  $D(G) - 1$  ( $\eta(G) - 1$  or  $s(G) - 1$  respectively) that do not have a zero-sum subsequence (of the required length). 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.

### 5.A Cyclic groups

Clearly, we can rephrase Corollary 2.4.1 as follows: let  $G$  be cyclic of order  $n \geq 2$  and  $S \in \mathcal{F}(G)$  a sequence of length  $\eta(G) - 1$ . Then  $S$  has no short zero-sum subsequence if and only if  $S = g^{n-1}$  for some  $g \in G$  with  $\text{ord}(g) = n$ . A. Bialostocki and P. Dierker (see [7, Lemma 4]) first characterized the extremal case for the  $s(G)$  invariant.

**Theorem 5.1** (Bialostocki-Dierker). *Let  $G$  be cyclic of order  $n \geq 2$ . Then every sequence  $S \in \mathcal{F}(G)$  of length  $|S| = s(G) - 1$  that has no zero-sum subsequence of length  $n$  has the form  $S = T^{n-1}$  for some sequence  $T$  over  $G$ .*

Let  $S$  and  $T = gh$  be as above with  $g, h \in G$ . Then  $-g + S = 0^{n-1}(g-h)^{n-1}$  has no zero-sum subsequence of length  $n$  and hence  $\text{ord}(g-h) = n$ . Conversely, for all  $a, b \in G$  with  $\text{ord}(a-b) = n$  the sequence  $a^{n-1}b^{n-1}$  has no zero-sum subsequence of length  $n$ .

Theorem 5.1 was the starting point for a huge variety of investigations (see [10, 33, 11, 39, 8, 100, 53, 75, 54]). We present a short proof of Theorem 5.1 which is based on the following result of W. Gao (see [37, Theorem 1]).

**Proposition 5.2** (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*

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

*Proof.* The proof is based on Kneser's Addition Theorem and on Proposition 4.9.  $\square$

*Proof of Theorem 5.1.* Let  $S \in \mathcal{F}(G)$  be a sequence of length  $2n - 2$  which has no zero-sum subsequence of length  $n$ . Since  $0 \in \Sigma(g + S)$  for every  $g \in G$ , Proposition 5.2 implies that, for every  $g \in G$ , the sequence  $g + S$  has a zero-sumfree subsequence  $g + S_1$  of length  $n - 1$ . Then Corollary 2.4 implies that  $g + S_1 = a^{n-1}$  hence  $S_1 = c^{n-1}$  with  $c = a - g$ . Then  $S = c^{n-1}S_2$  for some sequence  $S_2 \in \mathcal{F}(G)$  of length  $|S_2| = n - 1$  and  $-c + S = 0^{n-1}(-c + S_2)$ . Since  $-c + S$  has no zero-sum subsequence of length  $n$ , we infer that  $-c + S_2$  is zero-sumfree whence  $-c + S_2 = d^{n-1}$  for some  $d \in G$ . Thus it follows that  $S = c^{n-1}(c + d)^{n-1}$ .  $\square$

In order to study the structure of minimal zero-sum sequences of length greater than or equal to  $(|G| + 1)/2$ , we introduce the index of a zero-sum sequence (see [16, 42, 18]). After a simple lemma we state the crucial structural result, which was achieved independently by S. Savchev and F. Chen and by P. Yuan.

**Definition 5.3.**

1. Let  $g \in G$  be a non-zero element with  $\text{ord}(g) = n < \infty$ . For a sequence

$$S = (n_1g) \cdot \dots \cdot (n_lg), \quad \text{where } l \in \mathbb{N}_0 \quad \text{and} \quad n_1, \dots, n_l \in [1, n],$$

we define

$$\|S\|_g = \frac{n_1 + \dots + n_l}{n}.$$

2. Let  $S$  be a zero-sum sequence for which  $\langle \text{supp}(S) \rangle \subset G$  is cyclic. Then we call

$$\text{ind}(S) = \min\{\|S\|_g \mid g \in G \text{ with } \langle \text{supp}(S) \rangle = \langle g \rangle\} \in \mathbb{N}_0$$

the *index* of  $S$ .

3. If  $G$  is cyclic, then let  $l(G)$  denote the smallest integer  $l \in \mathbb{N}$  such that every minimal zero-sum sequence  $S \in \mathcal{F}(G)$  of length  $|S| \geq l$  satisfies  $\text{ind}(S) = 1$ .

**Lemma 5.4.** *Let  $G$  be cyclic and  $S \in \mathcal{B}(G)$ . Then*

$$\begin{aligned} \text{ind}(S) &= \min\{\|S\|_g \mid g \in G \text{ with } \text{supp}(S) \subset \langle g \rangle\} \\ &= \min\{\|S\|_g \mid g \in G \text{ with } G = \langle g \rangle\}. \end{aligned}$$

*Proof.* We set  $|G| = n$ ,

$$I_1 = \min\{\|S\|_g \mid g \in G \text{ with } \text{supp}(S) \subset \langle g \rangle\} \quad \text{and}$$

$$I_2 = \min\{\|S\|_g \mid g \in G \text{ with } G = \langle g \rangle\}.$$

Let  $|S| = l$ ,  $g \in G$  with  $\text{ord}(g) = m$  and  $S = (a_1g) \cdots (a_lg)$  with  $a_1, \dots, a_l \in [1, m]$  such that  $\|S\|_g = I_1$ . First we verify that  $I_1 = I_2$  and then we show that  $I_1 = \text{ind}(S)$ .

1. Obviously, we have  $I_1 \leq I_2$ , 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

$$\begin{aligned} S &= (a_1 \frac{n}{m}h) \cdots (a_l \frac{n}{m}h) \quad \text{with } a_1 \frac{n}{m}, \dots, a_l \frac{n}{m} \in [1, n], \\ \|S\|_h &= \frac{\frac{n}{m}a_1 + \dots + \frac{n}{m}a_l}{n} = \frac{a_1 + \dots + a_l}{m} = \|S\|_g \end{aligned}$$

and hence  $I_2 \leq \|S\|_h = \|S\|_g = I_1$ .

2. Obviously, we have  $I_1 \leq \text{ind}(S)$ , and it remains to verify the reverse inequality. We set  $\langle a_1g, \dots, a_lg \rangle = K$  and pick an  $a \in [1, m]$  with  $a \mid m$  and  $K = \langle ag \rangle$ . Then  $\text{ord}(ag) = a^{-1}m$ . For every  $i \in [1, l]$  we have  $a_i g \in \langle ag \rangle = \{ag, 2ag, \dots, (a^{-1}m)ag\}$  and hence  $a_i = aa'_i$  with  $a'_i \in [1, a^{-1}m]$ . Thus we obtain

$$\begin{aligned} S &= (a'_1 ag) \cdots (a'_l ag), \\ \|S\|_g &= \frac{a(a'_1 + \dots + a'_l)}{m} = \frac{a'_1 + \dots + a'_l}{a^{-1}m} = \|S\|_{ag} \end{aligned}$$

and hence  $I_1 = \|S\|_g = \|S\|_{ag} \geq \text{ind}(S)$ .  $\square$

**Theorem 5.5.** *Let  $G$  be cyclic of order  $n \geq 1$ . If  $n \in \{1, 2, 3, 4, 5, 7\}$ , then  $\mathfrak{l}(G) = 1$ , and otherwise we have  $\mathfrak{l}(G) = \lfloor \frac{n}{2} \rfloor + 2$ .*

*Proof.* See [101, Theorem 3.1] or [89, Proposition 10].  $\square$

Theorem 5.5 allows a structural description of long zero-sumfree sequences over cyclic groups. The second statement of the following corollary was first proved by J.D. Bovey, P. Erdős and I. Niven ([9]) and the fourth statement by A. Geroldinger and Y.ould Hamidoune ([59]). Note that the bounds given in 5.6.4 are attained.

**Corollary 5.6.** *Let  $G$  be cyclic of order  $n \geq 3$ ,  $S \in \mathcal{F}(G)$  a zero-sumfree sequence of length*

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

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

$$\nu_g(S) \geq \frac{n+5}{6} \text{ if } n \text{ is odd, and } \nu_g(S) \geq 3 \text{ if } n \text{ is even.}$$

*Proof.* 1. See [58, Theorem 5.4.5].

2. We write  $S$  in the form  $S = S_1 \cdot \dots \cdot S_k (gh)^l g^{m-l}$ , where  $k, m \in \mathbb{N}_0$ ,  $l \in [0, m]$ ,  $g \neq h$ ,  $S_1, \dots, S_k$  are squarefree, and  $|S_i| = 3$  for all  $i \in [1, k]$ . It can be checked that  $|\Sigma(gh)| = 3$  and  $|\Sigma(S_j)| \geq 6$  for all  $j \in [1, k]$  (here we need 1). By Corollary 4.3 it follows that

$$n-1 \geq |\Sigma(S)| \geq 6k + 3l + (m-l) \geq 6k + 2l + 2m - \nu_g(S) = 2|S| - \nu_g(S)$$

and therefore  $\nu_g(S) \geq 2|S| - n + 1$ .

3. and 4. The sequence  $S_1 = (-\sigma(S))S$  is a minimal zero-sum sequence of length  $|S_1| \geq (n+3)/2$ . Thus Theorem 5.5 implies that  $\text{ind}(S_1) = 1$ . Thus there is an element  $h \in G$  with  $\text{ord}(h) = n$  such that

$$S_1 = (xh)h^u(2h)^v(x_1h) \cdot \dots \cdot (x_t h),$$

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

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

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

$$\max\{\nu_h(S), \nu_{2h}(S)\} = \max\{u, v\} \geq |S| - \frac{n-1}{3} \geq \frac{n+5}{6}.$$

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

$$\nu_h(S) = u = 2|S| - n + r + t \geq 2 + r + t \geq 3.$$

□

## 5.B Groups of higher rank

For  $G = C_n^r$ , with  $n, r \in \mathbb{N}$  and  $n \geq 2$ , we consider 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  $|S| = \mathfrak{s}(G) - 1$  that has no zero-sum subsequence of length  $n$  has the form  $S = T^{n-1}$  for some sequence  $T$  over  $G$ .

If  $r = 1$ , then  $G$  has Property **D** by Theorem 5.1. For groups of rank two, Property **C** was first considered by P. van Emde Boas and Property **D** by W. Gao (see [29, 41], [40, Lemma 4.7]).

Suppose that Property **D** holds. Then, by definition, there exists some  $c(G) \in \mathbb{N}$  such that  $\mathfrak{s}(G) = c(G)(n - 1) + 1$ . Moreover, a simple argument shows that Property **C** holds (see [47, Section 7]) and that  $\eta(G) = (c(G) - 1)(n - 1) + 1$  (see [27, Lemma 2.3]). For  $r = 1$  we have  $c(G) = 2$  and for  $r = 2$  we have  $c(G) = 4$  (see Theorem 4.13). In case of higher ranks bounds for  $c(G)$  are given by N. Alon and M. Dubiner ([3]) and then in [76, 28, 27, 26]).

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 [27, Lemma 2.3.3] and the subsequent discussion). In [50] it is shown that Property **C** and Property **D** are both multiplicative, provided that the  $c(\cdot)$  invariants of all involved groups coincide. We provide the precise formulation for Property **D**.

**Theorem 5.7.** *Let  $G = C_{mn}^r$  with  $m, n, r \in \mathbb{N}$ . If both  $C_m^r$  and  $C_n^r$  have Property **D** and*

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

*then  $G$  has Property **D**.*

In [47, Conjecture 7.2] it is conjectured that every group  $G = C_n^r$ , where  $r \in \mathbb{N}$  and  $n \in \mathbb{N}_{\geq 2}$ , has Property **D**. More results in groups of higher rank may be found in [51].

From now on we restrict our discussion on groups of rank two. We say that  $G = C_n \oplus C_n$  with  $n \geq 2$  has Property **B** if every minimal zero-sum sequence  $S \in \mathcal{F}(G)$  of length  $|S| = \mathfrak{D}(G) = 2n - 1$  contains some element with multiplicity  $n - 1$ . This property was first addressed in [44], and it is conjectured that every group (of the above form) satisfies Property **B**.

**Proposition 5.8.** *Let  $G = C_n \oplus C_n$  with  $n \geq 2$  and let  $S \in \mathcal{F}(G)$ .*

1. If  $S$  has length  $D(G)$ , 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  $x_1, \dots, x_n \in [0, n - 1]$  with  $x_1 + \dots + x_n \equiv 1 \pmod{n}$  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

$$S = (e_1 e_2 (-x e_1 + e_2))^{n-1}.$$

3. If  $S$  has length  $\mathfrak{s}(G) - 1$ , 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  $g \in \text{supp}(S)$  there exists a basis  $(e_1, e_2)$  of  $G$  and some  $x \in [1, n - 1]$  with  $\gcd(x, n) = 1$  such that

$$-g + S = (0e_1 e_2 (-x e_1 + e_2))^{n-1}.$$

*Proof.* For 1. see [58, Theorem 5.8.7], and for 2. see [93]. To verify 3., let  $S = T^{n-1}$  be as in 3.(a) and let  $g \in \text{supp}(S)$ . 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 reverse implication is obvious.  $\square$

Suppose that the group  $C_n \oplus C_n$ , with  $n \geq 2$ , satisfies Property **B**. Then Proposition 5.8 completely describes the structure all minimal zero-sum sequences over  $C_n \oplus C_n$  of length  $D(C_n \oplus C_n) = 2n - 1$ , and Wolfgang A. Schmid even characterized the structure of all minimal zero-sum sequences over  $C_n \oplus C_{nm}$ , for any  $m \in \mathbb{N}$ , of length  $D(C_n \oplus C_{nm}) = n + mn - 1$  (see [93], which generalizes results from [45, 90]). Similar statements hold true for Properties **C** and **D**.

Since Property **B** implies Property **C** (see [46, Theorem 6.2] and [47, Theorem 6.7.2.(b)]), the emphasis of research was placed on Property **B**. The next theorem

gathers some results supporting Property **B** (see also [58, Section 5.8] and [77]). Most recent results will be discussed during the Course. Clearly,  $C_2 \oplus C_2$  has Property **B**.

**Theorem 5.9.** *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  $|S| = D(G)$ , then  $|\text{supp}(S)| \in [3, p]$ .*
2. *If  $S$  is zero-sumfree of length  $D(G) - 1$ ,  $\varepsilon > 0$  and  $p$  sufficiently large, then  $S$  contains some element  $g$  with multiplicity  $v_g(S) > p^{1/4-\varepsilon}$ .*

*Proof.* 1. See [58, Proposition 5.8.5]. Note that for every  $j \in [3, p]$  there is an  $S_j \in \mathcal{A}(G)$  of length  $|S_j| = D(G)$  and with  $|\text{supp}(S_j)| = j$ .

2. See [50, 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

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

### 5.C Arithmetical consequences

Some simple arithmetical consequences of Property **B** can be found in [58, Chapter 6]. In this subsection we restrict to cyclic groups and start with a result, first proved in [43] and based on Theorem 5.5.

**Theorem 5.10.** *Let  $H$  be a Krull monoid with cyclic class group  $G$  of order  $n \geq 2$  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 1.14 it suffices to consider  $\mathcal{B}(G)$ . Assume to the contrary that there is some  $k \in \mathbb{N}$  such that  $\rho_{2k+1}(G) \geq kn + 2$ . Let  $k \in \mathbb{N}$  be minimal with this property whence  $\rho_{2k-1}(G) = (k-1)n + 1$  and  $\rho_{2k+1}(G) \geq kn + 2$ . Then there exists a  $B \in \mathcal{B}(G)$  and minimal zero-sum sequences  $U_1, \dots, U_{2k+1}, V_1, \dots, V_\rho$  with  $\rho = \rho_{2k+1}(G)$  and

$$B = U_1 \cdots U_{2k+1} = V_1 \cdots V_\rho. \quad (*)$$

We may suppose that  $|B|$  is maximal such that an equation (\*) holds. Furthermore, we may suppose that  $|U_1| \geq \dots \geq |U_{2k+1}|$ , and since  $\rho_{2k}(G) = kn$ , it follows that  $0 \nmid B$  whence  $|U_{2k+1}| \geq 2$ .

Suppose there is some  $h \in G$  such that  $(-h)h \mid B$ , say  $h \mid V_1$  and  $(-h) \mid V_2$ . Then

$$V_1 V_2 = ((-h)h) V_2' \quad \text{with} \quad V_2' \in \mathcal{A}(G).$$

Thus we may suppose that there is an  $\ell \in \mathbb{N}_0$  such that  $|V_1| = \dots = |V_\ell| = 2$ ,  $3 \leq |V_{\ell+1}| \leq \dots \leq |V_\rho|$  and there is no  $h \in G$  with  $(-h)h \mid V_{\ell+1} \cdot \dots \cdot V_\rho$ . If  $\ell = 0$ , then

$$\rho \leq \frac{|U_1 \cdot \dots \cdot U_{2k+1}|}{3} \leq kn + 1,$$

a contradiction. Thus we have  $\ell \geq 1$ .

Suppose there is some  $i \in [1, 2k+1]$  such that  $\text{ind}(U_i) = 1$ . Then there is some  $g \in G$  with  $\text{ord}(g) = n$  such that  $U_i = (a_1g) \cdot \dots \cdot (a_sg)$  with  $s = |U_i|$ ,  $a_1, \dots, a_s \in [1, n]$  and  $\|U_i\|_g = 1$ . Assume to the contrary that  $s < n$ . Then there is some  $\nu \in [1, s]$ , say  $\nu = 1$ , with  $a_1 \geq 2$ , and there is some  $j \in [1, \rho]$  such that  $(a_1g) \mid V_j$ . Then

$$U'_i = (a_1g)^{-1}g((a_1 - 1)g)U_i \in \mathcal{B}(G), \quad V'_j = (a_1g)^{-1}g((a_1 - 1)g)V_j \in \mathcal{B}(G)$$

and

$$B' = U_i^{-1}U'_iU_1 \cdot \dots \cdot U_{2k+1} = V_j^{-1}V'_jV_1 \cdot \dots \cdot V_\rho.$$

Since  $\|U_i\|_g = \|U'_i\|_g = 1$ , it follows that  $U'_i \in \mathcal{A}(G)$ . Since  $\rho = \rho_{2k+1}(G)$ , it follows that  $V'_j \in \mathcal{A}(G)$ . But this is a contradiction to the maximality of  $|B|$ . Thus  $s = n$  and  $U_i = g^n$ .

If  $|U_{2k}| \leq \lfloor \frac{n}{2} \rfloor + 1$ , then

$$\rho \leq \frac{|U_1 \cdot \dots \cdot U_{2k-1}U_{2k}U_{2k+1}|}{2} \leq \frac{1}{2}((2k-1)n + \lfloor \frac{n}{2} \rfloor + 1 + \lfloor \frac{n}{2} \rfloor + 1) \leq kn + 1,$$

a contradiction. Thus  $|U_1| \geq \dots \geq |U_{2k}| \geq \lfloor \frac{n}{2} \rfloor + 2$ , and Proposition 3.2 implies that  $\text{ind}(U_1) = \dots = \text{ind}(U_{2k}) = 1$ . Therefore, for all  $i \in [1, 2k]$ , we have  $U_i = g_i^n$  where  $g_i \in G$  with  $\text{ord}(g_i) = n$ .

Suppose there are distinct  $i, j \in [1, 2k+1]$  such that  $U_i = g^n$  and  $U_j = (-g)^n$  for some  $g \in G$ . Then  $\ell \geq n$ , and after renumbering if necessary we may suppose that  $V_1 = \dots = V_n = (-g)g$ . Since  $(U_iU_j)^{-1}U_1 \cdot \dots \cdot U_{2k+1} = V_{n+1} \cdot \dots \cdot V_\rho$ , it follows that  $(k-1)n + 1 = \rho_{2k-1}(G) \geq (k-1)n + 2$ , a contradiction. Thus there are no two  $U_i, U_j$  of such a form and hence  $\ell \leq |U_{2k+1}|$ .

Suppose that  $\text{ind}(U_{2k+1}) = 1$ . Then  $U_{2k+1} = g_{2k+1}^n$  for some  $g_{2k+1} \in G$  with  $\text{ord}(g_{2k+1}) = n$ . Since  $\ell \geq 1$ , it follows that  $g_{2k+1} \in \{-g_1, \dots, -g_{2k}\}$ , a contradiction. Thus  $\text{ind}(U_{2k+1}) \geq 2$ . Now Proposition 3.2 implies that

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

and therefore we obtain that

$$\begin{aligned} \rho &\leq \ell + \frac{|B| - 2\ell}{3} = \frac{|B| + \ell}{3} = \frac{2kn + |U_{2k+1}| + \ell}{3} \\ &\leq \frac{2kn + 2|U_{2k+1}|}{3} \leq \frac{2kn + n + 2}{3} \leq kn + \frac{2}{3}, \end{aligned}$$

a contradiction. □

**Corollary 5.11.** *Let  $H$  be a Krull monoid with cyclic class group  $G$  of order  $n \geq 2$  such that every class contains a prime. Then for every  $k \in \mathbb{N}$  and every  $l \in \mathbb{N}_0$  we have  $\mathcal{V}_k(H) = [\lambda_k(H), \rho_k(H)]$ ,*

$$\rho_{2k+j}(H) = kn + j \quad \text{for } j \in [0, 1] \quad \text{and}$$

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

provided that  $ln + j \geq 1$ .

*Proof.* As in the proof of Theorem 3.3 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  $n \geq 3$ , and let  $k \in \mathbb{N}$ . By Theorem 3.3 we obtain that  $\mathcal{V}_k(H) = [\lambda_k(G), \rho_k(G)]$ . The assertion on  $\rho_{2k+j}(G)$  follows from Theorem 5.10, and the assertion on  $\lambda_{ln+j}(G)$  follows from Corollary 3.4.  $\square$

**Corollary 5.12.** *Let  $G$  be either cyclic or an elementary 2-group with Davenport constant  $D(G) = n \geq 4$ . 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 3.11 implies that  $\Delta(G) = \Delta(G')$  and  $\rho_k(G) = \rho_k(G')$  for all  $k \in \mathbb{N}$ . Then Corollary 2.16 implies that  $G'$  is either cyclic or an elementary 2-group. Corollary 3.5 and Theorem 5.10 imply that

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

and thus it follows that  $G \cong G'$ .  $\square$

**Acknowledgement** This work was supported by the Austrian Science Fund FWF, Project No. P18779-N13.



# Bibliography

- [1] S.D. Adhikari and Yong-Gao Chen, *Davenport constant with weights and some related questions II*, J. Comb. Theory, Ser. A **115** (2008), 178 – 184.
- [2] S.D. Adhikari and P. Rath, *Davenport constant with weights and some related questions*, Integers **6** (2006), Paper A30, 6p.
- [3] N. Alon and M. Dubiner, *A lattice point problem and additive number theory*, Combinatorica **15** (1995), 301 – 309.
- [4] E. Balandraud, *Un nouveau point de vue isopérimétrique appliqué au théorème de Kneser*, manuscript.
- [5] G. Bhowmik, I. Halupczok, and J.-C. Schlage-Puchta, *Inductive methods and zero-sum free sequences*, 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] J.D. Bovey, P. Erdős, and I. Niven, *Conditions for zero sum modulo  $n$* , Can. Math. Bull. **18** (1975), 27 – 29.
- [10] Y. Caro, *Zero-sum Ramsey numbers-stars*, Discrete Math. **104** (1992), 1 – 6.
- [11] ———, *Zero-sum problems - a survey*, Discrete Math. **152** (1996), 93 – 113.
- [12] S.T. Chapman (ed.), *Arithmetical Properties of Commutative Rings and Monoids*, Lect. Notes Pure Appl. Math., vol. 241, Chapman & Hall/CRC, 2005.

- [13] S.T. Chapman and J. Coykendall, *Factorization Problems in Integral Domains and Monoids*, Pure and Applied Mathematics, Chapman & Hall/CRC, to appear.
- [14] ———, *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*, manuscript.
- [26] Y. Edel, *A product construction for sequences in finite abelian groups of odd order without zero-sum subsequences of length  $\exp(G)$* , Des. Codes Cryptography, to appear.
- [27] 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.

- [28] C. Elsholtz, *Lower bounds for multidimensional zero sums*, *Combinatorica* **24** (2004), 351 – 358.
- [29] P. van Emde Boas, *A combinatorial problem on finite abelian groups II*, Reports ZW-1969-007, Math. Centre, Amsterdam, 1969.
- [30] P. van Emde Boas and D. Kruyswijk, *A combinatorial problem on finite abelian groups*, Reports ZW-1967-009, Math. Centre, Amsterdam, 1967.
- [31] P. Erdős, A. Ginzburg, and A. Ziv, *Theorem in the additive number theory*, *Bull. Research Council Israel* **10** (1961), 41 – 43.
- [32] B.W. Finklea, T. Moore, V. Ponomarenko, and Z.J. Turner, *On groups with excessive Davenport constant*, manuscript.
- [33] C. Flores and O. Ordaz, *On the Erdős-Ginzburg-Ziv theorem*, *Discrete Math.* **152** (1996), 321 – 324.
- [34] M. Freeze and A. Geroldinger, *Unions of sets of lengths*, *Funct. Approximatio, Comment. Math.*, to appear.
- [35] G.A. Freiman, *Foundations of a Structural Theory of Set Addition*, *Translations of Mathematical Monographs*, vol. 37, American Mathematical Society, 1973.
- [36] G.A. Freiman and A. Geroldinger, *An addition theorem and its arithmetical application*, *J. Number Theory* **85** (2000), 59 – 73.
- [37] W. Gao, *Addition theorems for finite abelian groups*, *J. Number Theory* **53** (1995), 241 – 246.
- [38] ———, *A combinatorial problem on finite abelian groups*, *J. Number Theory* **58** (1995), 100 – 103.
- [39] ———, *An addition theorem for finite cyclic groups*, *Discrete Math.* **163** (1997), 257 – 265.
- [40] ———, *On Davenport’s constant of finite abelian groups with rank three*, *Discrete Math.* **222** (2000), 111 – 124.
- [41] ———, *Two zero sum problems and multiple properties*, *J. Number Theory* **81** (2000), 254 – 265.
- [42] ———, *Zero sums in finite cyclic groups*, *Integers* **0** (2000), Paper A14, 9p.
- [43] W. Gao and A. Geroldinger, *On products of  $k$  atoms*, *Monatsh. Math.*, to appear.
- [44] ———, *On long minimal zero sequences in finite abelian groups*, *Period. Math. Hung.* **38** (1999), 179 – 211.

- [45] ———, *On the order of elements in long minimal zero-sum sequences*, Period. Math. Hung. **44** (2002), 63 – 73.
- [46] ———, *On zero-sum sequences in  $\mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$* , Integers **3** (2003), Paper A08, 45p.
- [47] ———, *Zero-sum problems in finite abelian groups: a survey*, Expo. Math. **24** (2006), 337 – 369.
- [48] ———, *On the number of subsequences with given sum of sequences over finite abelian  $p$ -groups*, Rocky Mt. J. Math. **37** (2007), 1541 – 1550.
- [49] 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.
- [50] W. Gao, A. Geroldinger, and W.A. Schmid, *Inverse zero-sum problems*, Acta Arith. **128** (2007), 245 – 279.
- [51] W. Gao, Q.H. Hou, W.A. Schmid, and R. Thangadurai, *On short zero-sum subsequences II*, Integers **7** (2007), Paper A21, 22p.
- [52] W. Gao and Y. Li, *Remarks on group rings and the Davenport constant*, Ars Comb., to appear.
- [53] 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.
- [54] W. Gao, R. Thangadurai, and J. Zhuang, *Addition theorems on the cyclic groups of order  $p^l$* , Discrete Math.
- [55] W. Gao and J. Zhuang, *Sequences not containing long zero-sum subsequences*, Eur. J. Comb. **27** (2006), 777 – 787.
- [56] A. Geroldinger, *Über nicht-eindeutige Zerlegungen in irreduzible Elemente*, Math. Z. **197** (1988), 505 – 529.
- [57] 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.
- [58] ———, *Non-Unique Factorizations. Algebraic, Combinatorial and Analytic Theory*, Pure and Applied Mathematics, vol. 278, Chapman & Hall/CRC, 2006.
- [59] A. Geroldinger and Y.ould Hamidoune, *Zero-sumfree sequences in cyclic groups and some arithmetical application*, J. Théor. Nombres Bordx. **14** (2002), 221 – 239.

- [60] A. Geroldinger and R. Schneider, *On Davenport's constant*, J. Comb. Theory, Ser. A **61** (1992), 147 – 152.
- [61] B. Girard, *A new upper bound for the cross number of finite abelian groups*, Isr. J. Math., to appear.
- [62] P.A. Grillet, *Commutative Semigroups*, Kluwer Academic Publishers, 2001.
- [63] D.J. Grynkiewicz, *A step beyond Kemperman's structure theorem*, manuscript.
- [64] ———, *On an extension of the Erdős-Ginzburg-Ziv Theorem to hypergraphs*, Eur. J. Comb. **26** (2005), 1154 – 1176.
- [65] ———, *Quasi-periodic decompositions and the Kemperman structure theorem*, Eur. J. Comb. **26** (2005), 559 – 575.
- [66] ———, *A weighted Erdős-Ginzburg-Ziv Theorem*, Combinatorica **26** (2006), 445 – 453.
- [67] D.J. Grynkiewicz, O. Ordaz, M.T. Varela, and F. Villarroel, *On Erdős-Ginzburg-Ziv inverse theorems*, Acta Arith. **129** (2007), 307 – 318.
- [68] F. Halter-Koch, *Non-unique factorizations of algebraic integers*, Funct. Approximatio, Comment. Math., to appear.
- [69] ———, *Ideal Systems. An Introduction to Multiplicative Ideal Theory*, Marcel Dekker, 1998.
- [70] Y.ould Hamidoune, *The global isoperimetric methodology applied to Kneser's theorem*, manuscript, –.
- [71] ———, *Hyper-atoms and the Kemperman's critical pair theory*, manuscript, –.
- [72] ———, *A weighted generalization of Gao's  $n + D - 1$  theorem*, manuscript, –.
- [73] Y.ould Hamidoune, O. Serra, and G. Zémor, *On some subgroup chains related to Kneser's theorem*, manuscript, –.
- [74] H. Harborth, *Ein Extremalproblem für Gitterpunkte*, J. Reine Angew. Math. **262** (1973), 356 – 360.
- [75] F. Hennecart, *La fonction de Brakemeier dans le problème d'Erdős-Ginzburg-Ziv*, Acta Arith. **117** (2005), 35 – 50.
- [76] S. Kubertin, *Nullsummen in  $\mathbb{Z}_p^d$* , Master's thesis, Technical University Clausthal, 2002.

- [77] G. Lettl and W.A. Schmid, *Minimal zero-sum sequences in  $C_n \oplus C_n$* , Eur. J. Comb. **28** (2007), 742 – 753.
- [78] G. Lettl and Zhi-Wei Sun, *On covers of abelian groups by cosets*, Acta Arith., to appear.
- [79] H.B. Mann, *Additive group theory - a progress report*, Bull. Am. Math. Soc. **79** (1973), 1069 – 1075.
- [80] ———, *Addition Theorems: The Addition Theorems of Group Theory and Number Theory*, R.E. Krieger, 1976.
- [81] 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.
- [82] C.P. Milies and S.K. Sehgal, *An Introduction to Group Rings*, Kluwer Academic Publishers, 2002.
- [83] M.B. Nathanson, *Additive Number Theory: Inverse Problems and the Geometry of Sumsets*, Springer, 1996.
- [84] J.E. Olson, *A combinatorial problem on finite abelian groups I*, J. Number Theory **1** (1969), 8 – 10.
- [85] 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.
- [86] ———, *On the maximal cardinality of half-factorial sets in cyclic groups*, Math. Ann. **333** (2005), 759 – 785.
- [87] C. Reiher, *On Kemnitz' conjecture concerning lattice points in the plane*, Ramanujan J. **13** (2007), 333 – 337.
- [88] K. Rogers, *A combinatorial problem in abelian groups*, Proc. Camb. Philos. Soc. **59** (1963), 559 – 562.
- [89] S. Savchev and F. Chen, *Long zero-free sequences in finite cyclic groups*, Discrete Math. **307** (2007), 2671 – 2679.
- [90] ———, *Minimal zero-sum sequences of maximum length in the group  $C_3 \oplus C_{3k}$* , Integers **7** (2007), Paper A42, 6p.
- [91] W.A. Schmid, *Characterization of class groups of Krull monoids via their systems of sets of lengths: a status report*, manuscript.
- [92] ———, *Characterization of elementary  $p$ -groups of rank two via the system of sets of lengths*, manuscript.

- [93] ———, *Inverse zero-sum problems II*, manuscript.
- [94] ———, *A realization theorem for sets of lengths*, manuscript.
- [95] ———, *Differences in sets of lengths of Krull monoids with finite class group*, J. Théor. Nombres Bordx. **17** (2005), 323 – 345.
- [96] ———, *Half-factorial sets in finite abelian groups: a survey*, Grazer Math. Ber. **348** (2005), 41 – 64.
- [97] W.A. Schmid and J.J. Zhuang, *On short zero-sum subsequences over  $p$ -groups*, Ars Comb., to appear.
- [98] Zhi-Wei Sun, *Zero-sum problems in abelian  $p$ -groups and covers of the integers by residue classes*, Isr. J. Math., to appear.
- [99] T. Tao and V.H. Vu, *Additive Combinatorics*, Cambridge University Press, 2006.
- [100] C. Wang, *Note on a variant of the Erdős-Ginzburg-Ziv Theorem*, Acta Arith. **108** (2003), 53 – 59.
- [101] P. Yuan, *On the index of minimal zero-sum sequences over finite cyclic groups*, J. Comb. Theory, Ser. A **114** (2007), 1545 – 1551.