



A characterization of class groups via sets of lengths

Alfred Geroldinger, Wolfgang Schmid

► To cite this version:

Alfred Geroldinger, Wolfgang Schmid. A characterization of class groups via sets of lengths. Journal of the Korean Mathematical Society, 2019, 56 (4), pp.869-915. 10.4134/JKMS.j180467. hal-01131955v3

HAL Id: hal-01131955

<https://hal.science/hal-01131955v3>

Submitted on 14 Mar 2019

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

A CHARACTERIZATION OF CLASS GROUPS VIA SETS OF LENGTHS

ALFRED GEROLDINGER AND WOLFGANG A. SCHMID

ABSTRACT. Let H be a Krull monoid with class group G such that every class contains a prime divisor. Then every nonunit $a \in H$ can be written as a finite product of irreducible elements. If $a = u_1 \cdot \dots \cdot u_k$, with irreducibles $u_1, \dots, u_k \in H$, then k is called the length of the factorization and the set $L(a)$ of all possible k is the set of lengths of a . It is well-known that the system $\mathcal{L}(H) = \{L(a) \mid a \in H\}$ depends only on the class group G . We study the inverse question asking whether the system $\mathcal{L}(H)$ is characteristic for the class group. Let H' be a further Krull monoid with class group G' such that every class contains a prime divisor and suppose that $\mathcal{L}(H) = \mathcal{L}(H')$. We show that, if one of the groups G and G' is finite and has rank at most two, then G and G' are isomorphic (apart from two well-known exceptions).

1. INTRODUCTION

Let H be a cancellative semigroup with unit element. If an element $a \in H$ can be written as a product of k irreducible elements, say $a = u_1 \cdot \dots \cdot u_k$, then k is called the length of the factorization. The set $L(a)$ of all possible factorization lengths is the set of lengths of a , and $\mathcal{L}(H) = \{L(a) \mid a \in H\}$ is called the system of sets of lengths of H . Clearly, if H is factorial, then $|L(a)| = 1$ for each $a \in H$. Suppose there is some $a \in H$ with $|L(a)| > 1$, say $k, l \in L(a)$ with $k < l$. Then, for every $m \in \mathbb{N}$, we observe that $L(a^m) \supset \{km + \nu(l - k) \mid \nu \in [0, m]\}$ which shows that sets of lengths can become arbitrarily large. Under mild conditions on the ideal theory of H every nonunit of H , has a factorization into irreducibles and all sets of lengths are finite.

Sets of lengths (together with parameters controlling their structure) are the most investigated invariants in factorization theory. They occur in settings ranging from numerical monoids, noetherian domains, monoids of ideals and of modules to maximal orders in central simple algebras (for recent progress see [4, 6, 12]). The focus of the present paper is on Krull monoids with finite class group such that every class contains a prime divisor. Rings of integers in algebraic number fields are such Krull monoids, and classical notions from algebraic number theory (dating back to the 19th century) state that the class group determines the arithmetic of the ring of integers. This idea has been formalized and justified. In the 1970s Narkiewicz posed the inverse question whether or not arithmetical phenomena (in other words, phenomena describing the non-uniqueness of factorizations) characterize the class group ([27, Problem 32; page 469]). Very quickly first affirmative answers were given by Halter-Koch, Kaczorowski, and Rush ([26, 23, 29]). Indeed, it is not too difficult to show that the system of sets of factorizations determines the class group ([15, Sections 7.1 and 7.2]).

These answers are not really satisfactory because the given characterizations are based on rather abstract arithmetical properties which play only little role in other parts of factorization theory. Since, on the other hand, sets of lengths are of central interest in factorization theory, it is natural to ask whether their structure is rich enough to do characterizations.

Let H be a commutative Krull monoid with finite class group G and suppose that every class contains a prime divisor (recall that an integral domain is a Krull domain if and only if its monoid of nonzero elements is a Krull monoid). It is classical that H is factorial if and only if $|G| = 1$, and by a result due

2010 *Mathematics Subject Classification.* 11B30, 11R27, 13A05, 13F05, 20M13.

Key words and phrases. Krull monoids, class groups, arithmetical characterizations, sets of lengths, zero-sum sequences.

This work was supported by the Austrian Science Fund FWF, Project Number P26036-N26, by the Austrian-French Amadée Program FR03/2012, and by the ANR Project Caesar, Project Number ANR-12-BS01-0011.

to Carlitz in 1960 we know that all sets of lengths are singletons (i.e., $|L| = 1$ for all $L \in \mathcal{L}(H)$) if and only if $|G| \leq 2$. Let us suppose now that $|G| \geq 3$. Then the monoid $\mathcal{B}(G)$ of zero-sum sequences over G is again a Krull monoid with class group isomorphic to G , every class contains a prime divisor, and $\mathcal{L}(H) = \mathcal{L}(\mathcal{B}(G))$ (as usual, we set $\mathcal{L}(G) = \mathcal{L}(\mathcal{B}(G))$). The Characterization Problem can be formulated as follows ([15, Section 7.3], [17, page 42], [33]).

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

The system of sets of lengths $\mathcal{L}(G)$ for finite abelian groups is studied with methods from Additive Combinatorics. Zero-sum theoretical invariants, such as the Davenport constant, play a central role. Recall that, although the precise value of the Davenport constant is well-known for p -groups and for groups of rank at most two (see Proposition 2.2), its precise value is unknown in general (even for groups of the form $G = C_n^3$). Thus it is not surprising that all answers to the Characterization Problem so far have been restricted to very special groups including cyclic groups, elementary 2-groups, and groups of the form $C_n \oplus C_n$ ([7, 32]). Apart from two well-known (trivial) pairings, the answer is always positive. Starting from $C_n \oplus C_n$, Zhong studied the Characterization Problem for groups of the form C_n^r in a series of papers ([21, 38, 37]). The goal of the present paper is to settle the Characterization Problem for groups of rank at most two. Here is our main result.

Theorem 1.1. *Let G be an abelian group such that $\mathcal{L}(G) = \mathcal{L}(C_{n_1} \oplus C_{n_2})$ where $n_1, n_2 \in \mathbb{N}$ with $n_1 \mid n_2$ and $n_1 + n_2 > 4$. Then $G \cong C_{n_1} \oplus C_{n_2}$.*

The difficulty of the Characterization Problem stems from the fact that most sets of lengths over any finite abelian group are arithmetical progressions with difference 1 (see Proposition 3.1.3, or [15, Theorem 9.4.11]). If G and G' are finite abelian groups with $G \subset G'$, then clearly $\mathcal{L}(G) \subset \mathcal{L}(G')$. Thus, in order to characterize a group G , we first have to find distinctive sets of lengths for G (i.e., sets of lengths which do occur in $\mathcal{L}(G)$, but in no other or only in a small number of further groups), and second we will have to show that certain sets are not sets of lengths in $\mathcal{L}(G)$. These distinctive sets of lengths for rank two groups are identified in Proposition 5.5 which is the core of our whole approach, and Proposition 4.1 provides sets which do not occur as sets of lengths for rank two groups. After gathering some background material in Section 2, we summarize key results on the structure of sets of lengths in Propositions 3.1, 3.2, and 3.3. Furthermore, we provide some explicit constructions which will turn out to be crucial (Propositions 3.4 – 3.7). After that, we are well-prepared for the main parts given in Sections 4 and 5.

2. THE ARITHMETIC OF KRULL MONOIDS: BACKGROUND

We gather the required tools from the algebraic and arithmetic theory of Krull monoids. Our notation and terminology are consistent with the monographs [15, 17, 22]. Let $\mathbb{N}$ denote the set of positive integers, $\mathbb{P} \subset \mathbb{N}$ the set of prime numbers and put $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$. For real numbers $a, b \in \mathbb{R}$, we set $[a, b] = \{x \in \mathbb{Z} \mid a \leq x \leq b\}$. Let $A, B \subset \mathbb{Z}$ be subsets of the integers. We denote by $A + B = \{a + b \mid a \in A, b \in B\}$ their *sumset*, and by $\Delta(A)$ the *set of (successive) distances* of A (that is, $d \in \Delta(A)$ if and only if $d = b - a$ with $a, b \in A$ distinct and $[a, b] \cap A = \{a, b\}$). For $k \in \mathbb{N}$, we denote by $k \cdot A = \{ka \mid a \in A\}$ the *dilation* of A by k . If $A \subset \mathbb{N}$, then the *elasticity* of A is defined as

$$\rho(A) = \sup \left\{ \frac{m}{n} \mid m, n \in A \right\} = \frac{\sup A}{\min A} \in \mathbb{Q}_{\geq 1} \cup \{\infty\} \text{ and we set } \rho(\{0\}) = 1.$$

Monoids and Factorizations. By a *monoid*, we 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). The multiplicative semigroup of non-zero elements of an integral domain is a monoid. Let H be a monoid. We denote by $H^\times$ the set of invertible elements of H , by $\mathcal{A}(H)$ the set of atoms (irreducible elements) of H , and by $H_{\text{red}} = H/H^\times = \{aH^\times \mid a \in H\}$ the associated reduced monoid of H . A monoid F is free abelian, with basis $P \subset F$, and we write $F = \mathcal{F}(P)$ if every $a \in F$ has a unique representation of the form

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

and we call

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

The monoid $Z(H) = \mathcal{F}(\mathcal{A}(H_{\text{red}}))$ is called the *factorization monoid* of H , and the homomorphism $\pi: Z(H) \rightarrow H_{\text{red}}$, defined by $\pi(u) = u$ for each $u \in \mathcal{A}(H_{\text{red}})$ is the *factorization homomorphism* of H . For $a \in H$,

$$Z_H(a) = Z(a) = \pi^{-1}(aH^\times) \subset Z(H) \quad \text{is the set of factorizations of } a, \quad \text{and}$$

$$L_H(a) = L(a) = \{|z| \mid z \in Z(a)\} \subset \mathbb{N}_0 \quad \text{is the set of lengths of } a.$$

Thus H is factorial if and only if H_{red} is free abelian (equivalently, $|Z(a)| = 1$ for all $a \in H$). The monoid H is called *atomic* if $Z(a) \neq \emptyset$ for all $a \in H$ (equivalently, every nonunit can be written as a finite product of irreducible elements). For the remainder of this work, we suppose that H is atomic. Note that, $L(a) = \{0\}$ if and only if $a \in H^\times$, and $L(a) = \{1\}$ if and only if $a \in \mathcal{A}(H)$. We denote by

$$\mathcal{L}(H) = \{L(a) \mid a \in H\} \quad \text{the system of sets of lengths of } H, \quad \text{and by}$$

$$\Delta(H) = \bigcup_{L \in \mathcal{L}(H)} \Delta(L) \subset \mathbb{N} \quad \text{the set of distances of } H.$$

For $k \in \mathbb{N}$, we set $\rho_k(H) = k$ if $H = H^\times$, and

$$\rho_k(H) = \sup\{\sup L \mid L \in \mathcal{L}(H), k \in L\} \in \mathbb{N} \cup \{\infty\}, \quad \text{if } H \neq H^\times.$$

Then

$$\rho(H) = \sup\{\rho(L) \mid L \in \mathcal{L}(H)\} = \lim_{k \rightarrow \infty} \frac{\rho_k(H)}{k} \in \mathbb{R}_{\geq 1} \cup \{\infty\}$$

is the *elasticity* of H . The monoid H is said to be

- *half-factorial* if $\Delta(H) = \emptyset$. If H is not half-factorial, then $\min \Delta(H) = \gcd \Delta(H)$.
- *decomposable* if there exist submonoids H_1, H_2 with $H_i \not\subset H^\times$ for $i \in [1, 2]$ such that $H = H_1 \times H_2$ (otherwise H is called *indecomposable*).

For a free abelian monoid $\mathcal{F}(P)$, we introduce a distance function $d: \mathcal{F}(P) \times \mathcal{F}(P) \rightarrow \mathbb{N}_0$, by setting

$$d(a, b) = \max \left\{ \left\lfloor \frac{a}{\gcd(a, b)} \right\rfloor, \left\lfloor \frac{b}{\gcd(a, b)} \right\rfloor \right\} \in \mathbb{N}_0 \quad \text{for } a, b \in \mathcal{F}(P),$$

and we note that $d(a, b) = 0$ if and only if $a = b$. For a subset $\Omega \subset \mathcal{F}(P)$, we define the *catenary degree* $c(\Omega)$ as the smallest $N \in \mathbb{N}_0 \cup \{\infty\}$ with the following property: for each $a, b \in \Omega$, there are elements $a_0, \dots, a_k \in \Omega$ such that $a = a_0, a_k = b$, and $d(a_{i-1}, a_i) \leq N$ for all $i \in [1, k]$. Note that $c(\Omega) = 0$ if and only if $|\Omega| \leq 1$. For an element $a \in H$, we call $c_H(a) = c(a) = c(Z_H(a))$ the *catenary degree* of a , and $c(H) = \sup\{c(a) \mid a \in H\} \in \mathbb{N}_0 \cup \{\infty\}$ is the *catenary degree* of H . The monoid H is factorial if and only if $c(H) = 0$, and if H is not factorial, then $2 + \sup \Delta(H) \leq c(H)$ ([15, Theorem 1.6.3]).

Krull monoids. A monoid H is *Krull* if it is completely integrally closed and satisfies the ascending chain condition on divisorial ideals. An integral domain R is a Krull domain if and only if its multiplicative monoid $R \setminus \{0\}$ is a Krull monoid, and this generalizes to Marot rings ([16]). The theory of Krull monoids is presented in detail in [25, 15], and for a survey we refer to [12].

Much of the arithmetic of a Krull monoid can be seen in an associated monoid of zero-sum sequences. This is a Krull monoid again which can be studied with methods from Additive Combinatorics. To introduce the necessary concepts, let G be an additively written abelian group, $G_0 \subset G$ a subset, and let $\mathcal{F}(G_0)$ be the free abelian monoid with basis G_0 . In Additive Combinatorics, the elements of $\mathcal{F}(G_0)$ are called *sequences* over G_0 . If $S = g_1 \cdot \dots \cdot g_l \in \mathcal{F}(G_0)$, where $l \in \mathbb{N}_0$ and $g_1, \dots, g_l \in G_0$, then $\sigma(S) = g_1 + \dots + g_l$ is called the *sum* of S , and the monoid

$$\mathcal{B}(G_0) = \{S \in \mathcal{F}(G_0) \mid \sigma(S) = 0\} \subset \mathcal{F}(G_0)$$

is called the *monoid of zero-sum sequences* over G_0 (these objects are also referred to in the literature as block monoids). The embedding $\mathcal{B}(G_0) \hookrightarrow \mathcal{F}(G_0)$ is a divisor homomorphism and $\mathcal{B}(G_0)$ is a Krull monoid. The monoid $\mathcal{B}(G)$ is factorial if and only if $|G| \leq 2$. If $|G| \neq 2$, then $\mathcal{B}(G)$ is a Krull monoid with class group isomorphic to G and every class contains precisely one prime divisor. For every arithmetical invariant $*(H)$ defined for a monoid H , it is usual to write $*(G_0)$ instead of $*(\mathcal{B}(G_0))$. In particular, we set $\mathcal{A}(G_0) = \mathcal{A}(\mathcal{B}(G_0))$ and $\mathcal{L}(G_0) = \mathcal{L}(\mathcal{B}(G_0))$. Similarly, arithmetical properties of $\mathcal{B}(G_0)$ are attributed to G_0 . Thus, G_0 is said to be

- (in)decomposable if $\mathcal{B}(G_0)$ is (in)decomposable,
- (non-) half-factorial if $\mathcal{B}(G_0)$ is (non-)half-factorial.

Proposition 2.1. *Let H be a Krull monoid with class group G , and suppose that each class contains a prime divisor. Then there is a transfer homomorphism $\beta: H \rightarrow \mathcal{B}(G)$ such that the following hold.*

1. $\mathsf{L}_H(a) = \mathsf{L}_{\mathcal{B}(G)}(\beta(a))$ for each $a \in H$ and $\mathcal{L}(H) = \mathcal{L}(G)$.
2. If $|G| \geq 3$, then $\mathsf{c}(H) = \mathsf{c}(\mathcal{B}(G))$.

Proof. See [15, Section 3.4]. □

The above result generalizes to *transfer Krull monoids* H over abelian groups G , which also satisfy the relationship $\mathcal{L}(H) = \mathcal{L}(G)$. Hence all characterization results, such as Theorem 1.1, also apply to them ([12]).

Zero-Sum Theory. Let G be an additive abelian group, $G_0 \subset G$ a subset, and $G_0^\bullet = G_0 \setminus \{0\}$. Then $[G_0] \subset G$ denotes the subsemigroup and $\langle G_0 \rangle \subset G$ the subgroup generated by G_0 . For a sequence

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

we set $\varphi(S) = \varphi(g_1) \cdot \dots \cdot \varphi(g_l)$ for any homomorphism $\varphi: G \rightarrow G'$, and in particular, we have $-S = (-g_1) \cdot \dots \cdot (-g_l)$. We call

$\text{supp}(S) = \{g \in G \mid \mathsf{v}_g(S) > 0\} \subset G$ the *support* of S , $\mathsf{v}_g(S)$ the *multiplicity* of g in S ,

$$|S| = l = \sum_{g \in G} \mathsf{v}_g(S) \in \mathbb{N}_0 \text{ the length of } S, \text{ and } \mathsf{k}(S) = \sum_{g \in G} \frac{1}{\text{ord}(g)} \in \mathbb{Q} \text{ the cross number of } S.$$

Moreover, $\Sigma(S) = \left\{ \sum_{i \in I} g_i \mid \emptyset \neq I \subset [1, l] \right\}$ is the *set of subsequence sums* of S . The sequence S is said to be

- *zero-sum free* if $0 \notin \Sigma(S)$,
- a *zero-sum sequence* if $\sigma(S) = 0$,
- a *minimal zero-sum sequence* if it is a nontrivial zero-sum sequence and every proper subsequence is zero-sum free.

Both Davenport constants, namely

- the (small) *Davenport constant* $\mathsf{d}(G_0) = \sup\{|S| \mid S \in \mathcal{F}(G_0) \text{ is zero-sum free}\} \in \mathbb{N}_0 \cup \{\infty\}$ and
- the (large) *Davenport constant* $\mathsf{D}(G_0) = \sup\{|U| \mid U \in \mathcal{A}(G_0)\} \in \mathbb{N}_0 \cup \{\infty\}$

are classical invariants in zero-sum theory. For $n \in \mathbb{N}$, let C_n denote a cyclic group with n elements. Suppose that G is finite. A tuple $(e_i)_{i \in I}$ is called a *basis* of G if all elements are nonzero and $G = \oplus_{i \in I} \langle e_i \rangle$. For $p \in \mathbb{P}$, let $\mathsf{r}_p(G)$ denote the p -rank of G , $\mathsf{r}(G) = \max\{\mathsf{r}_p(G) \mid p \in \mathbb{P}\}$ denote the *rank* of G , and let $\mathsf{r}^*(G) = \sum_{p \in \mathbb{P}} \mathsf{r}_p(G)$ be the *total rank* of G . If $|G| > 1$, then $G \cong C_{n_1} \oplus \dots \oplus C_{n_r}$, and we set $\mathsf{d}^*(G) = \sum_{i=1}^r (n_i - 1)$, where $r, n_1, \dots, n_r \in \mathbb{N}$ with $1 < n_1 \mid \dots \mid n_r$, $r = \mathsf{r}(G)$, and $n_r = \exp(G)$ is the exponent of G . If $|G| = 1$, then $\mathsf{r}(G) = \mathsf{r}^*(G) = 0$, $\exp(G) = 1$, and $\mathsf{d}^*(G) = 0$. We will use the following well-known results (see [15, Chapter 5]).

Proposition 2.2. *Let G be a finite abelian group. Then $1 + \mathsf{d}^*(G) \leq 1 + \mathsf{d}(G) = \mathsf{D}(G) \leq |G|$. If G is a p -group or $\mathsf{r}(G) \leq 2$, then $\mathsf{d}(G) = \mathsf{d}^*(G)$.*

We will make substantial use of the following result (see [15, Theorem 6.4.7] and [19, Theorem 1.1]).

Proposition 2.3. *Let H be a Krull monoid with finite class group G where $|G| \geq 3$ and every class contains a prime divisor. Then $\mathbf{c}(H) \in [3, \mathbf{D}(G)]$, and we have*

1. $\mathbf{c}(H) = \mathbf{D}(G)$ if and only if G is either cyclic or an elementary 2-group.
2. $\mathbf{c}(H) = \mathbf{D}(G) - 1$ if and only if G is isomorphic either to $C_2^{r-1} \oplus C_4$ for some $r \geq 2$ or to $C_2 \oplus C_{2n}$ for some $n \geq 2$.

Let $A \in \mathcal{B}(G_0)$ and $d = \min\{|U| \mid U \in \mathcal{A}(G_0)\}$. If $A = BC$ with $B, C \in \mathcal{B}(G_0)$, then

$$\mathbf{L}(B) + \mathbf{L}(C) \subset \mathbf{L}(A).$$

If $A = U_1 \cdots U_k = V_1 \cdots V_l$ with $U_1, \dots, U_k, V_1, \dots, V_l \in \mathcal{A}(G_0)$ and $k < l$, then

$$ld \leq \sum_{\nu=1}^l |V_\nu| = |A| = \sum_{\nu=1}^k |U_\nu| \leq k\mathbf{D}(G_0), \text{ whence } \frac{|A|}{\mathbf{D}(G_0)} \leq \min \mathbf{L}(A) \leq \max \mathbf{L}(A) \leq \frac{|A|}{d}.$$

We need the concept of relative block monoids (as introduced by Halter-Koch in [24], and recently studied by Baeth et al. in [3]). Let G be an abelian group. For a subgroup $K \subset G$ let

$$\mathcal{B}_K(G) = \{S \in \mathcal{F}(G) \mid \sigma(S) \in K\} \subset \mathcal{F}(G),$$

and let $\mathbf{D}_K(G)$ denote the smallest $l \in \mathbb{N} \cup \{\infty\}$ with the following property:

- Every sequence $S \in \mathcal{F}(G)$ of length $|S| \geq l$ has a subsequence T with $\sigma(T) \in K$.

Clearly, $\mathcal{B}_K(G) \subset \mathcal{F}(G)$ is a submonoid with

$$\mathcal{B}(G) = \mathcal{B}_{\{0\}}(G) \subset \mathcal{B}_K(G) \subset \mathcal{B}_G(G) = \mathcal{F}(G)$$

and $\mathbf{D}_{\{0\}}(G) = \mathbf{D}(G)$. The following result is well-known ([3, Theorem 2.2]). Since there seems to be no proof in the literature and we make substantial use of it, we provide the simple arguments.

Proposition 2.4. *Let G be an abelian group and $K \subset G$ a subgroup.*

1. $\mathcal{B}_K(G)$ is a Krull monoid. If $|G| = 2$ and $K = \{0\}$, then $\mathcal{B}_K(G) = \mathcal{B}(G)$ is factorial. In all other cases the embedding $\mathcal{B}_K(G) \hookrightarrow \mathcal{F}(G)$ is a divisor theory with class group isomorphic to G/K and every class contains precisely $|K|$ prime divisors.
2. The monoid homomorphism $\theta: \mathcal{B}_K(G) \rightarrow \mathcal{B}(G/K)$, defined by $\theta(g_1 \cdots g_l) = (g_1 + K) \cdots (g_l + K)$ is a transfer homomorphism. If $|G/K| \geq 3$, then $\mathbf{c}(\mathcal{B}_K(G)) = \mathbf{c}(\mathcal{B}(G/K))$.
3. $\mathbf{D}_K(G) = \sup\{|U| \mid U \text{ is an atom of } \mathcal{B}_K(G)\} = \mathbf{D}(G/K)$.

Proof. 1. If $|G| = 1$, then $\mathcal{B}(G) = \mathcal{F}(G)$ is factorial, the class group is trivial, and there is precisely one prime divisor. If $|G| = |K| = 2$, then $\mathcal{B}_K(G) = \mathcal{F}(G)$ is factorial, the class group is trivial, and there are precisely two prime divisors. If $|G| = 2$ and $|K| = 1$, then $\mathcal{B}_K(G) = \mathcal{B}(G)$ is factorial, and hence a Krull monoid with trivial class group. Suppose that $|G| \geq 3$. Clearly, the embedding $\mathcal{B}_K(G) \hookrightarrow \mathcal{F}(G)$ is a divisor homomorphism. To verify that it is a divisor theory, let $g \in G$ be given. If $\text{ord}(g) = n \geq 3$, then $g = \gcd(g^n, g(-g))$. If $\text{ord}(g) = 2$, then there is an element $h \in G \setminus \{0, g\}$ and $g = \gcd(g^2, gh(g-h))$. If $\text{ord}(g) = \infty$, then $g = \gcd((-g)g, g(2g)(-3g))$.

The map $\varphi: \mathcal{F}(G) \rightarrow G/K$, defined by $\varphi(S) = \sigma(S) + K$ for every $S \in \mathcal{F}(G)$, is a monoid epimorphism. If $S, S' \in \mathcal{F}(G)$, then $\sigma(S) + K = \sigma(S') + K$ if and only if $S' \in [S] = S\mathbf{q}(\mathcal{B}_K(G))$. Thus φ induces a group isomorphism $\Phi: \mathbf{q}(\mathcal{F}(G))/\mathbf{q}(\mathcal{B}_K(G)) \rightarrow G/K$, defined by $\Phi([S]) = \sigma(S) + K$, and we have $[S] \cap G = \sigma(S) + K$. Thus the class $[S]$ contains precisely $|K|$ prime divisors.

2. This follows from 1., from Proposition 2.1, and from the reference given there.

3. Since a sequence $S \in \mathcal{F}(G)$ is an atom of $\mathcal{B}_K(G)$ if and only if $S \neq 1$, $\sigma(S) \in K$ and $\sigma(T) \notin K$ for all proper subsequences T of S , it follows that $\mathbf{D}_K(G) = \sup\{|U| \mid U \text{ is an atom of } \mathcal{B}_K(G)\}$. Since θ is a transfer homomorphism, we get $\theta(\mathcal{A}(\mathcal{B}_K(G))) = \mathcal{A}(G/K)$ and $\theta^{-1}(\mathcal{A}(G/K)) = \mathcal{A}(\mathcal{B}_K(G))$. Therefore $|U| = |\theta(U)|$ for all $U \in \mathcal{B}_K(G)$, and it follows that

$$\sup\{|U| \mid U \in \mathcal{A}(\mathcal{B}_K(G))\} = \sup\{|V| \mid V \in \mathcal{A}(G/K)\} = \mathbf{D}(G/K). \quad \square$$

3. STRUCTURAL RESULTS ON $\mathcal{L}(G)$ AND FIRST BASIC CONSTRUCTIONS

Let G be an abelian group. If G is infinite, then every finite subset $L \subset \mathbb{N}_{\geq 2}$ is contained in $\mathcal{L}(G)$ ([15, Theorem 7.4.1]). If G is finite, then sets of lengths have a well-studied structure. In order to describe it, we recall the concept of an AAMP. 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 *almost arithmetical multiprogression* (AAMP for short) with *difference* d , *period* $\mathcal{D}$, *length* l and *bound* M , if

$$(3.1) \quad L = y + (L' \cup L^* \cup L'') \subset y + \mathcal{D} + d\mathbb{Z}$$

where $\min L^* = 0$, L^* is an interval of $\mathcal{D} + d\mathbb{Z}$ (this means that L^* is finite nonempty and $L^* = (\mathcal{D} + d\mathbb{Z}) \cap [0, \max L^*]$), l is maximal such that $ld \in L^*$, $L' \subset [-M, -1]$, $L'' \subset \max L^* + [1, M]$ and $y \in \mathbb{Z}$. The set of minimal distances $\Delta^*(G) \subset \Delta(G)$ is defined as

$$\Delta^*(G) = \{\min \Delta(G_0) \mid G_0 \subset G \text{ with } \Delta(G_0) \neq \emptyset\} \subset \Delta(G).$$

Proposition 3.1 (Structural results on $\mathcal{L}(G)$). *Let G be a finite abelian group with $|G| \geq 3$.*

1. *There exists some $M \in \mathbb{N}_0$ such that every set of lengths $L \in \mathcal{L}(G)$ is an AAMP with some difference $d \in \Delta^*(G)$ and bound M .*
2. *For every $M \in \mathbb{N}_0$ and every finite nonempty set $\Delta^* \subset \mathbb{N}$, there is a finite abelian group G^* such that for every AAMP L with difference $d \in \Delta^*$ and bound M there is a $y_L \in \mathbb{N}$ with*

$$y + L \in \mathcal{L}(G^*) \quad \text{for all} \quad y \geq y_L.$$

3. *If $A \in \mathcal{B}(G)$ such that $\text{supp}(A) \cup \{0\}$ is a subgroup of G , then $\mathbf{L}(A)$ is an arithmetical progression with difference 1.*

Proof. We refer to [15, Theorems 4.4.11 and 7.6.8]) and to [34]. □

Proposition 3.2 (Structural results on $\Delta(G)$ and on $\Delta^*(G)$).

Let $G = C_{n_1} \oplus \dots \oplus C_{n_r}$ where $r, n_1, \dots, n_r \in \mathbb{N}$ with $r = r(G)$, $1 < n_1 \mid \dots \mid n_r$, and $|G| \geq 3$.

1. *$\Delta(G)$ is an interval with*

$$[1, \max\{\exp(G) - 2, k - 1\}] \subset \Delta(G) \subset [1, D(G) - 2] \quad \text{where} \quad k = \sum_{i=1}^{r(G)} \left\lfloor \frac{n_i}{2} \right\rfloor.$$

2. *$1 \in \Delta^*(G) \subset \Delta(G)$, $[1, r(G) - 1] \subset \Delta^*(G)$, and $\max \Delta^*(G) = \max\{\exp(G) - 2, r(G) - 1\}$.*
3. *If G is cyclic of order $|G| = n \geq 4$, then $\max(\Delta^*(G) \setminus \{n - 2\}) = \lfloor \frac{n}{2} \rfloor - 1$.*

Proof. We refer to [15, Section 6.8], to [18], and to [20]. □

Proposition 3.3 (Results on $\rho_k(G)$ and on $\rho(G)$).

Let G be a finite abelian group with $|G| \geq 3$, and let $k \in \mathbb{N}$.

1. *$\rho(G) = D(G)/2$ and $\rho_{2k}(G) = kD(G)$.*
2. *$1 + kD(G) \leq \rho_{2k+1}(G) \leq kD(G) + D(G)/2$. If G is cyclic, then equality holds on the left side.*

Proof. We refer to [15, Chapter 6.3], [11, Theorem 5.3.1], and to [14] for recent progress. □

In the next propositions we provide examples of sets of lengths over cyclic groups, over groups of rank two, and over groups of the form $C_2^{r-1} \oplus C_n$ with $r, n \in \mathbb{N}_{\geq 2}$. All examples will have difference $d = \max \Delta^*(G)$ and period $\mathcal{D}$ with $\{0, d\} \subset \mathcal{D} \subset [0, d]$ and $|\mathcal{D}| = 3$, and we write them down in a form used in Equation (3.1) in order to highlight their periods. It will be crucial for our approach (see Proposition 5.5) that the sets given in Proposition 3.4.2 do not occur over cyclic groups (Proposition 3.5). It is well-known that sets of lengths over cyclic groups and over elementary 2-groups have many features in common, and this carries over to rank two groups and groups of the form $C_2^{r-1} \oplus C_n$ (see Propositions 3.4.2, 3.6.2, and 5.5). For a set $L \in \mathcal{L}(G)$ there is a $B \in \mathcal{B}(G)$ such that $L = \mathbf{L}(B)$ and hence $m + L = \mathbf{L}(0^m B) \in \mathcal{L}(G)$ for all $m \in \mathbb{N}_0$. Therefore the interesting sets of lengths $L \in \mathcal{L}(G)$ are

those which do not stem from such a shift. These are those sets $L \in \mathcal{L}(G)$ with $-m + L \notin \mathcal{L}(G)$ for every $m \in \mathbb{N}$.

Proposition 3.4. *Let $G = C_{n_1} \oplus C_{n_2}$ where $n_1, n_2 \in \mathbb{N}$ with $2 < n_1 \mid n_2$, and let $d \in [3, n_1]$.*

1. *For each $k \in \mathbb{N}$, we have*

$$(2k+2) + \{0, d-2, n_2-2\} + \{\nu(n_2-2) \mid \nu \in [0, k-1]\} \cup \{(kn+2) + (d-2)\} = \\ (2k+2) + \{0, d-2\} + \{\nu(n_2-2) \mid \nu \in [0, k]\} \in \mathcal{L}(G).$$

2. *For each $k \in \mathbb{N}$, we have*

$$\left((2k+3) + \{0, n_1-2, n_2-2\} + \{\nu(n_2-2) \mid \nu \in [0, k]\} \right) \cup \left\{ (kn_2+3) + (n_1-2) + (n_2-2) \right\} \in \mathcal{L}(G).$$

Proof. Let (e_1, e_2) be a basis of G with $\text{ord}(e_i) = n_i$ for $i \in [1, 2]$, and let $k \in \mathbb{N}$. For $i \in [1, 2]$, we set $U_i = e_i^{n_i}$ and $V_i = (-e_i)e_i$. Then

$$(-U_i)^k U_i^k = (-U_i)^{k-\nu} U_i^{k-\nu} V_i^{\nu n_i} \quad \text{for all } \nu \in [0, k],$$

and hence

$$\mathsf{L}((-U_i)^k U_i^k) = 2k + \{\nu(n_i-2) \mid \nu \in [0, k]\}.$$

1. We set $h = (d-1)e_1$, $W_1 = (-e_1)^{d-1}h$, and $W_2 = e_1^{n_1-(d-1)}h$. Then $Z(U_1 W_1) = \{U_1 W_1, V_1^{d-1} W_2\}$ and $\mathsf{L}(U_1 W_1) = \{2, d\}$. Therefore

$$\begin{aligned} \mathsf{L}((-U_2)^k U_2^k U_1 W_1) &= \mathsf{L}((-U_2)^k U_2^k) + \mathsf{L}(U_1 W_1) \\ &= \{2k + \nu(n_2-2) \mid \nu \in [0, k]\} + \{2, d\} \\ &= (2k+2) + \{\nu(n_2-2) \mid \nu \in [0, k]\} + \{0, d-2\}. \end{aligned}$$

2. We define

$$W_1 = e_1^{n_1-1} e_2^{n_2-1} (e_1 + e_2), \quad W_2 = (-e_1) e_2^{n_2-1} (e_1 + e_2), \quad W_3 = e_1^{n_1-1} (-e_2) (e_1 + e_2), \quad W_4 = (-e_1) (-e_2) (e_1 + e_2), \\ \text{and} \quad B_k = W_1 (-U_1) (-U_2) U_2^k (-U_2)^k.$$

Then any factorization of B_k is divisible by precisely one of $W_1, \dots, W_4$, and we obtain that

$$\begin{aligned} B_k &= W_1 (-U_1) (-U_2) U_2^k (-U_2)^k = W_2 V_1^{n_1-1} (-U_2) U_2^k (-U_2)^k \\ &= W_3 (-U_1) V_2^{n_2-1} U_2^k (-U_2)^k = W_4 V_1^{n_1-1} V_2^{n_2-1} U_2^k (-U_2)^k. \end{aligned}$$

Thus it follows that

$$\begin{aligned} \mathsf{L}(B_k) &= \{3, n_1+1, n_2+1, n_1+n_2-1\} + \mathsf{L}(U_2^k (-U_2)^k) \\ &= (2k+3) + \{\nu(n_2-2) \mid \nu \in [0, k]\} \cup \\ &\quad (2k+3) + (n_1-2) + \{\nu(n_2-2) \mid \nu \in [0, k]\} \cup \\ &\quad (2k+3) + (n_2-2) + \{\nu(n_2-2) \mid \nu \in [0, k]\} \cup \\ &\quad (2k+3) + (n_1-2) + (n_2-2) + \{\nu(n_2-2) \mid \nu \in [0, k]\}. \end{aligned}$$

Thus $\max \mathsf{L}(B_k) = (kn_2+3) + (n_1-2) + (n_2-2)$ and

$$\mathsf{L}(B_k) = \left((2k+3) + \{0, n_1-2, n_2-2\} + \{\nu(n_2-2) \mid \nu \in [0, k]\} \right) \cup \{\max \mathsf{L}(B_k)\}. \quad \square$$

Proposition 3.5. *Let G be a cyclic group of order $|G| = n \geq 4$, and let $d \in [3, n-1]$.*

1. *For each $k \in \mathbb{N}_0$, we have*

$$(2k+2) + \{0, d-2\} + \{\nu(n-2) \mid \nu \in [0, k]\} \in \mathcal{L}(G).$$

2. For each $k \in \mathbb{N}_0$, we set

$$L_k = \left((2k+3) + \{0, d-2, n-2\} + \{\nu(n-2) \mid \nu \in [0, k]\} \right) \cup \left\{ (kn+3) + (d-2) + (n-2) \right\}.$$

Then for each $k \in \mathbb{N}_0$ and each $m \in \mathbb{N}_0$, we have $-m + L_k \notin \mathcal{L}(G)$.

Proof. Let $k \in \mathbb{N}_0$.

1. Let $g \in G$ with $\text{ord}(g) = n$, $U = g^n$, $V = (-g)g$, $W_1 = ((d-1)g)(-g)^{d-1}$, $W_2 = ((d-1)g)g^{n-(d-1)}$, and $B_k = ((-U)U)^k U W_1$. Then $Z(UW_1) = \{UW_1, W_2V^{d-1}\}$ and $L(UW_1) = \{2, d\}$. Since every factorization of B_k is divisible either by W_1 or by W_2 , it follows that

$$\begin{aligned} L(B_k) &= L((-U)^k U^k) + L(UW_1) = \{2k + \nu(n-2) \mid \nu \in [0, k]\} + \{2, d\} \\ &= (2k+2) + \{\nu(n-2) \mid \nu \in [0, k]\} + \{0, d-2\}. \end{aligned}$$

2. Note that $\max L_k = (kn+3) + (d-2) + (n-2) = (k+1)n + (d-1)$. Assume to the contrary that there is a $B_k \in \mathcal{B}(G)$ such that $L(B_k) = L_k$. Then $\min L(B_k) = 2k+3$ and, by Proposition 3.3,

$$(k+1)n + (d-1) = \max L(B_k) \leq \rho_{2k+3}(G) = (k+1)n + 1,$$

a contradiction. If $m \in \mathbb{N}_0$ and $B_{m,k} \in \mathcal{B}(G)$ such that $L(B_{m,k}) = -m + L_k$, then $L(0^m B_{m,k}) = L_k \in \mathcal{L}(G)$. Thus $-m + L_k \notin \mathcal{L}(G)$ for any $m \in \mathbb{N}_0$. $\square$

Proposition 3.6. Let $G = C_2^{r-1} \oplus C_n$ where $r, n \in \mathbb{N}_{\geq 2}$ and n is even.

1. For each $k \in \mathbb{N}_0$, we have

$$L_k = (2k+2) + \{0, n-2, n+r-3\} + \{\nu(n-2) \mid \nu \in [0, k]\} \in \mathcal{L}(G) \quad \text{yet} \quad L_k \notin \mathcal{L}(C_n).$$

2. For each $k \in \mathbb{N}_0$, we have

$$\left((2k+3) + \{0, r-1, n-2\} + \{\nu(n-2) \mid \nu \in [0, k]\} \right) \cup \left\{ (kn+3) + (r-1) + (n-2) \right\} \in \mathcal{L}(G).$$

Proof. Let $k \in \mathbb{N}_0$, $(e_1, \dots, e_{r-1}, e_r)$ be a basis of G with $\text{ord}(e_1) = \dots = \text{ord}(e_{r-1}) = 2$ and $\text{ord}(e_r) = n$. We set $e_0 = e_1 + \dots + e_{r-1}$, $U_i = e_i^{\text{ord}(e_i)}$ for each $i \in [1, r]$, $U_0 = (e_0 + e_r)(e_0 - e_r)$, $V_r = (-e_r)e_r$,

$$V = e_1 \cdot \dots \cdot e_{r-1}(e_0 + e_r)(-e_r), \quad \text{and} \quad W = e_1 \cdot \dots \cdot e_{r-1}(e_0 + e_r)e_r^{n-1}.$$

1. Obviously, $L((-W)W) = \{2, n, n+r-1\}$ and

$$\begin{aligned} L((-W)W(-U_r)^k U_r^k) &= L((-W)W) + L((-U_r)^k U_r^k) \\ &= \{2, n, n+r-1\} + \{2k + \nu(n-2) \mid \nu \in [0, k]\} \\ &= (2k+2) + \{0, n-2, n+r-3\} + \{\nu(n-2) \mid \nu \in [0, k]\} \end{aligned}$$

Since $\min L_k = 2k+2$, $\max L_k = (k+1)n + r-1$, and $\rho_{2k+2}(C_n) = (k+1)n$ by Proposition 3.3, $r \geq 2$ implies that $L_k \notin \mathcal{L}(C_n)$.

2. Let L_k denote the set in the statement. We define

$$B_k = U_0 U_1 \cdot \dots \cdot U_{r-1} (-U_r)^{k+1} U_r^{k+1}$$

and assert that $L(B_k) = L_k$. Let z be a factorization of B_k . We distinguish two cases.

CASE 1: $U_1 \mid z$.

Then $U_0 U_1 \cdot \dots \cdot U_{r-1} \mid z$ which implies that $z = U_0 U_1 \cdot \dots \cdot U_{r-1} ((-U_r)U_r)^{k+1-\nu} V_r^{\nu n}$ for some $\nu \in [0, k+1]$ and hence $|z| \in r + (2k+2) + \{\nu(n-2) \mid \nu \in [0, k+1]\}$.

CASE 2: $U_1 \nmid z$.

Then either $V \mid z$ or $W \mid z$. If $V \mid z$, then $z = (-V) V V_r^{n-1} ((-U_r)U_r)^{k-\nu} V_r^{\nu n}$ for some $\nu \in [0, k]$ and hence $|z| \in (n+1) + 2k + \{\nu(n-2) \mid \nu \in [0, k]\}$. If $W \mid z$, then $z = (-W) W V_r ((-U_r)U_r)^{k-\nu} V_r^{\nu n}$ for some $\nu \in [0, k]$ and hence $|z| \in 3 + 2k + \{\nu(n-2) \mid \nu \in [0, k]\}$. Putting all together the assertion follows. $\square$

Proposition 3.7. *Let G be a finite abelian group, $g \in G$ with $\text{ord}(g) = n \geq 5$, and $B \in \mathcal{B}(G)$ such that $((-g)g)^{2n} \mid B$. Suppose $\mathcal{L}(B)$ is an AAMP with period $\{0, d, n-2\}$ for some $d \in [1, n-3] \setminus \{(n-2)/2\}$.*

1. *If $S \in \mathcal{A}(\mathcal{B}_{\langle g \rangle}(G))$ with $S \mid B$, then $\sigma(S) \in \{0, g, -g, (d+1)g, -(d+1)g\}$.*
2. *If $S_1, S_2 \in \mathcal{A}(\mathcal{B}_{\langle g \rangle}(G))$ with $S_1 S_2 \mid B$, then $\sigma(S_i) \in \{0, g, -g\}$ for at least one $i \in [1, 2]$.*

Proof. By definition, there is a $y \in \mathbb{Z}$ such that $\mathcal{L}(B) \subset y + \{0, d, n-2\} + (n-2)\mathbb{Z}$. We set $U = g^n$ and $V = (-g)g$.

1. Let $S \in \mathcal{A}(\mathcal{B}_{\langle g \rangle}(G))$ with $S \mid B$ and set $\sigma(S) = kg$ with $k \in [0, n-1]$. If $k \in \{0, 1, n-1\}$, then we are done. Suppose that $k \in [2, n-2]$. Since S is an atom in $\mathcal{B}_{\langle g \rangle}(G)$, it follows that $W_1 = S(-g)^k \in \mathcal{A}(G)$ and $W'_1 = Sg^{n-k} \in \mathcal{A}(G)$. We consider a factorization $z \in \mathcal{Z}(B)$ with $UW_1 \mid z$, say $z = UW_1 y$. Then $z' = W'_1 V^k y$ is a factorization of B of length $|z'| = |z| + k - 1$. Since $\mathcal{L}(B)$ is an AAMP with period $\{0, d, n-2\}$ for some $d \in [1, n-3] \setminus \{(n-2)/2\}$ it follows that $k-1 \in \{d, n-2-d\}$.

2. Let $S_1, S_2 \in \mathcal{A}(\mathcal{B}_{\langle g \rangle}(G))$ with $S_1 S_2 \mid B$, and assume to the contrary $\sigma(S_i) = k_i e$ with $k_i \in [2, n-2]$ for each $i \in [1, 2]$. As in 1. it follows that

$$W_1 = S_1(-g)^{k_1}, \quad W'_1 = S_1 g^{n-k_1}, \quad W_2 = S_2(-g)^{k_2}, \quad \text{and} \quad W'_2 = S_2 g^{n-k_2}$$

are in $\mathcal{A}(G)$. We consider a factorization $z \in \mathcal{Z}(B)$ with $UW_1 U W_2 \mid z$, say $z = UW_1 U W_2 y$. Then $z_1 = W'_1 V^{k_1-1} U W_2 y \in \mathcal{Z}(B)$ with $|z_1| = |z| + k_1 - 1$ and hence $k_1 - 1 \in \{d, n-2-d\}$. Similarly, $z_2 = U W_1 W'_2 V^{k_2-1} y \in \mathcal{Z}(B)$, hence $k_2 - 1 \in \{d, n-2-d\}$, and furthermore it follows that $k_1 = k_2$. Now $z_3 = W'_1 V^{k_1-1} W'_2 V^{k_2-1} y \in \mathcal{Z}(B)$ is a factorization of length $|z_3| = |z| + k_1 + k_2 - 2$. Thus, if $k_1 - 1 = d$, then $2d \in \{n-2, n-2+d\}$, a contradiction, and if $k_1 - 1 = n-2-d$, then $2(n-2-d) \in \{n-2, n-2+(n-2-d)\}$, a contradiction. $\square$

4. A SET OF LENGTHS NOT CONTAINED IN $\mathcal{L}(C_{n_1} \oplus C_{n_2})$

The aim of this section is to prove the following proposition.

Proposition 4.1. *Let $G = C_{n_1} \oplus C_{n_2}$ where $n_1, n_2 \in \mathbb{N}$ with $n_1 \mid n_2$ and $6 \leq n_1 < n_2$. Then $\{2, n_2, n_1 + n_2 - 2\} \notin \mathcal{L}(G)$.*

Let $G = C_{n_1} \oplus C_{n_2}$ where $n_1, n_2 \in \mathbb{N}$ with $n_1 \mid n_2$. If $6 \leq n_1 < n_2$ does not hold, then $\{2, n_2, n_1 + n_2 - 2\}$ may or may not be a set of lengths (e.g., if $2 = n_1 \leq n_2$, then $\{2, n_2\} \in \mathcal{L}(G)$). By Proposition 3.6, $\{2, n_2, n_1 + n_2 - 2\} \in \mathcal{L}(C_2^{n_1-2} \oplus C_{n_2})$, whence Proposition 4.1 implies that $\mathcal{L}(C_{n_1} \oplus C_{n_2}) \neq \mathcal{L}(C_2^{n_1-2} \oplus C_{n_2})$. Its proof is based on the characterization of all minimal zero-sum sequences of maximal length over groups of rank two. This characterization is due to Gao, Gryniewicz, Reiher, and the present authors ([8, 9, 35, 28]). We repeat the formulation given in [5, Theorem 3.1] and then derive a corollary.

Lemma 4.2. *Let $G = C_{n_1} \oplus C_{n_2}$ where $n_1, n_2 \in \mathbb{N}$ with $1 < n_1 \mid n_2$. A sequence U over G of length $D(G) = n_1 + n_2 - 1$ is a minimal zero-sum sequence if and only if it has one of the following two forms:*

•

$$U = e_j^{\text{ord}(e_j)-1} \prod_{\nu=1}^{\text{ord}(e_i)} (x_\nu e_j + e_i), \quad \text{where}$$

- (a) $\{i, j\} = \{1, 2\}$ and (e_1, e_2) is a basis of G with $\text{ord}(e_1) = n_1$ and $\text{ord}(e_2) = n_2$,
- (b) $x_1, \dots, x_{\text{ord}(e_i)} \in [0, \text{ord}(e_j) - 1]$ and $x_1 + \dots + x_{\text{ord}(e_i)} \equiv 1 \pmod{\text{ord}(e_j)}$.

In this case, we say that U is of type I with respect to the basis (e_i, e_j) ;

•

$$U = (e_1 + y e_2)^{s n_1 - 1} e_2^{n_2 - s n_1 + \epsilon} \prod_{\nu=1}^{n_1 - \epsilon} (-x_\nu e_1 + (-x_\nu y + 1) e_2), \quad \text{where}$$

- (a) (e_1, e_2) is a basis of G with $\text{ord}(e_1) = n_1$ and $\text{ord}(e_2) = n_2$,
- (b) $y \in [0, n_2 - 1]$, $\epsilon \in [1, n_1 - 1]$, and $s \in [1, n_2/n_1 - 1]$,

- (c) $x_1, \dots, x_{n_1-\epsilon} \in [1, n_1 - 1]$ with $x_1 + \dots + x_{n_1-\epsilon} = n_1 - 1$,
- (d) $n_1 y e_2 \neq 0$, and
- (e) either $s = 1$ or $n_1 y e_2 = n_1 e_2$.

In this case, we say that U is of type II with respect to the basis (e_1, e_2) .

We record some observations on this result. If $n_1 = n_2$, then sequences of type II do not exist as the condition $n_1 y e_2 \neq 0$ cannot hold. Assume that $n_1 \neq n_2$. There are examples of sequences that are both of type I and of type II. However, such sequences are of a rather special form.

If a sequence U is of type I with $j = 2$, then it contains an element with multiplicity $n_2 - 1$. Thus, U is of type II only when $s = 1$ and $\epsilon = n_1 - 1$ and consequently $x_1 = n_1 - 1$, that is, $U = e_2^{n_2-1}(e_1 + y e_2)^{n_1-1}(e_1 + (-(n_1 - 1)y + 1)e_2)$ with $y \in [0, n_2 - 1]$ and $n_1 y e_2 \neq 0$. Such a sequence is indeed of type I.

If a sequence U is of type I with $j = 1$, then it contains an element of order n_1 with multiplicity $n_1 - 1$. Since the order of $e_1 + y e_2$ cannot be n_1 , as $n_1 y e_2 \neq 0$, and the order of e_2 is not n_1 either, this is only possible when $\epsilon = 1$ and consequently $x_1 = \dots = x_{n_1-1} = 1$, that is, $U = (e_1 + y e_2)^{s n_1 - 1} e_2^{n_2 - s n_1 + 1} (-e_1 + (-y + 1)e_2)^{n_1 - 1}$. If $n_1 y e_2 = n_1 e_2$, then indeed $e'_1 = -e_1 + (-y + 1)e_2$ is an element of order n_1 , we get that (e'_1, e_2) is a basis of G and U is of type I with respect to the basis (e'_1, e_2) , indeed, $U = e_1'^{n_1-1}((n_1 - 1)e'_1 + e_2)^{s n_1 - 1} e_2^{n_2 - s n_1 + 1}$ for some $s \in [1, n_2/n_1 - 1]$.

Corollary 4.3. *Let $G = C_{n_1} \oplus C_{n_2}$ where $n_1, n_2 \in \mathbb{N}$ with $n_1 \mid n_2$ and $6 \leq n_1 < n_2$, and let $U \in \mathcal{A}(G)$ with $|U| = D(G) = n_1 + n_2 - 1$.*

1. *If $h(U) = n_2 - 1$, then U is of type I with respect to a basis (e_1, e_2) with $\text{ord}(e_1) = n_1$ and $\text{ord}(e_2) = n_2$, that is*

$$U = e_2^{\text{ord}(e_2)-1} \prod_{\nu=1}^{\text{ord}(e_1)} (x_\nu e_2 + e_1)$$

where $x_1, \dots, x_{n_1} \in [0, n_2 - 1]$ with $x_1 + \dots + x_{n_1} \equiv 1 \pmod{n_2}$.

2. *If $h(U) = n_2 - 2$, then*

$$U = (e_1 + y e_2)^{n_1-1} e_2^{n_2-2} (-x e_1 + (-x y + 1)e_2) (- (n_1 - 1 - x)e_1 + (-(n_1 - 1 - x)y + 1)e_2),$$

where (e_1, e_2) is a basis with $\text{ord}(e_1) = n_1$, $\text{ord}(e_2) = n_2$, $y \in [0, n_2 - 1]$, and $x \in [1, (n_1 - 1)/2]$.

3. *If $h(U) = n_2 - 3$, then*

$$U = (e_1 + y e_2)^{n_1-1} e_2^{n_2-3} \prod_{\nu=1}^3 (-x_\nu e_1 + (-x_\nu y + 1)e_2),$$

where (e_1, e_2) is a basis with $\text{ord}(e_1) = n_1$, $\text{ord}(e_2) = n_2$, $y \in [0, n_2 - 1]$, and $x_1, x_2, x_3 \in [1, n_1 - 1]$ with $x_1 + x_2 + x_3 \equiv n_1 - 1 \pmod{n_1}$ (if $y \neq 0$, then $x_1 + x_2 + x_3 = n_1 - 1$).

4. *There is at most one element $g \in G$ with $v_g(U) \geq n_2 - 3$. In particular, if $h(U) \geq n_2 - 3$, then there is precisely one element $g \in G$ with $v_g(U) = h(U)$.*

Proof. We use all notation as in Lemma 4.2.

1. If U is of type II with respect to the basis (e_1, e_2) , then as observed above $s = 1$, $\epsilon = n_1 - 1$, and

$$U = (e_1 + y e_2)^{n_1-1} e_2^{n_2-1} (e_1 + ((-n_1 + 1)y + 1)e_2),$$

which shows that U is also of type I with respect to the basis (e_1, e_2) . If U is of type I with respect to the basis (e_2, e_1) then $h(U) = n_2 - 1$ implies that U is also of type I with respect to the basis (e_1, e_2) .

2. Suppose that U is of type I with respect to the basis (f_2, f_1) . Then U has the form

$$U = f_1^{n_1-1} (x_1 f_1 + f_2)^{n_2-2} (x_2 f_1 + f_2) (x_3 f_1 + f_2).$$

Thus U has the asserted form with $y = 0$, $e_1 = f_1$, and with $e_2 = x_1 f_1 + f_2$. In this case we only have two summands the congruence condition modulo n_2 , and hence we obtain an equality in the integers. Suppose

that U is of type II with respect to the basis (e_1, e_2) . Then $s = 1$, $\epsilon = n_1 - 2$, and thus the assertion follows.

3. Suppose that U is of type I with respect to the basis (f_1, f_2) . Then U has the form

$$U = f_1^{n_1-1}(x_1f_1 + f_2)^{n_2-3}(x_2f_1 + f_2)(x_3f_1 + f_2)(x_4f_1 + f_2).$$

Thus U has the asserted form with $y = 0$, $e_1 = f_1$, and with $e_2 = x_1f_1 + f_2$. Suppose that U is of type II with respect to the basis (e_1, e_2) . Then $s = 1$, $\epsilon = n_1 - 3$, and thus the assertion follows.

4. Assume to the contrary that there are two distinct elements $g_1, g_2 \in G$ with $\mathbf{v}_{g_1}(U) \geq n_2 - 3$ and $\mathbf{v}_{g_2}(U) \geq n_2 - 3$. Then

$$(n_2 - 3) + (n_2 - 3) \leq \mathbf{v}_{g_1}(U) + \mathbf{v}_{g_2}(U) \leq |U| = n_1 + n_2 - 1,$$

which implies that $n_2 \leq n_1 + 5$. Hence $2n_1 \leq n_2 \leq n_1 + 5$ and $n_1 \leq 5$, a contradiction. $\square$

We recall a technique frequently used in [13] and then provide a minor modification of [13, Lemma 5.3].

Lemma 4.4. *Let G be a finite abelian group and let $S \in \mathcal{F}(G)$ be a zero-sum free sequence.*

If $\prod_{g \in \text{supp}(S)} (1 + \mathbf{v}_g(S)) > |G|$, then there is an $A \in \mathcal{A}(G)$ with $|A| \geq 3$ such that $(-A)A \mid (-S)S$.

Proof. We observe that

$$|\{T \in \mathcal{F}(G) \mid T \text{ is a subsequence of } S\}| = \prod_{g \in \text{supp}(S)} (1 + \mathbf{v}_g(S)).$$

Thus, if $\prod_{g \in \text{supp}(S)} (1 + \mathbf{v}_g(S)) > |G|$, then there exist distinct sequences $T'_1, T'_2 \in \mathcal{F}(G)$ such that $T'_1 \mid S$, $T'_2 \mid S$, and $\sigma(T'_1) = \sigma(T'_2)$. We set $T'_1 = TT_1$ and $T'_2 = TT_2$ where $T = \gcd(T'_1, T'_2)$ and $T_1, T_2 \in \mathcal{F}(G)$. Then $\sigma(T_1) = \sigma(T_2)$ and $(-T_1)T_2$ is a zero-sum subsequence of $(-S)S$. Let $A \in \mathcal{A}(G)$ with $A \mid (-T_1)T_2$. Assume to the contrary that $|A| = 2$. Then $A = (-g)g$ for some $g \in G$. Since S is zero-sum free, we infer (after renumbering if necessary) that $(-g) \mid (-T_1)$ and $g \mid T_2$, a contradiction to $\gcd(T_1, T_2) = 1$. Therefore we obtain that $|A| \geq 3$, which implies that $|\gcd(A, (-g)g)| \leq 1$ for each $g \in G$, and thus $(-A)A \mid (-S)S$. $\square$

Lemma 4.5. *Let $t \in \mathbb{N}$ and $\alpha, \alpha_1, \dots, \alpha_t, \alpha'_1, \dots, \alpha'_t \in \mathbb{R}$ with $\alpha_1 \geq \dots \geq \alpha_t \geq 0$, $\alpha'_1 \geq \dots \geq \alpha'_t \geq 0$, $\alpha'_i \leq \alpha_i$ for each $i \in [1, t]$, and $\sum_{i=1}^t \alpha_i \geq \alpha \geq \sum_{i=1}^t \alpha'_i$. Then*

$$\prod_{\nu=1}^t (1 + x_\nu) \quad \text{is minimal}$$

over all $(x_1, \dots, x_t) \in \mathbb{R}^t$ with $\alpha'_i \leq x_i \leq \alpha_i$ for each $i \in [1, t]$ and $\sum_{i=1}^t x_i = \alpha$, if

$$x_i = \alpha_i \text{ for each } i \in [1, s] \quad \text{and} \quad x_i = \alpha'_i \text{ for each } i \in [s+2, t]$$

where $s \in [0, t]$ is maximal with $\sum_{i=1}^s \alpha_i \leq \alpha$.

Proof. Since continuous functions attain minima on compact sets, the above function has a minimum at some point $(m_1, \dots, m_t) \in \mathbb{R}^t$. Suppose there are $i, j \in [1, t]$ such that $i < j$ and $m_i < m_j$. Then $\alpha'_j \leq \alpha'_i \leq m_i < m_j \leq \alpha_j \leq \alpha_i$, and thus we can exchange m_i and m_j . Therefore, after renumbering if necessary, we may suppose that $m_1 \geq \dots \geq m_t$. Since for $x \geq y \geq 0$ and $\delta > 0$ we have

$$(1 + x + \delta)(1 + y - \delta) = (1 + x)(1 + y) - \delta(x - y) - \delta^2 < (1 + x)(1 + y),$$

it follows that all but at most one of the m_i is equal to α_i or α'_i . It remains to show that there is an $s \in [1, t]$ such that $m_i = \alpha_i$ for $i \in [1, s]$ and $m_i = \alpha'_i$ for each $i \in [s+2, t]$. Assume to the contrary that this is not the case. Then there are $i, j \in [1, t]$ with $i < j$ such that $m_i < \alpha_i$ and $\alpha'_j < m_j$. Using again the just mentioned inequality and that $m_i \geq m_j$, we obtain a contradiction to the minimum being attained at $(m_1, \dots, m_t)$. $\square$

Proof of Proposition 4.1. Assume to the contrary that there is an $A \in \mathcal{B}(G)$ such that $\mathsf{L}(A) = \{2, n_2, n_1 + n_2 - 2\}$. Then there are $U, V \in \mathcal{A}(G)$ with $|U| \geq |V|$ such that $A = UV$. We set

$$U = SU' \quad \text{and} \quad V = (-S)V', \quad \text{where } U', V' \in \mathcal{F}(G), \text{ and } S = \gcd(U, -V).$$

Since $2(n_1 + n_2 - 2) \leq |A| = |U| + |V| \leq 2\mathsf{D}(G) = 2(n_1 + n_2 - 1)$, there are the following three cases:

- (I) $|A| = 2(n_1 + n_2 - 2)$. Then, a factorization of A of length $n_1 + n_2 - 2$ must contain only minimal zero-sum sequences of length 2 and thus $U' = V' = 1$.
- (II) $|A| = 2(n_1 + n_2 - 2) + 1$. Then, a factorization of A of length $n_1 + n_2 - 2$ must contain one minimal zero-sum of length 3 and otherwise only minimal zero-sum sequences of length 2, thus $U' = g_1g_2$ and $V' = (-g_1 - g_2)$ for some $g_1, g_2 \in G$.
- (III) $|A| = 2(n_1 + n_2 - 1)$. Then a factorization of A of length $n_1 + n_2 - 2$ must contain either one minimal zero-sum subsequence of length 4 and otherwise minimal zero-sum sequences of length 2, or two minimal zero-sum sequences of length 3 and otherwise only minimal zero-sum sequences of length 2. Thus, there are the following two subcases.
 - $U' = g_1g_2$, $V' = h_1h_2$ where $g_1, g_2, h_1, h_2 \in G$ such that $g_1g_2h_1h_2 \in \mathcal{A}(G)$.
 - $U' = g_1g_2(-h_1 - h_2)$ and $V' = h_1h_2(-g_1 - g_2)$ where $g_1, g_2, h_1, h_2 \in G$.

We start with the following two assertions.

A1. Let $W \in \mathcal{A}(G)$ with $|W| < |U|$ and $W \mid (-S)S$. Then $|W| \in \{2, n_1\}$.

A2. Let $W_1, W_2 \in \mathcal{A}(G)$ such that $W_1(-W_1)W_2(-W_2) \mid S(-S)$. Then $\{|W_1|, |W_2|\} \neq \{n_1\}$.

Proof of A1. Suppose $|W| > 2$. Then $(-W)W \mid (-S)S$ and we set $(-S)S = (-W)WT(-T)$ with $T \in \mathcal{F}(G)$ and obtain that

$$UV = (-W)WT(-T)(U'V').$$

Let z be a factorization of $U'V'$. Then $|z| \in [0, 2]$. If $T = 1$, then UV has a factorization of length $2 + |z| \in \{2, n_2, n_1 + n_2 - 2\}$ which implies $|z| = 0$ and hence $|W| = |U|$, a contradiction. Thus $T \neq 1$. Since $T(-T)$ has a factorization of length $|T| = |S| - |W|$, the above decomposition gives rise to a factorization of UV of length t where

$$3 \leq t = 2 + |T| + |z| = 2 + |S| - |W| + |z| \in \{n_2, n_1 + n_2 - 2\}.$$

We distinguish four cases.

Suppose that $U' = V' = 1$. Then $z = 1$, $|z| = 0$, and $|S| = |U| = n_1 + n_2 - 2$. Thus $t = n_1 + n_2 - |W| \in \{n_2, n_1 + n_2 - 2\}$, and the assertion follows.

Suppose that $U' = g_1g_2$ and $V' = (-g_1 - g_2)$ for some $g_1, g_2 \in S$. Then $|z| = 1$ and $|S| = n_1 + n_2 - 3$. Thus $t = n_1 + n_2 - |W| \in \{n_2, n_1 + n_2 - 2\}$, and the assertion follows.

Suppose that $U' = g_1g_2$, $V' = h_1h_2$ where $g_1, g_2, h_1, h_2 \in G$ such that $g_1g_2h_1h_2 \in \mathcal{A}(G)$. Then $|z| = 1$ and $|S| = n_1 + n_2 - 3$. Thus $t = n_1 + n_2 - |W| \in \{n_2, n_1 + n_2 - 2\}$, and the assertion follows.

Suppose that $U' = g_1g_2(-h_1 - h_2)$ and $V' = h_1h_2(-g_1 - g_2)$ where $g_1, g_2, h_1, h_2 \in G$. Then $|z| = 2$ and $|S| = n_1 + n_2 - 4$. Thus $t = n_1 + n_2 - |W| \in \{n_2, n_1 + n_2 - 2\}$, and the assertion follows. $\square(\mathbf{A1})$

Proof of A2. Assume to the contrary that $|W_1| = |W_2| = n_1$. Then there are $W_5, \dots, W_k \in \mathcal{A}(G)$ such that

$$UV = W_1(-W_1)W_2(-W_2)W_5 \cdots W_k,$$

where $k \in \mathsf{L}(UV) = \{2, n_2, n_1 + n_2 - 2\}$ and hence $k = n_2$. Since

$$|W_5 \cdots W_k| = |UV| - 4n_1 \leq 2(n_1 + n_2 - 1) - 4n_1 = 2(n_2 - n_1 - 1),$$

it follows that

$$k - 4 \leq \max \mathsf{L}(W_5 \cdots W_k) \leq |W_5 \cdots W_k|/2 \leq n_2 - n_1 - 1 < n_2 - 4,$$

a contradiction. $\square(\mathbf{A2})$

We distinguish two cases depending on the size of $\mathsf{h}(S)$.

CASE 1: $h(S) \geq n_2/2$.

We set $S = g^v S'$ where $g \in G$, $v = h(S)$, and $S' \in \mathcal{F}(G)$. Then

$$U_1 = (-g)^{n_2-v} S' U' \in \mathcal{B}(G), \quad V_1 = g^{n_2-v} (-S') V' \in \mathcal{B}(G).$$

Clearly, we have

$$(U')^{-1} U_1 = (-g)^{n_2-v} S' = -((V')^{-1} V_1).$$

We will often use that if some $W \in \mathcal{A}(G)$ divides $(U')^{-1} U_1$, then $(-W)$ divides $(V')^{-1} V_1$ and hence $(-W)W \mid (-S)S$. Now we choose factorizations $x_1 \in \mathcal{Z}(U_1)$ and $y_1 \in \mathcal{Z}(V_1)$. Note that $|x_1| \leq n_2 - v$ and $|y_1| \leq n_2 - v$ as each minimal zero-sum sequence in x_1 and y_1 contains $(-g)$ and g , respectively. Then $UV = U_1 V_1 ((-g)g)^{2v-n_2}$ has a factorization of length t where

$$2 + (2v - n_2) \leq t = |x_1| + |y_1| + (2v - n_2) \leq 2(n_2 - v) + (2v - n_2) = n_2.$$

Assume to the contrary that $t = 2$. Then $v = n_2/2$ and both, $U = g^{n_2/2} S' U'$ and $U' = (-g)^{n_2/2} S' U'$, are minimal zero-sum sequences, a contradiction, as $SU' \notin \mathcal{A}(\mathcal{B}_{\langle g \rangle}(G))$ as its length is greater than $n_1 = D_{\langle g \rangle}(G) = D(G/\langle g \rangle)$. Thus $t = n_2$, $|x_1| = |y_1| = n_2 - v$, and hence $\mathcal{L}(U_1) = \mathcal{L}(V_1) = \{n_2 - v\}$. If $W \in \mathcal{A}(G)$ with $|W| = 2$ and $W \mid U_1$, then $W = (-g)g$. Similarly, if $W' \in \mathcal{A}(G)$ with $|W'| = 2$ and $W' \mid V_1$, then $W' = (-g)g$. By definition of v , not both U_1 and V_1 are divisible by an atom of length 2. Now we distinguish four cases depending on the form of U' and V' , which we determined above.

CASE 1.1: $U' = V' = 1$.

Then $V_1 = -U_1$, say $V_1 = W_1 \cdot \dots \cdot W_{n_2-v}$. Since none of the W_i has length 2, it follows that $|W_1| = \dots = |W_{n_2-v}| = n_1$ and hence

$$2(n_2 + n_1 - 2) = 2|V| = 2(2v - n_2) + 2|V_1| = 2(2v - n_2) + 2n_1(n_2 - v),$$

which implies that $v = n_2 - 1$. Consequently $|S| = n_1 - 1$ and $S \in \mathcal{A}(\mathcal{B}_{\langle g \rangle}(G))$. This implies that (use an elementary direct argument or [11, Theorem 5.1.8]),

$$S = (2e_1 + a_1 e_2) \prod_{\nu=2}^{n_1-1} (e_1 + a_\nu e_2),$$

where (e_1, e_2) is a basis of G . Let $r \in [0, n_2 - 1]$ such that $r \equiv -a_1 + a_2 + a_3 \pmod{n_2}$. Then

$W_1 = (2e_1 + a_1 e_2)(-e_1 - a_2 e_2)(-e_1 - a_3 e_2)e_2^r$ and $W_2 = (2e_1 + a_1 e_2)(-e_1 - a_2 e_2)(-e_1 - a_3 e_2)(-e_2)^{n_2-r}$ are minimal zero-sum sequences dividing $(-V)V$. Since $|W_1| = 3 + r$, $|W_2| = 3 + n_2 - r$, and $|W_1 W_2| = n_2 + 6 > 2n_1$, at least one of them does not have length n_1 , a contradiction.

CASE 1.2: $U' = g_1 g_2$ and $V' = (-g_1 - g_2)$ for some $g_1, g_2 \in G$.

We set

$$x_1 = X_1 \cdot \dots \cdot X_{n_2-v} \quad \text{and} \quad y_1 = Y_1 \cdot \dots \cdot Y_{n_2-v}$$

where all $X_i, Y_j \in \mathcal{A}(G)$, $g_1 g_2 \mid X_1 X_2$ (or even $g_1 g_2 \mid X_1$), and $(-g_1 - g_2) \mid Y_1$. We distinguish three subcases.

CASE 1.2.1: $v = n_2 - 1$.

By Corollary 4.3, with all notations as introduced there, we get $U = e_2^{n_2-1} \prod_{\nu=1}^{n_1} (e_1 + x_\nu e_2)$. Thus $g = e_2$ and $U' \mid \prod_{\nu=1}^{n_1} (e_1 + x_\nu e_2)$, whence after renumbering if necessary we have $g_i = x_i e_1 + e_2$ for each $i \in [1, 2]$. Therefore we have

$$V = (-2e_1 - (x_1 + x_2)e_2)(-e_2)^{n_2-1} \prod_{\nu=3}^{n_1} (-e_1 - x_\nu e_2) = (-g_1 - g_2)(-S).$$

Assume to the contrary that there are $i, j \in [3, n_1]$ distinct with $x_i \neq x_j$. If $q \in [1, n_2 - 1]$ with $q \equiv -(x_i - x_j) \pmod{n_2}$, then

$$W'_1 = (e_1 + x_i e_2)(-e_1 - x_j e_2)e_2^q \quad \text{and} \quad W'_2 = (e_1 + x_i e_2)(-e_1 - x_j e_2)(-e_2)^{n_2-q}$$

are atoms dividing $(-S)S$, both have length greater than two but not both have length n_1 , a contradiction to **A1**. Therefore we have $x_3 = \dots = x_{n_1}$. Since $x_1 + \dots + x_{n_1} \equiv 1 \pmod{n_2}$, it follows that $x_1 \neq x_3$ or $x_2 \neq x_3$, say $x_2 \neq x_3$. Therefore there is an $r \in [1, n_2 - 1]$ with $r \equiv x_2 - x_3$ such that

$$W_1 = (- (x_1 + x_2)e_2 - 2e_1)(x_1e_2 + e_1)(x_3e_2 + e_1)e_2^r \in \mathcal{A}(G)$$

and

$$W_2 = (x_2e_2 + e_1)(-x_3e_2 - e_1)(-e_2)^r \in \mathcal{A}(G).$$

Thus it follows that

$$UV = W_1W_2 \prod_{\nu=4}^{n_1} ((x_\nu e_2 + e_1)(-x_\nu e_2 - e_1))((-e_2)e_2)^{n_2-1-r}$$

has a factorization of length

$$2 + (n_1 - 3) + (n_2 - 1 - r) = n_1 + n_2 - 2 - r \in \{2, n_2, n_1 + n_2 - 2\},$$

and hence $r = n_1 - 2$. Now we define

$$W'_1 = (- (x_1 + x_2)e_2 - 2e_1)(x_1e_2 + e_1)(x_3e_2 + e_1)(-e_2)^{n_2-r}$$

and

$$W'_2 = (x_2e_2 + e_1)(-x_3e_2 - e_1)e_2^{n_2-r} \in \mathcal{A}(G).$$

Thus it follows that

$$UV = W'_1W'_2 \prod_{\nu=4}^{n_1} ((x_\nu e_2 + e_1)(-x_\nu e_2 - e_1))((-e_2)e_2)^{r-1}$$

has a factorization of length

$$2 + (n_1 - 3) + (r - 1) = n_1 - 2 + r = 2n_1 - 4 \notin \{2, n_2, n_1 + n_2 - 2\}, \text{ a contradiction.}$$

CASE 1.2.2: $v = n_2 - 2$.

Since $V' \mid Y_1$ it follows that $Y_2 \mid (-S)S$ and we thus may assume that $X_2 = -Y_2$. Furthermore, $|Y_2|$ cannot have length 2, since $-g \nmid S'$. Hence **A1** gives that $|Y_2|$ has length n_1 . It follows that $|Y_1| = 2$ and $|X_1| = 3$. This implies that $-g_1 - g_2 = -g$ whence $v_{-g}(V) = n_2 - 1$ and $v_g(U) = n_2 - 2$. By Corollary 4.3, with all notations as introduced there, we obtain that

$$U = (e_1 + ye_2)^{n_1-1}e_2^{n_2-2}(-xe_1 + (-xy + 1)e_2)(-(n_1 - 1 - x)e_1 + (-(n_1 - 1 - x)y + 1)e_2).$$

Since $g_1 + g_2 = g = e_2$, it follows that $x = 1$ and that

$$V = (-(e_1 + ye_2))^{n_1-2}(-e_2)^{n_2-1}((n_1 - 2)e_1 + ((n_1 - 2)y + 1)e_2).$$

Then $W = (e_1 + ye_2)^2((n_1 - 2)e_1 + ((n_1 - 2)y + 1)e_2)(-e_2)^r$, where $r \in [0, n_2 - 1]$ such that $r \equiv n_1y + 1 \pmod{n_2}$, is a minimal zero-sum sequence. Since $r \equiv 1 \pmod{n_1}$, it follows that $r \in [1, n_2 - n_1 + 1]$. Thus, $W \mid (-S)S$, hence $|W| = n_1$, and thus $r = n_1 - 3$. We consider $W' = (e_1 + ye_2)^2((n_1 - 2)e_1 + ((n_1 - 2)y + 1)e_2)e_2^{n_2-(n_1-3)}$. Again, $W' \mid (-S)S$. Yet $|W'| = 3 + (n_2 - (n_1 - 3)) = n_2 - n_1 + 6$, a contradiction.

CASE 1.2.3: $v \leq n_2 - 3$.

Then $Y_2Y_3 \mid (V')^{-1}V_1$, and since $|Y_2| \neq 2 \neq |Y_3|$, we infer that $|Y_2| = |Y_3| = n_1$. Thus $(-Y_2)(-Y_3) \mid (U')^{-1}U_1$ and $Y_2(-Y_2)Y_3(-Y_3) \mid S(-S)$, a contradiction to **A2**.

CASE 1.3: $U' = g_1g_2$ and $V' = h_1h_2$, where $g_1, g_2, h_1, h_2 \in G$ such that $g_1g_2h_1h_2 \in \mathcal{A}(G)$.

We set

$$x_1 = X_1 \cdot \dots \cdot X_{n_2-v} \quad \text{and} \quad y_1 = Y_1 \cdot \dots \cdot Y_{n_2-v}$$

where all $X_i, Y_j \in \mathcal{A}(G)$, $g_1g_2 \mid X_1X_2$ (or even $g_1g_2 \mid X_1$), and $h_1h_2 \mid Y_1Y_2$ (or even $h_1h_2 \mid Y_1$). We distinguish four cases.

CASE 1.3.1: $v = n_2 - 1$.

By Corollary 4.3, we have

$$U = e_2^{n_2-1} \prod_{\nu=1}^{n_1} (e_1 + x_\nu e_2) \text{ and } -V = e_2^{n_2-1} \prod_{\nu=1}^{n_1} (e'_1 + x'_\nu e_2),$$

where (e_1, e_2) and (e'_1, e_2) are both bases with $\text{ord}(e_2) = n_2$ and $x_i, x'_i \in [0, n_2 - 1]$ for each $i \in [1, n_1]$. Since $|S| = |U| - 2$, it follows that, after renumbering if necessary, $\prod_{\nu=3}^{n_1} (e_1 + x_\nu e_2) \mid (-V)$ and hence, after a further renumbering if necessary, $e_1 + x_i e_2 = e'_1 + x'_i e_2$ for each $i \in [3, n_1]$. Thus, if we write $-V$ with respect to the basis (e_1, e_2) , it still has the above structure. Therefore we may assume that $e_1 = e'_1$ and $x_i = x'_i$ for each $i \in [3, n_1]$. Therefore

$$g_i = e_1 + x_i e_2 \quad \text{and} \quad h_i = -e_1 - x'_i e_2 \quad \text{for each } i \in [1, 2].$$

Since $g_1 + g_2 = -h_1 - h_2$, it follows that $x_1 + x_2 \equiv -x'_1 - x'_2 \pmod{n_2}$ and hence $x_1 - x'_1 \equiv x'_2 - x_2 \pmod{n_2}$. Let $r \in [0, n_2 - 1]$ such that $r \equiv x_1 - x'_1 \pmod{n_2}$. Then

$$W_1 = g_1 h_1 (-e_2)^r, \quad W'_1 = g_1 h_1 e_2^{n_2-r}, \quad W_2 = g_2 h_2 e_2^r, \quad \text{and} \quad W'_2 = g_2 h_2 (-e_2)^{n_2-r}$$

are minimal zero-sum sequences which give rise to the factorizations

$$\begin{aligned} UV &= W_1 W_2 ((-e_2) e_2)^{n_2-r-1} \prod_{\nu=3}^{n_1} ((e_1 + x_\nu e_2)(-e_1 - x_\nu e_2)) \\ &= W'_1 W'_2 ((-e_2) e_2)^{r-1} \prod_{\nu=3}^{n_1} ((e_1 + x_\nu e_2)(-e_1 - x_\nu e_2)). \end{aligned}$$

These factorizations have length $2 + (n_2 - r - 1) + (n_1 - 2) = n_1 + n_2 - 2 - (r - 1)$ and $2 + (r - 1) + (n_1 - 2) = n_1 + r - 1$. Since not both of them can be in $\{2, n_2, n_1 + n_2 - 2\}$, a contradiction.

CASE 1.3.2: $v = n_2 - 2$.

Assume to the contrary that $h(U) = h(V) = n_2 - 1$. Since, by Corollary 4.3, the elements $g', g'' \in G$ with $v_{g'}(U) = n_2 - 1$ and $v_{g''}(V) = n_2 - 1$ are uniquely determined, it follows that $g = g' = -g''$ and hence $v = h(S) = n_2 - 1$, a contradiction. Thus, after exchanging U and V if necessary, we may assume that $h(U) = n_2 - 2$ and it remains to consider the two cases $h(V) = n_2 - 1$ and $h(V) = n_2 - 2$.

CASE 1.3.2.1: $h(U) = n_2 - 2$ and $h(V) = n_2 - 1$.

By Corollary 4.3, we infer that

$$\begin{aligned} U &= (e_1 + y e_2)^{n_1-1} e_2^{n_2-2} (-x e_1 + (-xy + 1) e_2) (- (n_1 - 1 - x) e_1 + (- (n_1 - 1 - x) y + 1) e_2), \\ -V &= e_2^{n_2-1} \prod_{\nu=1}^{n_1} (e'_1 + x_\nu e_2), \end{aligned}$$

where (e_1, e_2) and (e'_1, e_2) are bases and all parameters are as in Corollary 4.3. Since $|S| = |U| - 2$, it follows that $(e_1 + y e_2)^{n_1-3} \mid (-V)$ and hence, after renumbering if necessary, $e'_1 + x_1 e_2 = \dots = e'_1 + x_{n_1-3} e_2 = e_1 + y e_2$. Thus, if we write $-V$ with respect to the basis (e_1, e_2) , it still has the above structure. Therefore we may assume that $e_1 = e'_1$ and $y = x_1 = \dots = x_{n_1-3}$. Thus we obtain that

$$-V = e_2^{n_2-1} (e_1 + y e_2)^{n_1-3} \prod_{\nu=n_1-2}^{n_1} (e_1 + x_\nu e_2).$$

Note that $e_2 \in \{-h_1, -h_2\}$, $e_2 \notin \{g_1, g_2\}$, say $-h_1 = e_2$ and $-h_2 = e_1 + x_{n_1} e_2$, and $g_1 + g_2 = -(h_1 + h_2) = e_1 + (x_{n_1} + 1) e_2$. This condition on the sum shows that

$$\{g_1, g_2\} = \{-x e_1 + (-xy + 1) e_2, -(n_1 - 1 - x) e_1 + (- (n_1 - 1 - x) y + 1) e_2\}.$$

This implies that $(e_1 + y e_2)^{n_1-1} \mid (-V)$ and hence, after renumbering if necessary,

$$-V = e_2^{n_2-1} (e_1 + y e_2)^{n_1-1} (e_1 + x_{n_1} e_2).$$

Since $g_1 + g_2 = -(n_1 - 1)e_1 - (y(n_1 - 1) - 2)e_2$, it follows that the sequence

$$W_1 = g_1 g_2 (-e_1 - y e_2) (-e_2)^r,$$

where $r \in [0, n_2 - 1]$ and $r \equiv -y n_1 + 2 \pmod{n_2}$, is a minimal zero-sum sequence. Since $r \equiv 2 \pmod{n_1}$, we infer that $r \in [2, n_2 - 2]$ and that $W_1 \mid UV$. Since $g_1 + g_2 = -(h_1 + h_2)$, we obtain that

$$W_2 = h_1 h_2 (e_1 + y e_2) e_2^r \in \mathcal{B}(G), \quad \mathsf{L}(W_2) = \{2\} \quad \text{and} \quad W_2 \mid UV.$$

Therefore it follows that

$$UV = W_1 W_2 ((-e_2) e_2)^{n_2 - 2 - r} ((e_1 + y e_2) (-e_1 - y e_2))^{n_1 - 2},$$

and hence $n_1 + n_2 - 1 - r \in \mathsf{L}(UV) = \{2, n_2, n_1 + n_2 - 2\}$, a contradiction, since $r \equiv 2 \pmod{n_1}$.

CASE 1.3.2.2: $\mathsf{h}(U) = \mathsf{h}(V) = n_2 - 2$.

By Corollary 4.3, we infer that

$$U = (e_1 + y e_2)^{n_1 - 1} e_2^{n_2 - 2} U'' \quad \text{and} \quad -V = (e'_1 + y' e_2)^{n_1 - 1} e_2^{n_2 - 2} (-V''),$$

where (e_1, e_2) and (e'_1, e_2) are bases, $U'', V'' \in \mathcal{F}(G)$ with $|U''| = |V''| = 2$, and $y, y' \in [0, n_2 - 1]$. Since $|S| = |U| - 2$, it follows that $(e'_1 + y' e_2)^{n_1 - 3} \mid U$ and hence $e'_1 + y' e_2 = e_1 + y e_2$. Thus, if we write $-V$ with respect to the basis (e_1, e_2) , it still has the above structure. Therefore we may assume that $e_1 = e'_1$ and $y = y'$. Therefore it follows that

$$U = (e_1 + y e_2)^{n_1 - 1} e_2^{n_2 - 2} g_1 g_2 \quad \text{and} \quad V = (-e_1 - y e_2)^{n_1 - 1} (-e_2)^{n_2 - 2} h_1 h_2,$$

and hence $g_1 + g_2 = -(n_1 - 1)e_1 - (y(n_1 - 1) - 2)e_2$. Thus

$$W_1 = g_1 g_2 (-e_1 - y e_2) (-e_2)^r,$$

where $r \in [0, n_2 - 1]$ and $r \equiv -y n_1 + 2 \pmod{n_2}$, is a minimal zero-sum sequence. Since $r \equiv 2 \pmod{n_1}$, we infer that $r \in [2, n_2 - 2]$ and that $W_1 \mid UV$. Since $g_1 + g_2 = -(h_1 + h_2)$, we obtain that

$$W_2 = h_1 h_2 (e_1 + y e_2) e_2^r \in \mathcal{A}(G) \quad \text{and} \quad W_2 \mid UV.$$

Therefore it follows that

$$UV = W_1 W_2 ((-e_2) e_2)^{n_2 - 2 - r} ((e_1 + y e_2) (-e_1 - y e_2))^{n_1 - 2},$$

and hence $n_1 + n_2 - 2 - r \in \mathsf{L}(UV) = \{2, n_2, n_1 + n_2 - 2\}$, a contradiction, since $r \equiv 2 \pmod{n_1}$.

CASE 1.3.3: $v = n_2 - 3$.

Then $X_3 \mid (U')^{-1} U_1$ and hence $|X_3| = n_1$. Since

$$|X_1 X_2 X_3| = |U_1| = |U| - v + (n_2 - v) = n_1 + 5,$$

it follows that $|X_1 X_2| = 5$, and hence X_1 or X_2 has length two. Similarly, we obtain that Y_1 or Y_2 has length two, a contradiction to the earlier mentioned fact that not both, U_1 and V_1 are divisible by an atom of length two.

CASE 1.3.4: $v \leq n_2 - 4$.

Then $Y_3 Y_4 \mid (V')^{-1} V_1$, and since $|Y_3| \neq 2 \neq |Y_4|$, we infer that $|Y_3| = |Y_4| = n_1$. Thus $(-Y_3)(-Y_4) \mid (U')^{-1} U_1$ and $Y_3(-Y_3)Y_4(-Y_4) \mid S(-S)$, a contradiction to **A2**.

CASE 1.4: $U' = g_1 g_2 (-h_1 - h_2)$ and $V' = h_1 h_2 (-g_1 - g_2)$, where $g_1, g_2, h_1, h_2 \in G$.

We set

$$x_1 = X_1 \cdots X_{n_2 - v} \quad \text{and} \quad y_1 = Y_1 \cdots Y_{n_2 - v}$$

where all $X_i, Y_j \in \mathcal{A}(G)$, $g_1 g_2 (-h_1 - h_2) \mid X_1 X_2 X_3$ (or even $g_1 g_2 (-h_1 - h_2) \mid X_1 X_2$ or $g_1 g_2 (-h_1 - h_2) \mid X_1$), and $h_1 h_2 (-g_1 - g_2) \mid Y_1 Y_2 Y_3$ (or even $h_1 h_2 (-g_1 - g_2) \mid Y_1 Y_2$ or $h_1 h_2 (-g_1 - g_2) \mid Y_1$). We distinguish five subcases 1.4.1 – 1.4.5.

CASE 1.4.1: $v = n_2 - 1$.

By Corollary 4.3 we have

$$U = e_2^{n_2-1} \prod_{\nu=1}^{n_1} (e_1 + x_\nu e_2) \quad \text{and} \quad -V = e_2^{n_2-1} \prod_{\nu=1}^{n_1} (e'_1 + x'_\nu e_2),$$

where (e_1, e_2) and (e'_1, e_2) are both bases with $\text{ord}(e_2) = n_2$ and $x_\nu, x'_\nu \in [0, n_2 - 1]$ for each $\nu \in [1, n_1]$. Since $|S| = |U| - 3$, it follows that, after renumbering if necessary, $\prod_{\nu=4}^{n_1} (e_1 + x_\nu e_2) \mid (-V)$ and hence, after a further renumbering if necessary, $e_1 + x_\nu e_2 = e'_1 + x'_\nu e_2$ for each $\nu \in [4, n_1]$. Thus, if we write $-V$ with respect to the basis (e_1, e_2) , it still has the above structure. Therefore we may assume that $e_1 = e'_1$ and $x_\nu = x'_\nu$ for each $\nu \in [4, n_1]$. Furthermore, we obtain that

$$\begin{aligned} g_1 &= e_1 + x_1 e_2, \quad g_2 = e_1 + x_2 e_2, \quad -h_1 - h_2 = e_1 + x_3 e_2 \\ h_1 &= -e_1 - x'_1 e_2, \quad h_2 = -e_1 - x'_2 e_2, \quad \text{and} \quad -g_1 - g_2 = -e_1 - x'_3 e_2, \end{aligned}$$

a contradiction, since $\text{ord}(e_1) = n_1 > 3$

CASE 1.4.2: $v = n_2 - 2$.

Arguing as at the beginning of CASE 1.3.2 we may assume $h(U) = n_2 - 2$ and it is sufficient to consider the two subcases $h(V) = n_2 - 1$ and $h(V) = n_2 - 2$.

CASE 1.4.2.1: $h(U) = n_2 - 2$ and $h(V) = n_2 - 1$.

By Corollary 4.3, we infer that $-V = e_2^{n_2-1} \prod_{\nu=1}^{n_1} (e'_1 + x_\nu e_2)$ and

$$U = (e_1 + y e_2)^{n_1-1} e_2^{n_2-2} (-x e_1 + (-xy + 1) e_2) (- (n_1 - 1 - x) e_1 + (- (n_1 - 1 - x) y + 1) e_2),$$

where (e_1, e_2) and (e'_1, e_2) are bases and all parameters are as in Corollary 4.3. Since $|S| = |U| - 3$, it follows that $(e_1 + y e_2)^{n_1-4} \mid (-V)$ and hence, after renumbering if necessary, $e'_1 + x_1 e_2 = \dots = e'_1 + x_{n_1-4} e_2 = e_1 + y e_2$. Thus, if we write $-V$ with respect to the basis (e_1, e_2) , it still has the above structure. Therefore we may assume that $e_1 = e'_1$ and $y = x_5 = \dots = x_{n_1}$. Thus we obtain that

$$-V = e_2^{n_2-1} (e_1 + y e_2)^{n_1-4} \prod_{\nu=1}^4 (e_1 + x_\nu e_2).$$

Since

$$\gcd \left((-x e_1 + (-xy + 1) e_2) (- (n_1 - 1 - x) e_1 + (- (n_1 - 1 - x) y + 1) e_2), -V \right) = 1,$$

it follows that

$$g_1 g_2 (-h_1 - h_2) = (e_1 + y e_2) (-x e_1 + (-xy + 1) e_2) (- (n_1 - 1 - x) e_1 + (- (n_1 - 1 - x) y + 1) e_2).$$

Thus $v_{e_1 + y e_2}(S) = n_1 - 2$ and hence, after renumbering if necessary,

$$-V = e_2^{n_2-1} (e_1 + y e_2)^{n_1-2} (e_1 + x_1 e_2) (e_1 + x_2 e_2).$$

We observe that

$$\begin{aligned} (-x e_1 + (-xy + 1) e_2) + (- (n_1 - 1 - x) e_1 + (- (n_1 - 1 - x) y + 1) e_2) &= e_1 + (- (n_1 - 1) y + 2) e_2, \\ (-e_1 - x_1 e_2) + (-e_1 - x_2 e_2) &= (n_1 - 2) (e_1 + y e_2) + (n_2 - 1) e_2 = -2 e_1 + ((n_1 - 2) y - 1) e_2. \end{aligned}$$

Consequently, there are $r, r' \in [0, n_2 - 1]$ such that

$$W_1 = (-x e_1 + (-xy + 1) e_2) (- (n_1 - 1 - x) e_1 + (- (n_1 - 1 - x) y + 1) e_2) (-e_1 - y e_2) (-e_2)^r \in \mathcal{A}(G) \quad \text{and}$$

$$W_2 = (-e_1 - x_1 e_2) (-e_1 - x_2 e_2) (e_1 + y e_2)^2 e_2^{r'} \in \mathcal{A}(G)$$

(note that $y \notin \{-x_1, -x_2\}$). Clearly we have

$$r \equiv 2 - n_1 y \pmod{n_2} \quad \text{and} \quad r' \equiv 1 - n_1 y \pmod{n_2}.$$

This implies that $r \equiv 2 \pmod{n_1}$ and $r' = r - 1$. Therefore, we obtain that

$$UV = W_1 W_2 ((e_1 + y e_2) (-e_1 - y e_2))^{n_1-3} ((-e_2) e_2)^{n_2-r-1},$$

and thus $n_1 + n_2 - 2 - r \in \mathcal{L}(UV) = \{2, n_2, n_1 + n_2 - 2\}$, a contradiction, since $r \equiv 2 \pmod{n_1}$.

CASE 1.4.2.2: $\mathbf{h}(U) = \mathbf{h}(V) = n_2 - 2$.

By Corollary 4.3, we infer that

$$U = (e_1 + ye_2)^{n_1-1} e_2^{n_2-2} U'' \text{ and } -V = (e'_1 + y'e_2)^{n_1-1} e_2^{n_2-2} (-V''),$$

where (e_1, e_2) and (e'_1, e_2) are bases, $U'', V'' \in \mathcal{F}(G)$ with $|U''| = |V''| = 2$, and $y, y' \in [0, n_2 - 1]$. Since $|S| = |U| - 3$, it follows that $(e'_1 + y'e_2)^{n_1-4} | U$. If $n_1 > 6$, it follows that $e'_1 + y'e_2 = e_1 + ye_2$. If $n_1 = 6$, so n_1 even, then

$$U'' = (-xe_1 + (-xy + 1)e_2) \left(-(n_1 - 1 - x)e_1 + (-(n_1 - 1 - x)y + 1)e_2 \right)$$

is not a square whence $(e'_1 + y'e_2)^2 \neq U''$ and it follows again that $e'_1 + y'e_2 = e_1 + ye_2$. Thus, if we write $-V$ with respect to the basis (e_1, e_2) , it still has the above structure. Therefore we may assume that $e_1 = e'_1$ and $y = y'$. Therefore it follows that

$$U = (e_1 + ye_2)^{n_1-1} e_2^{n_2-2} U'' \text{ and } V = (-e_1 - ye_2)^{n_1-1} (-e_2)^{n_2-2} V'',$$

a contradiction to $|S| = |U| - 3$.

CASE 1.4.3: $v = n_2 - 3$.

Note that

$$|X_1 X_2 X_3| = |U_1| = |U| - v + (n_2 - v) = n_1 + n_2 - 1 + n_2 - (2n_2 - 6) = n_1 + 5.$$

Suppose that U' divides a product of two of the X_1, X_2, X_3 , say $U' | X_1 X_2$. Then $X_3 | (U')^{-1} U_1$ and hence $|X_3| = n_1$. Thus $|X_1 X_2| = 5$ and either X_1 or X_2 has length two. Since X_3 divides $(U')^{-1} U_1$, it follows that $-X_3$ divides $V_1(V')^{-1}$. After considering a new factorization of V_1 if necessary we may suppose without restriction that $Y_3 = -X_3$. Arguing as above we infer that Y_1 or Y_2 has length two, a contradiction to the earlier mentioned fact that not both, U_1 and V_1 are divisible by an atom of length two.

Thus from now on we may assume that for every $X \in \mathcal{A}(G)$ dividing U_1 we have $|\gcd(X, U')| = 1$, and for every $Y \in \mathcal{A}(G)$ dividing V_1 we have $|\gcd(Y, V')| = 1$. Arguing as at the beginning of CASE 1.3.2 we obtain that $\mathbf{h}(U) = n_2 - 3$ or $\mathbf{h}(V) = n_2 - 3$, say $\mathbf{h}(U) = n_2 - 3$. By Corollary 4.3, we infer that

$$U = (e_1 + ye_2)^{n_1-1} e_2^{n_2-3} \prod_{\nu=1}^3 (-x_\nu e_1 + (-x_\nu y + 1)e_2),$$

with all parameters as described there. Since $|S| = |U| - 3$, it follows that $(e_1 + ye_2)^{n_1-4} | (-V)$ and thus

$$V = (-e_1 - ye_2)^{n_1-4} (-e_2)^{n_2-3} V'' \text{ where } V'' \in \mathcal{F}(G) \text{ with } |V''| = 6.$$

Since

$$U_1 = (-e_2)^3 (e_1 + ye_2)^{n_1-1} \prod_{\nu=1}^3 (-x_\nu e_1 + (-x_\nu y + 1)e_2) = X_1 X_2 X_3,$$

it follows that $(-e_2) | X_\nu$ for each $\nu \in [1, 3]$. Since $(e_1 + ye_2)^{n_1-1} (-e_2)^3$ is zero-sum free, each of the X_ν is divisible by at least one of the elements from $\prod_{\nu=1}^3 (-x_\nu e_1 + (-x_\nu y + 1)e_2)$. Thus, after renumbering if necessary, it follows that for each $\nu \in [1, 3]$

$$X_\nu = (-e_2)(-x_\nu e_1 + (-x_\nu y + 1)e_2)(e_1 + ye_2)^{x_\nu}.$$

This implies that $x_1 + x_2 + x_3 = n_1 - 1$. Since $|\gcd(X_\nu, U')| = 1$ for each $\nu \in [1, 3]$, it follows that $U' = \prod_{\nu=1}^3 (-x_\nu e_1 + (-x_\nu y + 1)e_2)$, and hence

$$V = (-e_1 - ye_2)^{n_1-1} (-e_2)^{n_2-3} V'.$$

Since

$$V_1 = e_2^3 (-e_1 - ye_2)^{n_1-1} V' = Y_1 Y_2 Y_3,$$

it follows that $e_2 \mid Y_\nu$ for each $\nu \in [1, 3]$. Since $(-e_1 - ye_2)^{n_1-1} e_2^3$ is zero-sum free, each of the Y_ν is divisible by at least one of the elements from V' . Setting $h_3 = -g_1 - g_2$ and renumbering if necessary, it follows that for each $\nu \in [1, 3]$

$$Y_\nu = e_2 h_\nu (-e_1 - ye_2)^{y_\nu},$$

where $y_1, y_2, y_3 \in \mathbb{N}_0$ with $y_1 + y_2 + y_3 = n_1 - 1$. For each $\nu \in [1, 3]$ it follows that $h_\nu = y_\nu e_1 + (yy_\nu - 1)e_2$. Therefore we obtain that

$$\begin{aligned} 0 &= g_1 + g_2 + h_3 = \left(-x_1 e_1 + (-x_1 y + 1)e_2 \right) + \left(-x_2 e_1 + (-x_2 y + 1)e_2 \right) + \left(y_3 e_1 + (yy_3 - 1)e_2 \right) \\ &= \left(-x_1 - x_2 + y_3 \right) e_1 + \left((-x_1 - x_2 + y_3)y + 1 \right) e_2, \end{aligned}$$

a contradiction, as not both, $-x_1 - x_2 + y_3$ and $(-x_1 - x_2 + y_3)y + 1$, can be multiples of n_1 .

CASE 1.4.4: $v = n_2 - 4$.

Then $X_4 \mid (U')^{-1}U_1$ and hence $|X_4| = n_1$. Since

$$|X_1 X_2 X_3 X_4| = |U_1| = |U| - v + (n_2 - v) = n_1 + 7,$$

it follows that $|X_1 X_2 X_3| = 7$, and hence X_1, X_2 , or X_3 has length two. Similarly, we obtain that Y_1, Y_2 , or Y_3 has length two, a contradiction to the earlier mentioned fact that not both, U_1 and V_1 are divisible by an atom of length two.

CASE 1.4.5: $v \leq n_2 - 5$.

Then $Y_4 Y_5 \mid (V')^{-1}V_1$, and since $|Y_4| \neq 2 \neq |Y_5|$, we infer that $|Y_4| = |Y_5| = n_1$. Thus $(-Y_4)(-Y_5) \mid (U')^{-1}U_1$ and $Y_4(-Y_4)Y_5(-Y_5) \mid S(-S)$, a contradiction to **A2**.

CASE 2: $h(S) < n_2/2$.

We distinguish two subcases, depending on the parity of n_2 .

CASE 2.1: n_2 is odd.

Since n_2 is odd, we have $3n_1 \leq n_2$ and $n_1 \geq 7$. We write $S = \prod_{\nu=1}^k a_\nu^{\alpha_\nu}$ with $a_1, \dots, a_k \in G$ pairwise distinct and $\alpha_1 \geq \dots \geq \alpha_k \geq 1$. Since $|S| = \sum_{\nu=1}^k \alpha_\nu \geq n_2 + n_1 - 4$ and $\alpha_1 \leq (n_2 - 1)/2$, it follows that $k \geq 3$. We define $T_1 = S(a_1 a_2 a_3)^{-1}$ and set $T_1 = \prod_{i=1}^l b_i^{\beta_i}$ with $b_1, \dots, b_l \in G$ pairwise distinct and $\beta_1 \geq \dots \geq \beta_l \geq 1$. Since $\beta_1 \leq \alpha_1 \leq (n_2 - 1)/2$, $\sum_{i=1}^l \beta_i = |S| - 3 \geq n_2 + n_1 - 7$, and $n_2 - 1 < n_1 + n_2 - 7$, it follows that $l \geq 3$. Applying Lemma 4.5 (with parameters $t = l$, $\alpha = |T_1|$, $\alpha'_1 = \dots = \alpha'_t = 0$ and $\alpha_1 = \dots = \alpha_t = (n_2 - 1)/2$; note that we have $s + 1 = 3$) we infer that

$$\begin{aligned} \prod_{\nu=1}^l (1 + \beta_\nu) &\geq \left(1 + \frac{n_2 - 1}{2} \right)^2 (1 + (|T_1| - (n_2 - 1))) \\ &\geq \left(1 + \frac{n_2 - 1}{2} \right)^2 (1 + 1) = \frac{n_2^2 + 2n_2 + 1}{2} > n_1 n_2. \end{aligned}$$

Thus Lemma 4.4 implies that there is a $W_1 \in \mathcal{A}(G)$ with $|W_1| \geq 3$ such that $(-W_1)W_1 \mid (-T_1)T_1$. Since $|W_1| < |U|$, **A1** implies that $W_1 = n_1$. We write $W_1 = W'_1(-W''_1)$ with $W'_1 W''_1 \mid T_1$.

We define $T_2 = S(W'_1 W''_1)^{-1}$ and note that $(-S)S = W_1(-W_1)T_2(-T_2)$. Furthermore,

$$|T_2| = |S| - n_1 \geq n_2 - 4 \quad \text{and} \quad |\text{supp}(T_2)| \geq 3.$$

We set $T_2 = \prod_{\nu=1}^m c_\nu^{\gamma_\nu}$ with $c_1, \dots, c_m \in G$ pairwise distinct and $\gamma_1 \geq \dots \geq \gamma_m \geq 1$. Applying Lemma 4.5 (with parameters $t = m$, $\alpha = |T_2|$, $\alpha'_1 = \dots = \alpha'_3 = 1$, $\alpha'_4 = \dots = \alpha'_t = 0$ and $\alpha_1 = \dots = \alpha_t = (n_2 - 1)/2$;

note that we have $s + 1 = 3$) we infer that

$$\begin{aligned} \prod_{\nu=1}^m (1 + \gamma_\nu) &\geq \left(1 + \frac{n_2 - 1}{2}\right) \left(1 + |T_2| - \left(\frac{n_2 - 1}{2} + 1\right)\right) (1 + 1) \\ &= \frac{n_2 + 1}{2} \frac{n_2 - 7}{2} 2 = \frac{1}{2} (n_2^2 - 6n_2 - 7) > n_1 n_2. \end{aligned}$$

Thus Lemma 4.4 implies that there is a $W_2 \in \mathcal{A}(G)$ with $|W_2| \geq 3$ such that $(-W_2)W_2 \mid (-T_2)T_2$. Since $|W_2| < |U|$, **A1** implies that $W_2 = n_1$. Therefore we obtain that $W_1(-W_1)W_2(-W_2) \mid (-S)S$, a contradiction to **A2**.

CASE 2.2: n_2 is even.

We distinguish three cases; the first one is that $|U| = |V| = n_1 + n_2 - 2$ and the two others deal with the case $|U| = n_1 + n_2 - 2$, further distinguishing based on the description recalled in Lemma 4.2.

CASE 2.2.1: $|U| = |V| = n_1 + n_2 - 2$.

First we handle the case $n_2 > 12$. The special case $n_2 = 12$ will follow by the same strategy but the details will be different.

We write $S = \prod_{\nu=1}^k a_\nu^{\alpha_\nu}$ with $\alpha_1 \geq \dots \geq \alpha_k$. Since $\sum_{\nu=1}^k \alpha_\nu = n_2 + n_1 - 2$ and $\alpha_1 \leq (n_2 - 2)/2$, it follows that $k \geq 3$.

We define $T_1 = \prod_{\nu=1}^l b_\nu^{\beta_\nu}$ with $\beta_1 \geq \dots \geq \beta_l$ to be a subsequence of S of length $n_2 - 2$ such that $\beta_2 \leq n_2/2 - 3$ and such that $T_1^{-1}S$ contains at least 4 distinct elements or 3 elements with multiplicity at least 2. Applying Lemma 4.5 (with parameters $t = l$, $\alpha = |T_1| = n_2 - 2$, $\alpha'_1 = \dots = \alpha'_t = 0$, and $\alpha_1 = (n_2 - 2)/2$, $\alpha_2 = \dots = \alpha_t = (n_2 - 6)/2$; note that we have $s + 1 = 3$) we infer that

$$\prod_{\nu=1}^l (1 + \beta_\nu) \geq \left(1 + \frac{n_2 - 2}{2}\right) \left(1 + \frac{n_2 - 6}{2}\right) (1 + 2) = 3 \left(\frac{n_2^2}{4} - n_2\right) > n_1 n_2,$$

where the last inequality holds because $n_2 > 12$. Thus Lemma 4.4 implies that there is a $W_1 \in \mathcal{A}(G)$ with $|W_1| \geq 3$ such that $(-W_1)W_1 \mid (-T_1)T_1$. Since $|W_1| < |U|$, **A2** implies that $|W_1| = n_1$. We write $W_1 = W'_1(-W''_1)$ with $W'_1 W''_1 \mid T_1$.

We define $T_2 = S(W'_1 W''_1)^{-1} = \prod_{\nu=1}^m c_\nu^{\gamma_\nu}$ with $\gamma_1 \geq \dots \geq \gamma_m$. We note that $T_1^{-1}S \mid T_2$, $(-S)S = W_1(-W_1)T_2(-T_2)$, and $|T_2| = n_2 - 2$. By construction of $T_1^{-1}S$, we obtain that either $(\gamma_3 \geq 2)$ or $(\gamma_3 \geq 1$ and $\gamma_4 \geq 1)$. Applying Lemma 4.5 (with parameters $t = m$, $\alpha = |T_2|$, $\alpha_1 = \dots = \alpha_t = (n_2 - 2)/2$, and either $(\alpha'_1 = \dots = \alpha'_3 = 2, \alpha'_4 = \dots = \alpha'_t = 0)$ or $(\alpha'_1 = \dots = \alpha'_4 = 1, \alpha'_5 = \dots = \alpha'_t = 0)$) we infer that either

$$\prod_{\nu=1}^m (1 + \gamma_\nu) \geq \left(1 + \frac{n_2}{2} - 1\right) \left(1 + (|T_2| - \left(\frac{n_2}{2} - 1\right) - 2)\right) (1 + 2) = \frac{n_2}{2} \left(\frac{n_2}{2} - 2\right) 3 > n_1 n_2,$$

or

$$\prod_{\nu=1}^m (1 + \gamma_\nu) \geq \left(1 + \frac{n_2}{2} - 1\right) \left(1 + |T_2| - \left(\frac{n_2}{2} - 1\right) - 2\right) (1 + 1)(1 + 1) = \frac{n_2}{2} \left(\frac{n_2}{2} - 2\right) 4 > n_1 n_2.$$

Thus Lemma 4.4 implies that there is a $W_2 \in \mathcal{A}(G)$ with $|W_2| \geq 3$ such that $(-W_2)W_2 \mid (-T_2)T_2$. Since $|W_2| < |U|$, **A1** implies that $|W_2| = n_1$. Therefore we obtain that $W_1(-W_1)W_2(-W_2) \mid (-S)S$, a contradiction to **A2**.

Now suppose that $n_2 = 12$. Then $n_1 = 6$ and $|S| = 16$. Again we set $S = \prod_{\nu=1}^k a_\nu^{\alpha_\nu}$ with $\alpha_1 \geq \dots \geq \alpha_k$. Since $h(S) \leq 5$, we infer that $k \geq 4$. We define $T_1 = S(a_1 a_2 a_3 a_4)^{-1}$ and set $T_1 = \prod_{\nu=1}^l b_\nu^{\beta_\nu}$ with $\beta_1 \geq \dots \geq \beta_l$. Observe that $\beta_1 \leq 4$. Applying Lemma 4.5 (with parameters $t = l$, $\alpha = |T_1| = 12$,

$\alpha'_1 = \dots = \alpha'_t = 0$, and $\alpha_1 = \dots = \alpha_t = 4$) we infer that

$$\prod_{\nu=1}^l (1 + \beta_\nu) \geq (1 + 4)^3 > n_1 n_2.$$

Thus Lemma 4.4 implies that there is a $W_1 \in \mathcal{A}(G)$ with $|W_1| \geq 3$ such that $(-W_1)W_1 \mid (-T_1)T_1$. Since $|W_1| < |U|$, **A1** implies that $|W_1| = n_1 = 6$. We write $W_1 = W'_1(-W''_1)$ with $W'_1 W''_1 \mid T_1$.

We define $T_2 = S(W'_1 W''_1)^{-1} = \prod_{\nu=1}^m c_\nu^{\gamma_\nu}$ with $\gamma_1 \geq \dots \geq \gamma_m$. We note that $|T_2| = n_2 - 2 = 10$ and $m \geq 4$. Applying Lemma 4.5 (with parameters $t = m$, $\alpha = |T_2| = 10$, $\alpha'_1 = \dots = \alpha'_4 = 1$, $\alpha'_5 = \dots = \alpha'_t = 0$, and $\alpha_1 = \dots = \alpha_t = 5$) we infer that

$$\prod_{\nu=1}^m (1 + \gamma_\nu) \geq (1 + 5)(1 + 3)(1 + 1)(1 + 1) > n_1 n_2,$$

and we obtain a contradiction as above.

CASE 2.2.2: U is of type I, as given in Lemma 4.2.

Then

$$\frac{n_2}{2} - 1 \geq h(S) \geq h(U) - 3 \geq \text{ord}(e_j) - 4,$$

which implies that $\text{ord}(e_j) = n_1$ so $j = 1$. We assert that

$$v_{e_1}(UV) + v_{-e_1}(UV) \geq n_1 + 1.$$

If this holds, then Lemma 5.2 in [13] implies that $L(UV) \cap [3, n_1] \neq \emptyset$, a contradiction. Since $v_{-e_1}(V) \geq v_{-e_1}(-S) \geq v_{e_1}(U) - 3$, we obtain that

$$v_{e_1}(UV) + v_{-e_1}(UV) \geq (n_1 - 1) + (n_1 - 1) - 3 = 2n_1 - 5 \geq n_1 + 1.$$

CASE 2.2.3: U is of type II, as given in Lemma 4.2.

We observe that

$$\frac{n_2}{2} - 1 \geq h(S) \geq h(U) - 3 = \max\{sn_1 - 1, n_2 - sn_1 + \epsilon\} - 3.$$

This implies that $s = \frac{n_2}{2n_1}$, hence $v_{e_2}(U) = \frac{n_2}{2} + \epsilon$. Thus $\epsilon \in [1, 2]$ and $e_2^{\epsilon+1} \mid U'$.

Assume to the contrary that $U' = g_1 g_2 (-h_1 - h_2) = e_2^3$. Then $V' = (-2e_2)h_1 h_2$, $|V| = D(G)$, and

$$v_{-e_2}(V) \geq v_{-e_2}(-S) = v_{e_2}(S) = v_{e_2}(U) - 3 \geq \frac{n_2}{2} + \epsilon - 3.$$

Thus $v_{-e_2}(V) \geq 1$, which implies that $V^* = (-2e_2)^{-1}(-e_2)^2 V \in \mathcal{A}(G)$, but $|V^*| = |V| + 1 = D(G) + 1$, a contradiction.

Since $\epsilon = 2$ implies that $U' = e_2^3$, we obtain that $\epsilon = 1$, $v_{e_2}(U') = 2$, $v_{-e_2}(V') = 0$, and

$$v_{-e_2}(V) = v_{-e_2}(-S) = v_{e_2}(S) = v_{e_2}(U) - 2 = \frac{n_2}{2} - 1.$$

We consider

$$U_1 = e_2^{-v_{e_2}(U)} (-e_2)^{v_{-e_2}(V)} U \quad \text{and} \quad V_1 = (-e_2)^{-v_{-e_2}(V)} e_2^{v_{e_2}(U)} V.$$

Neither U_1 nor V_1 is divisible by an atom of length 2, and since $|V_1| = |V| + 2 > D(G)$, $V_1 \notin \mathcal{A}(G)$. Therefore we obtain that

$$2 < \max L(U_1) + \max L(V_1) \leq \frac{|U_1|}{3} + \frac{|V_1|}{3} = \frac{|UV|}{3} \leq \frac{2n_1 + 2n_2 - 2}{3} < n_2,$$

a contradiction. $\square$

5. CHARACTERIZATION OF THE SYSTEM $\mathcal{L}(C_{n_1} \oplus C_{n_2})$

In this section we prove Theorem 1.1. We start with two propositions which gather various special cases which have been settled before. The first groups, for which the Characterization Problem has been solved, are cyclic groups and elementary 2-groups ([10]). We use the characterization of groups $C_n \oplus C_n$ ([32]) and [5]). The core of this section is Proposition 5.5.

Proposition 5.1. *Let G be an abelian group such that $\mathcal{L}(G) = \mathcal{L}(C_{n_1} \oplus C_{n_2})$ where $n_1, n_2 \in \mathbb{N}$ with $n_1 \mid n_2$ and $n_1 + n_2 > 4$. Then G is finite, and we have*

1. $d(G) = d(C_{n_1} \oplus C_{n_2}) = n_1 + n_2 - 2$ and $\exp(G) = n_2$;
2. If $n_1 = n_2$, then $G \cong C_{n_1} \oplus C_{n_2}$.

Proof. 1. The finiteness of G and the equality of the Davenport constants follows from [15, Proposition 7.3.1]. The statement on the exponents follows from [36, Proposition 5.2] or from [5, Proposition 5.4].

2. This follows from [32, Theorem 4.1]. $\square$

Proposition 5.2. *Let $n_1, n_2 \in \mathbb{N}$ with $n_1 \mid n_2$ and $n_1 + n_2 > 4$, and let $G = H \oplus C_{n_2}$ where $H \subset G$ is a subgroup with $\exp(H) \mid n_2$. Suppose that $\mathcal{L}(G) = \mathcal{L}(C_{n_1} \oplus C_{n_2})$.*

1. $d(H) \leq n_1 - 1$, and if $d^*(H) = n_1 - 1$, then $d(G) = d^*(G)$.
2. If $d(G) = d^*(G)$, then $G \cong C_{n_1} \oplus C_{n_2}$.
3. If $n_1 \in [1, 5]$, then $G \cong C_{n_1} \oplus C_{n_2}$.

Proof. 1. Proposition 5.1 implies that

$$n_1 + n_2 - 2 = d(G) \geq d(H) + (n_2 - 1) \quad \text{and hence} \quad d(H) \leq n_1 - 1.$$

If $d^*(H) = n_1 - 1$, then

$$n_1 + n_2 - 2 = d(G) \geq d^*(G) = d^*(H) + (n_2 - 1) = n_1 + n_2 - 2.$$

2. This follows from [5, Theorem 5.6].

3. By 2., it is sufficient to show that $d(G) = d^*(G)$. Suppose that H is cyclic. Then $r(G) \leq 2$ and Proposition 2.2 implies that $d(G) = d^*(G)$. Suppose that H is noncyclic. Then $2 \leq r(H) \leq d(H) \leq n_1 - 1$, and hence $n_1 \in [3, 5]$. Suppose that $n_1 = 3$. Then $d(H) = 2$ and $H \cong C_2 \oplus C_2$. Thus $d^*(H) = 2 = n_1 - 1$, and the assertion follows from 1. Suppose that $n_1 = 4$. Then $d(H) \in [2, 3]$ and H is isomorphic to $C_2 \oplus C_2$ or to C_2^3 . If $H \cong C_2^3$, then $d^*(H) = n_1 - 1$, and the assertion follows from 1. Suppose that $H \cong C_2 \oplus C_2$ and set $n_2 = 2m$. If m is even, then $d(G) = d^*(G)$ by [11, Corollary 4.2.13]. If m is odd, then $d(G) = d^*(G)$ by [36, Theorem 3.13]. Suppose that $n_1 = 5$. Then $d(H) \in [2, 4]$ and H is isomorphic to one of the following groups: $C_2^2, C_2^3, C_2^4, C_2 \oplus C_4, C_3 \oplus C_3$. If H is isomorphic to one of the groups in $\{C_2^4, C_2 \oplus C_4, C_3 \oplus C_3\}$, then $d^*(H) = n_1 - 1$. If $H \cong C_2 \oplus C_2$, then $d(G) = d^*(G)$ as outlined above. Suppose that $H \cong C_2^3$. Then $G = C_2^3 \oplus C_{n_2}$ and we set $n_2 = 2m$. If m is even, then again [11, Corollary 4.2.13] implies that $d(G) = d^*(G)$. If m is odd, then this follows from [1]. $\square$

We need the following characterization of decomposable subsets.

Lemma 5.3. *Let G be a finite abelian group and $G_0 \subset G$ a subset.*

1. *The following statements are equivalent.*
 - (a) G_0 is decomposable.
 - (b) There are nonempty subsets $G_1, G_2 \subset G_0$ such that $G_0 = G_1 \uplus G_2$ and $\mathcal{B}(G_0) = \mathcal{B}(G_1) \times \mathcal{B}(G_2)$.
 - (c) There are nonempty subsets $G_1, G_2 \subset G_0$ such that $G_0 = G_1 \uplus G_2$ and $\mathcal{A}(G_0) = \mathcal{A}(G_1) \uplus \mathcal{A}(G_2)$.
 - (d) There are nonempty subsets $G_1, G_2 \subset G_0$ such that $\langle G_0 \rangle = \langle G_1 \rangle \oplus \langle G_2 \rangle$.

2. There exist a uniquely determined $t \in \mathbb{N}$ and (up to order) uniquely determined nonempty indecomposable sets $G_1, \dots, G_t \subset G_0$ such that

$$G_0 = \biguplus_{\nu=1}^t G_\nu \quad \text{and} \quad \langle G_0 \rangle = \bigoplus_{\nu=1}^t \langle G_\nu \rangle.$$

Proof. For 1. see [30, Lemma 3.7] and [2, Lemma 3.2], and for 2. we refer to [30, Proposition 3.10]. $\square$

We need the invariant

$$\mathfrak{m}(G) = \max\{\min \Delta(G_0) \mid G_0 \subset G \text{ is a non-half-factorial subset with } k(A) \geq 1 \text{ for all } A \in \mathcal{A}(G_0)\}.$$

Lemma 5.4. *Let G be a finite abelian group, $G_0 \subset G$ a subset with $\min \Delta(G_0) = \max \Delta^*(G)$, and let $G_0 = \biguplus_{\nu=1}^t G_\nu$ be the decomposition into indecomposable components. If $\exp(G) > \mathfrak{m}(G) + 2$, then each component G_ν is either half-factorial or equal to $\{-g_\nu, g_\nu\}$ for some $g_\nu \in G$ with $\text{ord}(g_\nu) = \exp(G)$. Moreover, at least one of the components G_ν is not half-factorial.*

Proof. See [31, Corollary 5.2]. $\square$

Proposition 5.5. *Let $n_1, n_2 \in \mathbb{N}$ with $n_1 \mid n_2$ and $6 \leq n_1 < n_2$, and let G be a finite abelian group with $\exp(G) = n_2$ and $\mathfrak{d}(G) = n_1 + n_2 - 2$. Suppose that $\mathcal{L}(G)$ contains, for all $k \in \mathbb{N}$, the sets*

$$L_k = \left\{ (kn_2 + 3) + (n_1 - 2) + (n_2 - 2) \right\} \cup \left\{ (2k + 3) + \{0, n_1 - 2, n_2 - 2\} + \{\nu(n_2 - 2) \mid \nu \in [0, k]\} \right\}.$$

Then G is isomorphic to one of the following groups:

$$C_{n_1} \oplus C_{n_2}, \quad C_2^s \oplus C_{n_2} \text{ with } s \in \{n_1 - 2, n_1 - 1\}, \quad C_2^{n_1-4} \oplus C_4 \oplus C_{n_2}, \quad \text{or } C_2 \oplus C_{n_1-1} \oplus C_{n_2} \text{ with } 2 \mid (n_1 - 1) \mid n_2.$$

Proof. We set $G = H \oplus C_{n_2}$ where $H \subset G$ is a subgroup with $\exp(H) \mid n_2$. If H is cyclic, then $\mathfrak{d}(G) = |H| + n_2 - 2$ whence $|H| = n_1$ and $G \cong C_{n_1} \oplus C_{n_2}$. For the remainder of the proof we suppose that H is non-cyclic. Since $\mathfrak{d}(H) + n_2 - 1 \leq \mathfrak{d}(G) = n_1 + n_2 - 2$, it follows that $\mathfrak{d}(H) \leq n_1 - 1$, and hence $\exp(H) \leq \mathfrak{d}(H) \leq n_1$. Since $\exp(H) = n_1$ would imply that H is cyclic of order n_1 , it follows that $\exp(H) \leq n_1 - 1$. We have $\mathfrak{r}(H) \leq \mathfrak{d}(H) \leq n_1 - 1$. If $\mathfrak{r}(H) = n_1 - 1$, then $H \cong C_2^{n_1-1}$ and hence $G \cong C_2^{n_1-1} \oplus C_{n_2}$. Thus for the remainder of the proof we suppose that $\mathfrak{r}(H) \in [2, n_1 - 2]$.

We start with the following two assertions.

A1. $\exp(G) > \mathfrak{m}(G) + 2$.

A2. Let $G_0 \subset G$ with $\min \Delta(G_0) = n_2 - 2$. Then $G_0 = \{g, -g\} \cup G_1$ where $\text{ord}(g) = n_2$, $G_1 \subset G$ is half-factorial, and $\langle G_1 \rangle \cap \langle g \rangle = \{0\}$.

Proof of A1. Assume to the contrary that $n_2 \leq \mathfrak{m}(G) + 2$. By [32, Proposition 3.6], we have

$$\mathfrak{m}(G) \leq \max\{\mathfrak{r}^*(G) - 1, K(G) - 1\}, \text{ where } K(G) \text{ is the cross number of } G.$$

So $\mathfrak{r}^*(G) \leq \log_2 |G|$, $K(G) \leq \frac{1}{2} + \log |G| \leq \frac{1}{2} + \log_2 |G|$ by [15, Theorem 5.5.5] whence $\mathfrak{m}(G) \leq -\frac{1}{2} + \log_2 |G|$. If $H = C_{m_1} \oplus \dots \oplus C_{m_s}$, with $s = \mathfrak{r}(H) \geq 2$, $m_1, \dots, m_s \in \mathbb{N}$, and $1 < m_1 \mid \dots \mid m_s \mid n_2$, then

$$\log_2 |H| = \sum_{i=1}^s \log_2 m_i \leq \sum_{i=1}^s (m_i - 1) = \mathfrak{d}^*(H) \leq \mathfrak{d}(H).$$

Therefore we obtain that

$$\begin{aligned} n_2 - 2 \leq \mathfrak{m}(G) &\leq -\frac{1}{2} + \log_2 |G| = -\frac{1}{2} + \log_2 n_2 + \log_2 |H| \leq -\frac{1}{2} + \log_2 n_2 + \mathfrak{d}(H) \\ &\leq -\frac{3}{2} + \log_2 n_2 + n_1 \leq -\frac{3}{2} + \log_2 n_2 + \frac{n_2}{2} \end{aligned}$$

and hence

$$\frac{n_2}{2} \leq \log_2 n_2 + \frac{1}{2}, \text{ a contradiction to } n_2 \geq 7. \quad \square(\text{Proof of A1})$$

Proof of A2. By Lemma 5.3, G_0 has a decomposition into indecomposable subsets, say $G_0 = \cup_{\nu=1}^t G_\nu$. Proposition 3.2.2 implies that $\max \Delta^*(G) = n_2 - 2 = \min \Delta(G_0)$. By A1 and Lemma 5.4, the sets G_ν have the following structure: there is an $s \in [1, t]$ such that $G_\nu = \{-g_\nu, g_\nu\}$ with $\text{ord}(g_\nu) = n_2$ for each $\nu \in [1, s]$, and $G_{s+1}, \dots, G_t$ are half-factorial. Now it follows that $s = 1$ because, by Lemma 5.3.2,

$$\langle G_0 \rangle = \bigoplus_{\nu=1}^t \langle G_\nu \rangle \subset G = H \oplus C_{n_2} \quad \text{and} \quad \exp(H) < n_2. \quad \square(\text{Proof of A2})$$

By assumption, for every $k \in \mathbb{N}$ the sets $L_k =$

$$\left\{ (kn_2 + 3) + (n_1 - 2) + (n_2 - 2) \right\} \cup \left((2k + 3) + \{0, n_1 - 2, n_2 - 2\} + \{\nu(n_2 - 2) \mid \nu \in [0, k]\} \right) \in \mathcal{L}(G).$$

Clearly, these sets are AAMPs with difference $n_2 - 2$ and period $\{0, n_1 - 2, n_2 - 2\}$ and, for all sufficiently large $k \in \mathbb{N}$, L_k is not an AAMP with some difference d which is not a multiple of $n_2 - 2$ ([15, Theorem 4.2.7]). Let $k \in \mathbb{N}$ be sufficiently large. In the course of the proof we will meet certain bounds and will assume that k exceeds all of them.

We choose $B_k \in \mathcal{B}(G)$ such that $\mathsf{L}(B_k) = L_k$. By [15, Proposition 9.4.9], there exists an $M_1 \in \mathbb{N}$ (not depending on k) such that $B_k = V_k S_k$, where V_k and S_k are zero-sum sequences with the following properties:

$$\min \Delta(\text{supp}(V_k)) = n_2 - 2 \quad \text{and} \quad |S_k| \leq M_1,$$

(indeed in the terminology of [15, Proposition 9.4.9], we have $V_k \in V[\![V]\!]$ and $S_k \in \mathcal{B}(G)[\mathcal{U}, V]$ for a given full almost generating set $\mathcal{U}$; but we do not need these additional properties). By A2, we obtain that

$$\text{supp}(V_k) = \{-g_k, g_k\} \cup A_k, \quad \text{where } \text{ord}(g_k) = n_2 \text{ and } A_k \subset G \text{ is half-factorial with } \langle g_k \rangle \cap \langle A_k \rangle = \{0\}.$$

Since for each two elements $g, g' \in G$ with $\text{ord}(g) = \text{ord}(g') = n_2$, there is a group automorphism $\varphi: G \rightarrow G$ with $\varphi(g) = g'$, and since $\mathsf{L}(B) = \mathsf{L}(\varphi(B))$ for all $B \in \mathcal{B}(G)$, we may assume without restriction that there is a $g \in G$ such that $g_k = g$ for every $k \in \mathbb{N}$. Applying a further automorphism if necessary we may suppose that $G = H \oplus \langle g \rangle$. We will require an additional assertion

A3. There exist a constant $M_2 \in \mathbb{N}$ (not depending on k), $C_k \in \mathcal{B}(\text{supp}(V_k))$, and $D_k \in \mathcal{B}(G^\bullet)$ with the following properties:

- $B_k = C_k D_k$ with $|D_k| \leq M_2$,
- For any factorization $z = W_1 \cdots W_\gamma \in \mathcal{Z}(B_k)$ with $W_1, \dots, W_\gamma \in \mathcal{A}(G)$ there are I, J such that $[1, \gamma] = I \uplus J$, $\prod_{i \in I} W_i = C_k$ and $\prod_{j \in J} W_j = D_k$.

Proof of A3. Let $z = X_1 \cdots X_\alpha Y_1 \cdots Y_\beta$ be a factorization of B_k , where $X_1, \dots, X_\alpha, Y_1, \dots, Y_\beta$ are atoms, and $Y_1, \dots, Y_\beta$ are precisely those atoms which contain some element from S_k . Then $\beta \leq |S_k| \leq M_1$ and $X_1 \cdots X_\alpha$ divides V_k (in $\mathcal{B}(G)$). For any element $a \in \text{supp}(V_k)$ let $m_a(z) \in \mathbb{N}_0$ be maximal such that $a^{\text{ord}(a)m_a(z)}$ divides $X_1 \cdots X_\alpha$. Since $\beta \leq M_1$, there is a constant $M_3(z) \in \mathbb{N}$ (not depending on k) such that $v_a(B_k) - \text{ord}(a)m_a(z) \leq M_3(z)$. Now we define, for each $a \in \text{supp}(V_k)$,

$$m_a = \min\{m_a(z) \mid z \in \mathcal{Z}(B_k)\}, \quad C_k = \prod_{a \in \text{supp}(V_k)} a^{\text{ord}(a)m_a}, \quad \text{and} \quad D_k = C_k^{-1} B_k.$$

Since there is a constant $M_3 \in \mathbb{N}$ (not depending on k) such that $v_a(B_k) - \text{ord}(a)m_a \leq M_3$ for all $a \in \text{supp}(V_k)$, there is a constant $M_2 \in \mathbb{N}$ (not depending on k) such that $|D_k| = |B_k| - |C_k| \leq M_2$. $\square(\text{Proof of A3})$

Since $C_k \in \mathcal{B}(\text{supp}(V_k))$, $\mathsf{L}(C_k)$ is an arithmetical progression with difference $n_2 - 2$ and by A3 we have

$$\mathsf{L}(B_k) = \mathsf{L}(C_k) + \mathsf{L}(D_k) = \bigcup_{m \in \mathsf{L}(D_k)} (m + \mathsf{L}(C_k)).$$

Assume to the contrary that $\mathsf{L}(D_k) = \{m\}$. Then $-m + L_k = -m + \mathsf{L}(B_k) = \mathsf{L}(C_k) \in \mathcal{L}(C_{n_2})$, a contradiction to Proposition 3.5.2. This implies that $|\mathsf{L}(D_k)| > 1$. Since $\text{supp}(C_k) \subset \text{supp}(V_k) \subset \{-g, g\} \cup$

A_k , where A_k is half-factorial and $\langle g \rangle \cap \langle A_k \rangle = \{0\}$, it follows that $C_k = C'_k C''_k$, with $C'_k \in \mathcal{B}(\{g, -g\})$, $C''_k \in \mathcal{B}(A_k)$, $\mathsf{L}(C_k) = \mathsf{L}(C'_k) + \mathsf{L}(C''_k)$, and $|\mathsf{L}(C''_k)| = 1$. Thus, if $\mathsf{L}(C''_k) = \{m_k\}$, then

$$\mathsf{L}(C_k) = \mathsf{L}(C'_k 0^{m_k}) \quad \text{and} \quad \mathsf{L}(B_k) = \mathsf{L}(C_k D_k) = \mathsf{L}(C'_k 0^{m_k} D_k).$$

Therefore, after changing notation if necessary, we suppose from now on that

$$B_k = C_k D_k, \quad \mathsf{L}(B_k) = \mathsf{L}(C_k) + \mathsf{L}(D_k), \quad \text{where } \text{supp}(C_k) \subset \{0, g, -g\} \text{ and } D_k \in \mathcal{B}(G) \text{ with } |D_k| \leq M_2.$$

We continue with the following assertion, whose proof follows from Proposition 3.7.

- A4.** • Let $T \in \mathcal{F}(G)$ with $T \mid D_k$. If $T \in \mathcal{A}(\mathcal{B}_{\langle g \rangle}(G))$, then $\sigma(T) \in \{0, g, -g, (n_1 - 1)g, -(n_1 - 1)g\}$.
 • If $z = T_1 \cdots T_\gamma \in \mathcal{Z}_{\mathcal{B}_{\langle g \rangle}(G)}(D_k)$ with $T_1, \dots, T_\gamma \in \mathcal{A}(\mathcal{B}_{\langle g \rangle}(G))$, then at most one of the elements $\sigma(T_1), \dots, \sigma(T_\gamma)$ does not lie in $\{0, g, -g\}$.

We shall use the following notation. If $z = T_1 \cdots T_\gamma$ is as above, then we set

$$\sigma(z) = \sigma(T_1) \cdots \sigma(T_\gamma) \in \mathcal{F}(\langle g \rangle).$$

We continue with an additional assertion.

A5.

$$\mathsf{L}_{\mathcal{B}(G)}(B_k) = \bigcup_{z \in \mathcal{Z}_{\mathcal{B}_{\langle g \rangle}(G)}(D_k)} \mathsf{L}_{\mathcal{B}(\langle g \rangle)}(C_k \sigma(z)), \quad \text{where the union on}$$

the right hand side consists of at least two distinct sets which are not contained in each other.

Proof of A5. Assume to the contrary that all sets of lengths on the right hand side are contained in one fixed set $L_1 = \mathsf{L}_{\mathcal{B}(\langle g \rangle)}(C_k \sigma(z^*))$ with $z^* \in \mathcal{Z}_{\mathcal{B}_{\langle g \rangle}(G)}(D_k)$. Then $\mathsf{L}(B_k) \in \mathcal{L}(C_{n_2})$, a contradiction to Proposition 3.5. To show that the set on the left side is in the union on the right side, we choose a factorization $z^* = W_1 \cdots W_\gamma \in \mathcal{Z}_{\mathcal{B}(G)}(B_k)$, where $W_1, \dots, W_\gamma \in \mathcal{A}(G)$. For each $\nu \in [1, \gamma]$, we set $W_\nu = X_\nu Y_\nu$ where $X_\nu, Y_\nu \in \mathcal{F}(G)$ such that

$$C_k = X_1 \cdots X_\gamma \quad \text{and} \quad D_k = Y_1 \cdots Y_\gamma.$$

For each $\nu \in [1, \gamma]$, we have $\sigma(W_\nu) = 0 \in G$, hence $\sigma(Y_\nu) = -\sigma(X_\nu) \in \langle g \rangle$, $Y_\nu \in \mathcal{B}_{\langle g \rangle}(G)$, and we choose a factorization $z_\nu \in \mathcal{Z}_{\mathcal{B}_{\langle g \rangle}(G)}(Y_\nu)$. Then

$$z = z_1 \cdots z_\gamma \in \mathcal{Z}_{\mathcal{B}_{\langle g \rangle}(G)}(D_k).$$

Then, for each $\nu \in [1, \gamma]$, $W'_\nu = X_\nu \sigma(z_\nu) \in \mathcal{A}(\langle g \rangle)$ and $W'_1 \cdots W'_\gamma = C_k \sigma(z) \in \mathcal{F}(\langle g \rangle)$. Therefore $z' = W'_1 \cdots W'_\gamma \in \mathcal{Z}_{\mathcal{B}(\langle g \rangle)}(C_k \sigma(z))$ and

$$|z^*| = \gamma = |z'| \in \mathsf{L}_{\mathcal{B}(\langle g \rangle)}(C_k \sigma(z)).$$

Conversely, let $z = S_1 \cdots S_\beta \in \mathcal{Z}_{\mathcal{B}_{\langle g \rangle}(G)}(D_k)$ and $z' = W'_1 \cdots W'_\gamma \in \mathcal{Z}_{\mathcal{B}(\langle g \rangle)}(C_k \sigma(z))$ be given, where $S_1, \dots, S_\beta \in \mathcal{A}(\mathcal{B}_{\langle g \rangle}(G))$, $W'_1, \dots, W'_\gamma \in \mathcal{A}(\langle g \rangle)$, and we write

$$\sigma(z) = s_1 \cdots s_\beta, \quad \text{where } s_1 = \sigma(S_1), \dots, s_\beta = \sigma(S_\beta).$$

Note that $s_1, \dots, s_\beta$ satisfy the properties given in **A4**.

Claim: We can find a renumbering such that

$$W'_\nu = s_\nu T_\nu \quad \text{with} \quad T_\nu \in \mathcal{F}(\{-g, g\}) \quad \text{for all } \nu \in [1, \beta].$$

Proof of the Claim. We proceed in three steps.

First, we may assume without restriction that $s_1 = \dots = s_\delta = 0$ and $0 \notin \{s_{\delta+1}, \dots, s_\beta\}$. Then at least δ of the $W'_1, \dots, W'_\gamma$ are equal to 0. After renumbering if necessary, we may suppose that $W'_1 = \dots = W'_\delta = 0$, and we set $T_1 = \dots = T_\delta = 1 \in \mathcal{F}(\{-g, g\})$.

Second, suppose there is a $\nu \in [\delta+1, \beta]$ such that $s_\nu \in \{(n_1-1)g, n_2-(n_1-1)g\}$, say $\nu = \delta+1$. Then $s_{\delta+1}$ divides (in $\mathcal{F}(G)$) one element of $\{W'_{\delta+1}, \dots, W'_\gamma\}$, say $W'_{\delta+1}$. Then we set $T_{\delta+1} = s_{\delta+1}^{-1} W'_{\delta+1} \in \mathcal{F}(\{-g, g\})$.

To handle the last step, we observe that, by **A4**, all remaining s_ν lie in $\{-g, g\}$. Since $\beta \leq |D_k| \leq M_2$ and the multiplicities of g and of $-g$ in C_k are growing with k , and k is sufficiently large, for each $\nu \leq \beta$ the product $\prod_{\lambda=\nu}^\gamma W'_\lambda$ is divisible by g and by $-g$. Thus we can pick a suitable W'_ν and the assertion follows. $\square$

Now we define

$$W''_\nu = \begin{cases} S_\nu T_\nu & \text{for each } \nu \in [1, \beta], \\ W'_\nu & \text{for each } \nu \in [\beta + 1, \gamma]. \end{cases}$$

Then, by construction, we have $B_k = W''_1 \cdots W''_\gamma$. Let $\nu \in [1, \beta]$. Since $W'_\nu \in \mathcal{A}(\langle g \rangle)$, it follows that $T'_\nu \in \mathcal{F}(\langle g \rangle)$ is zero-sum free. Since $S_\nu \in \mathcal{A}(\mathcal{B}_{\langle g \rangle}(G))$, it follows that $W''_\nu \in \mathcal{A}(G)$. Thus $W''_1, \dots, W''_\beta \in \mathcal{A}(G)$, and we have constructed a factorization of B_k of length $\gamma = |z'|$. $\square$ (Proof of **A5**)

A6. Let

$$z = T_1 \cdots T_\gamma \in \mathcal{Z}_{\mathcal{B}_{\langle g \rangle}(G)}(D_k) \quad \text{and} \quad z' = T'_1 \cdots T'_{\gamma'} \in \mathcal{Z}_{\mathcal{B}_{\langle g \rangle}(G)}(D_k),$$

where $\gamma, \gamma' \in \mathbb{N}$, $T_1, \dots, T_\gamma, T'_1, \dots, T'_{\gamma'} \in \mathcal{A}(\mathcal{B}_{\langle g \rangle}(G))$, and $z \neq z'$. Furthermore, let

$$F = C_k \sigma(T_1) \cdots \sigma(T_\gamma) \in \mathcal{B}(\langle g \rangle) \quad \text{and} \quad F' = C_k \sigma(T'_1) \cdots \sigma(T'_{\gamma'}) \in \mathcal{B}(\langle g \rangle),$$

and define

$$F = SF_1 \text{ and } F' = SF_2, \quad \text{where } S, F_1, F_2 \in \mathcal{F}(\langle g \rangle) \text{ and } S = \gcd_{\mathcal{F}(\langle g \rangle)}(F, F').$$

Then one of the following statements holds:

- (i) $d(z, z') \geq n_1 - 1$.
- (ii) $\{F_1, F_2\} = \{((-g)g)^v, 0^v\}$ with $v \in \mathbb{N}$.

Proof of A6. Note that $\gcd(F_1, F_2) = 1$, $\sigma(F_1) = \sigma(F_2) = -\sigma(S)$, $C_k \mid S$, and

$$(*) \quad d_{\mathcal{B}_{\langle g \rangle}(G)}(z, z') \geq d_{\mathcal{F}(\langle g \rangle)}(F, F') = d_{\mathcal{F}(\langle g \rangle)}(F_1, F_2) = \max\{|F_1|, |F_2|\}.$$

Since $|F| = |C_k| + |z|$, $|F_1| + |S| = |C_k| + |z|$, $|F_2| + |S| = |C_k| + |z'|$, we obtain $|F_2| - |F_1| = |z'| - |z|$ and

$$(**) \quad d(z, z') \geq ||z| - |z'|| + 2 = ||F_1| - |F_2|| + 2.$$

Using $(*)$ and $(**)$ we observe that $\max\{|F_1|, |F_2|\} \geq n_1 - 1$ as well as $||F_1| - |F_2|| \geq n_1 - 3$ implies (i). To simplify the discussion, we suppose that $\max\{|F_1|, |F_2|\} \leq n_1 - 1$ (of course we could also assume that $\max\{|F_1|, |F_2|\} \leq n_1 - 2$; the slightly weaker assumption allows us to give a more complete description of (F_1, F_2) without additional efforts). Based on the structural description of $\sigma(z)$ and $\sigma(z')$ given in **A4** we distinguish four cases.

CASE 1: $\sigma(z)\sigma(z') \in \mathcal{F}(\{0, g, -g\})$.

We set

$$S = (g^{n_2})^{k_1} ((-g)^{n_2})^{k_2} ((-g)g)^{k_3} (\delta g)^{k_4} 0^{k_5},$$

where $\delta \in \{-1, 1\}$, $k_1, \dots, k_5 \in \mathbb{N}_0$ and $k_3 < n_2$. We distinguish two cases.

CASE 1.1: $F_1 = 1$ or $F_2 = 1$, say $F_2 = 1$.

Then $\sigma(S) = 0$, $\sigma(F_1) = 0$, and $k_4 = 0$. We have $F_1 = 0^{\mathbf{v}_0(F_1)} ((-g)g)^{\mathbf{v}_g(F_1)}$ and $|F_1| > 0$. Then $\min L(SF_2) = \min L(S) = k_1 + k_2 + k_3 + k_5$ and $\min L(SF_1) = k_1 + k_2 + k_3 + k_5 + \mathbf{v}_0(F_1) + \mathbf{v}_g(F_1) - \epsilon(n_2 - 2)$ where

$$\epsilon = \begin{cases} 0 & k_3 + \mathbf{v}_g(F_1) < n_2 \\ 1 & \text{otherwise} \end{cases}.$$

Thus $\mathbf{v}_0(F_1) + \mathbf{v}_g(F_1)$ is congruent to $\min L(SF_1) - \min L(SF_2)$ modulo $n_2 - 2$ and hence congruent either to 0 or to $n_1 - 2$ or to $(n_2 - 2) - (n_1 - 2) = n_2 - n_1$ modulo $n_2 - 2$. Since $0 < |F_1| = \mathbf{v}_0(F_1) + 2\mathbf{v}_g(F_1) \leq n_1 - 1$, it follows that $(\mathbf{v}_0(F_1), \mathbf{v}_g(F_1)) \in \{(n_1 - 2, 0), \{n_1 - 3, 1\}\}$, hence $|F_1| - |F_2| = |F_1| \geq n_1 - 2$, and thus (i) holds.

CASE 1.2: $F_1 \neq 1$ and $F_2 \neq 1$.

By symmetry we may suppose that $0 \nmid F_1$. Then $g \mid F_1$ or $(-g) \mid F_1$, and by symmetry we may suppose that $g \mid F_1$. We distinguish two cases.

CASE 1.2.1: $(-g) \mid F_1$.

Then $F_2 = 0^{v_0(F_2)}$, and hence $\sigma(S) = 0 = \sigma(F_1)$. This implies $k_4 = 0$ and $F_1 = ((-g)g)^{v_g(F_1)}$. Then

$$\min L(SF_2) = k_1 + k_2 + k_3 + v_0(F_2) + k_5 \quad \text{and} \quad \min L(SF_1) = k_1 + k_2 + k_3 + v_g(F_1) - \epsilon(n_2 - 2) + k_5$$

where $\epsilon \in \{0, 1\}$. Thus $v_0(F_2) - v_g(F_1)$ is congruent to $\min L(SF_1) - \min L(SF_2)$ modulo $n_2 - 2$ and hence congruent either to 0 or to $n_1 - 2$ or to $n_2 - n_1$ modulo $n_2 - 2$. This implies that either

$$v_0(F_2) = v_g(F_1) \quad \text{or} \quad v_0(F_2) = v_g(F_1) + n_1 - 2 \quad \text{or} \quad v_g(F_1) = v_0(F_2) + n_1 - 2.$$

If $v_0(F_2) = v_g(F_1) + n_1 - 2$, then $v_g(F_1) \geq 1$ implies that $|F_2| \geq v_0(F_2) \geq n_1 - 1$, and hence (i) holds.

If $v_g(F_1) = v_0(F_2) + n_1 - 2$, then $v_0(F_2) \geq 1$ implies that $v_g(F_1) \geq n_1 - 1$ whence $|F_1| = 2v_g(F_1) \geq 2(n_1 - 1) > n_1$, a contradiction. If $v_0(F_2) = v_g(F_1)$, then (ii) holds.

CASE 1.2.2: $(-g) \nmid F_1$.

Then $F_1 = g^{v_g(F_1)}$ and $F_2 = (-g)^{v_{-g}(F_2)} 0^{v_0(F_2)}$. Note that $v_g(F_1) + v_{-g}(F_2) > 0$, $v_g(F_1), v_{-g}(F_2) \in [0, n_1 - 1]$, and $n_2 \geq 2n_1$. However, $\sigma(F_1) = \sigma(F_2)$ implies that $v_g(F_1) + v_{-g}(F_2) \equiv 0 \pmod{n_2}$, a contradiction.

CASE 2: $\sigma(z)\sigma(z') \in ((n_1 - 1)g)\mathcal{F}(\{0, -g, g\})$ or $\sigma(z)\sigma(z') \in (-(n_1 - 1)g)\mathcal{F}(\{0, -g, g\})$.

After applying the group automorphism which sends each $h \in G$ onto its negative, if necessary, we may suppose that $\sigma(z)\sigma(z') \in ((n_1 - 1)g)\mathcal{F}(\{0, -g, g\})$. After exchanging z and z' , if necessary, we may suppose that $\sigma(z) \in \mathcal{F}(\{0, -g, g\})$ and $\sigma(z') \in ((n_1 - 1)g)\mathcal{F}(\{0, -g, g\})$. We set

$$S = (g^{n_2})^{k_1} ((-g)^{n_2})^{k_2} ((-g)g)^{k_3} (\delta g)^{k_4} 0^{k_5},$$

where $\delta \in \{-1, 1\}$, $k_1, \dots, k_5 \in \mathbb{N}_0$ and $k_3 < n_2$. If $\sigma(F_1) = 0$, then $\sigma(F_2) = 0$ and hence $|F_2| \geq n_1$, a contradiction. Thus it follows that $\sigma(F_1) \neq 0$, and hence there are the following three cases.

CASE 2.1: $g \mid F_1$ and $(-g) \mid F_1$.

It follows that $F_2 = ((n_1 - 1)g)0^{v_0(F_2)}$ and hence $\sigma(F_2) = (n_1 - 1)g = \sigma(F_1) = (v_g(F_1) - v_{-g}(F_1))g$, a contradiction to $|F_1| \leq n_1 - 1$.

CASE 2.2: $g \mid F_1$ and $(-g) \nmid F_1$.

Then $F_1 = g^{v_g(F_1)} 0^{v_0(F_1)}$, $F_2 = ((n_1 - 1)g)(-g)^{n_1 - 1 - v_g(F_1)} 0^{v_0(F_2)}$, and we can write SF_1 and SF_2 as follows:

$$\begin{aligned} SF_1 &= (g^{n_2})^{l_1} ((-g)^{n_2})^{l_2} ((-g)g)^{l_3} 0^{l_4 + v_0(F_1)} \\ SF_2 &= (g^{n_2})^{l_1} ((-g)^{n_2})^{l_2} ((-g)g)^{l_3 - v_g(F_1)} 0^{l_4 + v_0(F_2)} \left(((n_1 - 1)g)(-g)^{n_1 - 1} \right) \end{aligned}$$

where $l_1, \dots, l_4 \in \mathbb{N}_0$, $l_4 = v_0(S)$, and $l_3 \geq v_g(F_1)$ (the last inequality holds because k is large enough). Therefore

$$m_1 = l_1 + l_2 + l_3 + l_4 + v_0(F_1) \in L_k \quad \text{and} \quad m_2 = l_1 + l_2 + l_3 - v_g(F_1) + l_4 + v_0(F_2) + 1 \in L_k$$

which implies that $m_1 - m_2 = v_0(F_1) + v_g(F_1) - v_0(F_2) - 1$ is congruent to either 0 or to $n_1 - 2$ or to $n_2 - n_1$ modulo $n_2 - 2$. We distinguish three cases.

CASE 2.2.1: $v_0(F_1) + v_g(F_1) \equiv v_0(F_2) + 1 \pmod{n_2 - 2}$.

Since $|F_1| < n_1$ and $|F_2| < n_1$, it follows that $v_0(F_1) + v_g(F_1) = v_0(F_2) + 1$. Since

$$|F_2| = v_0(F_2) + 1 + (n_1 - 1 - v_g(F_1)) = v_0(F_1) + v_g(F_1) + (n_1 - 1 - v_g(F_1)) = n_1 - 1 + v_0(F_1),$$

it follows that $|F_2| \geq n_1 - 1$ and hence (i) holds.

CASE 2.2.2: $v_0(F_1) + v_g(F_1) \equiv v_0(F_2) + n_1 - 1 \pmod{n_2 - 2}$.

Similarly, we obtain that $v_0(F_1) + v_g(F_1) = v_0(F_2) + n_1 - 1$. Thus $|F_1| \geq n_1 - 1$ and hence (i) holds.

CASE 2.2.3: $v_0(F_1) + v_g(F_1) \equiv n_2 - n_1 + v_0(F_2) + 1 \pmod{n_2 - 2}$.

We obtain that $v_0(F_1) + v_g(F_1) = -(n_1 - 3) + v_0(F_2)$ which implies that $v_0(F_2) > n_1 - 3$. Therefore $|F_2| = v_0(F_2) + 1 + n_1 - 1 - v_g(F_1) = n_1 + v_0(F_1) + (n_1 - 3) - v_0(F_2) + v_0(F_2) = 2n_1 - 3 + v_0(F_1) \geq n_1$, a contradiction.

CASE 2.3: $g \nmid F_1$ and $(-g) \mid F_1$.

Then

$$F_1 = (-g)^{v_{-g}(F_1)} 0^{v_0(F_1)} \quad \text{and} \quad F_2 = ((n_1 - 1)g) g^{n_2 - (n_1 - 1) - v_{-g}(F_1)} 0^{v_0(F_2)}.$$

We can write SF_1 and SF_2 as

$$\begin{aligned} SF_1 &= (g^{n_2})^{l_1} ((-g)^{n_2})^{l_2} ((-g)g)^{l_3} 0^{l_4 + v_0(F_1)} \quad \text{and} \\ SF_2 &= (g^{n_2})^{l_1} ((-g)^{n_2})^{l_2} ((-g)g)^{l_3 - v_{-g}(F_1)} 0^{l_4 + v_0(F_2)} (g^{n_2 - (n_1 - 1)} ((n_1 - 1)g)) \end{aligned}$$

where $l_1, \dots, l_4 \in \mathbb{N}_0$, $l_4 = v_0(S)$, and $l_3 \geq v_{-g}(F_1)$ (the last inequality holds because k is large enough). Therefore

$$m_1 = l_1 + l_2 + l_3 + l_4 + v_0(F_1) \in L_k \quad \text{and} \quad m_2 = l_1 + l_2 + l_3 - v_{-g}(F_1) + l_4 + v_0(F_2) + 1 \in L_k.$$

which implies that $m_1 - m_2 = v_0(F_1) + v_{-g}(F_1) - v_0(F_2) - 1$ is congruent to either 0 or to $n_1 - 2$ or to $n_2 - n_1$ modulo $n_2 - 2$. We distinguish three cases.

CASE 2.3.1: $v_0(F_1) + v_{-g}(F_1) \equiv v_0(F_2) + 1 \pmod{n_2 - 2}$.

We obtain that $v_0(F_1) + v_{-g}(F_1) = v_0(F_2) + 1$ and hence

$$|F_2| = 1 + v_0(F_2) + n_2 - (n_1 - 1) - v_{-g}(F_1) = v_0(F_1) + n_2 - (n_1 - 1) \geq n_1, \quad \text{a contradiction.}$$

CASE 2.3.2: $v_0(F_1) + v_{-g}(F_1) \equiv v_0(F_2) + n_1 - 1 \pmod{n_2 - 2}$.

We obtain that $v_0(F_1) + v_{-g}(F_1) = v_0(F_2) + n_1 - 1$. Therefore $|F_1| \geq n_1 - 1$ and hence (i) holds.

CASE 2.3.3: $v_0(F_1) + v_{-g}(F_1) \equiv n_2 - n_1 + v_0(F_2) + 1 \pmod{n_2 - 2}$.

We obtain that $v_0(F_1) + v_{-g}(F_1) = v_0(F_2) - n_1 + 3$ and therefore

$|F_2| = v_0(F_2) + 1 + n_2 - (n_1 - 1) - v_{-g}(F_1) = v_0(F_1) + n_1 - 3 + 1 + n_2 - (n_1 - 1) = v_0(F_1) - 1 + n_2 \geq n_1$, a contradiction.

CASE 3: $\sigma(z)\sigma(z') \in ((n_1 - 1)g)^2 \mathcal{F}(\{0, -g, g\})$ or $\sigma(z)\sigma(z') \in (-(n_1 - 1)g)^2 \mathcal{F}(\{0, -g, g\})$.

After applying the group automorphism which sends each $h \in G$ onto its negative, if necessary, we may suppose that $\sigma(z)\sigma(z') \in ((n_1 - 1)g)^2 \mathcal{F}(\{0, -g, g\})$, whence $\sigma(z) \in ((n_1 - 1)g) \mathcal{F}(\{0, -g, g\})$ and $\sigma(z') \in ((n_1 - 1)g) \mathcal{F}(\{0, -g, g\})$.

We set

$$S = ((n_1 - 1)g) (g^{n_2})^{k_1} ((-g)^{n_2})^{k_2} ((-g)g)^{k_3} (\delta g)^{k_4} 0^{k_5},$$

where $\delta \in \{-1, 1\}$, $k_1, \dots, k_5 \in \mathbb{N}_0$ and $k_3 < n_2$. We distinguish two cases.

CASE 3.1: $F_1 = 1$ or $F_2 = 1$, say $F_2 = 1$.

Since $F_2 = 1$, it follows that $L(S) \subset L_k$. Let $l_1 \in L(F_1)$. Then $l_1 + L(S) \subset L_k$ and hence l_1 is congruent either to 0 or to $n_1 - 2$ or to $n_2 - n_1$ modulo $n_2 - 2$. Since $l_1 > 0$, it follows that $|F_1| - |F_2| = |F_1| \geq n_1 - 2$, and hence (i) holds.

CASE 3.2: $F_1 \neq 1$ and $F_2 \neq 1$.

We have $0 \nmid F_1$ or $0 \nmid F_2$, say $0 \nmid F_1$. Then $g \mid F_1$ or $(-g) \mid F_1$. We distinguish three cases.

CASE 3.2.1: $g \mid F_1$ and $(-g) \nmid F_1$.

Then $F_1 = g^{v_g(F_1)}$ and $F_2 = (-g)^{v_{-g}(F_2)} 0^{v_0(F_2)}$. Since $\sigma(F_1) = \sigma(F_2)$, it follows that $v_g(F_1) + v_{-g}(F_2) \equiv 0 \pmod{n_2}$, and hence

$$\max\{v_g(F_1), v_{-g}(F_2)\} \geq \frac{n_2}{2} \geq n_1,$$

a contradiction.

CASE 3.2.2: $g \mid F_1$ and $(-g) \mid F_1$.

Then $(-g)g \mid F_1$ whence $F_2 = 0^{\mathbf{v}_0(F_2)}$. This implies that $0 = \sigma(F_2) = \sigma(F_1)$ and thus $F_1 = ((-g)g)^{\mathbf{v}_g(F_1)}$. As above it follows that $\mathbf{v}_g(F_1) - \mathbf{v}_0(F_2)$ is congruent either to 0 or to $n_1 - 2$ or to $n_2 - n_1$ modulo $n_2 - 2$.

If $\mathbf{v}_g(F_1) = \mathbf{v}_0(F_2)$, then (ii) holds.

If $\mathbf{v}_g(F_1) = \mathbf{v}_0(F_2) + n_1 - 2$, then $|F_1| = 2\mathbf{v}_g(F_1) \geq 2n_1 - 4 \geq n_1$, a contradiction.

Suppose that $\mathbf{v}_g(F_1) - \mathbf{v}_0(F_2) \equiv n_2 - n_1 \pmod{n_2 - 2}$. Then $|F_1| < n_1$ implies that $\mathbf{v}_g(F_1) - \mathbf{v}_0(F_2) = -n_1 + 2$. Since $\mathbf{v}_g(F_1) \geq 1$, it follows that $|F_2| \geq \mathbf{v}_0(F_2) \geq n_1 - 1$, and hence (i) holds.

CASE 3.2.3: $g \nmid F_1$ and $(-g) \mid F_1$.

Then $F_1 = (-g)^{\mathbf{v}_{-g}(F_1)}$ and $F_2 = g^{\mathbf{v}_g(F_2)} 0^{\mathbf{v}_0(F_2)}$. Since $\sigma(F_1) = \sigma(F_2)$, it follows that $\mathbf{v}_{-g}(F_1) + \mathbf{v}_g(F_2) \equiv 0 \pmod{n_2}$, and hence

$$\max\{\mathbf{v}_{-g}(F_1), \mathbf{v}_g(F_2)\} \geq \frac{n_2}{2} \geq n_1,$$

a contradiction.

CASE 4: $\sigma(z)\sigma(z') \in ((n_1 - 1)g)(-(n_1 - 1)g)\mathcal{F}(\{0, -g, g\})$.

After exchanging z and z' if necessary we may suppose that $\sigma(z) \in ((n_1 - 1)g)\mathcal{F}(\{0, -g, g\})$ and $\sigma(z') \in (-(n_1 - 1)g)\mathcal{F}(\{0, -g, g\})$. We set

$$SF_1 = (g^{n_2})^{l_1} ((-g)^{n_2})^{l_2} ((g(-g))^{l_3} ((n_1 - 1)g(-g)^{n_1-1}) 0^{l_4 + \mathbf{v}_0(F_1)})$$

and

$$SF_2 = (g^{n_2})^{l'_1} ((-g)^{n_2})^{l'_2} ((g(-g))^{l'_3} ((-(n_1 - 1)g)g^{n_1-1}) 0^{l_4 + \mathbf{v}_0(F_2)})$$

where $l_1, l'_1, \dots, l_3, l'_3, l_4 \in \mathbb{N}_0$. Since

$$F_1 = ((n_1 - 1)g)g^{\mathbf{v}_g(F_1)}(-g)^{\mathbf{v}_{-g}(F_1)}0^{\mathbf{v}_0(F_1)} \quad \text{and} \quad F_2 = (-(n_1 - 1)g)g^{\mathbf{v}_g(F_2)}(-g)^{\mathbf{v}_{-g}(F_2)}0^{\mathbf{v}_0(F_2)},$$

it follows that

$$(n_1 - 1 + \mathbf{v}_g(F_1) - \mathbf{v}_{-g}(F_1))g = \sigma(F_1) = \sigma(F_2) = (-n_1 + 1 + \mathbf{v}_g(F_2) - \mathbf{v}_{-g}(F_2))g$$

and hence

$$2n_1 - 2 \equiv (\mathbf{v}_g(F_2) - \mathbf{v}_g(F_1)) + (\mathbf{v}_{-g}(F_1) - \mathbf{v}_{-g}(F_2)) \pmod{n_2}.$$

We distinguish four cases.

CASE 4.1: $g \mid F_1$ and $(-g) \mid F_1$.

Then $\mathbf{v}_g(F_2) = 0 = \mathbf{v}_{-g}(F_2)$ and hence

$$2n_1 - 2 \equiv -\mathbf{v}_g(F_1) + \mathbf{v}_{-g}(F_1) \pmod{n_2}.$$

If $n_2 \geq 3n_1$, then $|F_1| \geq n_1$, a contradiction. Thus $n_2 = 2n_1$, $\mathbf{v}_{-g}(F_1) + 2 \equiv \mathbf{v}_g(F_1) \pmod{n_2}$, and so $\mathbf{v}_{-g}(F_1) + 2 = \mathbf{v}_g(F_1)$. Therefore we obtain that

$$SF_2 = (g^{n_2})^{l_1} ((-g)^{n_2})^{l_2} ((g(-g))^{l_3 - \mathbf{v}_g(F_1) - (n_1 - 1)} (-g)^{n_2} ((-(n_1 - 1)g)g^{n_1-1}) 0^{l_4 + \mathbf{v}_0(F_2)})$$

Therefore

$m_1 = l_1 + l_2 + l_3 + l_4 + 1 + \mathbf{v}_0(F_1) \in L_k$ and $m_2 = l_1 + l_2 + l_3 + l_4 - (\mathbf{v}_g(F_1) + n_1 - 1) + 2 + \mathbf{v}_0(F_2) \in L_k$ which implies that $m_1 - m_2 = \mathbf{v}_0(F_1) - \mathbf{v}_0(F_2) + \mathbf{v}_g(F_1) + n_1 - 2$ is congruent to either 0 or to $n_1 - 2$ or to $n_2 - n_1$ modulo $n_2 - 2$. We distinguish three cases.

CASE 4.1.1: $\mathbf{v}_0(F_1) + \mathbf{v}_g(F_1) + n_1 \equiv \mathbf{v}_0(F_2) + 2 \pmod{n_2 - 2}$.

The left and the right hand side cannot be equal, since $\mathbf{v}_g(F_1) \geq 2$ would imply that $|F_2| \geq \mathbf{v}_0(F_2) \geq n_1$. Therefore we have

$$\mathbf{v}_0(F_1) + \mathbf{v}_g(F_1) + n_1 = \mathbf{v}_0(F_2) + n_2$$

and thus $|F_1| \geq \mathbf{v}_0(F_1) + \mathbf{v}_g(F_1) \geq n_2 - n_1 = n_1$, a contradiction.

CASE 4.1.2: $\mathbf{v}_0(F_1) + \mathbf{v}_g(F_1) + n_1 \equiv \mathbf{v}_0(F_2) + n_1 \pmod{n_2 - 2}$.

This implies that $\mathbf{v}_0(F_1) + \mathbf{v}_g(F_1) = \mathbf{v}_0(F_2)$ whence $\mathbf{v}_0(F_2) \geq \mathbf{v}_g(F_1) \geq 2$, $\mathbf{v}_0(F_1) = 0$, and $\mathbf{v}_g(F_1) = \mathbf{v}_0(F_2)$. Therefore we obtain $F_1 = ((n_1 - 1)g)g^{\mathbf{v}_0(F_2)}(-g)^{\mathbf{v}_0(F_2)-2}$ and $F_2 = (-(n_1 - 1)g)0^{\mathbf{v}_0(F_2)}$. Now consider a factorization z_1 of SF_1 which is divisible by the atom $X = ((n_1 - 1)g)g^{n_1+1}$ and by $(g(-g))^{\mathbf{v}_0(F_2)-2}$. It gives rise to a factorization

$$z_2 = z_1 X^{-1} (g(-g))^{-(\mathbf{v}_0(F_2)-2)} \left((-(n_1 - 1)g)g^{n_1-1} \right) 0^{\mathbf{v}_0(F_2)} \in Z(SF_2)$$

of length $|z_2| = |z_1| - (1 + \mathbf{v}_0(F_2) - 2) + 1 + \mathbf{v}_0(F_2) = |z_1| + 2$. Since $n_1 \geq 5$ and $\min \Delta(L_k) = \min\{n_1 - 2, n_2 - n_1\} \geq 3$, L_k cannot contain the lengths $|z_1|$ and $|z_1| + 2 = |z_2|$, a contradiction.

CASE 4.1.3: $\mathbf{v}_0(F_1) + \mathbf{v}_g(F_1) \equiv \mathbf{v}_0(F_2) + 2 \pmod{n_2 - 2}$.

This implies that $\mathbf{v}_0(F_1) + \mathbf{v}_g(F_1) = \mathbf{v}_0(F_2) + 2$. Since $\mathbf{v}_g(F_1) \geq 3$, it follows that $\mathbf{v}_0(F_2) > 0$ and hence $\mathbf{v}_0(F_1) = 0$. Therefore we obtain $F_1 = ((n_1 - 1)g)g^{\mathbf{v}_0(F_2)+2}(-g)^{\mathbf{v}_0(F_2)}$ and $F_2 = (-(n_1 - 1)g)0^{\mathbf{v}_0(F_2)}$. Now consider a factorization z_2 of SF_2 which is divisible by the atom $X = (-(n_1 - 1)g)(-g)^{n_1+1}$. It gives rise to a factorization

$$z_1 = z_2 X^{-1} 0^{-\mathbf{v}_0(F_2)} ((n_1 - 1)g(-g)^{n_1-1}) ((-g)g)^{\mathbf{v}_0(F_2)+2}$$

of length $|z_1| = |z_2| + 2$, a contradiction.

CASE 4.2: $g \mid F_1$ and $(-g) \nmid F_1$.

Then $\mathbf{v}_g(F_2) = 0 = \mathbf{v}_{-g}(F_1)$, hence

$$n_2 - 2n_1 + 2 \equiv \mathbf{v}_g(F_1) + \mathbf{v}_{-g}(F_2) \pmod{n_2}$$

and thus $n_2 - 2n_1 + 2 = \mathbf{v}_g(F_1) + \mathbf{v}_{-g}(F_2)$. Furthermore, we obtain that

$$\max\{\mathbf{v}_g(F_1), \mathbf{v}_{-g}(F_2)\} \geq \frac{n_2 - 2n_1 + 2}{2},$$

and hence $n_2 \in \{2n_1, 3n_2\}$. We obtain that

$$SF_2 = (g^{n_2})^{l_1} ((-g)^{n_2})^{l_2} ((g(-g))^{l_3 - \mathbf{v}_g(F_1) - (n_1 - 1)} (-g)^{n_2} ((-(n_1 - 1)g)g^{n_1-1}) 0^{l_4 + \mathbf{v}_0(F_2)})$$

Therefore $m_1 = l_1 + l_2 + l_3 + l_4 + 1 + \mathbf{v}_0(F_1) \in L_k$ and

$$m_2 = l_1 + l_2 + l_3 + l_4 - (\mathbf{v}_g(F_1) + n_1 - 1) + 2 + \mathbf{v}_0(F_2) \in L_k$$

which implies that $m_1 - m_2 = \mathbf{v}_0(F_1) - \mathbf{v}_0(F_2) + \mathbf{v}_g(F_1) + n_1 - 2$ is congruent to either 0 or to $n_1 - 2$ or to $n_2 - n_1$ modulo $n_2 - 2$. We distinguish three cases.

CASE 4.2.1: $\mathbf{v}_0(F_1) + \mathbf{v}_g(F_1) + n_1 \equiv \mathbf{v}_0(F_2) + 2 \pmod{n_2 - 2}$.

The left and the right hand side cannot be equal, because otherwise we would have $|F_2| \geq \mathbf{v}_0(F_2) + 1 \geq n_1$. Therefore we have

$$\mathbf{v}_0(F_1) + \mathbf{v}_g(F_1) + n_1 = \mathbf{v}_0(F_2) + n_2$$

and thus $|F_1| \geq \mathbf{v}_0(F_1) + \mathbf{v}_g(F_1) \geq n_2 - n_1 \geq n_1$, a contradiction.

CASE 4.2.2: $\mathbf{v}_0(F_1) + \mathbf{v}_g(F_1) + n_1 \equiv \mathbf{v}_0(F_2) + n_1 \pmod{n_2 - 2}$.

This implies that $\mathbf{v}_0(F_1) + \mathbf{v}_g(F_1) = \mathbf{v}_0(F_2)$ whence $\mathbf{v}_0(F_2) \geq \mathbf{v}_g(F_1) \geq 1$, $\mathbf{v}_0(F_1) = 0$, and $\mathbf{v}_g(F_1) = \mathbf{v}_0(F_2)$. Therefore we obtain $F_1 = ((n_1 - 1)g)g^{\mathbf{v}_0(F_2)}$ and $F_2 = (-(n_1 - 1)g)(-g)^{n_2 - 2n_1 + 2 - \mathbf{v}_0(F_2)} 0^{\mathbf{v}_0(F_2)}$ and hence $|F_2| = 1 + n_2 - 2n_1 + 2$ which implies that $n_2 = 2n_1$ and $|F_2| = 3$. Thus $\mathbf{v}_0(F_2) \in \{1, 2\}$.

Suppose that $\mathbf{v}_0(F_2) = 1$. Then $\mathbf{v}_g(F_1) = 1$, $F_1 = ((n_1 - 1)g)g$, and $F_2 = (-(n_1 - 1)g)(-g)0$. Consider a factorization z_1 of SF_1 divisible by $X = ((n_1 - 1)g)g^{n_1+1}$. This gives rise to a factorization

$$z_2 = z_1 X^{-1} 0((-g)g) \left((-(n_1 - 1)g)g^{n_1-1} \right)$$

of length $|z_2| = |z_1| + 2$, a contradiction.

Suppose that $\mathbf{v}_0(F_2) = 2$. Then $\mathbf{v}_g(F_1) = 2$, $F_1 = ((n_1 - 1)g)g^2$, and $F_2 = (-(n_1 - 1)g)0^2$. Consider a factorization z_1 of SF_1 divisible by $X = ((n_1 - 1)g)g^{n_1+1}$. This gives rise to a factorization

$$z_2 = z_1 X^{-1} 0^2 \left((-(n_1 - 1)g)g^{n_1-1} \right)$$

of length $|z_2| = |z_1| + 2$, a contradiction.

CASE 4.2.3: $\mathbf{v}_0(F_1) + \mathbf{v}_g(F_1) \equiv \mathbf{v}_0(F_2) + n_2 - 2n_1 + 2 \pmod{n_2 - 2}$.

Suppose that $n_2 = 3n_1$. Then $\mathbf{v}_0(F_1) + \mathbf{v}_g(F_1) \equiv \mathbf{v}_0(F_2) + n_1 + 2 \pmod{n_2 - 2}$, and equality cannot hold because $|F_1| \geq \mathbf{v}_0(F_1) + \mathbf{v}_g(F_1)$. This implies that $(n_2 - 2) + \mathbf{v}_0(F_1) + \mathbf{v}_g(F_1) = \mathbf{v}_0(F_2) + n_1 + 2$ and hence $2n_1 - 4 + \mathbf{v}_0(F_1) + \mathbf{v}_g(F_1) = \mathbf{v}_0(F_2)$, a contradiction to $\mathbf{v}_0(F_2) \leq |F_2| \leq n_1 - 1$.

This implies that $n_2 = 2n_1$ and $\mathbf{v}_0(F_1) + \mathbf{v}_g(F_1) = \mathbf{v}_0(F_2) + 2$. Since $2 = \mathbf{v}_g(F_1) + \mathbf{v}_{-g}(F_2)$, we infer that $\mathbf{v}_g(F_1) \in [1, 2]$.

Suppose $\mathbf{v}_g(F_1) = 2$. Then $\mathbf{v}_{-g}(F_2) = 0$ and $\mathbf{v}_0(F_1) = \mathbf{v}_0(F_2) = 0$, and we have $F_1 = ((n_1 - 1)g)g^2$ and $F_2 = (-(n_1 - 1)g)$. Consider a factorization z_2 of SF_2 containing the atom $X = (-(n_1 - 1)g)(-g)^{n_1+1}$. This gives rise to a factorization

$$z_1 = z_2 X^{-1} \left(((n_1 - 1)g)(-g)^{n_1-1} \right) ((-g)g)^2$$

of length $|z_1| = |z_2| + 2$, a contradiction.

Suppose $\mathbf{v}_g(F_1) = 1$. Then $\mathbf{v}_{-g}(F_2) = 1$, $\mathbf{v}_0(F_1) = 1$, $\mathbf{v}_0(F_2) = 0$, and we have $F_1 = ((n_1 - 1)g)g0$ and $F_2 = (-(n_1 - 1)g)(-g)$. Consider a factorization z_2 of SF_2 containing the atom $X = (-(n_1 - 1)g)(-g)^{n_1+1}$. This gives rise to a factorization

$$z_1 = z_2 X^{-1} \left(((n_1 - 1)g)(-g)^{n_1-1} \right) ((-g)g)0$$

of length $|z_1| = |z_2| + 2$, a contradiction.

CASE 4.3: $g \nmid F_1$ and $(-g) \mid F_1$.

Then $\mathbf{v}_g(F_1) = 0$ and $\mathbf{v}_{-g}(F_2) = 0$ and hence

$$2n_1 - 2 \equiv \mathbf{v}_g(F_2) + \mathbf{v}_{-g}(F_1) \pmod{n_2}.$$

This implies that $\mathbf{v}_g(F_2) = \mathbf{v}_{-g}(F_1) = n_1 - 1$ and hence $|F_1| \geq n_1$ and $|F_2| \geq n_1$, a contradiction.

CASE 4.4: $g \nmid F_1$ and $(-g) \nmid F_1$.

Then $\mathbf{v}_g(F_1) = 0 = \mathbf{v}_{-g}(F_1)$ and hence

$$2n_1 - 2 \equiv \mathbf{v}_g(F_2) - \mathbf{v}_{-g}(F_2) \pmod{n_2}.$$

If $n_2 \geq 3n_1$, then $|F_2| \geq n_1$, a contradiction. Thus $n_2 = 2n_1$ and hence $\mathbf{v}_g(F_2) = \mathbf{v}_{-g}(F_2) - 2$. Therefore we obtain that

$$SF_2 = (g^{n_2})^{l_1} ((-g)^{n_2})^{l_2} ((g(-g))^{l_3 + \mathbf{v}_g(F_2) - (n_1 - 1)} (-g)^{n_2} (((-n_1 + 1)g)g^{n_1-1}) 0^{l_4 + \mathbf{v}_0(F_2)})$$

Therefore

$$m_1 = l_1 + l_2 + l_3 + l_4 + 1 + \mathbf{v}_0(F_1) \in L_k$$

and

$$m_2 = l_1 + l_2 + l_3 + l_4 + \mathbf{v}_g(F_2) - (n_1 - 1) + 2 + \mathbf{v}_0(F_2) \in L_k$$

which implies that $m_1 - m_2 = \mathbf{v}_0(F_1) - \mathbf{v}_0(F_2) - \mathbf{v}_g(F_2) + (n_1 - 1) - 1$ is congruent to either 0 or to $n_1 - 2$ or to $n_2 - n_1$ modulo $n_2 - 2$. We distinguish three cases.

CASE 4.4.1: $\mathbf{v}_0(F_2) + \mathbf{v}_g(F_2) \equiv \mathbf{v}_0(F_1) + n_1 - 2 \pmod{n_2 - 2}$.

This implies that $\mathbf{v}_0(F_2) + \mathbf{v}_g(F_2) = \mathbf{v}_0(F_1) + n_1 - 2$, and hence $|F_2| \geq \mathbf{v}_{-g}(F_2) \geq \mathbf{v}_g(F_2) + 2 \geq n_1$, a contradiction.

CASE 4.4.2: $\mathbf{v}_0(F_2) + \mathbf{v}_g(F_2) + (n_1 - 2) \equiv \mathbf{v}_0(F_1) + n_1 - 2 \pmod{n_2 - 2}$.

This implies that $v_0(F_2) + v_g(F_2) = v_0(F_1)$ and hence $v_0(F_2) = 0$. Therefore we obtain that $F_1 = ((n_1 - 1)g)0^{v_0(F_1)}$ and $F_2 = (- (n_1 - 1)g)g^{v_0(F_1)+2}$. Now consider a factorization z_1 of SF_1 containing the atom $X = ((n_1 - 1)g)g^{n_1+1}$. This gives rise to a factorization

$$z_2 = z_1 X^{-1} \left((- (n_1 - 1)g)g^{n_1-1} \right) ((-g)g)^{v_0(F_1)+2} 0^{-v_0(F_1)}$$

of length $|z_2| = |z_1| + 2$, a contradiction.

CASE 4.4.3: $v_0(F_2) + v_g(F_2) + (n_2 - n_1) \equiv v_0(F_1) + n_1 - 2 \pmod{n_2 - 2}$.

Since $n_2 = 2n_1$, the congruence simplifies to $v_0(F_2) + v_g(F_2) + 2 \equiv v_0(F_1) \pmod{n_2 - 2}$ which implies that $v_0(F_2) + v_g(F_2) + 2 = v_0(F_1)$. Thus $v_0(F_2) = 0$, $F_1 = ((n_1 - 1)g)0^{v_0(F_1)}$, and $F_2 = (- (n_1 - 1)g)g^{v_0(F_1)-2}(-g)^{v_0(F_1)}$. Now consider a factorization z_1 of SF_1 containing the atom $X = ((n_1 - 1)g)(-g)^{n_1-1}$. This gives rise to a factorization

$$z_2 = z_1 X^{-1} \left((- (n_1 - 1)g)(-g)^{n_1+1} \right) ((-g)g)^{v_0(F_1)-2} 0^{-v_0(F_1)}$$

of length $|z_2| = |z_1| - 2$, a contradiction. □(Proof of **A6**)

We state the final assertion

A7. $n_1 - 1 \leq c_{\mathcal{B}_{\langle g \rangle}(G)}(D_k)$.

Proof of A7. By **A5**, we have

$$\mathcal{L}_{\mathcal{B}(G)}(B_k) = \bigcup_{z \in \mathcal{Z}_{\mathcal{B}_{\langle g \rangle}(G)}(D_k)} \mathcal{L}_{\mathcal{B}(\langle g \rangle)}(C_k \sigma(z)),$$

and the union on the right hand side consists of at least two distinct sets which are not contained in each other. Assume to the contrary that $c_{\mathcal{B}_{\langle g \rangle}(G)}(D_k) \leq n_1 - 2$ and choose a factorization $z_0 \in \mathcal{Z}_{\mathcal{B}_{\langle g \rangle}(G)}(D_k)$.

We assert that for each $z \in \mathcal{Z}_{\mathcal{B}_{\langle g \rangle}(G)}(D_k)$ there exists an $l(z) \in \mathbb{Z}$ such that $\sigma(z) = \sigma(z_0)0^{-l(z)}((-g)g)^{l(z)}$. Let $z \in \mathcal{Z}_{\mathcal{B}_{\langle g \rangle}(G)}(D_k)$ be given, and let $z_0, \dots, z_k = z$ be an $(n_1 - 2)$ -chain of factorizations concatenating z_0 and z . Since $d(z_{i-1}, z_i) < n_1 - 1$, it follows that the pair (z_{i-1}, z_i) is of type (ii) in **A6** for each $i \in [1, k]$. Therefore $\sigma(z_i) = \sigma(z_{i-1})0^{-l_i}((-g)g)^{l_i}$ for some $l_i \in \mathbb{Z}$ and each $i \in [1, k]$, and hence the assertion follows with $l(z) = l_1 + \dots + l_k$.

We choose a factorization $z^* \in \mathcal{Z}_{\mathcal{B}_{\langle g \rangle}(G)}(D_k)$ such that

$$l(z^*) = \max\{l(z) \mid z \in \mathcal{Z}_{\mathcal{B}_{\langle g \rangle}(G)}(D_k)\},$$

and assert that

$$\mathcal{L}_{\mathcal{B}(\langle g \rangle)}(C_k \sigma(z)) \subset \mathcal{L}_{\mathcal{B}(\langle g \rangle)}(C_k \sigma(z^*)) \quad \text{for each } z \in \mathcal{Z}_{\mathcal{B}_{\langle g \rangle}(G)}(D_k).$$

Let $z \in \mathcal{Z}_{\mathcal{B}_{\langle g \rangle}(G)}(D_k)$ be given. Then $\sigma(z^*) = \sigma(z)0^{-(l(z^*)-l(z))}((-g)g)^{l(z^*)-l(z)}$. If

$$y \in \mathcal{L}_{\mathcal{B}(\langle g \rangle)}(C_k \sigma(z)), \quad \text{then } y0^{-(l(z^*)-l(z))}((-g)g)^{l(z^*)-l(z)} \in \mathcal{L}_{\mathcal{B}(\langle g \rangle)}(C_k \sigma(z^*))$$

is a factorization of length $|y|$, and hence $\mathcal{L}_{\mathcal{B}(\langle g \rangle)}(C_k \sigma(z)) \subset \mathcal{L}_{\mathcal{B}(\langle g \rangle)}(C_k \sigma(z^*))$.

Therefore we obtain that

$$\mathcal{L}_{\mathcal{B}(G)}(B_k) = \bigcup_{z \in \mathcal{Z}_{\mathcal{B}_{\langle g \rangle}(G)}(D_k)} \mathcal{L}_{\mathcal{B}(\langle g \rangle)}(C_k \sigma(z)) = \mathcal{L}(C_k \sigma(z^*)), \quad \text{a contradiction to the fact}$$

that the union consists of least two distinct sets not contained in each other. □(Proof of **A7**)

Using **A7** and Proposition 2.4.2, we infer that

$$n_1 - 1 \leq c_{\mathcal{B}_{\langle g \rangle}(G)}(D_k) \leq c(\mathcal{B}_{\langle g \rangle}(G)) = c(\mathcal{B}(G/\langle g \rangle)) \leq D(G/\langle g \rangle) = D(H) \leq n_1.$$

We distinguish two cases.

CASE 1: $c(\mathcal{B}(G/\langle g \rangle)) = n_1$.

Then $D(G/\langle g \rangle) = n_1$, Proposition 2.3.1 implies that $G/\langle g \rangle$ is either cyclic of order n_1 or an elementary 2-group of rank $n_1 - 1$. Since $H \cong G/\langle g \rangle$, it follows that $G \cong C_{n_1} \oplus C_{n_2}$ or $G \cong C_2^{n_1-1} \oplus C_{n_2}$.

CASE 2: $c(\mathcal{B}(G/\langle g \rangle)) = n_1 - 1$.

We distinguish two cases.

CASE 2.1: $D(G/\langle g \rangle) = n_1$.

Then Proposition 2.3.2 implies that $G/\langle g \rangle$ is isomorphic either to $C_2 \oplus C_{n_1-1}$, where $n_1 - 1$ is even, or to $C_2^{n_1-4} \oplus C_4$. Since $H \cong G/\langle g \rangle$, it follows that $G \cong C_2 \oplus C_{n_1-1} \oplus C_{n_2}$ or $G \cong C_2^{n_1-4} \oplus C_4 \oplus C_{n_2}$.

CASE 2.2: $D(G/\langle g \rangle) = n_1 - 1$.

Then $c(\mathcal{B}(G/\langle g \rangle)) = D(G/\langle g \rangle) = n_1 - 1$, and (again by Proposition 2.3.1) $G/\langle g \rangle$ is cyclic of order $n_1 - 1$ or an elementary 2-group of rank $n_1 - 2$. If $G/\langle g \rangle$ is cyclic, then G has rank two and $d(G) = d(G/\langle g \rangle) + d(\langle g \rangle) = n_1 - 2 + n_2 - 1 < n_1 + n_2 - 2 = d(G)$, a contradiction. Thus $G/\langle g \rangle$ is an elementary 2-group and $G \cong C_2^{n_1-2} \oplus C_{n_2}$. $\square$

Proof of Theorem 1.1. Let G be an abelian group such that $\mathcal{L}(G) = \mathcal{L}(C_{n_1} \oplus C_{n_2})$ where $n_1, n_2 \in \mathbb{N}$ with $n_1 \mid n_2$ and $n_1 + n_2 > 4$.

Proposition 5.1 implies that G is finite with $\exp(G) = n_2$ and $d(G) = d(C_{n_1} \oplus C_{n_2}) = n_1 + n_2 - 2$. If $n_1 = n_2$, then $G \cong C_{n_1} \oplus C_{n_2}$ by Proposition 5.1.2. Thus we may suppose that $n_1 < n_2$, and we set $G = H \oplus C_{n_2}$ where $H \subset G$ is a subgroup with $\exp(H) \mid n_2$. If $n_1 \in [1, 5]$, then the assertion follows from Proposition 5.2.3, and hence we suppose that $n_1 \geq 6$. Since $\mathcal{L}(G) = \mathcal{L}(C_{n_1} \oplus C_{n_2})$, Proposition 3.4 implies that, for each $k \in \mathbb{N}$, the sets

$$L_k = \left\{ (kn_2 + 3) + (n_1 - 2) + (n_2 - 2) \right\} \cup \left((2k + 3) + \{0, n_1 - 2, n_2 - 2\} + \{\nu(n_2 - 2) \mid \nu \in [0, k]\} \right)$$

are in $\mathcal{L}(G)$. Therefore Proposition 5.5 implies that G is isomorphic to one of the following groups

$C_{n_1} \oplus C_{n_2}$, $C_2^s \oplus C_{n_2}$ with $s \in \{n_1 - 2, n_1 - 1\}$, $C_2^{n_1-4} \oplus C_4 \oplus C_{n_2}$, $C_2 \oplus C_{n_1-1} \oplus C_{n_2}$ with $2 \mid (n_1 - 1) \mid n_2$.

Since

$$d^*(C_2^{n_1-4} \oplus C_4 \oplus C_{n_2}) = n_1 + n_2 - 2 = d(G) \quad \text{and} \quad d^*(C_2 \oplus C_{n_1-1} \oplus C_{n_2}) = n_1 + n_2 - 2 = d(G),$$

Proposition 5.2.2 implies that G cannot be isomorphic to any of these two groups. Proposition 3.6 (with $k = 0$, $n = n_2$, and $r = n_1 - 1$) implies that

$$\{2, n_2, n_1 + n_2 - 2\} \in \mathcal{L}(C_2^{n_1-2} \oplus C_{n_2}) \subset \mathcal{L}(C_2^{n_1-1} \oplus C_{n_2}).$$

However, Proposition 4.1 shows that $\{2, n_2, n_1 + n_2 - 2\} \notin \mathcal{L}(C_{n_1} \oplus C_{n_2}) = \mathcal{L}(G)$ whence $G \cong C_{n_1} \oplus C_{n_2}$. $\square$

REFERENCES

- [1] P.C. Baayen, $C_2 \oplus C_2 \oplus C_2 \oplus C_{2n}!$, Reports ZW-1969-006, Math. Centre, Amsterdam, 1969.
- [2] N.R. Baeth and A. Geroldinger, *Monoids of modules and arithmetic of direct-sum decompositions*, Pacific J. Math. **271** (2014), 257 – 319.
- [3] N.R. Baeth and J. Hoffmeier, *Atoms of the relative block monoid*, Involve **2** (2009), 29 – 36.
- [4] N.R. Baeth and R. Wiegand, *Factorization theory and decomposition of modules*, Am. Math. Mon. **120** (2013), 3 – 34.
- [5] P. Baginski, A. Geroldinger, D.J. Gryniewicz, and A. Philipp, *Products of two atoms in Krull monoids and arithmetical characterizations of class groups*, Eur. J. Comb. **34** (2013), 1244 – 1268.
- [6] S.T. Chapman, M. Fontana, A. Geroldinger, and B. Olberding (eds.), *Multiplicative Ideal Theory and Factorization Theory*, Proceedings in Mathematics and Statistics, vol. 170, Springer, 2016.
- [7] W. Gao and A. Geroldinger, *Systems of sets of lengths II*, Abh. Math. Semin. Univ. Hamb. **70** (2000), 31 – 49.
- [8] ———, *On zero-sum sequences in $\mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$* , Integers **3** (2003), Paper A08, 45p.
- [9] W. Gao, A. Geroldinger, and D.J. Gryniewicz, *Inverse zero-sum problems III*, Acta Arith. **141** (2010), 103 – 152.
- [10] A. Geroldinger, *Systeme von Längenmengen*, Abh. Math. Semin. Univ. Hamb. **60** (1990), 115 – 130.
- [11] ———, *Additive group theory and non-unique factorizations*, Combinatorial Number Theory and Additive Group Theory, Advanced Courses in Mathematics CRM Barcelona, Birkhäuser, 2009, pp. 1 – 86.
- [12] ———, *Sets of lengths*, Amer. Math. Monthly **123** (2016), 960 – 988.
- [13] A. Geroldinger, D.J. Gryniewicz, and W.A. Schmid, *The catenary degree of Krull monoids I*, J. Théor. Nombres Bordx. **23** (2011), 137 – 169.

- [14] A. Geroldinger, D.J. Gryniewicz, and P. Yuan, *On products of k atoms II*, Mosc. J. Comb. Number Theory **5** (2015), 73 – 129.
- [15] A. Geroldinger and F. Halter-Koch, *Non-Unique Factorizations. Algebraic, Combinatorial and Analytic Theory*, Pure and Applied Mathematics, vol. 278, Chapman & Hall/CRC, 2006.
- [16] A. Geroldinger, S. Ramacher, and A. Reinhart, *On v -Marot Mori rings and C -rings*, J. Korean Math. Soc. **52** (2015), 1 – 21.
- [17] A. Geroldinger and I. Ruzsa, *Combinatorial Number Theory and Additive Group Theory*, Advanced Courses in Mathematics - CRM Barcelona, Birkhäuser, 2009.
- [18] A. Geroldinger and P. Yuan, *The set of distances in Krull monoids*, Bull. Lond. Math. Soc. **44** (2012), 1203 – 1208.
- [19] A. Geroldinger and Q. Zhong, *The catenary degree of Krull monoids II*, J. Australian Math. Soc. **98** (2015), 324 – 354.
- [20] ———, *The set of minimal distances in Krull monoids*, Acta Arith. **173** (2016), 97 – 120.
- [21] ———, *A characterization of class groups via sets of lengths II*, J. Théor. Nombres Bordx. **29** (2017), 327 – 346.
- [22] D.J. Gryniewicz, *Structural Additive Theory*, Developments in Mathematics 30, Springer, Cham, 2013.
- [23] F. Halter-Koch, *Factorization of algebraic integers*, Grazer Math. Berichte **191** (1983).
- [24] ———, *Relative block semigroups and their arithmetical applications*, Comm. Math. Univ. Carol. **33** (1992), 373 – 381.
- [25] ———, *Ideal Systems. An Introduction to Multiplicative Ideal Theory*, Marcel Dekker, 1998.
- [26] J. Kaczorowski, *A pure arithmetical characterization for certain fields with a given class group*, Colloq. Math. **45** (1981), 327 – 330.
- [27] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, Polish Scientific Publ., 1974.
- [28] C. Reiher, *A proof of the theorem according to which every prime number possesses property B* , PhD Thesis, Rostock, 2010 (2010).
- [29] D.E. Rush, *An arithmetic characterization of algebraic number fields with a given class group*, Math. Proc. Camb. Philos. Soc. **94** (1983), 23 – 28.
- [30] W.A. Schmid, *Arithmetic of block monoids*, Math. Slovaca **54** (2004), 503 – 526.
- [31] ———, *Periods of sets of lengths: a quantitative result and an associated inverse problem*, Colloq. Math. **113** (2008), 33 – 53.
- [32] ———, *Arithmetical characterization of class groups of the form $\mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$ via the system of sets of lengths*, Abh. Math. Semin. Univ. Hamb. **79** (2009), 25 – 35.
- [33] ———, *Characterization of class groups of Krull monoids via their systems of sets of lengths: a status report*, Number Theory and Applications, Hindustan Book Agency, 2009, pp. 189 – 212.
- [34] ———, *A realization theorem for sets of lengths*, J. Number Theory **129** (2009), 990 – 999.
- [35] ———, *Inverse zero-sum problems II*, Acta Arith. **143** (2010), 333 – 343.
- [36] ———, *The inverse problem associated to the Davenport constant for $C_2 \oplus C_2 \oplus C_{2n}$, and applications to the arithmetical characterization of class groups*, Electron. J. Comb. **18(1)** (2011), Research Paper 33.
- [37] Q. Zhong, *A characterization of finite abelian groups via sets of lengths in transfer Krull monoids*, Commun. Algebra **46** (2018), 4021 – 4041.
- [38] ———, *Sets of minimal distances and characterizations of class groups of Krull monoids*, Ramanujan J. **45** (2018), 719 – 737.