ON A PROPERTY OF MINIMAL ZERO-SUM SEQUENCES AND RESTRICTED SUMSETS

WEIDONG GAO AND ALFRED GEROLDINGER

Abstract. Let G be an additively written abelian group and S a sequence in $G \setminus \{0\}$ with length $|S| \ge 4$. Suppose that S is a product of two subsequences, say $S = BC$, such that the element $g+h$ occurs in the sequence S whenever $g \cdot h$ is a subsequence of B or of C. Then S contains a proper zero-sum subsequence, apart from some well-characterized exceptional cases. This result is closely connected with restricted set addition in abelian groups. Moreover, it solves a problem on the structure of minimal zero-sum sequences, which recently occurred in the theory of non-unique factorizations.

1. Introduction and Main Results

Let G be an additively written finite abelian group and $S = \prod_{i=1}^{l} g_i$ a (multiplicatively written, finite) sequence in G. Then S is called a minimal zero-sum sequence, if $\sigma(S) = \sum_{i=1}^{l} g_i = 0$ and $\sum_{i \in I} g_i \ne 0$ for all $\emptyset \ne I \subsetneq [1, l]$. It is still an open problem to determine the maximal possible length $|S| = l$ of a minimal zero-sum sequence S, and only first steps have been made to determine the structure of minimal zero-sum sequences which have maximal possible lengths (cf. [6] for a more detailed description of these problems and an extensive list of recent literature).

In this paper we show that minimal zero-sum sequences are not additively closed (in the sense of Definition 3.4).

Theorem 1.1. *Let G be an abelian group and $S \in \mathcal{F}(G)$ a minimal zero-sum sequence with $|S| \ge 7$. If $S = BC$, where B, C are subsequences of S with $|B| \ge |C| \ge 2$, then either B or C contains a subsequence $T = g \cdot h$ whose sum $\sigma(T) = g + h$ does not occur in S.*

This result answers a question which recently occurred in the theory of non-unique factorizations (cf. [1] and [2] for a survey). Suppose that S is a sequence with sum zero. Then in general, S allows distinct factorizations into products of minimal zero-sum subsequences, say

$$S = U_1 \cdot \ldots \cdot U_k \quad \text{and} \quad S = V_1 \cdot \ldots \cdot V_l$$

where $U_1, \ldots, U_k, V_1, \ldots, V_l$ are minimal zero-sum subsequences of S. It is the central problem of factorization theory to describe the variety of possible distinct factorizations of some given element. More precisely, the above property of minimal zero-sum sequences allows a deeper investigation of catenary degrees in Krull monoids with finite divisor class groups (in particular, in a forthcoming article the present results will be used to sharpen Theorem 3.1 and hence Theorem 4.4 in [8]; cf. also [7], [4]).

We formulate a result which, among others, implies Theorem 1.1.

2000 *Mathematics Subject Classification.* 11B50, 11B75, 11P99.
Key words and phrases. zero-sum sequences, non-unique factorizations, restricted sumsets.
This work was supported by the Austrian Science Fund FWF (Project-Nr. P16770-N12).

Theorem 1.2. *Let G be an abelian group and $S \in \mathcal{F}(G \setminus \{0\})$ a sequence with $|S| \ge 4$. Suppose that $S = BC$ with $B, C \in \mathcal{F}(G)$ and that $\sigma(T) \in \operatorname{supp}(S)$ for all subsequences T of B with $|T| = 2$ and for all subsequences T of C with $|T| = 2$. Then S contains a proper zero-sum subsequence, apart from the following exceptions:*

1. $\min\{|B|, |C|\} = 1$*, say* $|C| = 1$*, and S has one of the following forms:*
   (a) $B = g^k$ *and* $C = 2g$ *for some* $g \in G$ *and* $k \in [3, \operatorname{ord}(g) - 1)$.
   (b) $B = g^k \cdot (2g)$ *and* $C = 3g$ *for some* $g \in G$ *and* $k \in [2, \operatorname{ord}(g) - 4)$.
   (c) $B = g \cdot e \cdot (g + e)$ *and* $C = 2g + e$ *for some* $g, e \in G$ *with* $\operatorname{ord}(e) = 2$ *and* $\operatorname{ord}(g) \ge 5$.
2. $B = g \cdot 9g \cdot 10g$ *and* $C = 11g \cdot 3g \cdot 14g$ *for some* $g \in G$ *with* $\operatorname{ord}(g) = 16$.

Clearly, Theorem 1.2 implies Theorem 1.1. We discuss a further consequence dealing with restricted sumsets. In order to avoid the repetition of the exceptional cases, we formulate it only for the cases $|S| \ge 7$ and $\min\{|B|, |C|\} \ge 2$.

Corollary 1.3. *Let G be an abelian group, $S \subset G \setminus \{0\}$ a finite subset with $|S| \ge 7$ and $S = B \cup C$ a partition with* $\min\{|B|, |C|\} \ge 2$. *If*

$$(B \dotplus B) \;\cup\; (C \dotplus C) \;\subset\; S$$

(the union of the restricted sumsets), then S contains a proper subset which sums to zero (i.e., there are $s_1, \ldots, s_k \in S$ with $k < |S|$ such that $\sum_{i=1}^{k} s_i = 0$).

Obviously, Corollary 1.3 is a special case of Theorem 1.2. On the other hand, Theorem 1.2 can easily be obtained from Corollary 1.3. Indeed, in the course of the proof of Theorem 1.2 the general case of sequences will be reduced to the case of sets which allows us to apply Kneser's Addition Theorem (cf. the proof of Proposition 3.5). Since the conjecture of Erdös-Heilbronn has been solved by Dias da Silva and Hamidoune (cf. [3] and [15, Chapter 3]), restricted sumsets have also been studied in the setting of general finite abelian groups (cf. [12, 13, 14], [10], [5] and the literature cited there). However, up to now there are no analogues of the Theorems of Scherk, Kneser and Kemperman. Since the conjectured analogues (cf. [11], section 4) could give a simpler access to Corollary 1.3, it might in converse turn out that Corollary 1.3 is a useful tool for tackling that conjecture.

2. Preliminaries

Let $\mathbb{N}$ denote the set of positive integers, $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$ and for $a, b \in \mathbb{Z}$ we set

$$[a, b] = \{x \in \mathbb{Z} \mid a \le x \le b\}.$$

For $a \in \mathbb{Z}$ and $b \in \mathbb{Z} \cup \{\infty\}$ let $[a, b) = \{x \in \mathbb{Z} \mid a \le x < b\}$. If A, B are sets, then $A \subset B$ means that A is contained in B but may be equal to B.

Throughout, all abelian groups will be written additively. Let G be an abelian group, $\alpha \in G$ and $A, B \subset G$ non-empty subsets. Then

$$A + B = \{a + b \mid a \in A,\ b \in B\} \subset G$$

denotes their *sumset*, $\alpha + B = \{\alpha\} + B$ and

$$A \dotplus B = \{a + b \mid a \in A,\ b \in B,\ a \ne b\} \subset A + B$$

denotes the *restricted sumset of A and B*. Since $A + B = \bigcup_{a \in A} (a + B)$, we have $|B| = |a + B| \le |A + B|$; if $B < G$ is a subgroup and $|A + B|$ is finite, then $|B|$ divides $|A + B|$.

Let $\mathcal{F}(G)$ denote the free abelian monoid with basis G. An element $S \in \mathcal{F}(G)$ is called a *sequence in* G and will be written in the form

$$S = \prod_{i=1}^{l} g_i = \prod_{g \in G} g^{\mathsf{v}_g(S)} \in \mathcal{F}(G)$$

where all $\mathsf{v}_g(S) \in \mathbb{N}_0$ and $\mathsf{v}_g(S) = 0$ for all but finitely many $g \in G$. Clearly, $\mathcal{F}(G)$ is a factorial monoid, and we use all notions of elementary divisibility theory (cf. [9, chapter 10]). For every $g \in G$ we call $\mathsf{v}_g(S)$ the *multiplicity of* g *in* S. We say that g *occurs in* S, if $\mathsf{v}_g(S) > 0$. The unit element $1 \in \mathcal{F}(G)$ is called the *empty sequence*. A sequence $T \in \mathcal{F}(G)$ is a *subsequence of* S, if $\mathsf{v}_g(T) \le \mathsf{v}_g(S)$ for every $g \in G$, and T is called a *proper subsequence of* S, if it is a subsequence with $1 \ne T \ne S$. If T is a subsequence of S, then there exists a subset $I \subset [1, l]$ such that

$$T = \prod_{i \in I} g_i \quad \text{and hence} \quad T^{-1}S = \prod_{i \in [1,l] \setminus I} g_i .$$

We denote by

1. $|S| = l = \sum_{g \in G} \mathsf{v}_g(S) \in \mathbb{N}_0$ the *length of* S (in particular, we have $|1| = 0$),
2. $\sigma(S) = \sum_{i=1}^{l} g_i = \sum_{g \in G} \mathsf{v}_g(S) g \in G$ the *sum of* S,
3. $\operatorname{supp}(S) = \{g_i \mid i \in [1, l]\} = \{g \in G \mid \mathsf{v}_g(S) > 0\} \subset G$ the *support of* S, and by
4. $\Sigma(S) = \{\sum_{i \in I} g_i \mid \emptyset \ne I \subset [1, l]\} \subset G$ the set of sums of non-empty subsequences of S.

The sequence S is called

1. *zero-sumfree*, if $0 \notin \Sigma(S)$,
2. *squarefree*, if $\mathsf{v}_g(S) \le 1$ for all $g \in G$,
3. a *zero-sum sequence*, if $\sigma(S) = 0$,
4. a *minimal zero-sum sequence*, if it is a non-empty zero-sum sequence and every proper zero-sum subsequence is zero-sumfree.

Clearly, S is squarefree if and only if $|S| = |\operatorname{supp}(S)|$, and, roughly speaking, a squarefree sequence is a set.

3. Proof of Theorem 1.2

In this section we give the proof of Theorem 1.2. We first handle the special cases where $\min\{|B|, |C|\} \le 2$ and the case $|S| \le 7$. Then we are well prepared to tackle the general case, which will be done by induction on the length of the sequence.

Throughout the rest of this section, let $G = (G, +)$ be an additively written abelian group. A subset $A \subset G$ is called *additively closed* if $A + A \subset A$. We define a corresponding notion for sequences.

Definition 3.1. A sequence $S \in \mathcal{F}(G)$ is called *additively closed*, if $\sigma(T) \in \operatorname{supp}(S)$ for all subsequences T of S with length $|T| = 2$.

Let $S \in \mathcal{F}(G)$ be a sequence and $A = \operatorname{supp}(S)$. If A is additively closed, then A is a subgroup and S is additively closed. Conversely, if S is additively closed, then for the restricted sumset $A \dot{+} A$ we have $A \dot{+} A \subset A$. The next lemma gives a straightforward characterization of this condition.

Lemma 3.2. *Let $A \subset G$ be a finite subset with $|A| \ge 2$. Then the following statements are equivalent:*

1. $A \dot{+} A \subset A$.
2. *Either $A = \{0, g\}$ or $A = \{0, g, -g\}$ for some $g \in G$ with $2g \ne 0$ or $A \cup \{0\}$ is an elementary 2-group or $A < G$ is a subgroup.*

Proof. 1. $\Longrightarrow$ 2. If all elements of $A \setminus \{0\}$ have order two, then $A \cup \{0\}$ is additively closed whence an elementary 2-group.

Suppose that A contains elements of order greater than two and that there is no $g \in G$ with $\operatorname{ord}(g) > 2$ such that $A = \{0, g\}$ or $A = \{0, g, -g\}$. We show that for every $g \in A$ we have $2g \in A$. This implies that $A + A \subset A$ whence $A < G$ is a subgroup.

Let $g \in A$. We assert that there exists some $h \in A \setminus \{g, -g\}$ such that either $h = 2g$ or $2h \ne 0$. If $2g = 0$, then any $h \in A$ with $\operatorname{ord}(h) > 2$ has the required property. Suppose that $2g \ne 0$. By assumption there exists some $g' \in A \setminus \{0, g, -g\}$. If $2g' \ne 0$, then we set $h = g'$. Suppose that $2g' = 0$. Then $g' \ne g$, $g + g' \in A \setminus \{g\}$ and $2(g + g') = 2g \ne 0$. If $g + g' \ne -g$, then we set $h = g + g'$. If $g + g' = -g$, then $g' = -2g$, $0 = 2g' = -4g$ whence $h = g' = 2g \in A \setminus \{g, -g\}$.

Clearly, if $h = 2g \in A$, then we are done. Suppose that $h \in A \setminus \{g, -g\}$ with $2h \ne 0$. We assert that $g - h \in A$. Since $g + h \ne g - h$, this implies that

$$2g = (g + h) + (g - h) \in A \dotplus A \subset A.$$

If there is some $i \in \mathbb{N}$ such that $g + (i-1)h \in A$ and $g + ih = 0$, then $-h = g + (i-1)h \in A \setminus \{g\}$ whence $g + (-h) \in A$. Suppose that no such $i \in \mathbb{N}$ exists. We assert that $g + ih \in A$ for all $i \in \mathbb{N}_0$. For $i \in [0, 1]$ this is clear. Let $i \ge 2$ and suppose that $g + jh \in A$ for all $j \in [0, i-1]$. Then $g + (i-2)h \in A \setminus \{0\}$ whence $h \ne g + (i-1)h$ and $h + (g + (i-1)h) = g + ih \in A$. Since A is finite, h has finite order whence $g - h \in A$.

2. $\Longrightarrow$ 1. Obvious. □

Corollary 3.3. *Let $S \in \mathcal{F}(G \setminus \{0\})$ be a sequence with $|S| \ge 2$. Then the following statements are equivalent:*

1. *S is additively closed.*
2. *$\operatorname{supp}(S) \cup \{0\}$ is an elementary 2-group and $\mathsf{v}_g(S) = 1$ for every $g \in \operatorname{supp}(S)$.*

If S is additively closed and $|S| \ge 4$, then S contains a proper zero-sum subsequence.

Proof. 1. $\Longrightarrow$ 2. We set $A = \operatorname{supp}(S)$. Then $A \subset G \setminus \{0\}$, $|A| \ge 2$ and $A \dotplus A \subset A$. Hence Lemma 3.2 implies that $A \cup \{0\}$ is an elementary 2-group. Since $0 \notin A$ and S is additively closed, it follows that S is squarefree.

2. $\Longrightarrow$ 1. Obvious.

The remaining statement follows immediately from the characterization. □

Definition 3.4. Let $S \in \mathcal{F}(G)$ be a sequence and $B, C \in \mathcal{F}(G)$ subsequences such that $S = BC$. We say that S is *additively closed with respect to* (B, C), if $\sigma(T) \in \operatorname{supp}(S)$ for all subsequences T of B with $|T| = 2$ and for all subsequences T of C with $|T| = 2$.

Let $S = BC \in \mathcal{F}(G)$ as above and let $\mathbb{B} = \operatorname{supp}(B)$ and $\mathbb{C} = \operatorname{supp}(C)$. If

$$(\mathbb{B} + \mathbb{B}) \cup (\mathbb{C} + \mathbb{C}) \subset \operatorname{supp}(S),$$

then S is additively closed with respect to (B, C). If S is additively closed with respect to (B, C), then

$$(\mathbb{B} \dotplus \mathbb{B}) \cup (\mathbb{C} \dotplus \mathbb{C}) \subset \operatorname{supp}(S).$$

Clearly, S is additively closed, if and only if it is additively closed with respect to $(S, 1)$.

Proposition 3.5. *Let $S = BC \in \mathcal{F}(G \setminus \{0\})$ be a sequence with $|B| \ge 3$ and $|C| = 1$, and suppose that S is additively closed with respect to (B, C). Then S contains a proper zero-sum subsequence, apart from the following exceptions:*

1. *$B = g^k$ and $C = 2g$ for some $g \in G$ and $k \in [3, \operatorname{ord}(g) - 1)$.*

2. *$B = g^k \cdot (2g)$ and $C = 3g$ for some $g \in G$ and $k \in [2, \mathrm{ord}(g) - 4)$.*
3. *$B = g \cdot e \cdot (g + e)$ and $C = 2g + e$ for some $g, e \in G$ with $\mathrm{ord}(e) = 2$ and $\mathrm{ord}(g) \ge 5$.*

Proof. Suppose that B is additively closed. If $|B| \ge 4$, then by Corollary 3.3, B (and hence S) has a proper zero-sum subsequence. If $|B| = 3$, then Corollary 3.3 implies that $B = e_1 \cdot e_2 \cdot (e_1 + e_2)$ with $\mathrm{ord}(e_1) = \mathrm{ord}(e_2) = 2$ whence B is a proper zero-sum subsequence of S.

From now on we suppose that B is not additively closed. This implies that $C \nmid B$ and that B has a subsequence T with $|T| = 2$ and $\sigma(T) = C$. We set

$$\mathbb{B} = \mathrm{supp}(B).$$

Suppose that $|\mathbb{B}| = 1$. Then $B = g^k$ and $C = 2g$ for some $g \in G$ and some $k \ge 3$. Thus, either S has a proper zero-sum subsequence or $k \le \mathrm{ord}(g) - 2$.

Suppose that $|\mathbb{B}| = 2$, say $B = g^k h^l$ with $g, h \in G$ and $k \ge l \ge 1$. Since $g + h \in \mathrm{supp}(S) \setminus \{g, h\}$, it follows that $C = g + h$. Since $k \ge 2$, we infer that $h = 2g$. If $l \ge 2$, then $h + h = 4g = g$ whence $0 = 3g = g + h \in \mathrm{supp}(S)$, a contradiction. Therefore we obtain that $B = g^k \cdot (2g)$ with $k \ge 2$. If $k \ge \mathrm{ord}(g) - 4$, then clearly S has a proper zero-sum subsequence.

Suppose that $|\mathbb{B}| = 3$, say $B = g_1^{k_1} g_2^{k_2} g_3^{k_3}$ with $k_1, k_2, k_3 \in \mathbb{N}$ and $C = g_2 + g_3$. Then $g_1 + g_2 \in \mathrm{supp}(S) \setminus \{g_1, g_2, g_2 + g_3\}$ whence $g_3 = g_1 + g_2$, and $g_1 + g_3 \in \mathrm{supp}(S) \setminus \{g_1, g_3, g_2 + g_3\}$ whence $g_2 = g_1 + g_3$. This implies that $g_2 = g_1 + (g_1 + g_2)$ whence $2g_1 = 0$ and $2g_2 = 2g_3$. If $k_1 \ge 2$, then g_1^2 is a proper zero-sum subsequence of B. Suppose that $k_1 = 1$. If $k_2 \ge 2$, then $2g_3 = 2g_2 \in \mathrm{supp}(S) \setminus \{g_2, g_2 + g_3, g_3\}$ whence $2g_2 = g_1$ and $g_3 = g_1 + g_2 = 3g_2$. Thus $g_1 + g_3 = 5g_2 \in \mathrm{supp}(S) = \{g_1 = 2g_2, g_2, g_3 = 3g_2, g_2 + g_3 = 4g_2\}$, a contradiction. Thus we infer that $k_2 = 1$. If $k_3 \ge 2$, then $2g_2 = 2g_3 \in \mathrm{supp}(S) \setminus \{g_3, g_2, g_2 + g_3\}$ whence $2g_3 = g_1$ and $g_2 = g_1 + g_3 = 3g_3$. Thus $g_1 + g_2 = 5g_3 \in \mathrm{supp}(S) = \{g_1 = 2g_3, g_2 = 3g_3, g_3, g_2 + g_3 = 4g_3\}$, a contradiction. Thus $k_3 = 1$ and S has form 3.

Suppose that $|\mathbb{B}| \ge 4$. We assert that S contains a proper zero-sum subsequence and proceed by induction on $|B|$.

Let $|B| = 4$. Firstly, suppose that, for every $h \in \mathbb{B}$, $h^{-1}S$ is not additively closed with respect to $(h^{-1}B, C)$. Then B is squarefree and, for every $h \in \mathbb{B}$, there is some subsequence T of B with $|T| = 2$ and $h = \sigma(T)$. We set $\mathbb{B} = \{g_1, g_2, g_3, g_4\}$. Since $\mathbb{B} \dotplus \mathbb{B} \subset \mathrm{supp}(S)$ and $|\mathrm{supp}(S)| = 5$, we may suppose that $g_1 + g_2 = g_3 + g_4$. Moreover, we may assume that $g_1 = g_2 + g_3$. Then it follows that

$$2g_2 = g_1 + g_2 - g_3 = g_4 \in \{g_1 + g_2, g_2 + g_3, g_1 + g_3\}$$

whence $g_4 = g_1 + g_3$. Then $g_1 + g_2 = g_3 + g_4 = g_3 + g_1 + g_3$, $g_2 = 2g_3$, $g_4 = 4g_3$, $g_1 = 3g_3$ and $\mathbb{B} = \{g_3, 2g_3, 3g_3, 4g_3\}$. Thus either $4g_3 + 3g_3 \in \mathbb{B}$ or $4g_3 + 2g_3 \in \mathbb{B}$ which implies that B contains a proper zero-sum subsequence.

Secondly, suppose that there is some $h \in \mathbb{B}$ such that $h^{-1}S$ is additively closed with respect to $(h^{-1}B, C)$. If $(h^{-1}B, C) \ne (g \cdot e \cdot (g + e), 2g + e)$, with g, e as described above, then $h^{-1}S$ (and hence S) has a proper zero-sum subsequence. Suppose that $B = g \cdot e \cdot (g + e) \cdot h$ and $C = 2g + e$. Since $|\mathbb{B}| = 4$ and $C \nmid B$, it follows that $g + h \in \mathrm{supp}(S) \setminus \{g + e, 2g + e\}$ whence $g + h = e$ and $g \cdot e \cdot h$ is a proper zero-sum subsequence of S.

Suppose that $|B| \ge 5$. If there exists some $h \in G$ such that $h^2 \mid B$, then $h^{-1}S$ is additively closed with respect to $(h^{-1}B, C)$. Since $|\mathrm{supp}(h^{-1}B)| \ge 4$ and $|h^{-1}B| < |B|$, the induction hypothesis implies that $h^{-1}S$ (and hence S) has a proper zero-sum subsequence.

For the remainder of the proof, we suppose that B is squarefree. Suppose that there exists some $h \in \mathbb{B}$ such that $h \ne \sigma(T)$ for every subsequence T of B with length $|T| = 2$. Then $h^{-1}S$ is additively closed with respect to $(h^{-1}B, C)$. Since $|\mathrm{supp}(h^{-1}B)| = |h^{-1}B| \ge 4$ and $|h^{-1}B| < |B|$, $h^{-1}S$ (and hence S) has a proper zero-sum subsequence by induction hypothesis.

Now, we suppose that for every $h \in \mathbb{B}$ there is some subsequence T of B with length $|T| = 2$ such that $h = \sigma(T)$. If there exists some $h \in \mathbb{B}$ with $2h = 0$ and T is a subsequence of B with $|T| = 2$ and

$\sigma(T) = h$, then $h \cdot T$ is a proper zero-sum subsequence of S. Hence, from now on we may suppose that $2h \neq 0$ for all $h \in \mathbb{B}$.

Let $T = g_0 \cdot g_0'$ be a subsequence of B with $\sigma(T) = C$, and let $A = \{g_1, \ldots, g_k\} = \mathbb{B} \setminus \{g_0, g_0'\}$ whence $|A| = k \geq 3$. Then

$$g_0 + A \subset \operatorname{supp}(S) \setminus \{g_0, g_0 + g_0'\} \quad \text{and} \quad g_0' + A \subset \operatorname{supp}(S) \setminus \{g_0', g_0 + g_0'\}.$$

Case 1: $g_0' \in g_0 + A$ and $g_0 \in g_0' + A$. Thus there exist $i, j \in [1, k]$ such that $g_0' = g_0 + g_i$ and $g_0 = g_0' + g_j$ whence $g_0 = g_0 + g_i + g_j$. Since $2g_i \neq 0$, we infer that $i \neq j$ whence $g_i \cdot g_j$ is a proper zero-sum subsequence of B.

Case 2: ($g_0' \notin g_0 + A$) or ($g_0 \notin g_0' + A$). Without restriction, we suppose that $g_0' \notin g_0 + A$. This implies that $g_0 + A \subset \operatorname{supp}(S) \setminus \{g_0, g_0', g_0 + g_0'\} = A$ whence $g_0 + A = A$. This implies that

$$a + \nu g_0 \in A \quad \text{for all } a \in A \text{ and all } \nu \in \mathbb{N}_0.$$

Since A is finite, we infer that $\operatorname{ord}(g_0) < \infty$ whence $a + g_0, a - g_0 \in A$. Thus we obtain that $2a \in \operatorname{supp}(S)$ for every $a \in A$.

We assert that $\{2g_0, 2g_0'\} \subset \operatorname{supp}(S)$. First we show that $2g_0' \in \operatorname{supp}(S)$. By the above assumption, there exist $i, j \in [0, k]$ distinct such that $g_0' = g_i + g_j$. Without restriction we suppose that $g_i \neq g_0$. Then $g_0' + g_i \in \operatorname{supp}(S) \setminus \{g_i, g_0', g_0 + g_0'\}$ whence there is some $l \in [0, k] \setminus \{i\}$ such that $g_0' + g_i = g_l$. If $l = j$, then we have

$$g_0' + g_i = g_j \quad \text{and} \quad g_i + g_j = g_0'$$

whence $2g_i = 0$, a contradiction. Thus we have $l \neq j$ and

$$2g_0' = g_0' + (g_i + g_j) = g_l + g_j \in \operatorname{supp}(S).$$

Similarly, we obtain that $2g_0 \in \operatorname{supp}(S)$.

So on the one hand, we have shown that

$$\mathbb{B} + \mathbb{B} \subset \operatorname{supp}(S) \quad \text{whence} \quad |\mathbb{B} + \mathbb{B}| \leq |\mathbb{B}| + 1,$$

and on the other hand, Kneser's Addition Theorem (cf. [15, Theorem 4.2]) implies that

$$\text{either} \quad |\mathbb{B} + \mathbb{B}| \geq 2|\mathbb{B}| \quad \text{or} \quad |\mathbb{B} + \mathbb{B}| = 2|\mathbb{B} + K| - |K|,$$

where

$$K = \{g \in G \mid g + B + B = B + B\} < G$$

is the stabilizer of $B + B$. If $2|\mathbb{B}| \leq |\mathbb{B} + \mathbb{B}| \leq |\mathbb{B}| + 1$, then $|\mathbb{B}| \leq 1$, a contradiction. Thus we infer that

$$|\mathbb{B} + \mathbb{B}| = |\mathbb{B} + K| + |\mathbb{B} + K| - |K| \leq |\mathbb{B}| + 1.$$

Since $|\mathbb{B}| \leq |\mathbb{B} + K|$ and $|K| \leq |\mathbb{B} + K|$, this implies that $|\mathbb{B} + K| - |K| \in \{0, 1\}$.

Suppose that $|\mathbb{B} + K| = |K| + 1$. Since $|K|$ divides $|\mathbb{B} + K| = |K| + 1$, it follows that $|K| = 1$ and $|\mathbb{B}| \leq |\mathbb{B} + K| = |K| + 1 = 2$, a contradiction.

Suppose that $|\mathbb{B} + K| = |K|$. Then

$$\mathbb{B} \subset \mathbb{B} + K = \bigcup_{b' \in \mathbb{B}} (b' + K) = b + K$$

for some $b \in \mathbb{B}$. Since $g_0, g_1 \in \mathbb{B}$ and $g_0 + g_1 \in g_0 + A = A \subset \mathbb{B}$, it follows that $g_0 + g_1 \in (2b + K) \cap (b + K)$, whence $b \in K$. This implies that $\mathbb{B} \subset K$ whence $\mathbb{B} + \mathbb{B} \subset K$. Since $|K|$ divides $|\mathbb{B} + \mathbb{B} + K| = |\mathbb{B} + \mathbb{B}|$, we obtain that $\mathbb{B} + \mathbb{B} = K$. Thus there are $b, b' \in \mathbb{B}$ such that $b + b' = 0$. Since $2b \neq 0$, it follows that $b \neq b'$ and $b \cdot b'$ is a proper zero-sum subsequence of S. □

Remark: In the above proof we could use a result of Kemperman-Scherk instead of Kneser's Addition Theorem, which is most probably better known. For some historical remarks and the interdependence of both results we refer to [11, section 1].

Proposition 3.6. *Let $S = BC \in \mathcal{F}(G \setminus \{0\})$ be a sequence with $|S| \ge 4$, $\min\{|B|, |C|\} = 2$, and suppose that S is additively closed with respect to (B, C). Then S contains a proper zero-sum subsequence.*

Proof. Without restriction we may suppose that $\min\{|B|, |C|\} = |B| = 2$, and we set

$$B = g_1 \cdot g_2, \ g = g_1 + g_2, \ \text{ and } \{i, j\} = \{1, 2\}.$$

Assume to the contrary, that S does not contain a proper zero-sum subsequence. By assumption we have $g \mid C$ and there is some $h \in G$ such that $g \cdot h \mid C$. Since $g_1 \cdot g_2 \cdot g$ is a subsequence of S, it follows that $\mathrm{ord}(g) > 2$.

Assertion 1: $g \cdot \prod_{\nu=0}^{\lambda}(\nu g + h)$ is a subsequence of C for every $\lambda \in [0, \mathrm{ord}(g))$. In particular, $\mathrm{ord}(g) < \infty$, and we set $\mathrm{ord}(g) = n$.
Proof of Assertion 1: We proceed by induction on λ. Clearly, the assertion holds for $\lambda = 0$. Now let $\lambda \in \mathbb{N}_0$ with $\lambda \le \mathrm{ord}(g) - 2$, and suppose that $g \prod_{\nu=0}^{\lambda}(\nu g + h)$ is a subsequence of C. Setting $T = g \cdot (\lambda g + h)$ we infer that $\sigma(T) = (\lambda + 1)g + h \in \mathrm{supp}(S)$.

If $(\lambda + 1)g + h = g_i$, then $(\lambda g + h) \cdot g_j$ is a proper zero-sum subsequence of S, a contradiction.

If $(\lambda + 1)g + h = g$, then $0 = \lambda g + h \in \mathrm{supp}(S)$, a contradiction.

If $(\lambda + 1)g + h = \nu g + h$ for some $\nu \in [0, \lambda]$, then $(\lambda + 1 - \nu)g = 0$, a contradiction to $\lambda \le \mathrm{ord}(g) - 2$.

Thus $g \cdot \prod_{\nu=0}^{\lambda+1}(\nu g + h)$ is a subsequence of C.

Assertion 2:

$$S_\lambda = g \cdot \prod_{\nu=0}^{n-1}(\nu g + h) \cdot \prod_{\nu=2}^{\lambda}(\nu h + g)$$

is a subsequence of C for every $\lambda \in [1, \mathrm{ord}(h))$.

Once we have established the validity of Assertion 2, we can complete the proof as follows. We observe that $\mathrm{ord}(h) = m < \infty$. If $m = 2$, then $(g + h) \cdot (-g + h)$ is a proper zero-sum subsequence of S, a contradiction. Suppose that $m \ge 3$. Then S_{m-1} is a subsequence of C, whence $(-g + h) \cdot (-h + g)$ is a proper zero-sum subsequence of S, a contradiction.

Proof of Assertion 2: We proceed by induction on λ. If $\lambda = 1$, then $S_\lambda = g \cdot \prod_{\nu=0}^{n-1}(\nu g + h)$ is a subsequence of C by Assertion 1. Suppose that $\lambda \in \mathbb{N}$ with $\lambda \le \mathrm{ord}(h) - 2$ and that S_λ is a subsequence of C. Setting $T = h \cdot (\lambda h + g)$ we infer that $\sigma(T) = (\lambda + 1)h + g \in \mathrm{supp}(S)$.

If $(\lambda + 1)h + g = g_i$, then $(\lambda h + g) \cdot ((n - 1)g + h) \cdot g_j$ is a proper zero-sum subsequence of S, a contradiction.

If $(\lambda + 1)h + g = g$, then $0 = (\lambda + 1)h$, a contradiction.

If $(\lambda + 1)h + g = h$, then $0 = \lambda h + g \in \mathrm{supp}(S)$, a contradiction.

If $(\lambda + 1)h + g = \nu h + g$ for some $\nu \in [1, \lambda]$, then $(\lambda + 1 - \nu)h = 0$, a contradiction.

If $(\lambda + 1)h + g = \nu g + h$ for some $\nu \in [1, n - 1]$, then $\lambda h + (n - \nu + 1)g = 0$. If $(\lambda, \nu) \ne (2, n - 1)$, then $((\lambda - 1)h + g) \cdot ((n - \nu)g + h)$ is a proper zero-sum subsequence of S, a contradiction. If $(\lambda, \nu) = (2, n - 1)$, then $2h + 2g = 0$ whence $g \cdot h \cdot (g + h)$ is a proper zero-sum subsequence of S, a contradiction.

Thus $S_{\lambda+1}$ is a subsequence of C. □

Lemma 3.7. *Let $S = BC \in \mathcal{F}(G \setminus \{0\})$ be a squarefree sequence having the following properties:*

1. *S is additively closed with respect to (B, C).*
2. *For every $a \in \mathrm{supp}(S)$ there is some $T \in \mathcal{F}(G)$ with $a = \sigma(T)$, $|T| = 2$ and ($T \mid B$ or $T \mid C$).*
3. $\min\{|B|, |C|\} \ge 3$.
4. *S does not contain a proper zero-sum subsequence.*

Then $\mathrm{supp}(S)$ *does not contain an element of order two, and one of the two sequences* B *or* C*, say* B*, contains a subsequence* T *with* $|T| = 2$ *such that* $\sigma(T)T \mid B$*.*

Proof. Assume to the contrary that $a \in \mathrm{supp}(S)$ has order two. If $T \in \mathcal{F}(G)$ is as in Assumption 2., then $a \cdot T$ is a proper zero-sum subsequence of S, a contradiction.

As for the second assertion, we assume to the contrary that neither B nor C has the required property. Without restriction we may suppose that $|B| \ge |C|$. Let $T = h \cdot h'$ be a subsequence of C whence $\sigma(T) \mid B$, say $\sigma(T) = g_1$ and $B = \prod_{i=1}^{l} g_i$. Since B does not have the required property, the sequence $\prod_{i=2}^{l}(g_1 + g_i)$ divides C whence $|C| \ge |B| - 1$. Thus $|C| \in \{|B|, |B| - 1\}$ and $\{h, h'\} \cap \{g_1 + g_i \mid i \in [2, l]\} \ne \emptyset$, say $h = g_1 + g_2$. Then $h = g_1 + g_2 = h + h' + g_2$ whence $h' \cdot g_2$ is a proper zero-sum subsequence of S. □

Proposition 3.8. *Let* $S = BC \in \mathcal{F}(G \setminus \{0\})$ *be a sequence with* $|B| = |C| = 3$*, and suppose that* S *is additively closed with respect to* (B, C)*. Then* S *contains a proper zero-sum subsequence, apart from the case where*

$$B = g \cdot 9g \cdot 10g \quad \textit{and} \quad C = 11g \cdot 3g \cdot 14g \quad \textit{for some } g \in G \textit{ with } \mathrm{ord}(g) = 16.$$

Proof. Suppose that S is not squarefree, say $a^2 \mid S$ for some $a \in \mathrm{supp}(B)$. Then $S' = (a^{-1}B)(C)$ is additively closed with respect to $(a^{-1}B, C)$. Since $\min\{|a^{-1}B|, |C|\} = 2$, Proposition 3.6 implies that $a^{-1}S$, and hence S, has a proper zero-sum subsequence.

Suppose there exists some $a \in \mathrm{supp}(S)$ such that $a \ne \sigma(T)$ for all $T \in \mathcal{F}(G)$ with $|T| = 2$ and ($T \mid B$ or $T \mid C$). Without restriction we may suppose that $a \mid B$. Then $S' = (a^{-1}B)(C)$ is additively closed with respect to $(a^{-1}B, C)$. Arguing as above we infer that S has a proper zero-sum subsequence.

Thus we may suppose that S is squarefree and for every $a \in \mathrm{supp}(S)$ there is some $T \in \mathcal{F}(G)$ with $a = \sigma(T)$, $|T| = 2$ and ($T \mid B$ or $T \mid C$). Suppose that S does not contain a proper zero-sum subsequence. We show that B and C have the given special form.

Since S satisfies all assumptions of Lemma 3.7, $\mathrm{supp}(S)$ does not contain elements of order two, and there exists some $T \in \mathcal{F}(G)$ with $|T| = 2$ such that $T\sigma(T) \mid B$, say $B = g_1 \cdot g_2 \cdot (g_1 + g_2)$. Then it follows that $2g_1 + g_2 \notin \{g_1, g_2, g_1 + g_2\}$ whence $2g_1 + g_2 \in \mathrm{supp}(C)$. Since $g_1 + 2g_2 \notin \{g_1, g_2, g_1 + g_2, 2g_1 + g_2\}$, it follows that

$$S = \underbrace{g_1 \cdot g_2 \cdot (g_1 + g_2)}_{B} \cdot \underbrace{(2g_1 + g_2) \cdot (g_1 + 2g_2) \cdot h}_{C} \quad \text{for some } h \in G.$$

If $3g_1 + 3g_2 \in \{g_1, g_2, g_1 + g_2\}$, then it easy to see that S has a proper zero-sum subsequence. Therefore we get $h = 3g_1 + 3g_2$. If $5g_1 + 4g_2 \in \{g_1, g_1 + g_2, g_1 + 2g_2\}$, then S has a proper zero-sum subsequence. Thus $5g_1 + 4g_2 = g_2$ whence $5g_1 + 3g_2 = 0$. Similarly, we consider $4g_1 + 5g_2$ and obtain that $3g_1 + 5g_2 = 0$. Thus it follows that

$$2g_1 = 2g_2, \; g_2 = -7g_1 \quad \text{and } 5g_1 - 21g_1 = -16g_1 = 0$$

whence

$$S = \underbrace{(g_1 \cdot 9g_1 \cdot 10g_1)}_{B} \cdot \underbrace{(11g_1 \cdot 3g_1 \cdot 14g_1)}_{C}.$$

□

Proposition 3.9. *Let* $S = BC \in \mathcal{F}(G \setminus \{0\})$ *be a sequence with* $|B| = 3$*,* $|C| = 4$ *and suppose that* S *is additively closed with respect to* (B, C)*. Then* S *contains a proper zero-sum subsequence.*

Proof. Suppose that S is not squarefree, say $a^2 \mid S$ for some $a \in \mathrm{supp}(S)$. First suppose that $a \in \mathrm{supp}(C)$. Then $S' = (B)(a^{-1}C)$ is additively closed with respect to $(B, a^{-1}C)$. By Proposition 3.8, S' is either a minimal zero-sum sequence or S' contains a proper zero-sum subsequence. Hence $S = aS'$ contains a proper zero-sum subsequence. If $a \in \mathrm{supp}(B)$, then $S' = (a^{-1}B)(C)$ is additively closed with respect to $(a^{-1}B, C)$ and Proposition 3.6 implies that S' (and hence $S = aS'$) contains a proper zero-sum subsequence.

Suppose that there exists some $a \in \operatorname{supp}(S)$ such that

$$a \notin \{\sigma(T) \mid |T| = 2, T \text{ is a subsequence of } B \text{ or } C\}.$$

Arguing as above we obtain that $S = aS'$ contains a proper zero-sum subsequence.

Thus we may suppose that S is squarefree, $|B| = 3$, $|C| = 4$ and that for every $a \in \operatorname{supp}(S)$ there is some $T \in \mathcal{F}(G)$ with $a = \sigma(T)$, $|T| = 2$ and ($T \mid B$ or $T \mid C$). Assume to the contrary that S does not contain a proper zero-sum subsequence. Then all assumptions of Lemma 3.7 are satisfied, and in particular $\operatorname{supp}(S)$ does not contain elements of order two. The argument reduces to two cases.

Case 1: For every $T \in \mathcal{F}(G)$ with $|T| = 2$ and $T \mid B$ it follows that $\sigma(T) \nmid B$. We set $B = g_1 \cdot g_2 \cdot g_3$. Then $(g_1 + g_2) \cdot (g_1 + g_3) \cdot (g_2 + g_3)$ is a subsequence of C. Since for every $h \in \operatorname{supp}(C)$ there is some T with $|T| = 2$ and ($T \mid B$ or $T \mid C$) such that $h = \sigma(T)$, we may suppose without restriction that

$$S = \underbrace{g_1 \cdot g_2 \cdot g_3}_{B} \cdot \underbrace{(g_1 + g_2) \cdot (g_1 + g_3) \cdot (g_2 + g_3) \cdot (2g_1 + g_2 + g_3)}_{C}.$$

If $g_1 + g_2 + 2g_3 \in \{g_1, g_2, g_3\}$, then it follows immediately that S contains a proper zero-sum subsequence. If $g_1 + g_2 + 2g_3 = 2g_1 + g_2 + g_3$, then $g_3 = g_1$, a contradiction. Thus it follows that $g_1 + g_2 + 2g_3 = g_1 + g_2$ whence $2g_3 = 0$, a contradiction.

Case 2: B contains a subsequence T with $|T| = 2$ such that $\sigma(T) \mid B$, say $B = g_1 \cdot g_2 \cdot (g_1 + g_2)$. Without loss of generality we suppose that $\operatorname{ord}(g_1) \ge \operatorname{ord}(g_2) > 2$.

Then we infer that $(2g_1 + g_2) \cdot (g_1 + 2g_2)$ is a subsequence of C. Then $3g_1 + 3g_2 \in \operatorname{supp}(S)$. If $3g_1 + 3g_2 \in \{g_1, g_2, g_1 + g_2\}$, then S contains a proper zero-sum subsequence. Thus suppose that

$$S = \underbrace{g_1 \cdot g_2 \cdot (g_1 + g_2)}_{B} \cdot \underbrace{(2g_1 + g_2) \cdot (g_1 + 2g_2) \cdot (3g_1 + 3g_2) \cdot h}_{C} \quad \text{for some } h \in G.$$

Since $h = \sigma(T)$ for some $T \in \mathcal{F}(G)$ with $|T| = 2$ and ($T \mid B$ or $T \mid C$), it follows that $h \in \{5g_1 + 4g_2, 4g_1 + 5g_2\}$, say $h = 5g_1 + 4g_2$. Setting $T = (g_1 + 2g_2) \cdot (5g_1 + 4g_2)$ we infer that $\sigma(T) = 6g_1 + 6g_2 \in \{g_1, g_2, g_1 + g_2, 2g_1 + g_2, 3g_1 + 3g_2\}$. If $6g_1 + 6g_2 = g_1$, then $(g_1 + g_2) \cdot (g_1 + 2g_2) \cdot (3g_1 + 3g_2)$ is a proper zero-sum subsequence of S. If $6g_1 + 6g_2 = g_2$, then $(g_1 + g_2) \cdot (2g_1 + g_2) \cdot (3g_1 + 3g_2)$ is a proper zero-sum subsequence of S. If $6g_1 + 6g_2 = g_1 + g_2$, then $g_2 \cdot (5g_1 + 4g_2)$ is a proper zero-sum subsequence of S. If $6g_1 + 6g_2 = 2g_1 + g_2$, then $g_2 \cdot (g_1 + g_2) \cdot (3g_1 + 3g_2)$ is a proper zero-sum subsequence of S. If $6g_1 + 6g_2 = 3g_1 + 3g_2$, then $0 = 3g_1 + 3g_2 \in \operatorname{supp}(S)$. Thus in all cases we derive a contradiction. □

Proof of Theorem 1.2. The cases $\min\{|B|, |C|\} \in \{0, 1, 2\}$ (whence in particular the cases $|S| \in \{4, 5\}$) are settled by Corollary 3.3, Proposition 3.5 and Proposition 3.6. If $|B| = |C| = 3$, then the assertion follows from Proposition 3.8.

Let $S = BC$ with $\min\{|B|, |C|\} \ge 2$ and $|S| \ge 7$. We assert that S contains a proper zero-sum subsequence and proceed by induction on $|S|$. For $|S| = 7$ this follows from Proposition 3.9, and moreover the case $\min\{|B|, |C|\} = 2$ is settled. Suppose that every sequence $S' = B'C' \in \mathcal{F}(G \setminus \{0\})$, which is additively closed with respect to (B', C') and with $7 \le |S'| < |S|$, $|B'| \ge 2$, $|C'| \ge 2$, contains a proper zero-sum subsequence.

Let $S = BC$ with $|S| \ge 8$ and $\min\{|B|, |C|\} \ge 3$.

Suppose that S is not squarefree, say $a^2 \mid S$ for some $a \in \operatorname{supp}(B)$. Then $S' = (a^{-1}B)(C)$ is additively closed with respect to $(a^{-1}B, C)$, $|a^{-1}B| \ge 2$, $|C| \ge 3$ and $|S'| \ge 7$. Thus, by induction hypothesis, S' and hence $aS' = S$ contains a proper zero-sum subsequence.

Suppose there exists some $a \in \operatorname{supp}(S)$ such that $a \ne \sigma(T)$ for all $T \in \mathcal{F}(G)$ with $|T| = 2$ and ($T \mid B$ or $T \mid C$). Without restriction we may suppose that $a \mid B$. Then $S' = (a^{-1}B)(C)$ is additively closed with respect to $(a^{-1}B, C)$, $|a^{-1}B| \ge 2$, $|C| \ge 3$ and $|S'| \ge 7$. Again, by induction hypothesis, $aS' = S$ contains a proper zero-sum subsequence.

Suppose that S is squarefree and that for every $a \in \operatorname{supp}(S)$ there exists some $T \in \mathcal{F}(G)$ with $a = \sigma(T)$, $|T| = 2$ and ($T \mid B$ or $T \mid C$). Assume to the contrary that S does not contain a proper zero-sum subsequence. Then, by Lemma 3.7, $\operatorname{supp}(S)$ does not contain elements of order two.

Assertion: There exist subsequences $T' = \prod_{i=1}^{k} a_i$ of S having the following properties:

1. $\{\sum_{i=1}^{j} a_i \mid j \in [2,k]\} \subset \operatorname{supp}(S)$,
2. either $a_1 \cdot a_2 \cdot (a_1 + a_2) \mid B$ or $a_1 \cdot a_2 \cdot (a_1 + a_2) \mid C$, and
3. for all $i \in [2,k]$ either $(a_1 + \ldots + a_{i-1}) \cdot a_i \mid B$ or $(a_1 + \ldots + a_{i-1}) \cdot a_i \mid C$.

If T is a subsequence of S having the above properties with maximal possible length, then $|T| \ge |S| - 2$.

Assuming this Assertion, we first complete the proof of the Theorem. The proof of the Assertion will be given in the next step.

Let $T = \prod_{i=1}^{k} a_i$ be a subsequence of S having the properties formulated in the Assertion with length $|T| \ge |S| - 2$. For every $l \in [1,k]$, we set

$$B_l = \gcd(B, \prod_{i=1}^{l} a_i) \quad \text{and} \quad C_l = \gcd(C, \prod_{i=1}^{l} a_i)$$

whence $B_l C_l = \prod_{i=1}^{l} a_i$. For a sequence $A \in \mathcal{F}(G)$ we set $2\hat{\ } A = \prod_{g \in G_0} g$ where $G_0 = \operatorname{supp}(A) \dot{+} \operatorname{supp}(A)$.

For every $l \in [3, k-1]$ each of the sequences

$$\prod_{i=1}^{l} a_i,\ \prod_{i=3}^{l-1} (a_1 + \ldots + a_i),\ 2\hat{\ } B_l,\ 2\hat{\ } C_l \tag{1}$$

is a subsequence of $\prod_{i=l}^{k} (a_1 + \ldots + a_i)^{-1} \cdot S$ whence

$$U_l = \operatorname{lcm}\left(\prod_{i=1}^{l} a_i,\ \prod_{i=3}^{l-1} (a_1 + \ldots + a_i),\ 2\hat{\ } B_l,\ 2\hat{\ } C_l \right)$$

is a subsequence of $\prod_{i=l}^{k} (a_1 + \ldots + a_i)^{-1} \cdot S$ and

$$|U_l| \le |S| - (k - l + 1) \le |S| - (|S| - 2 - l + 1) = l + 1. \tag{2}$$

Since

$$k - 1 = |T| - 1 \ge |S| - 3 \ge 5,$$

we may consider equation (2) for $l = 5$. Since $(a_1 + a_2 + a_3) \cdot a_4$ is a subsequence of B or C, it follows that $a_4 \ne a_1 + a_2 + a_3$. Similarly, since $(a_1 + a_2 + a_3 + a_4) \cdot a_5$ is a subsequence of B or C, it follows that $a_5 \ne a_1 + a_2 + a_3 + a_4$. Since $\operatorname{lcm}\{\prod_{i=1}^{5} a_i, (a_1 + a_2 + a_3) \cdot (a_1 + a_2 + a_3 + a_4)\}$ is a squarefree sequence of length at most 6, which has no proper zero-sum subsequence, it follows that $a_5 = a_1 + a_2 + a_3$ and

$$U_5 = a_1 \cdot a_2 \cdot a_3 \cdot a_4 \cdot (a_1 + a_2 + a_3) \cdot (a_1 + a_2 + a_3 + a_4).$$

By assumption we may suppose without restriction that $a_1 \cdot a_2 \cdot (a_1 + a_2) \mid B$. Then $(a_1 + a_2) \cdot a_3 \mid B$, whence $a_1 \cdot a_2 \cdot a_3 \mid B_5$.

Since $2\hat{\ } B_5 \mid U_5$, it follows that $a_1 + a_2 \in \operatorname{supp}(U_5)$ whence $a_1 + a_2 \in \{a_3, a_4\}$. Since $(a_1 + a_2) \cdot a_3 \mid B$, it follows that $a_3 \ne a_1 + a_2$ whence $a_1 + a_2 = a_4$ and

$$U_5 = a_1 \cdot a_2 \cdot a_3 \cdot \underbrace{(a_1 + a_2)}_{a_4} \cdot \underbrace{(a_1 + a_2 + a_3)}_{a_5} \cdot \underbrace{(2a_1 + 2a_2 + a_3)}_{a_1 + a_2 + a_3 + a_4}.$$

Similarly, we have $a_2 + a_3 \in \operatorname{supp}(U_5)$ and clearly, $a_2 + a_3 \notin \{a_2, a_3, a_1 + a_2, a_1 + a_2 + a_3\}$. If $a_2 + a_3 = 2a_1 + 2a_2 + a_3$, then $2a_1 + a_2 = 0$ and $a_1 \cdot (a_1 + a_2)$ is a proper zero-sum subsequence of S, a contradiction. Thus we infer that $a_2 + a_3 = a_1$ and

$$U_5 = a_1 \cdot a_2 \cdot \underbrace{(a_1 - a_2)}_{a_3} \cdot \underbrace{(a_1 + a_2)}_{a_4} \cdot \underbrace{2a_1}_{a_5} \cdot \underbrace{(3a_1 + a_2)}_{a_1+a_2+a_3+a_4} .$$

Furthermore, we have $a_1+a_3 \in \operatorname{supp}(U_5)$ and clearly, $a_1+a_3 \notin \{a_1, a_3, a_5, a_4\}$. If $a_1+a_3 = a_1+a_2+a_3+a_4$, then $a_2 \cdot a_4$ is a proper zero-sum subsequence of S, a contradiction. Thus we obtain that $a_1 + a_3 = a_2$ whence $a_1 + a_3 = a_1 - a_3$ and $2a_3 = 0$, a contradiction.

Proof of the Assertion: By Lemma 3.7, one of the two sequences B or C, say sequence B, has a subsequence $T = a_1 \cdot a_2$ such that $T\sigma(T) = a_1 \cdot a_2 \cdot (a_1 + a_2)$ is a subsequence of B. If $|B| \ge 4$, then there exists some $a_3 \in \operatorname{supp}(B) \setminus \{a_1, a_2, a_1 + a_2\}$ and $T' = a_1 \cdot a_2 \cdot a_3$ satisfies all required properties. Suppose that $|B| = 3$. Then $C = \prod_{i=1}^{l} c_i$ has length $|C| = l \ge 5$. Since $|\{c_1 + c_2, \ldots, c_1 + c_l\}| = l - 1 > |B|$, there exists some $i \in [2, l]$, say $i = 2$, such that $(c_1 + c_2) \mid C$, whence $c_1 \cdot c_2 \cdot (c_1 + c_2) \mid C$. Then there exists some $i \in [3, l]$, say $i = 3$, with $c_3 \ne c_1 + c_2$ and the sequence $T' = c_1 \cdot c_2 \cdot c_3$ satisfies all required properties.

Let $T = \prod_{i=1}^{k} a_i$ be a subsequence of S having the required properties and suppose that $|T|$ is maximal possible. Then $k \ge 3$, and we assume to the contrary that $|T| \le |S| - 3$. We set $B_k = \gcd(B, T)$ and $C_k = \gcd(C, T)$ whence $B_k C_k = T$.

Without restriction we may suppose that $a_1 + \ldots + a_k \in \operatorname{supp}(B)$. If $B_k = B$, then $B = \prod_{\nu \in I} a_\nu$ for some $I \subset [1, k]$ whence $a_1 + \ldots + a_k = a_i$ for some $i \in I$ and S has a proper zero-sum subsequence, a contradiction. Thus $B_k \ne B$. If $B_k^{-1}B$ contains some element a_{k+1} with $a_{k+1} \ne a_1 + \ldots + a_k$, then the sequence $a_{k+1} \cdot T$ satisfies all required properties, a contradiction to the maximality of $|T|$. Thus it follows that $B = b_0 \cdot B_k$ with $b_0 = a_1 + \ldots + a_k$. Since

$$|T| = |B_k C_k| \le |S| - 3 = |BC| - 3 = |B_k| + |C| - 2,$$

it follows that $|C_k^{-1}C| \ge 2$.

Case 1: $a_k \mid C$. Then $a_1 + \ldots + a_{k-1} \in \operatorname{supp}(C)$ and there exists some $a'_k \in \operatorname{supp}(C_k^{-1}C)$ with $a'_k \ne a_1 + \ldots + a_{k-1}$. We set

$$T' = a_k^{-1} \cdot a'_k \cdot T, \; B'_k = \gcd(T', B) \quad \text{and} \quad C'_k = \gcd(T', C).$$

Then $T' = B'_k C'_k$, $B'_k = B_k$ and $C'_k = a_k^{-1} a'_k C_k$ whence $|{C'_k}^{-1} C| \ge 2$. Since $a_1 + \ldots a_{k-1} + a'_k \ne a_1 + \ldots + a_k = b_0$ and since S does not contain a proper zero-sum subsequence, it follows that $a_1 + \ldots + a_{k-1} + a'_k \notin \operatorname{supp}(B_k) \cup \{b_0\} = \operatorname{supp}(B)$ whence $a_1 + \ldots + a_{k-1} + a'_k \in \operatorname{supp}(C)$. If $a'_{k+1} \in \operatorname{supp}({C'_k}^{-1}C)$ with $a'_{k+1} \ne a_1 + \ldots + a_{k-1} + a'_k$, then $a'_{k+1}T'$ satisfies all required properties, a contradiction to the maximality of $|T|$.

Case 2: $a_k \mid B$. Then $a_1 + \ldots + a_{k-1} \in \operatorname{supp}(B)$ and $a_1 + \ldots + a_k = b_0$ implies that $a_1 + \ldots + a_{k-1} \ne b_0$ whence $a_1 + \ldots + a_{k-1} + b_0 \in \operatorname{supp}(S)$. If $a_1 + \ldots + a_{k-1} + b_0 \in \operatorname{supp}(C)$, then for some $a'_{k+1} \in \operatorname{supp}(C_k^{-1}C)$ with $a'_{k+1} \ne a_1 + \ldots + a_{k-1} + b_0$ the sequence $a_k^{-1} T b_0 a'_{k+1}$ satisfies all required properties, a contradiction to the maximality of $|T|$. Thus we infer that $a_1 + \ldots + a_{k-1} + b_0 \in \operatorname{supp}(B)$. If $a_1 + \ldots + a_{k-1} + b_0 \ne a_k$, then we obtain again a contradiction to the maximality of $|T|$. Therefore it follows that

$$(*) \qquad a_1 + \ldots + a_k = b_0 \quad \text{and} \quad a_1 + \ldots + a_{k-1} + b_0 = a_k.$$

Adding these two equations we infer that $2(a_1 + \ldots + a_{k-1}) = 0$ whence $a_1 \cdot \ldots \cdot a_{k-1} \cdot (a_1 + \ldots + a_{k-1})$ is a proper zero-sum subsequence of S, a contradiction. □

Acknowledgement: We would like to thank the referee for his careful reading.

References

[1] D.D. Anderson, editor. *Factorization in Integral Domains*, volume 189 of *Lecture Notes in Pure and Applied Math.* Marcel Dekker, 1997.

[2] S.T. Chapman, editor. *Arithmetical Properties of Commutative Rings and Monoids*, Lecture Notes in Pure Appl. Math. Marcel Dekker.

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

[4] A. Foroutan. Monotone chains of factorizations. *Int. J. of commutative rings*, 3, 2003.

[5] L. Gallardo, G. Grekos, L. Habsieger, F. Hennecart, B. Landreau, and A. Plagne. Restricted addition in $\mathbb{Z}/n\mathbb{Z}$ and an application to the Erdös-Ginzburg-Ziv problem. *J. Lond. Math. Soc.*, 65:513 – 523, 2002.

[6] W. Gao and A. Geroldinger. On zero-sum sequences in $\mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$. *Integers*, 3:A8, 45pp, 2003.

[7] A. Geroldinger. Factorizations of algebraic numbers. In *Number Theory, Ulm*, volume 1380 of *Lecture Notes in Math.*, pages 63 – 74. Springer, 1989.

[8] A. Geroldinger. Chains of factorizations in orders of global fields. *Colloq. Math.*, 72:83 – 102, 1997.

[9] F. Halter-Koch. *Ideal Systems. An Introduction to Multiplicative Ideal Theory.* Marcel Dekker, 1998.

[10] Y.O. Hamidoune, A.S. Lladó, and O. Serra. On restricted sums. *Comb. Probab. Comput.*, 9:513 – 518, 2000.

[11] V. Lev. Restricted set addition in abelian groups: results and conjectures. *J. Théor. Nombres Bordx., to appear.*

[12] V. Lev. Restricted set addition in groups I: the classical setting. *J. Lond. Math. Soc.*, 62:27 – 40, 2000.

[13] V. Lev. Restricted set addition in groups II: a generalization of the Erdös-Heilbronn conjecture. *The Electronic Journal of Combinatorics*, 7:R4, 2000.

[14] V. Lev. Restricted set addition in groups III: integer sumsets with generic restrictions. *Period. Math. Hung.*, 42:89 – 98, 2001.

[15] M.B. Nathanson. *Additive Number Theory: Inverse Problems and the Geometry of Sumsets.* Springer, 1996.

Center for Combinatorics, Nankai University, Tianjin 300071, P.R. China
E-mail address: wdgao_1963@yahoo.com.cn

Institut für Mathematik, Karl-FranzensUniversität, Heinrichstrasse 36, 8010 Graz, Austria
E-mail address: alfred.geroldinger@uni-graz.at