Rev. Mat. Iberoam. **32** (2016), no. 2, 571–588
DOI 10.4171/RMI/895

The system of sets of lengths in Krull monoids under set addition

Alfred Geroldinger and Wolfgang A. Schmid

Abstract. Let H be a Krull monoid with class group G and suppose that each class contains a prime divisor. Then every element $a \in H$ has a factorization into irreducible elements, and the set $\mathsf{L}(a)$ of all possible factorization lengths for a is the set of lengths of a. We consider the system $\mathcal{L}(H) = \{\mathsf{L}(a) \mid a \in H\}$ of all sets of lengths, and we characterize (in terms of the class group G) when $\mathcal{L}(H)$ is additively closed under set addition.

1. Introduction and main result

By a monoid, we mean a commutative cancellative semigroup with unit element, and we say that a monoid is atomic if every non-unit can be written as a finite product of irreducible elements (also called atoms). Let H be an atomic monoid. If $a \in H$ is a non-unit and $a = u_1 \cdots u_k$ is a factorization of a into k atoms, then k is called the length of the factorization. The set $\mathsf{L}(a) \subset \mathbb{N}$ of all possible factorization lengths is called the set of lengths of a. It is convenient to set $\mathsf{L}(a) = \{0\}$ for each unit $a \in H$, and we denote by $\mathcal{L}(H) = \{\mathsf{L}(a) \mid a \in H\}$ the system of sets of lengths of H. All v-noetherian monoids (in particular, Krull monoids and the monoids of non-zero elements of noetherian domains) are atomic monoids in which all sets of lengths are finite. Let $a, b \in H$. Then the sumset $\mathsf{L}(a) + \mathsf{L}(b) = \{l + l' \mid l \in \mathsf{L}(a),\, l' \in \mathsf{L}(b)\}$ is contained in $\mathsf{L}(ab)$. Thus, if $|\mathsf{L}(a)| > 1$ and $k \in \mathbb{N}$, then the k-fold sumset $k\mathsf{L}(a) = \mathsf{L}(a) + \cdots + \mathsf{L}(a)$ is contained in $\mathsf{L}(a^k)$, and hence $|\mathsf{L}(a^k)| > k$.

The system of sets of lengths $\mathcal{L}(H)$ is said to be *additively closed* if the sumset $L + L' \in \mathcal{L}(H)$ for all sets of lengths $L, L' \in \mathcal{L}(H)$. Clearly, set addition is commutative, $\{0\} = \mathsf{L}(1) \in \mathcal{L}(H)$ is the zero-element, and it is the only invertible element. Thus $\mathcal{L}(H)$ is additively closed if and only if $(\mathcal{L}(H), +)$ is a commutative reduced semigroup with respect to set addition. Indeed, in this case it is an acyclic semigroup in the sense of [8]. In this paper, Cilleruelo, Hamidoune,

Mathematics Subject Classification (2010): Primary 11B30; Secondary 11P70, 13A05, 20M13, 20M14.
Keywords: Krull monoids, sets of lengths, zero-sum sequences, minimal sets of distances, maximal orders.

and Serra study addition theorems in acyclic semigroups, and systems of subsets of certain semigroups with set addition as the operation belong to their main examples.

The system of sets of lengths (together with invariants controlling sets of lengths, such as elasticities and sets of distances) are the best investigated invariants in factorization theory. However, the system of sets of lengths has been explicitly determined only in some very special cases (they include Krull monoids with small class groups, see Theorem 7.3.2 in [15] and [3]; certain numerical monoids, [1]; and self-idealizations of principal ideal domains, see Corollary 16 in [7]). Recent studies of direct-sum decompositions in module theory revealed monoids of modules which are Krull and whose systems of sets of lengths are additively closed (see Section 6.3 in [3]). This phenomenon has not been observed so far in any relevant cases, and it has surprising consequences. Note that, if $H' \subset H$ is a divisor-closed submonoid, then $\mathcal{L}(H') \subset \mathcal{L}(H)$, and in all cases studied so far, a proper containment of the monoids implied a proper containment of their systems of sets of lengths. In contrast to this, suppose that H is an atomic monoid such that $\mathcal{L}(H)$ is additively closed. Then the direct product $H \times H$ is an atomic monoid, H is a divisor-closed submonoid of $H \times H$ (up to units), and $\mathcal{L}(H \times H) = \{L + L' \mid L, L' \in \mathcal{L}(H)\} = \mathcal{L}(H)$. Proposition 2.2 provides more sophisticated consequences of the fact that a system of sets of lengths is additively closed.

Krull monoids having the property that each class contains a prime divisor have found the greatest interest in factorization theory, and they will be the focus of the present paper. Their arithmetic can be studied with methods from additive combinatorics ([12]). Based on a couple of recent results (see the proofs of Propositions 3.1 and 3.13), we show that their systems of sets of lengths are additively closed only in a very small number of exceptional cases. Here is our main result.

Theorem 1.1. *Let H be a Krull monoid with class group G and suppose that each class contains a prime divisor. Then the system of sets of lengths $\mathcal{L}(H)$ is additively closed under set addition if and only if G has one of the following forms:*

(a) *G is cyclic of order $|G| \le 4$.*

(b) *G is an elementary 2-group of rank $r \le 3$.*

(c) *G is an elementary 3-group of rank $r \le 2$.*

(d) *G is infinite.*

Clearly, the groups given in (a)–(c) are precisely those groups G with $\exp(G) + \mathsf{r}(G) \le 5$. In Section 2 we outline that it is sufficient to prove Theorem 1.1 for a special class of Krull monoids and that the statement of Theorem 1.1 is valid too for classes of non-Krull monoids (see Proposition 2.1). The proof of Theorem 1.1 will be given in Section 3. The idea of the proof will be outlined after Proposition 3.1 when we have the required concepts at our disposal.

2. Context and applications

We denote by $\mathbb{N}$ the set of positive integers and set $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$. For real number $a, b \in \mathbb{R}$, we denote by $[a, b] = \{x \in \mathbb{Z} \mid a \le x \le b\}$ the discrete interval between a and b. For every positive integer $n \in \mathbb{N}$, C_n means a cyclic group of order n. Let $L, L' \subset \mathbb{Z}$ be subsets of the integers. Then $L + L' = \{a + b \mid a \in L, b \in L'\}$ is the *sumset* of L and L'. For $k \in \mathbb{N}$, we denote by $kL = L + \cdots + L$ the *k-fold sumset* of L and by $k \cdot L = \{ka \mid a \in L\}$ the *dilation* of L by k. A positive integer $d \in \mathbb{N}$ is called a *distance* of L if there exist elements $k, l \in L$ such that $k < l$, $d = l - k$, and $[k, l] \cap L = \{k, l\}$. We denote by $\Delta(L)$ the *set of distances* of L. We use the convention that $\max \emptyset = \min \emptyset = 0$.

By a *monoid*, we always mean a commutative semigroup with identity which satisfies the cancellation laws. If R is a domain, then the multiplicative monoid $R^\bullet = R \setminus \{0\}$ of nonzero elements of R is a monoid, and all terminology introduced for monoids will be used for domains in an obvious sense. In particular, we say that R is atomic if $R^\bullet$ is atomic, and we set $\mathcal{L}(R) = \mathcal{L}(R^\bullet)$ for the system of sets of lengths of R, and so on. A monoid F is called *free abelian with basis $P \subset F$* if every $a \in F$ has a unique representation of the form

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

Let F be free abelian with basis P. We set $F = \mathcal{F}(P)$ and call

- $|a| = \sum_{p \in P} \mathsf{v}_p(a)$ the *length* of a and
- $\operatorname{supp}(a) = \{p \in P \mid \mathsf{v}_p(a) > 0\}$ the *support* of a.

Clearly, $P \subset F$ is the set of primes of F, and if P is nonempty, then, for the system of sets of lengths, we have $\mathcal{L}(F) = \{\{y\} \mid y \in \mathbb{N}_0\}$. A monoid H is said to be a *Krull monoid* if it satisfies one of the following equivalent properties (see Theorem 2.4.8 in [15] or Chapter 22 of [19]):

(a) H is completely integrally closed and satisfies the ascending chain condition on divisorial ideals.

(b) H has a divisor homomorphism into a free abelian monoid (i.e., there is a homomorphism $\varphi\colon H \to \mathcal{F}(P)$ such that, for each two elements $a, b \in H$, a divides b in H if and only if $\varphi(a)$ divides $\varphi(b)$ in $\mathcal{F}(P)$).

A domain R is a Krull domain if and only if $R^\bullet$ is a Krull monoid, and thus property (a) shows that a noetherian domain is Krull if and only if it is integrally closed. Holomorphy rings in global fields and regular congruence monoids in these domains are Krull monoids with finite class groups such that each class contains infinitely many prime divisors (see Section 2.11 of [15]). Monoid domains and power series domains that are Krull are discussed in [21] and [6]. For monoids of modules that are Krull we refer to [5], [9], and [3].

We discuss a Krull monoid of a combinatorial flavor which plays a universal role in the study of sets of lengths in Krull monoids. Let G be an additive abelian group. Following the tradition of combinatorial number theory ([18]), the elements of $\mathcal{F}(G)$ will be called *sequences* over G. Let $S = g_1 \cdots g_l \in \mathcal{F}(G)$ be a sequence over G. Then $\sigma(S) = g_1 + \cdots + g_l \in G$ is the sum of S, and S is called a *zero-sum sequence* if $\sigma(S) = 0$. Clearly, the set $\mathcal{B}(G)$ of all zero-sum sequences over G is a submonoid of $\mathcal{F}(G)$, and the embedding $\mathcal{B}(G) \hookrightarrow \mathcal{F}(G)$ is a divisor homomorphism. Thus $\mathcal{B}(G)$ is a Krull monoid by Property (b). It is easy to check that $\mathcal{B}(G)$ is free abelian if and only if $|G| \le 2$. Suppose that $|G| \ge 3$. Then $\mathcal{B}(G)$ is a Krull monoid with class group isomorphic to G and each class contains precisely one prime divisor (see Proposition 2.5.6 in [15]).

The following proposition gathers together results demonstrating the universal role of the Krull monoid $\mathcal{B}(G)$ in the study of sets of lengths.

Proposition 2.1.

1) *If H is a Krull monoid with class group G such that each class contains a prime divisor, then $\mathcal{L}(H) = \mathcal{L}\big(\mathcal{B}(G)\big)$.*
2) *Let $\mathcal{O}$ be a holomorphy ring in a global field K, A a central simple algebra over K, and H a classical maximal $\mathcal{O}$-order of A such that every stably free left R-ideal is free. Then $\mathcal{L}(H) = \mathcal{L}\big(\mathcal{B}(G)\big)$, where G is a ray class group of $\mathcal{O}$ and hence finite abelian.*
3) *Let H be a seminormal order in a holomorphy ring of a global field with principal order $\widehat{H}$ such that the natural map $\mathfrak{X}(\widehat{H}) \to \mathfrak{X}(H)$ is bijective and there is an isomorphism $\overline{\vartheta}\colon \mathcal{C}_v(H) \to \mathcal{C}_v(\widehat{H})$ between the v-class groups. Then $\mathcal{L}(H) = \mathcal{L}\big(\mathcal{B}(G)\big)$, where $G = \mathcal{C}_v(H)$ is finite abelian.*

Proof. 1) See Section 3.4 of [15]. 2) See Theorem 1.1 in [24], and [4] for related results of this flavor. 3) See Theorem 5.8 in [16] for a more general result in the setting of weakly Krull monoids. □

Statements 2) and 3) say that the systems of sets of lengths of the monoids under consideration coincide with the system of sets of lengths of a Krull monoid as in Theorem 1.1, and hence we know when they are additively closed. Without going into details, we would like to mention that the same is true for certain non-commutative Krull monoids ([13]). Furthermore, Frisch [10] showed that, for the domain R of integer-valued polynomials over the integers, we have $\mathcal{L}(R) = \mathcal{L}\big(\mathcal{B}(G)\big)$ for an infinite group G.

We end this section by highlighting a surprising consequence of when the system of sets of lengths of a domain is additively closed.

Proposition 2.2. *Let R be an atomic domain, let $n \ge 2$ be an integer, and let $T_n(R)$ be the semigroup of upper triangular matrices with nonzero determinant. Then $\mathcal{L}(R) \subset \mathcal{L}\big(T_n(R)\big)$, and equality holds if and only if $\mathcal{L}(R)$ is additively closed.*

Proof. Let $H = R^\bullet$ denote the monoid of nonzero elements of R. Then Theorem 4.2 in [2] implies that $\mathcal{L}\big(T_n(H)\big)$ coincides with the system of sets of lengths of the n-fold direct product of H. Therefore

$$\mathcal{L}\big(T_n(H)\big) = \mathcal{L}(H \times \cdots \times H) = \big\{L_1 + \cdots + L_n \mid L_1, \ldots, L_n \in \mathcal{L}(H)\big\},$$

and thus the assertion follows. □

3. Proof of Theorem 1.1

Let G be an additively written finite abelian group. Then $G \cong C_{n_1} \oplus \ldots \oplus C_{n_r}$ with $1 < n_1 \mid \ldots \mid n_r$, where $r = \mathsf{r}(G) \in \mathbb{N}_0$ is the rank of G and $n_r = \exp(G)$ is the exponent of G. A tuple of elements $(e_1, \ldots, e_s) \in G^s$, with $s \in \mathbb{N}$, is said to be independent if $e_1, \ldots, e_s$ are non-zero and $\langle e_1, \ldots, e_s \rangle = \langle e_1 \rangle \oplus \ldots \oplus \langle e_s \rangle$. Furthermore, $(e_1, \ldots, e_s)$ is said to be a basis of G if it is independent and $\langle e_1, \ldots, e_s \rangle = G$.

We gather the necessary concepts describing the arithmetic of monoids of zero-sum sequences (for details and proofs, we refer to [15] and [12]). Let $G_0 \subset G$ be a subset. Then $\mathcal{B}(G_0) = \mathcal{B}(G) \cap \mathcal{F}(G_0)$ denotes the submonoid of zero-sum sequences over G_0. An atom of $\mathcal{B}(G_0)$ is a minimal zero-sum sequence over G_0, and we denote by $\mathcal{A}(G_0)$ the set of atoms of $\mathcal{B}(G_0)$. A sequence $S = g_1 \cdots g_l \in \mathcal{F}(G_0)$ is a (minimal) zero-sum sequence if and only if $-S = (-g_1) \cdots (-g_l)$ is a (minimal) zero-sum sequence. The set $\mathcal{A}(G_0)$ is finite and

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

is the *Davenport constant* of G_0. It is easy to see that $1 + \sum_{i=1}^{r}(n_i - 1) \le \mathsf{D}(G)$. We will use without further mention that equality holds for p-groups and for groups with rank $\mathsf{r}(G) \le 2$ (see Chapter 5 of [15]).

Factorization sets and sets of lengths. Let $\mathsf{Z}(G_0) = \mathcal{F}(\mathcal{A}(G_0))$ denote the factorization monoid of $\mathcal{B}(G_0)$ (thus, $\mathsf{Z}(G_0)$ is the monoid of formal products of minimal zero-sum sequences over G_0), and let $\pi \colon \mathsf{Z}(G_0) \to \mathcal{B}(G_0)$ denote the canonical epimorphism. For $A \in \mathcal{B}(G_0)$, $\mathsf{Z}(A) = \pi^{-1}(A) \subset \mathsf{Z}(G_0)$ is the set of factorizations of A. For a factorization $z \in \mathsf{Z}(A)$, we call $|z| \in \mathbb{N}_0$ the length of z and $\mathsf{L}(A) = \{|z| \mid z \in \mathsf{Z}(A)\} \subset \mathbb{N}_0$ is the set of lengths of A. Clearly, this coincides with the former informal definition. In particular, $\mathsf{L}(A) = \{0\}$ if and only if $A = 1$, and $\mathsf{L}(A) = \{1\}$ if and only if $A \in \mathcal{A}(G_0)$. Furthermore,

$$\mathcal{L}(G_0) := \mathcal{L}\big(\mathcal{B}(G_0)\big) = \{\mathsf{L}(B) \mid B \in \mathcal{B}(G_0)\}$$

is the system of sets of lengths of $\mathcal{B}(G_0)$. If $z, z' \in \mathsf{Z}(G_0)$ are two factorizations, say

$$z = U_1 \cdots U_l V_1 \cdots V_m \quad \text{and} \quad z' = U_1 \cdots U_l W_1 \cdots W_n\,,$$

where $l, m, n \in \mathbb{N}_0$, and all $U_i, V_j, W_k \in \mathcal{A}(G_0)$ with $\{V_1, \ldots, V_m\} \cap \{W_1, \ldots, W_n\} = \emptyset$, then $\mathsf{d}(z, z') = \max\{m, n\} \in \mathbb{N}_0$ is the distance between z and z'. The distance function $\mathsf{d} \colon \mathsf{Z}(G_0) \times \mathsf{Z}(G_0) \to \mathbb{N}_0$ has the usual properties of a metric.

Elasticities. Let $|G| \ge 3$. For $k \in \mathbb{N}$, we define

$$\rho_k(G) = \max\{\max L \mid k \in L \in \mathcal{L}(G)\}$$

and recall that (see Section 6.3 of [15])

$$\rho_{2k}(G) = k\mathsf{D}(G)\,, \quad 1 + k\mathsf{D}(G) \le \rho_{2k+1}(G) \le k\mathsf{D}(G) + \left\lfloor \frac{\mathsf{D}(G)}{2} \right\rfloor,$$

and that

$$\rho(G) = \max\left\{\frac{\max L}{\min L} \mid L \in \mathcal{L}(G)\right\} = \lim_{k\to\infty} \frac{\rho_k(G)}{k} = \frac{\mathsf{D}(G)}{2}\,.$$

Moreover, for $A \in \mathcal{B}(G)$, the following statements are equivalent:

- $\max \mathsf{L}(A)/\min \mathsf{L}(A) = \mathsf{D}(G)/2$.
- $A = (-U_1)U_1 \cdots (-U_j)U_j$ with $j \in \mathbb{N}$, $U_i \in \mathcal{A}(G)$ and $|U_i| = \mathsf{D}(G)$ for $i \in [1, j]$ (in which case $2j = \min \mathsf{L}(A)$).

Catenary degrees. The catenary degree $\mathsf{c}(A)$ of an element $A \in \mathcal{B}(G_0)$ is the smallest $N \in \mathbb{N}_0$ such that, for any two factorizations $z, z' \in \mathsf{Z}(A)$, there exist factorizations $z = z_0, z_1, \ldots, z_k = z'$ of A such that $\mathsf{d}(z_{i-1}, z_i) \le N$ for each $i \in [1, k]$. Then

$$\mathsf{c}(G_0) = \sup\{\mathsf{c}(A) \mid A \in \mathcal{B}(G_0)\}$$

denotes the catenary degree of G_0. It is easy to show that $\mathsf{c}(A) \le \max \mathsf{L}(A)$ and that $\mathsf{c}(G_0) \le \mathsf{D}(G_0)$.

Sets of distances. The set

$$\Delta(G_0) = \bigcup_{L\in\mathcal{L}(G_0)} \Delta(L)$$

is the *set of distances* of $\mathcal{B}(G_0)$. It is easy to verify that, for distinct $z, z' \in \mathsf{Z}(A)$, one has $d(z, z') \ge 2 + |(|z| - |z'|)|$. In particular, $|\mathsf{Z}(A)| \ge 2$ implies $2 + \max \Delta(\mathsf{L}(A)) \le \mathsf{c}(A)$, and if $\mathcal{B}(G_0)$ is not factorial, then $2 + \max \Delta(G_0) \le \mathsf{c}(G_0)$. We will further need that $\min \Delta(G_0) = \gcd \Delta(G_0)$, and we call

$$\Delta^*(G) = \{\min \Delta(G_1) \mid G_1 \subset G \text{ with } \Delta(G_1) \ne \emptyset\} \subset \Delta(G)$$

the *set of minimal distances* of $\mathcal{B}(G)$. We denote by $\Delta_1(G)$ the set of all $d \in \mathbb{N}$ with the following property:

> For every $k \in \mathbb{N}$ there is an $L \in \mathcal{L}(G)$ having the following form: $L = L' \cup \{y + \nu d \mid \nu \in [0, l]\} \cup L''$, where $l \ge k$, and L' and L'' are subsets of L with $\max L' < y$ and $y + ld < \min L''$.

The relevance of the sets $\Delta^*(G)$ and $\Delta_1(G)$ stems from their occurrence in the structure theorem for sets of lengths (see Proposition 3.1 below), and it will play a crucial role in the proof of Theorem 1.1. Let $d \in \mathbb{N}$, $M \in \mathbb{N}_0$ 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* $\mathcal{D}$, and *bound* M, if

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

where $y \in \mathbb{Z}$ is a shift parameter,

- L^* is finite nonempty with $\min L^* = 0$ and $L^* = (\mathcal{D} + d\mathbb{Z}) \cap [0, \max L^*]$, and
- $L' \subset [-M, -1]$ and $L'' \subset \max L^* + [1, M]$.

Proposition 3.1. *Let G be a finite abelian group.*

1) *There is a constant $M \in \mathbb{N}_0$ such that each $L \in \mathcal{L}(G)$ is an* AAMP *with difference $d \in \Delta^*(G)$ and bound M.*
2) $\Delta^*(G) \subset \Delta_1(G) \subset \{d_1 \in \Delta(G) \mid d_1$ *divides some* $d \in \Delta^*(G)\}$.
3) $\max \Delta^*(G) = \max\{\exp(G) - 2, \mathsf{r}(G) - 1\}$.

Proof. See Corollary 4.3.16 and Section 4.7 of [15] and [17]. □

Note that the description in 1) is best possible by the realization theorem in [23].

The proof of Theorem 1.1 is based on (all parts of) Proposition 3.1. We proceed in a series of propositions. The generic case is handled at the very end (in Proposition 3.13). The key idea is as follows. We choose a d_0 such that $L = \{2, 2 + d_0\} \in \mathcal{L}(G)$. If $\mathcal{L}(G)$ would be additively closed, then the k-fold sumset of L is in $\mathcal{L}(G)$ and hence $d \in \Delta_1(G)$. Comparing the maxima of $\Delta(G)$, $\Delta_1(G)$, and $\Delta^*(G)$, we obtain a contradiction. Unfortunately, $\max \Delta(G)$ is known only in very special cases (even $\max \Delta(C_n \oplus C_n)$ is unknown). If G is an elementary 2-group, then $\Delta(G) = \Delta^*(G)$. Thus elementary 2-groups need some extra care, and the same is true for elementary 3-groups. We start with an already known case, then we handle two special groups, and after that study elementary 2-groups (Proposition 3.5) and elementary 3-groups (Proposition 3.12).

Proposition 3.2. *Suppose that G is cyclic. Then $\mathcal{L}(G)$ is additively closed if and only if $|G| \le 4$.*

Proof. See Proposition 6.14 in [3]. □

Lemma 3.3. *Let $G = C_2 \oplus C_4$. Then $\mathcal{L}(G)$ is not additively closed.*

Proof. By an argument on page 411 of [15], for every $U \in \mathcal{A}(G)$ of length $|U| = 5$, there exist $(e_1, e_2) \in G^2$ with $\mathrm{ord}(e_1) = 2$ and $\mathrm{ord}(e_4) = 4$ such that $U = e_2^3 e_1(e_1 + e_2)$. Considering $U(-U)$ for such a U, it follows that $L = \{2, 4, 5\} \in \mathcal{L}(G)$.

We assert that the sumset $L + L = L_2 = \{4, 6, 7, 8, 9, 10\} \notin \mathcal{L}(G)$, which implies that $\mathcal{L}(G)$ is not additively closed.

We have $\mathsf{D}(G) = 5$ and $\rho(G) = 5/2$. Assume to the contrary that $L_2 \in \mathcal{L}(G)$. Since $\max L_2 / \min L_2 = 5/2$ and by a result recalled in Section 2, there exist minimal zero-sum sequences $U, V \in \mathcal{A}(G)$ with $|U| = |V| = 5$ such that

$$\mathsf{L}\big((-U)U(-V)V\big) = L_2\,.$$

Let (e_1, e_2) as above be given and suppose that $U = e_2^3 e_1(e_1 + e_2)$. We go through all cases for V and show that $5 \in \mathsf{L}\big((-U)U(-V)V\big)$, which implies the wanted contradiction. Note that $\mathrm{ord}(2e_2) = \mathrm{ord}(e_1 + 2e_2) = \mathrm{ord}(e_1) = 2$ and that $\mathrm{ord}(e_2) = \mathrm{ord}(-e_2) = \mathrm{ord}(e_1 + e_2) = \mathrm{ord}(e_1 - e_2) = 4$. Therefore we have

$$\begin{aligned} \{V \in \mathcal{A}(G) \mid |V| = 5\} = \{\, & V_1 = e_2^3 e_1(e_1 + e_2),\ -V_1,\\ & V_2 = e_2^3(e_1 + 2e_2)(e_1 - e_2),\ -V_2,\\ & V_3 = (e_1 + e_2)^3 e_1 e_2,\ -V_3,\\ & V_4 = (e_1 + e_2)^3(e_1 + 2e_2)(-e_2),\ -V_4 \,\}\,. \end{aligned}$$

Since

$$(-U)U(-V_1)V_1 = \big((e_1+e_2)^2e_2^2\big)\big(e_2^4\big)\big(e_1^2\big)(-U)(-U)\,,$$
$$(-U)U(-V_2)V_2 = \big(e_2^4\big)\big((e_1+e_2)(e_1+2e_2)e_2\big)\big(e_1(e_1-e_2)e_2\big)(-U)(-V_2)\,,$$
$$(-U)U(-V_3)V_3 = \big((e_1+e_2)^4\big)\big(e_2^4\big)\big(e_1^2\big)(-U)(-V_3)\,, \text{ and}$$
$$(-U)U(-V_4)V_4 = \big((e_1+e_2)^4\big)\big((e_1+2e_2)e_2^2e_1\big)\big((-e_2)e_2\big)(-U)(-V_4)\,,$$

it follows that $5 \in \mathsf{L}\big((-U)U(-V_\nu)V_\nu\big)$ for each $\nu \in [1,4]$. □

Lemma 3.4. *Let $G = C_5 \oplus C_5$. Then $\mathcal{L}(G)$ is not additively closed.*

Proof. Let $k \in \mathbb{N}$, (e_1, e_2) be a basis of G and $U = e_1^4e_2^4(e_1+e_2)$. Then $\mathsf{L}\big((-U)U\big) = \{2,5,8,9\}$, and we consider the k-fold sumset $L_k = L+\dots+L$. Clearly, $\min L_k = 2k$ and $\min(L_k \setminus \{2k\}) = 2k+3$. We assert that, for all sufficiently large k, $L_k \notin \mathcal{L}(G)$ which implies that $\mathcal{L}(G)$ is not additively closed.

We have $\mathsf{D}(G) = 9$, $\rho(G) = 9/2$, and we set $\{U_1, -U_1, \dots, U_s, -U_s\} = \{W \in \mathcal{A}(G) \mid |W| = 9\}$. Let $k \in \mathbb{N}$ and suppose that $L_k \in \mathcal{L}(G)$. Since $\max L_k / \min L_k = 9/2$ and by a result recalled in Section 2, there exist $k_1, \dots, k_s \in \mathbb{N}_0$ with $k_1 + \dots + k_s = k$ such that

$$\mathsf{L}\big((-U_1)^{k_1}U_1^{k_1}\cdots(-U_s)^{k_s}U_s^{k_s}\big) = L_k\,.$$

If k is sufficiently large, then there is a $\nu \in [1,s]$ such that $k_\nu \ge 2$. We assert that $3 \in \mathsf{L}(U_\nu^2)$ for each $\nu \in [1,s]$. This implies $2k+1 \in \mathsf{L}\big((-U_1)^{k_1}U_1^{k_1}\cdots(-U_s)^{k_s}U_s^{k_s}\big)$, a contradiction.

To prove the assertion, let $W \in \mathcal{A}(G)$ be of length $|W| = 9$. By Proposition 4.2 in [11], there exists a basis (f_1, f_2) of G such that

$$W = f_1^4(a_1f_1+f_2)(a_2f_1+f_2)(a_3f_1+f_2)(a_4f_1+f_2)(a_5f_1+f_2)\,,$$

with $a_1, \dots, a_5 \in [0,4]$. Then $W^2 = \big(f_1^5\big)S$ for some zero-sum sequence S over G. Since $|S| = 13 > \mathsf{D}(G) = 9$, $S \notin \mathcal{A}(G)$. It follows immediately that $\mathsf{L}(S) = \{2\}$ and hence $3 \in \mathsf{L}(W^2)$. □

We continue with elementary 2-groups. Let $G = C_2^r$ with $r \ge 2$. It is well-known that $\Delta(G) = \Delta^*(G) = [1, r-1]$ (see Corollary 6.8.3 in [15]). The next proposition summarizes our results for elementary 2-groups.

Proposition 3.5. *Let $G = C_2^r$ with $r \in \mathbb{N}$.*

1) *If $r = 1$, then $\mathcal{L}(G) = \big\{\{y\} \mid y \in \mathbb{N}_0\big\}$. In particular, $\mathcal{L}(G)$ is additively closed.*
2) *If $r = 2$, then $\mathcal{L}(G) = \big\{y + 2k + [0,k] \;\big|\; y, k \in \mathbb{N}_0\big\}$. In particular, $\mathcal{L}(G)$ is additively closed.*
3) *If $r = 3$, then* $$\mathcal{L}(C_2^3) = \big\{y + (k+1) + [0,k] \;\big|\; y \in \mathbb{N}_0,\ k \in [0,2]\big\} \cup \big\{y+k+[0,k] \;\big|\; y \in \mathbb{N}_0,\ k \ge 3\big\} \cup \big\{y+2k+2\cdot[0,k] \;\big|\; y, k \in \mathbb{N}_0\big\}.$$ *In particular, $\mathcal{L}(G)$ is additively closed.*
4) *If $r \ge 4$, then $\mathcal{L}(G)$ is not additively closed.*

The proof of Proposition 3.5 will be done in a series of lemmas. Since we believe that some are of interest in their own right we state them in more generality than needed for the immediate purpose at hand. We fix our notation which will remain valid till the end of the proof of Proposition 3.5. Let $G = C_2^r$ with $r \in \mathbb{N}$ and let $(e_1, \ldots, e_r)$ be a basis of G. Let $I, J \subset [1, r]$ be subsets. We denote by $I \triangle J = (I \cup J) \setminus (I \cap J)$ the symmetric difference. For an element $i \in [0, r] \setminus I$ we write $i \notin I$. If I is nonempty, then we set

$$e_I = \sum_{i \in I} e_i \,, \quad U_I = e_I \prod_{i \in I} e_i \,, \quad \text{and} \quad V_I = e_I \prod_{i \in [0,r] \setminus I} e_i \,.$$

Moreover, we set $e_0 = e_{[1,r]}$, $G_0 = \{e_0, \ldots, e_r\}$, and $V_0 = e_0 \cdots e_r$. Obviously, $\mathcal{A}(G_0) = \{h^2 \mid h \in G_0\} \cup \{V_0\}$ and $\mathcal{A}(G_0 \cup \{e_I\}) = \mathcal{A}(G_0) \cup \{U_I, V_I, e_I^2\}$.

Lemma 3.6. *Let $r \ge 3$.*

1) *Let $U = f_0 \cdots f_s \in \mathcal{A}(G)$ with $s \ge 2$.*
   (a) *The tuple $(f_1, \ldots, f_s)$ is independent and $f_0 = f_1 + \cdots + f_s$.*
   (b) *If $k \in \mathbb{N}$, then $\mathsf{L}(U^{2k}) = 2k + (s-1) \cdot [0, k] \in \mathcal{L}(G)$. In particular, $\Delta(\{f_0, \ldots, f_s\}) = \{s-1\}$.*
2) *If $A \in \mathcal{B}(G)$ and A is squarefree in $\mathcal{F}(G)$, then $\mathsf{c}(A) \le r$ and $\max \Delta(\mathsf{L}(A)) \le r - 2$.*

Proof. 1a) Corollary 5.1.9 in [15] implies that $(f_1, \ldots, f_s)$ is independent. Since U has sum zero, it follows that $f_0 = f_1 + \cdots + f_s$.

1b) Let $k \in \mathbb{N}$. Obviously, $\mathsf{L}(U^2) = \{2, s+1\}$, and $U, f_0^2, \ldots, f_s^2$ are the only atoms dividing U^{2k}. Thus $\mathsf{L}(U^{2k})$ is the k-fold sumset of $\mathsf{L}(U^2)$, and hence it has the asserted form. Let $d \in \Delta(\{f_0, \ldots, f_s\})$. Then there is a $B \in \mathcal{B}(\{f_0, \ldots, f_s\})$ with $d \in \Delta(\mathsf{L}(B))$. There is a $k \in \mathbb{N}$ such that $B \mid U^{2k}$, and we set $U^{2k} = BC$ with $C \in \mathcal{B}(\{f_0, \ldots, f_s\})$. If $m \in \mathsf{L}(C)$, then $m + \mathsf{L}(B) \subset \mathsf{L}(U^{2k}) = 2k + (s-1) \cdot [0, k]$, and hence $d = s - 1$.

2) Since $\max \Delta(\mathsf{L}(A)) \le \max\{0, \mathsf{c}(A) - 2\}$, it is sufficient to prove the statement on $\mathsf{c}(A)$ (recall our convention that $\max \emptyset = 0$). Furthermore, it is sufficient to consider squarefree zero-sum sequences A with $0 \nmid A$. We proceed by induction on $|A|$. Since $\mathsf{c}(A) \le \max \mathsf{L}(A)$, the assertion holds for all A with $\max \mathsf{L}(A) \le r$.

Let A be a squarefree zero-sum sequence with $0 \nmid A$, and let $z = U_1 \cdots U_m$ and $z' = V_1 \cdots V_n$ be factorizations of A with $m, n \in \mathbb{N}$ and $U_1, \ldots, U_m, V_1, \ldots, V_n \in \mathcal{A}(G)$. If $m \le r$ and $n \le r$, then $\mathsf{d}(z, z') \le r$, and we are done. So we suppose without restriction that $m > r$.

Suppose that $|V_1| = \ldots = |V_n| = \mathsf{D}(G) = r + 1$. Since A is squarefree, $\gcd_{\mathcal{F}(G)}(V_1, V_2) = 1$ whence $V_1 V_2 = W_1 \cdots W_t$ with $t \in [3, r]$, $W_1, \ldots, W_t \in \mathcal{A}(G)$, and $|W_1| \le r$. Since $\mathsf{d}(V_1 \cdots V_n, W_1 \cdots W_t V_3 \cdots V_n) = t \le r$, we may suppose – after a suitable change of notation – that $|V_1| \le r$.

Let $I \subset [1, m]$ be minimal such that $V_1 \mid \prod_{i \in I} U_i$, say $I = [1, l]$. Then $l \le |V_1| \le r < m$, and there are $k \in \mathbb{N}$ and $W_2, \ldots, W_k \in \mathcal{A}(G)$, such that

$$U_1 \cdots U_m = V_1 W_2 \cdots W_k U_{l+1} \cdots U_m = V_1 \cdots V_n \,.$$

By induction hypothesis, there are r-chains of factorizations from $U_1 \cdots U_{m-1}$ to $V_1 W_2 \cdots W_k U_{l+1} \cdots U_{m-1}$ and from $W_2 \cdots W_k U_{l+1} \cdots U_m$ to $V_2 \cdots V_n$. Multiplying the first chain with U_m and the second chain with V_1 we obtain an r-chain from $U_1 \cdots U_m$ to $V_1 \cdots V_n$. □

We already investigated the minimal zero-sum sequences over G_0 and one additional element. Next we consider the problem for two additional elements.

Lemma 3.7. *Let $r \ge 3$ and let $I, J \subset [1, r]$ with $|I|, |J| \in [2, r-1]$. The minimal zero-sum sequences over $G_0 \cup \{e_I, e_J\}$ which are divisible by $e_I e_J$ are*

- $U_{I,J} = e_I e_J \prod_{i \in I \triangle J} e_i$ *if $I \cap J \ne \emptyset$,*
- $V_{I,J} = e_I e_J \prod_{i \notin I \triangle J} e_i$ *if both $I \not\subset J$ and $J \not\subset I$.*

Proof. Let $A \in \mathcal{A}(G)$ with $e_I e_J \mid A$. If $I = J$, then $A = e_I^2 = U_{I,I}$. Suppose that $I \ne J$. Then $\mathsf{v}_{e_I}(A) = \mathsf{v}_{e_J}(A) = 1$.

If $e_0 \nmid A$, it follows that $A = e_I e_J \prod_{i \in I \triangle J} e_i$. Since A is neither divisible by U_I nor by U_J, it follows that $I \cap J \ne \emptyset$.

If $e_0 \mid A$, it follows that $A = e_I e_J \prod_{i \notin I \triangle J} e_i$. Again, any product of such a type lies in $\mathcal{A}(G)$ if and only if it is neither divisible by U_I nor by U_J (as it could only decompose as $U_I V_J$ and $U_J V_I$), which is the case precisely when neither $I \subset J$ nor $J \subset I$. □

We continue to use the notation $U_{I,J}$ and $V_{I,J}$ for all subsets $I, J \subset [1, r]$ (then $U_{I,J}$ and $V_{I,J}$ are not necessarily minimal zero-sum sequences).

Lemma 3.8. *Let $r \ge 3$ and let $I, J \subset [1, r]$ with $|I|, |J| \in [2, r]$.*

1) $\mathsf{L}(U_I U_J) = \{2, 1 + |I \cap J|\}$ *if $I \cap J \ne \emptyset$, and* $\mathsf{L}(U_I U_J) = \{2\}$ *otherwise.*
2) $\mathsf{L}(V_I V_J) = \{2, 1 + \delta + r + 1 - |I \cup J|\}$, *where $\delta = 0$ if $I \cap J \ne \emptyset$ and $\delta = 1$ otherwise.*
3) $\mathsf{L}(U_I V_J) = \{2, 1 + \delta + |I \setminus J|\}$, *where $\delta = 0$ if both $J \not\subset I$ and $I \not\subset J$, and $\delta = 1$ otherwise.*

Proof. 1) First, we note that if there exists a factorization of $U_I U_J$ other than this one, then it must contain a minimal zero-sum sequence containing both e_I and e_J. We have $U_I U_J = U_{I,J} \prod_{i \in I \cap J} e_i^2$. For $I \cap J \ne \emptyset$, we know by Lemma 3.7 that $U_{I,J}$ is a minimal zero-sum sequence, and we thus have a factorization of length $1 + |I \cap J|$. If however $I \cap J = \emptyset$, then $U_{I,J} = U_I U_J$.

2) Suppose $I \cap J = \emptyset$. Then $V_I V_J = U_I U_J \prod_{i \notin I \cup J} e_i^2$ and these two are the only factorizations not involving a minimal zero-sum sequence containing both e_I and e_J. In this case $U_{I,J}$, is not minimal. The only remaining factorization is thus $V_{I,J} V_0$

Suppose $I \cap J \ne \emptyset$. Then $V_I V_J$ is not divisible by U_I, U_J and $V_{I,J}$, since we do not have e_i in $V_I V_J$ for $i \in I \cap J$. The only other factorization is thus $U_{I,J} \prod_{i \notin I \cup J} e_i^2$.

3) If $J \subset I$, we note that $V_I \mid U_I V_J$ and we get the factorization $V_I U_J \prod_{i \in I \setminus J} e_i^2$. The only other factorization is $U_{I,J} V_0$.

If $J \not\subset I$, we note that e_i for $i \in J \setminus I$ does not appear in $U_I V_J$. Thus, $U_I V_J$ is not divisible by U_J and $U_{I,J}$. The only possibly other decomposition is thus $V_{I,J} \prod_{i \in I \setminus J} e_i^2$. Note that $V_{I,J}$ is minimal if and only if $I \not\subset J$. □

Lemma 3.9. *Let $r \geq 3$ and let $A \in \mathcal{A}(G)$ be such that $e_I \mid A$, where $I \subset [1, r]$ with $|I| \in [2, r-1]$. Then there exist $B, B' \in \mathcal{B}(G) \setminus \{1\}$ with $\max \mathsf{L}(B) \leq |I|$ and $\max \mathsf{L}(B') \leq r + 1 - |I|$ such that $AV_0 = V_I B = U_I B'$. In particular, if neither B nor B' is a minimal zero-sum sequence, then $\min(\mathsf{L}(AV_0) \setminus \{2\}) \leq \min\{|I| + 1, r + 2 - |I|\} \leq (r+3)/2$.*

Proof. Clearly, the sequences $F = e_I^{-1} A$, $S_V = \prod_{i \in I} e_i$, and $S_U = \prod_{i \notin I} e_i$ are zero-sum free, and we have $AV_0 = V_I(S_V F) = U_I(S_U F)$. We set $B = S_V F$ and $B' = S_U F$, and by Lemma 6.4.3 in [15] we infer that $\max \mathsf{L}(B) \leq |S_V|$ and $\max \mathsf{L}(B') \leq |S_U|$. The additional statement follows immediately. □

Lemma 3.10. *Let $r \geq 3$.*

1) *Let $A \in \mathcal{B}(G)$ with $\Delta(\mathsf{L}(A)) \neq \emptyset$. The following statements are equivalent:*
   (a) $r - 1 \in \Delta(\mathsf{L}(A))$.
   (b) *There is a basis $(f_1, \ldots, f_r)$ of G such that*
$$\operatorname{supp}(A) \setminus \{0\} = \{f_1, \ldots, f_r, f_1 + \cdots + f_r\}.$$
2) *Let $G_1 \subset G \setminus \{0\}$ be a subset. Then $\min \Delta(G_1) = r - 1$ if and only if $G_1 = \{f_1, \ldots, f_r, f_1 + \cdots + f_r\}$ for some basis $(f_1, \ldots, f_r)$ of G.*

Proof. 1) Lemma 3.6 shows that (b) implies (a). Conversely, let $A \in \mathcal{B}(G)$ such that $r - 1 \in \Delta(\mathsf{L}(A))$, say $[l, l+r-1] \cap \mathsf{L}(A) = \{l, l+r-1\}$. Since $\mathsf{c}(G) = r+1$ by Theorem 6.4.7 in [15], there exist factorizations z_1 and z_2 of A with $|z_1| = l$ and $|z_2| = l+r-1$ such that $\mathsf{d}(z_1, z_2) = r+1$, say $z_1 = U_1 \cdots U_s z$, $z_2 = V_1 \cdots V_t z$ where $z = \gcd(z_1, z_2)$, $U_1, \ldots, U_s, V_1, \ldots, V_t \in \mathcal{A}(G)$, and $\max\{s, t\} = t = r+1$. Since $|z_1| = s + |z| = l$ and $|z_2| = t + |z| = l + r - 1$, it follows that $t - s = r - 1$ whence $s = 2$ and $t = r + 1$. Thus $U_1 U_2 = V_1 \cdots V_{r+1}$, whence $U_1 = U_2$, $|U_1| = r+1$, and $|V_1| = \ldots = |V_{r+1}| = 2$. Without loss of generality assume that $U_1 = V_0$.

Assume A is not of the claimed form. Then there exists some $e_I \mid A$ with $|I| \in [2, r-1]$. Let $D \mid z$ with $D \in \mathcal{A}(G)$ be such that $e_I \mid D$. By Lemma 3.9 we have $DV_0 = V_I C_V = U_I C_U$ with $C_U, C_V \in \mathcal{B}(G) \setminus \{1\}$. Since $\max \mathsf{L}(DV_0) + |z| \in \mathsf{L}(A)$, the 'in particular' statement of Lemma 3.9 implies $C_U \in \mathcal{A}(G)$ or $C_V \in \mathcal{A}(G)$.

Thus, we have that $V_0 V_I C_V (D^{-1} z)$ or $V_0 U_I C_U (D^{-1} z)$ is a factorization of A of length $|z_1|$. Yet, by Lemma 3.8 it follows that $\mathsf{L}(V_0 V_I) = \{2, 1 + (r + 1 - |I|)\}$ and $\mathsf{L}(V_0 U_I) = \{2, 1 + |I|\}$. Thus, $l + r - |I|$ or $l + |I| - 1$ is an element of $\mathsf{L}(A)$, a contradiction.

2) That $\min \Delta(\{f_1, \ldots, f_r, f_1 + \cdots + f_r\}) = r - 1$ for a basis $(f_1, \ldots, f_r)$ follows by Lemma 3.6. Conversely, if $\min \Delta(G_1) = r-1$, then there exists some $A \in \mathcal{B}(G_1)$

with $r-1 \in \Delta(\mathsf{L}(A))$. By the first part, we get that $\operatorname{supp}(A) = \{f_1, \dots, f_r, f_1 + \dots + f_r\}$ for a basis $(f_1, \dots, f_r)$. If G_1 would contain any other element, it would equal $f_I = \sum_{i \in I} f_i$ with some $I \subset [1, r]$ and $|I| \in [2, r-1]$. Then, $f_I \prod_{i \in I} f_i \in \mathcal{A}(G_1)$ and Lemma 3.8.1 yields $|I| - 1 \in \Delta(G_1)$, a contradiction. □

Lemma 3.11. *Let $r \ge 4$, $B \in \mathcal{B}(G)$, and let $z_0 \in \mathsf{Z}(B)$ be a factorization of length $|z_0| = \min \mathsf{L}(B)$ such that $V_0^2 \,|\, z_0$. If $\min\big(\mathsf{L}(B) \setminus \min \mathsf{L}(B)\big) = \min \mathsf{L}(B) + (r-2)$, then $|\operatorname{supp}(B) \setminus (G_0 \cup \{0\})| = 1$ and this extra element is the sum of two distinct elements from G_0.*

Proof. By 2) in Lemma 3.10, $\operatorname{supp}(B) \setminus (G_0 \cup \{0\}) \ne \emptyset$, and hence there exists some $I \subset [0, r]$ such that $e_I \notin G_0$ and $e_I \mid B$. Let $A_I \in \mathcal{A}(G)$ be such that $A_I \mid z_0$ and $e_I \mid A_I$. Since $\min \mathsf{L}(B) - 2 + \mathsf{L}(A_I V_0) \subset \mathsf{L}(B)$ and since $r > (r+3)/2$, it follows by Lemma 3.9 that $A_I V_0 = W_I C_I$ with $W_I \in \{U_I, V_I\}$ and $C_I \in \mathcal{A}(G)$.

By Lemma 3.8 we have that $\mathsf{L}(U_I V_0) = \{2, |I| + 1\}$. Thus if $W_I = U_I$, we infer that $|I| - 1 \ge r - 2$ and thus $|I| = r - 1$. We also have $\mathsf{L}(V_I V_0) = \{2, 2 + r - |I|\}$. Thus if $W_I = V_I$, we infer that $|I| = 2$. Therefore we have shown that each non-zero element in $\operatorname{supp}(B) \setminus G_0$ is the sum of two distinct elements from G_0.

Now, we assume to the contrary that there exist two distinct sets $I, J \subset [1, r]$ such that $e_I, e_J \notin G_0$ and $e_I e_J \mid B$. Let $z_0' = W_I C_I ((A_I V_0)^{-1} z_0)$ be the factorization constructed above and note that V_0 divides z_0'. Let $A_J \in \mathcal{A}(G)$ be such that $A_J \mid z_0'$ and $e_J \mid A_J$. Note that $A_J \ne W_I$. As above we obtain that $A_J V_0$ equals $W_J C_J$ with $W_J \in \{U_J, V_J\}$, $C_J \in \mathcal{A}(G)$, and $|J| \in \{2, r-1\}$. In particular, we have a factorization $z_0'' \in \mathsf{Z}(B)$ of minimal length with $W_I W_J \,|\, z_0''$ and hence $\min \mathsf{L}(B) - 2 + \mathsf{L}(W_I W_J) \subset \mathsf{L}(B)$.

We analyze $\mathsf{L}(W_I W_J)$, and distinguish four cases. We use Lemma 3.8 throughout.

Case 1. $W_I = U_I$ and $W_J = U_J$.

We have $|I| = |J| = r - 1$ and thus $|I \cap J| = r - 2$ as $I \ne J$. Now $\mathsf{L}(U_I U_J) = \{2, |I \cap J| + 1\} = \{2, r-1\}$, a contradiction.

Case 2. $W_I = U_I$ and $W_J = V_J$.

We have $|I| = r - 1$ and $|J| = 2$. If $J \subset I$, then $\mathsf{L}(U_I V_J) = \{2, 2 + |I \setminus J|\} = \{2, r-1\}$, a contradiction. If $J \not\subset I$, then $\mathsf{L}(U_I V_J) = \{2, 1 + |I \setminus J|\} = \{2, r-1\}$, a contradiction.

Case 3. $W_I = V_I$ and $W_J = U_J$.

Completely analogous to Case 2.

Case 4. $W_I = V_I$ and $W_J = V_J$.

We have $|I| = |J| = 2$. If $I \cap J = \emptyset$, then $\mathsf{L}(V_I V_J) = \{2, 2 + r + 1 - |I \cup J|\} = \{2, r-1\}$, a contradiction. If $I \cap J \ne \emptyset$, then $\mathsf{L}(V_I V_J) = \{2, 1 + r + 1 - |I \cup J|\} = \{2, r-1\}$, a contradiction. □

Proof of Proposition 3.5. For $r \le 3$ the claim follows from Theorem 7.3.2 in [15]. We assume $r \ge 4$ and need to show that $\mathcal{L}(G)$ is not additively closed.

By Lemma 3.6, we infer that $L' = \{4, r+2, 2r\} \in \mathcal{L}(G)$ and $L_k'' = 2k + (r-1) \cdot [0, k] \in \mathcal{L}(G)$ for each $k \in \mathbb{N}$. We assert that the sumset $L_k = L' + L_k'' \notin \mathcal{L}(G)$ for all sufficiently large $k \in \mathbb{N}$. Assume to the contrary that there exist $B_k = 0^{v_k} B_k'$, where $v_k \in \mathbb{N}_0$ and $B_k' \in \mathcal{B}(G \setminus \{0\})$, such that $\mathsf{L}(B_k) = L_k$ for each $k \in \mathbb{N}$. Note that $\min L_k = 2k+4$, $\min L_k \setminus \{2k+4\} = 2k+r+2 = \min L_k + (r-2)$, and $\max L_k = k(r+1)+2r$. We consider a factorization of minimal length and one of maximal length, say

$$B_k = 0^{v_k} X_1 \cdots X_{2k+4-v_k} = 0^{v_k} Y_1 \cdots Y_{k(r+1)+2r-v_k}$$

where all $X_i, Y_j \in \mathcal{A}(G) \setminus \{0\}$. Then

$$\begin{aligned} v_k + 2\big(k(r+1)+2r-v_k\big) \le v_k + \sum_{\nu=1}^{k(r+1)+2r-v_k} |Y_\nu| = |B_k| \\ = v_k + \sum_{\nu=1}^{2k+4-v_k} |X_\nu| \le v_k + (2k+4-v_k)(r+1)\,. \end{aligned}$$

Since the difference between the upper and lower bound equals $4 - v_k(r-1)$, it follows that $v_k \le 1$, that at most 4 of the atoms $Y_1, \ldots, Y_{k(r+1)+2r-v_k}$ do not have length 2, at most four of the atoms $X_1, \ldots, X_{2k+4-v_k}$ do not have length $r+1$, and thus at least k of the X_i have length $r+1$. Since $\mathcal{A}(G)$ is finite, it follows that, for all sufficiently large k, any factorization of B_k of minimal length contains a minimal zero-sum sequence of length $r+1$ with multiplicity at least 6.

Now suppose that k is sufficiently large that this holds, and without restriction suppose that V_0 is the atom with multiplicity 6. By Lemma 3.11, $|\operatorname{supp}(B_k) \setminus (G_0 \cup \{0\})| = 1$ and this additional element is the sum of two distinct elements from G_0. Without restriction we may suppose that $e_0 + e_r = \sum_{i=1}^{r-1} e_i$ is this element. We set $I = [1, r-1]$ and assert that $\mathsf{v}_{e_I}(B_k) \in [2,4]$.

Assume to the contrary that $\mathsf{v}_{e_I}(B_k) = 1$. Then U_I and V_I are the only minimal zero-sum sequences containing e_I that divide B_k. We set $B_k = U_I C_k = V_I D_k$, with $C_k, D_k \in \mathcal{B}(G_0)$, and obtain that $\mathsf{Z}(B_k) = U_I \mathsf{Z}(C_k) \cup V_I \mathsf{Z}(D_k)$. By Lemma 3.6, $\mathsf{L}(C_k)$ and $\mathsf{L}(D_k)$ are arithmetical progressions with difference $r-1$, and thus $\mathsf{L}(B_k)$ is a union of two arithmetical progression with difference $r-1$, a contradiction to $\mathsf{L}(B_k) = L_k$.

The only minimal zero-sum sequences containing e_I over $\operatorname{supp}(B_k) \subset G_0 \cup \{0, e_I\}$ are e_I^2, U_I, and V_I, having lengths 2, r, and 3, respectively. If e_I^2 occurs, then rechecking the above chain of inequalities shows that there are at most two minimal zero-sum sequences in a factorization of minimal length that do not have length $r+1$, and hence $\mathsf{v}_{e_I}(B_k) \le 4$. If e_I^2 does not occur, then we also obtain that $\mathsf{v}_{e_I}(B_k) \le 4$, because we know that there are at most 4 of the minimal zero-sum sequences in a factorization of minimal length do not have length $r+1$.

Now, we assert that $\max \mathsf{L}(B_k) - 1 \in \mathsf{L}(B_k)$, a contradiction to $\max L_k - 1 \notin L_k$. Consider a factorization $z \in \mathsf{Z}(B_k)$ of maximal length $|z| = \max \mathsf{L}(B_k)$. We know that most 4 atoms dividing z do not have length 2, and thus the atoms e_0^2 and e_r^2 divide z; recall that V_0 has multiplicity 6 in B_k. Since $\mathsf{v}_{e_I}(B_k) \in [2,4]$ and the only atoms containing e_I over $\operatorname{supp}(B_k) \subset G_0 \cup \{0, e_I\}$ are e_I^2, U_I, and V_I, z is divisible by e_I^2, or by U_I^2, or by V_I^2, or by $U_I V_I$. Clearly, no factorization of maximal length is divisible by U_I^2 or by V_I^2. Since $U_I V_I = e_I^2 V_0$, we may assume without restriction that z is divisible by the atom e_I^2. Since z is also divisible by e_0^2 and by e_r^2, and since $e_I^2 e_0^2 e_r^2 = V_I^2$, we obtain a factorization of length $|z| - 1 = \max \mathsf{L}(B_k) - 1$, yielding the desired contradiction. □

We continue with elementary 3-groups. If $r \in [1,3]$, then $\Delta(C_3^r) = \Delta^*(C_3^r) = [1, \max\{r-1, 1\}]$ (this follows from Corollary 5.1 in [14]). If $r \ge 4$, then $[1, r-1] = \Delta^*(C_3^r) \subset \Delta(C_3^r)$, and it is an open problem whether equality holds or not.

Proposition 3.12. *Let $G = C_3^r$ with $r \in \mathbb{N}$.*

1) *If $r = 1$, then $\mathcal{L}(G) = \{y + 2k + [0,k] \mid y, k \in \mathbb{N}_0\}$. In particular, $\mathcal{L}(G)$ is additively closed.*
2) *If $r = 2$, then*

$$\mathcal{L}(G) = \big\{\{1\}\big\} \cup \big\{[2k, \nu] \mid k \in \mathbb{N}_0, \nu \in [2k, 5k]\big\} \cup \big\{[2k+1, \nu] \mid k \in \mathbb{N}, \nu \in [2k+1, 5k+2]\big\}.$$

In particular, $\mathcal{L}(G)$ is additively closed.

3) *If $r \ge 3$, then $\mathcal{L}(G)$ is not additively closed.*

Proof. Let $r \ge 2$, $(e_1, \ldots, e_r)$ be a basis of G, and $U = e_1^2 \cdots e_r^2 e_0$ with $e_0 = e_1 + \cdots + e_r$. We assert that

$$\mathsf{L}\big((-U)U\big) = [2, r+2] \cup \{2r+1\}.$$

Suppose that $(-U)U = V_1 \cdots V_s$ with $s \in \mathbb{N}$ and $V_1, \ldots, V_s \in \mathcal{A}(G)$. If $(-e_0)e_0 \in \{V_1, \ldots, V_s\}$, then $s = 2r+1$. Otherwise, we may suppose without restriction that $e_0 \mid V_s$ and $-e_0 \mid V_{s-1}$. There is a subset $J \subset [1,r]$ such that

$$V_s = e_0 \prod_{j \in J}(-e_j) \prod_{i \in I} e_i^2 \quad \text{and} \quad I = [1,r] \setminus I.$$

This implies that

$$V_{s-1} = (-e_0) \prod_{j \in J} e_j \prod_{i \in I} (-e_i)^2 = -V_s.$$

Therefore we obtain that $V_1 \cdots V_{s-2} = \prod_{j \in J}\big((-e_j)e_j\big)$ and hence $s = |J| + 2$. Summing up we infer that

$$\mathsf{L}\big((-U)U\big) = \{2r+1\} \cup \{2 + |J| \mid J \subset [0,r]\} = \{2r+1\} \cup [2, r+2].$$

1) By Theorem 7.3.2 in [15], $\mathcal{L}(G)$ has the given form, which immediately implies that $\mathcal{L}(G)$ is additively closed.

2) Suppose that $r = 2$. It is sufficient to show that $\mathcal{L}(G)$ has the asserted form. Then it can be verified immediately that $\mathcal{L}(G)$ is additively closed.

We have $\mathsf{D}(G) = 5$, $\rho(G) = 5/2$, $\Delta(G) = \{1\}$ (see Corollary 6.4.9 in [15]), and $\rho_k(G) = \lfloor k\mathsf{D}(G)/2 \rfloor$ by Theorem 6.3.4 in [15] for all $k \ge 2$. These facts imply that every $L \in \mathcal{L}(G)$ equals one of the sets given on the right hand side. So it remains to verify that conversely every set L given on the right hand side can be realized as a set of lengths in $\mathcal{L}(G)$. Clearly, $\{k\} \in \mathcal{L}(G)$ for each $k \in \mathbb{N}_0$. Let $k \in \mathbb{N}$.

First, we assert that $[2k, \nu] \in \mathcal{L}(G)$ for all $\nu \in [2k, 5k]$, and we proceed by induction on k. The construction above shows that $[2, 5] \in \mathcal{L}(G)$. If $W_3 = e_1 e_2 (-e_0)$, then $\mathsf{L}\big((-W_3)W_3\big) = [2, 3] \in \mathcal{L}(G)$. If $W_4 = e_1^2 e_2 (e_1 - e_2)$, then $\mathsf{L}\big((-W_4)W_4\big) = [2, 4] \in \mathcal{L}(G)$. Thus the assertion holds for $k = 1$. Suppose the assertion holds for $k \in \mathbb{N}$. If $\nu \in [2k, 5k]$ and $A_\nu \in \mathcal{B}(G)$ with $\mathsf{L}(A_\nu) = [2k, \nu]$, then $\mathsf{L}(0^2 A_\nu) = [2k+2, \nu+2]$. Thus it remains to show that $[2k+2, 5k+3], [2k+2, 5k+4]$, and $[2k+2, 5k+5] \in \mathcal{L}(G)$. If U, W_3, and W_4 are as above, then

$$\begin{aligned} \mathsf{L}\big((-U)^k U^k\big) &= [2k, 5k]\,, \\ \mathsf{L}\big((-U)^k U^k (-W_3) W_3\big) &= [2k+2, 5k+3]\,, \\ \mathsf{L}\big((-U)^k U^k (-W_4) W_4\big) &= [2k+2, 5k+4]\,, \quad \text{and} \\ \mathsf{L}\big((-U)^{k+1} U^{k+1}\big) &= [2k+2, 5k+5]\,. \end{aligned}$$

Next, we assert that $[2k+1, \nu] \in \mathcal{L}(G)$ for all $\nu \in [2k+1, 5k+2]$. If $k \in \mathbb{N}$, $\nu \in [2k, 5k]$, and $A_\nu \in \mathcal{B}(G)$ with $\mathsf{L}(A_\nu) = [2k, \nu]$, then $\mathsf{L}(0A_\nu) = [2k+1, \nu+1]$. Since $\rho_{2k+1}(G) = 5k+2$, there is a $B_k \in \mathcal{B}(G)$ with $2k+1, 5k+2 \in \mathsf{L}(B_k)$ and hence $\mathsf{L}(B_k) = [2k+1, 5k+2] \in \mathcal{L}(G)$.

3) Suppose that $r \ge 3$. Let $k \in \mathbb{N}$. We consider the k-fold sumset $L_k = L + \cdots + L$ of $L = \mathsf{L}\big((-U)U\big)$. We assert that, for all sufficiently large k, $L_k \notin \mathcal{L}(G)$, which implies that $\mathcal{L}(G)$ is not additively closed. We set $\{U_1, -U_1, \ldots, U_s, -U_s\} = \{W \in \mathcal{A}(G) \mid |W| = \mathsf{D}(G)\}$. Let $k \in \mathbb{N}$ and suppose that $L_k \in \mathcal{L}(G)$. Since $\max L_k / \min L_k$ equals $\rho(G)$ and by a result recalled in Section 2, there exist $k_1, \ldots, k_s \in \mathbb{N}_0$ with $k_1 + \cdots + k_s = k$ such that

$$\mathsf{L}\big((-U_1)^{k_1} U_1^{k_1} \cdots (-U_s)^{k_s} U_s^{k_s}\big) = L_k\,.$$

Note that $\max L_k = k(2r+1)$ and that $\max\big(L_k \setminus \{k(2r+1)\}\big) = k(2r+1) - (r-1)$. There is a unique factorization of length $\max L_k$. It consists entirely of atoms having length two. If k is sufficiently large, then there is a $\nu \in [1, s]$ such that $k_\nu \ge 3$, say $\nu = 1$ and $U_1 = gS$ with $g \in G$ and $S \in \mathcal{F}(G)$. Then the factorization of length $\max L_k$ contains the product $\big((-g)g\big)^3$. Since

$$\big((-g)g\big)^3 = (g^3)\big((-g)^3\big)\,,$$

it follows that $\max L_k - 1 \in \mathsf{L}\big((-U_1)^{k_1} U_1^{k_1} \cdots (-U_s)^{k_s} U_s^{k_s}\big)$, a contradiction. □

Finally, we handle the generic case.

Proposition 3.13. *Let G be a finite abelian group with $\exp(G) = n \ge 4$ and $r = \mathsf{r}(G) \ge 2$. Then $\mathcal{L}(G)$ is not additively closed.*

Proof. If $G = C_5 \oplus C_5$ or $G = C_2 \oplus C_4$, then the assertion follows from Lemma 3.3 and from Lemma 3.4. Let $G = C_{n_1} \oplus \ldots \oplus C_{n_r}$ with $1 < n_1 \mid \ldots \mid n_r$, $|G| \ge 5$, and suppose that G is distinct from the above two groups. Simple examples (see Theorem 6.6.2 in [15]) show that

$$\{2, d\} \in \mathcal{L}(G) \quad \text{for all} \quad d \in \big[3, \max\{n, d_0\}\big] , \quad \text{where} \quad d_0 = 1 + \sum_{i=1}^{\mathsf{r}(G)} \Big\lfloor \frac{n_i}{2} \Big\rfloor .$$

Assume to the contrary that $\mathcal{L}(G)$ is additively closed. Then $d-2 \in \Delta_1(G)$ for each d as above, in particular $d_0 - 2 \in \Delta_1(G)$, and the interval $[1, n-2] \subset \Delta_1(G)$. We use that $\max \Delta_1(G) \le \max \Delta^*(G) = \max\{r-1, n-2\}$ by Proposition 3.1.

If $r-1 \ge n-2$, then $n \ge 4$ implies that $d_0 - 2 > r - 1 = \max \Delta^*(G)$, a contradiction. Thus it follows that $r-1 < n-2$. We distinguish three cases.

Case 1. $G = C_n \oplus C_n$.

If n is even, then $d_0 - 2 = n-1 > n-2 = \max \Delta^*(G)$, a contradiction. Suppose that n is odd. Then $n \ge 7$ and $n-4 \in \Delta_1(G)$. By Corollary 3.8 in [22], it follows that

$$\max \Delta^*(C_n \oplus C_n) \setminus \{n-3, n-2\} = \frac{n-3}{2} .$$

Since $n \ge 7$, it follows that $n-4 > (n-3)/2$, a contradiction.

Case 2. G has a proper subgroup isomorphic to $C_n \oplus C_n$.

Then $d_0 - 2 \ge n-1 > n-2 = \max \Delta^*(G)$, a contradiction.

Case 3. G has no subgroup isomorphic to $C_n \oplus C_n$.

Then it follows that $n_{r-1} \le n_r/2$. If $r = n-2$, then $n \ge 6$ (because $G \notin \{C_2 \oplus C_4, C_5, C_5 \oplus C_5\}$) and thus

$$d_0 - 2 \ge r - 1 + \Big\lfloor \frac{n}{2} \Big\rfloor - 1 = n - 4 + \Big\lfloor \frac{n}{2} \Big\rfloor > n-2 ,$$

a contradiction.

Suppose that $r \le n-3$. Then $n \ge 5$. If $n = 5$, then G is either cyclic or has a subgroup isomorphic to $C_5 \oplus C_5$, a contradiction. Thus $n \ge 6$. Then Theorem 3.2 in [22] implies that

$$\Delta^*(G) \subset [1, \max\{\mathsf{m}(G), \lfloor n/2 \rfloor - 1\}] \cup \{n-2\} , \quad \text{where}$$

$$\mathsf{m}(G) = \max\{\min \Delta(G_0) \mid G_0 \subset G \text{ is a non-half-factorial LCN-set}\} .$$

Since $\mathsf{m}(G) < n-3$, by Lema 4.2 in [17], it follows that $\max\{\mathsf{m}(G), \lfloor n/2 \rfloor - 1\}] \le n-4$. This implies that $n-3 \notin \Delta^*(G)$, but $n-3 \in \Delta_1(G)$, a contradiction to 2) in Proposition 3.1. □

Proof of Theorem 1.1. Let H be a Krull monoid with class group G and suppose that each class contains a prime divisor. By Proposition 2.1, it is sufficient to consider the monoid $\mathcal{B}(G)$ instead of the monoid H.

First suppose that G is infinite. By the realization theorem of Kainrath, every finite subset $L \subset \mathbb{N}_{\ge 2}$ can be realized as a set of lengths in $\mathcal{L}(G)$. Thus we obtain that

$$\mathcal{L}(G) = \{L \subset \mathbb{N}_{\ge 2} \mid L \text{ is finite and nonempty}\} \ \cup \ \{\{0\}, \{1\}\} ,$$

(see [20] or Theorem 7.4.1 in [15]), which shows that $\mathcal{L}(G)$ is additively closed.

Suppose now that G is finite. Cyclic groups are considered in Proposition 3.2, elementary 2-groups are treated in Proposition 3.5, and elementary 3-groups in Proposition 3.12. The case of non-cyclic groups with exponent $n \geq 4$ is settled by Proposition 3.13. □

Acknowledgement. We would like to thank the referee for reading the paper very carefully and for making many helpful remarks.

References

[1] Amos, J., Chapman, S. T., Hine, N. and Paixão, J.: Sets of lengths do not characterize numerical monoids. *Integers* **7** (2007), A50, 8pp.

[2] Bachman, D., Baeth, N. R. and Gossell, J.: Factorizations of upper triangular matrices. *Linear Algebra Appl.* **450** (2014), 138–157.

[3] Baeth, N. R. and Geroldinger, A.: Monoids of modules and arithmetic of direct-sum decompositions. *Pacific J. Math.* **271** (2014), 257–319.

[4] Baeth, N. R. and Smertnig, D.: Factorization theory from commutative to non-commutative settings. *J. Algebra* **441** (2015), 475–551.

[5] Baeth, N. R. and Wiegand, R.: Factorization theory and decomposition of modules. *Amer. Math. Monthly* **120** (2013), no. 1, 3–34.

[6] Chang, G. W.: Every divisor class of Krull monoid domains contains a prime ideal. *J. Algebra* **336** (2011), 370–377.

[7] Chang, G. W. and Smertnig, D.: Factorization in the self-idealization of a PID. *Boll. Unione Mat. Ital. (9)* **6** (2013), 363–377.

[8] Cilleruelo, J., Hamidoune, Y. O. and Serra, O.: Addition theorems in acyclic semigroups. In *Additive number theory*, 99–104. Springer, 2010.

[9] Facchini, A.: Direct-sum decompositions of modules with semilocal endomorphism rings. *Bull. Math. Sci.* **2** (2012), no2, 225–279.

[10] Frisch, S.: A construction of integer-valued polynomials with prescribed sets of lengths of factorizations. *Monatsh. Math.* **171** (2013), no. 3-4, 341–350.

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

[12] Geroldinger, A.: Additive group theory and non-unique factorizations. In *Combinatorial number theory and additive group theory*, 1–86. Advanced Courses in Mathematics, CRM Barcelona, Birkhäuser Verlag, Basel, 2009.

[13] Geroldinger, A.: Non-commutative Krull monoids: a divisor theoretic approach and their arithmetic. *Osaka J. Math.* **50** (2013), 503–539.

[14] Geroldinger, A., Grynkiewicz, D. J. and Schmid, W. A.: The catenary degree of Krull monoids I. *J. Théor. Nombres Bordeaux* **23** (2011), no. 1, 137–169.

[15] Geroldinger, A. and Halter-Koch, F.: *Non-unique factorizations. Algebraic, combinatorial and analytic theory.* Pure and Applied Mathematics 278, Chapman & Hall/CRC, Boca Ratón, FL, 2006.

[16] Geroldinger, A., Kainrath, F. and Reinhart, A.: Arithmetic of seminormal weakly Krull monoids and domains. *J. Algebra* **444** (2015), 201–245.

[17] Geroldinger, A. and Zhong, Q.: The set of minimal distances in Krull monoids. *Acta Arith.* **173** (2016), 97–120.

[18] Grynkiewicz, D. J.: *Structural additive theory.* Developments in Mathematics, Springer, 2013.

[19] Halter-Koch, F.: *Ideal systems. An introduction to multiplicative ideal theory.* Monographs and Textbooks in Pure and Applied Mathematics 211, Marcel Dekker, New York, 1998.

[20] Kainrath, F.: Factorization in Krull monoids with infinite class group. *Colloq. Math.* **80** (1999), no. 1, 23–30.

[21] Kim, H. and Park, Y. S.: Krull domains of generalized power series. *J. Algebra* **237** (2001), no. 1, 292–301.

[22] Schmid, W. A.: 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), no. 1, 25–35.

[23] Schmid, W. A.: A realization theorem for sets of lengths. *J. Number Theory* **129** (2009), no. 5, 990–999.

[24] Smertnig, D.: Sets of lengths in maximal orders in central simple algebras. *J. Algebra* **390** (2013), 1–43.

Received July 6, 2014; revised March 7, 2015.

Alfred Geroldinger: Institut für Mathematik und Wissenschaftliches Rechnen, Karl–Franzens–Universität Graz, NAWI Graz, Heinrichstraße 36, 8010 Graz, Austria.
E-mail: alfred.geroldinger@uni-graz.at

Wolfgang A. Schmid: Université Paris 13, Sorbonne Paris Cité, LAGA, CNRS, UMR 7539, Université Paris 8, F-93430, Villetaneuse, France.
E-mail: schmid@math.univ-paris13.fr

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.