Wolfgang Alexander Schmid
Arithmetic of block monoids

Mathematica Slovaca, Vol. 54 (2004), No. 5, 503--526

Persistent URL: http://dml.cz/dmlcz/129295

Math. Slovaca, **54** (2004), No. 5, 503–526

Mathematica Slovaca

ARITHMETIC OF BLOCK MONOIDS

Wolfgang A. Schmid

(Communicated by Stanislav Jakubec)

ABSTRACT. We investigate block monoids, the monoid of zero-sum sequences, over abelian groups and their divisor-closed submonoids. We derive some results that can be used as tools when investigating the arithmetic of such monoids. Moreover, we investigate block monoids over so-called simple sets, the somehow simplest kind of sets with the property that the block monoids have non-unique factorization.

1. Introduction

We are interested in the arithmetic of Krull monoids with finite class group where every class contains a prime divisor. In particular, the multiplicative monoids of rings of integers are monoids with these properties. To understand the arithmetic of such monoids we investigate the arithmetic of block monoids over the divisor class group and of its divisor-closed submonoids.

Let G be an additively written, abelian group and $G_0 \subset G$ some subset. We denote by $\mathcal{F}(G_0)$ the free abelian monoid with basis G_0 and we refer to its elements as sequences. Then $\mathcal{B}(G_0)$, the block monoid over G_0, is the set of all zero-sum sequences, i.e. sequences $S = \prod_{i=1}^{l} g_i \in \mathcal{F}(G_0)$ such that the sum $\sigma(S) = \sum_{i=1}^{l} g_i = 0 \in G$. Since the embedding $\mathcal{B}(G_0) \hookrightarrow \mathcal{F}(G_0)$ is a divisor homomorphism, every block monoid is a Krull monoid (respectively a semigroup with divisor theory).

Block monoids were introduced in [Na79] and are used, via the notion of the divisor class group and appropriate transfer homomorphisms, to investigate various phenomena of non-unique-factorization for arbitrary Krull monoids and especially for algebraic number fields (cf. e.g. [Ge-HK92]). In particular, if one

2000 Mathematics Subject Classification: Primary 11R27, 20K99, 13F05.
Keywords: block monoid, factorization, Krull monoid, zero-sum sequence.

This work was supported by ÖAD Amadée 2003-2004, Projekt 05/2003.

is only interested in lengths of factorizations, then studying the associated block monoid is equivalent to studying the Krull monoid itself.

For a detailed description of the notion of the associated block monoid of a Krull monoid and further examples of Krull monoids respectively the application of block monoids we refer to the survey articles [HK97a] and [Ch-Ge97] in [An97] and the references given there. For the algebraic theory of Krull monoids, cf. [HK98; Chap. 22, Chap. 23].

In this article we do not investigate a particular phenomenon of non-unique-factorization in block monoids, but the results we obtain can be seen as tools suitable for application to different types of problems related to block monoids, such as half-factorial sets or differences in sets of lengths, cf. [Sch03b].

In particular, we will construct for some given $G_0 \subset G$ a set G_0^* such that $\mathcal{B}(G_0)$ and $\mathcal{B}(G_0^*)$ have the same arithmetic, but G_0^* is easier to handle from a group theoretical point of view (cf. Theorem 3.17).

In Section 4 we investigate the sets of atoms of block monoids over so-called simple sets (cf. Theorem 4.7). Sets which are simple sets in our terminology can be found in various contexts in treatise on factorization problems (cf. e.g. [Ch-Sm03a], [Ga-Ge98b], [Ga-Ge00], [Ge87], [Sl76]). Hence, it seems worthwhile to investigate them independently and beyond the needs of some particular problem.

2. Preliminaries

In this section we fix some notations and terminology, in particular for monoids and abelian groups. They mostly will be consistent with the usual ones in factorization theory (cf. the survey articles [HK97a] and [Ch-Ge97] in [An97]).

Let $\mathbb{Q}$ denote the rational numbers, $\mathbb{Z}$ the integers, $\mathbb{N}$ the set of positive integers, $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$ and $\mathbb{P} \subset \mathbb{N}$ the set of prime numbers. For $r, s \in \mathbb{Z}$ we set $[r, s] = \{z \in \mathbb{Z} : \ r \le z \le s\}$.

For a set P we denote by $|P| \in \mathbb{N}_0 \cup \{\infty\}$ its cardinality. For $x \in \mathbb{Q}$ let $\lceil x \rceil = \min\{z \in \mathbb{Z} : \ x \le z\}$ and $\lfloor x \rfloor = \max\{z \in \mathbb{Z} : \ x \ge z\}$.

A monoid is a commutative cancellative semigroup with identity element and we use multiplicative notation.

Let A, B be two subsets of some semigroup with operation $*$, then $A * B = \{a * b : \ a \in A \text{ and } b \in B\}$. In particular we will use this for subsets of $\mathbb{N}_0$ and addition as operation.

Let H be a monoid with identity element $1_H = 1 \in H$. We denote by $H^\times$ the group of invertible elements of H, and we call H *reduced* if $H^\times = \{1\}$. Let $H_1, H_2 \subset H$ be submonoids. Then we write $H = H_1 \times H_2$ if, for each $a \in H$, there exist uniquely determined $b \in H_1$ and $c \in H_2$ such that $a = bc$. For some subset $E \subset H$ we denote by $[E] \subset H$ the submonoid generated by E and we call H *finitely generated*, if there exists some finite $E' \subset H$ such that $[E'] = H$.

A submonoid $S \subset H$ is called *divisor-closed* if $a \in S$ and $b, c \in H$ such that $a = bc$ implies $b \in S$ and $c \in S$, i.e. for each $a \in S$ all divisors of a in H are elements of S. An element $u \in H \backslash H^\times$ is called *irreducible* (or an *atom*), if for all $a, b \in H$, $u = ab$ implies $a \in H^\times$ or $b \in H^\times$ and it is called *prime* (or a *prime element*) if for all $a, b \in H$, $u = ab$ implies $u \mid a$ or $u \mid b$. Let $\mathcal{A}(H) \subset H$ denote the set of atoms and $\mathcal{P}(H) \subset H$ the set of primes. Then $\mathcal{P}(H) \subset \mathcal{A}(H)$ and we call H *atomic* (respectively *factorial*) if every $a \in H \setminus H^\times$ has a factorization into a product of atoms (respectively primes).

Let $a \in H \setminus H^\times$ and $a = u_1 \cdots u_k$ a factorization of a into atoms $u_1, \ldots, u_k \in \mathcal{A}(H)$. Then k is called the *length of the factorization* and $\mathsf{L}_H(a) = \{k \in \mathbb{N} : \ a \text{ has a factorization length } k\} \subset \mathbb{N}$ denotes the set of lengths of a. We set $\mathsf{L}(a) = \{0\}$ for all $a \in H^\times$. The monoid H is called *BF-monoid* if it is atomic and $|\mathsf{L}(a)| < \infty$ for all $a \in H$, and it is called half-factorial monoid if it is atomic and $|\mathsf{L}(a)| = 1$ for all $a \in H$.

Let H be an atomic monoid. Then $\mathcal{L}(H) = \{\mathsf{L}(a) : \ a \in H\}$ denotes the system of sets of lengths of H.

For a set P we denote by $\mathcal{F}(P)$ the free abelian monoid with basis P. Every $a \in \mathcal{F}(P)$ has a unique representation in the form

$$a = \prod_{p \in P} p^{\mathsf{v}_p(a)}$$

where $\mathsf{v}_p(a) \in \mathbb{N}_0$ and $\mathsf{v}_p(a) = 0$ for all but finitely many $p \in P$.

A monoid homomorphism $\phi \colon H \to D$ is called a *divisor homomorphism* if, for all $a, b \in H$, $\phi(a) \mid \phi(b)$ implies $a \mid b$. The monoid H is called *Krull monoid* if it has a divisor homomorphism into a free monoid (cf. [HK98; Sec. 22.8, Sec. 23.4]). Every Krull monoid is a BF-monoid (cf. [Ch-Ge97; Lemma 2.7]).

Let G be an additively written abelian group and $G_0 \subset G$ a subset. Then $\langle G_0 \rangle \subset G$ denotes the subgroup generated by G_0, where $\langle \emptyset \rangle = \{0\}$.

The set G_0 (respectively its elements) is called *independent* if $0 \notin G_0$, $\emptyset \neq G_0$ and, given distinct elements $e_1, \ldots, e_r \in G_0$ and $m_1, \ldots, m_r \in \mathbb{Z}$, $\sum_{i=1}^{r} m_i e_i = 0$ implies that $m_1 e_1 = \cdots = m_r e_r = 0$. If we say that $\{e_1, \ldots, e_r\}$ is independent, then we will assume that the elements $e_1, \ldots, e_r$ are distinct.

An element $g \in G$ is called *torsion element* if there exists some $n \in \mathbb{N}$ such that $ng = 0$. If g is a torsion element, then we denote by $\operatorname{ord}(g) = \min\{n \in \mathbb{N} : ng = 0\}$ its order. G is called *abelian torsion group* if all elements of G are torsion elements.

For $n \in \mathbb{N}$ let C_n denote a cyclic group with n elements. Let G be a finite abelian group. Then there exist a uniquely determined $r \in \mathbb{N}$ and uniquely determined $n_1, \dots, n_r \in \mathbb{N}$ such that $G \cong C_{n_1} \oplus \cdots \oplus C_{n_r}$ and either $1 < n_1 \mid \dots \cdots \mid n_r$ or $r = 1$ and $n_r = 1$; $\mathsf{r}(G) = r$ is called the *rank* of G and $\exp(G) = n_r$ is called the *exponent* of G.

Furthermore if $|G| > 1$, then there exist a uniquely determined $r^* \in \mathbb{N}$ and up to order uniquely determined prime powers $q_1, \dots, q_{r^*}$, such that $G \cong C_{q_1} \oplus \cdots \oplus C_{q_{r^*}}$ and $\mathsf{r}^*(G) = r^*$ is called the *total-rank* of G.

G is called *p-group* if $\exp(G) = p^k$ with $p \in \mathbb{P}$ and $k \in \mathbb{N}$ and G is called *elementary p-group* if $\exp(G) = p \in \mathbb{P}$. Elementary p-groups are in a natural way vector spaces over the field $\mathbb{F}_p$ with p elements.

An element

$$S = \prod_{i=1}^{l} g_i = \prod_{g \in G_0} g^{\mathsf{v}_g(S)} \in \mathcal{F}(G_0)$$

is called a *sequence* in G_0, and for $g \in G_0$ we call $\mathsf{v}_g(S)$ the *multiplicity* of g in S. A sequence T is called *subsequence* of S if T divides S (in $\mathcal{F}(G_0)$). Let T be a subsequence of S, then we denote by $T^{-1}S$ the codivisor of T, i.e. the sequence $T' \in \mathcal{F}(G_0)$ such that $TT' = S$. We denote by

- $|S| = l \in \mathbb{N}_0$ the *length* of S.
- $\sigma(S) = \sum_{i=1}^{l} g_i \in G$ the *sum* of S.
- $\operatorname{supp}(S) = \{g_i : i \in [1, l]\} \subset G_0$ the *support* of S.
- $\mathsf{k}(S) = \sum_{i=1}^{l} \frac{1}{\operatorname{ord}(g_i)}$ the *cross number* of S.

Note that the sequence 1, the identity element of $\mathcal{F}(G_0)$, has length 0, sum 0, support $\emptyset$ and cross number 0. If we consider $|\cdot|$, v_g, σ and k as maps from $\mathcal{F}(G_0)$ to $(\mathbb{N}_0, +)$, G and $(\mathbb{Q}_{\geq 0}, +)$ respectively, then these maps define monoid-homomorphisms.

The sequence S is called a *zero-sum sequence* (a *block*), if $\sigma(S) = 0$, and S is called *zero-sumfree* if $\sigma(T) \neq 0$ for all subsequences $1 \neq T$ of S. A zero-sum sequence $1 \neq S$ is called *minimal zero-sum sequence* if for each proper subsequence T (i.e. with $T \neq S$), T is zero-sumfree. The empty sequence is the only zero-sum sequence that is zero-sumfree, but it is not a minimal zero-sum sequence.

The set $\mathcal{B}(G_0)$ consisting of all zero-sum sequences in G_0 is a submonoid of $\mathcal{F}(G_0)$, called the *block monoid over* G_0. It is a Krull monoid, thus it is a BF-monoid and its atoms are just the minimal zero-sum sequences. If $G_1 \subset G_0$, then $\mathcal{B}(G_1) \subset \mathcal{B}(G_0)$ is a divisor-closed submonoid. For ease of notation, we will write $\mathcal{A}(G_0)$ instead of $\mathcal{A}(\mathcal{B}(G_0))$ and do analogously for $\mathcal{P}(G_0)$ and $\mathcal{L}(G_0)$.

3. Submonoids of $\mathcal{B}(G)$

In this section we will investigate submonoids of $\mathcal{B}(G)$. As a first result we will show that the divisor-closed submonoids of $\mathcal{B}(G)$ are just the block monoids generated by subsets $G_0 \subset G$. Having this at hand we give methods to find, for some $H = \mathcal{B}(G_0)$, related monoids that are easier to handle, yet having the same systems of sets of lengths.

We start with a definition.

DEFINITION 3.1.

(1) A reduced monoid H is called

  (a) *minimal non-half-factorial*, if H is not half-factorial, but each divisor-closed submonoid $H' \subsetneq H$ is half-factorial.

  (b) *decomposable*, if there exist divisor-closed submonoids

$$\{1\} \neq H_1, H_2 \subsetneq H$$

  such that $H = H_1 \times H_2$ (otherwise *indecomposable*).

(2) A subset G_0 of an abelian group G is called *factorial* (*half-factorial*, *non-half-factorial*, *minimal non-half-factorial*, *decomposable*, *indecomposable*), if the block monoid $\mathcal{B}(G_0)$ has this property.

The following lemma will underline the importance of Definition 3.1.

LEMMA 3.2. *Let G be an abelian group and let $H \subset \mathcal{B}(G)$ be a submonoid. Then H is divisor-closed if and only if there exists a subset $G_0 \subset G$ such that $H = \mathcal{B}(G_0)$. Moreover, if G is an abelian torsion group, then G_0 is uniquely determined.*

Proof. Clearly for each $G_0 \subset G$ the monoid $\mathcal{B}(G_0)$ is a divisor-closed submonoid of $\mathcal{B}(G)$. Let $H \subset \mathcal{B}(G)$ be a divisor-closed submonoid. We set

$$G_0 = \bigcup_{B \in H} \operatorname{supp}(B).$$

We will prove that $H = \mathcal{B}(G_0)$. Obviously $H \subset \mathcal{B}(G_0)$. To prove the other inclusion, we note that for each $g \in G_0$ there exists some $S_g \in H$ such that $\mathsf{v}_g(S_g) > 0$. If $C = \prod_{i=1}^{l} g_i \in \mathcal{B}(G_0)$, then $C \mid \prod_{i=1}^{l} S_{g_i}$ in $\mathcal{B}(G_0)$, and since $\prod_{i=1}^{l} S_{g_i} \in H$, we obtain $C \in H$.

If G is an abelian torsion group, we have that $g^{\operatorname{ord}(g)} \in \mathcal{B}(G_0)$ if and only if $g \in G_0$. Clearly, this implies that G_0 is uniquely determined. $\square$

In Definition 3.1 we assigned monoid-theoretical properties to subsets of abelian groups. Next we will characterize subsets with these properties by their group-theoretical properties.

PROPOSITION 3.3. *Let G be an abelian group and let $G_0 \subset G$ a non-empty subset of torsion elements.*

(1) $\mathcal{P}(G_0) = \{g^{\mathrm{ord}(g)} : \langle G_0 \rangle = \langle g \rangle \oplus \langle G_0 \setminus \{g\} \rangle\}$.

(2) *G_0 is factorial if and only if $G_0 \setminus \{0\}$ is independent.*

Proof.

(1) Let $g \in G_0$ such that $\langle G_0 \rangle = \langle g \rangle \oplus \langle G_0 \setminus \{g\} \rangle$ and $B_1, B_2 \in \mathcal{B}(G_0)$ such that $g^{\mathrm{ord}(g)} \mid B_1 B_2$. Clearly $\mathsf{v}_g(B_1) > 0$ or $\mathsf{v}_g(B_2) > 0$. Without restriction we assume $\mathsf{v}_g(B_1) > 0$. We get $\sigma(B_1) = \mathsf{v}_g(B_1) g + h$ with $h \in \langle G_0 \setminus \{g\} \rangle$, hence $\mathsf{v}_g(B_1) g = 0$ and $\mathrm{ord}(g) \mid \mathsf{v}_g(B_1)$. Thus $g^{\mathrm{ord}(g)} \mid B_1$ and we get

$$\{g^{\mathrm{ord}(g)} : \langle G_0 \rangle = \langle g \rangle \oplus \langle G_0 \setminus \{g\} \rangle\} \subset \mathcal{P}(G_0).$$

Conversely, let $P \in \mathcal{P}(G_0)$. We first prove that $|\mathrm{supp}(P)| = 1$. Assume to the contrary, there exist distinct elements $g, h \in G_0$ with $g \mid P$ and $h \mid P$. We consider $P^{\mathrm{ord}(g)} = (g^{\mathsf{v}_g(P)\,\mathrm{ord}(g)}) B$ with $B \in \mathcal{B}(G_0 \setminus \{g\})$. Clearly $P \nmid B$ and $P \nmid g^{\mathsf{v}_g(P)\,\mathrm{ord}(g)}$, but $P \mid (g^{\mathsf{v}_g(P)\,\mathrm{ord}(g)}) B = P^{\mathrm{ord}(g)}$, which is a contradiction. Thus $P = g^{\mathrm{ord}(g)}$ with some $g \in G_0$.

It remains to verify that $\langle g \rangle \cap \langle G_0 \setminus \{g\} \rangle = \{0\}$. Assume to the contrary, that there exists some $n \in [1, \mathrm{ord}(g) - 1]$ and some $h \in \langle G_0 \setminus \{g\} \rangle$ such that $ng + h = 0$. Then there is some $S \in \mathcal{F}(G_0 \setminus \{g\})$ such that $\sigma(S) = h$. Thus we obtain $g^n S \in \mathcal{B}(G_0)$, $P \nmid g^n S$, but $P \mid (g^n S)^{\mathrm{ord}(g)}$, a contradiction.

(2) Clearly, we have $\{g^{\mathrm{ord}(g)} : g \in G_0\} \subset \mathcal{A}(G_0)$ and

$$\mathcal{A}(G_0) \subset \{g^{\mathrm{ord}(g)} : g \in G_0\}$$

if and only if $G_0 \setminus \{0\}$ is independent. Since block monoids are atomic, $\mathcal{B}(G_0)$ is factorial if and only if $\mathcal{A}(G_0) = \mathcal{P}(G_0)$. Consequently, if $\mathcal{B}(G_0)$ is factorial, then by (1),

$$\mathcal{A}(G_0) = \mathcal{P}(G_0) \subset \{g^{\mathrm{ord}(g)} : g \in G_0\},$$

hence $G_0 \setminus \{0\}$ is independent. Conversely, if $G_0 \setminus \{0\}$ is independent, then $\langle G_0 \rangle = \langle g \rangle \oplus \langle G_0 \setminus \{g\} \rangle$ for every $g \in G_0$, hence $\mathcal{P}(G_0) = \mathcal{A}(G_0)$. □

For a further characterization of factorial sets, cf. [Ge-HK92; Proposition 3]. At this point we give a group-theoretical characterization of half-factorial sets. The structure of half-factorial sets is in general not known (cf. [Ga-Ge98b] for various results on half-factorial sets). The fact that the characterization of half-factorial sets involves the cross numbers of atoms may serve as motivation for the investigations on atoms of simple sets. Moreover, we give some results on minimal non-half-factorial subsets.

The first part of the following proposition was obtained independently by several authors (cf. [Sk76; Theorem 3.1], [Sl76; Lemma 2] and [Za76; Proposition 1]).

PROPOSITION 3.4. *Let G be an abelian group and $G_0 \subset G$ a non-empty subset of torsion elements.*

(1) *The following conditions are equivalent:*
   (a) *G_0 is half-factorial.*
   (b) *$\mathsf{k}(A) = 1$ for each $A \in \mathcal{A}(G_0)$.*

(2) *The following conditions are equivalent:*
   (a) *G_0 is minimal non-half-factorial.*
   (b) *G_0 is not half-factorial and every proper subset $G_1 \subsetneq G_0$ is half-factorial.*
   (c) *There exists some $A \in \mathcal{A}(G_0)$ with*

$$\mathsf{k}(A) \neq 1 \qquad \textit{and} \quad \operatorname{supp}(A) = G_0$$

and for each $U \in \mathcal{A}(G_0)$ with $\operatorname{supp}(U) \subsetneq G_0$

$$\mathsf{k}(U) = 1\,.$$

(3) *Every minimal non-half-factorial set is finite.*

(4) *Every non-half-factorial set contains a minimal non-half-factorial subset.*

Proof.

(1) cf. [Ch-Ge97; Proposition 5.4] for a proof in the terminology of this article.

(2) (a) $\Longrightarrow$ (b): Clearly, G_0 is not half-factorial. Let $G_1 \subsetneq G_0$. Then $\mathcal{B}(G_1) \subsetneq \mathcal{B}(G_0)$ is a divisor-closed submonoid, hence it is half-factorial and consequently G_1 is half-factorial.

(b) $\Longrightarrow$ (c): For each $U \in \mathcal{A}(G_0)$ with $\operatorname{supp}(U) \subsetneq G_0$ we get that $\operatorname{supp}(U)$ is half-factorial. Since $U \in \mathcal{A}(\operatorname{supp}(U))$, we get $\mathsf{k}(U) = 1$. Since G_0 is not half-factorial, there exists some block $A \in \mathcal{A}(G_0)$ with $\mathsf{k}(A) \neq 1$ and clearly $\operatorname{supp}(A) = G_0$.

(c) $\Longrightarrow$ (a): If $A \in \mathcal{A}(G_0)$ with $\mathsf{k}(A) \neq 1$, then $\mathcal{B}(\operatorname{supp}(A))$ is non-half-factorial. Therefore G_0 is not half-factorial. Let $H \subsetneq \mathcal{B}(G_0)$ be a divisor-closed submonoid. By Lemma 3.2 there exists some $G_1 \subsetneq G_0$ such that $H = \mathcal{B}(G_1)$. Let $U \in \mathcal{A}(G_1)$. Clearly $\operatorname{supp}(U) \subset G_1 \subsetneq G_0$, hence $\mathsf{k}(U) = 1$ and H is half-factorial.

(3) follows immediately from (2)(c).

(4) is obvious for finite sets and clearly every non-half-factorial set contains some finite non-half-factorial set, e.g. $\operatorname{supp}(A)$ for some atom A with $\mathsf{k}(A) \neq 1$. $\square$

Proposition 3.4 can be used to determine all abelian torsion groups G that are half-factorial respectively factorial. This result was obtained in [Car] as result on number-fields and in [Za76; Theorem 8] it is formulated for Krull domains. In [Sk76; Proposition 3.2] the result was formulated for monoids. For convenience we state the proof.

PROPOSITION 3.5. *Let G be an abelian torsion group. Then the following statements are equivalent:*

(1) *G is factorial.*
(2) *G is half-factorial.*
(3) $|G| \le 2$.

Proof.

(1) $\Longrightarrow$ (2): Obvious.

(2) $\Longrightarrow$ (3): Let G be half-factorial. By Proposition 3.4.(1), $\mathsf{k}(A) = 1$ for each $A \in \mathcal{A}(G)$. Assume there exists some $g \in G$ with $\mathrm{ord}(g) = n > 2$, then $-gg \in \mathcal{A}(G)$ and $\mathsf{k}(-gg) = \frac{2}{n} \ne 1$. Thus $\mathrm{ord}(g) \le 2$ for each $g \in G$. Assume there exist two independent elements $g, h \in G$, then $(g+h)gh \in \mathcal{A}(G)$ and $\mathsf{k}\big((g+h)gh\big) = \frac{3}{2} \ne 1$. Consequently, if G is half-factorial, then $|G| \le 2$.

(3) $\Longrightarrow$ (1): Let $|G| \le 2$. By Proposition 3.3.(2) we get that G is factorial. □

Next we investigate decomposable and indecomposable monoids respectively sets.

LEMMA 3.6. ([Ge94; Lemma 2]) *Let H be a reduced atomic monoid.*

(1) *If $P = \mathcal{P}(H)$ is the set of all primes of H and $T \subset H$ the set of all $b \in H$ satisfying $p \nmid b$ for each $p \in P$, then $H = \mathcal{F}(P) \times T$.*
(2) *Let $H_1, H_2 \subset H$ be two submonoids. If $H = H_1 \times H_2$ and $a = a_1 a_2 \in H$ with $a_1 \in H_1$ and $a_2 \in H_2$, then*
$$\mathsf{L}_H(a) = \mathsf{L}_{H_1}(a_1) + \mathsf{L}_{H_2}(a_2)\,.$$
(3) *If $H = H_1 \times H_2$, then H is half-factorial if and only if H_1 and H_2 are half-factorial.*
(4) *If H is minimal non-half-factorial, then H is indecomposable.*

Proof.

(1) Cf. [Ge94; Lemma 2].

(2) From the definition of $\times$ it follows that for each $a \in H$ there exist uniquely determined $a_1 \in H_1$ and $a_2 \in H_2$ such that $a = a_1 a_2$ and we obtain $\mathcal{A}(H) = \mathcal{A}(H_1) \dot\cup \mathcal{A}(H_2)$. Thus the statement follows easily.

(3) follows immediately from (2).

(4) Let H be minimal non-half-factorial and assume to the contrary that there exist $\{1\} \ne H_1, H_2 \subsetneq H$ such that $H = H_1 \times H_2$. If H_1 and H_2 are half-factorial, then, by (3), H is half-factorial, which is a contradiction. However, if H_i is not half-factorial for some $i \in [1,2]$, then H is not minimal non-half-factorial, since H_i is a proper divisor-closed submonoid, which is a contradiction. Consequently, H is indecomposable. □

This lemma implies that, for almost all problems concerning sets of length, one can restrict to monoids without prime elements. In particular, for any $G_0 \subset G$ with $0 \in G_0$, we get that by Proposition 3.3.(1), $0 \in \mathcal{P}(G_0)$. Consequently, it is sufficient to investigate subsets not containing the 0 element.

The following result gives a characterization of indecomposable sets. Using this we will prove that every finitely generated, divisor-closed submonoid of $\mathcal{B}(G)$ can be uniquely written as product of indecomposable submonoids (cf. Theorem 3.11).

Proposition 3.7. *Let G be an abelian group and $G_0 \subset G$ a non-empty subset of torsion elements. Then the following conditions are equivalent:*

(1) *G_0 is decomposable.*
(2) *G_0 has a partition $G_0 = G_1 \dot\cup G_2$ with non-empty sets G_1, G_2 such that $\mathcal{B}(G_0) = \mathcal{B}(G_1) \times \mathcal{B}(G_2)$.*
(3) *G_0 has a partition $G_0 = G_1 \dot\cup G_2$ with non-empty sets G_1, G_2 such that $\langle G_0 \rangle = \langle G_1 \rangle \oplus \langle G_2 \rangle$.*

Proof. (1) and (2) are equivalent by Lemma 3.2, and clearly (3) implies (2). It remains to prove that (2) implies (3). Let $G_0 = G_1 \dot\cup G_2$ be a partition with non-empty subsets $G_1, G_2 \subset G_0$ such that $\mathcal{B}(G_0) = \mathcal{B}(G_1) \times \mathcal{B}(G_2)$. We have to verify that $\langle G_1 \rangle \cap \langle G_2 \rangle = \{0\}$. Let

$$g^* = \sum_{g \in G_1} n_g g = \sum_{g \in G_2} (-n_g) g \in \langle G_1 \rangle \cap \langle G_2 \rangle$$

with $n_g \in \mathbb{N}_0$ for each $g \in G_0$ and $n_g = 0$ for all but finitely many. (To consider just non-negative n_g is no restriction, since the order of all elements is finite.)

Then $B = \prod_{g \in G_0} g^{n_g} \in \mathcal{B}(G_0)$ has a factorization of the form $B = B_1 B_2$ with $B_i \in \mathcal{B}(G_i)$ for each $i \in [1,2]$. Obviously, we have $B_i = \prod_{g \in G_i} g^{n_g}$, hence $g^* = \sum_{g \in G_1} n_g g = 0$. □

Definition 3.8. Let G be an abelian group and $G_0 \subset G$ a non-empty subset of torsion elements. A non-empty subset $G_1 \subset G_0$ is called a *component* of G_0 if $\langle G_0 \rangle = \langle G_1 \rangle \oplus \langle G_0 \setminus G_1 \rangle$.

Lemma 3.9. *Let G be an abelian group and let $G_0 \subset G$ be a subset of torsion elements.*

(1) *If $|G_0| = 1$, then G_0 is indecomposable.*
(2) *If $|G_0| > 1$ and $\mathcal{P}(G_0) \neq \emptyset$, then G_0 is decomposable.*

P r o o f . The first part of the lemma is obvious. Let $|G_0| > 1$ and $P \in \mathcal{P}(G_0)$. From Proposition 3.3.(1) we know that $P = g^{\mathrm{ord}(g)}$ with some $g \in G_0$ such that $\langle G_0 \rangle = \langle g \rangle \oplus \langle G_0 \setminus \{g\} \rangle$, hence setting $G_1 = \{g\}$ we get that G_0 is decomposable. □

PROPOSITION 3.10. *Let G be an abelian group and $G_0 \subset G$ a non-empty and finite subset of torsion elements. Then there exist a uniquely determined $d \in \mathbb{N}$ and (up to order) uniquely determined indecomposable sets $\emptyset \ne G_1, \dots, G_d \subset G_0$ such that*

$$G_0 = \dot{\bigcup}_{i=1}^{d} G_i \qquad \text{and} \qquad \langle G_0 \rangle = \bigoplus_{i=1}^{d} \langle G_i \rangle .$$

P r o o f . We prove the existence of such sets via induction on $|G_0|$. For $|G_0| = 1$ it is obvious that G_0 is indecomposable, hence we set $d = 1$ and $G_0 = G_1$. Let $|G_0| > 1$. If G_0 is indecomposable, we set $d = 1$ and $G_0 = G_1$. Let G_0 be decomposable. Hence there exists some $\emptyset \ne G_0' \subsetneq G_0$ such that

$$\langle G_0 \rangle = \langle G_0' \rangle \oplus \langle G_0 \setminus G_0' \rangle .$$

Since $|G_0'| < |G_0|$ and $|G_0 \setminus G_0'| < |G_0|$, we get that there exist $d', d'' \in \mathbb{N}$ and indecomposable sets $\emptyset \ne G_1', \dots, G_{d'}' \subset G_0'$, such that

$$\langle G_0' \rangle = \bigoplus_{i=1}^{d'} \langle G_i' \rangle ,$$

as-well as indecomposable sets $\emptyset \ne G_1'', \dots, G_{d''}'' \subset G_0 \setminus G_0'$ such that

$$\langle G_0 \setminus G_0' \rangle = \bigoplus_{i=1}^{d''} \langle G_i'' \rangle .$$

Clearly, $G_0 = \dot{\bigcup}_{i=1}^{d'} G_i' \dot{\cup} \dot{\bigcup}_{i=1}^{d''} G_i''$ and

$$\langle G_0 \rangle = \bigoplus_{i=1}^{d'} \langle G_i' \rangle \oplus \bigoplus_{i=1}^{d''} \langle G_i'' \rangle .$$

It remains to prove uniqueness. We proceed by induction on the minimal number d^* for which there exist non-empty, indecomposable sets $G_1, \dots, G_{d^*}$ having the required properties. If $d^* = 1$, then G_0 is indecomposable and the assertion follows. Suppose $d^* > 1$ and let

$$\emptyset \ne G_1, \dots, G_{d^*} \subset G_0$$

be indecomposable sets with the required properties. Furthermore, let $\bar{d} \in \mathbb{N}$ and

$$\emptyset \ne H_1, \dots, H_{\bar{d}} \subset G_0$$

be indecomposable sets with

$$G_0 = \dot{\bigcup}_{i=1}^{\bar{d}} H_i \qquad \text{and} \quad \langle G_0 \rangle = \bigoplus_{i=1}^{\bar{d}} \langle H_i \rangle .$$

We assert that there exists some $j \in [1, \bar{d}]$ such that $G_{d^*} = H_j$. We have

$$G_{d^*} = G_{d^*} \cap G_0 = G_{d^*} \cap \left(\dot{\bigcup}_{i=1}^{\bar{d}} H_i \right) = \dot{\bigcup}_{i=1}^{\bar{d}} (G_{d^*} \cap H_i)$$

and hence $\langle G_{d^*} \rangle = \bigoplus_{i=1}^{\bar{d}} \langle G_{d^*} \cap H_i \rangle$. Since G_{d^*} is indecomposable, Proposition 3.7 implies that there is some $j \in [1, \bar{d}]$ such that $G_{d^*} = G_{d^*} \cap H_j$ and $G_{d^*} \cap H_i = \emptyset$ for each $i \in [1, \bar{d}] \setminus \{j\}$. Consequently, $G_{d^*} \subset H_j$.

Similarly, we obtain $H_j \subset G_k$ for some $k \in [1, d^*]$. This implies that $G_{d^*} \subset H_j \subset G_k$ and hence $k = d^*$ and $G_{d^*} = H_j$.

We consider the set $G_0 \setminus G_{d^*} = \dot{\bigcup}_{i=1}^{d^*-1} G_i$. By induction hypothesis we get that $d^* - 1 = \bar{d} - 1$ and that the indecomposable sets are uniquely determined. □

THEOREM 3.11. *Let G be an abelian torsion group and let $\{1\} \neq H \subset \mathcal{B}(G)$ be a finitely generated, divisor-closed submonoid. Then there exist a uniquely determined $d \in \mathbb{N}$ and up to order uniquely determined indecomposable, divisor-closed submonoids $\{1\} \neq H_1, \dots, H_d \subset \mathcal{B}(G)$ such that $H = H_1 \times \dots \times H_d$.*

Proof. By Lemma 3.2 there exists a uniquely determined subset $G_0 \subset H$ such that $H = \mathcal{B}(G_0)$ and, since $\{1\} \neq H$ and H is finitely generated, we have that $0 < |G_0| < \infty$. By Proposition 3.10 we obtain that there exist a uniquely determined $d \in \mathbb{N}$ and (up to order) uniquely determined indecomposable sets $\emptyset \neq G_1, \dots, G_d \subset G_0$ such that

$$G_0 = \dot{\bigcup}_{i=1}^{d} G_i \qquad \text{and} \qquad \langle G_0 \rangle = \bigoplus_{i=1}^{d} \langle G_i \rangle .$$

By Proposition 3.7 and induction on d we obtain $\mathcal{B}\left(\dot{\bigcup}_{i=1}^{d} G_i\right) = \mathcal{B}(G_1) \times \dots \cdots \times \mathcal{B}(G_d)$. Clearly, $\mathcal{B}(G_i)$ is indecomposable for each $i \in [1, d]$, which proves the existence of the decomposition.

Conversely, for any decomposition $d' \in \mathbb{N}$ and indecomposable, divisor-closed submonoids $\{1\} \neq H'_1, \dots, H'_d \subset H$ such that $H = H'_1 \times \dots \times H'_{d'}$, we obtain by Lemma 3.2 that for each $j \in [1, d']$, $H'_j = \mathcal{B}(G'_j)$ with some uniquely determined indecomposable set $G'_j \neq \emptyset$. Clearly, $G_0 = \dot{\bigcup}_{i=1}^{d'} G'_j$ and again by induction on d'

and Proposition 3.7 we obtain that $\langle G_0\rangle = \bigoplus_{j=1}^{d'} \langle G'_j\rangle$. By Proposition 3.10 we have $d' = d$ and for each $i \in [1,d]$ there exists some $j \in [1,d]$ such that $G_i = G'_j$ and thus $H_i = H'_j$. □

In the sequel we recall the notion of transfer homomorphisms (cf. [HK97a] for a detailed treatment). We will apply transfer homomorphisms to construct, for some set $G_0 \subset G$, an associated subset that has an easier structure, yet the same system of sets of lengths (cf. Lemma 3.15 and Theorem 3.17). Moreover, we will show how this procedure can be used to construct sets with prescribed properties (e.g. half-factorial sets).

We demonstrate this procedure in a simple special case.

EXAMPLE 3.12. Let $p \in \mathbb{P}$, $G = C_{p^2}^2$, $\{e_1, e_2\}$ be an independent generating subset of G and $G_0 = \{e_1 + e_2, pe_1, pe_2\}$. Then

$$\mathcal{A}(G_0) = \left\{(e_1+e_2)^{jp}(pe_1)^{p-j}(pe_2)^{p-j} : j \in [1,p]\right\} \cup \left\{(pe_1)^p, (pe_2)^p\right\}.$$

In particular, for each $B \in \mathcal{B}(G_0)$ we get $p \mid \mathsf{v}_{e_1+e_2}(B)$. Hence for $G_0^* = \{p(e_1+e_2), pe_1, pe_2\}$ the map

$$\phi : \begin{cases} \mathcal{B}(G_0) & \to \mathcal{B}(G_0^*), \\ (e_1+e_2)^x (pe_1)^y (pe_2)^z & \mapsto \big(p(e_1+e_2)\big)^{\frac{x}{p}} (pe_1)^y (pe_2)^z \end{cases}$$

is an isomorphism.

DEFINITION 3.13. A monoid epimorphism $\Theta \colon H \to B$ of reduced monoids is called a *transfer homomorphism* if the following two conditions are satisfied:

(1) $\Theta^{-1}(1) = \{1\}$.
(2) If $a \in H$ and $\Theta(a) = \beta\gamma$ with $\beta, \gamma \in B$, then there exist $b, c \in H$ such that $a = bc$, $\Theta(b) = \beta$ and $\Theta(c) = \gamma$.

LEMMA 3.14. *Let $\Theta \colon H \to B$ be a transfer homomorphism of reduced atomic monoids.*

(1) $\mathsf{L}_H(a) = \mathsf{L}_B\big(\Theta(a)\big)$ *for each* $a \in H$.
(2) *H is half-factorial if and only if B is half-factorial.*
(3) *If H is minimal non-half-factorial, then B is minimal non-half-factorial.*

Proof.

(1) is proved in [HK97; Lemma 5.4].

(2) is obvious from (1).

(3) Let H be minimal non-half-factorial. Clearly B is not half-factorial. Let $B' \subsetneq B$ be a divisor-closed submonoid. We need to prove that B' is half-factorial. We show that

$$H' = \Theta^{-1}(B') \subset H$$

is a proper divisor-closed submonoid. Thus H' is half-factorial, hence by (2), $B' = \Theta(H')$ is half-factorial.

Since Θ is surjective, we get $H' \subsetneq H$, and since Θ is a homomorphism, we get H' is a submonoid of H. It remains to prove that H' is divisor-closed. Let $a \in H'$ and $a = bc$. We get $\Theta(a) = \Theta(b)\Theta(c) \in B'$. Since B' is divisor-closed, we get $\Theta(b), \Theta(c) \in B'$, consequently $b, c \in H'$ and H' is divisor-closed. $\square$

LEMMA 3.15. *Let G be an abelian group, $G_0 \subset G$ a non-empty subset of torsion elements, $g \in G_0$ and $m = \min\{m' \in \mathbb{N} : \ m'g \in \langle G_0 \setminus \{g\}\rangle\}$. Then $m \mid \operatorname{ord}(g)$ and*

$$\Theta = \Theta_{g,m} : \begin{cases} \mathcal{B}(G_0) & \to \mathcal{B}\big(G_0 \setminus \{g\} \cup \{mg\}\big)\,, \\ B & \mapsto g^{-\mathsf{v}_g(B)}(mg)^{\frac{\mathsf{v}_g(B)}{m}} B \end{cases}$$

is a transfer homomorphism.

Proof. Let $n = \operatorname{ord}(g)$ and $G_0^* = G_0 \setminus \{g\} \cup \{mg\}$. Since $0 = ng \in \langle G_0 \setminus \{g\}\rangle$, we get $m \in [1, n]$.

If $m = 1$, we get $G_0 = G_0^*$, $\Theta = \mathrm{id}_{\mathcal{B}(G_0)}$ and the statement is obvious. Suppose that $1 < m < n$. First we prove that Θ is well-defined. This means we need to prove that for any $B \in \mathcal{B}(G_0)$ we get $m \mid \mathsf{v}_g(B)$.

Let $B \in \mathcal{B}(G_0)$. Since B has sum zero, it follows that $\mathsf{v}_g(B)g \in \langle G_0 \setminus \{g\}\rangle$. If $x, y \in \mathbb{Z}$ with $xm + y\mathsf{v}_g(B) = \gcd\big(m, \mathsf{v}_g(B)\big)$, then

$$\gcd\big(m, \mathsf{v}_g(B)\big)g = x(mg) + y\big(\mathsf{v}_g(B)g\big) \in \langle G_0 \setminus \{g\}\rangle\,.$$

Thus the minimality of m implies that $m = \gcd\big(m, \mathsf{v}_g(B)\big)$. Setting $B = g^n$ we infer that $m \mid n$.

Obviously Θ is an epimorphism and $\Theta^{-1}(1) = \{1\}$.

Let $B \in \mathcal{B}(G_0)$ and $C, C_1, C_2 \in \mathcal{B}(G_0^*)$, such that $\phi(B) = C$ and $C = C_1C_2$. We need to prove that there exist $B_1, B_2 \in \mathcal{B}(G_0)$, such that $\Theta(B_i) = C_i$ for each $i \in [1,2]$ and $B = B_1B_2$. We set $t = \min\Big\{\mathsf{v}_{mg}(C_1), \frac{\mathsf{v}_g(B)}{m}\Big\}$. Then

$$\mathsf{v}_{mg}(C_1C_2) = \mathsf{v}_{mg}(B) + \frac{\mathsf{v}_g(B)}{m}$$

implies that

$$\mathsf{v}_{mg}(C_2) = \mathsf{v}_{mg}(B) + \frac{\mathsf{v}_g(B)}{m} - \mathsf{v}_{mg}(C_1) \geq \frac{\mathsf{v}_g(B)}{m} - t\,.$$

Thus

$$B_1 = g^{mt}(mg)^{-t}C_1 \in \mathcal{B}(G_0)$$

and

$$B_2 = g^{\mathsf{v}_g(B)-mt}(mg)^{-\frac{\mathsf{v}_g(B)}{m}+t}C_2 \in \mathcal{B}(G_0)$$

have the required properties.

Consequently, Θ is a transfer homomorphism. □

The converse of Lemma 3.14.(3) is not true, as the following example will show.

EXAMPLE 3.16. Let $p \in \mathbb{P}$ and $G = C_{p^2}$ with generating element e and let $G_0 = \{e, pe, 2pe\}$. The set G_0 is not minimal non-half-factorial. since the proper subset $\{pe, 2pe\}$ is non-half-factorial. If we consider $g = e$, using the notation of Lemma 3.15, we get $m = p$ and

$$G_0^* = G_0 \setminus \{e\} \cup \{pe\} = \{pe, 2pe\}.$$

Clearly, G_0^* is a minimal non-half-factorial set.

THEOREM 3.17. *Let G be an abelian group and let $G_0 \subset G$ a non-empty, finite subset of torsion elements. Then there exists a non-empty, finite subset $G_0^* \subset G$, such that*

$$g \in \langle G_0^* \setminus \{g\}\rangle \qquad \textit{for each} \quad g \in G_0^*$$

and a transfer homomorphism $\Theta\colon \mathcal{B}(G_0) \to \mathcal{B}(G_0^*)$.

Proof. We proceed by induction on $l(G_0) = \sum_{g\in G_0} \operatorname{ord}(g) \in \mathbb{N}$.

If $l(G_0) = 1$, then $G_0 = \{0\}$ and $0 \in \langle G_0 \setminus \{0\}\rangle$, hence the assertion holds with $G_0^* = G_0$.

Suppose that $l(G_0) > 1$ and assume that the assertion holds for all $\emptyset \neq G_0' \subset G$ of torsion elements with $l(G_0') < l(G_0)$. If $g \in \langle G_0 \setminus \{g\}\rangle$ for all $g \in G_0$, we set $G_0^* = G_0$.

Suppose there exists some $g \in G_0$ with $g \notin \langle G_0 \setminus \{g\}\rangle$. By Lemma 3.15 there exists some $m \in \mathbb{N}_{\geq 2}$ with $m \mid \operatorname{ord}(g)$ and a transfer homomorphism

$$\Theta_1 : \mathcal{B}(G_0) \to \mathcal{B}(G_0')$$

with $G_0' = G_0 \setminus \{g\} \cup \{mg\}$.

Since

$$l(G_0') = l(G_0) - \operatorname{ord}(g) + \operatorname{ord}(mg) < l(G_0),$$

there exists some non-empty, finite set G_0^* such that $g \in \langle G_0^* \setminus \{g\}\rangle$ for each $g \in G_0^*$ and a transfer homomorphism

$$\Theta_2 : \mathcal{B}\big(G_0 \setminus \{g\} \cup \{mg\}\big) \to \mathcal{B}(G_0^*).$$

Since the composition of transfer homomorphisms is again a transfer homomorphism, we get

$$\Theta_2 \circ \Theta_1 : \mathcal{B}(G_0) \to \mathcal{B}(G_0^*)$$

is a transfer homomorphism. □

LEMMA 3.18. ([Ga-Ge98; Lemma 3.3]) *Let G be an abelian torsion group, $G_0 \subset G$ a half-factorial set and $g \in G \setminus \langle G_0 \rangle$ such that $pg \in G_0$ for some $p \in \mathbb{P}$. Then $G_0 \cup \{g\}$ is half-factorial.*

Proof. Since $g \notin \langle G_0 \rangle$ and p is prime, we get that $p = \min\{m' \in \mathbb{N} : m'g \in \langle G_0 \rangle\}$. Consequently, by Lemma 3.14.(2) and Lemma 3.15, $G_0 \cup \{g\}$ is half-factorial if and only if $G_0 \setminus \{g\} \cup \{pg\} = G_0$ is half-factorial. □

4. Simple sets

Let G be an abelian torsion group and $G_0 \subset G$ a non-empty subset. By Proposition 3.3.(2) we know that $\mathcal{B}(G_0)$ is factorial if and only if $G_0 \setminus \{0\}$ is independent. Thus a subset $G_0 \subset G \setminus \{0\}$ for which $\mathcal{B}(G_0)$ is not factorial, but is most simple from a group theoretical point of view consists of independent elements and one additional element.

As mentioned in the Introduction such sets have been frequently investigated. In particular, they are used as examples for minimal non-half-factorial sets (cf. [Ga-Ge00; Proposition 5.2]). However, there are several classes of groups, for example cyclic groups of prime power order (cf. [Ge87; Proposition 6]) and elementary p-groups with $p \le 7$ (cf. [Na79; Problem II] for $p = 2$ and [Sch03a]), in which every minimal non-half-factorial set is of this type.

This motivates the following definition.

DEFINITION 4.1. Let G be an abelian group. A non-empty set $G_0 \subset G \setminus \{0\}$ of torsion elements is called *simple* if there exist some $g \in G_0$ such that $G_0 \setminus \{g\}$ is independent, $g \in \langle G_0 \setminus \{g\} \rangle$, but $g \notin \langle G_1 \rangle$ for any $G_1 \subsetneq G_0 \setminus \{g\}$.

In the following lemma we prove some basic results on simple sets.

LEMMA 4.2. *Let G be an abelian group and $G_0 \subset G$ a simple set.*

(1) $2 \le |G_0| < \infty$.
(2) *If G is finite, then $|G_0| \le \mathsf{r}^*(G) + 1$. In particular, if G is cyclic of prime power order, then $|G_0| = 2$.*
(3) *G_0 is indecomposable.*

Proof.

(1) The set $G_0 \setminus \{g\}$ is independent hence non-empty. Since $g \in G_0$, we get $|G_0| \ge 2$. By definition $g \in \langle G_0 \setminus \{g\} \rangle$, but $g \notin \langle G_1 \rangle$ for any $G_1 \subsetneq G_0 \setminus \{g\}$. Hence

$$g = \sum_{h \in G_0 \setminus \{g\}} z_h h$$

with $z_h \in \mathbb{Z}$ for all $h \in G_0 \setminus \{g\}$ and $z_h = 0$ for all but finitely many. However, $g \notin \langle G_1 \rangle$ for any $G_1 \subsetneq G_0 \setminus \{g\}$. Consequently, $z_h \neq 0$ for all $h \in G_0 \setminus \{g\}$. This means that $G_0 \setminus \{g\}$ must be finite.

(2) Let G be finite. Any independent subset of G has not more than $\mathsf{r}^*(G)$ elements, hence $|G_0 \setminus \{g\}| \le \mathsf{r}^*(G)$. If G is cyclic of prime power order, then $\mathsf{r}^*(G) = 1$.

(3) Assume to the contrary that G_0 is decomposable. By Proposition 3.7 there exist non-empty subsets $G_1, G_2 \subset G_0$ such that $G_0 = G_1 \dot\cup G_2$ and $\mathcal{B}(G_0) = \mathcal{B}(G_1) \times \mathcal{B}(G_2)$. Since $g \in \langle G_0 \setminus \{g\} \rangle$, there exists some $A \in \mathcal{A}(G_0)$ with $\mathsf{v}_g(A) = 1$. Since $\mathcal{A}(G_0) = \mathcal{A}(G_1) \dot\cup \mathcal{A}(G_2)$, we may suppose without restriction that $A \in \mathcal{A}(G_1)$. This implies that $g \in \langle G_1 \setminus \{g\} \rangle$, a contradiction. $\square$

The arithmetic of block monoids generated by simple sets is not as simple, as one might expect. We start with an example.

EXAMPLE 4.3.

(1) Let $G = (\mathbb{Z}/4\mathbb{Z})^3$ with independent and generating elements $\{e_1, e_2, e_3\}$. Then $G_0 = \{g, e_1, e_2, e_3\}$ with $g = -(2e_1 + e_2 + e_3)$ is simple. Since $U = g^2 e_2^2 e_3^2$ is an atom with $\mathsf{k}(U) = \frac{3}{2}$ and $\operatorname{supp}(U) \subsetneq G_0$, Proposition 3.4.(1) shows that G_0 is non-half-factorial, but not minimal non-half-factorial.

(2) Let $G = \mathbb{Z}/30\mathbb{Z}$ and $G_0 = \{1+30\mathbb{Z}, 6+30\mathbb{Z}, 10+30\mathbb{Z}, 15+30\mathbb{Z}\}$. Then G_0 is simple and minimal non-half-factorial.

However, if G is an elementary p-group, then simple subsets of G are either half-factorial or minimal non-half-factorial.

LEMMA 4.4. *Let G be an elementary p-group.*

(1) *Let $G_1 \subset G$ be independent, $g \in G \setminus G_1$ and $G_0 = G_1 \cup \{g\}$. Then the following conditions are equivalent:*
   (a) *G_0 is indecomposable.*
   (b) *G_0 is simple. In particular, if G_0 is minimal non-half-factorial, then G_0 is simple.*

(2) *Let $G_0 \subset G$ be simple. Then for every $h \in G_0$ the set $G_0 \setminus \{h\}$ is independent, $h \in \langle G_0 \setminus \{h\} \rangle$ and $h \notin \langle G_1 \rangle$ for every $G_1 \subsetneq G_0 \setminus \{h\}$.*

(3) *Every simple set is either half-factorial or minimal non-half-factorial.*

Proof.

(1) (a) $\Longrightarrow$ (b): Let G_0 be indecomposable. Then $g \neq 0$ and G_0 is not independent. Hence $\langle g \rangle \cap \langle G_1 \rangle \neq \{0\}$ and consequently $g \in \langle G_1 \rangle$. Assume $g \in \langle G_2 \rangle$ for some $G_2 \subsetneq G_1$. Then $G_2 \cup \{g\}$ is a component of G_0, which is a contradiction. Consequently, G_0 is simple.

(b) $\Longrightarrow$ (a): Let G_0 be simple, then G_0 is indecomposable by Lemma 4.2.(3). If G_0 is minimal non-half-factorial, then it is indecomposable by Lemma 3.6.(4) and hence simple.

(2) Let $g \in G_0$ such that $G_0 \setminus \{g\} = \{e_1, \ldots, e_r\}$ is independent, $g \in \langle G_0 \setminus \{g\} \rangle$ and $g \notin \langle G_1 \rangle$ for every $G_1 \subsetneq G_0 \setminus \{g\}$. Then $g = \sum_{i=1}^{r} a_i e_i$ with $a_i \in [1, p-1]$. We consider G as a $\mathbb{F}_p$-vector space and by linear algebra we infer that $\dim_{\mathbb{F}_p} \langle G_0 \rangle = |G_0| - 1$ and for every $h \in G_0$ we have $\langle G_0 \rangle = \langle G_0 \setminus \{h\} \rangle$. Thus $G_0 \setminus \{h\}$ is independent, $h \in \langle G_0 \setminus \{h\} \rangle$ and $h \notin \langle G_1' \rangle$ for every $G_1' \subsetneq G_0 \setminus \{h\}$.

(3) Suppose G_0 is simple. By (2) every proper subset of G_0 is independent and consequently half-factorial. Thus if G_0 is not half-factorial, then G_0 is minimal non-half-factorial. $\square$

The following theorem will prove that the notion of simple sets is not too restrictive.

THEOREM 4.5. *Let G be an abelian group, $G_0 \subset G$ be a subset of torsion elements and $g \in G_0$ be such that $G_0 = G_0' \cup \{g\}$ with $G_0' \subset G$ independent. Then there exist a set $G_0^* \subset G$ and a transfer homomorphism*

$$\Theta \colon \mathcal{B}(G_0) \to \mathcal{B}(G_0^*),$$

where $G_0^* \setminus \{0\}$ is simple or empty.

Proof. If $G_0 \setminus \{0\}$ is independent, then by Proposition 3.3.(2), G_0 is factorial. In this case we set $G_0^* = \{0\}$ and the map

$$\Theta : \begin{cases} \mathcal{B}(G_0) & \to \mathcal{B}(G_0^*), \\ B & \mapsto 0^{\mathsf{k}(B)} \end{cases}$$

is a transfer homomorphism.

Hence we may suppose without restriction that $G_0 \setminus \{0\}$ is not independent. Thus we get $\langle g \rangle \cap \langle G_0 \setminus \{g\} \rangle \neq \{0\}$. Let $m \in \mathbb{N}$ be minimal such that $mg \in \langle G_0 \setminus \{g\} \rangle$. By Lemma 3.15 there exists a transfer homomorphism

$$\Theta_1 \colon \mathcal{B}(G_0) \to \mathcal{B}\big(G_0 \setminus \{g\} \cup \{mg\}\big).$$

Thus from now on we may suppose that $m = 1$.

Let $G_1 \subset G_0$ be a minimal subset such that $g \in G_1$ and $g \in \langle G_1 \setminus \{g\} \rangle$. Thus G_1 is simple. If $G_1 = G_0$, we set $G_0^* = G_0$ and are done. Suppose that $G_2 = G_0 \setminus G_1 \neq \emptyset$. Since $G_0 \setminus \{g\}$ is independent and $g \in \langle G_1 \setminus \{g\} \rangle$, it follows that $\langle G_1 \rangle \cap \langle G_2 \rangle = \{0\}$. Proposition 3.7 implies that $\mathcal{B}(G_0) = \mathcal{B}(G_1) \times \mathcal{B}(G_2)$. Since G_2 is independent and $\mathcal{B}(G_2)$ is factorial, the map

$$\Theta_2 : \begin{cases} \mathcal{B}(G_0) = \mathcal{B}(G_1) \times \mathcal{B}(G_2) & \to \mathcal{B}\big(G_1 \cup \{0\}\big), \\ B = B_1 B_2 & \mapsto B_1 0^{\mathsf{k}(B_2)} \end{cases}$$

is a transfer homomorphism. Hence we set $G_0^* = G_1 \cup \{0\}$ and are done. □

In the last part of this section we study the set of atoms $\mathcal{A}(G_0)$ for simple sets $G_0 \subset G$. For simple sets consisting of two elements, this set was determined in [Ge87] and [Ch-Sm03a] (cf. Proposition 4.8).

Definition 4.6. Let G be an abelian group and $G_0 \subset G$ be a simple set. Suppose that $G_0 = G_1 \cup \{g\}$ with $G_1 = \{e_1, \dots, e_r\}$ independent, $\mathrm{ord}(e_i) = n_i$ for each $i \in [1, r]$ and $g = -\sum_{i=1}^{r} b_i e_i$ with $b_i \in [1, n_i - 1]$ for each $i \in [1, r]$.

(1) For $j \in \mathbb{N}$ let $W_j(G_1, g) = W_j \in \mathcal{B}(G_0)$ denote the unique block with $\mathsf{v}_g(W_j) = j$ and $\mathsf{v}_{e_i}(W_j) \in [0, n_i - 1]$ for each $i \in [1, r]$ (clearly, $\mathsf{v}_{e_i}(W_j) \equiv j b_i \bmod n_i$).
(2) $\mathsf{i}(G_1, g) = \{j \in \mathbb{N} : W_j \in \mathcal{A}(G_0)\}$.

Theorem 4.7. *Let G be an abelian group, $r \in \mathbb{N}$, $G_1 = \{e_1, \dots, e_r\}$ be an independent set with $\mathrm{ord}(e_i) = n_i$ for each $i \in [1, r]$, $g = -\sum_{i=1}^{r} b_i e_i$ with $b_i \in [1, n_i - 1]$ for each $i \in [1, r]$ and $G_0 = G_1 \cup \{g\}$.*

(1) $\mathcal{A}(G_0) = \{e_i^{n_i} : i \in [1, r]\} \cup \{W_j : j \in \mathsf{i}(G_1, g)\}$.
(2) $\mathsf{i}(G_1, g) = \{j \in [1, \mathrm{ord}(g)] : W_k \nmid W_j$ *for each* $k \in [1, j-1]\}$. *In particular,* $\{1, \mathrm{ord}(g)\} \subset \mathsf{i}(G_1, g) \subset [1, \mathrm{ord}(g)]$.
(3) *Let* $I = \{i \in [1, r] : b_i \neq n_i - 1\}$ *and* $N = \max(\{0\} \cup \{n_i : i \in [1, r] \setminus I\})$. *Then*
$$[1, N] \cup \bigcup_{i \in I} \mathsf{i}(\{e_i\}, -b_i e_i) \subset \mathsf{i}(G_1, g),$$
and if $n_1 = \dots = n_r$ *and* $b_1 = \dots = b_r$, *then equality holds.*
(4) $\min(\mathsf{i}(G_1, g) \setminus \{1\}) = \min\{\lceil \frac{n_i}{b_i} \rceil : i \in [1, r]\}$.
(5) $\mathsf{i}(G_1, g) = \{1, \mathrm{ord}(g)\}$ *if and only if* $\mathrm{ord}(g) \mid n_i$ *and* $b_i = \frac{n_i}{\mathrm{ord}(g)}$ *for each* $i \in [1, r]$.
(6) *If* $\mathsf{i}(G_1, g) \neq \{1, \mathrm{ord}(g)\}$, *then* $\min(\mathsf{i}(G_1, g) \setminus \{1\}) \le \lceil \frac{\mathrm{ord}(g)}{2} \rceil$.

Thus in an important special case, $\mathsf{i}(G_1, g)$ (and hence $\mathcal{A}(G_0)$) is completely determined by associated $\mathsf{i}(\cdot, \cdot)$ for sets G_0' with $|G_0'| = 2$. We mentioned already that for these sets two descriptions are known. We cite the description given in [Ch-Sm03; Theorem 2.1] (cf. [Ge87; Lemma 1] for a similar description).

Proposition 4.8. ([Ch-Sm03; Theorem 2.1]) *Let G be an abelian group, $e \in G$ with $\mathrm{ord}(e) = n \ge 3$, $a \in [2, n-1]$ and $d = \gcd(a, n)$. For $k \in [1, \frac{a}{d}]$ let $q_k \in \mathbb{N}_0$ and $r_k \in [0, a-1]$ such that $kn = q_k a + r_k$. Then*
$$\mathsf{i}(\{e\}, ae) = [1, \lfloor \tfrac{n}{a} \rfloor - 1] \cup \{q_k : r_k < r_i \text{ for each } i \in [1, k-1]\}.$$

Now we formulate a corollary to Proposition 4.8, which we need in the proof of Theorem 4.7. For convenience we will give an independent proof for it.

COROLLARY 4.9. *Let G be an abelian group, $e \in G$ with $\mathrm{ord}(e) = n \geq 3$, $b \in [1, n-2]$, $d = \gcd(b, n)$ and $b' \in \big[1, \mathrm{ord}(-be) - 1\big]$ such that $bb' \equiv d \bmod n$. Then*

$$\{\lceil \tfrac{n}{b} \rceil, b'\} \subset \mathsf{i}\big(\{e\}, -be\big).$$

Proof. Obviously, $\{-be, e\}$ is a simple set. In order to show that $b' \in \mathsf{i}\big(\{e\}, -be\big)$, we have to verify that $W_{b'} = (-be)^{b'} e^d$ is an atom. Since for every $B \in \mathcal{B}\big(\{-be, e\}\big)$ we have $d \mid \mathsf{v}_e(B)$, and because $b' = \min\{v \in \mathbb{N} : \sigma\big((-be)^v e^d\big) = 0\}$, it follows that $W_{b'}$ is an atom.

In order to show that $\lceil \frac{n}{b} \rceil \in \mathsf{i}\big(\{e\}, -be\big)$, we have to verify that

$$W_{\lceil \frac{n}{b} \rceil} = (-be)^{\lceil \frac{n}{b} \rceil} e^{\lceil \frac{n}{b} \rceil b - n}$$

is an atom. Since for each $j \in \big[1, \lceil \frac{n}{b} \rceil - 1\big]$ we get $W_j = (-be)^j e^{jb}$ and because $\lceil \frac{n}{b} \rceil b - n < b$, it follows that $W_{\lceil \frac{n}{b} \rceil}$ is an atom. □

In [Ge87; Proposition 10] a more explicit description of $\mathsf{i}(\cdot, \cdot)$ for simple sets with two elements is given. It uses continued fraction expansions and is quite complicated to formulate. Since we will not need this explicit description, we do not cite this result. However, we give as an example the two easiest cases.

EXAMPLE 4.10. Let $e \in G$ with $\mathrm{ord}(e) = p \in \mathbb{P}$ and $b \in [2, p-2]$.

(1) If $b \mid p+1$, say $qb = p+1$, then $\mathsf{i}\big(\{e\}, -be\big) = \{1, q, p\}$.
(2) Let $q = \lceil \frac{p}{b} \rceil$ and $r = \lceil \frac{p}{b} \rceil - p$. If $r \mid b+1$, say $sr = b+1$, then $\mathsf{i}\big(\{e\}, -be\big) = \{1, q, sq-1, p\}$.

Next we give some lemmata that will be used in the proof of Theorem 4.7. Let all notations be as in Theorem 4.7.

LEMMA 4.11. ([Ga-Ge02; Lemma 2.2]) *We have*

$$\mathrm{ord}(g) = \mathrm{lcm}\left(\left\{ \frac{n_i}{\gcd(b_i, n_i)} : i \in [1, r] \right\}\right).$$

LEMMA 4.12. *Let $j \in \mathbb{N}$.*

(1) *If $W \in \mathcal{B}(G_0)$ with $\mathsf{v}_g(W) = j$, then $W_j \mid W$.*
(2) *If $A \in \mathcal{A}(G_0)$ with $\mathsf{v}_g(A) = j$, then $W_j = A$.*
(3) *If $W_j \notin \mathcal{A}(G_0)$, then there exists some $k \in [1, j-1]$ such that $W_j = W_k W_{j-k}$.*

Proof.

(1) Let $W \in \mathcal{B}(G_0)$ with $\mathsf{v}_g(W) = j$. Then

$$\sum_{i=1}^{r} \mathsf{v}_{e_i}(W) e_i = -jg = \sum_{i=1}^{r} \mathsf{v}_{e_i}(W_j) e_i .$$

Since G_1 is independent, it follows that for all $i \in [1,r]$ there are $k_i \in \mathbb{Z}$ such that $\mathsf{v}_{e_i}(W) = \mathsf{v}_{e_i}(W_j) + k_i n_i$. Since $\mathsf{v}_{e_i}(W) \in \mathbb{N}_0$ and $\mathsf{v}_{e_i}(W_j) \in [0, n_i - 1]$, it follows that $k_i \in \mathbb{N}_0$ for all $i \in [1,r]$. Hence we obtain that $W_j \mid W$.

(2) follows immediately from (1).

(3) Suppose that $W_j \notin \mathcal{A}(G_0)$. Then there exists some $A \in \mathcal{A}(G_0)$ with $A \mid W_j$. Clearly, $\mathsf{v}_g(A) \le j$ and by (2), $\mathsf{v}_g(A) \ne j$. Assume $\mathsf{v}_g(A) = 0$, then $A \in \mathcal{A}(G_1)$. Since G_1 is independent, we get $A = e_i^{n_i}$ for some $i \in [1,r]$. However, we know $\mathsf{v}_{e_i}(W_j) < n_i$ and $A \nmid W_j$. Thus $\mathsf{v}_g(A) \in [1, j-1]$ and by (2) we get $A = W_k$ for some $k \in [1, j-1]$. Clearly, $\mathsf{v}_g\big(W_k^{-1}W_j\big) = j - k > 0$ and $\mathsf{v}_{e_i}\big(W_k^{-1}W_j\big) < n_i$ for all $i \in [1,r]$, hence $W_k^{-1}W_j = W_{j-k}$. □

LEMMA 4.13. *Let $r \ge 2$, $g' = -\sum_{i=1}^{r-1} b_i e_i$, $G_1' = \{e_1, \dots, e_{r-1}\}$ and $\{g'\} \cup G_1'$ be a simple set. Then*

$$\mathsf{i}(G_1', g') \subset \mathsf{i}(G_1, g),$$

and equality holds if there exists some $i' \in [1, r-1]$ such that $n_{i'} = n_r$ and $b_{i'} = b_r$.

Proof. We set $W_j' = W_j(G_1', g')$ for each $j \in \mathbb{N}$. Let $k \in \mathsf{i}(G_1', g')$ and assume $k \notin \mathsf{i}(G_1, g)$. Then $W_k \notin \mathcal{A}(G_0)$ and by Lemma 4.12.(3) there exists some $l \in [1, k-1]$ such that $W_l \mid W_k$. This implies $W_l' \mid W_k'$, a contradiction. Hence $k \in \mathsf{i}(G_1, g)$ and $\mathsf{i}(G_1', g') \subset \mathsf{i}(G_1, g)$.

Let $i' \in [1, r-1]$ such that $n_{i'} = n_r$ and $b_{i'} = b_r$. Let $k \in \mathbb{N}$ with $k \notin \mathsf{i}(G_1', g')$. There exists some $l \in [1, k-1]$ such that $W_l' \mid W_k'$. Consequently, we obtain that

$$\mathsf{v}_{e_r}(W_l) = \mathsf{v}_{e_{i'}}(W_l) \le \mathsf{v}_{e_{i'}}(W_k) = \mathsf{v}_{e_r}(W_k),$$

which implies that $W_l \mid W_k$ and $k \notin \mathsf{i}(G_1, g)$. Thus $\mathsf{i}(G_1', g') = \mathsf{i}(G_1, g)$. □

LEMMA 4.14. *Let $b_{i'} = n_{i'} - 1$ for some $i' \in [1,r]$. Then*

$$[1, n_{i'}] \subset \mathsf{i}(G_1, g).$$

Proof. Let $j \in [1, n_{i'}]$. Clearly $\mathsf{v}_{e_{i'}}(W_j) = n_{i'} - j$, hence $W_k \nmid W_j$ for each $k \in [1, j-1]$. Thus W_j is an atom. □

Proof of Theorem 4.7.

(1) Let $A \in \mathcal{A}(G_0)$ with $\mathsf{v}_g(A) > 0$. Then Lemma 4.12.(2) gives immediately

$$A \in \big\{W_j : j \in \mathsf{i}(G_1, g)\big\}.$$

Let $A' \in \mathcal{A}(G_0)$ with $\mathsf{v}_g(A') = 0$. Then $\operatorname{supp}(A') \subset G_1$ and since G_1 is independent, we get from Proposition 3.3.(2) that G_1 is factorial and $\mathcal{A}(G_1) = \big\{e_i^{n_i} : i \in [1,r]\big\}$.

(2) Let $j > \operatorname{ord}(g)$. Then $g^{\operatorname{ord}(g)} \mid W_j$, hence $j \notin \mathsf{i}(G_1, g)$ and $\mathsf{i}(G_1, g) \subset [1, \operatorname{ord}(g)]$. The other statements follow from (1) and Lemma 4.12.(3).

(3) First we show that $[1, N] \subset \mathsf{i}(G_1, g)$. If $I = [1, r]$, then $N = 0$ and $[1, N] = \emptyset$. If $I \subsetneq [1, r]$, then Lemma 4.14 implies the assertion.

Suppose that $I \neq \emptyset$ and let $i \in I$, say $i = 1$.

We have to show that $\mathsf{i}(\{e_1\}, -b_1 e_1) \subset \mathsf{i}(G_1, g)$. For $s \in [1, r]$ we set

$$g^{(s)} = -\sum_{i=1}^{s} b_i e_i \qquad \text{and} \qquad G_1^{(s)} = \{e_1, \ldots, e_s\},$$

hence $G_0^{(s)} = G_1^{(s)} \cup \{g^{(s)}\}$ is simple.

We assert that $\mathsf{i}(\{e_1\}, -b_1 e_1) \subset \mathsf{i}(G_1^{(s)}, g^{(s)})$ for every $s \in [1, r]$. We proceed by induction on s. For $s = 1$ the assertion is clear. Suppose that $s > 1$ and that $\mathsf{i}(\{e_1\}, -b_1 e_1) \subset \mathsf{i}(G_1^{(s-1)}, g^{(s-1)})$. Since G_0^{s-1} is simple, Lemma 4.13 shows that $\mathsf{i}(G_1^{(s-1)}, g^{(s-1)}) \subset \mathsf{i}(G_1^{(s)}, g^{(s)})$, hence the assertion follows.

Now let $b_1 = \cdots = b_r$ and $n_1 = \cdots = n_r$. If $b_1 = n_1 - 1$, then we get, applying Lemma 4.12.(3), $[1, n_1] \subset \mathsf{i}(G_1, g) \subset [1, n_1]$. If $b_1 < n_1 - 1$, we start with the set $\{-b_1 e_1, e_1\}$ and apply $r - 1$ times Lemma 4.13.

(4) Corollary 4.9 and (3) imply that

$$\left\{ \left\lceil \tfrac{n_i}{b_i} \right\rceil : i \in [1, r] \right\} \subset \mathsf{i}(G_1, g) \setminus \{1\}.$$

Hence it suffices to verify that $W_j \notin \mathcal{A}(G_0)$ for $j \in [2, m-1]$, where $m = \min\left\{ \left\lceil \tfrac{n_i}{b_i} \right\rceil : i \in [1, r] \right\}$. Let $j \in [2, m-1]$. Since $j b_i < n_i$ for each $i \in [1, r]$, we obtain

$$W_j = g^j \prod_{i=1}^{r} e_i^{j b_i}.$$

Therefore $W_1 \mid W_j$ and $W_j \notin \mathcal{A}(G_0)$.

(5) If $\operatorname{ord}(g) \mid n_i$ and $b_i = \frac{n_i}{\operatorname{ord}(g)}$ for each $i \in [1, r]$, then (4) implies that $\min(\mathsf{i}(G_1, g) \setminus \{1\}) = \operatorname{ord}(g)$, hence $\mathsf{i}(G_1, g) = \{1, \operatorname{ord}(g)\}$ by (2).

Conversely, let $\mathsf{i}(G_1, g) = \{1, \operatorname{ord}(g)\}$ and let $i \in [1, r]$. Then (4) and Lemma 4.11 imply that

$$\begin{aligned} \frac{n_i}{\gcd(b_i, n_i)} &\le \operatorname{lcm}\left(\left\{ \frac{n_\nu}{\gcd(b_\nu, n_\nu)} : \nu \in [1, r] \right\} \right) = \operatorname{ord}(g) \\ &= \min\left\{ \left\lceil \frac{n_\nu}{b_\nu} \right\rceil : \nu \in [1, r] \right\} \le \left\lceil \frac{n_i}{b_i} \right\rceil. \end{aligned}$$

If $b_i \nmid n_i$, then $\gcd(b_i, n_i) \le \frac{b_i}{2}$, hence

$$2 \frac{n_i}{b_i} \le \frac{n_i}{\gcd(b_i, n_i)} \le \left\lceil \frac{n_i}{b_i} \right\rceil < \frac{n_i}{b_i} + 1,$$

which is a contradiction. Thus $b_i \mid n_i$ and $\operatorname{ord}(g) = \frac{n_i}{b_i}$.

(6) Let $m = \min(\mathsf{i}(G_0, g) \setminus \{1\})$ and suppose $m < \operatorname{ord}(g)$. We need to show that $m \le \lceil \frac{\operatorname{ord}(g)}{2} \rceil$. By (4) we have $m = \min\{\lceil \frac{n_i}{b_i} \rceil : i \in [1,r]\}$, hence we may suppose without restriction that $m = \lceil \frac{n_1}{b_1} \rceil$. By Lemma 4.11 we have $\operatorname{ord}(g) = \operatorname{lcm}\left(\left\{\frac{n_\nu}{\gcd(b_\nu, n_\nu)} : \nu \in [1,r]\right\}\right)$, hence $\operatorname{ord}(g)$ is a multiple of $\frac{n_1}{\gcd(b_1,n_1)}$. If $\operatorname{ord}(g) \ge 2\frac{n_1}{\gcd(b_1,n_1)}$, then

$$m = \left\lceil \frac{n_1}{b_1} \right\rceil \le \frac{n_1}{\gcd(b_1, n_1)} \le \frac{\operatorname{ord}(g)}{2} .$$

Suppose that $\operatorname{ord}(g) = \frac{n_1}{\gcd(b_1,n_1)}$. If $\gcd(b_1, n_1) = b_1$, then $m = \frac{n_1}{b_1} = \operatorname{ord}(g)$, which is a contradiction. Thus $2\gcd(b_1, n_1) \le b_1$ and $\frac{n_1}{b_1} \le \frac{n_1}{2\gcd(b_1,n_1)} = \frac{\operatorname{ord}(g)}{2}$, hence $m = \lceil \frac{n_1}{b_1} \rceil \le \lceil \frac{\operatorname{ord}(g)}{2} \rceil$. □

In general, equality does not hold in Theorem 4.7.(3). We will illustrate this by the following example.

EXAMPLE 4.15. Let all notations be as in Theorem 4.7. Suppose that $r = 2$, $n_1 = n_2 = n > 3$ are odd and $g = 2e_1 - 2e_2$. Then $I = \{i \in [1,2] : b_i \ne n-1\} = [1,2]$, $N = 0$ and

$$\mathsf{i}(\{e_1\}, 2e_1) = \left[1, \left\lfloor \frac{n}{2} \right\rfloor\right] \cup \{n\} \qquad \text{and} \qquad \mathsf{i}(\{e_1\}, -2e_1) = \left\{1, \left\lfloor \frac{n}{2} \right\rfloor + 1, n\right\}.$$

However, for $j \in [1, \lfloor \frac{n}{2} \rfloor]$ we get

$$W_j = g^j e_1^{n-2j} e_2^{2j} \qquad \text{and} \qquad W_{j+\lfloor \frac{n}{2} \rfloor} = g^{j+\lfloor \frac{n}{2} \rfloor} e_1^{n-1-2j} e_2^{2j-1} ,$$

hence $\mathsf{i}(\{e_1, e_2\}, g) = [1, n]$.

Acknowledgement

I would like to thank Professor A. Geroldinger for his advice and support during the preparation of the article.

REFERENCES

[An97] *Factorization in Integral Domains* (D. D. Anderson, ed.), Based on the proceedings of the conference, March 21, 1996, and the special session in commutative ring theory, March 22–23, 1996, at the 909th meeting of the Amer. Math. Soc., Iowa City, IA, USA. Lecture Notes in Pure and Appl. Math. 189, Marcel Dekker, New York, NY, 1997.

[Car] CARLITZ, L.: *A Characterization of algebraic number fields with class number two*, Proc. Amer. Math. Soc **11** (1960), 391–392.

[Ch-Ge97] CHAPMAN, S.—GEROLDINGER, A.: *Krull domains and monoids, their sets of lengths and associated combinatorial problems.* In: Factorization in Integral Domains (D. D. Anderson, ed.), Based on the proceedings of the conference, March 21, 1996, and the special session in commutative ring theory, March 22–23, 1996, at the 909th meeting of the Amer. Math. Soc., Iowa City, IA, USA. Lecture Notes in Pure and Appl. Math. 189, Marcel Dekker, New York, 1997, pp. 73 112.

[Ch-Sm03] CHAPMAN, S. T. SMITH, W. W.: *On factorization in block monoids formed by* $\{\overline{1},\overline{a}\}$ *in* $\mathbb{Z}_n$, Proc. Edinb. Math. Soc. (2) **46** (2003), 257 267.

[Ga-Ge98] GAO, W. GEROLDINGER, A.: *Half-factorial domains and half-factorial subsets in abelian groups*, Houston J. Math. **24** (1998), 593–611.

[Ga-Ge00] GAO, W. GEROLDINGER, A.: *Systems of sets of lengths II*, Abhandl. Math. Sem. Univ. Hamburg **70** (2000), 31 49.

[Ga-Ge02] GAO, W. GEROLDINGER, A.: *On the order of elements in long minimal zero-sum sequences*, Period. Math. Hungar. **44** (2002), 63 73.

[Ge87] GEROLDINGER, A.: *On non-unique factorizations into irreducible elements II.* In: Colloq. Math. Soc. János Bolyai 51, North Holland, Amsterdam, 1987, pp. 723 757.

[Ge94] GEROLDINGER, A.: *T-block monoids and their arithmetical applications to certain integral domains*, Comm. Algebra **22** (1994), 1603–1615.

[Ge-HK92] GEROLDINGER, A.—HALTER-KOCH, F.: *Non-unique factorizations in block semigroups and arithmetical applications*, Math. Slovaca **42** (1992), 641–661.

[Ge-Ka92] GEROLDINGER, A.—KACZOROWSKI, J.: *Analytic and arithmetic theory of semigroups with divisor theory*, Sém. Théor. Nombres Bordeaux (2) **4** (1992), 199 238.

[HK97] HALTER-KOCH, F.: *Finitely generated monoids, finitely primary monoids and factorization properties of integral domains.* In: Factorization in Integral Domains (D. D. Anderson, ed.), Based on the proceedings of the conference, March 21, 1996, and the special session in commutative ring theory, March 22–23, 1996, at the 909th meeting of the Amer. Math. Soc., Iowa City, IA, USA. Lecture Notes in Pure and Appl. Math. 189, Marcel Dekker, New York, 1997, pp. 31–72.

[HK98] HALTER-KOCH, F.: *Ideal Systems. An Introduction to Multiplicative Ideal Theory.* Pure and Applied Mathematics, Marcel Dekker 211, New York, 1998.

[Na79] NARKIEWICZ, W.: *Finite abelian groups and factorization problems*, Colloq. Math. **17** (1979), 319 330.

[Sch03] SCHMID, W. A.: *Half-factorial sets in elementary p-groups*, Far East J. Math. Sci. (To appear).

[Sch03] SCHMID, W. A.: *Differences in sets of lengths of Krull monoids with finite class group*, J. Théor. Nombres Bordeaux (To appear).

[Sk76] SKULA, L.: *On c-semigroups*, Acta Arith. **31** (1976), 247 257.

[Sl76] ŚLIWA, J.: *Factorizations of distinct length in algebraic number fields*, Acta Arith. **31** (1976), 399 417.

[Za76] ZAKS, A.: *Half factorial domains*, Bull. Amer. Math. Soc. **82** (1976), 721 723.

Received July 7, 2003

Institut für Mathematik
Karl-Franzens-Universität
Heinrichstrasse 36
A-8010 Graz
AUSTRIA

E-mail: wolfgang.schmid@uni-graz.at