HOUSTON JOURNAL OF MATHEMATICS

Volume 24, No. 4, 1998

HALF-FACTORIAL DOMAINS AND HALF-FACTORIAL SUBSETS OF ABELIAN GROUPS

WEIDONG GAO AND ALFRED GEROLDINGER
Communicated by Klaus Kaiser

1. INTRODUCTION

An integral domain (resp. a commutative, cancellative monoid) D is said to be *atomic*, if every non-zero non-unit element $a \in D$ allows a factorization into irreducible elements of D, say $a = u_1 \dots u_k$. In this case k is called the length of the factorization and the *set of lengths* $L(a) \subseteq \mathbb{N}_+$ is defined as the set of all possible $k \in \mathbb{N}_+$. D is said to be *half-factorial*, if it is atomic and $\#L(a) = 1$ for every non-zero non-unit $a \in D$(equivalently, D has elasticity one). Obviously, noetherian domains are atomic and factorial domains are half-factorial. In 1960 L. Carlitz characterized half-factorial rings of integers in algebraic number fields. W. Narkiewicz, L. Skula, J. Sliwa and A. Zaks studied half-factorial Krull domains. Nowadays much work in the context of general integral domains is done by D.D Anderson, D. F. Anderson, S. Chapman and W. Smith (see [AA94, And97, AP97, ACS94a, ACS94b, ACS94c, ACS95] and the references cited there).

A subset G_0 of an abelian group G is said to be *half-factorial*, if the block monoid $\mathcal{B}(G_0)$ over G_0 is half-factorial. We shall be mainly interested in the structure and the (maximal) size of half-factorial subsets. Define

$$\mu(G) = \sup\{|G_0| \ \big| \ G_0 \subseteq G \text{ is half-factorial}\} \in \mathbb{N} \cup \{\infty\} \ .$$

The connection between the two notions is as follows. Let D be a Krull domain (resp. a Krull monoid) with divisor class group G and let $G_0 \subseteq G$ denote the set of classes containing prime divisors. Then D is half-factorial if and only if G_0

1991 *Mathematics Subject Classification.* 11B, 11R27, 13F05.

Key words and phrases. half-factoriality, Krull domains, abelian groups.

The first author hold an Austrian Lise Meitner Fellowship (Project-Number M00397-MAT) and would like to thank the FWF for all the assistance.

is half-factorial. However, the significance of half-factorial subsets extends this interpretation. We give two examples.

Let D be a ring of integers in an algebraic number field and let $k \in \mathbb{N}_+$. In the sixties W. Narkiewicz introduced the following counting function:

$$G_k(x) = \#\{aD \mid a \in D, \mathcal{N}(a) \le x, \#L(a) \le k\} .$$

In [Ger90] it was shown that

$$G_k(x) \sim Cx(\log x)^{\mu(G)/|G|-1}(\log\log x)^B$$

with B, C non-negative, real numbers. For a generalization see [GHKK95].

The current motivation for the present paper stems from investigations of possible distances in arbitrarily long sets of lengths. For this one has to study minimal non half-factorial subsets. The interested reader is referred to [GG98b].

The whole paper is based on a characterization of half-factoriality going back to L. Skula and J. Sliwa (see Lemma 3.2). This result makes it possible to apply methods from additive group theory and combinatorics to the investigation of half-factoriality. In section 4 we derive an upper bound for $\mu(G)$ by counting the number of solutions of a congruence mod n. In section 5 we characterize half-factorial subsets in cyclic groups in terms of splittable subsets of natural numbers. In the final section we obtain lower bounds for $\mu(G)$ using generalizations of the Erdös-Ginzburg-Ziv Theorem. In particular, we show that half-factorial subsets of maximal size do not necessarily generate the group. Hence there are groups G having proper subgroups H with $\mu(H) = \mu(G)$.

2. Preliminaries

Let $\mathbb{N}_+$ denote the positive integers, $\mathbb{N} = \mathbb{N}_+ \cup \{0\}$ and $\mathbb{P} \subseteq \mathbb{N}_+$ the set of prime numbers. For $p \in \mathbb{P}$ let $v_p : \mathbb{Q} \to \mathbb{Z}$ be the p-adic valuation with $v_p(p) = 1$. For $n \in \mathbb{N}_+$ let $[1, n] = \{j \in \mathbb{N} \mid 1 \le j \le n\}$.

Throughout, let G be an abelian group and $G_0 \subseteq G$ a non-empty subset. Then $\langle G_0 \rangle$ (resp. $[G_0]$) denotes the subgroup (resp. submonoid) generated by G_0. If G is a torsion group, then $\langle G_0 \rangle = [G_0]$. We say that G_0 is a *generating subset* of G, if $[G_0] = G$. G_0 is said to be an *independent subset*, if $0 \notin G_0$ and given distinct elements $e_1, \ldots, e_r \in G$ and integers $m_1, \ldots, m_r \in \mathbb{Z}$, the relation $\sum_{i=1}^{r} m_i e_i = 0$ implies that $m_1 e_1 = \cdots = m_r e_r = 0$. The following simple lemma will be used several times.

Lemma 2.1. *Let G be an abelian group, $e_1, \dots, e_r$ independent elements with* $\operatorname{ord}(e_1) = \dots = \operatorname{ord}(e_r) = n \in \mathbb{N}_+$ *and* $m_1, \dots, m_r \in \mathbb{Z}$. *Then*

$$\operatorname{ord}(\sum_{i=1}^{r} m_i e_i) = \frac{n}{\gcd\{m_1, \dots, m_r, n\}}.$$

PROOF. For every $1 \le i \le r$ we have $\operatorname{ord}(m_i e_i) = \frac{n}{\gcd\{m_i, n\}}$. Since $e_1, \dots, e_r$ are independent, it follows that

$$\operatorname{ord}(\sum_{i=1}^{r} m_i e_i) = \operatorname{lcm}\{\frac{n}{\gcd\{m_1, n\}}, \dots, \frac{n}{\gcd\{m_r, n\}}\}$$

which implies the assertion. □

If G is finite and $|G| > 1$, then $G = \oplus_{i=1}^{r} C_{n_i}$ with $1 < n_1 | \dots | n_r$ where $r = r(G)$ is the *rank* of G and $n_r = \exp(G)$ is the *exponent* of G. Let $e_1, \dots, e_r \in G$ with $\operatorname{ord}(e_i) = n_i$ for $1 \le i \le r$. We say that $(e_1, \dots, e_r)$ is a *basis* of G, if $\{e_1, \dots, e_r\}$ is a generating subset consisting of independent elements (equivalently, $G = \oplus_{i=1}^{r} \langle e_i \rangle$).

Let $\mathcal{F}(G_0)$ denote the free abelian monoid with basis G_0. An element $S = \prod_{i=1}^{l} g_i \in \mathcal{F}(G_0)$ is called a *sequence* in G_0; it has a unique representation of the form

$$S = \prod_{g \in G_0} g^{v_g(S)}$$

where $v_g(S) \in \mathbb{N}$ for all $g \in G_0$ and $v_g(S) = 0$ for all but finitely many $g \in G_0$. Then

$$|S| = l = \sum_{g \in G_0} v_g(S) \in \mathbb{N}$$

is called the *length* of S,

$$k(S) = \sum_{i=1}^{l} \frac{1}{\operatorname{ord}(g_i)} \in \mathbb{Q}$$

is the *cross number* of S and

$$\iota(S) = \sum_{i=1}^{l} g_i \ \in G$$

denotes the sum of the elements of S.

We say that S is a *zero sequence* (resp. a *block*) if

$$\sum_{i=1}^{l} g_i = \sum_{g \in G_0} v_g(S) g = 0 \in G \ .$$

The set $\mathcal{B}(G_0)$ of all blocks is a submonoid of $\mathcal{F}(G_0)$, called the *block monoid* over G_0. The sequence S is a *minimal zero sequence*, if no proper subsequence is a zero sequence. The set of minimal zero sequences $\mathcal{U}(G_0)$ is just the set of irreducible elements of the monoid $\mathcal{B}(G_0)$. Let

$$\mathcal{D}(G_0) = \sup\{|U| \ \Big| \ U \in \mathcal{U}(G_0)\} \in \mathbb{N} \cup \{\infty\}$$

denote *Davenport's constant* of G_0. If G_0 is finite, then $\mathcal{U}(G_0)$ and hence $\mathcal{D}(G_0)$ are finite. For standard terminology in the theory of non-unique factorizations the reader is referred to the survey articles of S. Chapman, F. Halter-Koch and the second author in [And97]. The terminology concerning zero sequences is consistent with the one used in [GG98a].

3. Half-factorial subsets: First results

We start with the very definition.

Definition 1. Let G be an abelian group.

1. A non-empty subset $G_0 \subseteq G$ is said to be *half-factorial*, if the block monoid $\mathcal{B}(G_0)$ is half-factorial.
2. $$\mu(G) = \sup\{|G_0| \ \Big| G_0 \subseteq G \text{ is half-factorial}\} \in \mathbb{N} \cup \{\infty\}.$$

W. Narkiewicz gave a geometric interpretation of $\mu(G)$, see [Nar79], Proposition 5.

Lemma 3.1. *Let G be an abelian group with $|G| > 1$.*

1. *Half-factoriality is a property of finite character i.e., a subset $G_0 \subseteq G$ is half-factorial if and only if every finite subset of G_0 is half-factorial.*
2. *If $G_0 \subseteq G$ is half-factorial, then so is $G_0 \cup \{0\}$. In particular, $\{0, g\}$ is half-factorial for every $g \in G$, whence $\mu(G) \geq 2$.*
3. *If $H < G$ is a subgroup, then $\mu(H) \leq \mu(G)$.*
4. *If G_1, G_2 are subgroups of G with $G_1 \cap G_2 = \{0\}$, then $\mu(G) \geq \mu(G_1) + \mu(G_2) - 1$.*
5. *An independent subset is half-factorial.*

Proof. 1., 2. and 3. are obvious.

4. Let $H_i \subseteq G_i$ be half-factorial subsets with $|H_i| = \mu(G_i)$ for $1 \leq i \leq 2$. Then

$$\mathcal{B}(H_1 \cup H_2) = \mathcal{B}(H_1) \times B(H_2)$$

is half-factorial, $H_1 \cap H_2 \subseteq \{0\}$; whence

$$\mu(G) \ge |H_1 \cup H_2| \ge |H_1| + |H_2| - 1.$$

5. Let $G_0 = \{e_i \mid i \in I\}$ be an independent subset. Since for every $i \in I$ the monoid $\mathcal{B}(\{e_i\})$ is half-factorial, the block monoid

$$\mathcal{B}(G_0) = \coprod_{i \in I} \mathcal{B}(\{e_i\})$$

is half-factorial.

□

The following result, due to Skula and Sliwa, plays a key role in the investigation of half-factorial subsets. It will be used without further quoting. A proof in the present terminology may be found in [CG97], Proposition 5.4.

Lemma 3.2. *Let G be an abelian torsion group and $G_0 \subseteq G$ a non-empty subset. Then the following conditions are equivalent:*

1. *G_0 is half-factorial,*
2. *$k(U) = 1$ for every $U \in \mathcal{U}(G_0)$.*

Lemma 3.3. *Let G be an abelian torsion group, $G_0 \subseteq G$ a half-factorial subset 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. Consider an irreducible block

$$U = g^k \prod_{i=1}^{s} g_i^{k_i} \in \mathcal{U}(G_0 \cup \{g\}).$$

We have to show that $k(U) = 1$. Setting $k = lp + j$ with $l \in \mathbb{N}$ and $0 \le j \le p-1$ we obtain that

$$jg = -l(pg) - \sum_{i=1}^{s} k_i g_i.$$

If $j \neq 0$, there is some $x \in \mathbb{N}_+$ such that $jx = 1 + mp$ for some $m \in \mathbb{Z}$ which implies that

$$g = -x\big(m(pg) + l(pg) + \sum_{i=1}^{s} k_i g_i\big) \in \langle G_0 \rangle,$$

a contradiction. Therefore, $k = lp$ and

$$U' = (pg)^l \prod_{i=1}^{s} g_i^{k_i} \in \mathcal{U}(G_0)$$

with $k(U') = 1$. Assume to the contrary, that $p \not| \mathrm{ord}(g)$. Then there are $m, n \in \mathbb{Z}$ such that $1 = mp + n\mathrm{ord}(g)$; whence $g = (mp + n\mathrm{ord}(g))g = mpg \in \langle G_0 \rangle$, a contradiction. Thus we have $p|\mathrm{ord}(g)$, $\mathrm{ord}(pg) = \frac{\mathrm{ord}(g)}{p}$ and $k(U) = k(U') = 1$. □

In the sixties L. Claborn showed that for every abelian group G there exists a Dedekind domain R whose class group $Cl(R)$ is isomorphic to G. The question was raised whether for every given G there is a half-factorial Dedekind domain R with $Cl(R) \simeq G$. Theorem 3.6 in [CG97] shows that this question is equivalent to the following:

Does every abelian group have a half-factorial generating subset?

For direct sums of cyclic groups this is obvious. In [MS86] Michel and Steffan found various other classes for which the answers is yes. The general case is wide open. However, it is at least easy to see that infinite groups have infinite half-factorial subsets, as the following result shows.

Proposition 3.4. *Let G be an abelian group. If G is infinite, it has an infinite half-factorial subset. In particular, $\mu(G) < \infty$ if and only if G is finite.*

PROOF. If G is finite, then $\mu(G) \le |G| < \infty$. Suppose that G is infinite and consider the following three cases.

Case 1: G contains a subgroup isomorphic to $\mathbb{Z}$. By the very definition it follows that $\{-1\} \cup \mathbb{N} \subseteq \mathbb{Z}$ is a half-factorial subset.

Case 2: G contains an infinite independent subset. Then Lemma 3.1.5 implies the assertion.

Case 3: There is some prime $p \in \mathbb{P}$ such that for every $k \in \mathbb{N}_+$ the group G contains some element of order greater than p^k. Let $k \in \mathbb{N}_+$ and $g \in G$ with $\mathrm{ord}(g) = p^l$ for some $l > k$. An inductive argument applied to Lemma 3.3 shows that $\{p^i g | 0 \le i \le l\}$ is a half-factorial subset. □

Proposition 3.5. *Let G be a finite abelian group which is either cyclic or elementary (i.e., $\exp(G)$ is squarefree) and $G_0 \subseteq G$ a half-factorial subset with $|G_0| = \mu(G)$. Then G_0 is a generating subset. In particular, $\mu(G) > \mu(H)$ for all proper subgroups $H < G$.*

PROOF. Assume to the contrary that $\langle G_0 \rangle \neq G$.

Case 1: G is elementary. Then there is a non-trivial direct summand such that $G = \langle G_0 \rangle \oplus G_2$; whence Lemma 3.1 implies that

$$\mu(G) \ge \mu(\langle G_0 \rangle) + \mu(G_2) - 1 > \mu(\langle G_0 \rangle) \ge |G_0| = \mu(G),$$

a contradiction.

Case 2: $G = C_n$ for some $n \in \mathbb{N}_+$. Suppose that $|\langle G_0 \rangle| = m$ and let $p \in \mathbb{P}$ with $v_p(n) > v_p(m)$. Choose some $h \in G_0$ with

$$v_p(\mathrm{ord}(h)) = \max\{v_p(\mathrm{ord}(g)) | g \in G_0\} = v_p(m).$$

Then there is some $g \in G$ with $pg = h$. Since $v_p(\mathrm{ord}(g)) = pv_p(m)$, it follows that $g \notin \langle G_0 \rangle$. Thus Lemma 3.3 implies that $G_0 \cup \{g\}$ is half-factorial, a contradiction to $|G_0| = \mu(G)$.

Therefore, G_0 generates G which implies that $\mu(G) > \mu(H)$ for every proper subgroup $H < G$. □

Lemma 3.6. *Let $G = C_n^r$ with $r, n \in \mathbb{N}_+, (e_1, \ldots, e_r)$ a basis of G and $a = \sum_{i=1}^r a_i e_i$, $a' = \sum_{i=1}^r a_i' e_i \in G$ distinct with $\mathrm{ord}(a) = \mathrm{ord}(a')$ and $1 \le a_i, a_i' \le n$ for every $1 \le i \le r$. Let $G_0 \subseteq G$ be a half-factorial subset with $\{e_1, \ldots, e_r, a\} \subseteq G_0$. Then we have*

1. $\sum_{i=1}^r (n - a_i) = n - \gcd\{a_1, \ldots, a_r, n\}$,
2. *If $a' \in G_0$ and $r = 2$, then $a_1 \neq a_1'$ and $a_2 \neq a_2'$.*
3. *If $a' \in G_0$, then $a_i = a_i'$ implies that $\mathrm{ord}(a_i e_i) < \mathrm{ord}(a)$ for every $1 \le i \le r$.*

PROOF. 1. By Lemma 2.1 we have $\mathrm{ord}(a) = \frac{n}{\gcd\{a_1, \ldots, a_r, n\}}$. Since

$$U = a \prod_{i=1}^r e_i^{n-a_i} \in \mathcal{F}(G_0)$$

is a minimal zero sequence, Lemma 3.2 implies that

$$1 = k(U) = \frac{1}{n}\big(\gcd\{a_1, \ldots, a_r, n\} + \sum_{i=1}^r (n - a_i)\big).$$

2. Suppose $a' \in G_0$ and $r = 2$. Since $\mathrm{ord}(a) = \mathrm{ord}(a') = \frac{n}{\gcd\{a_1, \ldots, a_r, n\}}$, 1. implies that

$$(n - a_1) + (n - a_2) = (n - a_1') + (n - a_2').$$

Hence the assertion follows because $a \neq a'$.

3. Assume to the contrary that $a' \in G_0, a_1 = a_1'$ and $\mathrm{ord}(a_1 e_1) = \mathrm{ord}(a)$. Then there are $n_2, \ldots, n_r \in \mathbb{N}$ such that

$$U = a^{\mathrm{ord}(a)-1} a' \prod_{j=2}^r e_j^{n_j} \in \mathcal{U}(G_0).$$

Note that U is irreducible, since $(a_1e_1)^{\mathrm{ord}(a)-1}a_1'e_1$ is irreducible. Furthermore, $a \neq a'$ implies that $\sum_{j=2}^{r} n_j > 0$. Therefore,

$$k(U) = \frac{\mathrm{ord}(a)-1}{\mathrm{ord}(a)} + \frac{1}{\mathrm{ord}(a')} + \frac{1}{n}\sum_{j=2}^{r} n_j > 1,$$

a contradiction. □

We present a method to count elements in an r-fold product of a finite set. Let Z be a finite set, $r \in \mathbb{N}_+$, $E \subseteq Z$ and $H \subseteq Z^r$. For $a = (a_1, \ldots, a_r) \in H$ and $V \subseteq [1, r]$ define

$$V(a) = \{j \in [1, r] \mid a_j \in E\}$$

and

$$H(V) = \#\{a \in H \mid V(a) = V\}.$$

Let $\mathcal{V}$ be a system of subsets of $[1, r]$ such that $V(a) \in \mathcal{V}$ for every $a \in H$. Then

$$\sum_{V \in \mathcal{V}} H(V) = |H|$$

and for every $1 \leq j \leq r$

$$\sum_{\substack{V \in \mathcal{V} \\ j \in V}} H(V) = \#\{a \in H \mid j \in V(a)\}.$$

Suppose that $|V| \geq k \geq 1$ for every $V \in \mathcal{V}$. Then

$$k \sum_{V \in \mathcal{V}} H(V) \leq \sum_{j=1}^{r} \sum_{\substack{V \in \mathcal{V} \\ j \in V}} H(V);$$

whence

$$|H| \leq \frac{1}{k} \sum_{j=1}^{r} \sum_{\substack{V \in \mathcal{V} \\ j \in V}} H(V).$$

Proposition 3.7. *Let $G = C_{p^k}^r$ with $k, r \in \mathbb{N}_+$, $p \in \mathbb{P}$ and $G_0 \subseteq G$ a generating half-factorial subset. Then we have*

1. $|G_0| \leq 1 + r(p^k - 1)$,
2. *If $k = 1$, then $|G_0| \leq 1 + \frac{rp}{2}$.*

PROOF. By Lemma 2.1 in [GG98b] G_0 contains a basis $(e_1, \dots, e_r)$.

1. For $1 \le \nu \le k$ set $H_\nu = \{g \in G_0 \mid \operatorname{ord}(g) = p^\nu\}$. Then

$$G_0 \subseteq \{0\} \cup \bigcup_{\nu=1}^{k} H_\nu.$$

Let $1 \le \nu \le k$. In order to estimate $|H_\nu|$ we use all notations introduced above with $Z = \mathbb{Z}/p^k\mathbb{Z}, E = \{a + p^k\mathbb{Z} \mid \operatorname{ord}(a + p^k\mathbb{Z}) = p^\nu\}$ and $H = H_\nu$. If $a \in H_\nu$, then $|V(a)| \ge 1$. Set

$$\mathcal{V} = \{V \subseteq [1, r] \mid |V| \ge 1\}.$$

For $1 \le j \le r$ we have

$$\begin{aligned}\sum_{\substack{V \in \mathcal{V} \\ j \in V}} H_\nu(V) &= \#\{a \in H_\nu \mid j \in V(a)\} \\ &= \#\{a \in H_\nu \mid \operatorname{ord}(a_j + p^k\mathbb{Z}) = p^\nu\} \\ &\le \#\{a_j + p^k\mathbb{Z} \in Z \mid \operatorname{ord}(a_j + p^k\mathbb{Z}) = p^\nu\} \\ &= p^\nu - p^{\nu-1}\end{aligned}$$

where the inequality follows from Lemma 3.6.3. Therefore

$$|H_\nu| \le \sum_{j=1}^{r} \sum_{\substack{V \in \mathcal{V} \\ j \in V}} H_\nu(V) \le r(p^\nu - p^{\nu-1})$$

and

$$|G_0| \le 1 + \sum_{\nu=1}^{k} |H_\nu| \le 1 + r(p^k - 1).$$

2. Set $H = G_0 \setminus \{0, e_1, \dots, e_r\}, Z = \mathbb{Z}/p\mathbb{Z}$ and $E = Z \setminus \{0 + p\mathbb{Z}\}$. Let $a \in H$. Then

$$V(a) = \{j \in [1, r] \mid p \nmid a_j\}$$

and $0 \ne a$ implies that $V(a) \ne \emptyset$. Assume to the contrary that $|V(a)| = 1$. Then $a = a_j e_j$ for some $j \in [1, r]$; whence $a_j = 1$ by Lemma 3.6.1, a contradiction. Thus $|V(a)| \ge 2$ and we set

$$\mathcal{V} = \{V \subseteq [1, r] \mid |V| \ge 2\}.$$

Then Lemma 3.6.3 implies that for every $1 \le j \le r$

$$\sum_{\substack{V \in \mathcal{V} \\ j \in V}} H(V) \le p - 2.$$

Therefore we infer that

$$|G_0| \le 1 + r + |H| \le 1 + r + \frac{1}{2}\sum_{j=1}^{r}(p-2) = 1 + \frac{rp}{2}.$$

□

4. An upper bound for $\mu(G)$.

In this section we follow ideas of J. Sliwa developed in [Sli82]. However, note that Lemma 2 and its Corollary in that paper are incorrect.

Lemma 4.1. *Let G be a bounded abelian group of exponent n and $G_0 \subseteq G$ a non-empty subset. Then the following conditions are equivalent:*

1. $k(U) \in \mathbb{N}_+$ *for every* $U \in \mathcal{U}(G_0)$,
2. *there exists some* $f \in \mathrm{Hom}(G, \mathbb{Z}/n\mathbb{Z})$ *such that* $G_0 \subseteq \{g \in G \mid f(g) = \frac{n}{\mathrm{ord}(g)} + n\mathbb{Z}\}$.

Proof. 1) $\Rightarrow$ 2) Define a map $f : G_0 \to \mathbb{Z}/n\mathbb{Z}$ by $f(g) = \frac{n}{\mathrm{ord}(g)} + n\mathbb{Z}$ for every $g \in G_0$. In order to show that f extends to a homomorphism $f : \langle G_0 \rangle \to \mathbb{Z}/n\mathbb{Z}$ let, for every $g \in G_0$, integers $m_g \in \{0, \ldots, \mathrm{ord}(g) - 1\}$ be given such that $\sum_{g \in G_0} m_g g = 0$. We have to verify that $\sum_{g \in G_0} m_g f(g) = 0$. Since $B = \prod_{g \in G_0} g^{m_g} \in \mathcal{B}(G_0)$ allows a factorization into irreducible blocks, it follows that $k(B) \in \mathbb{N}$. Therefore,

$$\sum_{g \in G_0} m_g f(g) = \sum_{g \in G_0} \frac{m_g n}{\mathrm{ord}(g)} + n\mathbb{Z} = nk(B) + n\mathbb{Z} = 0.$$

Since $\mathbb{Z}/n\mathbb{Z}$ is an injective $\mathbb{Z}/n\mathbb{Z}$ module, $f : \langle G_0 \rangle \to \mathbb{Z}/n\mathbb{Z}$ may be extended to a $\mathbb{Z}/n\mathbb{Z}$ (and hence $\mathbb{Z}$) module homomorphism $f : G \to \mathbb{Z}/n\mathbb{Z}$.

2) $\Rightarrow$ 1) Let $U = \prod_{g \in G_0} g^{m_g} \in \mathcal{U}(G_0)$ be given. Then for some $f \in \mathrm{Hom}(G, \mathbb{Z}/n\mathbb{Z})$ having the above property we infer that

$$0 = f(0) = f\Big(\sum_{g \in G_0} m_g g\Big) = \sum_{g \in G_0} \frac{m_g n}{\mathrm{ord}(g)} + n\mathbb{Z} = nk(U) + n\mathbb{Z};$$

whence $k(U) \in \mathbb{N}_+$.

□

Let G be a finite abelian group. Define $\mu_0(G)$ as the maximal size of a subset $G_0 \subseteq G$ for which the equivalent conditions of Lemma 4.1 hold. Then Lemma 3.2 implies that

$$\mu(G) \le \mu_0(G).$$

Using property 2) of Lemma 4.1 we shall determine $\mu_0(C_n^r)$. To do so we have count to the number of solutions of a certain congruence. For $n, k \in \mathbb{N}_+$ let

$$\sigma_k(n) = \sum_{1 \le d \mid n} d^k$$

the sum of the kth powers of the divisors of n.

Proposition 4.2. *Let $r, n \in \mathbb{N}_+$, $d, a_1, \ldots, a_r \in \mathbb{Z}$ and $c = \gcd\{a_1, \ldots, a_r, n\}$.*

1. *If $c \mid d$, then*

$$\#\{\mathbf{x} \in [1,n]^r \mid \sum_{i=1}^r a_i x_i = d \mod n\} = cn^{r-1}.$$

2. *If $c = 1$, then*

$$\#\{\mathbf{x} \in [1,n]^r \mid \sum_{i=1}^r a_i x_i \equiv \gcd\{x_1, \ldots, x_r, n\} \mod n\} = \sigma_{r-1}(n).$$

3. $\#\{\mathbf{x} \in [1,n]^r \mid \sum_{i=1}^r a_i x_i \equiv \gcd\{x_1, \ldots, x_r, n\} \mod n\} = \sigma_{r-1}(n')$ *for some divisor n' of n.*

PROOF. 1. see Proposition 3.1 in [McC86].

2. Suppose $c = 1$. If $d \mid n$ and $\sum_{i=1}^r a_i x_i \equiv d \mod n$, then $\gcd\{x_1, \ldots, x_r, n\} \mid d$. Therefore, we have

$$\begin{aligned}
&\#\{\mathbf{x} \in [1,n]^r \mid \sum_{i=1}^r a_i x_i \equiv \gcd\{x_1, \ldots, x_r, n\} \mod = n\} \\
&\quad = \sum_{1 \le d \mid n} \#\{\mathbf{x} \in [1,n]^r \mid \sum_{i=1}^r a_i x_i \equiv d \mod n,\ d \mid \gcd\{x_1, \ldots, x_r, = n\}\} \\
&\quad = \sum_{1 \le d \mid n} \#\{\mathbf{y} \in [1, \frac{n}{d}]^r \mid \sum_{i=1}^r a_i y_i \equiv 1 \mod \frac{n}{d}\} \\
&\quad = \sum_{1 \le d \mid n} (\frac{n}{d})^{r-1} = \sigma_{r-1}(n).
\end{aligned}$$

3. We proceed by induction on n. Obviously, the assertion holds for $n = 1$. Suppose $n \ge 2$. If $c = 1$, then the assertion holds by part 2). Suppose there is some $p \in \mathbb{P}$ such that $p \mid \gcd\{a_1, \ldots, a_r, n\}$. Then there is a bijection between the set of all $\mathbf{x} \in [1,n]^r$ with

$$\sum_{i=1}^r a_i x_i \equiv \gcd\{x_1, \ldots, x_r, n\} \mod n$$

and the set of all $\mathbf{y} \in [1, \frac{n}{p}]^r$ with

$$\sum_{i=1}^{r} a_i y_i \equiv \gcd\{y_1, \ldots, y_r, \frac{n}{p}\} \mod \frac{n}{p}.$$

Hence the assertion follows by induction hypothesis. □

Theorem 4.3. *$\mu_0(C_n^r) = \sigma_{r-1}(n)$ where $n, r \in \mathbb{N}_+$.*

PROOF. Let $G = C_n^r$, $(e_1, \ldots, e_r)$ a basis of G, $f \in \mathrm{Hom}(G, \mathbb{Z}/n\mathbb{Z})$ and $G_f = \{g \in G \mid f(g) = \frac{n}{\mathrm{ord}(g)} + n\mathbb{Z}\}$. By Lemma 4.1 we have to estimate $|G_f|$. Suppose $f(e_i) = a_i + n\mathbb{Z}$ for $1 \le i \le r$ and let $g = \sum_{i=1}^r x_i e_i \in G$ with $x_1, \ldots, x_r \in [1, n]$. Then Lemma 2.1 implies that $\mathrm{ord}(g) = \frac{n}{\gcd\{x_1, \ldots, x_r, n\}}$. Therefore we infer that

$$G_f = \{\sum_{i=1}^{r} x_i e_i \mid \mathbf{x} \in [1, n]^r, \ \sum_{i=1}^{r} a_i x_i \equiv \gcd\{x_i, \ldots, x_r, n\} \mod n\}.$$

Proposition 4.2 implies that $|G_f| = \sigma_{r-1}(n')$ for some divisor n' of n. Furthermore, if f is surjective, then $\gcd\{a_1, \ldots, a_r, n\} = 1$; whence $|G_f| = \sigma_{r-1}(n)$. □

Corollary 4.4. *Let G be a finite abelian group of exponent n and rank r. Then $\mu(G) \le \sigma_{r-1}(n)$.*

PROOF. Set $G = C_{n_1} \oplus \cdots \oplus C_{n_r}$ with $1 < n_1 | \ldots | n_r = n$. Then

$$\mu(G) \le \mu(C_n^r) \le \mu_0(C_n^r) = \sigma_{r-1}(n).$$

□

5. Splittable sets and cyclic groups

In this section we characterize half-factorial subsets of cyclic groups in terms of splittable sets. This notion was introduced by A. Zaks (cf. Theorem 4 in [Zak76]) and further studied by P. Erdös and A. Zaks in [EZ90].

Definition 2. A set $N \subseteq \mathbb{N}_+$ is said to be *splittable*, if given distinct elements $n_1, \ldots, n_l \in N$ and positive integers $k_1, \ldots, k_l \in \mathbb{N}_+$ such that $\sum_{i=1}^l \frac{k_i}{n_i} \in \mathbb{N}_+$, then there exist $k_i' \in \{0, \ldots, k_i\}$ for every $1 \le i \le l$ such that $\sum_{i=1}^l \frac{k_i'}{n_i} = 1$.

Lemma 5.1. *Let $N \subseteq \mathbb{N}_+$ be chain of divisors (i.e., $n, n' \in N$ with $n' < n$ implies $n' | n$). Then N is splittable.*

PROOF. Let $n_1, \dots, n_l \in N$ with $n_1 | \dots | n_l$ and $k_1, \dots, k_l \in \mathbb{N}_+$ such that $\sum_{i=1}^{l} \frac{k_i}{n_i} = s \in \mathbb{N}_+$. If $s = 1$, we are done. Suppose $s \geq 2$. Set $m = \prod_{i=1}^{l} n_i$ and $m_i = \frac{m}{n_i}$ for $1 \leq i \leq l$. Then $m_l | \dots | m_1$ and $\sum_{i=1}^{l} k_i m_i = sm$. Let $t \in \mathbb{N}_+$ be the smallest integer such that $\sum_{i=1}^{t} k_i m_i > m$. Then

$$0 \leq m - \sum_{i=1}^{t-1} k_i m_i < k_t m_t$$

and $m_t \mid m - \sum_{i=1}^{t-1} k_i m_i$. Therefore there is some $k_t' \in \{0, \dots, k_t - 1\}$ such that $m - \sum_{i=1}^{t-1} k_i m_i = k_t' m_t$; whence

$$1 = \sum_{i=1}^{t-1} \frac{k_i}{n_i} + \frac{k_t'}{n_t}.$$

□

Lemma 5.2. *Let $G_0 \subseteq \mathbb{Z}/n\mathbb{Z}$ with $2 \leq n \in \mathbb{N}_+$ a generating half-factorial subset. Then there exists some $\varphi \in \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ such that $\varphi(G_0) \subseteq \{a + n\mathbb{Z} \mid 1 \leq a \leq n,\ a | n\}$.*

PROOF. By Lemma 4.1 there exists some $f \in \mathrm{End}(\mathbb{Z}/n\mathbb{Z})$ such that

$$G_0 \subseteq G_f = \{g \in G \mid f(g) = \frac{n}{\mathrm{ord}(g)} + n\mathbb{Z}\}.$$

Suppose $f(1 + n\mathbb{Z}) = r + n\mathbb{Z}$ for some $1 \leq r \leq n$ and set $s = \gcd(r, n)$. Then

$$G_f = \{a + n\mathbb{Z} \mid ar \equiv \gcd(a, n) \mod n\};$$

whence $s | a$ for $a + n\mathbb{Z} \in G_f$. Since $\langle G_0 \rangle = \langle G_f \rangle = \mathbb{Z}/n\mathbb{Z}$, it follows that $s = 1$. Therefore

$$G_f = \{a + n\mathbb{Z} \mid ar \equiv \gcd(ar, n) \mod n\}.$$

Define $\varphi : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ by $\varphi(x + n\mathbb{Z}) = rx + n\mathbb{Z}$ for $x \in \mathbb{Z}$. Then

$$\begin{aligned} \varphi(G_f) &= \{ar + n\mathbb{Z} \mid ar \equiv \gcd(ar, n) \mod n\} \\ &= \{b + n\mathbb{Z} \mid 1 \leq b \leq n,\ b \equiv \gcd(b, n) \mod n\} \\ &= \{b + n\mathbb{Z} \mid 1 \leq b \leq n,\ b | n\}. \end{aligned}$$

□

Theorem 5.3. *Let $n \in \mathbb{N}_+$, $A \subseteq [1, n]$, $D = \{d \in \mathbb{N}_+ \mid d \text{ divides } n\}$ and $G_0 = \{a + n\mathbb{Z} \mid a \in A\}$.*

1. If G_0 is a generating half-factorial subset, then there is some $\varphi \in \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ such that $\varphi(G_0) \subseteq \{d + n\mathbb{Z} \mid d \in D\}$ and $\{\mathrm{ord}(g) \mid g \in G_0\} \subseteq \mathbb{N}_+$ is splittable.

2. If $A \subseteq D$ and $\{\frac{n}{a} \mid a \in A\} \subseteq \mathbb{N}_+$ is splittable, then G_0 is half-factorial.

3. $\mu(C_n) = \max\{|A| \mid A \subset D,\ A \text{ is splittable}\}$.

PROOF. 1. The first assertion follows from Lemma 5.2. Since for every $\varphi \in \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ and every $g \in G_0$ $\mathrm{ord}(g) = \mathrm{ord}\big(\varphi(g)\big)$ we may assume that

$$G_0 \subset \{a_i + n\mathbb{Z} \mid 1 \le i \le k,\ a_i \in D\}.$$

Then for every $1 \le i \le k$ we have $\mathrm{ord}(a_i + n\mathbb{Z}) = \frac{n}{a_i} = n_i$. Suppose that $\sum_{i=1}^k \frac{k_i}{n_i} \in \mathbb{N}_+$. Consider the sequence

$$B = \prod_{i=1}^k (a_i + n\mathbb{Z})^{k_i}.$$

Then

$$k(B) = \sum_{i=1}^k \frac{k_i}{n_i} = \frac{1}{n} \sum_{i=1}^k k_i a_i \in \mathbb{N}_+;$$

whence $\sum_{i=1}^k k_i a_i \equiv 0 \mod n$ i.e., B is a block. Therefore, there is some irreducible block $U = \prod_{i=1}^k (a_i + n\mathbb{Z})^{k_i'}$ dividing B. Thus $0 \le k_i' \le k_i$ for every $1 \le i \le k$ and

$$1 = k(U') = \sum_{i=1}^k \frac{k_i'}{n_i}.$$

2. Suppose that $A = \{a_1, \ldots, a_k\} \subset D$ and $\{n_i = \frac{n}{a_i} \mid 1 \le i \le k\}$ is splittable. Let some

$$U = \prod_{i=1}^k (a_i + n\mathbb{Z})^{k_i} \in \mathcal{U}(G_0)$$

be given. Then $\sum_{i=1}^k k_i a_i \equiv 0 \mod n$; whence

$$k(U) = \sum_{i=1}^k \frac{k_i}{n_i} = \frac{1}{n} \sum_{i=1}^k k_i a_i \in \mathbb{N}_+.$$

By assumption there are $k_i' \in \{0, \ldots, k_i\}$ such that

$$\sum_{i=1}^k \frac{k_i'}{n_i} = \frac{1}{n} \sum_{i=1}^k k_i' a_i = 1.$$

Therefore, $U' = \prod_{i=1}^k (a_i + n\mathbb{Z})^{k_i'}$ is a zero subsequence of U whence $U' = U$ and $1 = k(U') = k(U)$.

3. If $A \subset D$ is splittable, then $|A| \le \mu(C_n)$ by 2. Conversely, let $G_0 \subset \mathbb{Z}/n\mathbb{Z}$ be half-factorial with $|G_0| = \mu(G)$. Then G_0 is a generating subset by Proposition 3.5. Therefore 1) implies that $\mu(G) = |G_0| \le \max\{|A| \mid A \subset D \text{ is splittable}\}$. □

Main parts of the following Corollary were first achieved by Skula (Proposition 3.4 in [Sku76]), Sliwa (Lemma 1 in [Sli76]), Zaks (Corollary 5 in [Zak76]) and by Michel and Steffan (Proposition 5 in [MS86]).

Corollary 5.4. *Let $p \in \mathbb{P}$ be a prime and $k \in \mathbb{N}_+$.*

1. $G_0 = \{p^i + p^k\mathbb{Z} \mid 0 \le i \le k\} \subseteq \mathbb{Z}/p^k\mathbb{Z}$ is a generating half-factorial subset. For every generating half-factorial subset $H \subseteq \mathbb{Z}/p^k\mathbb{Z}$ there is some $\varphi \in \mathrm{Aut}(\mathbb{Z}/p^k\mathbb{Z})$ such that $\varphi(H) \subseteq G_0$. In particular, $\mu(\mathbb{Z}/p^k\mathbb{Z}) = k + 1$.

2. Let $\mathbb{Z}(p^\infty) \simeq G = \{\frac{a}{p^i} \mid a \in \mathbb{Z},\ i \in \mathbb{N}\}/\mathbb{Z} \subseteq (\mathbb{Q}/\mathbb{Z}, +)$. Then $G_0 = \{\frac{1}{p^i} + \mathbb{Z} \mid i \in \mathbb{N}\} \subseteq G$ is a generating half-factorial subset.

PROOF. 1. G_0 is half-factorial by Theorem 5.3.2 and Lemma 5.2. The second assertion follows from Theorem 5.3.1. Using Proposition 3.5 we infer that $\mu(\mathbb{Z}/p^k\mathbb{Z}) = k + 1$.

2. G_0 is a generating subset by construction. Since half-factoriality is a property of finite character (see Lemma 3.1.1) implies that G_0 is half-factorial. □

6. LOWER BOUNDS FOR $\mu(G)$

Definition 3. For a finite abelian group G let $s(G) \in \mathbb{N}_+$ denote the minimum of all $s \in \mathbb{N}_+$ such that every $S \in \mathcal{F}(G)$ with $|S| \ge s$ has a zero subsequence S' with $|S'| = \exp(G)$.

For a finite abelian group G the invariant $s(G)$ plays a key role in zero sum theory. Furthermore, it allows a geometric interpretation if $G = (\mathbb{Z}/n\mathbb{Z})^r$. We list some main results on $s(G)$. For more information the reader is referred to the paper of Alon and Dubiner [AD93].

Lemma 6.1. *Let G be a finite abelian group and $n \in \mathbb{N}_+$. Then we have*

1. *(Erdös-Ginzburg-Ziv-Theorem) $s(C_n) = 2n - 1$,*
2. *$s(G) \le |G| + \exp(G) - 1$,*
3. *$s(C_n \oplus C_n) \le 6n - 5$,*
4. *For every $r \in \mathbb{N}_+$ there is some constant $c(r) \in \mathbb{N}_+$ such that $s(C_n^r) \le c(r)n$.*

PROOF. 1) was first proved by Erdös, Ginzburg and Ziv in [EGZ61]. For a variety of different proofs of 1) and for 3) and 4) cf. [AD93]. 2) is due to Gao and Yang [GY97]. □

Corollary 6.2. *Let G be a finite abelian group of order n, m a divisor of n and $S \in \mathcal{F}(G)$ a zero sequence of length $|S| = 2n - m$. Then S contains a zero subsequence S' of length $|S'| = n$.*

PROOF. Let H be a subgroup of G with $|G/H| = m$ and $\varphi : G \to G/H$ the canonical epimorphism. Since

$$|\varphi(S)| = |S| = m(2|H| - 1)$$

we can apply Erdös-Ginzburg-Ziv-Theorem $(2|H| - 1)$-times to obtain subsequences $S_1, \ldots, S_{2|H|-2}$ such that $S = S_0 S_1 \ldots S_{2|H|-2}$, $|S_1| = \cdots = |S_{2|H|-2}| = m$ and $\varphi(S_1), \ldots, \varphi(S_{2|H|-2})$ have sum zero in G/H. But this implies that $|S_0| = m$ and $\varphi(S_0)$ is a zero subsequence in G/H. Therefore $T = \prod_{i=0}^{2|H|-2} \iota(S_i)$ is a sequence in H. Applying the Erdös-Ginzburg-Ziv-Theorem to T we obtain the assertion. □

Theorem 6.3. *Let $G = H \oplus C_n$ be a finite abelian group with $\exp(H) = m$ and $\exp(G) = n$ where $m|n$.*

1. *If $D(G) < 2n$ or $s(H) \le n + m$, then $\mu(G) \ge \frac{|G|}{n} + 1$.*
2. *If n is even, $D(G) < 2n$ and $|G| = n^2$, then $\mu(G) \ge n + 2$.*

Remark. Note that $|G| \le n^2$ implies $|H| \le n$; whence Lemma 6.1.2 yields $s(H) \le n + m - 1$. Part 2) shows that the Corollary after Lemma 2 in [Sli82] is incorrect.

PROOF. Set $G = H \oplus \langle a \rangle$ with $\mathrm{ord}(a) = n$ and $n = mk$. Define

$$G_0 = \{0\} \cup \{h + a \mid h \in H\}.$$

Then $|G_0| = 1 + |H| = 1 + \frac{|G|}{n}$.

1. To show that G_0 is half-factorial we verify that $k(U) = 1$ for every $0 \ne U \in \mathcal{U}(G_0)$. Let $0 \ne U = \prod_{i \in I}(h_i + a) \in \mathcal{U}(G_0)$ be given. Since $k(U) = \frac{|U|}{n}$, we have to check that $|U| = n$. Clearly, $n = \mathrm{ord}(a)$ divides $|U|$.

If $D(G) < 2n$, then $1 < |U| \le D(G) < 2n$ implies that $|U| = n$.

Suppose that $s(H) \le n + m$. Assume to the contrary that

$$|S| \ge 2n = n + km.$$

By definition of $s(H)$ there exist k zero sequences $V_\nu = \prod_{i \in I_\nu} h_i$ with $|V_\nu| = \exp(H) = m$ for $1 \le \nu \le k$ such that $V_1 \ldots V_k \mid \prod_{i \in I} h_i$. Then

$$S' = \prod_{\nu=1}^{k} \prod_{i \in I_\nu} (h_i + a)$$

is a proper zero subsequence of S, a contradiction.

2. Suppose that n is even, $D(G) < 2n$ and $|H| = n$. Set $a^* = \frac{n}{2}a$ and $G_0^* = G_0 \cup \{a^*\}$. To show that G_0^* is half-factorial it remains to consider blocks

$U \in \mathcal{U}(G_0)$ of the form

$$U = a^* \prod_{i \in I} (h_i + a) \in \mathcal{U}(G_0).$$

Since U has sum zero and $D(G) < 2n$, it follows that $|I| \in \{\frac{n}{2}, \frac{3n}{2}\}$. Assume to the contrary, that $|I| = \frac{3n}{2}$. Then by Corollary 6.2 the sequence $\prod_{i \in I} h_i$ contains a zero subsequence $\prod_{i \in I'} h_i$ with $|I'| = n$. Therefore, $\prod_{i \in I'}(h_i + a)$ is a proper zero subsequence of U, a contradiction. This implies that $|I| = \frac{n}{2}$ and

$$k(U) = \frac{1}{2} + |I|\frac{1}{n} = 1.$$

□

Part 2) of the following Corollary was first established in [GK92] Theorem 8.

Corollary 6.4. *Let $n, r \in \mathbb{N}_+$ and $\Omega(n)$ the number of prime divisors of n counted with multiplicity.*

1. $1 + (r - 2[\frac{r}{2}])\Omega(n) + n[\frac{r}{2}] \le \mu(C_n^r) \le \sigma_{r-1}(n)$.
2. *If $n = p \in \mathbb{P}$, then*

$$1 + (r - 2[\frac{r}{2}]) + p[\frac{r}{2}] \le \mu(C_p^r) \le 1 + \frac{rp}{2}.$$

3. *If $n = p \in \mathbb{P}$ and $k \in \mathbb{N}_+$, then*

$$1 + p^k \le \mu(C_{p^k} \oplus C_{p^k}) \le \frac{p^{k+1} - 1}{p - 1}.$$

PROOF. 1. The right inequality follows from Corollary 4.4. Let $n = p_1 \dots p_s$ with $s = \Omega(n)$ and $p_1, \dots, p_s \in \mathbb{P}$. Then $\{\prod_{i=1}^k p_i \mid 0 \le k \le s\}$ is a splittable set of divisors of n; whence $\mu(C_n) \ge s + 1 = \Omega(n) + 1$ (cf. Theorem 5.3 and Lemma 5.1). Theorem 6.3 implies that $\mu(C_n \oplus C_n) \ge n + 1$. Thus the left inequality follows from Lemma 3.1.4 by induction on r.

2. Since $\Omega(p) = 1$, the left inequality follows from 1. Let $G_0 \subseteq G = C_p^r$ be a half-factorial subset with $|G_0| = \mu(G)$. By Proposition 3.5 G_0 is a generating subset; whence Proposition 3.7 implies that $|G_0| \le 1 + \frac{rp}{2}$.

3. This is a consequence of 1. □

Corollary 6.5. *Let $p \in \mathbb{P}$, $k, s \in \mathbb{N}_+$ with $k \ge 2$, $p + k \ge 6$ and $G = (C_{p^k})^{(p+1)s}$. Then $\mu(G) \ge 1 + sp^{p(k-1)}$. If $G_0 \subseteq G$ is half-factorial with $|G_0| = \mu(G)$, then $\langle G_0 \rangle \ne G$ but $\mu(\langle G_0 \rangle) = \mu(G)$.*

PROOF. Set $H = C_{p^{k-1}}^{p} \oplus C_{p^k}$. Then $\exp(H) = p^k$ and $D(H) = p^k + p(p^{k-1} - 1) < 2p^k$. Thus Theorem 6.3 implies that $\mu(H) \geq 1 + p^{p(k-1)}$. By Lemma 3.1.4 we infer that

$$\mu(G) \geq \mu(H^s) \geq 1 + s(\mu(H) - 1) \geq 1 + sp^{p(k-1)}.$$

Let $G_0 \subseteq G$ be a generating half-factorial subset. Then Proposition 3.7 shows that

$$|G_0| \leq 1 + s(p+1)(p^k - 1).$$

Since $2 \leq k$ and $p + k \geq 6$ it follows that $|G_0| < \mu(G)$. Therefore, if $G_0 \subseteq G$ is half-factorial with $|G_0| = \mu(G)$, then $\langle G_0 \rangle \neq G$ but

$$\mu(G) = |G_0| \leq \mu(\langle G_0 \rangle) \leq \mu(G).$$

□

REFERENCES

[AA94] D.D. Anderson and D.F. Anderson. Elasticity of factorizations in integral domains II. *Houston J. Math.*, 20:1 – 15, 1994.

[ACS94a] D.F. Anderson, S. Chapman, and W. Smith. On Krull half-factorial domains with infinite cyclic divisor class group. *Houston J. Math.*, 20:561 – 570, 1994.

[ACS94b] D.F. Anderson, S. Chapman, and W. Smith. Overrings of half-factorial domains. *Canadian Math. Bull.*, 37:437 – 442, 1994.

[ACS94c] D.F. Anderson, S. Chapman, and W. Smith. Some factorization properties of Krull domains with infinite cyclic divisor class group. *J. Pure Appl. Algebra*, 96:97 – 112, 1994.

[ACS95] D.F. Anderson, S. Chapman, and W. Smith. Overrings of half-factorial domains II. *Comm. Algebra*, 23:3961 – 3976, 1995.

[AD93] N. Alon and M. Dubiner. Zero-sum sets of prescribed size. In *Combinatorics, Paul Erdös is Eighty, Vol. 1*, pages 33 – 50. J. Bolyai Math. Soc., 1993.

[And97] D. D. Anderson. *Factorization in integral domains.* Marcel Dekker, 1997.

[AP97] D.F. Anderson and J. Park. Locally half-factorial domains. *Houston J. Math.*, 23:617 – 630, 1997.

[CG97] S. Chapman and A. Geroldinger. Krull domains and monoids, their sets of lengths and associated combinatorial problems. In *Factorization in integral domains*, volume 189 of *Lecture Notes in Pure Appl. Math.*, pages 73 – 112. Marcel Dekker, 1997.

[EGZ61] P. Erdös, A. Ginzburg, and A. Ziv. Theorem in the additive number theory. *Bull. Research Council Israel*, 10:41 – 43, 1961.

[EZ90] P. Erdös and A. Zaks. Reducible sums and splittable sets. *J. Number Theory*, 36:89 – 94, 1990.

[Ger90] A. Geroldinger. Ein quantitatives Resultat über Faktorisierungen verschiedener Länge in algebraischen Zahlkörpern. *Math. Z.*, 205:159 – 162, 1990.

[GG98a] W. Gao and A. Geroldinger. On long minimal zero sequences in finite abelian groups. 1998.

[GG98b] W. Gao and A. Geroldinger. Systems of sets of lengths II. 1998.

[GHKK95] A. Geroldinger, F. Halter-Koch, and J. Kaczorowski. Non-unique factorizations in orders of global fields. *J. reine angew. Math.*, 459:89 – 118, 1995.

[GK92] A. Geroldinger and J. Kaczorowski. Analytic and arithmetic theory of semigroups with divisor theory. *J. Theorie d. Nombres Bordeaux*, 4:199 – 238, 1992.

[GY97] W. Gao and Y.X. Yang. Note on a combinatorial constant. *J. Math. Res. and Expo.*, 17:139 – 140, 1997.

[McC86] P.J. McCarthy. *Introduction to Arithmetical functions*. Springer, 1986.

[MS86] D. Michel and J.L. Steffan. Repartition des ideaux premiers parmi les classes d ideaux dans un anneau de Dedekind et equidecomposition. *J. Algebra*, 98:82 – 94, 1986.

[Nar79] W. Narkiewicz. Finite abelian groups and factorization problems. *Colloq. Math.*, 42:319 – 330, 1979.

[Sku76] L. Skula. On c-semigroups. *Acta Arithm.*, 31:247 – 257, 1976.

[Sli76] J. Sliwa. Factorizations of distinct lengths in algebraic number fields. *Acta Arith.*, 31:399 – 417, 1976.

[Sli82] J. Sliwa. Remarks on factorizations in algebraic number fields. *Coll. Math.*, 46:123 – 130, 1982.

[Zak76] A. Zaks. Half-factorial domains. *Bull. AMS*, 82:721 – 723, 1976.

Received February 7, 1998

(Gao) Department of Computer Science and Technology, University of Petroleum, Beijing, Shuiku Road, Changping, Beijing 102200, P.R. China

E-mail address: wdgao@mail.bjpeu.edu.cn

(Geroldinger) Institut für Mathematik, Karl-Franzens Universität, Heinrichstrasse 36, 8010 Graz, Austria

E-mail address: alfred.geroldinger@kfunigraz.ac.at