ARITHMETICAL CHARACTERIZATION OF CLASS GROUPS OF THE FORM $\mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$ VIA THE SYSTEM OF SETS OF LENGTHS

WOLFGANG A. SCHMID

Abstract. Let H be a Krull monoid with finite class group such that each class contains a prime divisor (e.g., the multiplicative monoid of the ring of algebraic integers of some number field). It is shown that it can be determined whether the class group is of the form $\mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$, for $n \geq 3$, just by considering the system of sets of lengths of H.

1. Introduction

Let R be the ring of integers of an algebraic number field with class group G. As is very well-known, R is factorial if and only if $|G| = 1$. L. Carlitz [1] showed that R is half-factorial (see below) if and only if $|G| \leq 2$, thus characterizing rings of algebraic integers whose class groups have two elements in an arithmetical way. In the 1970s W. Narkiewicz asked (cf. [16]) whether arbitrary class groups can be characterized in an arithmetical way as well (see [14, 17] for the first solutions, [11, Chapter 7] for an exposition of various results of this type, and [4] for a recent contribution). In L. Carlitz' investigations to consider sets of lengths of factorizations was crucial. We recall the definition; we do so for Krull monoids, since now it is customary to investigate such problems in this more general context (see, e.g., [2, 11]).

Let H be a Krull monoid with finite class group G such that each class contains a prime divisor (e.g., the multiplicative monoid of the ring of algebraic integers of some number field, or more generally a regular congruence monoid in a holomorphy of some global field, cf. [11] in particular Examples 2.3.2 and 8.10.2). For $a \in H$, if $a = u_1 \dots u_\ell$ is a factorization into irreducible elements, then we say that a has a factorization of length ℓ. We denote by $\mathsf{L}(a)$ the set of all $\ell \in \mathbb{N}_0$ such that a has a factorization of length ℓ (for an invertible element this set is $\{0\}$). The set $\mathsf{L}(a)$ is called the set of lengths of a and the set $\mathcal{L}(H) = \{\mathsf{L}(a) \colon a \in H\}$ is called the system of sets of lengths of H. It is well known that $\mathcal{L}(H)$ just depends on the class group G, more

2000 *Mathematics Subject Classification.* 11R27 (13F05, 20K01).
Key words and phrases. class group, non-unique factorization, Krull monoid.
Supported by the Austrian Science Fund FWF (Project P18779-N13).

precisely it is equal to $\mathcal{L}(\mathcal{B}(G))$, where $\mathcal{B}(G)$ denotes the monoid of zero-sum sequences over G (see Section 2 for details). For brevity, we refer to $\mathcal{L}(\mathcal{B}(G))$ simply as the system of sets of lengths of G and use the short-hand notation $\mathcal{L}(G)$.

The investigation of systems of sets of lengths is a main subject of Non-Unique Factorization Theory (see, e.g., [2, 11]) and one of the goals of these investigations is to understand to what extent the converse of the above statement is true, i.e., under which conditions $\mathcal{L}(G) = \mathcal{L}(G')$, for finite abelian groups G and G', implies that G and G' are isomorphic (see [11, Section 7.3]). By L. Carlitz' result, it is known that $\mathcal{L}(G) = \{\{k\} \colon k \in \mathbb{N}_0\}$, i.e., $\mathcal{B}(G)$ is half-factorial, if and only if $|G| \le 2$. Thus, on the one hand groups of order 1 and 2 have the same system of sets of lengths, yet on the other hand this system is distinct from those of all other finite abelian groups. A. Geroldinger [9] started a systematic investigation of this problem. Roughly, his results can be summarized as follows: A cyclic group of order 3 and an elementary 2-group of rank 2 have the same system of sets of lengths and this system is distinct from those of all other types of finite abelian groups. A cyclic group of order at least 4 has a distinctive system of sets of lengths, i.e., no other (except, of course, for isomorphy) finite abelian group has the same system of sets of lengths. And, the same holds true for elementary 2-group of rank at least 3, groups that are the direct sum of a cyclic group of order at least 3 and a group of order 2, and some "small" groups (the Davenport constant, cf. Section 2 for a definition, of the group has to be at most 7 and at least 4).

Thus, the question arises whether apart from the two pairs of groups that are known to have the same system of sets of lengths all other finite abelian groups indeed have a distinctive system of sets of lengths, which would provide a new arithmetical characterization of the class group.

We recall that for infinite abelian groups the situation is very different; namely, by a result of F. Kainrath [15] all infinite abelian groups have the same system of sets of lengths, which is different from that of every finite abelian group. Moreover, the condition that each class contains a prime divisor is essential. Indeed, for each finite abelian and various types of infinite abelian groups G there exists a Krull monoid H with class group (isomorphic to) G such that H is half-factorial (see [10]).

In this paper we prove for a further class of groups, namely groups of the form $\mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$, for $n \ge 3$, that they have a distinctive system of sets of lengths (see Theorem 4.1). There are two crucial tools in our investigations. On the one hand, we use various results on the Davenport constant (and a variant thereof, the cross number), a classical invariant in combinatorial number theory (cf. Section 2). On the other hand, we use and establish results on $\Delta^*(G)$, an invariant introduced in [6]; in particular, we obtain a new upper bound for $\max \Delta^*(G)$ that is sharp for p-groups (see Theorem 3.1).

2. Preliminaries

Our notation and terminology is consistent with the monograph [11] to which we refer for a detailed discussion of the concepts discussed below.

Throughout the paper all intervals are intervals of integers, i.e., for $r, s \in \mathbb{Z}$, let $[r, s] = \{z \in \mathbb{Z} : r \le z \le s\}$.

We recall some terminology regarding finite abelian groups. Let G be a finite abelian group. We use additive notation and denote the identity element by 0. A subset $E \subset G \setminus \{0\}$ is called independent if $\sum_{e \in E} m_e e = 0$, where $m_e \in \mathbb{Z}$, implies that $m_e e = 0$ for each $e \in E$. For a subset $G_0 \subset G$, we denote by $\langle G_0 \rangle$ the subgroup generated by G_0; the subset is called a generating set if $\langle G_0 \rangle = G$.

For $n \in \mathbb{N}$, we denote by C_n a cyclic group with n elements. For each finite abelian group there exist uniquely determined positive integers $1 < n_1 \mid \cdots \mid n_r$ such that $G \cong C_{n_1} \oplus \cdots \oplus C_{n_r}$; the rank of G is $\mathsf{r}(G) = r$ and the exponent of G is $\exp(G) = n_r$. Moreover, there exist (up to ordering) uniquely determined prime-powers $q_1, \ldots, q_{r^*}$ such that $G \cong C_{q_1} \oplus \cdots \oplus C_{q_{r^*}}$; the total rank of G is $\mathsf{r}^*(G) = r^*$ and for p a prime the p-rank of G is $\mathsf{r}_p(G) = |\{i \in [1, r^*] : p \mid q_i\}|$. Thus, $\mathsf{r}^*(G) = \sum_{p \in \mathbb{P}} \mathsf{r}_p(G)$ and moreover $\mathsf{r}(G) = \max\{\mathsf{r}_p(G) : p \in \mathbb{P}\}$. The group G is called a p-group if its exponent is a prime-power, equivalently $\mathsf{r}(G) = \mathsf{r}^*(G)$.

In our investigations we need the following characterization of the total rank of a finite abelian group.

Lemma 2.1 ([11, Lemma A.6])**.** *The total rank of G is the maximal cardinality of a minimal (with respect to inclusion) generating subset of G.*

Next we recall the definition of a zero-sum sequence over a finite abelian group and related notions. For G_0 a subset of a finite abelian group G, let $\mathcal{F}(G_0)$ denote the multiplicatively written free abelian monoid over G_0; we denote its identity element by 1. An element $S \in \mathcal{F}(G_0)$ is called a sequence over G_0. For each sequence S over G_0 there exist uniquely determined $v_g \in \mathbb{N}_0$ such that $S = \prod_{g \in G_0} g^{v_g}$; we refer to $\mathsf{v}_g(S) = v_g$ as the multiplicity of g in S. Moreover, $|S| = \sum_{g \in G_0} v_g \in \mathbb{N}_0$ is called the length of S, $\sigma(S) = \sum_{g \in G_0} v_g g \in G$ the sum of S, and $\mathsf{k}(S) = \sum_{g \in G_0} v_g / (\operatorname{ord} g) \in \mathbb{Q}$ the cross number of S. The set $\operatorname{supp}(S) = \{g \in G_0 : \mathsf{v}_g(S) > 0\}$ is called the support of S. If $T \mid S$ (in $\mathcal{F}(G)$) then we say that T is a subsequence of S.

A sequence B is called a zero-sum sequence if $\sigma(B) = 0$; the set of all zero-sum sequences over G_0, denoted by $\mathcal{B}(G_0)$, form a submonoid of $\mathcal{F}(G_0)$. A zero-sum sequence A is called a minimal zero-sum sequence if $A \ne 1$ and $A = BC$ with $B, C \in \mathcal{B}(G_0)$ implies that $B = 1$ or $C = 1$, i.e., A has no proper and non-trivial zero-sum subsequence. The set of all minimal zero-sum sequences is denoted by $\mathcal{A}(G_0)$. The monoid $\mathcal{B}(G_0)$ is a Krull monoid and its irreducible elements are the minimal zero-sum sequences. If H is a Krull monoid with (finite) class group G and $G_P \subset G$ denotes the subset of classes containing prime divisors, then $\mathcal{L}(H) = \mathcal{L}(\mathcal{B}(G_P))$.

We denote by $\mathsf{D}(G) = \max\{|A| \colon A \in \mathcal{A}(G)\}$ the Davenport constant of G and by $\mathsf{K}(G) = \max\{\mathsf{k}(A) \colon A \in \mathcal{A}(G)\}$ the cross number of G. We recall that for $G \cong C_{n_1} \oplus \cdots \oplus C_{n_r} \cong C_{q_1} \oplus \cdots \oplus C_{q_{r^*}}$ with $n_i \mid n_{i+1}$ and prime powers q_i

$$(1) \quad \mathsf{D}(G) \geq 1 + \sum_{i=1}^{r}(n_i - 1) \quad \text{and} \quad \mathsf{K}(G) \geq \frac{1}{\exp(G)} + \sum_{i=1}^{r^*} \frac{q_i - 1}{q_i}.$$

In case G is a p-group equality holds in both inequalities, and in case $r \leq 2$ equality holds for the Davenport constant. We note that examples are known where $\mathsf{D}(G)$ actually exceeds the lower bound, e.g., this is the case for $C_6 \oplus C_2^4$ (cf. [7, Theorem 3.4]). Even for groups of rank three the value of $\mathsf{D}(G)$ is in general unknown, though for special types of groups it is known that equality holds at the lower bound; here we only need the fact that $\mathsf{D}(C_6 \oplus C_3^2) = 10$ (see [5]). However, no example is known where $\mathsf{K}(G)$ exceeds the lower bound. Recent results, due to B. Girard [13], show that if the smallest prime divisor of $|G|$ grows and $\mathsf{r}^*(G)$ is fixed, then $\mathsf{K}(G)$ is asymptotically equal to $\mathsf{r}^*(G)$ and thus asymptotically equal to the lower bound. In our investigations we frequently use the following upper bound on $\mathsf{K}(G)$ (cf. [11, Theorem 5.5.5]):

$$(2) \qquad \mathsf{K}(G) \leq \frac{1}{2} + \log |G|.$$

We refer to [11, Section 5.5] and [7] for a detailed exposition of these and various other results on $\mathsf{D}(G)$ and $\mathsf{K}(G)$.

3. Results on $\Delta^*(G)$

In order to investigate sets of lengths one considers the successive distances: if $L = \{\ell_1, \ell_2, \dots\} \subset \mathbb{Z}$ with $\ell_i < \ell_{i+1}$, then $\Delta(L) = \{\ell_2 - \ell_1, \ell_3 - \ell_2, \dots\}$. Furthermore, for G a finite abelian group and $G_0 \subset G$, let $\Delta(G_0) = \bigcup_{L \in \mathcal{L}(\mathcal{B}(G_0))} \Delta(L)$ and let

$$\Delta^*(G) = \{\min \Delta(G_0) \colon G_0 \subset G,\ \Delta(G_0) \neq \emptyset\}.$$

The relevance of the set $\Delta^*(G)$ is due to the fact that each $L \in \mathcal{L}(G)$ is an almost arithmetical multiprogression, with a universal bound, whose difference is an element of $\Delta^*(G)$ (see [11, Chapter 4]).

We recall some additional terminology, introduced in [19, Definition 4.1]: a subset $G_0 \subset G$ of a finite abelian group is called an LCN-set if

$\mathsf{k}(A) \ge 1$ for each $A \in \mathcal{A}(G_0)$. Moreover,

$$\mathsf{m}(G) = \max\{\min \Delta(G_0) \colon G_0 \subset G \text{ an LCN-set}, \ \Delta(G_0) \ne \emptyset\}, \tag{3}$$

with the convention that $\max \emptyset = 0$.

The aim of this section is to prove the following two results on $\Delta^*(G)$ that we need in Section 4 and are of some independent interest as well.

Theorem 3.1. *Let G be a finite abelian group with $|G| \ge 3$. Then*

$$\max \Delta^*(G) \le \max\{\exp(G) - 2, \mathsf{r}^*(G) - 1, \mathsf{K}(G) - 1\}.$$

In particular, if G is a p-group, then

$$\max \Delta^*(G) = \max\{\exp(G) - 2, \mathsf{r}(G) - 1\}.$$

In combination with (2), one obtains more explicit upper bounds on $\max \Delta^*(G)$.

Theorem 3.2. *Let G be a finite abelian group of exponent n and let $r \in \mathbb{N}$ be maximal such that G has a subgroup isomorphic to C_n^r. Then*

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

Thus, we have precise information on the large elements in $\Delta^*(G)$ provided $\exp(G)$ is large relative to $\mathsf{m}(G)$ (cf. (5) for the relevance of this result); using the upper bounds on $\mathsf{m}(G)$ to be established in Proposition 3.6 the result can be made more explicit, see below.

Next, we briefly recall some results that be need in the proofs of these two results (see [11, Section 6.8] for a detailed discussion). The first part of the following lemma is classical and was obtained by L. Skula and A. Zaks, the remaining parts are due to W. D. Gao and A. Geroldinger (see [9, 6] and also [11, Section 6.8]).

Lemma 3.3. *Let G be a finite abelian group and $G_0 \subset G$.*

1. *$\Delta(G_0) \ne \emptyset$ if and only if there exists some $A \in \mathcal{A}(G_0)$ with $\mathsf{k}(A) \ne 1$.*
2. *If $\Delta(G_0) \ne \emptyset$, then $\min \Delta(G_0) = \gcd \Delta(G_0)$.*
3. *If $G_1 \subset G_0$ and $\Delta(G_1) \ne \emptyset$, then $\Delta(G_1) \subset \Delta(G_0)$ and thus $\min \Delta(G_1) \mid \min \Delta(G_0)$.*
4. *If $\Delta(G_0) \ne \emptyset$, then $\min \Delta(G_0) \mid \exp(G)(\mathsf{k}(A) - 1)$ for each $A \in \mathcal{A}(G_0)$. In particular, if there exists some $A \in \mathcal{A}(G_0)$ with $\mathsf{k}(A) < 1$, then $\min \Delta(G_0) \le \exp(G) - 2$. Moreover, if $\max \Delta^*(G) \ne \emptyset$, then $\max \Delta^*(G) \le \max\{\exp(G) - 2, \mathsf{m}(G)\}$.*
5. *If G_0 is an LCN-set and $\Delta(G_0) \ne \emptyset$, then $\min \Delta(G_0) \le |G_0| - 2$.*

Constructions yielding the following result are given in [6, 12, 18, 19].

Lemma 3.4. *Let $n, r \in \mathbb{N}$. Then $[1, r-1] \cup [\max\{1, n-r-1\}, n-2] \subset \Delta^*(C_n^r)$, and if $n \ge 4$, then $\lfloor n/2 \rfloor - 1 \in \Delta^*(C_n^r)$. Moreover, $\mathsf{m}(C_n^r) \ge r - 1$.*

The following result was obtained in [18, Lemma 3.5, Corollary 3.1].

Lemma 3.5. *Let $G_0 \subset G$ with $\Delta(G_0) \neq \emptyset$. Suppose the following conditions are fulfilled:*

- *there exists some $g \in G_0$ such that $\Delta(G_0 \setminus \{g\}) = \emptyset$, and*
- *for some $U \in \mathcal{A}(G_0)$, $\mathsf{k}(U) = 1$ and $\gcd\{\mathsf{v}_g(U), \operatorname{ord} g\} = 1$.*

Then $\mathsf{k}(\mathcal{A}(G_0)) \subset \mathbb{N}$ and

$$\min \Delta(G_0) \mid \gcd\{\mathsf{k}(A) - 1 \colon A \in \mathcal{A}(G_0)\}.$$

In particular, the conditions hold if $\Delta(G_1) = \emptyset$ for each $G_1 \subsetneq G_0$ and there exists some $G_2 \subset G_0$ such that $\langle G_2 \rangle = \langle G_0 \rangle$ and $|G_2| \leq |G_0| - 2$.

The following proposition, in combination with the results recalled above, yields a proof of Theorem 3.1.

Proposition 3.6. *Let G be a finite abelian group. Then*

$$\mathsf{m}(G) \leq \max\{\mathsf{r}^*(G) - 1, \mathsf{K}(G) - 1\}.$$

In particular, if G is a p-group, then $\mathsf{m}(G) = \mathsf{r}(G) - 1$.

Proof. If G is a p-group, then $\mathsf{K}(G) \leq \mathsf{r}^*(G)$ (cf. the remark after (1)) and $\mathsf{r}^*(G) = \mathsf{r}(G)$. Consequently, the "in particular"-part follows directly from the general upper bound for $\max \Delta^*(G)$ and Lemma 3.4.

Let $G_0 \subset G$ be an LCN-set with $\Delta(G_0) \neq \emptyset$. We have to show that $\min \Delta(G_0) \leq \max\{\mathsf{r}^*(G) - 1, \mathsf{K}(G) - 1\}$. Since we seek an upper bound for $\min \Delta(G_0)$ and clearly a subset of an LCN-set is again an LCN-set, we may assume by Lemma 3.3 that for each $G_1 \subsetneq G_0$, $\Delta(G_1) = \emptyset$.

By Lemma 3.3 we know that $\min \Delta(G_0) \leq |G_0| - 2$. We suppose $|G_0| \geq \mathsf{r}^*(G) + 2$, since otherwise our claim follows. Let $H_0 \subset G_0$ be a minimal generating set for $\langle G_0 \rangle$. Since $\mathsf{r}^*(\langle G_0 \rangle) \leq \mathsf{r}^*(G)$, we have by Lemma 2.1 $|G_0 \setminus H_0| \geq 2$. Thus, by Lemma 3.5 $\min \Delta(G_0) \mid \gcd\{\mathsf{k}(A) - 1 \colon A \in \mathcal{A}(G_0)\} \leq \mathsf{K}(G) - 1$. □

Theorem 3.1 now obviously follows.

Proof of Theorem 3.1. The general result follows by Lemma 3.3 and Proposition 3.6. As in the proof of Proposition 3.6, the "in particular"-part follows by the general result, Lemma 3.4, and the result on $\mathsf{K}(G)$ recalled after (1). □

We proceed with the proof of Theorem 3.2.

Proof of Theorem 3.2. Let $G_0 \subset G$ such that $\Delta(G_0) \neq \emptyset$. We have to show that $\min \Delta(G_0) \in [\max\{1, n - r - 1\}, n - 2]$ or $\min \Delta(G_0) \leq \max\{\mathsf{m}(G), \lfloor n/2 \rfloor - 1\}$. By Lemma 3.3 we may assume that $\Delta(G_1) = \emptyset$ for each $G_1 \subsetneq G_0$, since each proper divisor of an element of $[\max\{1, n - r - 1\}, n - 2]$ is not greater than $\lfloor n/2 \rfloor - 1$.

Let $A \in \mathcal{A}(G_0)$ with minimal cross number. If $\mathsf{k}(A) \geq 1$, then (by definition) $\min \Delta(G_0) \leq \mathsf{m}(G)$. Thus, we may assume that $\mathsf{k}(A) < 1$. We note that $\operatorname{supp}(A) = G_0$. Let $\ell = \min\{\lceil \operatorname{ord} g / \mathsf{v}_g(A) \rceil \colon g \in G_0\}$ and let $h \in G_0$ be an element that attains the minimum. Note that

$\ell \ge 2$. Let $B = A^\ell$. Obviously, $\ell \in \mathsf{L}(B)$. We note that $h^{\operatorname{ord} h} \mid B$. Let $R = h^{-\operatorname{ord} h}B$. Since $|G_0| \ne 1$, clearly $R \ne 1$. Since $\mathsf{k}(A)$ is minimal, it follows that $\max \mathsf{L}(R) \le \mathsf{k}(R)/\mathsf{k}(A) = (\ell\,\mathsf{k}(A) - 1)/\mathsf{k}(A) = \ell - \mathsf{k}(A)^{-1} < \ell - 1$. Furthermore, since $1 + \max \mathsf{L}(R) \in \mathsf{L}(B)$ and $1 + \max \mathsf{L}(R) < \ell$, it follows that $\min \Delta(G_0) \le \ell - (1 + \max \mathsf{L}(R)) \le \ell - 2$.

Thus, we may assume that $\ell = n$, i.e., $\operatorname{ord} g = n$ and $\mathsf{v}_g(A) = 1$ for each $g \in G_0$, since otherwise $\ell - 2 \le \lfloor n/2 \rfloor - 1$. Consequently, $|G_0| = |A|$ and $\mathsf{k}(A) = |A|/n$; in particular, $|A| < n$.

Considering the block $A^n = \prod_{g \in G_0} g^n$, we get $\{|A|, n\} \subset \mathsf{L}(A^n)$ and thus by Lemma 3.3 $\min \Delta(G_0) \mid (n - |A|)$.

First, we assume that $G_1 = G_0 \setminus \{h\}$ is not independent. We assert that $\min \Delta(G_0) \le \lfloor n/2 \rfloor - 1$. Since G_1 is not independent, there exists some $h_1 \in G_1$ and some $m \in \mathbb{N}$ such that $mh_1 \in \langle G_1 \setminus \{h_1\} \rangle \setminus \{0\}$; suppose m is minimal with this property. Then $m \mid n$ and clearly $m \ne n$. Moreover, there exists some $U \in \mathcal{A}(G_1)$ such that $\mathsf{v}_{h_1}(U) = m$. Since $\Delta(G_1) = \emptyset$, by Lemma 3.3 $\mathsf{k}(U) = 1$. By Lemma 3.5 we know, since $\mathsf{k}(A) < 1$, that $\gcd\{\mathsf{v}_{h_1}(A), n\} \ne 1$ and thus $m \ne 1$. We now consider the block $C = A^{n-m}U$. On the one hand, we have $1 + n - m \in \mathsf{L}(C)$. On the other hand, we have $\mathsf{v}_{h_1}(C) = n$, that is, $C = h_1^n T$ with $T \in \mathcal{B}(G_0 \setminus \{h_1\})$. Consequently, $\mathsf{L}(T) = \{\mathsf{k}(T)\}$ and, since $\mathsf{k}(T) = (n - m)\frac{|A|}{n} + 1 - 1$, it follows that $1 + (n - m)\frac{|A|}{n} \in \mathsf{L}(C)$. Thus, $\min \Delta(G_0) \mid (n - m)(1 - \frac{|A|}{n}) = (n - |A|) - m(1 - \frac{|A|}{n})$. Since $\min \Delta(G_0) \mid (n - |A|)$, we have $\min \Delta(G_0) \mid m(1 - \frac{|A|}{n})$. Consequently, since $m \le n/2$, $\min \Delta(G_0) \le (n - |A|)/2 \le n/2 - 1$, implying the claim.

Second, we assume that $G_1 = G_0 \setminus \{h\}$ is independent. This implies $|A| - 1 = |G_1| \le r$ and $n - r - 1 \le n - |A| \le n - 2$. Since $n - |A| > 0$, the claim follows. □

The following result generalizes [19, Lemma 6.2] and is applied in Section 4.

Corollary 3.7. *Let G be a finite abelian group of exponent n, and let $d \in \mathbb{N}$ such that $d > \max\{\mathsf{m}(G), \lfloor n/2 \rfloor - 1\}$. Then $d \in \Delta^*(G)$ if and only if G has a subgroup isomorphic to C_n^{n-d-1}.*

Proof. The "if"-part is clear by Lemma 3.4 and the "only if"-part by the proof of Theorem 3.2. □

A. Geroldinger and Y. ould Hamidoune [12] proved $\max(\Delta^*(C_n) \setminus \{n-2\}) = \lfloor n/2 \rfloor - 1$. We obtain an analogous result for C_n^2, which in combination with Corollary 3.7 yields the result on cyclic groups as well.

Corollary 3.8. *Let $n \in \mathbb{N}$ with $n \ge 5$. Then $\max(\Delta^*(C_n^2) \setminus \{n-3, n-2\}) = \lfloor n/2 \rfloor - 1$.*

Proof. By Lemma 3.4 and Theorem 3.2, it remains to show $\mathsf{m}(C_n^2) \le \lfloor n/2 \rfloor - 1$.

By Proposition 3.6 we know that $\mathsf{m}(C_n^2) \le \max\{\mathsf{r}^*(C_n^2) - 1, \mathsf{K}(C_n^2) - 1\}$. We observe, using the trivial estimate $\mathsf{r}^*(C_n^2) \le \log_2 |C_n^2|$ and direct inspection for $n \le 15$, that $\mathsf{r}^*(C_n^2) \le \lfloor n/2 \rfloor$ for $n \ne 6$. And, using (2) and the results mentioned after (1) we get that $\mathsf{K}(C_n^2) < \lfloor n/2 \rfloor + 1$ for $n \ne 6$. Thus, the claim is proved for $n \ne 6$. Yet, in [19, Lemma 4.6] it is proved that $\mathsf{m}(C_6^2) \le 2$, completing the argument. □

As is apparent from the proof, results analogous to Corollary 3.8 can be obtained for each finite abelian group G for which $\exp(G)$ is sufficiently large relative to $|G|$.

4. Main result

In this section we proof our main result. As mentioned in the introduction $\mathcal{L}(C_2^2) = \mathcal{L}(C_3)$, thus the condition $n \ge 3$ below is necessary.

Theorem 4.1. *Let $n \in \mathbb{N}$ with $n \ge 3$ and let G be a finite abelian group with $\mathcal{L}(C_n^2) = \mathcal{L}(G)$. Then $C_n^2 \cong G$.*

We recall some more definitions and results that we need in order to prove this result. The invariants $\rho_k(G)$ are defined in the following way (see [11, Section 6.3] and [3] for a detailed account and [8] for recent results). Let G be a finite abelian group. For $k \in \mathbb{N}$, let

$$\rho_k(G) = \max\{\max L \colon L \in \mathcal{L}(G),\ k \in L\}.$$

It is known that, for $|G| \ne 2$, $\rho_{2k}(G) = k\,\mathsf{D}(G)$. Thus, if G' is another finite abelian group with $\mathcal{L}(G) = \mathcal{L}(G')$, then $\rho_k(G) = \rho_k(G')$ for each $k \in \mathbb{N}$ and consequently,

$$\text{if } |G| \ge 3, \text{ then } \mathsf{D}(G) = \mathsf{D}(G'). \tag{4}$$

The set $\Delta_1(G)$ is defined as the set of all $d \in \mathbb{N}$ such that the following holds:

for each $k \in \mathbb{N}$ there exists some $L \in \mathcal{L}(G)$ such that,
for some $y \in \mathbb{N}_0$, $\{y + di \colon i \in [0, k]\} \subset L \subset y + d\mathbb{Z}$.

Again, if $\mathcal{L}(G) = \mathcal{L}(G')$, then $\Delta_1(G) = \Delta_1(G')$. Since it is known (see [6, Proposition 5.1] also see [11, Corollary 4.3.16]) that $\Delta^*(G) \subset \Delta_1(G)$ and that for each $d \in \Delta_1(G)$ there exists some $d' \in \Delta^*(G)$ such that $d \mid d'$, it follows that

$$\{d \in \Delta^*(G) \colon d > \frac{\max \Delta^*(G)}{2}\} = \{d \in \Delta^*(G') \colon d > \frac{\max \Delta^*(G')}{2}\}. \tag{5}$$

In the following auxiliary result we investigate groups for which the relation of the constants $\mathsf{D}(G)$ and $\max \Delta^*(G)$ is equal to that for C_n^2, but opposed to $\mathsf{m}(C_n^2)$ the invariant $\mathsf{m}(G)$ is large.

Proposition 4.2. *Let G be a finite abelian group with $|G| \ge 3$ such that $\mathsf{D}(G) = 2\max\Delta^*(G) + 3$ and $\mathsf{m}(G) \ge \max\Delta^*(G) - \delta$ for some $\delta \in \mathbb{N}_0$.*

(1) *If $\mathsf{m}(G) \le \mathsf{K}(G) - 1$, then $\mathsf{r}(G) \ge \mathsf{D}(G) - 4(1+2\delta)$.*
(2) *If $\mathsf{m}(G) \le \mathsf{r}^*(G) - 1$, then $\mathsf{r}(G) \ge (\mathsf{D}(G) - 1 - 4\delta)/3$.*

Clearly this result is trivial for large δ; in fact, we apply it for $\delta = 0$ and $\delta = 1$ only. In the proof of this proposition we need the following lower bound for $\mathsf{D}(G)$, which follows quite directly from (1).

Lemma 4.3. *Let $|G| \ge 2$. Then $\mathsf{D}(G) \ge 4\,\mathsf{r}^*(G) - 3\,\mathsf{r}(G) + 1$.*

Proof. Let $G = \oplus_{i=1}^r C_{n_i}$ where $1 < n_1 \mid \cdots \mid n_r$. Further let $n_i = \prod_{j=1}^{s_i} q_j^{(i)}$ the factorization of n_i into, pairwise relatively prime, prime powers. Then $r = \mathsf{r}(G)$ and $\mathsf{r}^*(G) = \sum_{i=1}^r s_i$. By (1) we know that $\mathsf{D}(G) \ge 1 + \sum_{i=1}^r (n_i - 1)$. Thus, it suffices to prove that $\sum_{i=1}^r n_i \ge 4\,\mathsf{r}^*(G) - 2\,\mathsf{r}(G)$. Since $n_i \ge 4s_i - 2$ for each i (note that if $s_i = 2$ then $n_i \ge 6$), the above inequality follows by summing these inequalities. □

Proof of Proposition 4.2. We have

$$\mathsf{m}(G) \ge (\mathsf{D}(G) - 3 - 2\delta)/2. \tag{6}$$

1. Suppose that $\mathsf{m}(G) \le \mathsf{K}(G) - 1$. Combining this with (6) we get

$$2\,\mathsf{K}(G) + 1 + 2\delta \ge \mathsf{D}(G).$$

Let $A = \prod_{i=1}^{\ell} g_i \in \mathcal{A}(G)$ with $\mathsf{k}(A) = \mathsf{K}(G)$. We may assume that $0 \nmid A$. Since $\mathsf{D}(G) \ge \ell$ we get

$$1 + 2\delta \ge \ell - 2\,\mathsf{k}(A) = \sum_{i=1}^{\ell} \frac{\operatorname{ord} g_i - 2}{\operatorname{ord} g_i}.$$

Thus, at least $\ell - 3(1+2\delta)$ of the g_is have order 2. These $\ell - 3(1+2\delta)$ elements are independent, since otherwise A would have a proper and non-trivial zero-sum subsequence. Consequently, $\mathsf{r}_2(G) \ge \ell - 3(1+2\delta)$ and

$$\mathsf{r}(G) \ge \ell - 3(1+2\delta) \ge 2\,\mathsf{k}(A) - 3(1+2\delta) \ge \mathsf{D}(G) - 4(1+2\delta).$$

2. Suppose that $\mathsf{m}(G) \le \mathsf{r}^*(G) - 1$. Using Lemma 4.3 and (6) we get

$$\mathsf{r}^*(G) - 1 \ge \frac{4\,\mathsf{r}^*(G) - 3\,\mathsf{r}(G) - 2(1+\delta)}{2}.$$

Thus $3\,\mathsf{r}(G)/2 \ge \mathsf{r}^*(G) - \delta$, which together with (6) implies the result. □

Now, we prove Theorem 4.1. If n is small, additional considerations are needed; for clarity, these are separated from the general argument and given in Lemma 4.4.

Proof of Theorem 4.1, general case. We assume $n \geq 13$ or $n = 11$. By the discussion after (1) and (4) we know that $\mathsf{D}(G) = \mathsf{D}(C_n^2) = 2n-1$. Moreover, by (5) and Corollary 3.7 we know that $\max \Delta^*(G) = \max \Delta^*(C_n^2) = n-2$ and $n-3 \in \Delta^*(C_n^2)$ as well as $n-3 \in \Delta^*(G)$.

By Lemma 3.3, we know that $\max \Delta^*(G) = \max\{\exp(G)-2, \mathsf{m}(G)\}$. If $\mathsf{m}(G) < \exp(G)-3$, then we know by Corollary 3.7 that $\exp(G)-3 \in \Delta^*(G)$ if and only if G has a subgroup isomorphic to $C_{\exp(G)}^2$. Since $\mathsf{D}(G) = \mathsf{D}(C_n^2)$, we get $G \cong C_n^2$.

Thus, we assume $\mathsf{m}(G) \geq \exp(G) - 3$. Then we have $\mathsf{m}(G) \geq \max \Delta^*(G)-1$. Since $\mathsf{D}(G) = 2\max\Delta^*(G)+3$ and since by Proposition 3.6 $\mathsf{m}(G) \leq \max\{\mathsf{K}(G)-1, \mathsf{r}^*(G)-1\}$, at least one of the conditions in Proposition 4.2 is fulfilled. Therefore, $\mathsf{r}(G) \geq \min\{\mathsf{D}(G)-12, (\mathsf{D}(G)-5)/3\} = 2n/3-2$. Thus, by Lemma 3.4 we have $\lceil 2n/3-2 \rceil - 1 \in \Delta^*(G)$. A contradiction to (5), since by Corollary 3.8 this element is not contained in $\Delta^*(C_n^2)$. □

To complete the proof of Theorem 4.1 it remains to consider $n \in [3, 10]$ and $n = 12$. We recall that for $n = 3$ and $n = 4$, since the Davenport constant of C_n^2 equals 5 and 7, respectively, the result is known (see [9, Satz 4] and cf. the discussion in the introduction). Moreover, by (4) and (1) this problem readily reduces to distinguishing the systems of sets of lengths of finitely many groups. As far as possible, we settle this problem using the methods recalled and developed in this paper. It turns out that they are sufficient, yet need to be applied somewhat differently than in the general case, except for $n = 5$ and $n = 6$. In these two cases, we use results on the structure of certain "long" sets of lengths. To avoid a too long argument for these special cases, we present them in a rather ad-hoc way; for a general discussion of this method see Section 8 of the forthcoming paper [20].

Lemma 4.4. *Let $n \in [5, 10]$ or $n = 12$. Let G be a finite abelian group such that $\mathcal{L}(C_n^2) = \mathcal{L}(G)$. Then $C_n^2 \cong G$.*

Proof. As in the general part of the proof of Theorem 4.1, we have $\mathsf{D}(G) = \mathsf{D}(C_n^2) = 2n-1$, $\max \Delta^*(G) = \max \Delta^*(C_n^2) = n-2$, and $n-3 \in \Delta^*(C_n^2)$ as well as $n-3 \in \Delta^*(G)$. By Lemma 3.4 this implies $\exp(G) \leq n$ and $\mathsf{r}(G) \leq n-1$.

1. Suppose $n = 5$. If $\exp(G) = 5$, then $G \cong C_5^2$. Thus, we assume $\exp(G) \leq 4$. It follows that G is isomorphic to C_3^4 or to $C_4^2 \oplus C_2^2$. Yet, by [18, Theorem 5.1], we know that $\mathcal{L}(C_3^4) \neq \mathcal{L}(C_5^2)$. Thus, it remains to consider the case $G \cong C_4^2 \oplus C_2^2$. We observe that if $g \in G$ with $\operatorname{ord} g = 4$, then $\mathsf{L}(((-g)g)^{4k}) = \{2k + 2i \colon i \in [0, k]\}$ for each $k \in \mathbb{N}$.

We show that for sufficiently large k this set is not contained in $\mathcal{L}(C_5^2)$ and thus $\mathcal{L}(C_5^2) \neq \mathcal{L}(C_4^2 \oplus C_2^2)$, a contradiction. Suppose that $B_k \in \mathcal{B}(C_5^2)$ such that $\mathsf{L}(B_k) = \{2k + 2i \colon i \in [0, k]\}$. By [11, Theorem 9.4.10] it follows that $B_k = B_k' B_k''$ with zero-sum sequences $B_k' B_k''$ where $2 \mid \min \Delta(\operatorname{supp}(B_k''))$ and the length of B_k' is bounded by a constant just depending on C_5^2, namely by $\mathsf{b}_{\{0,2\}}(C_5^2) + \mathsf{D}(C_5^2) - 1$. By [19, Lemma 6.3] we have $\operatorname{supp}(B_k'') \subset \{0, e_1, e_2, -e_1 - e_2)\}$ for independent elements e_1, e_2. By [11, Proposition 4.3.4.1] and since $\mathcal{B}(C_5^2)$ is tame and $|B_k'|$ is bounded, there exists some constant C, independent of k, such that $\max \mathsf{L}(B_k) - \min \mathsf{L}(B_k) \le \max \mathsf{L}(B_k'') - \min \mathsf{L}(B_k'') + C$ and $\min \mathsf{L}(B_k'') \le \min \mathsf{L}(B_k) + C$. Since the only minimal non-trivial relation in $\mathcal{B}(\{0, e_1, e_2, -(e_1 + e_2)\})$ is given by $((-e_1 - e_2)e_1e_2)^5 = (-e_1-e_2)^5 e_1^5 e_2^5$, it follows that $\max \mathsf{L}(B_k'') - \min \mathsf{L}(B_k'') \le \frac{2}{3} \min \mathsf{L}(B_k'') \le \frac{2}{3}(\min \mathsf{L}(B_k) + C)$. Yet, $\max \mathsf{L}(B_k) - \min \mathsf{L}(B_k) = \min \mathsf{L}(B_k)$ and thus $2k = \min \mathsf{L}(B_k) \le \frac{2}{3}(\min \mathsf{L}(B_k)+C)+C = \frac{2}{3}(2k+C)+C$. Consequently $k \le \frac{5}{2}C$ and the claim follows.

2. Suppose $n = 6$. Clearly $\exp(G) \notin \{2, 5\}$ and moreover $\exp(G) \ne 4$, since $\max \Delta^*(C_4^3 \oplus C_2) = 3$ by Theorem 3.1. It follows that G is isomorphic to C_3^5, $C_6 \oplus C_2^4$, or C_6^2. Note that $\mathsf{D}(C_6 \oplus C_2^4) > 10$ and thus $\mathsf{D}(C_6 \oplus C_2^5) > 11$ and $\mathsf{D}(C_6 \oplus C_3^2) = 10$ (see the discussion after (1)).

First, suppose $G \cong C_6 \oplus C_2^4$. We proceed almost as in the case $n = 5$. Let $f_1, \ldots, f_4 \in G$ be independent elements of order 2 and $f_0 = \sum_{i=1}^4 e_i$. Further, for each $k \in \mathbb{N}$, let $C_k = (\prod_{i=0}^4 f_i)^{2k}$. Then $\mathsf{L}(C_k) = \{2k + 3i \colon i \in [0, k]\}$. We claim that for sufficiently large k this set is not contained in $\mathcal{L}(C_6^2)$ and thus $\mathcal{L}(C_6^2) \ne \mathcal{L}(G)$, a contradiction. Suppose that $B_k \in \mathcal{B}(C_6^2)$ such that $\mathsf{L}(B_k) = \{2k + 3i \colon i \in [0, k]\}$. Again, it follows that $B_k = B_k' B_k''$ with zero-sum sequences $B_k' B_k''$ where $3 \mid \min \Delta(\operatorname{supp}(B_k''))$ and the length of B_k' is bounded by a constant just depending on C_6^2. Again, we have $\operatorname{supp}(B_k'') \subset \{0, e_1, e_2, -e_1 - e_2)\}$ for independent elements e_1, e_2 of order 6 and there exists some constant C, independent of k, such that $\max \mathsf{L}(B_k) - \min \mathsf{L}(B_k) \le \max \mathsf{L}(B_k'') - \min \mathsf{L}(B_k'') + C$ and $\min \mathsf{L}(B_k'') \le \min \mathsf{L}(B_k) + C$. The only minimal non-trivial relation in $\mathcal{B}(\{0, e_1, e_2, -(e_1 + e_2)\})$ is given by $((-e_1 - e_2)e_1e_2)^6 = (-e_1 - e_2)^6 e_1^6 e_2^6$ and thus $\max \mathsf{L}(B_k'') - \min \mathsf{L}(B_k'') \le \min \mathsf{L}(B_k'') \le \min \mathsf{L}(B_k) + C$. Yet, $\max \mathsf{L}(B_k) - \min \mathsf{L}(B_k) = \frac{3}{2} \min \mathsf{L}(B_k)$ and thus $3k = \frac{3}{2} \min \mathsf{L}(B_k) \le (\min \mathsf{L}(B_k) + C) + C = (2k + C) + C$. Consequently $k \le 2C$ and the claim follows.

Second, suppose $G \cong C_3^5$. The argument is similar to the one above. Let $f_1, \ldots, f_5 \in G$ be independent elements and $f_0 = \sum_{i=1}^5 f_i$. Further, for each $k \in \mathbb{N}$, let $C_k = (f_0 \prod_{i=1}^5 f_i^2)^{3k}$. Then $\mathsf{L}(C_k) = \{3k + 4i \colon i \in [0, 2k]\}$.

Again, we claim that for sufficiently large k this set is not contained in $\mathcal{L}(C_6^2)$. Suppose that $B_k \in \mathcal{B}(C_6^2)$ such that $\mathsf{L}(B_k) = \{3k + 4i \colon i \in [0, 2k]\}$. We have $B_k = B_k' B_k''$ with zero-sum sequences $B_k' B_k''$ where $4 \mid \min \Delta(\operatorname{supp}(B_k''))$ and the length of B_k' is bounded by a constant just depending on C_6^2. By [19, Corollary 5.2] we have $\operatorname{supp}(B_k'') \subset \{0, e_1, -e_1, e_2, -e_2\}$ or $\operatorname{supp}(B_k'') \subset \{0, e_1, -e_1, e_2, 2e_2, 3e_2\}$ for independent elements $e_1, e_2 \in C_6^2$ of order 6. Again, there exists some constant C, independent of k, such that $\max \mathsf{L}(B_k) - \min \mathsf{L}(B_k) \le$

$\max \mathsf{L}(B''_k) - \min \mathsf{L}(B''_k) + C$ and $\min \mathsf{L}(B''_k) \le \min \mathsf{L}(B_k) + C$. The only minimal relations yielding factorizations of distinct lengths are $(-e_i)^6 e_i^6 = ((-e_i)e_i)^6$. Thus, it follows that $\max \mathsf{L}(B''_k) - \min \mathsf{L}(B''_k) \le 2 \min \mathsf{L}(B''_k) \le 2(\min \mathsf{L}(B_k) + C)$. Yet, $\max \mathsf{L}(B_k) - \min \mathsf{L}(B_k) = \frac{8}{3} \min \mathsf{L}(B_k)$ and thus $8k = \frac{8}{3} \min \mathsf{L}(B_k) \le 2(\min \mathsf{L}(B_k) + C) + C = 2(3k + C) + C$. Consequently $k \le \frac{3}{2} C$ and the claim follows.
3. Suppose $n = 7$. If $\exp(G) = 7$, then $G \cong C_7^2$. We assume $\exp(G) \le 6$. Since $3 \notin \Delta^*(C_7^2)$ (see Corollary 3.8), we have $\mathsf{r}(G) \le 3$ (cf. Lemma 3.4). Consequently, G is isomorphic to C_5^3 or to a proper subgroup of C_6^3. However, for these groups we know by Theorem 3.1, in the latter case using (2), that $\max \Delta^*(G) \le 4$.
4. Suppose $n = 8$. As above, we have $4 \notin \Delta^*(G)$ and $\mathsf{r}(G) \le 4$. If $\exp(G) < 8$, then $\mathsf{m}(G) = \max \Delta^*(G)$ and by Proposition 4.2 we have $\mathsf{r}(G) \ge \min\{11, 14/3\}$, a contradiction. Thus, we have $\exp(G) = 8$ and by Proposition 3.6 $\mathsf{m}(G) = \mathsf{r}(G) - 1 \le 3 < \max \Delta^*(G) - 1$. Thus, by Corollary 3.7 and since $\mathsf{D}(G) = \mathsf{D}(C_8^2)$, we have $G \cong C_8^2$.
5. Suppose $n = 9$. As above, we have $4 \notin \Delta^*(G)$ and $\mathsf{r}(G) \le 4$. Since $\exp(G) < 9$, implies $\mathsf{r}(G) \ge \min\{13, 16/3\}$, we have $\exp(G) = 9$. As above, it follows that $\mathsf{m}(G) \le 3$, implying $G \cong C_9^2$.
6. Suppose $n = 10$. As above, $\mathsf{r}(G) \le 5$ and $\exp(G) = 10$. By Proposition 3.6 and (2) $\mathsf{m}(C_{10} \oplus C_5^2) < 7$, and $\mathsf{m}(C_{10} \oplus C_2^k) \ge 7$ implies $k \ge 6$ and $5 \in \Delta^*(C_{10} \oplus C_2^k)$. Thus, $G \cong C_{10}^2$.
7. Suppose $n = 12$. As above, $\mathsf{r}(G) \le 6$ and $\exp(G) = 12$. We get that $\mathsf{m}(C_{12} \oplus C_6^2 \oplus C_2)$, $\mathsf{m}(C_{12} \oplus C_6 \oplus C_3^3)$, and $\mathsf{m}(C_{12} \oplus C_3^5)$ are each less than 9. Moreover, $\mathsf{m}(C_{12} \oplus C_6 \oplus C_2^k) \ge 9$ and $\mathsf{m}(C_{12} \oplus C_2^k) \ge 9$ implies $k \ge 6$ and $k \ge 8$, respectively; and the rank of such a group is thus at least 8. Therefore, $G \cong C_{12}^2$. □

Proof of Theorem 4.1, summary. The case $n \ge 13$ and $n = 11$ is considered in the "general case." For $n \le 4$ the result is known by [9, Satz 4], and for $n \in [5, 10]$ and $n = 12$ the result is obtained in Lemma 4.4. □

Acknowledgement

The author would like to thank the referee for a careful reading of the manuscript and suggestions.

References

[1] L. Carlitz. A characterization of algebraic number fields with class number two. *Proc. Amer. Math. Soc.*, 11:391–392, 1960.
[2] S. Chapman and A. Geroldinger. Krull domains and monoids, their sets of lengths, and associated combinatorial problems. In *Factorization in integral domains (Iowa City, IA, 1996)*, volume 189 of *Lecture Notes in Pure and Appl. Math.*, pages 73–112. Dekker, New York, 1997.
[3] S. T. Chapman, M. Freeze, and W. W. Smith. On generalized lengths of factorizations in Dedekind and Krull domains. In *Non-Noetherian commutative*

ring theory, volume 520 of *Math. Appl.*, pages 117–137. Kluwer Acad. Publ., Dordrecht, 2000.

[4] S. T. Chapman and W. W. Smith. An arithmetical characterization of finite elementary 2-groups. *Comm. Algebra*, 29(3):1249–1257, 2001.

[5] P. van Emde Boas. A combinatorial problem on finite Abelian groups. II. Technical report, Math. Centrum, Amsterdam, Afd. Zuivere Wisk. ZW 1969-007, 60 p. , 1969.

[6] W. Gao and A. Geroldinger. Systems of sets of lengths. II. *Abh. Math. Sem. Univ. Hamburg*, 70:31–49, 2000.

[7] W. Gao and A. Geroldinger. Zero-sum problems in finite abelian groups: a survey. *Expo. Math.*, 24:337–369, 2006.

[8] W. D. Gao and A. Geroldinger. On products of k atoms. *Monatsh. Math.*, to appear.

[9] A. Geroldinger. Systeme von Längenmengen. *Abh. Math. Sem. Univ. Hamburg*, 60:115–130, 1990.

[10] A. Geroldinger and R. Göbel. Half-factorial subsets in infinite abelian groups. *Houston J. Math.*, 29(4):841–858, 2003.

[11] A. Geroldinger and F. Halter-Koch. *Non-unique factorizations. Algebraic, Combinatorial and Analytic Theory.* Chapman & Hall/CRC, 2006.

[12] A. Geroldinger and Y. ould Hamidoune. Zero-sumfree sequences in cyclic groups and some arithmetical application. *J. Théor. Nombres Bordeaux*, 14(1):221–239, 2002.

[13] B. Girard. A new upper bound for the cross number of finite abelian groups. *Israel J. Math.*, to appear.

[14] J. Kaczorowski. A pure arithmetical definition of the class group. *Colloq. Math.*, 48(2):265–267, 1984.

[15] F. Kainrath. Factorization in Krull monoids with infinite class group. *Colloq. Math.*, 80(1):23–30, 1999.

[16] W. Narkiewicz. *Elementary and analytic theory of algebraic numbers.* Springer Monographs in Mathematics. Springer-Verlag, Berlin, third edition, 2004.

[17] D. E. Rush. An arithmetic characterization of algebraic number fields with a given class group. *Math. Proc. Cambridge Philos. Soc.*, 94(1):23–28, 1983.

[18] W. A. Schmid. Differences in sets of lengths of Krull monoids with finite class group. *J. Théor. Nombres Bordeaux*, 17(1):323–345, 2005.

[19] W. A. Schmid. Periods of sets of lengths: a quantitative result and an associated inverse problem. *Colloq. Math.*, 113(1):33–53, 2008.

[20] W. A. Schmid. Characterization of class groups of Krull monoids via their systems of sets of lengths: a status report, *HRI proceedings*, to appear.

Institut für Mathematik und Wissenschaftliches Rechnen, Karl-Franzens-Universität, Heinrichstrasse 36, 8010 Graz, Austria

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