Krull domains and monoids, their sets of lengths and associated combinatorial problems

Scott Chapman, Trinity University, Department of Mathematics, San Antonio, Texas 78212-7200

Alfred Geroldinger, Institut für Mathematik, Karl-Franzens-Universität, 8010 Graz, Austria

1. INTRODUCTION

This is a survey article on the theory of non-unique factorization. This field has its origins in algebraic number theory. Today, problems involving the factorization of elements into irreducibles are studied in general integral domains using a huge variety of techniques (see [A-A-Z1], [A-A-Z2] and [A-A-Z3]). In this paper, we consider factorization properties of Krull domains, including integrally closed noetherian domains and rings of integers in algebraic number fields. We restrict our interest to sets of lengths and the invariants derived from them. Our results are valid mainly for Krull domains with finite divisor class group.

Although our emphasis and the main applications of the theory of non-unique factorization lies in ring theory, this paper is written in the language of monoids. The reason for this is not for higher

generality, but usefulness and simplicity. We start in chapter 2 with Krull monoids by discussing their sets of lengths and various constants which control these sets. We gather in this chapter many results which have appeared in the literature using different notation and terminology. In chapter 3, we study block monoids. These are suitably constructed monoids which provide the opportunity to understand and describe more clearly the invariants which have been previously introduced. Having these monoids at our disposal, we can reduce ring theoretical problems to problems in finitely generated monoids and are able to apply geometrical methods. There is another striking example of the usefulness of this approach. Results for Krull monoids can be applied to investigate one-dimensional noetherian domains R which are not integrally closed, but have non-zero conductor $\mathrm{Ann}_R(\overline{R}/R)$. In chapter 4, we give a short account of the analytic aspects of non-unique factorization. Chapter 5 is devoted to the investigation of the combinatorial problems which arise during the work in chapters 2, 3 and 4.

2. KRULL MONOIDS

We divide this chapter into two sections. In Section 2.1, we develop the algebraic properties of Krull monoids and provide a wide array of examples. In Section 2.2 we begin discussion of sets of lengths and define several combinatorial constants which play a key role in describing the arithmetic of a Krull monoid.

2.1 Definition and Examples of Krull monoids

Throughout this paper, a monoid is a commutative and cancellative semigroup with unit element. Our main interest lies in monoids which are multiplicative monoids of integral domains. Let R be an integral domain. Then $R^\bullet = R \setminus \{0\}$ denotes its multiplicative monoid, $R^\times = R^{\bullet\times}$ the unit group of R, $\mathcal{P}(R)$ the set of maximal ideals of R, $\mathcal{I}(R)$ the multiplicative monoid of integral invertible ideals of R (with usual ideal multiplication as composition) and $\mathcal{H}(R) \subseteq \mathcal{I}(R)$ the submonoid of principal ideals. Furthermore, $\mathcal{H}(R) \simeq R^\bullet/R^\times$, the embedding $\mathcal{H}(R) \hookrightarrow \mathcal{I}(R)$ is a homomorphism and $\mathcal{I}(R)/\mathcal{H}(R) = \mathrm{Pic}(R)$ is just the Picard group of the domain R.

For a non-zero ideal $\mathfrak{f} \subseteq R$ we set

$$\mathcal{I}_{\mathfrak{f}}(R) = \{I \in \mathcal{I}(R) \mid I + \mathfrak{f} = R\}$$

and

$$\mathcal{H}_{\mathfrak{f}}(R) = \mathcal{I}_{\mathfrak{f}}(R) \cap \mathcal{H}(R)\,.$$

Clearly, $\mathcal{I}_{\mathfrak{f}}(R)$ (resp. $\mathcal{H}_{\mathfrak{f}}(R)$) is a submonoid of $\mathcal{I}(R)$ (resp. $\mathcal{H}(R)$).

We use the standard notions of divisibility theory as developed in [Ja; section 2.14] or in [Gi; chapter 1]. Furthermore, our notation is consistent with F. Halter-Koch's survey article in this volume [HK9]. For the convenience of the reader, we briefly recall some concepts. If not stated otherwise, monoids will be written multiplicatively.

For a family of monoids $(H_p)_{p\in P}$

$$\coprod_{p\in P} H_p = \{(a_p)_{p\in P} \in \prod_{p\in P} H_p \mid a_p = 1 \quad \text{for almost all} \quad p \in P\}$$

denotes the coproduct of the H_p. For every $Q \subseteq P$ we view $\coprod_{p\in Q} H_p$ as a submonoid of $\coprod_{p\in P} H_p$. If all H_p are infinite cyclic (i.e., $H_p \simeq (\mathbb{N}_0, +)$), then $\coprod_{p\in P} H_p$ is the free abelian monoid with basis P and will be denoted by $\mathcal{F}(P)$. In this case, every $a \in \mathcal{F}(P)$ has a unique representation

$$a = \prod_{p\in P} p^{v_p(a)}$$

with $v_p(a) \in \mathbb{N}_0$ and $v_p(a) = 0$ for almost all $p \in P$. Furthermore,

$$\sigma(a) = \sum_{p\in P} v_p(a) \in \mathbb{N}_0$$

is called the *size* of a.

Let D be a monoid. Then $D^\times$ denotes the group of invertible elements of D. D is called reduced, if $D^\times = \{1\}$. Clearly, $D_{\text{red}} = D/D^\times$ is reduced. $\mathcal{Q}(D)$ denotes a quotient group of D

with $D \subseteq \mathcal{Q}(D)$. The *root closure* $\widetilde{D}$ of D and the *complete integral closure* $\widehat{D}$ of D are defined by

$$\widetilde{D} = \{x \in \mathcal{Q}(D) \,|\, x^n \in D \quad \text{for some} \quad n \in \mathbb{N}\}$$

and

$$\widehat{D} = \{x \in \mathcal{Q}(D) \,|\, \text{there exists some } c \in D \text{ such that } cx^n \in D \text{ for all } n \in \mathbb{N}\}\,.$$

D is called *root closed*, if $D = \widetilde{D}$ and *completely integrally closed* if $D = \widehat{D}$. Clearly,

$$D \subseteq \widetilde{D} \subseteq \widehat{D} \subseteq \mathcal{Q}(D)\,.$$

A submonoid $H \subseteq D$ is called *saturated*, if $a, b \in H$, $c \in D$ and $a = bc$ implies that $c \in H$ (equivalently, $H = D \cap \mathcal{Q}(H)$).

A monoid homomorphism $\varphi : H \to D$ induces a monoid homomorphism $\varphi_{\text{red}} : H_{\text{red}} \to D_{\text{red}}$ and a group homomorphism $\mathcal{Q}(\varphi) : \mathcal{Q}(H) \to \mathcal{Q}(D)$.

Let $\varphi : H \to D$ be a monoid homomorphism. Then φ is called a *divisor homomorphism*, if $a, b \in H$ and $\varphi(a) \,|\, \varphi(b)$ implies that $a \,|\, b$. The following conditions are equivalent (cf. [G-HK2; Lemma 2.6]).

i) φ is a divisor homomorphism,
ii) φ_{red} is a divisor homomorphism,
iii) φ_{red} is injective and $\varphi(H) \subseteq D$ is saturated.

Definition 2.1. A divisor homomorphism $\varphi : H \to D$ into a free abelian monoid D is called a *divisor theory* (for H), if for all $\alpha \in D$ there are $a_1, \ldots, a_n \in H$ such that $\alpha = \gcd\{\varphi(a_1), \ldots \varphi(a_n)\}$. The quotient group $\mathcal{C}(H) = \mathcal{Q}(D)/\mathcal{Q}(\varphi)\big(\mathcal{Q}(H)\big)$ is called the *divisor class group* of H.

Dedekind domains serve as a classic example of a divisor theory. For, if R is a Dedekind domain, then $R^\bullet$ has a divisor theory $\varphi : R^\bullet \to \mathcal{I}(R)$ given by $\alpha \to \alpha R$. The prime divisors of $\mathcal{I}(R)$ are just the prime ideals of R and the divisor class group is the usual ideal class group of R. The definition of a divisor theory given above goes back to Skula (see [Sk1]). For a survey on monoids with divisor theory the reader is referred to [HK1].

Let H be a monoid. It follows directly from the definition that H admits a divisor theory if and only if the reduced monoid H_{red} admits a divisor theory. Recall the following two facts.

i) if H admits a divisor homomorphism into a free abelian group, then H admits a divisor theory.

ii) if $\varphi : H \to D$ and $\varphi' : H \to D'$ are divisor theories for H, then there exists a monoid isomorphism $\phi : D \to D'$ such that $\varphi' = \phi \circ \varphi$. In particular, the divisor class group of H just depends on H (and not on φ).

Both **i)** and **ii)** can be proved using the theory of divisorial ideals in H. Proofs may be found in the book of Gundlach ([Gu; chapter 9]). Using the same methods one can also show if H admits a divisor theory, then the canonical homomorphism $\partial : H \to \mathcal{I}_v(H)$ into the monoid of integral divisorial ideals of H is a divisor theory.

An alternate proof of **i)** and **ii)** involves defining families of monoid homomorphisms. A family $(\varphi_p : H \to \mathbb{N}_0)_{p \in P}$ of monoid homomorphisms is a *defining family for* H, if

$$H = \bigcap_{p \in P} \mathcal{Q}(\varphi_p)^{-1}(\mathbb{Z})$$

and the intersection is of finite character (cf. [G-HK2; HK2]). If H has a defining family of the above type, it has a defining family of essential surjective homomorphisms $(\psi_p : H \to \mathbb{N}_0)_{p \in P}$ (cf. [HK2]).

We summarize our discussion in the following theorem. The remaining equivalences can be found in [G-HK1; Theorem 1] and [Cho; Proposition 2].

Theorem 2.2. *For a monoid H following conditions are equivalent:*

1. *H admits a divisor theory.*
2. *The canonical homomorphism $\partial : H \to \mathcal{I}_v(H)$ into the monoid of integral divisorial ideals is a divisor theory.*
3. *H is completely integrally closed and satisfies the ascending chain condition on divisorial ideals.*
4. *$H = H^\times \times T$ and T is a saturated submonoid of a free abelian monoid.*
5. *H admits a divisor homomorphism into a free abelian monoid.*
6. *H has a defining family $(\varphi_p : H \to \mathbb{N}_0)_{p \in P}$.*

7. *H has a defining family $(\psi_p : H \to \mathbb{N}_0)_{p \in P}$ where all ψ_p are essential and surjective.*

Definition 2.3. A monoid H satisfying the equivalent conditions of the previous theorem is called a *Krull monoid*.

The notion of a Krull monoid was introduced by L. Chouinard in [Cho]. It is important for our purposes due to the following result which was stated by Skula in [Sk2] and first proved by Krause in [Kr] (a simple proof appears in [HK2; Satz 5]).

Theorem 2.4. *An integral domain R is a Krull domain if and only if its multiplicative monoid $R^\bullet$ is a Krull monoid. If R is Krull, then the divisor class group of the Krull monoid $R^\bullet$ is the usual divisor class group of the Krull domain R.*

We present a series of examples of Krull monoids which are not multiplicative monoids of Krull domains, but none the less are of interest.

a) Krull rings Let R be a Marot ring. Then R is a Krull ring (in the sense of [Hu]) if and only if the multiplicative monoid of regular elements of R is a Krull monoid (cf. [HK7]).

b) Hilbert monoids The monoid structures of several classical objects in commutative algebra and number theory are represented in the following construction. We will start in a very abstract way and specialize to well known examples which at first may seem unrelated. Let R be a Dedekind domain. Then $\mathcal{I}(R)$ is a free abelian monoid with basis $\mathcal{P}(R)$ (i. e., $\mathcal{I}(R) = \mathcal{F}\big(\mathcal{P}(R)\big)$). Let Γ_0 be a monoid, $\Gamma \subseteq \Gamma_0$ a submonoid and $\pi : R^\bullet \to \Gamma_0$ a monoid homomorphism. Then

$$H = R_{\Gamma,\pi} = \pi^{-1}(\Gamma) \subseteq R^\bullet$$

is a submonoid. Suppose $\Gamma \subseteq \Gamma_0^\times$ is a subgroup. Then $H^\times = H \cap R^\times$,

$$H/H^\times \simeq \{aR \,|\, a \in H\} \subseteq \mathcal{H}(R)\,.$$

and $H \hookrightarrow R^\bullet$ is a divisor homomorphism, since $H = \mathcal{Q}(H) \cap R^\bullet$. Therefore H admits a divisor theory (i. e., H is a Krull monoid).

Let $\{1\} \subseteq \Gamma' \subseteq \Gamma \subseteq \Gamma_0^\times$ be subgroups. Then

$$R_{\{1\},\pi} \subseteq R_{\Gamma',\pi} \subseteq R_{\Gamma,\pi} \subseteq R_{\Gamma_0^\times,\pi}\,,$$

$R_{\Gamma,\pi} \subseteq R_{\Gamma_0^\times,\pi}$ is saturated and there is a natural epimorphism

$$\rho : \mathcal{C}(R_{\Gamma',\pi}) \to \mathcal{C}(R_{\Gamma,\pi})\,.$$

Conversely, let $H \subseteq R_{\Gamma_0^\times,\pi}$ be a saturated submonoid with $R_{\{1\},\pi} \subseteq H$. We show that H is of the form $R_{\Gamma,\pi}$ for some subgroup $\Gamma \subseteq \Gamma_0^\times$. Since $H \subseteq R_{\Gamma_0^\times,\pi}$ is saturated, we have

$$H = \mathcal{Q}(H) \cap R_{\Gamma_0^\times,\pi}\,.$$

Let $\mathcal{Q}(\pi) : \mathcal{Q}(R^\bullet) \to \mathcal{Q}(\Gamma_0)$ be the extension of π to the quotient groups. Then $R_{\{1\},\pi} \subseteq H$ implies that $\mathrm{Ker}\big(\mathcal{Q}(\pi)\big) \subseteq \mathcal{Q}(H)$ and thus $\mathcal{Q}(H) = \mathcal{Q}(\pi)^{-1}\big(\mathcal{Q}(\pi)\mathcal{Q}(H)\big)$. Clearly,

$$\Gamma = \mathcal{Q}(\pi)\big(\mathcal{Q}(H)\big) \subseteq \Gamma_0^\times$$

and

$$H = \mathcal{Q}(\pi)^{-1}(\Gamma) \cap \pi^{-1}(\Gamma_0^\times) = \pi^{-1}(\Gamma)\,.$$

After these preliminaries we consider monoids Γ_0 of arithmetical interest. Let

$$\mathfrak{f}^* = \mathfrak{f}\,\omega_1 \ldots \omega_m$$

be a cycle of R. Hence, $\mathfrak{f}^*$ is a formal product of an ideal $\mathfrak{f} \in \mathcal{I}(R)$ and m distinct ring monomorphisms $\omega_1, \ldots, \omega_m \colon R \to \mathbb{R}$. For $1 \le i \le m$ we set $\sigma_i = \mathrm{sgn} \circ \omega_i$ where $\mathrm{sgn} : \mathbb{R} \to \{-1, 0, 1\}$ denotes the signum function.

We say that $a, b \in R$ are congruent modulo $\mathfrak{f}^*$, if $a \equiv b \bmod \mathfrak{f}$ and $\sigma_i(a) = \sigma_i(b)$ for $1 \le i \le m$. This defines a congruence relation on R. For every $a \in R$ we denote by $[a]$ the congruence class containing a and by $R/\mathfrak{f}^*$ the set of all congruence classes. Clearly, $R/\mathfrak{f}^*$ is a (not necessarily cancellative) semigroup with $[a][b] = [ab]$ for all $a, b \in R$. Let $\pi : R^\bullet \to R/\mathfrak{f}^* = \Gamma_0$ denote the canonical epimorphism and let $\Gamma \subseteq \Gamma_0^\times$ be a subgroup. Then

$$R_{\mathfrak{f}^*,\Gamma} = \pi^{-1}(\Gamma) = \{a \in R^\bullet \mid [a] \in \Gamma\}$$

is a Krull monoid, called the *Hilbert monoid* associated to $\mathfrak{f}^*$ and Γ. We may identify the reduced Hilbert monoid $(R_{\mathfrak{f}^*,\Gamma})_{\rm red}$ with

$$\mathcal{H}_{\mathfrak{f}^*,\Gamma}(R) = \{aR \,|\, a \in R^\bullet\,,\ [a] \in \Gamma\} \subseteq \mathcal{H}(R)\,.$$

Furthermore, the embedding

$$\mathcal{H}_{\mathfrak{f}^*,\Gamma}(R) \to \mathcal{I}_{\mathfrak{f}}(R)$$

is a divisor theory (cf. [HK2; Proof of Satz 7]). If $\Gamma = (R/\mathfrak{f}^*)^\times$, we simply write $\mathcal{H}_{\mathfrak{f}^*}(R)$ instead of $\mathcal{H}_{\mathfrak{f}^*,(R/\mathfrak{f}^*)^\times}(R)$.

This construction was first illustrated by F. Halter-Koch in [HK2] and generalizes the original examples of D. Hilbert. Clearly,

$$(R/\mathfrak{f})^\times = \{a + \mathfrak{f} \in R/\mathfrak{f} \,|\, a \in R\,,\ aR + \mathfrak{f} = R\}\,.$$

In [HK2; Hilfssatz 2 and Satz 7] it was verified that

$$(R/\mathfrak{f}^*)^\times = \{[a] \in R/\mathfrak{f}^* \,|\, a \in R\,,\ aR + \mathfrak{f} = R\}$$

and that there is an exact sequence of groups

$$0 \to (\mathbb{Z}/2\mathbb{Z})^m \to (R/\mathfrak{f}^*)^\times \to (R/\mathfrak{f})^\times \to 1\,.$$

Hence we have that

$$\begin{aligned}\mathcal{H}_{\mathfrak{f}^*}(R) &= \{aR \,|\, a \in R\,,\ [a] \in (R/\mathfrak{f}^*)^\times\} \\ &= \{aR \,|\, a \in R\,,\ aR + \mathfrak{f} = R\} \\ &= \{aR \,|\, a \in R\,,\ [a] \in (R/\mathfrak{f})^\times\} = \mathcal{H}_{\mathfrak{f}}(R)\,.\end{aligned}$$

We consider the following simple cases.

i) If $m = 0$, $\mathfrak{f} = (1) = R$, $\mathfrak{f}^* = \mathfrak{f} = R$, then $\mathcal{H}_{\mathfrak{f}}(R) = \mathcal{H}(R)$.

ii) Let $R = \mathbb{Z}$ and $\omega_1 : \mathbb{Z} \hookrightarrow \mathbb{R}$ be the embedding $\mathfrak{f} = f\mathbb{Z}$ for some $f \in \mathbb{N}$. Then

$$R_{\mathfrak{f}^*,\{1\}} = \{a \in \mathbb{Z} \,|\, a > 0\,,\ a \equiv 1 \bmod f\} = 1 + f\mathbb{N}\,,$$

the classical Hilbert monoid.

iii) Let R be the ring of integers in an algebraic number field K, $\omega_1, \ldots, \omega_{r_1} : K \to \mathbb{R}$ the real embeddings of K, $\mathfrak{f} = (R)$ and $\mathfrak{f}^* = \omega_1 \ldots \omega_{r_1}$. Then

$$H = R_{\mathfrak{f}^*,\{1\}} = \{a \in R^\bullet \mid \omega_i(a) > 0 \quad 1 \le i \le r\}$$

is the monoid of totally positive algebraic integers in K. Its divisor class group $\mathcal{C}(H)$ is called the ideal class group in the narrow sense (cf. [Na2; p.94]).

Let K be a global field (i. e., either an algebraic number field or an algebraic function field in one variable over a finite field). Let $S(K)$ denote the set of all non-archimedean places and for some $\nu \in S(K)$ let R_ν be the corresponding valuation domain. For a finite subset $S \subset S(K)$, $S \neq \emptyset$ in the function field case,

$$R = R_S = \bigcap_{\nu \in S(K)\setminus S} R_\nu \subseteq K$$

is called the holomorphy ring of K associated with S. R is a Dedekind domain with quotient field K. A cycle $\mathfrak{f}^*$ of R (in the sense of class field theory) is a cycle

$$\mathfrak{f}^* = \mathfrak{f}\omega_1 \ldots \omega_m$$

with $\mathfrak{f} \in \mathcal{I}(R)$, $m \ge 0$ and $\omega_1, \ldots, \omega_m : K \to \mathbb{R}$ real embeddings ($m = 0$ in the function field case). Then

$$\mathcal{H}_{\mathfrak{f}^*,\{1\}} = \{aR \mid a \in R,\ a \equiv 1 \bmod \mathfrak{f}^*\}$$

is the *principal ray modulo* $\mathfrak{f}^*$. Its divisor class group

$$\mathcal{C}(\mathcal{H}_{\mathfrak{f}^*,\{1\}}) = \mathcal{I}_\mathfrak{f}(R)/\mathcal{H}_{\mathfrak{f}^*,\{1\}}(R)$$

is a finite abelian group, called the *ray class group modulo* $\mathfrak{f}$. It gives rise to the following sequence of finite abelian groups:

$$0 \to \mathcal{H}_\mathfrak{f}(R)/\mathcal{H}_{\mathfrak{f}^*,\{1\}}(R) \to \mathcal{I}_\mathfrak{f}(R)/\mathcal{H}_{\mathfrak{f}^*,\{1\}}(R) \to \mathcal{I}_\mathfrak{f}(R)/\mathcal{H}_\mathfrak{f}(R) = \mathcal{I}(R)/\mathcal{H}(R) \to 0.$$

c) Submonoids of orders in Dedekind domains Let R be a Dedekind domain and $\mathfrak{o} \subseteq R$ an order in R. Thus, $\mathfrak{o}$ is one-dimensional noetherian, R is the integral closure of $\mathfrak{o}$ (in some quotient field of $\mathfrak{o}$) and R is a finitely generated $\mathfrak{o}$-module. Let

$$\mathfrak{f} = \mathrm{Ann}_{\mathfrak{o}}(R/\mathfrak{o}) = \{a \in \mathfrak{o} \mid aR \subseteq \mathfrak{o}\}$$

denote the conductor of $\mathfrak{o}$. If $\mathfrak{o} \neq R$, then $\mathfrak{o}$ is not integrally closed. Thus $\mathfrak{o}$ is not a Krull domain and hence $\mathcal{H}(\mathfrak{o})$ fails to be a Krull monoid. However, $\mathcal{H}(\mathfrak{o})$ contains a divisor closed submonoid that is Krull which yields information on the factorization properties of $\mathcal{H}(\mathfrak{o})$. This submonoid can be described as follows. The extension of ideals

$$\begin{aligned} \psi : \mathcal{I}_{\mathfrak{f}}(\mathfrak{o}) &\to \mathcal{I}_{\mathfrak{f}}(R) \\ I &\mapsto IR \end{aligned}$$

is a monoid isomorphism with

$$\psi^{-1}(J) = J \cap \mathfrak{o} \quad \text{for all} \quad J \in \mathcal{I}_{\mathfrak{f}}(R)$$

(cf. [G-HK-K; §3]). Therefore $\mathcal{I}_{\mathfrak{f}}(\mathfrak{o})$ is free abelian. The embedding

$$\mathcal{H}_{\mathfrak{f}}(\mathfrak{o}) \hookrightarrow \mathcal{I}_{\mathfrak{f}}(\mathfrak{o})$$

is a divisor theory and hence $\mathcal{H}_{\mathfrak{f}}(\mathfrak{o})$ is a Krull monoid.

Note that in general, $\psi\big(\mathcal{H}_{\mathfrak{f}}(\mathfrak{o})\big) \neq \mathcal{H}_{\mathfrak{f}}(R)$.

d) Block monoids Let G be an additively written abelian group and $G_0 \subseteq G$ a nonempty subset. Then

$$\mathcal{B}(G_0) = \Big\{ \prod_{g \in G_0} g^{n_g} \in \mathcal{F}(G_0) \mid \sum_{g \in G} n_g g = 0 \Big\} \subseteq \mathcal{F}(G_0)$$

is called the *block monoid over* G_0. Clearly, the embedding $i : \mathcal{B}(G_0) \hookrightarrow \mathcal{F}(G_0)$ is a divisor homomorphism and hence $\mathcal{B}(G_0)$ is a Krull monoid. Block monoids are the appropriate tool for studying factorization questions in Krull domains and will be discussed further in chapter 3.

e) Root closed finitely generated monoids Krull monoids are completely integrally closed and hence root closed. For finitely generated monoids the converse holds.

Proposition 2.5. *Let H be a monoid.*

1. *H is finitely generated if and only if $\widetilde{H}$ is finitely generated.*
2. *Suppose that H is finitely generated. Then H is a Krull monoid if and only if $H = \widetilde{H}$.*

Proof. See [Le], [HK6; Theorem 5] and [G-HK2; Proposition 6.1]. □

Let H be a finitely generated monoid such that $\widetilde{H}$ is reduced. By the above theorem, $\widetilde{H}$ is a saturated submonoid of a finitely generated free abelian monoid. Changing to additive notation, we may suppose that

$$H \subseteq (\mathbb{N}^s, +) \subseteq (\mathbb{Z}^s, +) \subseteq (\mathbb{Q}^s, +)$$

which allows us to study H by geometrical methods. For example, it turns out that

$$\widetilde{H} = \mathrm{cone}(H) \cap \mathbb{Z}^s$$

where $\mathrm{cone}(H)$ denotes the convex cone generated by H . It was this geometrical point of view which was used in the proof of Theorem 2.5.

Hence, finitely generated monoids $H \subseteq \mathbb{Z}^s$ with $H = \mathrm{cone}(H) \cap \mathbb{Z}^s$ are Krull monoids. In particular, this is the case for the set of solutions of linear diophantine inequalities. Let $m, s \in \mathbb{N}$, $A \in M_{m,s}(\mathbb{Z})$ and

$$H = \{x \in \mathbb{Z}^s | Ax \geq 0\} \subseteq \mathbb{Z}^s.$$

Then H is a root closed monoid which is finitely generated by [HK6; Theorem 1] and thus is Krull.

2.2 Sets of lengths in Krull monoids

Let H be a monoid. An element $u \in H \setminus H^\times$ is called *irreducible* (or an *atom*), if for all $a, b \in H$ $u = ab$ implies that $a \in H^\times$ or $b \in H^\times$. Let $\mathcal{A}(H)$ denote the set of atoms of H . If $\rho : H \to H_{\mathrm{red}}$ is the canonical epimorphism, then $\rho\big(\mathcal{A}(H)\big) = \mathcal{A}(H_{\mathrm{red}})$ and $\rho^{-1}\big(\mathcal{A}(H_{\mathrm{red}})\big) = \mathcal{A}(H)$. The free abelian monoid

$$\mathcal{Z}(H) = \mathcal{F}\big(\mathcal{A}(H_{\mathrm{red}})\big)$$

with basis $\mathcal{A}(H_{\text{red}})$ is called the *factorization monoid* of H. Furthermore, the canonical homomorphism

$$\pi = \pi_H : \mathcal{Z}(H) \to H_{\text{red}}$$

is called the *factorization homomorphism* of H and for $a \in H$ the elements of

$$\mathcal{Z}_H(a) = \mathcal{Z}(a) = \pi^{-1}(aH^\times) \subseteq \mathcal{Z}(H)$$

are called *factorizations* of a. We say that H is *atomic* if π is surjective (equivalently, H is generated by $\mathcal{A}(H) \cup H^\times$). So, when studying factorizations we may restrict ourselves to reduced monoids.

Let H be a reduced atomic monoid. For an element $z = \prod_{u \in \mathcal{A}(H)} u^{n_u} \in \mathcal{Z}(H)$,

$$\sigma(z) = \sum_{u \in \mathcal{A}(H)} n_u \in \mathbb{N}_0$$

is called the *length of the factorization* z. For $a \in H$,

$$L_H(a) = L(a) = \{\sigma(z) \,|\, z \in \mathcal{Z}(a)\} \subseteq \mathbb{N}_0$$

denotes the *set of lengths* of a. Furthermore, we call

$$\mathcal{L}(H) = \{L(a) \,|\, 1 \neq a \in H\}$$

the *system of sets of lengths* of H. $\mathcal{L}(H)$ is a subset of the power set of $\mathbb{N}$. By definition we have

i) $L(a) = \{0\}$ if and only if $a = 1$.

ii) $L(a) = \{1\}$ if and only if $a \in \mathcal{A}(H)$.

We say that H is *half-factorial* if for all $a \in H$ any two factorizations of a have the same length. Such monoids gained interest after Carlitz [Ca] showed (using different terminology) that a ring of integers in an algebraic number field is half-factorial if and only if its class number is less than or equal to two. Further results concerning domains that are half-factorial can be found in [Sk2] [Z1] and [Z2]. We will return to this topic later in chapter 5.

Lemma 2.6. *Let H be a reduced atomic monoid.*

1. *Then the following conditions are equivalent:*
- **i)** *H is half-factorial.*
- **ii)** *$\#L(a) = 1$ for all $a \in H$.*
- **iii)** *$\mathcal{L}(H) = \big\{\{n\} \mid n \in \mathbb{N}\big\}$.*

2. *If H is not half-factorial, then for every $N \in \mathbb{N}$ there exists some $a \in H$ with $\#L(a) \ge N$.*

Proof. The proof of **1.** is obvious. For the proof of **2.**, see [HK9; Lemma 2.2]. □

Let H be a Krull monoid with divisor theory $\varphi : H \to D$. We define

$$\mathcal{D}(H, D) = \sup\{\sigma(\varphi(u)) \mid u \in \mathcal{A}(H)\} \in \mathbb{N} \cup \{\infty\}.$$

Hence, $\mathcal{D}(H, D)$ is the maximum number of prime divisors of D dividing the image of some irreducible element of H. The following lemma lists some basic facts relating these concepts.

Lemma 2.7. *Let H be a Krull monoid with divisor theory $\varphi : H \to \mathcal{F}(P)$ and divisor class group G.*

1. *H is atomic.*

2. *An element $a \in H$ is prime in H if and only if $\varphi(a) \in P$.*

3. *H is a finite-factorization monoid (i. e., all sets $\mathcal{Z}(a)$ are finite).*

4. *All sets $L \in \mathcal{L}(H)$ are finite.*

5. *The following statements are equivalent:*
- **i)** *H is factorial.*
- **ii)** *$\mathcal{D}(H, D) = 1$.*
- **iii)** *$\#G = 1$.*

Proof. See [HK1; Korollar 2 and Satz 10] and [HK5; Corollary 3]. □

We restrict ourselves to arithmetical questions dealing with lengths of factorizations. For information on other arithmetical invariants, the reader is referred to [Ge10]. We introduce some arithmetical invariants which help describe the structure of sets of lengths. We list

some of their most elementary properties but offer a more thorough treatment after the introduction of block monoids.

We divide our discussion into four problem areas. Throughout, let H be a reduced atomic monoid.

a) The μ_k - functions We compare the minimum and the supremum of sets of lengths. Let $k \in \mathbb{N}$. We define the following three invariants:

$$\mu_k(H) = \sup\{\sup L \mid \min L \le k,\ L \in \mathcal{L}(H)\},$$
$$\mu_k^{'}(H) = \sup\{\sup L \mid k \in L,\ L \in \mathcal{L}(H)\} \text{ and}$$
$$\mu_k^{*}(H) = \sup\{\sup L \mid \min L = k,\ L \in \mathcal{L}(H)\},$$

using the convention $\sup \emptyset = 0$ if there is no $L \in \mathcal{L}(H)$ with $\min L = k$. By definition we have

$$\mu_k^{*}(H) \le \mu_k^{'}(H) \le \mu_k(H).$$

Let $a \in H$ with $\min L(a) = l \le k$. Choose some $u \in \mathcal{A}(H)$. Then $k \in L(au^{k-l})$ and

$$\sup L(au^{k-l}) \ge \sup L(a) + (k-l),$$

which implies $\mu_k^{'}(H) \ge \mu_k(H)$. Thus $\mu_k^{'}(H) = \mu_k(H)$.

Lemma 2.8. *Let H be a reduced atomic monoid and $k \in \mathbb{N}$. If $\mu_k(H) < \infty$, then $\mu_k^{*}(H) = \mu_k(H)$.*

Proof. Suppose $\mu_k(H) < \infty$ and let $a \in H$ be given with $\min L(a) \le k$ and $\max L(a) = \mu_k(H)$. For some $u \in \mathcal{A}(H)$ we set $b = au^{k - \min L(a)}$. Then

$$\min L(b) \le \min L(a) + k - \min L(a) = k$$

and

$$\mu_k(H) \ge \max L(b) \ge \max L(a) + k - \min L(a) \ge \mu_k(H),$$

which implies that $k = \min L(a)$ and hence $\mu_k^{*}(H) = \mu_k(H)$. □

The invariant $\mu_k(H)$ was introduced in [G-L] and special aspects of the μ_k-function have been investigated in various terminology. We point out the relationship between these concepts, but first gather some elementary properties of $\mu_k(H)$.

Lemma 2.9. *Let H be a reduced atomic monoid.*

1. $\mu_1(H) = 1$ *and* $k + l \le \mu_k(H) + \mu_l(H) \le \mu_{k+l}(H)$ *for all* $k, l \in \mathbb{N}$.
2. *If* $\mu_k(H) = k$ *for some* $k \in \mathbb{N}$, *then* $\mu_l(H) = l$ *for all* $1 \le l \le k$.
3. H *is half-factorial if and only if* $\mu_k(H) = k$ *for all* $k \in \mathbb{N}$.

Proof. The proofs of **1.** and **3.** are clear by the definition. To verify **2.**, suppose $\mu_k(H) = k$ for some $k \in \mathbb{N}$. Then for every $1 \le l < k$ we have that

$$l \le \mu_l(H) \le \mu_k(H) - \mu_{k-l}(H) \le k - (k - l) = l \ . \quad \square$$

An atomic monoid H is said to be *k-half-factorial* for some $k \in \mathbb{N}$, if $\mu_k(H) = k$. This property has been investigated in a series of papers (see [Ch-S3],[Ch-S4] and [Ch-S6]) and the interested reader is referred there for specific constructions. The following lemma shows that in finitely generated monoids there exists a constant $k \in \mathbb{N}$ such that k-half-factoriality implies half-factoriality. Some efforts have been made to determine the minimal $k \in \mathbb{N}$ with this property. We return to this problem in section 3.1 and chapter 5.

Proposition 2.10. *Let H be a finitely generated monoid. Then there exists some $k \in \mathbb{N}$ such that H is half-factorial if and only if H is k-half-factorial.*

Proof. We may suppose that H is reduced. Clearly, if H is half-factorial, then it is m-half-factorial for all $m \in \mathbb{N}$. So it remains to show the converse.

Let H be generated by $u_1, \ldots, u_s \in H$ and consider the set

$$S = \{(\mathbf{m}, \mathbf{n}) \in \mathbb{N}_0^{2s} \mid \prod_{i=1}^{s} u_i^{m_i} = \prod_{i=1}^{s} u_i^{n_i} \ne 1\} \, .$$

By Dickson's Theorem (see [Re; Satz 2]) the set of minimal points $S_0 \subseteq S$ is finite. For $\mathbf{m} \in \mathbb{N}_0^s$ we set

$$|\mathbf{m}| = \sum_{i=1}^{s} m_i \ .$$

Obviously, it is sufficient to verify that if

$$|\mathbf{m}| = |\mathbf{n}| \quad \text{for all } (\mathbf{m}, \mathbf{n}) \in S_0 \tag{$*$}$$

then H is half-factorial.

Suppose that $(*)$ holds and assume to the contrary that H is not half-factorial. Then there exists some $a \in H$ with

$$a = \prod_{i=1}^{s} u_i^{m_i} = \prod_{i=1}^{s} {u_i}^{n_i} ,$$

$$\min L(a) = |\mathbf{m}| < |\mathbf{n}|$$

and $|\mathbf{m}|$ minimal. Then $(\mathbf{m}, \mathbf{n}) \notin S_0$ and hence there exists some $(\mathbf{m}', \mathbf{n}') \in S_0$ with $\mathbf{m}' \le \mathbf{m}$ and $\mathbf{n}' \le \mathbf{n}$. But then we have

$$\prod_{i=1}^{s} u_i^{m_i - m_i'} = \prod_{i=1}^{s} u_i^{n_i - n_i'} \in H$$

and $|\mathbf{m} - \mathbf{m}'| < |\mathbf{n} - \mathbf{n}'|$, a contradiction to the minimality of $|\mathbf{m}|$. □

A further arithmetical concept closely related with the μ_k-function is the concept of elasticity. Let H be an atomic monoid. The *elasticity* $\varrho(H)$ of H is defined as

$$\varrho(H) = \sup\Big\{ \frac{\sup L}{\min L} \mid L \in \mathcal{L}(H) \Big\} \in \mathbb{R}_{\ge 1} \cup \{\infty\} .$$

A detailed study of elasticity is contained in an article by David Anderson in this volume ([An1]). It is easy to see that

$$\varrho(H) = \lim_{k \to \infty} \frac{\mu_k(H)}{k}$$

(cf. [HK8; Proposition 1]).

In section 5.3 we shall review what is known concerning $\mu_k(H)$ for Krull monoids H.

b) Distances of successive lengths Our next topic deals with possible distances of successive lengths of factorizations for elements

$a \in H$. For a finite set $L = \{x_1, \cdots, x_r\} \subseteq \mathbb{Z}$ with $x_1 < \cdots < x_r$ we set

$$\Delta(L) = \{x_i - x_{i-1} \,|\, 2 \le i \le r\} \subseteq \mathbb{N} ,$$

and

$$\Delta(H) = \bigcup_{L \in \mathcal{L}(H)} \Delta(L) \subseteq \mathbb{N} .$$

Hence, $\Delta(H)$ is the set of distances of successive lengths. The proof of the following property of $\Delta(H)$ is not difficult and can be found in [Ge6; Lemma 3].

Lemma 2.11. *Let H be a reduced atomic monoid. Then $min\Delta(H) = gcd\Delta(H)$.*

By definition we have that H is half-factorial if and only if $\Delta(H) = \emptyset$. A monoid H is called *d-congruence half-factorial*, if for all $a \in H$ and any two factorizations $z, z' \in \mathcal{Z}(a)$ we have

$$\sigma(z) \equiv \sigma(z') \mod d$$

(cf. [Ch-S2]). Hence H is d-congruence half-factorial with $d \in \mathbb{N}$ minimal if and only if $\min\Delta(H) = d$. We will consider the d-congruence half-factorial property, as well as the set $\Delta(H)$, in more detail in section 5.2.

c) Structure of sets of lengths An atomic monoid is either half-factorial or sets of lengths can become arbitrarily large. Hence, an obvious question is to describe such sets for Krull monoids. While in general these sets may not be perfect arithmetic progressions, they are almost arithmetic in the following sense.

Definition 2.12. A subset $L \subset \mathbb{Z}$ is called an *almost arithmetical progression bounded by* $M \in \mathbb{N}$, if

$$\begin{aligned} L = \{x_1, \ldots, x_\alpha , \quad & y + \delta_1 , && \ldots , && y + \delta_\eta , && y + d , \\ & y + \delta_1 + d , && \ldots , && y + \delta_\eta + d , && y + 2d , \\ & \vdots \\ & y + \delta_1 + (k-1)d , && \ldots , && y + \delta_\eta + (k-1)d , && y + kd , \quad z_1 , \ldots , z_\beta \} , \end{aligned}$$

where $\alpha, \beta, \eta, k, d \in \mathbb{N}_0$, $x_1 < \cdots < x_\alpha < y \le y + kd < z_1 < \cdots < z_\beta$, $0 < \delta_1 < \cdots < \delta_\eta < d$ and $\max\{\alpha, \beta, d\} \le M$.

The following Theorem solves the characterization question and can be found in [Ge2, Satz 1].

Theorem 2.13. *Let H be a Krull monoid which has only finitely many divisor classes containing prime divisors. Then there exists some $M \in \mathbb{N}$ such that every $L \in \mathcal{L}(H)$ is an almost arithmetical progression bounded by M.*

This result is sharp in the sense that all the parameters in Definition 2.12 are necessary (see [Ge9] for an example which illustrates this). Hence, the result raises further questions concerning the parameters of almost arithmetical progressions. The only invariant which has been investigated thus far deals with possible distances in arithmetical progressions. To be more precise, for H as in Theorem 2.13 let

$$\Delta_1(H)$$

denote the set of all $d \in \mathbb{N}$ such that for all $N \in \mathbb{N}$ there exists some $L \in \mathcal{L}(H)$ with $\#L \ge N$ and with

$$L = \{x_1, \ldots, x_\alpha, y, y + d, \ldots, y + kd, z_1, \ldots z_\beta\}$$

where $x_1 < \cdots < z_\beta, \alpha \le M$ and $\beta \le M$ with M as in Theorem 2.13. Notice that $\Delta_1(H) \subseteq \Delta(H)$, and that there are examples of differences which appear in $\Delta(H)$ which do not appear as a distance in arbitrarily long almost arithmetic progressions. We return to $\Delta_1(H)$ in section 5.2.

d) Systems of sets of lengths In algebraic number theory, the ideal class group G is considered as a measure for the deviation of the ring of integers R from being a unique factorization domain. G is thought to determine the arithmetic of R. A definition of a type of arithmetic equivalence is given by F. Halter-Koch in [HK1; Korollar 4].

In [Na2; problem 32], W. Narkiewicz asked for an arithmetical characterization of the ideal class group of a ring of integers in an

algebraic number field. Various answers to this question have been given by J. Kaczorowski, F. Halter-Koch, D.E. Rush, A. Czogala, U. Krause and others (see [Ge6 and Ge7 for a survey]). However, it is still unknown if it is possible to characterize the ideal class group by using only lengths of factorizations. To be more precise, we formulate the following problem:

Problem: Let H and H' be Krull monoids with finite divisor class groups G and G' such that each divisor class contains a prime divisor. If $\#G \geq 4$, does $\mathcal{L}(H) = \mathcal{L}(H')$ imply that $G = G'$?

We shall not consider this problem further but add the following remarks.

Remark. 1. Suppose that H and H' are the multiplicative monoids of the rings of algebraic integers R and R'. A positive answer to the Problem implies that sets of lengths completely determine the arithmetic of a ring of integers.

2. The analogous question for arbitrary orders in algebraic number fields ("do sets of lengths determine the arithmetic of an arbitrary order") has a negative answer (see [HK9; Example 3]).

3. Clearly, the assumption that each class contains a prime divisor is necessary for obtaining a positive answer.

4. The Problem is answered positively for cyclic groups in [Ge4].

3. BLOCK MONOIDS

Let G be an additively written abelian group and $\emptyset \neq G_0 \subseteq G$ a subset. Let $< G_0 >$ denote the subgroup and $[G_0]$ the submonoid generated by G_0. If we define the *content homomorphism*

$$\begin{aligned} \iota : \mathcal{F}(G_0) &\to G \\ \prod_{g \in G} g^{n_g} &\mapsto \sum_{g \in G_0} n_g g, \end{aligned}$$

then

$$\mathcal{B}(G_0) = \{S \in \mathcal{F}(G_0) \mid \iota(S) = 0\}$$

is called the *block monoid* over G_0. It is a Krull monoid, since the embedding $\mathcal{B}(G_0) \hookrightarrow \mathcal{F}(G_0)$ is a divisor homomorphism. We also have the following (see [HK1; Satz 4 and Korollar] for a proof).

Proposition 3.1. *Let G be an abelian group and G_0 a nonempty subset. Then the following holds:*

1. *The embedding $\mathcal{B}(G_0) \hookrightarrow \mathcal{F}(G_0)$ is a divisor theory if and only if $< G_0 >= [G_0 \setminus \{g\}]$ for every $g \in G_0$.*
2. *If $\#G \le 2$, then $\mathcal{B}(G)$ is factorial.*
3. *If $\#G \ge 3$, then $\mathcal{B}(G) \hookrightarrow \mathcal{F}(G)$ is a divisor theory with class group (isomorphic to) G and each class contains exactly one prime divisor.*

3.1 The block monoid associated to a Krull monoid

Let H be a reduced Krull monoid, $\varphi : H \to D = \mathcal{F}(P)$ its divisor theory and $\pi : D \to \mathcal{C}(H) = G$ the canonical epimorphism onto its divisor class group. Let $G_0 \subseteq G$ denote the set of classes containing prime divisors (i. e., $G_0 = \{g \in G \,|\, g \cap P \neq \emptyset\}$). We define a monoid epimorphism

$$\begin{array}{rcl} \overline{\boldsymbol{\beta}} : \mathcal{F}(P) & \to & \mathcal{F}(G_0) \\ p & \mapsto & [p] \end{array}$$

which maps each prime divisor onto its divisor class. This induces a monoid epimorphism

$$\boldsymbol{\beta} = \overline{\boldsymbol{\beta}} \circ \varphi : H \to \mathcal{B}(G_0)$$

and we obtain the following commutative diagram

$$\begin{array}{ccccc} H & \stackrel{\varphi}{\to} & D = \mathcal{F}(P) & \stackrel{\pi}{\to} & G \\ \downarrow \boldsymbol{\beta} & & \downarrow \overline{\boldsymbol{\beta}} & & \| \\ \mathcal{B}(G_0) & \hookrightarrow & \mathcal{F}(G_0) & \stackrel{\iota}{\to} & G \end{array} .$$

$\boldsymbol{\beta} : H \to \mathcal{B}(G_0)$ is called the *block homomorphism* and $\mathcal{B}(G_0)$ the *block monoid* associated with the Krull monoid H (resp. with the divisor theory $\varphi : H \to D$). The significance of this construction can be seen from the following lemma.

Lemma 3.2. *Let H be a reduced Krull monoid, $a \in H$ and $\beta : H \to \mathcal{B}(G_0)$ the corresponding block homomorphism. Then we have*

1. *a is irreducible in H if and only if $\beta(a)$ is irreducible in $\mathcal{B}(G_0)$, $\beta\big(\mathcal{A}(H)\big) = \mathcal{A}\big(\mathcal{B}(G_0)\big)$ and $\beta^{-1}\big(\mathcal{A}\big(\mathcal{B}(G_0)\big)\big) = \mathcal{A}(H)$.*
2. *$L_H(a) = L_{\mathcal{B}(G_0)}\big(\beta(a)\big)$ and $\mathcal{L}(H) = \mathcal{L}\big(\mathcal{B}(G_0)\big)$.*
3. *$\mathcal{D}(H, D) = \mathcal{D}(\mathcal{B}(G_0), \mathcal{F}(G_0))$.*
4. *$\varrho(H) = \varrho\big(\mathcal{B}(G_0)\big)$, $\Delta(H) = \Delta\big(\mathcal{B}(G_0)\big)$, $\Delta_1(H) = \Delta_1\big(\mathcal{B}(G_0)\big)$ and $\mu_k(H) = \mu_k\big(\mathcal{B}(G_0)\big)$ for every $k \in \mathbb{N}$.*

Proof. The proofs of **3.** and **4.** are immediate consequences of **1.** and **2.** Proofs of **1.** and **2.** may be found in [Ge2; Proposition 1]. Alternatively, notice that β satisfies the assumption of the Transfer Lemma in [HK9]. □

Lemma 3.2 states that sets of lengths (and hence all invariants dealing with lengths of factorizations) in a Krull monoid may be studied in the associated block monoid. Let us mention an important application: it is sufficient to prove the structure theorem for sets of lengths in Krull monoids (Theorem 2.13) for block monoids. We give a further example to illustrate how the Lemma 3.2 works.

Proposition 3.3. *Let H be a Krull monoid with divisor class group G and let $G_0 \subseteq G$ denote the set of classes containing prime divisors. Suppose that G_0 is finite. Then there exists a constant $k \in \mathbb{N}$ such that H is half-factorial if and only if H is k-half-factorial.*

Proof. By Lemma 3.2 it sufficient to prove the assertion for $\mathcal{B}(G_0)$ instead of H. Since G_0 is finite, $\mathcal{B}(G_0)$ is finitely generated (cf. [Ge2; Proposition 2]). Now Proposition 2.10 implies the result. □

Block monoids were introduced by W. Narkiewicz in [Na1] and first used systematically in [Ge2]. Consequently, block monoids have been attached to arbitrary divisor homomorphisms $\varphi : H \to D$ (cf. [Ge8]). For an overview the reader is referred to [HK9].

We use the following notation throughout the remainder of this article.

Notation: $\mathcal{L}(G_0) = \mathcal{L}\big(\mathcal{B}(G_0)\big)$, $\Delta(G_0) = \Delta\big(\mathcal{B}(G_0)\big), \Delta_1(G_0) = \Delta_1\big(\mathcal{B}(G_0)\big)$,
$\mathcal{D}(G_0) = \mathcal{D}(\mathcal{B}(G_0), \mathcal{F}(G_0)), \mu_k(G_0) = \mu_k(\mathcal{B}(G_0))$ and $\varrho(G_0) = \varrho(\mathcal{B}(G_0))$.

For an abelian group G and a subset $\emptyset \neq G_0 \subseteq G$, $\mathcal{D}(G_0)$ is called the *Davenport constant* of G. By definition we have

$$\mathcal{D}(G_0) = \sup\{\sigma(B) \,|\, B \in \mathcal{A}(\mathcal{B}(G_0))\}$$

Davenport's constant plays a central role in factorization theory (cf. [Ch]). Its properties will be discussed in section 5.1.

3.2 Realization theorems

As noted above, it is easy to see that block monoids admit a divisor theory. However, it is surprising that conversely every reduced Krull monoid is isomorphic to a block monoid. A proof of the following can be found in [G-HK1; Theorem 2].

Theorem 3.4. *For a monoid H the following conditions are equivalent:*

1. *H is a Krull monoid.*
2. *There exists an abelian group G and a subset $\emptyset \neq G_0 \subseteq G$ such that $H \simeq H^\times \times \mathcal{B}(G_0)$.*

Further realization theorems for Krull monoids as arithmetically closed submonoids of special type are derived in [G-HK1; section 4].

By Lemma 3.2, sets of lengths in a Krull monoid just depend on the pair (G, G_0). So one might ask for which pairs (G, G_0) there exists a Krull monoid H with divisor class group (isomorphic) G such that G_0 is the set of classes containing prime divisors. If there is such an H, we say that the pair (G, G_0) is realizable by H.

Theorem 3.5. *Let G be an abelian group, $(m_g)_{g\in G}$ a family of cardinal numbers and $G_0 = \{g \in G | m_g \neq 0\}$. Then the following conditions are equivalent:*

1. *There exists a Krull monoid H with divisor theory $\varphi\colon H \to \mathcal{F}(\mathcal{P})$, divisor class group C and a group isomorphism $\psi\colon G \to C$ such that $m_g = \mathrm{card}(\mathcal{P} \cap \psi(g))$ for all $g \in G$.*

2. $G = [G_0]$, *and for all* $g \in G_0$ *with* $m_g = 1$ *we have* $G = [G_0 \setminus \{g\}]$.

Proof. [HK1; Satz 5] □

Building on the work of L. Claborn, A. Grams and L. Skula characterized pairs (G, G_0) which are realizable by Dedekind domains.

Theorem 3.6. *Let* G *be an abelian group and* $G_0 \subseteq G$ *a nonempty subset. Then the following conditions are equivalent:*

1. *There exists a Dedekind domain* R *with ideal class group* G *such that* G_0 *is the set of classes containing prime ideals.*

2. $G = [G_0]$.

Proof. See [Gr; Theorem 1.4]. The result is also proved independently in [Sk2; Theorem 2.4]. □

4. ARITHMETICAL KRULL MONOIDS

Let R be the ring of integers in an algebraic number field and P some factorization property. Then one might ask for an asymptotic formula for the number of elements $\alpha \in R$ (counted up to associates) satisfying property P and with norm $N(\alpha)$ bounded by x. The prototype of these questions is to count the primes $p \in \mathbb{N}$ with $p \le x$. Such quantitative aspects of non-unique factorizations in algebraic number fields were first considered by E. Fogels in the forties. Systematic investigations were started by W. Narkiewicz in the sixties (see [Na2; Chapter 9]).

Quantitative investigations of phenomena of non-unique factorizations are interesting mainly for holomorphy rings in global fields (including rings of integers in algebraic number fields and in algebraic function fields in one variable over a finite field). However, it has turned out that most of the results can be derived for very general structures in the setting of abstract analytic number theory. It was this axiomatic procedure which recently allowed the extension of results from principal orders to arbitrary orders in global fields (see [G-HK-K]). A further advantage of the axiomatic method is that it allows us to describe and investigate the combinatorial structures

which are responsible for the various phenomena of non-unique factorization. Abstract analytic number theory is carefully presented in the monograph by J. Knopfmacher [Kn], who introduced the notion of an arithmetical formation. Our definition will be slightly different.

Definition 4.1. 1. A *norm (function)* $|\cdot|$ on a reduced monoid H is a monoid homomorphism $|\cdot| : H \to (\mathbb{N}, \cdot)$ satisfying $|a| = 1$ if and only if $a = 1$.

2. An *arithmetical Krull monoid (an arithmetical formation)* consists of a triple $[D, H, |\cdot|]$ where $D = \mathcal{F}(P)$ is a free abelian monoid, $H \subseteq D$ a saturated submonoid with finite divisor class group G and a norm $|\cdot| : D \to \mathbb{N}$ satisfying the following axiom: for every $g \in G$

$$\sum_{p \in P \cap g} |p|^{-s} = \frac{1}{\#G} \log \frac{1}{s-1} + h_g(s)$$

where $h_g(s)$ is regular in the half-plane $\mathrm{Re}(s) \geq 1$ and in some neighborhood of $s = 1$.

Examples and Remarks. 1. Let K be an algebraic number field and R a holomorphy ring in K (e.g., the ring of algebraic integers in K). For every ideal $I \in \mathcal{I}(R)$ we set $|I| = \#(R/I)$. Then $|\cdot| : \mathcal{I}(R) \to \mathbb{N}$ is a norm function.

Let $\mathfrak{f}^* = \mathfrak{f}\omega_1 \ldots \omega_m$ be a cycle of R with $\mathfrak{f} \in \mathcal{I}(R)$, $m \geq 0$ and real embeddings $\omega_1, \ldots, \omega_m : K \to \mathbb{R}$. Let $\pi : R^\bullet \to (R/\mathfrak{f}^*)^\times$ denote the canonical epimorphism, $\Gamma \subseteq (R/\mathfrak{f}^*)^\times$ a subgroup and $H = \mathcal{H}_{\mathfrak{f}^*,\Gamma}(R)$ the reduced Hilbert monoid associated with $\mathfrak{f}^*$ and Γ (see chapter 2). Then Chebotarev's density theorem implies that

$$[\mathcal{I}_{\mathfrak{f}}(R),\ H,\ |\cdot|]$$

is an arithmetical Krull monoid (see [HK4; Proposition 3]).

2. Let K be an algebraic number field, R its ring of integers and $\mathfrak{o} \subseteq R$ an order with conductor $\mathfrak{f}$. For every $I \in \mathcal{I}_{\mathfrak{f}}(\mathfrak{o})$ we have $(\mathfrak{o} : I) = (R : IR)$ and hence $|\cdot| : \mathcal{I}_{\mathfrak{f}}(\mathfrak{o}) \to \mathbb{N}$ is a norm function. The embedding

$$\mathcal{H}_{\mathfrak{f}}(\mathfrak{o}) \hookrightarrow \mathcal{I}_{\mathfrak{f}}(\mathfrak{o})$$

is a divisor theory with divisor class group isomorphic to $\mathrm{Pic}(\mathfrak{o})$. Thus

$$[\mathcal{H}_{\mathfrak{f}}(\mathfrak{o}),\ \mathcal{I}_{\mathfrak{f}}(\mathfrak{o}),\ |\cdot|]$$

is an arithmetical Krull monoid (cf. [G-HK-K; Prop. 3 and Remark after Definition 4]).

3. Suppose that in the above definition we just require that the functions $h_g(s)$ are regular in the open half-plane $\mathrm{Re}(s) > 1$. Then examples **1.** and **2.** can be carried out not only in algebraic number fields but in global fields. However, the asymptotic results are weaker. Apart from this, further variants of the analytical axiom have been studied. However, all axioms are modelled on the concrete situation in algebraic number fields or algebraic function fields (in one variable over a finite constant field). The reader is referred to [G-HK-K] or [G-K].

Let $[D, H, |\cdot|]$ be an arithmetical formation. For a subset $Z \subseteq H$ let

$$Z(x) = \#\{a \in H \mid\ |a| \le x,\ a \in Z\}$$

denote the associated counting function. Quantitative theory of non-unique factorizations studies $Z(x)$ for subsets Z of arithmetical interest. We restrict ourselves to subsets Z which give information on sets of lengths. Among others, the following sets have been studied for every $k \in \mathbb{N}$

$$M_k(H) = M_k = \{a \in H \mid\ \max L(a) \le k\},$$
$$G_k = \{a \in H \mid \#L(a) \le k\}$$

and

$$P = \{a \in H \mid L(a) \text{ is an arithmetical progression with distance } 1\}.$$

We say a subset $L \subset \mathbb{Z}$ is an arithmetical progression with distance 1, if $L = \{x, x+1, \ldots, x+m\}$ for some $x \in \mathbb{Z}$ and $m \in \mathbb{N}_0$. Moreover, note that

$$M_1 = \{a \in H \mid a \text{ is irreducible}\}.$$

For all these sets Z, the asymptotic behaviour of $Z(x)$ is of the form

$$Z(x) \sim Cx(\log x)^{-A}(\log\log x)^B \qquad (*)$$

with $C \in \mathbb{R}_{>0}$, $0 \le A \le 1$ and $B \in \mathbb{N}_0$. As usual, $f \sim g$ for two real valued functions f and g means that

$$\lim_{x\to\infty} \frac{f(x)}{g(x)} = 1\,.$$

We give a brief outline of a proof of formula $(*)$. We do it in a manner which allows us to obtain combinatorial descriptions of the involved exponents A and B. We proceed in three steps.

a) Block monoids Due to the following lemma, it is sufficient to study the sets Z in the associated block monoid.

Lemma 4.2. *Let H be a Krull monoid with divisor class group G such that each class contains a prime divisor and let $\beta : H \to \mathcal{B}(G)$ denote the block homomorphism. Then for each set Z we have*

$$Z(H) = \beta^{-1}\big(Z\big(\mathcal{B}(G)\big)\big)$$

(i. e., $Z(H) = \{a \in H \mid \beta(a) \in Z\big(\mathcal{B}(G)\big)\}$).

Proof. This follows immediately from Lemma 3.2. □

b) Combinatorial part Let G be a finite abelian group and $Z = Z\big(\mathcal{B}(G)\big) \subseteq \mathcal{B}(G)$. Our aim is to reveal the structure of Z. For this we introduce the following combinatorial tool.

For a subset $Q \subseteq G$ and a function $\sigma : G \setminus Q \to \mathbb{N}_0$ we set

$$\Omega(Q,\sigma) = \{S \in \mathcal{F}(G) \mid v_g(S) = \sigma(g) \text{ for all } g \in G \setminus Q\}\,.$$

and

$$|\,\sigma\,| = \sum_{g\in G\setminus Q} \sigma(g) \in \mathbb{N}_0\,.$$

Lemma 4.4. *Let* $Z = M_k$ *or* $Z = G_k$ *for some* $k \in \mathbb{N}$. *Then there exist finitely many pairs* $(G_1, \sigma_1), \ldots, (G_r, \sigma_r)$ *such that*

$$Z = \bigcup_{i=1}^{r} \Omega(G_i, \sigma_i)\,. \qquad (**)$$

Further we have:

i) *the representation* $(**)$ *is unique.*

ii) *if* $Z = M_k$, *then* $G_1 = \cdots = G_r = \emptyset$.

iii) *if* $Z = G_k$, *then* $\Delta(G_1) = \cdots = \Delta(G_r) = \emptyset$.

Proof. The existence and uniqueness of the representation $(**)$ is proved in [HK4; Proposition 9].

ii) Suppose that $\Omega(G_0, \sigma_0) \subseteq M_k$. If $g \in G_0$, then $B = (g^{\mathrm{ord}(g)})^{k+1} \in \mathcal{B}(G) \cap \Omega(G_0, \sigma_0)$ but $B \notin M_k$. This shows that $G_0 = \emptyset$.

iii) Suppose that $\Omega(G_0, \sigma_0) \subseteq G_k$. If $\Delta(G_0) \neq \emptyset$, there exists some $B \in \mathcal{B}(G_0)$ with $\#L(B) \geq 2$. Thus $B^{k+1} \in \Omega(G_0, \sigma_0) \cap \mathcal{B}(G)$ but $B^{k+1} \notin G_k$. This shows that $\Delta(G_0) = \emptyset$. □

The previous result gives rise to the following definition.

Definition 4.5. Let G be a finite abelian group.

1. For every $k \in \mathbb{N}$ let $\mathcal{D}_k(G) = \sup\{\sigma(B) \mid B \in \mathcal{B}(G),\ \max L(B) \leq k\}$.
2. $\eta(G) = \max\{\#G_0 \mid \Delta(G_0) = \emptyset\}$.

Clearly, $\mathcal{D}_1(G) = \mathcal{D}(G)$ is just Davenport's constant of G. The next lemma gives information on the structure of the set P.

Lemma 4.6. *Let* $G' = G \setminus \{0\}$ *and* $A^* = \prod_{g \in G'} g$. *Then for all* $A \in \mathcal{B}(G)$ *with* $A^* \mid A$ *we have* $A \in P$ *i. e.,*

$$\mathcal{B}(G) \setminus P \subseteq \bigcup_{g \in G'} \Omega(G \setminus \{g\},\ \sigma_g)$$

with $\sigma_g : \{g\} \to \mathbb{N}_0$ *and* $\sigma_g(g) = 0$ *for all* $g \in G'$.

Proof. See [Ge9]. □

c) Analytical part The above combinatorial results show that it is sufficient to study the asymptotic behaviour of functions $\Omega(Q,\sigma)(x)$ in order to obtain results for $Z(x)$. A function of the form $\Omega(Q,\sigma)(x)$ was first investigated by P. Remond for algebraic number fields (for citations and historical remarks the reader is referred to Narkiewicz's book [Na2; chapter 9]). The main analytical tool for these investigations is a Tauberian theorem of Ikehara-Delange. For the proof of the following lemma, see [HK4; Proposition 10].

Lemma 4.7. *Let* $Q \subseteq G$ *be a subset and* $\sigma : G \setminus Q \to \mathbb{N}_0$ *a function with* $|\,\sigma\,| > 0$ *if* $Q = \emptyset$. *Then, for* x *tending to infinity,*

$$\#\{a \in D \,|\, \boldsymbol{\beta}(a) \in \Omega(Q,\sigma)\,,\ \ |\,a\,| \le x\} \sim Cx(logx)^{-\eta}(log\ logx)^d$$

where

$$\eta = \frac{\#(G \setminus Q)}{\#G} \quad \text{and} \quad d = \begin{cases} |\,\sigma\,| & Q \neq \emptyset \\ |\,\sigma\,| - 1 & Q = \emptyset\,. \end{cases}$$

Theorem 4.8. *Let* $[D, H, |\cdot|]$ *be an arithmetical Krull monoid. Then we have for every* $k \in \mathbb{N}$

1. $M_k(x) \sim Cx(logx)^{-1}(log\ logx)^{D_k(G)}$ *for some* $C \in \mathbb{R}_{>0}$.
2. $G_k(x) \sim C(logx)^{\frac{\eta(G)-\#G}{\#G}}(log\ logx)^B$ *for some* $C \in \mathbb{R}_{>0}$ *and some* $B \in \mathbb{N}_0$.
3. $P(x) = H(x) + O\big(\frac{x}{(\log x)^{1/\#G}}\big)$, *in particular*

$$\lim_{x\to\infty} \frac{P(x)}{H(x)} = 1.$$

Proof. See [HK3], [Ge3], [Ge2; Satz 2] and [G-K; Theorem 7]. □

5. COMBINATORIAL PROBLEMS IN ABELIAN GROUPS

In chapters 2 and 4, we discussed arithmetical questions in Krull domains and defined invariants which describe their arithmetic. As explained in chapter 3, all these notions depend solely on the divisor class group of the domain and the distribution of prime divisors in the divisor classes. This final chapter is devoted to the investigation

of these group theoretical constants. The resulting problems belong to the zero sum area, a part of additive group theory or combinatorial number theory.

Let G be an abelian group. We use additive notation throughout this section. Let $S = (g_1, \ldots, g_l)$ be a finite sequence of elements of G. Usually, one says that S is a *zero sequence*, if $\sum_{i=1}^{l} g_i = 0$ and that S is a *minimal zero sequence*, if $\sum_{i \in I} g_i \neq 0$ for each proper subset $\emptyset \neq I \subset \{1, \ldots, l\}$. To be consistent with the previous chapters, we view S as an element of the free abelian monoid $\mathcal{F}(G)$ and use multiplicative notation. Hence,

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

and $\sigma(S) = l$ denotes the number of elements of S. By definition, S is a zero sequence if and only if S is a block and S is a minimal zero sequence if and only if S is an irreducible block. We define

$$-S = \prod_{i=1}^{l} (-g_i) \ ,$$

and, for every subset $G_0 \subseteq G$ set $-G_0 = \{-g \,|\, g \in G_0\}$. The cyclic group of order $n \in \mathbb{N}$ will be denoted by C_n and

$$C_n = \{\overline{a} = a + n\mathbb{Z} \,|\, 0 < a < n\} = \{\overline{1}, \ldots, \overline{n-1}\} \ .$$

For a real number $x \in \mathbb{R}$ let $[x] \in \mathbb{Z}$ be the smallest integer $d \in \mathbb{Z}$ with $d \leq x$.

5.1 On $D_k(G)$

Throughout section 5.1, let G is a finite abelian group and suppose that $G = \bigoplus_{i=1}^{r} C_{n_i}$ where $n_1 \mid n_2 \mid \cdots \mid n_r$. Then n_r is the exponent of the group and r is the maximal p-rank of G. We call r the rank of G. If k is a positive integer, set

$$M_k(G) = \sum_{i=1}^{r-1} (n_i - 1) + kn_r$$

and $M_1(G) = M(G)$.

Proposition 5.1. *Let k be a positive integer and G be as above.*
1. $M_k(G) \le \mathcal{D}_k(G) \le k\mathcal{D}(G) \le kn_r(1 + \log \frac{\#G}{n_r})$.
2. *If $G_1 \subsetneq G$ is a proper subgroup, then $\mathcal{D}_k(G_1) < \mathcal{D}_k(G)$.*
3. *If $G = G' \oplus G''$, then $\mathcal{D}_k(G') + \mathcal{D}(G'') - 1 \le \mathcal{D}_k(G)$.*

Proof. The upper bound for $\mathcal{D}(G)$ was first shown in [E-K]. For a simplified proof see [A-G-P; Theorem 1.1]. Proofs of all other assertions may be found in [HK3]. □

Proposition 5.2. *Let k be a positive integer and G be as above.*
1. *If rank $r \le 2$, then $M_k(G) = \mathcal{D}_k(G)$.*
2. *If G is a p-group, then $M(G) = \mathcal{D}(G)$.*

Proof. The assertions for $\mathcal{D}(G)$ were derived independently by Olson and Kruyswijk (see [Ol] and [E-K]). Halter-Koch proved **1.** for arbitrary k in [HK3]. □

There are infinitely many groups of rank four with $M(G) < \mathcal{D}(G)$ (see [G-S]). It is still an open problem whether there are groups of rank three with $M(G) < \mathcal{D}(G)$. For recent results for groups of rank three the reader is referred to [Ga].

5.2 On $\Delta(G_0)$

Proposition 5.3. *Let G be a finite abelian group.*
1. *Let $\emptyset \ne G_0 \subseteq G$ be a subset. If $\mathcal{D}(G_0) \ge 3$, then $\Delta(G_0) \subseteq \{1, \ldots, \mathcal{D}(G_0) - 2\}$. If $G_0 = -G_0$, then $\{\mathrm{ord}(g) - 2 | g \in G, \mathrm{ord}(g) > 2\} \subseteq \Delta(G_0)$.*
2. *$\Delta(G) = \emptyset$ if and only if $\#G \le 2$. $\Delta(G) = \{1\}$ if and only if $G \in \{C_3, C_3^2, C_2^2\}$. In all other cases we have $\#\Delta(G) \ge 2$ and $1 = \min \Delta(G)$.*
3. *$\Delta(C_n) = \{1, \ldots, n-2\}$ for every $n \ge 3$.*

Proof. The proofs can be found in [Ge2; Proposition 3 and the Example prior to Proposition 4] and [G-K; Proposition 4]. □

Suppose that G is a torsion abelian group and $G_0 \subseteq G$ a subset. We say that G_0 is *half-factorial*, if $\Delta(G_0) = \emptyset$ (equivalently, the block monoid $\mathcal{B}(G_0)$ is half-factorial). Our first aim is to gather some

results on half-factorial subsets. For a sequence $S = g_1 g_2 \cdots g_t$ of elements in G we set

$$k(S) = \sum_{i=1}^{t} \frac{1}{\mathrm{ord}(g_i)}.$$

$k(S)$ is known as the *cross number of* S. For properties of this invariant and its relevance in factorization theory the reader is referred to [Ch] and [Ch-G].

The following result was obtained independently in both [Sk2; Theorem1] and [Z1; Proposition 1].

Proposition 5.4. *Let G be an abelian torsion group and $G_0 \subseteq G$. The following statements are equivalent:*

1. *G_0 is half-factorial.*

2. *$k(B) = 1$ for all irreducible blocks $B \in \mathcal{B}(G_0)$.*

Proof. Assume that $k(B) = 1$ for all irreducible blocks. If $U_1, \ldots, U_r$, $V_1, \ldots, V_s$ are irreducible blocks in $\mathcal{B}(G_0)$ and $U_1 \cdots U_r = V_1 \cdots V_s$, then $k(U_1 \cdots U_r) = k(V_1 \cdots V_s)$ implies that $r = s$.

Assume that $k(B) \neq 1$ for some irreducible block $B = g_1 \cdots g_l \in \mathcal{B}(G_0)$. Let $m = \mathrm{lcm}\{\mathrm{ord}(g_1), \ldots, \mathrm{ord}(g_l)\}$, $n_i \mathrm{ord}(g_i) = m$ and $U_i = g_i^{\mathrm{ord}(g_i)}$ be an irreducible block in $\mathcal{B}(G_0)$ for each $1 \leq i \leq l$. Since

$$k(B) = \frac{n_1 + \cdots + n_l}{m} \neq 1$$

we have

$$B^m = U_1^{n_1} \cdots U_l^{n_l}.$$

Thus B^m has factorizations of two different lengths. □

Proposition 5.5. *Let G be a direct sum of cyclic groups. Then there exists a half-factorial subset G_0 such that $\langle G_0 \rangle = G$.*

Proof. Since G is a free $\mathbb{Z}$-module, it has a basis G_0, which has the required property. □

The question of whether Proposition 5.5 holds for all abelian groups is still open. The arithmetical relevance of this problem lies in its combination with the realization theorems in section 3.2. Given an

abelian group G which is a direct sum of cyclic groups, Proposition 5.5 thus provides a half-factorial Dedekind domain with class group G. A discussion of some other classes of abelian groups for which the assertion of 5.5 holds can be found in [M-S].

Proposition 5.6. *Let n be a positive integer, p a prime and $G_0 \subseteq C_{p^n}$ a nonempty subset of C_{p^n}. Then G_0 is half-factorial if and only if there exists an automorphism φ of C_{p^n} such that $\varphi(G_0) \subseteq \{\overline{1}, \overline{p}, \ldots, \overline{p^{n-1}}\}$.*

Proof. See [Sk2; Prop. 3.4] and [Z1;Corollary 5]. □

We characterize small half-factorial subsets of cyclic groups.

Proposition 5.7. *Let n be a positive integer and $G_0 \subseteq C_n$ with $\overline{0} \notin G_0$.*

1. *Suppose $G_0 = \{a + n\mathbb{Z}, b + n\mathbb{Z}\}$ and set*

$$n_1 = \frac{n \gcd(a, b, n)}{\gcd(a, n) \gcd(b, n)}.$$

Then G_0 is half-factorial if and only if $n_1 \le 2$ or

$$\frac{a}{\gcd(a, n)} \equiv \frac{b}{\gcd(b, n)} \pmod{n_1}.$$

2. *Suppose $G_0 = \{\overline{1}, \overline{a}, \overline{b}\}$ with $1 \le a, b < n$. Then G_0 is half-factorial if and only if $a \mid n$ and $b \mid n$.*

Proof. The proof of 1. is [Ge1; Proposition 5]. For the proof of 2., see [Ch-S1; Theorem 3.8]. □

Example. There is no analogue for the case $\#G_0 = 4$. Consider $G = C_{30}$ and $G_0 = \{\overline{1}, \overline{6}, \overline{10}, \overline{15}\}$. If

$$B = \overline{15} \cdot \overline{10} \cdot \overline{10} \cdot \overline{6} \cdot \overline{6} \cdot \overline{6} \cdot \overline{6} \cdot \overline{1}$$

then $k(B) = 2$ and hence $\Delta(G_0) \neq \emptyset$ by Proposition 5.4 [Ch-S1, Example 11].

In chapter 4 we defined

$$\eta(G) = \max\{\#G_0 \,|\, G_0 \subseteq G, G_0 \text{ half-factorial}\}.$$

This invariant was first studied by J. Sliwa [Sl], and then by J. Kaczorowski and the first author. However, very little is known about $\eta(G)$. We restate one result from [G-K; section 13].

Proposition 5.8. *For a prime* p *and an integer* $r \in \mathbb{N}$ *we have*

$$1 + (r - 2[\frac{r}{2}]) + p[\frac{r}{2}] \leq \eta(C_p^r) \leq 1 + [p\frac{r}{2}] \ .$$

Next we study subsets G_0 of finite abelian groups G which are not half-factorial. As pointed out in section 2.2, a central point is to determine $\min \Delta(G_0)$. There is an algorithm for doing so [Ge1; Proposition 3].

Proposition 5.9. *Let* $G_0 = \{g_1, \ldots, g_m\} \subseteq G$ *where* G *is finite abelian and* $\Delta(G_0) \neq 0$. *Let* $B_1, B_2, \ldots, B_\psi$ *be the irreducible blocks in* $\mathcal{B}(G_0)$ *and suppose that* $d = \min \Delta(G_0)$. *Then* d *is the solution of the following linear, integral optimization problem: minimize*

$$\sum_{i=1}^{\psi} x_i$$

under the restrictions

$$\sum_{i=1}^{\psi} v_{g_j}(B_i) \cdot x_i = 0$$

for every $j \in \{1, \ldots, m\}$ *and*

$$\sum_{i=1}^{\psi} x_i > 0$$

where $x_i \in \mathbb{Z}$ *for every* $i \in \{1, \ldots, \psi\}$.

For a cyclic group G and $G_0 \subseteq G$ containing a generator, $\min \Delta(G_0)$ can be determined easily from the irreducible blocks in $\mathcal{B}(G_0)$ [Ge1; Proposition 7].

Proposition 5.10. *Let* $n \geq 3$ *and* $G_0 \subseteq C_n$ *a subset with* $\overline{1} \in G_0$ *and* $\Delta(G_0) \neq \emptyset$. *Then*

$$\min \Delta(G_0) = \gcd\{\frac{1}{n} \sum_{i=1}^{n-1} i \cdot v_{\overline{i}}(B) - 1 \,|\, \overline{0} \neq B \in \mathcal{B}(G_0) \text{ irreducible}\} \ .$$

Example. We consider some special cases of the last result.

i. $\min \Delta(\{\overline{1}, \overline{n-1}\}) = n-2$.

ii. If n is odd then,

a. $\min \Delta(\{\overline{1}, \overline{\frac{n+1}{2}}\}) = 1$.

b. $\min \Delta(\{\overline{1}, \overline{\frac{n-1}{2}}\}) = \frac{n-3}{2}$.

Alternate calculations for these values can be found in [Ch-S2; Theorem 4] and [Ch-S1; Theorems 4.5 and 4.6].

If in addition G_0 consists of only two elements, then there is an explicit formula for $\min \Delta(G_0)$ not involving irreducible blocks of $\mathcal{B}(G_0)$. This result is obtained by methods of diophantine approximation in [Ge1; Theorem 1].

Proposition 5.11. *Let $n \geq 3$, $a \in \{2, \ldots, n-1\}$ with $\gcd(a,n) = 1$ and $l \in \{1, \ldots, n-1\}$ such that $al + 1 \equiv 0 \pmod{n}$. Suppose the continued fraction expansion of $\frac{n}{l} = [a_0; a_1, \ldots, a_m]$. Then*

$$\min \Delta(\{\overline{1}, \overline{a}\}) = \gcd\{a-1, \frac{al+1}{n} - 1, a_0 - 1, a_2, \ldots, a_{2s}\}$$

where s is determined explicitely.

Proposition 5.3 indicates that for any finite abelian group G with $\#G \geq 3$ we have $\min \Delta(G) = 1$. The next result shows that, apart from very few exceptions, there are always subsets $G_0 \subseteq G$ with $\min \Delta(G_0) > 1$. The proof can be found in [Ch-S1; Corollary 4.14].

Proposition 5.12. *Let G be a non-trivial finite abelian group. Then there exists a nonempty subset $G_0 \subseteq G$ with $\min \Delta(G_0) > 1$ if and only if $G \notin \{C_2, C_3, C_2 \oplus C_2, C_3 \oplus C_3\}$.*

We close with a result on $\Delta_1(G)$. The proof can be found in [Ge1; Propositions 1 and 2].

Proposition 5.13. *Let G be a finite abelian group. Setting*

$$S = \{\min \Delta(G_0) \mid \emptyset \neq G_0 \subseteq G, \Delta(G_0) \neq \emptyset\}$$

we obtain

$$S \subseteq \Delta_1(G) \subseteq \{d \mid d | s \text{ for some } s \in S\}.$$

5.3 On $\mu_k(G)$

We freely use the elementary properties of $\mu_k(G)$ mentioned in section 2.2.

Proposition 5.14. *Let $k \in \mathbb{N}$ and G be a non-trivial finite abelian group.*

1. $\mu_{2k}(G) = kD(G)$.
2. $kD(G) + 1 \le \mu_{2k+1}(G) \le kD(G) + \left\lfloor \frac{D(G)}{2} \right\rfloor$.
3. $\mu_{2k-1}(G) + D(G) \le \mu_{2k+1}(G)$.
4. *Let $m \in \mathbb{N}$ such that*

$$\mu_{2m+1}(G) - mD(G) = \max\{\mu_{2r+1}(G) - rD(G) | r \in \mathbb{N}\}.$$

Then

$$\mu_{2m+2i+1}(G) = \mu_{2m+1}(G) + iD(G)$$

for all $i \ge 1$.

Proof. Set $G' = G \setminus \{0\} \neq \emptyset$ and let $U \in \mathcal{B}(G)$ be irreducible with $\sigma(U) = D(G)$.

For 1. and 2., we obviously have $\max L((-U)^k U^k) = kD(G)$ and hence $\mu_{2k}(G) \ge kD(G)$. Similarly, $\max L((-U)^k U^{k+1}) \ge kD(G)+1$ and thus $\mu_{2k+1}(G) \ge kD(G)+1$. To prove the remaining inequality, let $B \in \mathcal{B}(G')$ be given with $\min L(B) = \ell \in \{2k, 2k+1\}$. Then

$$2 \max L(B) \le \sigma(B) \le D(G) \min L(B) = \ell D(G)$$

implies

$$\max L(B) \le \left\lfloor \frac{\ell D(G)}{2} \right\rfloor.$$

For 3., let $B \in \mathcal{B}(G')$ with $\min L(B) \le 2k-1$ and $\max L(B) = \mu_{2k-1}(G)$. Then $\min L(B(-U)U) \le 2k+1$ and $\max L(B) \ge D(G) + \mu_{2k-1}(G)$. This implies $\mu_{2k+1}(G) \ge D(G) + \mu_{2k-1}(G)$.

For 4., induction on 3. implies that, for all $i \ge 1$,

$$\mu_{2m+2i+1}(G) \ge \mu_{2m+1}(G) + iD(G).$$

By definition of m we infer that

$$\mu_{2m+2i+1}(G) - (m+i)D(G) \le \mu_{2m+1}(G) - mD(G),$$

which implies the assertion. □

Part 1. above improves a result found in [Ch-S5; Lemma 4], where it is shown using different notation that $\mu_{2kD(G)}(G) = kD(G)^2$ for every integer $k \ge 1$. For elementary 2-groups we are able to explicitly compute $\mu_\ell(G)$ for all positive integers ℓ.

Proposition 5.15. *Let $G = C_2^r$ be an elementary 2-group of rank $r \ge 1$ and let $\ell \ge 2$. Then*

$$\mu_\ell(G) = \left[\frac{\ell D(G)}{2}\right].$$

Proof. By Proposition 5.14, the assertion holds if ℓ is even. So let ℓ be odd. Proposition 5.14 part 2. implies that $\mu_\ell(G) \le \left[\frac{\ell D(G)}{2}\right]$. By Proposition 5.14 part 4, it is sufficient to verify that

$$\mu_3(G) \ge D(G) + \left[\frac{D(G)}{2}\right].$$

Let $e_1, \ldots, e_r$ be a generating system of G and $e_0 = \sum_{i=1}^r e_i$. Note that by Proposition 5.2 we have $\mathcal{D}(G) = r + 1$. We give 3 irreducible blocks U_1, U_2 and U_3 such that

$$\max L(U_1U_2U_3) = D(G) + \left[\frac{D(G)}{2}\right].$$

Set $U_1 = \prod_{i=0}^r e_i$.

Case 1 Suppose $r = 2k + 1$. Then set

$$U_2 = \left(\prod_{i=1}^{k+1} e_i\right)\left(\prod_{i=1}^{k} e_i + e_{i+k+1}\right)\left(\sum_{i=k+1}^{2k+1} e_i\right)$$

and

$$U_3 = \left(\prod_{i=k+2}^{2k+1} e_i\right)\left(\prod_{i=1}^{k} e_i + e_{i+k+1}\right)\left(\sum_{i=k+1}^{2k+1} e_i\right) e_0.$$

Case 2 Suppose $r = 2k$. Then set

$$U_2 = \left(\prod_{i=1}^{k} e_i\right)\left(\prod_{i=1}^{k} e_i + e_{i+k}\right)\left(\sum_{i=k+1}^{2k} e_i\right)$$

and

$$U_3 = \left(\prod_{i=1}^{k} e_i + e_{i+k}\right)\left(\prod_{i=k+1}^{2k} e_i\right)\left(\sum_{i=1}^{k} e_i\right). \quad \square$$

Proposition 5.16. *Let G be a bounded abelian torsion group with exponent m and $G_0 \subseteq G$ a nonempty subset. Then $\mu_m(G_0) = m$ if and only if $\mu_k(G_0) = k$ for all positive integers k.*

Proof. Suppose that $\mu_k(G_0) \neq k$ for some integer k. Then by Proposition 5.4 there exists some irreducible block

$$B = \prod_{i=1}^{l} g_i \in \mathcal{B}(G_0)$$

with cross number $k(B) \neq 1$. Thus

$$B^m = \left(\prod_{i=1}^{l} g_i\right)^m = \prod_{i=1}^{l} \left(g_i^{\mathrm{ord}(g_i)}\right)^{\frac{m}{\mathrm{ord}(g_i)}}$$

where $m \neq mk(B)$, and hence $\mu_m(G_0) \neq m$. $\square$

In general, the exponent of the group is the minimal possible m such that the above result holds. This can be seen from the following example.

Example. Let $k \geq 4$ be given. Then there exists a finite abelian group G (depending on k) and a subset G_0 for which $\mu_k(G_0) = k$ but $\mu_{k+1}(G_0) \neq k+1$. The argument runs as follows.

Let $m > k+1$ and set $G = \oplus_{i=1}^{k} C_m$. If $e_1, \ldots, e_k$ is a $\mathbb{Z}$-module basis for G and $e_0 = -\sum_{i=1}^{k} e_i$, then $G_0 = \{e_1, \ldots, e_k, e_0\}$ has the required property (see [Ch-S3; Examples 2.6 - 2.9]).

In special cases, the value m obtained in Proposition 5.16 can be improved, as the following result demonstrates.

Proposition 5.17. *Suppose that* G *is a non-trivial finite abelian group and* $G_0 \subseteq G$ *a nonempty subset which satisfies any of the following conditions:*

1. $G = C_{p^n}$ *for* p *a prime integer and* n *a positive integer.*
2. $G = C_{pq}$ *for distinct prime integers* p *and* q *.*
3. $\#G \leq 15$ *.*
4. G *is cyclic and* G_0 *contains a generator.*

Then $\mu_2(G_0) = 2$ *if and only if* $\mu_k(G_0) = k$ *for all integers* $k \geq 1$ *.*

Proof. The proofs of 1., 2. and 3. are slight modifications of [Ch-S3; Theorem 3.2], [Ch-S3; Corollary 3.5] and [Ch-S4; Theorem 1]. For 4. see [Ch-S6; Theorem 1]. □

REFERENCES

[A-G-P] W.R. Alford, A. Granville and C. Pomerance, *There are infinitely many Carmichael numbers*, Ann. Math. **140**: 703–722 (1994).

[A-A-Z1] D.D. Anderson, D.F. Anderson and M. Zafrullah, *Factorization in integral domains*, J. Pure Applied Algebra **69**: 1-19 (1990).

[A-A-Z2] D.D. Anderson, D.F. Anderson and M. Zafrullah, *Rings between* $D[X]$ *and* $K[X]$, Houston J. Math. **17**: 109-129 (1991).

[A-A-Z3] D.D. Anderson, D.F. Anderson and M. Zafrullah, *Factorization in integral domains, II*, J. Algebra **152**: 78-93 (1992).

[An1] D. F. Anderson, *Elasticity of factorization in integral domains, a survey*, these Proceedings.

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

[Ch] S. Chapman, *On the Davenport's constant, the Cross number, and their application in factorization theory*, in Zero-dimensional commutative rings, Lecture Notes in Pure Appl. Math., Marcel Dekker **171**: 167–190 (1995).

[Ch-G] S. Chapman and A. Geroldinger, *On cross numbers of minimal zero sequences*, Australasian J. Comb. **14**: 85–92 (1996).

[Ch-S1] S. Chapman and W.W. Smith, *Factorization in Dedekind domains with finite class group*, Israel J. Math. **71**: 65–95 (1990).

[Ch-S2] S. Chapman and W.W. Smith, *On a characterization of algebraic number fields with class number less than three*, J. Algebra **135**: 381–387 (1990).

[Ch-S3] S. Chapman and W.W. Smith, *On the HFD, CHFD, and the k-HFD properties in Dedekind domains*, Comm. Algebra **20**: 1955–1987 (1992).

[Ch-S4] S. Chapman and W.W. Smith, *On the k-HFD property in Dedekind domains with small class group*, Mathematika **39**: 330–340 (1992).

[Ch-S5] S. Chapman and W.W. Smith, *On the lengths of factorizations of elements in an algebraic number ring*, J. Number Theory **43**: 24–30 (1993).

[Ch-S6] S. Chapman and W.W. Smith, *Finite cyclic groups and the k-HFD property*, Colloq. Math. **70**: 219–226 (1996).

[Cho] L. Chouinard, *Krull semigroups and divisor class groups*, Canad. J. Math. **19**: 1459–1468 (1981).

[E-K] P. van Emde Boas and D. Kruyswijk, *A combinatorial problem on finite abelian groups III*, Report ZW-1969-008, Math. Centre Amsterdam.

[Ga] W. Gao, *On Davenport's constant of finite abelian groups with rank three.*

[Ge1] A. Geroldinger, *On non-unique factorizations into irreducible elements II*, Coll. Math. Soc. J. Bolyai, Number Theory, Budapest **51**:723–757 (1987).

[Ge2] A. Geroldinger, *Über nicht-eindeutige Zerlegungen in irreduzible Elemente*, Math. Z. **197**: 505–529 (1988).

[Ge3] A. Geroldinger, *Ein quantitatives Resultat über Faktorisierungen verschiedener Länge in algebraischen Zahlkörpern*, Math. Z. **205**: 159–162 (1990).

[Ge4] A. Geroldinger, *Systeme von Längenmengen*, Abh. Math. Sem. Univ. Hamburg **60**: 115–130 (1990).

[Ge5] A. Geroldinger, *Arithmetical characterizations of divisor class group*, Arch. Math. **54**: 455–464 (1990).

[Ge6] A. Geroldinger, *On the arithmetic of certain not integrally closed noetherian integral domains*, Comm. Algebra **19**: 685–698 (1991).

[Ge7] A. Geroldinger, *Arithmetical characterizations of divisor class group II*, Acta Math. Univ. Comenianae **61**: 193–208 (1992).

[Ge8] A. Geroldinger, *T-block monoids and their arithmetical applications to certain integral domains*, Comm. Algebra **22**: 1603–1615 (1994).

[Ge9] A. Geroldinger, *Factorization of algebraic integers*, Springer Lecture Notes in Mathematics **1380**, 63–74.

[Ge10] A. Geroldinger, *The catenary degree and tameness of factorizations in weakly Krull domains*, these Proceedings.

[G-HK1] A. Geroldinger and F. Halter-Koch, *Realization theorems for semigroups with divisor theory*, Semigroup Forum **44**: 229–237 (1992).

[G-HK2] A. Geroldinger and F. Halter-Koch, *Arithmetical theory of monoid homomorphisms*, Semigroup Forum **48**: 333–362 (1994).

[G-HK-K] A. Geroldinger, F. Halter-Koch and J. Kaczorowski, *Non-unique factorizations in orders of global fields*, J. Reine Angew. Math. **459**: 89–118 (1995).

[G-K] A. Geroldinger and J. Kaczorowski, *Analytic and arithmetic theory of semigroups with divisor theory*, Sém. Théorie d. Nombres Bordeaux **4**: 199–238 (1992).

[G-L] A. Geroldinger and G. Lettl, *Factorization problems in semigroups*, Semigroup Forum **40**: 23–38 (1990).

[G-S] A. Geroldinger and R. Schneider, *On Davenport's constant*, J. Comb. Theory Series A **61**: 147-152 (1992).

[Gi] R. Gilmer, *Commutative semigroup rings*, The University of Chicago Press (1984).

[Gr] A. Grams, *The distribution of prime ideals of a Dedekind domain*, Bull. Austral. Math. Soc. **11**: 429–441 (1974).

[Gu] K. B. Gundlach, *Einführung in die Zahlentheorie*, B. I. Hochschultaschenbücher **Bd. 772** (1972).

[HK1] F. Halter-Koch, *Halbgruppen mit Divisorentheorie*, Expo. Math. **8**: 27–66 (1990).

[HK2] F. Halter-Koch, *Ein Approximationssatz für Halbgruppen mit Divisorentheorie*, Result. Math. **19**: 74–82 (1991).

[HK3] F. Halter-Koch, *A generalization of Davenport's constant and its arithmetical applications*, Colloq. Math. **63**: 203–210 (1992).

[HK4] F. Halter-Koch, *Chebotarev formations and quantitative aspects of non-unique factorizations*, Acta Arith. **62**: 173–206 (1992).

[HK5] F. Halter-Koch, *Finiteness theorems for factorizations*, Semigroup Forum **44**: 112–117 (1992).

[HK6] F. Halter-Koch, *The integral closure of a finitely generated monoid and the Frobenius problem in higher dimensions, Semigroups, edited by C. Bonzini, A. Cherubini and C. Tibiletti*, World Scientific (1993), 86 – 93.

[HK7] F. Halter-Koch, *A characterization of Krull rings with zero divisors*, Archivum Math. (Brno) **29**: 119–122 (1993).

[HK8] F. Halter-Koch, *Elasticity of factorizations in atomic monoids and integral domains*, J. Théorie des Nombres Bordeaux **7**: 367–385 (1995).

[HK9] F. Halter-Koch, *Finitely generated monoids, finitely primary monoids and factorization properties of integral domains*, these Proceedings.

[Hu] J. Huckaba, *Commutative rings with zero divisors*, Marcel Dekker (1988).

[Ja] N. Jacobson, *Basic Algebra I*, W. H. Freeman & Co. (1985).

[Kn] J. Knopfmacher, *Abstract Analytic Number Theory*, North-Holland, 1975.

[Kr] U. Krause, *On monoids of finite real character*, Proc. Amer. Math. Soc. **105**: 546-554 (1989).

[Le] G. Lettl, *Subsemigroups of fintely generated groups with divisor theory*, Mh. Math. **106**: 205–210 (1988).

[M-S] D. Michel and J. Steffan, *Répartition des idéaux premiers parmi les classes d'idéaux dans un anneau de Dedekind et équidécomposition*, J. Algebra **98**: 82–94 (1986).

[Na1] W. Narkiewicz, *Finite abelian groups and factorization problems*, Coll. Math **42**: 319–330 (1979).

[Na2] W. Narkiewicz, *Elementary and analytic theory of algebraic numbers*, Springer (1990).

[Ol] J. Olson, *A combinatorial problem on finite abelian groups I and II*, J. Number Theory **1**: 8–11, 195–199 (1969).

[Re] L. Rédei, *Theorie der endlich erzeugbaren kommutativen Halbgruppen*, Physica Verlag (1963).

[Sk1] L. Skula, *Divisorentheorie einer Halbgruppe*, Math. Z. **114**: 113–120 (1970).

[Sk2] L. Skula, *On c-semigroups*, Acta Arith. **31**: 247–257 (1976).

[Sl] J. Sliwa, *Remarks on factorizations in number fields*, Acta Arith. **46** (1982).

[Z1] A. Zaks, *Half-factorial domains*, Bull. Amer. Math. Soc. **82**: 721–723 (1976).

[Z2] A. Zaks, *Half factorial domains*, Isr. J. Math. **37**: 281–302 (1980).