Non-Unique Factorizations: A Survey

Alfred Geroldinger[1] and Franz Halter-Koch[2]

[1] Institut für Mathematik, Karl-Franzens-Universität Graz, Heinrichstrasse 36, 8010 Graz, Austria, alfred.geroldinger@uni-graz.at
[2] Institut für Mathematik, Karl-Franzens-Universität Graz, Heinrichstrasse 36, 8010 Graz, Austria, franz.halterkoch@uni-graz.at

1 Introduction

It is well known that the ring of integers of an algebraic number field may fail to have unique factorization. In the development of algebraic number theory in the 19th century, this failure led to Dedekind's ideal theory and to Kronecker's divisor theory. Only in the late 20th century, starting with L. Carlitz' result concerning class number 2, W. Narkiewicz began a systematic combinatorial and analytic investigation of phenomena of non-unique factorizations in rings of integers of algebraic number fields (see Chapter 9 of [24] for a survey of the early history of the subject). In the sequel several authors started to investigate factorization properties of more general integral domains in the spirit of R. Gilmer's book [18] (see for example the series of papers [2], [3], [4] and the survey article [19] by R. Gilmer). It soon turned out that the investigation of factorization problems can successfully be carried out in the setting of commutative cancellative monoids, and this point of view opened the door to further applications of the theory. Among them the most prominent ones are the arithmetic of congruence monoids, the theory of zero-sum sequences over abelian groups and the investigation of Krull monoids describing the deviation from the Krull-Remak-Schmidt Theorem in certain categories of modules.

The proceedings [1] and [6] of two Conferences on Factorization Theory (held 1996 in Iowa City and 2003 in Chapel Hill) and the articles contained in [7] give a good survey on the development of the theory of non-unique factorizations over the past decade. Only recently the authors completed the monograph [16] which contains a thorough presentation of the algebraic, combinatorial and analytic aspects of the theory of non-unique factorizations, together with self-contained introductions to additive group theory, to the theory of v-ideals and to abstract analytic number theory.

The purpose of this survey article is to point out some highlights of the theory of non-unique factorizations (Theorem 5.6.**B.** and Theorem 7.4) with an emphasis on the presentation of the concepts which describe the various

phenomena of non-uniqueness in structures of arithmetical relevance. We concentrate on the presentation of the main results and, if at all, we only give the main ideas of the proofs. For more details we refer the reader to the monograph [16] and to the original papers in the volumes cited above.

2 Notations and Preliminaries

Let $\mathbb{N}$ denote the set of positive integers and let $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$. For any set P let $|P| \in \mathbb{N}_0 \cup \{\infty\}$ denote the number of elements in P. For integers $a, b \in \mathbb{Z}$ we define $[a, b] = \{x \in \mathbb{Z} \mid a \le x \le b\}$.

By a semigroup we mean a commutative semigroup with a unit element, and by a monoid we mean a semigroup satisfying the cancellation law. Unless stated otherwise, we use multiplicative notation and denote the unit element by 1. (Semigroup) homomorphisms are always assumed to respect the unit element. For a monoid H, we denote by $H^\times$ the set of invertible elements of H and by $H_{\red} = \{aH^\times \mid a \in H\}$ the associated reduced monoid of H. We say that H is reduced if $H^\times = \{1\}$. We denote by $\mathsf q(H)$ a quotient group of H. Let $S \subset H$ be a submonoid. We tacitly assume that $\mathsf q(S) \subset \mathsf q(H)$, and for $a \in \mathsf q(H)$ we denote by $[a] = [a]_{H/S} = a\,\mathsf q(S) \in \mathsf q(H)/\mathsf q(S)$ the class containing a. We set $H/S = \{[a] \mid a \in H\} \subset \mathsf q(H)/\mathsf q(S)$, and if $aH \cap S \ne \emptyset$ for all $a \in H$, then $H/S = \mathsf q(H)/\mathsf q(S)$ (this condition is fulfilled throughout the present article).

For $a, b \in H$, we write as usual $a \,|\, b$ (in H) if $b \in aH$, and $a \simeq b$ if $a \,|\, b$ and $b \,|\, a$ (equivalently, $aH^\times = bH^\times$). A submonoid $S \subset H$ is called *divisor-closed* if $a \in S$, $b \in H$ and $b \,|\, a$ implies that $b \in S$.

An element $x \in \mathsf q(H)$ is called *almost integral* over H if there exists some $c \in H$ such that $cx^n \in H$ for all $n \in \mathbb{N}$. The set $\widehat H$ of all elements of $\mathsf q(H)$ which are almost integral over H is a monoid, called the *complete integral closure* of H. The monoid H is called *completely integrally closed* if $\widehat H = H$. This definition coincides with the corresponding concept in commutative ring theory (note that the stronger concept of integral elements has no purely multiplicative analog).

For two semigroups H_1, H_2, we denote by $H_1 \times H_2$ their direct product, and we view H_1 and H_2 as subsemigroups of $H_1 \times H_2$. Thus every $a \in H_1 \times H_2$ has a uniquely determined decomposition $a = a_1 a_2$ with $a_1 \in H_1$ and $a_2 \in H_2$.

A monoid F is called *free* (*with basis* $P \subset F$) if every $a \in F$ has a unique representation in the form

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

In this case F is (up to canonical isomorphism) uniquely determined by P (and conversely P is uniquely determined by F). We set $F = \mathcal F(P)$, and if a is as in $(*)$, then we call

$$|a| = \sum_{p \in P} \mathsf{v}_p(a) \quad \text{the } \textit{length} \text{ of } a\,.$$

For every map $\varphi_0 \colon P \to S$ into a semigroup S there is a unique homomorphism $\varphi \colon \mathcal{F}(P) \to S$ such that $\varphi \,|\, P = \varphi_0$.

For a monoid H, we consider the v-operation and the theory of v-ideals as explained in [16, Chapter 2] or in [21, Section 11]. A monoid H is v-noetherian if it satisfies the ascending chain condition on v-ideals.

Integral domains are in the center of our interest. If R is an integral domain, then $R^\bullet = R \setminus \{0\}$ is a multiplicative monoid, and a subset $\mathfrak{a} \subset R^\bullet$ is a v-ideal of $R^\bullet$ if and only if $\mathfrak{a} \cup \{0\}$ is a divisorial ideal of R. In particular, $R^\bullet$ is v-noetherian if and only if R is a Mori domain.

We study the (multiplicative) arithmetic of an integral domain R by means of the monoid $R^\bullet$, and we attribute a factorization property or an invariant connected with factorizations to R if and only if it holds for $R^\bullet$.

Throughout this paper, let H be a monoid.

An element $a \in H$ is called

- an *atom* (or an irreducible element) if $a \notin H^\times$ and, for all $b, c \in H$, $a = bc$ implies $b \in H^\times$ or $c \in H^\times$. We denote by $\mathcal{A}(H)$ the set of all atoms of H.
- a *prime* (or a prime element) if $a \notin H^\times$ and, for all $b, c \in H$, $a \,|\, bc$ implies $a \,|\, b$ or $a \,|\, c$.

The monoid H is called

- *atomic* if every $a \in H \setminus H^\times$ is a product of atoms.
- *factorial* if it satisfies one of the following equivalent conditions:
  1. Every $a \in H \setminus H^\times$ is a product of primes.
  2. H is atomic, and every atom is a prime.
  3. Every $a \in H \setminus H^\times$ is a product of atoms, and this factorization is unique up to associates and the order of the factors.
  4. $H_{\red}$ is free (in that case $H_{\red}$ is free with basis $\{pH^\times \mid p \in P\}$ where P denotes the set of primes of H).
  5. $H = H^\times \times \mathcal{F}(P)$ for some subset $P \subset H$ (in that case P is a maximal set of pairwise non-associated primes of H).

Every prime is an atom, and every factorial monoid is atomic. An element $a \in H$ is an atom [a prime] of H if and only if $aH^\times$ is an atom [a prime] of $H_{\red}$. Thus $H_{\red}$ is atomic [factorial] if and only if H has this property. In a factorial monoid, every non-empty subset has a greatest common divisor which is uniquely determined up to associates.

By our convention, an integral domain R is atomic [factorial] if and only if $R^\bullet$ has this property, and these definitions coincide with the usual ones in commutative ring theory.

In the theory of non-unique factorizations we describe the deviation of a monoid from being factorial. For this, we have to formalize the notion of a factorization into irreducibles (see Definition 3.1 below). Having a precise notion of the set of all factorizations, we are able to investigate its structure. Since invertible elements play no role in the theory of factorizations, the reduced monoid $H_{\red}$ and not the monoid H itself is the basis for our definitions.

3 Arithmetic of monoids

In this section we present the concepts by which we describe the phenomena of non-unique factorizations.

Sets of Factorizations. The free monoid $\mathsf Z(H) = \mathcal F\big(\mathcal A(H_{\red})\big)$ is called the *factorization monoid* of H, and the unique homomorphism

$$\pi\colon \mathsf Z(H) \to H_{\red} \quad \text{satisfying} \quad \pi(u) = u \quad \text{for all} \quad u \in \mathcal A(H_{\red})$$

is called the *factorization homomorphism* of H. For $a \in H$, the set

$$\mathsf Z(a) = \pi^{-1}(aH^\times) \subset \mathsf Z(H) \quad \text{is the } \textit{set of factorizations} \text{ of } a.$$

Note that an element of $\mathsf Z(a)$ represents a naive factorization of a into atoms, where the order of the factors and the choice of the factors among associates is disregarded. An element $a \in H$ is said to have unique factorization if $|\mathsf Z(a)| = 1$. By definition, we have $\mathsf Z(a) = \{1\}$ for all $a \in H^\times$. The monoid H is atomic if and only if $\mathsf Z(a) \ne \emptyset$ for all $a \in H$, and H is factorial if and only if $|\mathsf Z(a)| = 1$ for all $a \in H$.

Sets of Lengths and distances. For $a \in H$, we call

$$\mathsf L(a) = \big\{|z| \bigm| z \in \mathsf Z(a)\big\} \subset \mathbb N_0 \quad \text{the } \textit{set of lengths} \text{ of } a\,.$$

We denote by $\Delta\big(\mathsf L(a)\big)$ the set of all $d \in \mathbb N$ for which there exists some $m \in \mathsf L(a)$ with $[m, m+d] \cap \mathsf L(a) = \{m,\, m+d\}$ (that is, $\Delta\big(\mathsf L(a)\big)$ is the set of all successive distances in sets of lengths of factorizations of a).

The system of sets of lengths and the set of distances of H are defined by

$$\mathcal L(H) = \big\{\mathsf L(a) \bigm| a \in H\big\} \quad \text{and} \quad \Delta(H) = \bigcup_{a \in H} \Delta\big(\mathsf L(a)\big)\,.$$

We denote by $\Delta^*(H)$ the set of all $d = \min \Delta(S)$ for some divisor-closed submonoid $S \subset H$ for which $\Delta(S) \ne \emptyset$. The set $\Delta^*(H)$ is a subset of $\Delta(H)$

which (among others) is of importance for the Structure Theorem for Sets of Lengths cited below.

The monoid H is called *half-factorial* if $|\mathsf{L}(a)| = 1$ for all $a \in H$, and it is called a BF-*monoid* if $\mathsf{L}(a)$ is finite and non-empty for all $a \in H$.

By definition, H is atomic if and only if $\mathsf{L}(a) \neq \emptyset$ for all $a \in H$, and H is half-factorial if and only if H is atomic and $\Delta(H) = \emptyset$. Every factorial monoid is half-factorial, every half-factorial monoid is a BF-monoid, and every BF-monoid is atomic. Every v-noetherian monoid is a BF-monoid (this requires some ideal-theoretic effort). In particular, every Mori domain is a BF-domain.

Distance of factorizations. Let $z, z' \in \mathsf{Z}(H)$, say

$$z = u_1 \cdot \ldots \cdot u_l v_1 \cdot \ldots \cdot v_m \quad \text{and} \quad z' = u_1 \cdot \ldots \cdot u_l w_1 \cdot \ldots \cdot w_n \,,$$

where $l, m, n \in \mathbb{N}_0$, $u_1, \ldots, u_l, v_1, \ldots, v_m, w_1, \ldots, w_n \in \mathcal{A}(H_{\red})$ and

$$\{v_1, \ldots, v_m\} \cap \{w_1, \ldots, w_n\} = \emptyset \,.$$

Then we call $\mathsf{d}(z, z') = \max\{m, n\} \in \mathbb{N}_0$ the *distance* of z and z'.

It is easily checked that the distance function $\mathsf{d}\colon \mathsf{Z}(H) \times \mathsf{Z}(H) \to \mathbb{N}_0$ is a metric satisfying $\mathsf{d}(xz, xz') = \mathsf{d}(z, z')$ for all $x, z, z' \in \mathsf{Z}(H)$.

If H fails to be factorial (resp. half-factorial), then there exist elements with arbitrary many distinct factorizations (resp. lengths) as the following lemma shows.

Lemma 3.1 *Let H be atomic.*

1. *If H is not factorial, then for every $k \in \mathbb{N}$ there exists some $a \in H$ such that $|\mathsf{Z}(a)| \ge k + 1$, and there exist factorizations $z, z' \in \mathsf{Z}(a)$ such that $\mathsf{d}(z, z') \ge 2k$.*
2. *If H is not half-factorial, then for every $k \in \mathbb{N}$ there exists some $a \in H$ such that $|\mathsf{L}(a)| \ge k + 1$.*

Proof. We may suppose that H is reduced, and we present a proof of the first assertion (the second one follows by similar simple arguments).

If H is not factorial, then there exists some $c \in H$ such that $|\mathsf{Z}(c)| > 1$. If $z, z' \in \mathsf{Z}(c)$ are distinct and $k \in \mathbb{N}$, then $\mathsf{Z}(c^k) \supset \{z^{k-i} z'^i \mid i \in [0, k]\}$. Hence $|\mathsf{Z}(c^k)| \ge k + 1$ and $\mathsf{d}(z^k, z'^k) = k\mathsf{d}(z, z') \ge 2k$. □

Sets of lengths are the best understood invariants of non-unique factorizations. Under suitable finiteness conditions (which are satisfied for orders in algebraic number fields, see Example 5.9) they are almost arithmetical multiprogressions with bounded parameters. We are going to describe this structure.

Almost Arithmetical Multiprogressions. Let $M \in \mathbb{N}$, $d \in \mathbb{N}$ and $\{0, d\} \subset \mathcal{D} \subset [0, d]$. A finite non-empty subset $L \subset \mathbb{Z}$ is called an *almost arithmetical multiprogression* (AAMP *for short*) *with difference* d, *period* $\mathcal{D}$ *and bound* M if there exists some $y \in \mathbb{Z}$ such that

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

with $L^* = (\mathcal{D} + d\mathbb{Z}) \cap [0, \max L^*]$, $L' \subset [-M, -1]$ and $L'' \subset \max L^* + [1, M]$. We call y the shift parameter, L^* the central part, L' the initial part and L'' the end part of the AAMP L.

The Structure Theorem for Sets of Lengths. We say that *the Structure Theorem for Sets of Lengths holds for* H if H is atomic and there exists some $M^* \in \mathbb{N}$ such that every $L \in \mathcal{L}(H)$ is an AAMP with some difference $d \in \Delta^*(H)$ and bound M^*.

For half-factorial monoids, the Structure Theorem for Sets of Lengths holds in a trivial way. If H is not half-factorial and the Structure Theorem for Sets of Lengths holds for H, then H is a BF-monoid and has arbitrarily large sets of lengths (by Lemma 3.1), but all these sets of lengths have bounded initial and end parts, and thus they have arbitrarily large central part.

Catenary degree. Let $z, z' \in \mathsf{Z}(H)$ and $N \in \mathbb{N}_0 \cup \{\infty\}$. We say that z and z' can be *concatenated by an* N*-chain* if there exists a finite sequence of factorizations $z = z_0, z_1, \ldots, z_k = z'$ in $\mathsf{Z}(a)$ such that $\mathsf{d}(z_{i-1}, z_i) \le N$ for all $i \in [1, k]$.

For an element $a \in H$, we define its *catenary degree* $\mathsf{c}(a)$ to be the smallest $N \in \mathbb{N}_0 \cup \{\infty\}$ such that any two factorizations of a can be concatenated by an N-chain, and we call

$$\mathsf{c}(H) = \sup\{\mathsf{c}(a) \mid a \in H\} \in \mathbb{N}_0 \cup \{\infty\} \quad \text{the } \textit{catenary degree} \text{ of } H.$$

The catenary degree $\mathsf{c}(a)$ measures how complex the set of factorizations of a is. Note that by definition we have either $\mathsf{c}(a) = 0$ or $\mathsf{c}(a) \ge 2$. In the following Lemma 3.2 (whose proof is straightforward) we list the basic properties of the catenary degree.

Lemma 3.2 *Let* H *be atomic and* $a \in H$.

1. *a has unique factorization if and only if $\mathsf{c}(a) = 0$. In particular, H is factorial if and only if $\mathsf{c}(H) = 0$.*
2. *If $\mathsf{c}(a) \le 2$, then $|\mathsf{L}(a)| = 1$. In particular, if $\mathsf{c}(H) \le 2$, then H is half-factorial.*
3. *If $|\mathsf{L}(a)| \ge 2$, then $2 + \sup \Delta\big(\mathsf{L}(a)\big) \le \mathsf{c}(a)$. In particular, if $\mathsf{c}(H) < \infty$, then $\Delta(H)$ is finite.*
4. *If $\mathsf{c}(a) \le 3$, then $\Delta\big(\mathsf{L}(a)\big) \subset \{1\}$, whence $\mathsf{L}(a) = [y, y + k]$ for some $y, k \in \mathbb{N}_0$.*

Tame degree and local tameness. For a factorization $x \in \mathsf{Z}(H)$ and $a \in H$ we define the *tame degree* $\mathsf{t}(a,x)$ to be the smallest $N \in \mathbb{N}_0 \cup \{\infty\}$ with the following property:

> If $\mathsf{Z}(a) \cap x\mathsf{Z}(H) \neq \emptyset$ and $z \in \mathsf{Z}(a)$, then there exists some factorization $z' \in \mathsf{Z}(a) \cap x\mathsf{Z}(H)$ such that $\mathsf{d}(z,z') \le N$.

We define $\mathsf{t}(H,x) = \sup\{\mathsf{t}(a,x) \mid a \in H\}$, and for a subset $X \subset \mathsf{Z}(H)$ we define $\mathsf{t}(a,X) = \sup\{\mathsf{t}(a,x) \mid x \in X\}$.

The monoid H is called *locally tame* if $\mathsf{t}(H,u) < \infty$ for all $u \in \mathcal{A}(H_{\red})$.

Local tameness is a basic finiteness property in factorization theory. In most settings, where the finiteness of some arithmetical invariant is derived, local tameness has to be proved first. In particular, local tameness is an essential tool in the proof of the Structure Theorem for Sets of Lengths.

4 Zero-sum sequences over abelian groups

Let G be an additive abelian group, $G_0 \subset G$ and $\mathcal{F}(G_0)$ the free (abelian, multiplicative) monoid with basis G_0. According to the tradition of combinatorial number theory, the elements of $\mathcal{F}(G_0)$ are called *sequences over* G_0. If $S \in \mathcal{F}(G_0)$, then

$$S = g_1 \cdot \ldots \cdot g_l = \prod_{g \in G_0} g^{\mathsf{v}_g(S)},$$

where $\mathsf{v}_g(S)$ is the g-adic value of S (also called the *multiplicity of g in S*), and $\mathsf{v}_g(S) = 0$ for all $g \in G_0 \setminus \{g_1, \ldots, g_l\}$. Then $|S| = l$ is the *length of S*. We call $\supp(S) = \{g_1, \ldots, g_l\}$ the *support* and $\sigma(S) = g_1 + \ldots + g_l$ the *sum* of S. The monoid

$$\mathcal{B}(G_0) = \{S \in \mathcal{F}(G_0) \mid \sigma(S) = 0\} = \mathcal{B}(G) \cap \mathcal{F}(G_0)$$

is called the *block monoid* over G_0. It is a divisor-closed submonoid of $\mathcal{B}(G)$. The elements of $\mathcal{B}(G_0)$ are called *zero-sum sequences* over G_0. The monoid $\mathcal{B}(G_0)$ is a BF-monoid, and the atoms of $\mathcal{B}(G_0)$ are the minimal zero-sum sequences (that is, zero-sum sequences without a proper zero-sum subsequence). If G_0 is finite, then the Structure Theorem for Sets of Lengths holds for $\mathcal{B}(G_0)$ (see Theorem 5.6.**B.**).

For every arithmetical invariant $*(D)$ defined for a monoid D, we write $*(G_0)$ instead of $*(\mathcal{B}(G_0))$. Hence $\mathcal{A}(G_0) = \mathcal{A}(\mathcal{B}(G_0))$, $\mathcal{L}(G_0) = \mathcal{L}(\mathcal{B}(G_0))$, $\Delta(G_0) = \Delta\big(\mathcal{B}(G_0)\big)$, $\mathsf{c}(G_0) = \mathsf{c}(\mathcal{B}(G_0))$ and so on.

A sequence is called *zero-sumfree* if it contains no non-empty zero-sum subsequence. Clearly, a sequence S is zero-sumfree if and only if the sequence $(-\sigma(S))S$ is a minimal zero-sum sequence. The investigation of the structure and length of zero-sum sequences and of zero-sumfree sequences with extremal

properties is a main topic in additive group theory. In this area there is a wealth of classical and still wide open questions (see [12] for a recent survey).

We recall the definition of two central invariants of finite abelian groups and discuss their arithmetical significance (Theorem 4.2). If G is a finite abelian group, then $\mathcal{A}(G)$ is finite and thus $\mathcal{B}(G)$ is a finitely generated monoid.

Definition 4.1 Let G be a finite abelian group. Then

$$\mathsf{D}(G) = \max\big\{|S| \;\big|\; S \in \mathcal{A}(G)\big\}$$

is called the *Davenport constant* of G. It is the smallest integer $l \in \mathbb{N}$ such that every sequence $S \in \mathcal{F}(G)$ of length $|S| \ge l$ has a non-empty zero-sum subsequence. For a sequence $S \in \mathcal{F}(G)$, we define its *cross number* by

$$\mathsf{k}(S) = \sum_{i=1}^{l} \frac{1}{\mathrm{ord}(g_i)}, \quad \text{and} \quad \mathsf{k}(G) = \max\{\mathsf{k}(S) \mid S \in \mathcal{F}(G) \ \text{ is zero-sumfree}\}$$

is called the (*little*) *cross number* of G.

In general, the precise values of $\mathsf{D}(G)$ and $\mathsf{k}(G)$ (in terms of the group invariants of G) are unknown. Among others, both $\mathsf{D}(G)$ and $\mathsf{k}(G)$ are known for p-groups, and $\mathsf{D}(G)$ is also known for cyclic groups and for groups of rank 2. For every finite abelian group G we have $\mathsf{D}(G) \le |G|$, and equality holds if and only if G is cyclic. A straightforward argument shows that

$$\mathsf{D}(G) = 2 \max\Big\{\frac{\max L}{\min L} \;\Big|\; L \in \mathcal{L}(G)\Big\} = \max\{\max L \mid L \in \mathcal{L}(G)\,,\ 2 \in L\}\,.$$

In order to investigate sets of lengths $L \in \mathcal{L}(G)$ with $\{2, \mathsf{D}(G)\} \subset L$ it is necessary to know the structure of minimal zero-sum sequences $S \in \mathcal{A}(G)$ of maximal length $|S| = \mathsf{D}(G)$.

It is conjectured that (apart from some explicitly known exceptions) a finite abelian group G is uniquely determined by the system of sets of lengths $\mathcal{L}(G)$. Up to now, this conjecture could only be verified for special classes of groups (including cyclic groups). Again, any progress concerning this problem heavily depends on the knowledge of the Davenport constant and of the structure of minimal zero-sum sequences of maximal length. It is worth mentioning that, in contrast to this conjecture, for any infinite abelian group G the system $\mathcal{L}(G)$ contains all finite non-empty subsets of $\mathbb{N}_{\ge 2}$ regardless of the structure of G (see [22]).

A subset G_0 of an abelian group G is called half-factorial if the monoid $\mathcal{B}(G_0)$ is half-factorial. Half-factorial subsets (and minimal non-half-factorial subsets as their counterparts) play a crucial role in the investigations of $\Delta^*(G)$ (see Theorem 4.2.3) and in some problems of the analytic theory of non-unique

factorizations (see Theorem 7.4). A recent survey of results concerning the structure and cardinality of half-factorial subsets was given by W.A. Schmid [26].

A classical criterion (due to A. Zaks and L. Skula) states that a subset G_0 of a finite abelian group G is half-factorial if and only if $\mathsf{k}(S) = 1$ for all $S \in \mathcal{A}(G_0)$.

Theorem 4.2 *Let G be a finite abelian group with $|G| \ge 3$, say*

$$G = C_{n_1} \oplus \ldots \oplus C_{n_r}\,, \quad \text{where } 1 < n_1 \,|\, \ldots \,|\, n_r = n\,, \quad \text{and} \quad k = \sum_{i=1}^{r} \Big\lfloor \frac{n_i}{2} \Big\rfloor\,.$$

1. *We have $\big[1, \max\{n-2,\, k-1\}\big] \subset \Delta(G) \subset \big[1, \mathsf{c}(G) - 2\big]$. In particular, $\min \Delta(G) = 1$, and both $\Delta(G)$ and $\mathsf{c}(G)$ grow with the exponent and with the rank of G.*
2. *$\mathsf{c}(G) \le \mathsf{D}(G)$, and equality holds if and only if G is cyclic or an elementary 2-group.*
3. *$\max \Delta^*(G) \le \max\{n-2,\, 2\mathsf{k}(G) - 1\}$, and if $|G| \le \max\{\mathsf{e}^{n/2},\, n^2\}$, then $\max \Delta^*(G) = n - 2$.*

For the proof of Theorem 4.2 we refer to [13], [25] and to [16]. Recall that $\mathsf{c}(G)$ measures how complex the set of factorizations of a zero-sum sequence $S \in \mathcal{B}(G)$ may be. Thus Theorem 4.2 asserts that this set of factorizations may become the more complex the larger G is. In contrast to that, the following Theorem 4.3 shows that (in a precise sense) "almost all" zero-sum sequences over a finite abelian group have catenary degree $\mathsf{c}(S) \le 3$. A similar quantitative result holds for factorizations of algebraic integers (see Theorem 7.4).

Theorem 4.3 *Let G be a finite abelian group.*

1. *Every sequence $S \in \mathcal{B}(G)$ for which $\mathrm{supp}(S) \cup \{0\} \subset G$ is a subgroup has catenary degree $\mathsf{c}(S) \le 3$.*
2. *For every $A \in \mathcal{B}(G)$ with $\mathrm{supp}(A) = G$ we have*

$$\frac{\big|\big\{S \in A\,\mathcal{B}(G) \;\big|\; |S| \le N\big\}\big|}{\big|\big\{S \in \mathcal{B}(G) \;\big|\; |S| \le N\big\}\big|} = 1 + O\Big(\frac{1}{N}\Big) \quad \text{for all} \quad N \in \mathbb{N}\,.$$

In particular,

$$\frac{\big|\big\{S \in \mathcal{B}(G) \;\big|\; \mathsf{c}(S) \le 3\,,\; |S| \le N\big\}\big|}{\big|\big\{S \in \mathcal{B}(G) \;\big|\; |S| \le N\big\}\big|} = 1 + O\Big(\frac{1}{N}\Big) \quad \text{for all} \quad N \in \mathbb{N}\,.$$

While the proof of the second assertion in Theorem 4.3 is carried out by a simple counting argument, the proof of the first one needs deep methods from additive group theory and occupies about 30 pages in [16].

5 Krull monoids and C-monoids

Let D be a factorial monoid and $H \subset D$ a submonoid. If H is "not too far" from D, then we can investigate the arithmetic of H by means of the unique factorization in D. The distance between H and D is measured by the notions of class groups and class semigroups (note that this in accordance with the philosophy that "the class group measures the deviation from being factorial"). Krull monoids and C-monoids are the most important classes of monoids which are investigated in this way.

Definition 5.1 (Krull monoids)

1. Let D be a monoid and $H \subset D$ a submonoid. Then $H \subset D$ is called *saturated* if $\mathsf{q}(H) \cap D = H$ (that is, if $a, b \in H$ and a divides b in D, then a divides b in H).
2. H is called a *Krull monoid* if $H_{\red}$ is a saturated submonoid of a free monoid.
3. Let H be a Krull monoid and suppose that $H_{\red} \subset D = \mathcal{F}(P)$ is a saturated submonoid of a free monoid such that every $p \in P$ is the greatest common divisor of finitely many elements of $H_{\red}$. Then we call D a monoid of *divisors* and P a set of *prime divisors* of H.
   Every Krull monoid possesses a monoid of divisors, and if D and D' are monoids of divisors of H, then there is a unique isomorphism $\Phi\colon D \to D'$ with $\Phi \,|\, H_{\red} = \id$. Hence the *class group*
   $$\mathcal{C}(H) = D/H_{\red} \quad \text{and the subset} \quad \{[p] \in \mathcal{C}(H) \mid p \in P\}$$
   of all classes containing primes are uniquely determined by H (up to canonical isomorphism).

The arithmetic of a Krull monoid is uniquely determined by its class group and the distribution of primes in the classes (for a precise statement see Theorem 6.6). In particular, a monoid is factorial if and only if it a Krull monoid with trivial class group. By definition, H is a Krull monoid if and only if $H_{\red}$ is a Krull monoid, and $\mathcal{C}(H) = \mathcal{C}(H_{\red})$.

In the following proposition we present (without proofs) several ideal-theoretic characterizations of Krull monoids (some of them are in accordance with the well-known characterizations of Krull domains). Full proofs can be found in [21] or [16].

Proposition 5.2 *Then the following statements are equivalent*:

1. *H is a Krull monoid.*
2. *$H_{\red}$ is a Krull monoid, and $H = H^\times \times H_0$ for some submonoid H_0 of H with $H_0 \cong H_{\red}$.*

3. *H is v-noetherian and completely integrally closed.*
4. *H is v-noetherian and every non-empty v-ideal of H is v-invertible.*

From the v-ideal theory of a Krull monoid H a monoid of divisors is obtained as follows. The monoid $\mathcal{I}_v^*(H)$ of all non-empty v-ideals, equipped with the v-multiplication, is a free monoid, and the set $\mathfrak{X}(H)$ of all v-maximal v-ideals is a basis of $\mathcal{I}_v^*(H)$. If we identify $H_{\red}$ with the set of all principal ideals of H in the natural way, then $H_{\red} \subset \mathcal{I}_v^*(H)$, the monoid $\mathcal{I}_v^*(H)$ is a monoid of divisors of H, and $\mathfrak{X}(H)$ is a set of prime divisors of H.

Examples 5.3 (Examples of Krull monoids)

1. *Block monoids.* Let G be an abelian group and $G_0 \subset G$ a subset. Then the block monoid $\mathcal{B}(G_0)$ is a saturated submonoid of $\mathcal{F}(G_0)$, and thus it is a Krull monoid. It can even be proved that every reduced Krull monoid is isomorphic to a block monoid over a suitable subset of some abelian group.

If $|G| \le 2$, then the block monoid $\mathcal{B}(G)$ is factorial, and if $|G| \ge 3$, then $\mathcal{F}(G)$ is a monoid of divisors of $\mathcal{B}(G)$, $\mathcal{C}\big(\mathcal{B}(G)\big) \cong G$, and every class contains precisely one prime.

2. *Multiplicative monoids of domains.* The multiplicative monoid $R^\bullet$ of a domain R is a Krull monoid if and only if R is a Krull domain, and in this case $\mathcal{C}(R^\bullet)$ is (canonically isomorphic to) the divisor class group $\mathcal{C}(R)$ of R.

3. *Regular congruence monoids in Krull domains.* Let R be a Krull domain, $\{0\} \neq \mathfrak{f} \lhd R$ an ideal and $\Gamma \subset (R/\mathfrak{f})^\times$ a subgroup. Then the monoid

$$H_\Gamma = \{a \in R^\bullet \mid a + \mathfrak{f} \in \Gamma\}$$

is a Krull monoid, called the (*regular*) *congruence monoid* defined in R modulo $\mathfrak{f}$ by Γ (see also Theorem 5.7 and Remarks 5.8).

4. *Regular Hilbert monoids.* Let $f \in \mathbb{N}_{\ge 2}$ and $\Gamma \subset (\mathbb{Z}/f\mathbb{Z})^\times$ a subgroup. Then the monoid $H_\Gamma = \{a \in \mathbb{N} \mid a + f\mathbb{Z} \in \Gamma\}$ is a Krull monoid with class group $\mathcal{C}(H_\Gamma) \cong (\mathbb{Z}/f\mathbb{Z})^\times/\Gamma$, and (by the Dirichlet Prime Number Theorem) every class contains infinitely many primes (see also Theorem 5.7, Remarks 5.8 and Example 5.9).

5. *Analytic theory.* If $[D, H, |\cdot|]$ is a quasi-formation, then H is a Krull monoid with finite class group and infinitely many primes in every class.

6. *Module theory.* Let R be a ring and $\mathcal{C}$ a class of (right) R-modules, closed under finite direct sums, direct summands and isomorphisms such that $\mathcal{C}$ has a set $V(\mathcal{C})$ of representatives (that is, every $A \in \mathcal{C}$ is isomorphic to a unique $[A] \in V(\mathcal{C})$). Then $V(\mathcal{C})$ becomes a commutative semigroup with multiplication $[A]\cdot[B] = [A \oplus B]$. If every $A \in \mathcal{C}$ has a semilocal endomorphism ring, then $V(\mathcal{C})$ is a Krull monoid (see [8]). Among many other cases, this condition is fulfilled if either R is semilocal (not necessarily commutative) and $\mathcal{C}$ is the class of all finitely generated projective R-modules (see [10]), or if R is commutative local noetherian and $\mathcal{C}$ is the class of all finitely generated R-modules (see [27] and [9]).

Definition 5.4

1. Let D be a monoid and $H \subset D$ a submonoid. Two elements $y, y' \in D$ are called *H-equivalent* if $y^{-1}H \cap D = y'^{-1}H \cap D$ (that is, for all $a \in D$ we have $ya \in H$ if and only if $y'a \in H$). H-equivalence is a congruence relation on D, and for $y \in D$ we denote by $[y]_H^D$ the congruence class of y. We define the *class semigroup*

$$\mathcal{C}(H,D) = \{[y]_H^D \mid y \in D\}, \quad \text{and} \quad \mathcal{C}^*(H,D) = \{[y]_H^D \mid y \in (D \setminus D^\times) \cup \{1\}\}$$

and is called the *reduced class semigroup*.

2. H is called a C-*monoid* if H is a submonoid of a factorial monoid F such that $F^\times \cap H = H^\times$ and $\mathcal{C}^*(H,F)$ is finite. In this case we say that H is a C-*monoid defined in* F.

If H is a C-monoid defined in a factorial monoid F, then F is far from being unique. However, there is a canonical choice for F which is given by the assertion **A.**3 of Theorem 5.6 below. The most important examples of C-monoids will be presented in Theorem 5.7.

For a saturated submonoid $H \subset D$, the distance between H and D is satisfactory codified in the class group $\mathsf{q}(D)/\mathsf{q}(H)$, but in the general case the more subtle concept of a class semigroup is needed. In Proposition 5.5 below we compare these two concepts and establish the connection between Krull monoids and C-monoids. For full proofs of all assertions concerning C-monoids we refer to [20], [14] and [16].

Proposition 5.5 *Let D be a monoid and $H \subset D$ a submonoid.*

1. *$\mathcal{C}(H,D)$ is finite if and only if both $\mathcal{C}^*(H,D)$ and $D^\times/H^\times$ are finite.*
2. *If $aD \cap H \neq \emptyset$ for all $a \in D$, then there are natural epimorphisms*

$$\theta\colon \mathcal{C}(H,D) \to D/H \quad \text{and} \quad \theta^*\colon \mathcal{C}^*(H,D) \to D/D^\times H\,,$$

and θ is an isomorphism if and only if $H \subset D$ is saturated.

3. *Every Krull monoid with finite class group is a C-monoid. In particular, the block monoid over a finite abelian group is a C-monoid.*
4. *Let H be a C-monoid defined in a factorial monoid F such that $\mathcal{C}^*(H,F)$ is a group. Then H is a Krull monoid.*

Theorem 5.6 (Main Theorem on C-monoids) *Let H be a* C-*monoid.*

A. Algebraic Properties.

1. *H is v-noetherian.*
2. *$\widehat{H}$ is a Krull monoid with finite class group, and there exists some $a \in H$ such that $a\widehat{H} \subset H$.*

3. Suppose that $\widehat{H} = \widehat{H}^\times \times D$ *with* $D \cong \widehat{H}_{\rm red}$, *let* F_0 *be a monoid of divisors of* D *and* $F = \widehat{H}^\times \times F_0$. *Then* H *is a* C*-monoid defined in* F, *and there is an epimorphism* $\mathcal{C}^*(H, F) \to \mathcal{C}(\widehat{H})$.

B. Arithmetical Properties. *H is locally tame,* $\mathsf{c}(H) < \infty$, *and the Structure Theorem for Sets of Lengths holds for* H.

Structure of the proof of **B**.

1. (Reduction step) By means of a transfer principle (see Proposition 6.4 and Theorem 6.5) we may assume that H is defined in a finitely generated factorial monoid F. Thus let $F = F^\times \times [p_1, \ldots, p_s]$ with pairwise non-associated prime elements $p_1, \ldots, p_s$.

2. (Local tameness) The finiteness of $\mathcal{C}^*(H, F)$ turns out to be equivalent with the following property by means of which local tameness can be verified by explicit calculations:

> There exist some $\alpha \in \mathbb{N}$ and a subgroup $V \subset F^\times$ such that $(F^\times : V) \,|\, \alpha$, $V(H \setminus H^\times) \subset H$, and for all $j \in [1, s]$ and $a \in p_j^\alpha F$ we have $a \in H$ if and only if $p_j^\alpha a \in H$.

3. (Catenary degree) H is a v-noetherian G-monoid and thus it is finitary. Every locally tame finitary monoid has finite catenary degree (of course, this argument uses the definitions and simple properties of finitary monoids and G-monoids, see [17]).

4. (Structure Theorem for Sets of Lengths) The proof splits into an abstract additive part and an ideal-theoretic part. Both steps rest on the concepts of pattern ideals and of tamely generated ideals which are defined as follows.

For a finite non-empty set $A \subset \mathbb{Z}$ the pattern ideal $\Phi(A)$ is the set of all $a \in H$ for which there is some $y \in \mathbb{Z}$ such that $y + A \subset \mathsf{L}(a)$.

A subset $\mathfrak{a} \subset H$ is called tamely generated if there exist a subset $E \subset \mathfrak{a}$ and a bound $N \in \mathbb{N}$ with the following property:

> For every $a \in \mathfrak{a}$ there exists some $e \in E$ such that $e \,|\, a$, $\sup \mathsf{L}(e) \le N$ and $\mathsf{t}(a, \mathsf{Z}(e)) \le N$.

In the additive part one proves that the Structure Theorem for Sets of Lengths holds for every BF-monoid H with finite set $\Delta(H)$ in which all pattern ideals are tamely generated. This is done in the spirit of additive number theory. To apply this additive result to a BF-monoid H, it must be proved that $\Delta(H)$ is finite and that all pattern ideals are tamely generated. For a finitely generated monoid, this is comparatively simple. For a C-monoid, the finiteness of $\Delta(H)$ follows from the finiteness of the catenary degree, while the tame generation of pattern ideals needs deep ideal-theoretic considerations.

Theorem 5.7 (C-monoids in ring theory)

A. *Let R be a Krull domain and $\mathfrak{f}$ an ideal of R such that $\mathcal{C}(R)$ and $R/\mathfrak{f}$ are both finite. Let $\emptyset \neq \Gamma \subset R/\mathfrak{f}$ be a multiplicatively closed subset and $H_\Gamma = \{a \in R^\bullet \mid a + \mathfrak{f} \in \Gamma\} \cup \{1\}$. Suppose that either $\mathfrak{f}$ is divisorial or R is noetherian. Then H_Γ is a* C*-monoid.*

B. *Let $f \in \mathbb{N}_{\ge 2}$ and $\emptyset \neq \Gamma \subset \mathbb{Z}/f\mathbb{Z}$ a multiplicatively closed subset. Then $H_\Gamma = \{a \in \mathbb{N} \mid a + f\mathbb{Z} \in \Gamma\} \cup \{1\}$ is a* C*-monoid.*

C. *Let A be a Mori domain, $R = \widehat{A}$ and $\mathfrak{f} = \{a \in R \mid aR \subset A\} \neq \{0\}$. Then R is a Krull domain. If $\mathcal{C}(R)$ and $R/\mathfrak{f}$ are both finite, then $A^\bullet$ is a* C*-monoid.*

Remarks 5.8 The monoid H_Γ considered in **A.** is called the *congruence monoid* defined in R modulo $\mathfrak{f}$ by Γ and that considered in **B.** is called the *Hilbert monoid* defined modulo $\mathfrak{f}$ by Γ (named after D. Hilbert who used such monoids to demonstrate the necessity of a proof for the uniqueness of prime factorizations in the integers).

Regular congruence monoids and Hilbert monoids were already considered in Examples 5.3 (3. and 4.). Using a more general concept of congruence monoids (including sign conditions, see [15] or [16]) it is possible to treat **A.** and **B.** in a uniform way.

Let A be a Mori domain as in **C.** (see [5] for a recent survey on Mori domains). Then $\mathfrak{f}$ is the largest ideal of $\widehat{A}$ lying in A (called the *conductor* of A), and $A = \{a \in \widehat{A} \mid a + \mathfrak{f} \in A/\mathfrak{f}\}$, whence in particular A is the congruence monoid defined in $\widehat{A}$ modulo $\mathfrak{f}$ by $A/\mathfrak{f}$.

We sketch the proof of **A.** (by the above remarks, that of **B.** and **C.** is essentially the same). Let $R^\bullet = R^\times \times R_0$ with a reduced Krull monoid R_0, let F_0 be a monoid of divisors of R_0 and $F = R^\times \times F_0$. Then H_Γ is a C-monoid defined in F (the main task is to deduce the finiteness of $\mathcal{C}^*(H_\Gamma, F)$ from that of $R/\mathfrak{f}$ and $\mathcal{C}(R)$).

Example 5.9 (Orders in Dedekind domains and algebraic number fields)

Let R be a Dedekind domain, $\{0\} \neq \mathfrak{f} \lhd R$ and $\Gamma \subset (R/\mathfrak{f})^\times$ a subgroup. Then the regular congruence monoid $H_\Gamma = \{a \in R^\bullet \mid a + \mathfrak{f} \in \Gamma\}$ is a Krull monoid (see Example 5.3.3). We denote by $\mathcal{I}_\mathfrak{f}(R)$ the (multiplicative) monoid of all non-zero ideals $\mathfrak{a} \lhd R$ with $\mathfrak{a} + \mathfrak{f} = R$, by $\mathcal{H}_\mathfrak{f}(R)$ its submonoid of principal ideals and by $\mathfrak{X}_\mathfrak{f}(R)$ the set of all prime ideals in $\mathcal{I}_\mathfrak{f}(R)$. Then

$$\mathcal{H}_\Gamma = \{aR \mid a \in H_\Gamma\} \ \subset \ \mathcal{H}_\mathfrak{f}(R)$$

is a submonoid (called a *generalized Hilbert monoid*), $\mathcal{I}_\mathfrak{f}(R)$ is a monoid of divisors and $\mathfrak{X}_\mathfrak{f}(R)$ is a set of prime divisors of $\mathcal{H}_\Gamma$. There is a canonical isomorphism $(H_\Gamma)_{\red} \cong \mathcal{H}_\Gamma$, and consequently $\mathcal{C}(H_\Gamma) = \mathcal{C}(\mathcal{H}_\Gamma)$. The monoid

$\mathcal{S}_{\mathfrak{f}}(R) = \{aR \mid a \in 1 + \mathfrak{f}\} \subset \mathcal{H}_\Gamma$ is called the *principal ray* and the group $\mathcal{I}_{\mathfrak{f}}(R)/\mathcal{S}_{\mathfrak{f}}(R)$ is called the *ray class group* modulo $\mathfrak{f}$. There is a natural exact sequence

$$0 \to \mathcal{H}_\Gamma/\mathcal{S}_{\mathfrak{f}}(R) \to \mathcal{I}_{\mathfrak{f}}(R)/\mathcal{S}_{\mathfrak{f}}(R) \to \mathcal{C}(H_\Gamma) \to 0$$

which shows that every class $C \in \mathcal{C}(H_\Gamma)$ is the union of $|\mathcal{H}_\Gamma/\mathcal{S}_{\mathfrak{f}}(R)|$ ray classes modulo $\mathfrak{f}$.

Let now $A \subset R$ be an order (that is, A is a subring of R such A and R have the same field of quotients, and R is a finitely generated A-module). Then A is a one-dimensional noetherian domain with integral closure $\widehat{A} = R$ and conductor $\mathfrak{f} = \{a \in A \mid aR \subset A\}$. Since $A = \{a \in R \mid a + \mathfrak{f} \in A/\mathfrak{f}\}$, the monoid $A^\bullet$ is the congruence monoid defined in R modulo $\mathfrak{f}$ by $A/\mathfrak{f}$, and if both $R/\mathfrak{f}$ and $\mathcal{C}(R)$ are finite, then $A^\bullet$ is a C-monoid (see Theorem 5.7 and the consecutive remarks). The monoid

$$A^* = \{a \in R^\bullet \mid a + \mathfrak{f} \in (A/\mathfrak{f})^\times\} = \{a \in A^\bullet \mid aA + \mathfrak{f} = A\}$$

is a regular congruence monoid in R and thus it is a Krull monoid (see Example 5.3.3). By the above, $\mathcal{I}_{\mathfrak{f}}(R)$ is a monoid of divisors and $\mathfrak{X}_{\mathfrak{f}}(R)$ is a set of prime divisors of A^*, and every class $C \in \mathcal{C}(A^*)$ is a union of ray classes modulo $\mathfrak{f}$.

We compare the class group $\mathcal{C}(A^*)$ with the Picard group

$$\mathrm{Pic}(A) = \frac{\{\text{invertible fractional ideals of } A\}}{\{\text{fractional principal ideals of } A\}} \quad \text{of} \quad A\,.$$

It is not difficult to prove that every non-zero ideal $\mathfrak{a} \lhd A$ with $\mathfrak{a} + \mathfrak{f} = A$ is invertible, and that every class $C \in \mathrm{Pic}(A)$ contains such an ideal. Hence there is an epimorphism $\mathcal{I}_{\mathfrak{f}}(R) \to \mathrm{Pic}(A)$, which maps an ideal $\mathfrak{a} \in \mathcal{I}_{\mathfrak{f}}(R)$ onto the class $[\mathfrak{a} \cap A] \in \mathrm{Pic}(A)$. This epimorphism induces an isomorphism $\mathcal{C}(A^*) \xrightarrow{\sim} \mathrm{Pic}(A)$.

Let finally R be the ring of integers of an algebraic number field and $A \subset R$ an order with conductor $\mathfrak{f}$. The ray class group $\mathcal{I}_{\mathfrak{f}}(R)/\mathcal{S}_{\mathfrak{f}}(R)$ is finite and every ray class contains infinitely many prime ideals (see [24, Theorem 3.7 and Corollary 7 to Proposition 7.16]). Consequently every class of $\mathcal{C}(A^*)$ contains infinitely many primes, and every class of $\mathrm{Pic}(A)$ contains infinitely many prime ideals.

6 Transfer principles

Transfer principles are a central tool in the theory of non-unique factorizations. By means of them it is possible to establish factorization properties in simple auxiliary monoids and then to apply the result to various cases of arithmetical interest. This section is rather technical, and we give no proofs (most of them are simple, see [14] or [16] for details).

Definition 6.1 A monoid homomorphism $\theta\colon H \to B$ is called a *transfer homomorphism* if it has the following properties:

(T 1) $B = \theta(H)B^\times$ and $\theta^{-1}(B^\times) = H^\times$.

(T 2) If $u \in H$, $b, c \in B$ and $\theta(u) = bc$, then there exist $v, w \in H$ such that $u = vw$, $\theta(v) \simeq b$ and $\theta(w) \simeq c$.

Proposition 6.2 *Let $\theta\colon H \to B$ be a transfer homomorphism.*

1. *If $u \in H$, then $u \in \mathcal{A}(H)$ if and only if $\theta(u) \in \mathcal{A}(B)$.*
2. *There is a unique homomorphism $\overline{\theta}\colon \mathsf{Z}(H) \to \mathsf{Z}(B)$ (referred to as the extension of θ to the factorization monoids) satisfying*

$$\overline{\theta}(uH^\times) = \theta(u)B^\times \quad \text{for all} \quad u \in \mathcal{A}(H)\,.$$

It is surjective and has the following properties:

a) If $z, z' \in \mathsf{Z}(H)$, then $|\overline{\theta}(z)| = |z|$ and $\mathsf{d}\big(\overline{\theta}(z), \overline{\theta}(z')\big) \le \mathsf{d}(z, z')$.

b) If $u \in H$, then $\overline{\theta}(\mathsf{Z}_H(u)) = \mathsf{Z}_B(\theta(u))$ and $\mathsf{L}_H(u) = \mathsf{L}_B(\theta(u))$. In particular, $\mathcal{L}(H) = \mathcal{L}(B)$.

Definition 6.3 Let $\theta\colon H \to B$ be a transfer homomorphism of atomic monoids and $\overline{\theta}\colon \mathsf{Z}(H) \to \mathsf{Z}(B)$ its extension to the factorization monoids.

1. (*Catenary degree in the fibres*) For $a \in H$, we denote by $\mathsf{c}(a, \theta)$ the smallest $N \in \mathbb{N}_0 \cup \{\infty\}$ with the following property:

   If $z, z' \in \mathsf{Z}(a)$ and $\overline{\theta}(z) = \overline{\theta}(z')$, then there exists a finite sequence of factorizations $z = z_0, \ldots, z_k = z' \in \mathsf{Z}(a)$ such that $\overline{\theta}(z_i) = \overline{\theta}(z)$ and $\mathsf{d}(z_{i-1}, z_i) \le N$ for all $i \in [1, k]$.

   We call $\mathsf{c}(H, \theta) = \sup\{\mathsf{c}(a, \theta) \mid a \in H\} \in \mathbb{N}_0 \cup \{\infty\}$ the *catenary degree in the fibres* of θ.
2. (*Tame degree in the fibres*) For $a \in H$ and $x \in \mathsf{Z}(H)$, we denote by $\mathsf{t}(a, x, \theta)$ the smallest $N \in \mathbb{N}_0 \cup \{\infty\}$ with the following property:

   If $\mathsf{Z}(a) \cap x\mathsf{Z}(H) \ne \emptyset$, $z \in \mathsf{Z}(a)$ and $\overline{\theta}(z) \in \overline{\theta}(x)\mathsf{Z}(B)$, then there exists some $z' \in \mathsf{Z}(a) \cap x\mathsf{Z}(H)$ such that $\overline{\theta}(z') = \overline{\theta}(z)$ and $\mathsf{d}(z, z') \le N$.

   We call $\mathsf{t}(H, x, \theta) = \sup\{\mathsf{t}(a, x, \theta) \mid a \in H\} \in \mathbb{N}_0 \cup \{\infty\}$ the *tame degree of x in the fibres* of θ.

Proposition 6.4 *Let $\theta\colon H \to B$ be a transfer homomorphism of atomic monoids.*

1. *If $a \in H$, then $\mathsf{c}\big(\theta(a)\big) \le \mathsf{c}(a) \le \max\big\{\mathsf{c}\big(\theta(a)\big), \mathsf{c}(a, \theta)\big\}$. In particular, $\mathsf{c}(B) \le \mathsf{c}(H) \le \max\{\mathsf{c}(B), \mathsf{c}(H, \theta)\}$.*

2. *If* $\overline{\theta}\colon \mathsf{Z}(H) \to \mathsf{Z}(B)$ *is the extension of* θ *to the factorization monoids and* $x \in \mathsf{Z}(H)$, *then* $\mathsf{t}\big(B, \overline{\theta}(x)\big) \le \mathsf{t}(H, x) \le \mathsf{t}\big(B, \overline{\theta}(x)\big) + \mathsf{t}(H, x, \theta)$. *In particular, if* $\mathsf{t}(H, u, \theta) < \infty$ *for all* $u \in \mathcal{A}(H_{\red})$ *and* B *is locally tame, then* H *is also locally tame.*

We apply the Propositions 6.2 and 6.4 to C-monoids and to Krull monoids. The application to C-monoids has already been mentioned and successfully used when we sketched the proof of Theorem 5.6.**B.** The transfer result for Krull monoids (Theorem 6.6) goes back to ideas of W. Narkiewicz (see [23]). It provides the link between factorization theory and additive group theory (see Section 4) and shows that (most) arithmetical invariants of a Krull monoid are in fact combinatorial invariants of the class group.

Theorem 6.5 (A transfer result for C-monoids) *Let* H *be a* C*-monoid. Then there is a transfer homomorphism* $\theta\colon H \to B$ *having the following properties*:

1. B *is* C*-monoid defined in a factorial monoid* D *with only finitely many non-associated primes such that* $D^\times$ *is finite.*
2. $\mathsf{c}(H, \theta) \le 2$.
3. *If* H *is defined in a factorial monoid* F *and* $u \in \mathcal{A}(H)$ *is a product of* m *primes in* F, *then* $\mathsf{t}(H, uH^\times, \theta) \le m + d$ *where* $d \in \N$ *depends only on* $\mathcal{C}^*(H, F)$.

Theorem 6.6 (A transfer result for Krull monoids) *Let* H *be a Krull monoid,* $D = \mathcal{F}(P)$ *a monoid of divisors of* H, $G = \mathcal{C}(H)$ *its class group and* $G_0 \subset G$ *the set of all classes containing primes. Let* $\widetilde{\boldsymbol{\beta}}\colon D \to \mathcal{F}(G_0)$ *be the unique homomorphism satisfying* $\widetilde{\boldsymbol{\beta}}(p) = [p]$ *for all* $p \in P$.

Then $\widetilde{\boldsymbol{\beta}}^{-1}(\mathcal{B}(G)) = H_{\red}$, *and the homomorphism* $\boldsymbol{\beta}\colon H \to \mathcal{B}(G_0)$, *defined by* $\boldsymbol{\beta}(a) = \widetilde{\boldsymbol{\beta}}(aH^\times)$, *is a transfer homomorphism satisfying* $\mathsf{c}(H, \boldsymbol{\beta}) \le 2$ *and* $\mathsf{t}(H, u, \boldsymbol{\beta}) \le \mathsf{D}(G) + 1$ *for all* $u \in \mathcal{A}(H_{\red})$.

Let now H be a Krull monoid with finite class group $G = \mathcal{C}(H)$, and suppose that every class contains primes. This holds true for every Krull monoid fitting into a quasi-formation (see Definition 7.1 and Examples 7.2).

Then Theorem 6.6 together with the Propositions 6.2 and 6.4 implies that $\mathcal{L}(H) = \mathcal{L}(G)$, $\Delta(H) = \Delta(G)$, $\Delta^*(H) = \Delta^*(G)$, and if $|G| \ge 3$, then also $\mathsf{c}(H) = \mathsf{c}(G)$. Hence all these quantities can be described with the methods of Section 4. In particular, we rediscover Carlitz' result that H is half-factorial if and only if $|G| \le 2$. Taking into account that the catenary degree $\mathsf{c}(H)$ measures how complex sets of factorizations of elements of H may be and that $\mathsf{c}(H) = \mathsf{c}(G)$ grows with the size of G (see Theorem 4.2.1) we approve the philosophy of classical algebraic number theory that the class group is a measure for the non-uniqueness of factorizations.

7 Analytic theory

The concept of quasi-formations stems from abstract analytic number theory (as presented in [16]) and allows us to formulate the analytic theory of algebraic numbers and algebraic functions in a uniform way.

Definition 7.1 A *quasi-formation* $[D, H, |\cdot|]$ consists of

- a free monoid $D = \mathcal{F}(P)$,
- a homomorphism $|\cdot| \colon D \to (\mathbb{N}, \cdot)$ such that $|a| = 1$ if and only if $a = 1$, and the Dirichlet series

$$\sum_{p \in P} |p|^{-s} \quad \text{converges for} \quad \Re(s) > 1\,,$$

- a saturated submonoid $H \subset D$ such that $G = D/H$ is finite, and for every $g \in G$ the function ψ_g, defined by

$$\psi_g(s) = \sum_{p \in P \cap g} |p|^{-s} \; - \; \frac{1}{|G|} \log \frac{1}{s-1} \quad \text{for} \quad \Re(s) > 1\,,$$

  has a holomorphic extension to $s = 1$.

If $[D, H, |\cdot|]$ is a quasi-formation, then H is a Krull monoid, D is a monoid of divisors of H, $G = \mathcal{C}(H)$, and every class contains a denumerable set of primes. We say that the Krull monoid H fits into a quasi-formation.

Examples 7.2 (Examples of quasi-formations)

1. Let R be the ring of integers of an algebraic number field or a holomorphy ring in an algebraic function field over a finite field and $H = \mathcal{H}(R)$ the (multiplicative) monoid of non-zero principal ideals of R (note that $H \cong (R^\bullet)_{\mathrm{red}}$). Let D be the (multiplicative) monoid of all non-zero ideals of R, and for $\mathfrak{a} \in D$ let $|\mathfrak{a}| = (D : \mathfrak{a})$. Then $[D, H, \cdot]$ is a quasi-formation. This can be verified using classical analytic number theory (see [24] for the number field case and [11] for the function field case).

More generally, every generalized Hilbert monoid (see Example 5.9) defined in R fits into a quasi-formation (we omit details).

2. Let $f \in \mathbb{N}_{\ge 2}$, $\Gamma \subset (\mathbb{Z}/f\mathbb{Z})^\times$ a subgroup and $H_\Gamma = \{a \in \mathbb{N} \mid a + f\mathbb{Z} \in \Gamma\}$ a regular Hilbert monoid. If $\mathbb{N}_f$ denotes the monoid of all $a \in \mathbb{N}$ which are relatively prime to f and $|a| = a$ for all $a \in \mathbb{N}_f$, then $[\mathbb{N}_f, H_\Gamma, |\cdot|]$ is a quasi-formation. Again this follows by classical analytic number theory.

The following Proposition 7.3 is based on the Tauberian Theorem of Ikehara and Delange. It is the key analytic tool for our arithmetical main result given in the Theorem 7.4. There we show that the set of elements having more than k distinct factorization lengths (provided that $|G| \ge 3$) and the set of all elements having catenary degree at most 3 both have density 1.

Proposition 7.3 *Let $[D, H, |\cdot|]$ be a quasi-formation, $G = D/H$, $G_0 \subset G$, $y \in G$, $S \in \mathcal{F}(G \setminus G_0)$ and $l \in \mathbb{N}_0$. Let $\Omega_y(G_0, S, l)$ denote the set of all sequences $C \in \mathcal{F}(G)$ with $\sigma(C) = y$, $\mathsf{v}_g(C) = \mathsf{v}_g(S)$ for all $g \in G \setminus G_0$ and $\mathsf{v}_g(C) \ge l$ for all $g \in G_0$, and suppose that $\Omega_y(G_0, S, 0) \not\subset \{1\}$. Let $\widetilde{\boldsymbol{\beta}}\colon D \to \mathcal{F}(G)$ be the homomorphism defined in* Theorem 6.6*, and for $x \in \mathbb{R}_{\ge 1}$ let*

$$\Omega_y(G_0, S, l)(x) = \big|\{a \in D \mid \widetilde{\boldsymbol{\beta}}(a) \in \Omega_y(G_0, S, l)\,,\ |a| \le x\}\big|\,.$$

Then we have, for $x \to \infty$,

$$\Omega_y(G_0, S, l)(x) \asymp x\,(\log x)^{\eta}\,(\log\log x)^{\delta}\,,$$

where

$$\eta = -1 + \frac{|G_0|}{|G|} \quad \text{and} \quad \delta = \begin{cases} |S|\,, & \text{if} \quad G_0 \neq \emptyset\,, \\ |S| - 1\,, & \text{if} \quad G_0 = \emptyset\,. \end{cases}$$

Theorem 7.4 *Let $[D, H, |\cdot|]$ be a quasi-formation and $G = D/H$.*

1. *If $|G| \ge 3$ and $k \in \mathbb{N}$, then we have (for $x \ge 3$)*

$$\frac{\big|\{a \in H \mid |\mathsf{L}(a)| > k\,, |a| \le x\}\big|}{\big|\{a \in H \mid |a| \le x\}\big|} = 1 + O\Big(\frac{(\log\log x)^{\psi_k(G)}}{(\log x)^{1-\mu(G)/|G|}}\Big)\,,$$

   where $\mu(G)$ is the maximal cardinality of a half-factorial subset of G and $\psi_k(G) \in \mathbb{N}_0$ is a combinatorial invariant depending only on G and k.

2. *For $x \ge 2$ we have*

$$\frac{\big|\{a \in H \mid \mathsf{c}(a) \le 3\,, |a| \le x\}\big|}{\big|\{a \in H \mid |a| \le x\}\big|} = 1 + O\big((\log x)^{-1/|G|}\big)\,.$$

Idea of the proof. 1. We show that the set $\mathcal{G}_k(H) = \{a \in H \mid |\mathsf{L}(a)| \le k\}$ is a finite union of sets of the form $\Omega_0(G_0, S_0, l_0)$ for some half-factorial subsets $G_0 \subset G$ and sequences $S_0 \in \mathcal{F}(G \setminus G_0)$. Then we apply Proposition 7.3.

2. Let $a \in H$ with $\mathsf{c}(a) > 3$. Then (since $\boldsymbol{\beta} = \widetilde{\boldsymbol{\beta}}\,|\,H\colon H \to \mathcal{B}(G)$ is a transfer homomorphism with $\mathsf{c}(H, \boldsymbol{\beta}) \le 2$, see Theorem 6.6) it follows that $\mathsf{c}(\boldsymbol{\beta}(a)) > 3$ (see Proposition 6.4), and thus Theorem 4.3.1 implies that $\operatorname{supp}\big(\boldsymbol{\beta}(a)\big) \cup \{0\} \neq G$, whence $\boldsymbol{\beta}(a) \in \Omega_0(G \setminus \{g\}, 1, 0)$ for some $g \in G$. Thus

$$\big|\{a \in H \mid \mathsf{c}(a) > 3,\ |a| \le x\}\big| \ll x(\log x)^{-1/|G|}$$

by Proposition 7.3, and so the assertion follows. □

References

1. D.D. Anderson (ed.), *Factorization in Integral Domains*, Lect. Notes Pure Appl. Math., vol. 189, Marcel Dekker, 1997.
2. D.D. Anderson, D.F. Anderson, and M. Zafrullah, *Factorizations in integral domains*, J. Pure Appl. Algebra **69** (1990), 1 – 19.
3. ———, *Factorizations in integral domains II*, J. Algebra **152** (1992), 78 – 93.
4. D.F. Anderson and D.N. El Abidine, *Factorization in integral domains III*, J. Pure Appl. Algebra **135** (1999), 107–127.
5. V. Barucci, *Mori domains*, in [7], pp. 57 – 73.
6. S.T. Chapman (ed.), *Arithmetical Properties of Commutative Rings and Monoids*, Lect. Notes Pure Appl. Math., vol. 241, Chapman & Hall/CRC, 2005.
7. S.T. Chapman and S. Glaz (eds.), *Non-Noetherian Commutative Ring Theory*, Kluwer Academic Publishers, 2000.
8. A. Facchini, *Direct sum decomposition of modules, semilocal endomorphism rings, and Krull monoids*, J. Algebra **256** (2002), 280 – 307.
9. A. Facchini, W. Hassler, L. Klingler, and R. Wiegand, *Direct-sum decompositions over one-dimensional Cohen-Macaulay local rings*, this volume.
10. A. Facchini and D. Herbera, K_0 *of a semilocal ring*, J. Algebra **225** (2000), 47 – 69.
11. M. Fried and M. Jarden, *Field Arithmetic, 2nd ed.*, Springer, 2005.
12. W. Gao and A. Geroldinger, *Zero-sum problems in abelian groups: a survey.*
13. ———, *Systems of sets of lengths II*, Abh. Math. Semin. Univ. Hamb. **70** (2000), 31 – 49.
14. A. Geroldinger and F. Halter-Koch, *Transfer principles in the theory of non-unique factorizations*, in [6], pp. 114 – 142.
15. ———, *Congruence monoids*, Acta Arith. **112** (2004), 263 – 296.
16. ———, *Non-Unique Factorizations. Algebraic, Combinatorial and Analytic Theory*, Pure and Applied Mathematics, vol. 279, Chapman & Hall/CRC, 2005.
17. A. Geroldinger, F. Halter-Koch, W. Hassler, and F. Kainrath, *Finitary monoids*, Semigroup Forum **67** (2003), 1 – 21.
18. R. Gilmer, *Multiplicative Ideal Theory*, vol. 90, Queen's Papers, 1992.
19. ———, *Forty years of commutative ring theory*, Rings, Modules, Algebras, and Abelian Groups, Lect. Notes Pure Appl. Math., vol. 236, Marcel Dekker, 2004, pp. 229 – 256.
20. F. Halter-Koch, C-*monoids and congruence monoids in Krull domains*, in [6], pp. 71 – 98.
21. ———, *Ideal Systems*, Marcel Dekker, 1998.
22. F. Kainrath, *Factorization in Krull monoids with infinite class group*, Colloq. Math. **80** (1999), 23 – 30.
23. W. Narkiewicz, *Finite abelian groups and factorization problems*, Colloq. Math. **42** (1979), 319 – 330.
24. ———, *Elementary and Analytic Theory of Algebraic Numbers, 3rd ed.*, Springer, 2004.
25. W.A. Schmid, *Differences in sets of lengths of Krull monoids with finite class group*, J. Théor. Nombres Bordx. **17** (2005), 323 – 345.
26. ———, *Half-factorial sets in finite abelian groups: a survey*, Grazer Math. Ber. **347** (2005).
27. R. Wiegand, *Direct-sum decompositions over local rings*, J. Algebra **240** (2001), 83 – 97.