

**THE ART OF FACTORIZATION
IN MULTIPLICATIVE
STRUCTURES**

An MAA PREP Workshop

organized by

Scott T. Chapman and Jim Coykendall

Alfred Geroldinger

University of Graz, Austria

San Antonio, May 20th - May 25th, 2007

1. Concepts in Factorization Theory

- What objects do we study ?
Some algebraic background and examples
- Definition of arithmetical invariants
which describe the non-uniqueness of factorizations

2. Transfer Principles - The Krull Case

- How are things proved ?
- Arithmetical Finiteness Results for Krull and weakly Krull monoids

3. More Finiteness Results - The Non-Krull Case

- Class semigroups
- C-monoids

4. Zero-sum Sequences and Additive Group Theory

- In the case of Krull monoids with finite class group,
arithmetical invariants can be studied
by methods from additive group theory

CITATIONS: Most of the discussed results can be found in the monograph [18]. For the development of the area and all the contributions of the various people and research groups we refer to the literature on the website of the workshop. Here we only mention some early papers and some most recent papers.

1. CONCEPTS IN FACTORIZATION THEORY

Some algebraic background and examples

Let H be a *monoid*: that is a (mult. written), commutative semi-group which has a unit element and satisfies the cancellation laws.

$\mathcal{A}(H)$ the set of *atoms* of H , H^\times the set of invertible elements, $\mathfrak{q}(H)$ a *quotient group* of H , $H_{\text{red}} = H/H^\times = \{aH^\times \mid a \in H\}$ the associated reduced monoid. Clearly, H_{red} is isomorphic to the monoid of principal ideals of H .

An element $x \in \mathfrak{q}(H)$ 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 $\mathfrak{q}(H)$ which are almost integral over H is a monoid, is a monoid again, called the *complete integral closure* of H , and H is said to be *completely integrally closed* if $\widehat{H} = H$. Furthermore,

$$\mathfrak{f} = (H : \widehat{H}) := \{x \in \mathfrak{q}(H) \mid x\widehat{H} \subset H\}$$

is called the *conductor* of H .

$(\mathcal{I}_v^*(H), \cdot_v)$ the *monoid of v -invertible v -ideals* of H endowed with v -multiplication.

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

$$a = \prod_{p \in P} p^{\mathbf{v}_p(a)} \quad \text{with } \mathbf{v}_p(a) \in \mathbb{N}_0 \text{ and } \mathbf{v}_p(a) = 0 \text{ for almost all } p \in P.$$

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 call

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

The following concepts have a long tradition in algebraic number theory:

Let $\varphi: H \rightarrow D$ be a monoid homomorphism. It is called

- *cofinal* if for every $a \in D$ there exists some $u \in H$ such that $a \mid \varphi(u)$.
- *a divisor homomorphism* if, for all $u, v \in H$, $\varphi(u) \mid \varphi(v)$ implies that $u \mid v$,
- *a divisor theory* (for H) if it is a divisor homomorphism, D is free, say $D = \mathcal{F}(P)$ for some set P , and, for every $p \in P$, there exists a finite subset $\emptyset \neq X \subset H$ satisfying $p = \gcd(\varphi(X))$.

The group

$$\mathcal{C}(\varphi) = \text{Coker}(\mathfrak{q}(\varphi)) = \mathfrak{q}(D)/\mathfrak{q}(\varphi(H))$$

is called the *class group* of φ . A submonoid $H \subset D$ is called *saturated* if the embedding $H \hookrightarrow D$ is a divisor homomorphism.

Theorem 1.1.

1. *A monoid H is called a Krull monoid if it satisfies one of the following two equivalent conditions:*
 - (a) *H is v -noetherian and completely integrally closed (L.G. Chouinard, 1981).*
 - (b) *H has a divisor theory.*
 - (c) *H_{red} is a saturated submonoid of a free monoid.*
2. *Suppose that H is a Krull monoid. Then the map $\varphi: H \rightarrow \mathcal{I}_v^*(H)$, defined by $a \mapsto aH$ for all $a \in H$, is a divisor theory, and the class group of φ is the v -class group $\mathcal{C}_v(H)$ of H .*
3. *R is a Krull domain if and only if R^\bullet is a Krull monoid (U. Krause, 1989).*
In particular, every noetherian integrally closed domain is a Krull domain.

Let R be an integral domain, \overline{R} its integral closure, \widehat{R} its complete integral closure and K a quotient field of R whence $R \subset \overline{R} \subset \widehat{R} \subset K$.

If R is noetherian, then $\overline{R} = \widehat{R}$, and the conductor $(R:\overline{R}) \neq \{0\}$ if and only if \overline{R} is a finitely generated R -module.

Since R is a domain, its multiplicative semigroup $R^\bullet = (R \setminus \{0\}, \cdot)$ is a monoid. We study the arithmetic of the domain R by means of the monoid R^\bullet .

We use all arithmetic notion and all notations defined for monoids also for domains. For example $\mathcal{A}(R) = \mathcal{A}(R^\bullet)$, and so on ..

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, $\mathcal{C}_v(R^\bullet) = \mathcal{C}_v(R)$ and R^\bullet is v -noetherian if and only if R is a Mori domain.

We denote by

- $\mathcal{H}(R)$ the *monoid of non-zero principal ideals*,
- $(\mathcal{I}_v^*(R), \cdot_v)$ the *monoid of v -invertible divisorial ideals* endowed with v -multiplication,
- $(\mathcal{I}^*(R), \cdot)$ the *monoid of invertible ideals* with usual ideal multiplication.

The embedding

$$\varphi: \mathcal{H}(R) \rightarrow \mathcal{I}^*(R)$$

is a cofinal divisor homomorphism and its class group

$$\mathcal{C}(\varphi) = \text{Pic}(R) = \mathfrak{q}(\mathcal{I}^*(R)) / \mathfrak{q}(\mathcal{H}(R))$$

is the *Picard group* of R .

A domain R is a *Dedekind domain* if and only if one of the following equivalent conditions is satisfied :

- R is a one-dimensional Krull domain or $R = K$.
- R is noetherian, integrally closed and every non-zero prime ideal of R is maximal.
- Every non-zero ideal is invertible.

A subring $R_0 \subset R$ is called an *order* in R if $\mathfrak{q}(R_0) = K$ and R is a finitely generated R_0 -module. If R_0 is an order in R , then

$$\mathfrak{f} = \{a \in R \mid aR \subset R_0\} = (R_0 : R) = \text{Ann}_{R_0}(R/R_0)$$

is a non-zero ideal of R , called the *conductor* of R_0 in R .

The following statements are equivalent :

1. R is one-dimensional, noetherian, and the integral closure \overline{R} of R is a finitely generated R -module.
2. R is an order in a Dedekind domain.

Therefore,

orders in Dedekind domains
are
one-dimensional Mori domains with non-trivial conductor

If R is a one-dimensional Mori domain, then

$$(\mathcal{I}_v^*(R), \cdot_v) = (\mathcal{I}^*(R), \cdot) \quad \text{and} \quad \mathcal{C}_v(R) = \text{Pic}(R).$$

Examples of monoids

1. Algebraic number theory. Let K be an algebraic number field (that is a finite extension field of \mathbb{Q}) and $R = \mathcal{O}_K$ the ring of integers of K (that is the integral closure of \mathbb{Z} in K). Then R^\bullet is a Krull monoid with finite class group such that every class contains infinitely many primes. Every subring of \mathcal{O}_K with quotient field K is an order in K . If R_0 is an order, then $(R^\times : R_0^\times) < \infty$, $\text{Pic}(R_0)$ is finite and every class contains infinitely many invertible prime ideals.

Suppose that K is a quadratic number field, that is $[K : \mathbb{Q}] = 2$. Then K is of the form $K = \mathbb{Q}(\sqrt{d})$, where $d \in \mathbb{Z} \setminus \{0, 1\}$ is squarefree, and $\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\omega$, where

$$\omega = \frac{1 + \sqrt{d}}{2}, \text{ if } d \equiv 1 \pmod{4} \quad \text{and} \quad \omega = \sqrt{d}, \text{ if } d \equiv 2 \text{ or } 3 \pmod{4}.$$

For $f \in \mathbb{N}$, is

$$\mathcal{O}_{K,f} = \mathbb{Z} + \mathbb{Z}f\omega = \mathbb{Z} + f\mathcal{O}_K$$

the unique order of index f in \mathcal{O}_K . The group $\mathcal{O}_{K,f}^\times / \{\pm 1\}$ is cyclic.

2. Zero-sum sequences over abelian groups. Let G be an additive abelian group, $G_0 \subset G$ a non-empty subset and $\mathcal{F}(G_0)$ the free monoid with basis G_0 . Then

$$\mathcal{B}(G_0) = \{S = g_1 \cdot \dots \cdot g_l \mid l \in \mathbb{N}_0, g_1, \dots, g_l \in G_0 \text{ with } g_1 + \dots + g_l = 0\} \subset \mathcal{F}(G_0)$$

is the submonoid consisting of sequences with sum zero (*block monoid* over G_0). The embedding $\mathcal{B}(G_0) \subset \mathcal{F}(G_0)$ is a divisor homomorphism and $\mathcal{B}(G_0)$ is a Krull monoid. If $|G| \neq 2$, then $\mathcal{B}(G) \subset \mathcal{F}(G)$ is a divisor theory with class group isomorphic to G , and every class contains a prime.

3. Monoids of ideals.

- We have
- H is v -noetherian if and only if $(\mathcal{I}_v^*(H), \cdot_v)$ is v -noetherian. If this holds and $(R:\widehat{R}) \neq \emptyset$, then \widehat{H} is a Krull monoid.
 - H is a Krull monoid if and only if $(\mathcal{I}_v^*(H), \cdot_v)$ is a Krull monoid. If this holds, then $\mathcal{I}_v^*(H)$ is a free monoid.
 - R is a Mori domain if and only if $(\mathcal{I}_v^*(R), \cdot_v)$ is v -noetherian. Suppose that R is a Mori domain. Then (\mathcal{I}^*, \cdot) is v -noetherian. If R is noetherian or $(R:\widehat{R}) \neq \{0\}$, then \widehat{R} is a Krull domain.

4. The multiplicative monoid of regular elements of a Mori ring. A commutative ring is called a *Mori ring* if it satisfies the ascending chain condition on regular divisorial ideals [30]. Recall [24] that a commutative ring is called a *Marot ring* if each regular ideal of R is generated by regular elements.

Let R be a Marot ring. We denote by $\mathfrak{z}(R)$ the set of zerodivisors of R , and by T the total quotient ring of R . For any subset $I \subset T$ we put $I^\bullet = I \setminus \mathfrak{z}(T)$. Then R is a Mori ring if and only if R^\bullet is a v -noetherian monoid.

5. 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 [9]). 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 [11]), or if R is commutative local noetherian and \mathcal{C} is the class of all finitely generated R -modules (see [39] and Faccini-Hassler-Klingler-Wiegand [10]).

Sets of factorizations

Definition 1.2.

1. The free monoid $\mathbf{Z}(H) = \mathcal{F}(\mathcal{A}(H_{\text{red}}))$, whose basis is the set of atoms in H_{red} , is called the *factorization monoid* of H . The homomorphism

$$\pi_H = \pi: \mathbf{Z}(H) \rightarrow H_{\text{red}}, \quad \text{defined by } \pi(z) = \prod_{u \in \mathcal{A}(H_{\text{red}})} u^{\nu_u(z)},$$

is called the *factorization homomorphism* of H .

2. For $a \in H$, we set

$$\mathbf{Z}_H(a) = \mathbf{Z}(a) = \pi^{-1}(aH^\times) \subset \mathbf{Z}(H),$$

and we call the elements $z \in \mathbf{Z}(a)$ the *factorizations* of a .

We say that a has *unique factorization* if $|\mathbf{Z}(a)| = 1$.

3. The monoid H is said to be
 - *atomic* if $|\mathbf{Z}(a)| > 0$ for all $a \in H$.
 - *factorial* if $|\mathbf{Z}(a)| = 1$ for all $a \in H$.
 - an FF-monoid (a *finite factorization monoid*) if $0 < |\mathbf{Z}(a)| < \infty$ for all $a \in H$.

Theorem 1.3. *Every Krull monoid is an FF-monoid.*

Proposition 1.4. *Let H be an FF-monoid, $S \subset H$ a submonoid and $\rho: S \rightarrow S_{\text{red}}$ the canonical epimorphism.*

1. *Suppose that $\rho(cH^\times \cap S)$ is finite for every $c \in S$. Then S is an FF-monoid.*
2. *If $(H^\times : S^\times) < \infty$, then S is an FF-monoid.*
3. *Suppose that there exists an element $f \in H$ such that $fH \subset S$. Then S is an FF-monoid if and only if $(H^\times : S^\times) < \infty$.*

Exercise 1.5.

Every order in an algebraic number field is an FF-domain.

Exercise 1.6. *The integral domain*

$$R = \mathbb{R} + X\mathbb{C}[X] = \{f \in \mathbb{C}[X] \mid f(0) \in \mathbb{R}\} = \mathbb{R}[X, iX] \subset \mathbb{C}[X]$$

is a one-dimensional noetherian domain with integral closure $\overline{R} = \mathbb{C}[X]$, $(R:\overline{R}) \neq \{0\}$ but R is not an FF-domain (see [1, Example 4.1] by Anderson-Anderson-Zafrullah, 1990).

Sets of Lengths

Definition 1.7.

1. For a factorization $z = u_1 \cdot \dots \cdot u_k \in \mathbf{Z}(a)$, with $k \in \mathbb{N}_0$ and atoms u_1, \dots, u_k , we call $|z| = k$ the *length* of z . The set

$$\mathbf{L}_H(a) = \mathbf{L}(a) = \{|z| \mid z \in \mathbf{Z}(a)\} \subset \mathbb{N}_0$$

is called the *set of lengths* of a , and the set

$$\mathcal{L}(H) = \{\mathbf{L}(a) \mid a \in H\}$$

is called the *system of sets of lengths* of H .

2. Clearly, the monoid H is

- *atomic* if $|\mathbf{L}(a)| > 0$ for all $a \in H$.
Furthermore, the monoid H is said to be
- *half-factorial* if $|\mathbf{L}(a)| = 1$ for all $a \in H$.
- a BF-monoid (a *bounded factorization monoid*) if $0 < |\mathbf{L}(a)| < \infty$ for all $a \in H$.

Clearly, $\mathbf{L}(a) = \{0\}$ if and only if $a \in H^\times$ and $\mathbf{L}(a) = \{1\}$ if and only if a is an atom. Every every FF-monoid is a BF-monoid and every factorial monoid is half-factorial.

Half-factoriality found a lot of attention: David F. Anderson, Chapman, Coykendall, Smith et. al.

Theorem 1.8.

1. (Carlitz 1961) \mathcal{O}_K is half-factorial if and only if $|\mathcal{C}(\mathcal{O}_K)| \leq 2$.
2. (Halter-Koch 1983) The following statements are equivalent:

(a) $\mathcal{O}_{K,f}$ is half-factorial.

(b) \mathcal{O}_K is half-factorial, $\mathcal{O}_K = \mathcal{O}_{K,f}\mathcal{O}_K^\times$, and f is either a prime or twice an odd prime.

There is no generalization to general orders (for the local case see [27])

3. (Claborn) Every abelian group is (isomorphic to) the class group of a Dedekind domain.

Conjecture: Every abelian group is the class group of a half-factorial Dedekind domain (see [17]).

Exercise 1.9. Suppose that H is atomic but not half-factorial. Then for every $N \in \mathbb{N}$ there exists some $c \in H$ such that

$$|\mathbf{L}(c)| \geq N + 1.$$

Proof. If $a = u_1 \cdot \dots \cdot u_k = v_1 \cdot \dots \cdot v_l$ with $k < l$, then

$$c = a^N = (u_1 \cdot \dots \cdot u_k)^\nu (v_1 \cdot \dots \cdot v_l)^{N-\nu} \quad \text{for all } \nu \in [0, N]$$

whence $\{\nu k + l(N - \nu) \mid \nu \in [0, N]\} \subset \mathbf{L}(c)$. □

Theorem 1.10. Every v -noetherian monoid is a BF-monoid.

Definition 1.11.

1. For a non-empty subset $L \subset \mathbb{N}$, we call

$$\rho(L) = \sup \left\{ \frac{m}{n} \mid m, n \in L \right\} = \frac{\sup L}{\min L} \in \mathbb{Q}_{\geq 1} \cup \{\infty\}$$

the *elasticity* of L , and we set $\rho(\{0\}) = 1$.

2. Let H be atomic. For $a \in H$, we call $\rho(a) = \rho(\mathbf{L}(a))$ the *elasticity* of a and

$$\rho(H) = \sup \{ \rho(a) \mid a \in H \} = \sup \{ \rho(L) \mid L \in \mathcal{L}(H) \} \in \mathbb{R}_{\geq 1} \cup \{\infty\}$$

the *elasticity* of H .

3. For $k \in \mathbb{N}$, we set $\rho_k(H) = k$ if $H = H^\times$, and

$$\rho_k(H) = \sup \{ \sup L \mid L \in \mathcal{L}(H), \min L \leq k \} \in \mathbb{N} \cup \{\infty\}, \quad \text{if } H \neq H^\times.$$

Proposition 1.12. *Let H be atomic and $H \neq H^\times$.*

1. *For all $k, l \in \mathbb{N}$ we have $k \leq \rho_k(H) \leq k\rho(H)$ and $\rho_k(H) + \rho_l(H) \leq \rho_{k+l}(H)$.*

2. *For every $k \in \mathbb{N}$ we have*

$$\begin{aligned} \rho_k(H) &= \sup \{ \sup L \mid L \in \mathcal{L}(H), k \in L \} \\ &\geq \sup \{ \sup L \mid L \in \mathcal{L}(H), k = \min L \}, \end{aligned}$$

and equality holds, if either $\rho_k(H) < \infty$ or if H contains a prime element.

3. *We have*

$$\rho(H) = \sup \left\{ \frac{\rho_k(H)}{k} \mid k \in \mathbb{N} \right\} = \lim_{k \rightarrow \infty} \frac{\rho_k(H)}{k},$$

Definition 1.13. Let $\emptyset \neq L \subset \mathbb{Z}$ be a non-empty subset.

1. A positive integer $d \in \mathbb{N}$ is called a *distance* of L if there exists some $l \in L$ such that $L \cap [l, l + d] = \{l, l + d\}$. We denote by $\Delta(L)$ the *set of all distances* of L .
Note that $\Delta(L) = \emptyset$ if and only if $|L| = 1$.
2. L is called an *arithmetical progression* (with *difference* $d \in \mathbb{N}$) if $\Delta(L) \subset \{d\}$. In particular, if $|L| = 1$, then L is an arithmetical progression with difference d for every $d \in \mathbb{N}$.
3. For a system \mathcal{L} of non-empty subsets of \mathbb{Z} we call

$$\Delta(\mathcal{L}) = \bigcup_{L \in \mathcal{L}} \Delta(L) \subset \mathbb{N} \quad \text{the set of distances of } \mathcal{L} .$$

4. We call

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

the *set of distances* of H .

Clearly,

$$H \quad \text{is half-factorial if and only if} \quad \Delta(H) = \emptyset ,$$

and $|\Delta(H)| = 1$ if and only if all sets of lengths are arithmetical progressions with the same difference.

Lemma 1.14. *If H is atomic and $\Delta(H)$ is finite, then $\min \Delta(H) = \gcd \Delta(H)$.*

Theorem 1.15. *Suppose that H is a Krull monoid with finite class group. Then $\Delta(H)$ is finite, $\rho(H) < \infty$ and $\rho_k(H) < \infty$ for all $k \in \mathbb{N}$.*

Proposition 1.16.

1. *Every order R of an algebraic number field has a finite set of distances $\Delta(R)$.*
2. *Let $R = \mathbb{Z}[\sqrt{-7}]$. Then $\rho_2(R) = \rho(R) = \infty$.*

Theorem 1.17 (Kainrath, 2005, [26]).

1. *For a finitely generated domain R the following statements are equivalent:*
 - (a) *$\mathcal{C}(\overline{R})$ and \overline{R}/R are both finite and the natural map $\text{spec}(\overline{R}) \rightarrow \text{spec}(R)$ is injective.*
 - (b) *$\rho(R) < \infty$.*
 - (c) *$\rho_k(R) < \infty$ for all $k \in \mathbb{N}$.*
2. *Suppose that R is a finitely generated k -algebra for some infinite perfect field k . Let \overline{k} denote the algebraic closure of k in \overline{R} and $\mathfrak{f} = (R:\overline{R})$. Then the following statements are equivalent:*
 - (a) *$\mathcal{C}(\overline{R})$ is finite and $\overline{R} = \overline{k} + \mathfrak{f}$.*
 - (b) *$\rho(R) < \infty$.*
 - (c) *$\rho_k(R) < \infty$ for all $k \in \mathbb{N}$.**If $\rho(R) < \infty$, then $\rho(R) = \rho(\overline{R})$.*

Almost arithmetical multiprogressions

Definition 1.18. Let $d \in \mathbb{N}$, $l, M \in \mathbb{N}_0$ and $\{0, d\} \subset \mathcal{D} \subset [0, d]$. A subset $L \subset \mathbb{Z}$ is called an

- *arithmetical multiprogression* (AMP for short) with *difference* d , *period* \mathcal{D} and *length* l , if L is an interval of $\min L + \mathcal{D} + d\mathbb{Z}$ (in part., $L \neq \emptyset$), and l is maximal such that $\min L + ld \in L$.
- *almost arithmetical multiprogression* (AAMP for short) with *difference* d , *period* \mathcal{D} , *length* l and *bound* M , if

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

where L^* is an AMP with difference d (whence $L^* \neq \emptyset$), period \mathcal{D} and length l such that $\min L^* = 0$, $L' \subset [-M, -1]$, $L'' \subset \max L^* + [1, M]$ and $y \in \mathbb{Z}$.

We call $y + L'$ the *initial part*, $y + L^*$ the *central part* and $y + L''$ the *end part* of L .

- *almost arithmetical progression* (AAP for short) with *difference* d , *bound* M and *length* l , if it is an AAMP with difference d , period $\{0, d\}$, bound M and length l .

Note that

- AMPs, AAMPs and AAPs are finite non-empty subsets of \mathbb{Z} ,
- The definition of an AAMP is *shift invariant*
- $L^* = (\mathcal{D} + d\mathbb{Z}) \cap [0, \max L^*]$.

Theorem 1.19.

Let H be a Krull monoid with finite class group G . Then there exist $M \in \mathbb{N}_0$ and a finite set $\Delta^(G) \subset \Delta(H)$ ($\Delta^*(G)$ will be defined on Friday) such that the following holds: every $L \in \mathcal{L}(H)$ is an AAMP with difference $d \in \Delta^*$ and bound M .*

Theorem 1.20 (W.A. Schmid, 2007, [38]).

Let $M \in \mathbb{N}_0$ and $\Delta^ \subset \mathbb{N}$ be a finite non-empty set. Then there exists a Krull monoid H with finite class group such that the following holds: for every AAMP L with difference $d \in \Delta^*$ and bound M there is some $y_{H,L} \in \mathbb{N}$ such that*

$$y + L \in \mathcal{L}(H) \quad \text{for all } y \geq y_{H,L}.$$

Indeed, there exists an algebraic number field such that its ring of integers has this property.

Theorem 1.21 (F. Kainrath, 1999, [25]).

Suppose that H is a Krull monoid with infinite class group such that every class contains a prime. Then for every finite set $L \subset \mathbb{N}_{\geq 2}$ there is an $a \in H$ such that $\mathsf{L}(a) = L$.

The assumption that every class contains a prime is indispensable (recall, that it is conjectured that for given G there is a half-factorial Dedekind domain with class group G).

Suppose that not every class contains a prime: see Chapman-David Anderson-Smith [3], Hassler [22]

Distance of factorizations and catenary degree

Definition 1.22.

1. Let $z, z' \in \mathbf{Z}(H)$, say

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

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

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

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

2. Let $z, z' \in \mathbf{Z}(H)$ 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 $z = z_0, z_1, \dots, z_k = z'$ in $\mathbf{Z}(a)$ such that $\mathbf{d}(z_{i-1}, z_i) \leq N$ for all $i \in [1, k]$.

3. For an element $a \in H$, we define its *catenary degree* $\mathbf{c}(a)$ 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

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

The catenary degree $\mathbf{c}(a)$ measures how complex the set of factorizations of a is. Note that by definition we have either $\mathbf{c}(a) = 0$ or $\mathbf{c}(a) \geq 2$.

Exercise 1.23. *The distance function $d: \mathbf{Z}(H) \times \mathbf{Z}(H) \rightarrow \mathbb{N}_0$ is a metric satisfying $d(xz, xz') = d(z, z')$ for all $x, z, z' \in \mathbf{Z}(H)$.*

Exercise 1.24. *If H is atomic but not factorial, then for every $k \in \mathbb{N}$ there exists some $a \in H$ such that $|\mathbf{Z}(a)| \geq k+1$, and there exist factorizations $z, z' \in \mathbf{Z}(a)$ such that $d(z, z') \geq 2k$.*

Exercise 1.25. *Let H be atomic and $a \in H$.*

1. $c(a) \leq \sup \mathbf{L}(a)$, and $c(a) = 0$ if and only if $|\mathbf{Z}(a)| = 1$.
2. If $z, z' \in \mathbf{Z}(a)$ and $z \neq z'$, then $2 + \left| |z| - |z'| \right| \leq d(z, z')$.
3. If $|\mathbf{Z}(a)| \geq 2$, then $2 + \sup \Delta(\mathbf{L}(a)) \leq c(a)$.
4. If $c(a) \leq 2$, then $|\mathbf{L}(a)| = 1$, and if $c(a) \leq 3$, then $\mathbf{L}(a)$ is an arithmetical progression with difference 1.

Exercise 1.26. *Suppose that H is atomic.*

1. H is factorial if and only if $c(H) = 0$.
2. If H is not factorial, then $2 + \sup \Delta(H) \leq c(H)$. In particular, if $c(H) < \infty$, then $\Delta(H)$ is finite.
3. If $c(H) = 2$, then H is half-factorial.
4. If $c(H) = 3$, then every $L \in \mathcal{L}(H)$ is an arithmetical progression with difference 1.

Example 1.27. There is a half-factorial Dedekind domain R with infinite catenary degree $c(R)$.

The omega invariants and the tame degrees

Definition 1.28. Suppose that H is atomic.

1. For $a, b \in H$ let $\omega(a, b)$ denote the smallest $N \in \mathbb{N}_0 \cup \{\infty\}$ with the following property:

For all $n \in \mathbb{N}$ and $a_1, \dots, a_n \in H$, if $a = a_1 \cdot \dots \cdot a_n$ and $b \mid a$, then there exists a subset $\Omega \subset [1, n]$ such that $|\Omega| \leq N$ and

$$b \mid \prod_{\nu \in \Omega} a_\nu.$$

In particular, if $b \nmid a$, then $\omega(a, b) = 0$. For $b \in H$ we define

$$\omega(H, b) = \sup \{ \omega(a, b) \mid a \in H \} \in \mathbb{N}_0 \cup \{\infty\}.$$

By definition, $b \in H$ is a prime if and only if $\omega(H, b) = 1$.

2. For $k \in \mathbb{N}$ and $b \in H$ we set

$$\tau_k(H, b) = \sup \left\{ \min \mathbf{L}(b^{-1}a) \mid a = u_1 \cdot \dots \cdot u_j \in bH \text{ with } j \in [0, k], \right. \\ \left. u_1, \dots, u_j \in \mathcal{A}(H) \text{ and } b \nmid u_i^{-1}a \text{ for all } i \in [1, j] \right\} \in \mathbb{N}_0 \cup \{\infty\}$$

and

$$\tau(H, b) = \sup \{ \tau_k(H, b) \mid k \in \mathbb{N} \} \in \mathbb{N}_0 \cup \{\infty\}.$$

3. For $a \in H$ and $x \in \mathbf{Z}(H)$ let $\mathbf{t}(a, x) \in \mathbb{N}_0 \cup \{\infty\}$ denote the smallest $N \in \mathbb{N}_0 \cup \{\infty\}$ with the following property:

If $\mathbf{Z}(a) \cap x\mathbf{Z}(H) \neq \emptyset$ and $z \in \mathbf{Z}(a)$, then there exists $z' \in \mathbf{Z}(a) \cap x\mathbf{Z}(H)$ such that $\mathbf{d}(z, z') \leq N$.

For subsets $H' \subset H$ and $X \subset \mathbf{Z}(H)$, we define

$$\mathbf{t}(H', X) = \sup \{ \mathbf{t}(a, x) \mid a \in H', x \in X \} \in \mathbb{N}_0 \cup \{\infty\}.$$

H is called *locally tame* if $\mathbf{t}(H, u) < \infty$ for all $u \in \mathcal{A}(H_{\text{red}})$ (equivalently, $\mathbf{t}(H, \mathbf{z}(c)) < \infty$ for all $c \in H$).

Exercise 1.29. *If H is atomic and $\omega(H, b) < \infty$ for all $b \in H$, then H is a BF-monoid.*

Proposition 1.30. *Suppose that H is atomic and $u \in \mathcal{A}(H)$.*

If u is prime, then

$(\mathfrak{t}(H, uH^\times), \omega(H, u), \tau_1(H, u)) = (0, 1, 0)$, and otherwise

$$\mathfrak{t}(H, uH^\times) = \max\{\omega(H, u), 1 + \tau(H, u)\} \in \mathbb{N}_{\geq 2} \cup \{\infty\}.$$

In particular, H is locally tame if and only if $\omega(H, v) < \infty$ and $\tau(H, v) < \infty$ for all $v \in \mathcal{A}(H)$.

Theorem 1.31 (G+Hassler, 2007, [20]).

If H is v -noetherian, then $\omega(H, b) < \infty$ for all $b \in H$.

Theorem 1.32. *Suppose that H is a Krull monoid with finite class group. Then H is locally tame and has finite catenary degree $\mathfrak{c}(H)$.*

Theorem 1.33. *Suppose that H is a Krull monoid with class group G such that every class contains a prime.*

Then the following statements are equivalent:

1. G is finite.
2. H is locally tame.
3. $\mathfrak{t}(H, u) < \infty$ for some $u \in \mathcal{A}(H_{\text{red}})$ that is not prime.

2. TRANSFER PRINCIPLES - THE KRULL CASE

The general idea

Definition 2.1. A monoid homomorphism $\theta: H \rightarrow B$ 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 $\theta(w) \simeq c$.

STRATEGY

- Study the arithmetic in B
- Shift the arithmetical results from B back to H .

Transfer homomorphisms have nice properties:

- $\theta: H \rightarrow D$ is a transfer homomorphism if and only if $\theta_{\text{red}}: H_{\text{red}} \rightarrow B_{\text{red}}$ is a transfer homomorphism.
- Compositions of transfer homomorphisms are transfer homomorphisms.

Proposition 2.2. *Let $\theta: H \rightarrow B$ be a transfer homomorphism and $u \in H$.*

1. *If $n \in \mathbb{N}$, $b_1, \dots, b_n \in B$ and $\theta(u) \simeq b_1 \cdot \dots \cdot b_n$, then there exist $u_1, \dots, u_n \in H$ such that $u \simeq u_1 \cdot \dots \cdot u_n$ and $\theta(u_\nu) \simeq b_\nu$ for all $\nu \in [1, n]$.*
2. *u is an atom of H if and only if $\theta(u)$ is an atom of B .*
3. *There is a unique homomorphism $\bar{\theta}: \mathbf{Z}(H) \rightarrow \mathbf{Z}(B)$ satisfying*

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

$\bar{\theta}$ is surjective and induces the commutative diagram

$$\begin{array}{ccc} \mathbf{Z}(H) & \xrightarrow{\bar{\theta}} & \mathbf{Z}(B) \\ \pi_H \downarrow & & \downarrow \pi_B \\ H_{\text{red}} & \xrightarrow{\theta_{\text{red}}} & B_{\text{red}}. \end{array}$$

Moreover it has the following additional properties:

- (a) *If $z, z' \in \mathbf{Z}(H)$, then $|\bar{\theta}(z)| = |z|$ and $\mathbf{d}(\bar{\theta}(z), \bar{\theta}(z')) \leq \mathbf{d}(z, z')$.*
 - (b) *$\bar{\theta}(\mathbf{Z}_H(u)) = \mathbf{Z}_B(\theta(u))$ and $\mathbf{L}_H(u) = \mathbf{L}_B(\theta(u))$.*
 - (c) *If $z \in \mathbf{Z}(u)$ and $\bar{y} \in \mathbf{Z}(\theta(u))$, then there exists some $y \in \mathbf{Z}(u)$ such that $\bar{\theta}(y) = \bar{y}$, $\bar{\theta}(\gcd(z, y)) = \gcd(\bar{\theta}(z), \bar{y})$ and $\mathbf{d}(z, y) = \mathbf{d}(\bar{\theta}(z), \bar{y})$.*
4. *H is atomic if and only if B is atomic.*
 5. *If H is atomic, then $\mathcal{L}(H) = \mathcal{L}(B)$, $\rho(H) = \rho(B)$, H has accepted elasticity if and only if B has accepted elasticity, and H is a BF-monoid if and only if B is a BF-monoid.*

Definition 2.3. Let $\theta: H \rightarrow B$ be a transfer homomorphism of atomic monoids and $\bar{\theta}: \mathbf{Z}(H) \rightarrow \mathbf{Z}(B)$ the unique homomorphism satisfying $\bar{\theta}(uH^\times) = \theta(u)B^\times$ for all $u \in \mathcal{A}(H)$. We call $\bar{\theta}$ the *extension of θ to the factorization monoids*.

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

If $z, z' \in \mathbf{Z}_H(a)$ and $\bar{\theta}(z) = \bar{\theta}(z')$, then there exist some $k \in \mathbb{N}_0$ and factorizations $z = z_0, \dots, z_k = z' \in \mathbf{Z}_H(a)$ such that $\bar{\theta}(z_i) = \bar{\theta}(z)$ and $\mathbf{d}(z_{i-1}, z_i) \leq N$ for all $i \in [1, k]$ (that is, z and z' can be concatenated by an N -chain in the fiber $\mathbf{Z}_H(a) \cap \bar{\theta}^{-1}(\bar{\theta}(z))$).

We define

$$\mathbf{c}(H, \theta) = \sup\{\mathbf{c}(a, \theta) \mid a \in H\} \in \mathbb{N}_0 \cup \{\infty\}.$$

2. (*Tame degree in the fibres*) For $a \in H$ and $x \in \mathbf{Z}(H)$, we denote by $\mathbf{t}(a, x, \theta)$ the smallest $N \in \mathbb{N}_0 \cup \{\infty\}$ with the following property:

If $\mathbf{Z}(a) \cap x\mathbf{Z}(H) \neq \emptyset$, $z \in \mathbf{Z}(a)$ and $\bar{\theta}(z) \in \bar{\theta}(x)\mathbf{Z}(B)$, then there exists some $z' \in \mathbf{Z}(a) \cap x\mathbf{Z}(H)$ such that $\bar{\theta}(z') = \bar{\theta}(z)$ and $\mathbf{d}(z, z') \leq N$.

We define

$$\mathbf{t}(H, x, \theta) = \sup\{\mathbf{t}(a, x, \theta) \mid a \in H\} \in \mathbb{N}_0 \cup \{\infty\}.$$

Theorem 2.4. *Let $\theta: H \rightarrow B$ be a transfer homomorphism of atomic monoids and $\bar{\theta}: Z(H) \rightarrow Z(B)$ its extension to the factorization monoids.*

1. *If $a \in H$ and $x \in Z(H)$, then either $\mathfrak{t}(a, x) = 0$ or*

$$\mathfrak{t}(\theta(a), \bar{\theta}(x)) \leq \mathfrak{t}(a, x) \leq \mathfrak{t}(\theta(a), \bar{\theta}(x)) + \mathfrak{t}(a, x, \theta).$$

In particular, if $u \in \mathcal{A}(H_{\text{red}})$, then

$$\mathfrak{t}(B, \bar{\theta}(u)) \leq \mathfrak{t}(H, u) \leq \mathfrak{t}(B, \bar{\theta}(u)) + \mathfrak{t}(H, u, \theta).$$

2. $\mathfrak{t}(B) \leq \mathfrak{t}(H)$, and if H is locally tame, then so is B .
3. If B is locally tame and $\mathfrak{t}(H, u, \theta) < \infty$ for all $u \in \mathcal{A}(H_{\text{red}})$, then H is locally tame.
4. If $a \in H$, then $\mathfrak{c}(\theta(a)) \leq \mathfrak{c}(a) \leq \max\{\mathfrak{c}(\theta(a)), \mathfrak{c}(a, \theta)\}$.
5. $\mathfrak{c}(B) \leq \mathfrak{c}(H) \leq \max\{\mathfrak{c}(B), \mathfrak{c}(H, \theta)\}$.

Chains can be lifted

1. Let $\bar{z}, \bar{z}' \in Z(\theta(a))$, $k \in \mathbb{N}_0$ and $z_0, z_1, \dots, z_k \in Z(a)$ such that $\bar{\theta}(z_0) = \bar{z}$ and $\bar{\theta}(z_k) = \bar{z}'$. Then $\bar{\theta}(z_0), \dots, \bar{\theta}(z_k) \in Z(\theta(a))$, $\mathfrak{d}(\bar{\theta}(z_{i-1}), \bar{\theta}(z_i)) \leq \mathfrak{d}(z_{i-1}, z_i)$ for all $i \in [1, k]$, and in particular $\mathfrak{c}(\theta(a)) \leq \mathfrak{c}(a)$.
2. Let $z, z' \in Z(a)$, $k \in \mathbb{N}_0$ and $\bar{z}_0, \bar{z}_1, \dots, \bar{z}_k \in Z(\theta(a))$ such that $\bar{\theta}(z) = \bar{z}_0$ and $\bar{\theta}(z') = \bar{z}_k$. Then there exists some $m \geq k$ and there exist factorizations $z = z_0, z_1, \dots, z_k, z_{k+1}, \dots, z_m = z' \in Z(a)$ such that

$$\bar{\theta}(z_i) = \bar{z}_i, \quad \mathfrak{d}(z_{i-1}, z_i) = \mathfrak{d}(\bar{z}_{i-1}, \bar{z}_i) \quad \text{for all } i \in [1, k]$$

and

$$\bar{\theta}(z_j) = \bar{z}_k, \quad \mathfrak{d}(z_{j-1}, z_j) \leq \mathfrak{c}(a, \theta) \quad \text{for all } j \in [k+1, m].$$

In particular, $\mathfrak{c}(a) \leq \max\{\mathfrak{c}(\theta(a)), \mathfrak{c}(a, \theta)\}$.

Monoid of zero-sum sequences

Let G be an additive abelian group and $\emptyset \neq G_0 \subset G$ a non-empty subset.

Definition 2.5.

1. Let $\mathcal{F}(G_0)$ be the free (multiplicative) monoid with basis G_0 . The elements of $\mathcal{F}(G_0)$ are called *sequences* over G_0 . We write sequences $S \in \mathcal{F}(G_0)$ in the form

$$S = \prod_{g \in G_0} g^{\mathbf{v}_g(S)} = g_1 \cdot \dots \cdot g_l \in \mathcal{F}(G_0),$$

where $\mathbf{v}_g(S) \in \mathbb{N}_0$ and $\mathbf{v}_g(S) = 0$ for almost all $g \in G$.

The term *sequences* stems from Combinatorial/Additive Number Theory (for a survey see [14], and for applications to geometry see [7, 6]).

Transfer Principles transport

”arithmetical problems” to ”zero- sum problems”

A paper by Erdős-Ginzburg-Ziv ([8], 1961) is considered as a starting paper in the zero-sum area.

We call $\mathbf{v}_g(S)$ the *multiplicity* of g in S , and we say that S *contains* g , if $\mathbf{v}_g(S) > 0$. S is called *squarefree* (in $\mathcal{F}(G)$) if $\mathbf{v}_g(S) \leq 1$ for all $g \in G$. The unit element $1 \in \mathcal{F}(G)$ is called the *empty sequence*. A sequence S_1 is called a *subsequence* of S if $S_1 \mid S$ in $\mathcal{F}(G)$ (equivalently, $\mathbf{v}_g(S_1) \leq \mathbf{v}_g(S)$ for all $g \in G$), and it is called a *proper subsequence* of S if it is a subsequence with $1 \neq S_1 \neq S$.

2. We call

$$|S| = l = \sum_{g \in G_0} \mathbf{v}_g(S) \in \mathbb{N}_0 \quad \text{the length of } S,$$

$$\text{supp}(S) = \{g \in G \mid \mathbf{v}_g(S) > 0\} \subset G \quad \text{the support of } S,$$

$$\sigma(S) = \sum_{i=1}^l g_i = \sum_{g \in G} \mathbf{v}_g(S)g \in G \quad \text{the sum of } S$$

and

$$\Sigma(S) = \left\{ \sum_{i \in I} g_i \mid \emptyset \neq I \subset [1, l] \right\} = \{ \sigma(T) \mid T \mid S, T \neq 1 \}$$

the set of subsums of S .

By definition, $\Sigma(S) \subset G$ consists of all sums of all non-empty subsequences of S . A sequence S is called a *zero-sumfree sequence* if $0 \notin \Sigma(S)$.

3. We denote by $\mathcal{B}(G_0) = \{S \in \mathcal{F}(G_0) \mid \sigma(S) = 0\}$ the *monoid of zero-sum sequences* (*block monoid*) over G . The elements of $\mathcal{B}(G_0)$ are called *zero-sum sequences*, and the atoms of $\mathcal{B}(G_0)$ are called *minimal zero-sum sequences*. We denote by $\mathcal{A}(G_0)$ the set of all minimal zero-sum sequences.

4. We define the *Davenport constant* of G_0 by

$$\mathbf{D}(G_0) = \sup\{|U| \mid U \in \mathcal{A}(G_0)\} \in \mathbb{N}_0 \cup \{\infty\}$$

and we define the *little Davenport constant* $\mathbf{d}(G_0)$ as

$$\mathbf{d}(G_0) = \sup\{|S| \mid S \in \mathcal{F}(G_0) \text{ is zero-sumfree}\} \in \mathbb{N}_0 \cup \{\infty\}.$$

Proposition 2.6 (Structure of block monoids). *Let G be an additive abelian group and $G_0 \subset G$ a non-empty subset.*

1. $\mathcal{B}(G_0) = \mathcal{B}(G) \cap \mathcal{F}(G_0)$ is a divisor-closed submonoid of $\mathcal{B}(G)$ and a saturated submonoid of $\mathcal{F}(G_0)$. In particular, $\mathcal{B}(G_0)$ is a reduced Krull monoid.
2. $\mathcal{B}(G_0) \subset \mathcal{F}(G_0)$ is a divisor theory if and only if $\langle G_0 \rangle = [G_0 \setminus \{g\}]$ for every $g \in G_0$.
3. If $H \subset \mathcal{B}(G_0)$ is a divisor-closed submonoid, then $H = \mathcal{B}(G_1)$ for some subset $G_1 \subset G_0$.
4. If $|G| \neq 2$, then $\mathcal{F}(G)$ is a monoid of divisors for $\mathcal{B}(G)$, $\mathcal{C}(\mathcal{B}(G)) \cong G$, and every divisor class of $\mathcal{B}(G)$ contains exactly one prime divisor.
5. If $|G| = 2$, $G = \{0, g\}$, then $\mathcal{B}(G) = \mathcal{F}(\{0, g^2\}) \cong \mathbb{N}_0^2$.
6. $\mathcal{B}(G)$ is factorial if and only if $|G| \leq 2$.

Theorem 2.7. *Let G be an additive abelian group and $G_0 \subset G$.*

1. Let G_0 be finite. Then $\mathcal{B}(G_0)$ is a reduced finitely generated Krull monoid. In particular, $\mathcal{A}(G_0)$ is finite, $\mathsf{D}(G_0) < \infty$, $\mathsf{D}(G_0) \leq 1 + \mathsf{d}(G_0)$ and $\mathsf{D}(G) = 1 + \mathsf{d}(G)$.
2. If $\mathsf{r}^*(G) < \infty$ and $\mathsf{D}(G_0) < \infty$, then there exists a finite subset $G_1 \subset G_0$ such that $\mathcal{B}(G_1) = \mathcal{B}(G_0)$.
3. If $G = [G_0]$, then the following statements are equivalent:
 - (a) G_0 is finite.
 - (b) $\mathsf{r}^*(G) < \infty$ and $\mathsf{D}(G_0) < \infty$.
 - (c) $\mathcal{B}(G_0)$ is finitely generated.

Krull monoids

Let H be a reduced Krull monoid, $F = \mathcal{F}(P)$ a free monoid such that $H \subset F$ is a saturated and cofinal submonoid, and $G = \mathfrak{q}(F)/\mathfrak{q}(H)$. Let $G_P = \{[p] = p\mathfrak{q}(H) \mid p \in P\} \subset G$ be the set of all classes containing primes and $D(G_P)$ the Davenport constant of G_P .

Consider the following diagram

$$\begin{array}{ccc} H & \longrightarrow & \mathcal{F}(P) \\ \beta \downarrow & & \downarrow \tilde{\beta} \\ \mathcal{B}(G_P) & \longrightarrow & \mathcal{F}(G_P) \end{array}$$

where $\tilde{\beta}$ is defined as follows

If $a = p_1 \cdot \dots \cdot p_l \in F$, then $\tilde{\beta}(a) = [p_1] \cdot \dots \cdot [p_l] = g_1 \cdot \dots \cdot g_l = S \in \mathcal{F}(G_P)$.

$\tilde{\beta}: F \rightarrow \mathcal{F}(G_P)$ is called the *class homomorphism* and $\beta = \tilde{\beta} \mid H: H \rightarrow \mathcal{B}(G_P)$ the *block homomorphism* of $H \subset F$.

NOTATION

For every arithmetical invariant $*(H)$ defined for a monoid H , we write $*(G_0)$ instead of $*(\mathcal{B}(G_0))$.

For example, we set

$$\mathcal{A}(G_0) = \mathcal{A}(\mathcal{B}(G_0)),$$

$$\mathcal{L}(G_0) = \mathcal{L}(\mathcal{B}(G_0)),$$

$$\Delta(G_0) = \Delta(\mathcal{B}(G_0))$$

and so on

Theorem 2.8.

The block homomorphism $\beta = \tilde{\beta} \mid H: H \rightarrow \mathcal{B}(G_P)$ is a transfer homomorphism

(W. Narkiewicz, 1979, [31])

In particular, we have:

- $a \in H \iff \tilde{\beta}(a) \in \mathcal{B}(G_P)$ (that is, the sequence of classes is a zero-sum sequence)
- a is an atom of $H \iff \tilde{\beta}(a)$ is a minimal zero-sum sequence
- $D(G_P)$ is the supremum of all $k \in \mathbb{N}_0 \cup \{\infty\}$ with the following property:

There exists an atom $u \in \mathcal{A}(H)$ such that u is a product of k primes in F .

Historical Remark: H. Davenport 1966: $D(G)$ is the maximal number of prime ideals occurring in the prime ideal decomposition of an irreducible element.

This was observed by K. Rogers in a paper [35] published in 1963.

- S is zero-sumfree if and only if a is not divisible by an element of $H \setminus H^\times$.

In particular, $d(G_P)$ is the supremum of all $k \in \mathbb{N}_0 \cup \{\infty\}$ with the following property:

There are primes $p_1, \dots, p_k \in P$ such that their product $p_1 \cdot \dots \cdot p_k$ is not divisible by any element of $H \setminus H^\times$.

Theorem 2.9. *Let H be a reduced Krull monoid, $F = \mathcal{F}(P)$ a free monoid such that $H \subset F$ is a saturated and cofinal submonoid, and $G = \mathfrak{q}(F)/\mathfrak{q}(H)$. Let $G_P \subset G$ be the set of all classes containing primes and $\mathbf{D} = \mathbf{D}(G_P)$. Let $\tilde{\beta}: F \rightarrow \mathcal{F}(G_P)$ be the class homomorphism and $\beta = \tilde{\beta}|_H: H \rightarrow \mathcal{B}(G_P)$ the block homomorphism of $H \subset F$.*

1. *H is an FF-monoid, $\tilde{\beta}(H) = \mathcal{B}(G_P)$, $\tilde{\beta}^{-1}(\mathcal{B}(G_P)) = H$, and β is a transfer homomorphism with the following properties:*

- $\mathbf{c}(H, \beta) \leq 2$.
- $\mathbf{c}(\beta(a)) \leq \mathbf{c}(a) \leq \max\{\mathbf{c}(\beta(a)), 2\}$ for all $a \in H$.
- $\mathbf{t}(H, u, \beta) \leq \mathbf{D} + 1$ for all $u \in \mathcal{A}(H)$.

2. *There exists a unique homomorphism $\bar{\beta}: \mathbf{Z}(H) \rightarrow \mathbf{Z}(\mathcal{B}(G_P))$ such that $\bar{\beta}(u) = \beta(u)$ for all $u \in \mathcal{A}(H)$. For every $a \in H$ we have $\bar{\beta}(\mathbf{Z}(a)) = \mathbf{Z}(\beta(a))$, $|\bar{\beta}(z)| = |z|$ for all $z \in \mathbf{Z}(a)$, and if $\beta(a)$ is squarefree in $\mathcal{F}(G)$, then $|\mathbf{Z}(a)| = |\mathbf{Z}(\beta(a))|$.*

3. $\mathcal{L}(H) = \mathcal{L}(G_P)$. *In particular, $\Delta(H) = \Delta(G_P)$, $\rho_k(H) = \rho_k(G_P)$ for all $k \in \mathbb{N}$, and $\rho(H) = \rho(G_P)$.*

4. *If $k \in \mathbb{N}$ and $\mathbf{D} \geq 2$, then*

$$\rho_k(H) \leq k\rho(H) \leq \frac{k\mathbf{D}}{d}, \quad \text{where } d = \min\{|u|_F \mid u \in \mathcal{A}(H), u \text{ not prime}\}.$$

If $G_P = -G_P$, $\mathbf{D} \geq 2$ and k is even, then $d = 2$ and $2\rho_k(H) = k\mathbf{D}$.

5. $\mathbf{c}(G_P) \leq \mathbf{c}(H) \leq \max\{\mathbf{c}(G_P), 2\}$ and $\mathbf{c}(H) \leq \mathbf{D}$.

6. *If $u \in \mathcal{A}(H)$ and $U = \beta(u)$, then*

$$\mathbf{t}(G_P, U) \leq \mathbf{t}(H, u) \leq \mathbf{t}(G_P, U) + \mathbf{D} + 1,$$

and if $d = |u|_F = |U|$, then

$$\mathbf{t}(H, u) \leq \max\left\{\mathbf{t}(G_P, U), \frac{3 + (d-1)(\mathbf{D}-1)}{2}\right\} \leq 1 + \frac{d(\mathbf{D}-1)}{2}.$$

In particular, $\mathfrak{t}(G_P) \leq \mathfrak{t}(H) \leq \mathfrak{t}(G_P) + D$, and

$$\mathfrak{t}(H) \leq \max\left\{\mathfrak{t}(G_P), \frac{3 + (D - 1)^2}{2}\right\} \leq 1 + \frac{D(D - 1)}{2}.$$

If $G_P = -G_P$ and H is not factorial, then $\mathfrak{t}(H) \geq D$.

Summary .

- The elasticities $\rho_k(H)$ and $\rho(H)$, the set of distances $\Delta(H)$, the catenary degree $\mathfrak{c}(H)$ and the local tame degrees $\mathfrak{t}(H, u)$ are bounded above by a rational expression in $D(G_P)$.
- If G_P is finite, then $\mathcal{B}(G_P)$ is finitely generated and $D(G_P)$ is finite.
- If G_P is finite, then it suffices to prove the Structure Theorem for Sets of Lengths for $\mathcal{B}(G_P)$, that is for a finitely generated monoid.
- OPEN PROBLEM: Suppose that $D(G_P)$ is finite:
Does the Structure Theorem for Sets of Lengths hold for H ?

Summary for the special case $G_P = G$ finite with $|G| \geq 3$.

- All invariants dealing with lengths of factorizations in H coincide with the corresponding invariants in $\mathcal{B}(G)$:

$$\mathcal{L}(H) = \mathcal{L}(G).$$

In particular, we have:

$$\rho_k(H) = \rho_k(G), \quad \rho(H) = \rho(G) \quad \text{and} \quad \Delta(H) = \Delta(G).$$

- The catenary degrees coincide:

$$\mathbf{c}(H) = \mathbf{c}(G).$$

- Unfortunately, the tame degrees do not coincide:

$$\mathbf{D}(G) \leq \mathbf{t}(G) \leq \mathbf{t}(H)$$

and, in general, we have inequality holds, that is $\mathbf{t}(G) < \mathbf{t}(H)$.

All what is known up to now is the following

Theorem 2.10. *Let H be a Krull monoid with class group $G \cong C_2^{2s}$ for some $s \in \mathbb{N}$, and suppose that every class contains a prime. Then*

$$\mathbf{t}(G) = \mathbf{t}(H) = 1 + 2s^2.$$

Weakly Krull domains

Weakly Krull domains were introduced by Anderson-Mott-Zafrullah in 1992 (see [2]). We restrict to the v -noetherian case.

Definition 2.11. R is called a *weakly Krull domain* if R is a Mori domain and $v\text{-max}(R) = \mathfrak{X}(R)$.

Every Krull domain which is not a field is weakly Krull, every one-dimensional Mori domain is weakly Krull, and in particular orders in algebraic number fields are weakly Krull domains.

STRATEGY

- We have

$$R = \bigcap_{\mathfrak{p} \in \mathfrak{X}(R)} R_{\mathfrak{p}}$$

- Study the arithmetic of the localizations $R_{\mathfrak{p}}$
- Show that

$$R^{\bullet} \rightarrow \mathcal{I}_v^*(R) \xrightarrow{\sim} \prod_{\mathfrak{p} \in \mathfrak{X}(R)} (R_{\mathfrak{p}}^{\bullet})_{\text{red}}$$

is a divisor homomorphism.

- Shift the arithmetical results from $\mathcal{I}_v^*(R)$ back to R .

Definition 2.12 (Primary monoids).

1. An element $q \in H$ is called *primary* if $q \notin H^\times$ and, for all $a, b \in H$, if $q \mid ab$ and $q \nmid a$, then $q \mid b^n$ for some $n \in \mathbb{N}$.
2. H is called *primary* if $\mathfrak{m} = H \setminus H^\times \neq \emptyset$ and one of the following equivalent statements are satisfied:
 - (a) $s\text{-spec}(H) = \{\emptyset, H \setminus H^\times\}$.
 - (b) Every $q \in \mathfrak{m}$ is primary.
 - (c) For all $a, b \in \mathfrak{m}$ there exists some $n \in \mathbb{N}$ such that $a \mid b^n$.

Lemma 2.13. R^\bullet is primary if and only if R is one-dimensional and local.

Definition 2.14 (Numerical monoids). By a *numerical monoid* S we mean an additive submonoid of \mathbb{N}_0 for which $\mathbb{N}_0 \setminus S$ is finite. For a numerical monoid S , we call $g(S) = \max(\mathbb{N}_0 \setminus S)$ its *Frobenius number* and $n(S) = |(\mathbb{N}_0 \setminus S)|$ its *gap number*.

Definition 2.15 (Finitely primary monoids). H is called *finitely primary* if there exist $s, \alpha \in \mathbb{N}$ with the following properties:

H is a submonoid of a factorial monoid $F = F^\times \times [p_1, \dots, p_s]$ with s pairwise non-associated prime elements p_1, \dots, p_s satisfying

$$H \setminus H^\times \subset p_1 \cdot \dots \cdot p_s F \quad \text{and} \quad (p_1 \cdot \dots \cdot p_s)^\alpha F \subset H.$$

If this is the case, then we say that H is finitely primary of *rank* s and *exponent* α .

Clearly, numerical monoids are finitely primary of rank 1.

Theorem 2.16. *Let $s, \alpha \in \mathbb{N}$.*

1. *Let H be finitely primary, and let $F = F^\times \times [p_1, \dots, p_s]$ be a factorial monoid with pairwise non-associated prime elements p_1, \dots, p_s such that $H \subset F$ is a submonoid satisfying*

$$H \setminus H^\times \subset p_1 \cdot \dots \cdot p_s F \quad \text{and} \quad (p_1 \cdot \dots \cdot p_s)^\alpha F \subset H.$$

Then $F^\times \cap H = H^\times$, $\text{supp}(x) = \{p_1, \dots, p_s\}$ for all $x \in H \setminus H^\times$, and $F = \widehat{H}$. In particular, F is uniquely determined by H .

2. *H is finitely primary of rank s if and only if H is primary, $(H : \widehat{H}) \neq \emptyset$ and $\widehat{H}_{\text{red}} \cong \mathbb{N}_0^s$.*
3. *H is finitely primary of rank s and exponent α if and only if H_{red} is finitely primary of rank s and exponent α .*
4. *Let H be finitely primary. Then H is strongly primary and thus it is a BF-monoid. H is an FF-monoid if and only if $(\widehat{H}^\times : H^\times) < \infty$.*
5. *Let H be finitely primary of rank s . Then H_{red} is finitely generated if and only if $s = 1$ and $(\widehat{H}^\times : H^\times) < \infty$.*

Exercise 2.17. *Let R be a one-dimensional local noetherian domain such that its integral closure \overline{R} is a finitely generated R -module. Then R^\bullet is finitely primary.*

More generally, we have

Theorem 2.18. *If R is a one-dimensional local Mori domain such that $(R : \widehat{R}) \neq \{0\}$, then R^\bullet is finitely primary.*

Exercise 2.19. *Let*

$$H = (\mathbb{N} \times \mathbb{N} \cup \{(0, 0)\}, +) \subset (\mathbb{N}_0^2, +).$$

- *H is finitely primary of rank 2 and exponent 1.*
- *If $\mathbf{x} \in H \setminus \{\mathcal{A}(H) \cup \{\mathbf{0}\}\}$, then $\min \mathbf{L}(\mathbf{x}) = 2$ and hence $\rho_2(H) = \infty$.*
- *$\mathfrak{c}(H) = 3$, whence $\Delta(H) = \{1\}$ and all sets of lengths are arithmetical progressions with difference 1.*

Theorem 2.20.

1. Let H be strongly primary (say v -noetherian and primary).
 - (a) Suppose that one of the following conditions is satisfied:
 - $\sup\{\min \mathbf{L}(c) \mid c \in H\} < \infty$.
 - There is some $u \in H \setminus H^\times$ such that $\rho_{\mathcal{M}(u)}(H) < \infty$.
 Then H is locally tame.
 - (b) If H is locally tame, then H has finite catenary degree $\mathbf{c}(H)$ and a finite set of distances $\Delta(H)$.
 - (c) If H is locally tame, then there exists $M \in \mathbb{N}$ such that, for every $a \in H$, the set of lengths $\mathbf{L}(a)$ has the form

$$\mathbf{L}(a) = y + (L' \cup \{\nu d \mid \nu \in [0, l]\} \cup L'') \subset y + d\mathbb{Z},$$
 where $d = \min \Delta(H)$, $l \in \mathbb{N}_0$, $L' \subset [-M, -1]$ and $L'' \subset ld + [1, M]$.
2. Let H be finitely primary of rank s and exponent α . Then H is locally tame, and we have:
 - (a) If $s = 1$, then $\rho(H) \leq 2\alpha - 1$ and $\mathbf{c}(H) \leq \mathbf{t}(H) \leq 3\alpha - 1$.
 - (b) If $s \geq 2$, then $\min \mathbf{L}(a) \leq 2\alpha$ for all $a \in H$, $\rho(H) = \mathbf{t}(H) = \infty$, and $\mathbf{c}(H) \leq 2\alpha + 1$.

OPEN PROBLEMS

- There are v -noetherian, primary monoids which are not locally tame (see [21]), but we conjecture that this cannot happen for Mori domains. That is,
all one-dimensional local Mori domains should be locally tame
The case where $(R:\widehat{R}) = \{0\}$ and R is not noetherian is open
- Is the structure theorem for sets of lengths sharp ??
We have at least the following weak result (see [21]) (what can be done in numerical monoids?)

Theorem 2.21. *Let $L \subset \mathbb{N}_{\geq 2}$ be a finite set. Then, for all sufficiently large $s \in \mathbb{N}$, there exist a primary C-monoid H defined in $(\mathbb{N}_0^s, +)$ with $\widetilde{H} = \mathbb{N}^s \cup \{\mathbf{0}\}$ and $\widehat{H} = \mathbb{N}_0^s$, and an element $a \in H$ such that $\mathbf{L}(a) = L$.*

- Suppose that R is the localization of an order in an algebraic number field (not a DVR).
Find more precise results on its arithmetic.
Do we have $\min \Delta(R) = 1$???
- $S = [d_1, \dots, d_r]$ a numerical monoid with $1 < d_1 \dots < d_r$ and $\gcd(d_1, \dots, d_r)$. Then $\rho(S) \leq 2g(S) + 1$ and $\mathbf{c}(S) \leq \mathbf{t}(S) \leq 3g(S) + 2$. Here we prove more precisely that

$$\rho(S) = \frac{d_r}{d_1}, \quad \mathbf{t}(S) \leq \frac{g(S) + d_r}{d_1} + 1,$$

and if $r = 2$, then

$$\mathbf{c}(S) = \mathbf{t}(S) = d_2 \quad \text{and} \quad \Delta(S) = \{d_2 - d_1\}.$$

Definition 2.22. Let G be an additive abelian group, $G_0 \subset G$ a subset, T a monoid and $\iota: T \rightarrow G$ a homomorphism. Let $\sigma: \mathcal{F}(G_0) \rightarrow G$ be the unique homomorphism satisfying $\sigma(g) = g$ for all $g \in G_0$. Then we call

$$\mathcal{B}(G_0, T, \iota) = \{S t \in \mathcal{F}(G_0) \times T \mid \sigma(S) + \iota(t) = 0\}$$

the T -block monoid over G_0 defined by ι . If $T = \{1\}$, then $\mathcal{B}(G_0, T, \iota) = \mathcal{B}(G_0)$ is the block monoid of all zero-sum sequences over G_0 .

Proposition 2.23. Let D be an atomic monoid, $P \subset D$ a set of primes and $T \subset D$ a submonoid such that $D = \mathcal{F}(P) \times T$. Let $H \subset D$ be a saturated submonoid, $G = \mathfrak{q}(D/H)$,

$$G_P = \{[p]_{D/H} \mid p \in P\} \subset G \quad \text{and} \quad G_1 = \{[u]_{D/H} \mid u \in \mathcal{A}(D)\} \subset G.$$

Let $\iota: T \rightarrow G$ be defined by $\iota(t) = [t]_{D/H}$, $F = \mathcal{F}(G_P) \times T$, $B = \mathcal{B}(G_P, T, \iota) \subset F$, and let $\tilde{\beta}: D \rightarrow F$ be the unique homomorphism satisfying $\tilde{\beta}(p) = [p]_{D/H}$ for all $p \in P$ and $\tilde{\beta}|_T = \text{id}_T$.

1. $\tilde{\beta}$ is a transfer homomorphism. For $a \in D$ we have $\tilde{\beta}(a) \in B$ if and only if $a \in H$.
2. $\beta = \tilde{\beta}|_H: H \rightarrow B$ is a transfer homomorphism. If H is atomic, then $\mathfrak{c}(H, \beta) \leq 2$ and $\mathfrak{t}(H, u, \beta) \leq \max\{\mathfrak{D}(G_P) + 1, \mathfrak{D}(G_1)\}$ for all $u \in \mathcal{A}(H)$.
3. $B \subset F$ is a saturated submonoid, and there is a homomorphism

$$\bar{\psi}: F/B \rightarrow G, \quad \text{given by } \bar{\psi}([\tilde{\beta}(c)]_{F/B}) = [c]_{D/H} \quad \text{for all } c \in D.$$

If $H \subset D$ is cofinal, then $B \subset F$ is also cofinal and $\bar{\psi}$ is an isomorphism.

Theorem 2.24. *Let R be a weakly Krull domain, $K = \mathfrak{q}(R)$, $\mathfrak{f} = (R : \widehat{R}) \neq \{0\}$, $\mathcal{P} = \{\mathfrak{p} \in \mathfrak{X}(R) \mid \mathfrak{p} \not\supset \mathfrak{f}\}$, $\mathcal{P}^* = \{\mathfrak{p} \in \mathfrak{X}(R) \mid \mathfrak{p} \supset \mathfrak{f}\}$, $G_{\mathcal{P}} = \{[\mathfrak{p}] \in \mathcal{C}_v(R) \mid \mathfrak{p} \in \mathcal{P}\}$ and*

$$T = \prod_{\mathfrak{p} \in \mathcal{P}^*} (R_{\mathfrak{p}}^{\bullet})_{\text{red}}.$$

For $\mathfrak{p} \in \mathcal{P}^$, let $s_{\mathfrak{p}}$ be the number of prime ideals $\widehat{\mathfrak{p}} \in \mathfrak{X}(\widehat{R})$ satisfying $\widehat{\mathfrak{p}} \cap R = \mathfrak{p}$.*

1. \mathcal{P}^* is finite, for each $\mathfrak{p} \in \mathcal{P}^*$ the monoid $R_{\mathfrak{p}}^{\bullet}$ is finitely primary of rank $s_{\mathfrak{p}}$, and there are (natural) isomorphisms

$$\mathcal{I}_v^*(R) \xrightarrow{\sim} \prod_{\mathfrak{p} \in \mathfrak{X}(R)} (R_{\mathfrak{p}}^{\bullet})_{\text{red}} \xrightarrow{\sim} \mathcal{F}(\mathcal{P}) \times T.$$

The diagonal embedding induces a cofinal divisor homomorphism

$$\varphi: R^{\bullet} \rightarrow \prod_{\mathfrak{p} \in \mathfrak{X}(R)} (R_{\mathfrak{p}}^{\bullet})_{\text{red}} \xrightarrow{\sim} \mathcal{F}(\mathcal{P}) \times T, \quad \text{and we set } H = \varphi(R^{\bullet}).$$

Then $H \subset \mathcal{F}(\mathcal{P}) \times T$ is saturated and cofinal, $H \cong (R^{\bullet})_{\text{red}}$, and

$$\mathcal{C}_v(R) \cong \mathcal{C}(\varphi) = (\mathcal{F}(\mathcal{P}) \times T) / H.$$

We identify these groups

(whence $[c]_{\varphi} \in \mathcal{C}_v(R)$ for all $c \in \mathcal{F}(\mathcal{P}) \times T$).

We denote by $\mathcal{B}(R) \subset \mathcal{F}(G_{\mathcal{P}}) \times T$ the block monoid and by $\beta_R: R^\bullet \rightarrow \mathcal{B}(R)$ the block homomorphism of R .

Then $\mathcal{B}(R) \subset \mathcal{F}(G_{\mathcal{P}}) \times T$ is saturated and cofinal, there is a (natural) isomorphism $\mathcal{F}(G_{\mathcal{P}}) \times T / \mathcal{B}(R) \xrightarrow{\sim} \mathcal{C}_v(R)$, β_R is a transfer homomorphism, and

$$\beta_R(a) = \left(\prod_{\mathfrak{p} \in \mathcal{P}} [\mathfrak{p}]^{v_{\mathfrak{p}}(a)} \right) (aR_{\mathfrak{p}}^\times)_{\mathfrak{p} \in \mathcal{P}^*} \in \mathcal{F}(G_{\mathcal{P}}) \times T \quad \text{for all } a \in R^\bullet.$$

If $\exp(\mathcal{C}_v(R)) < \infty$, then $\mathcal{B}(R) \subset \mathcal{F}(G_{\mathcal{P}}) \times T$ is faithfully saturated.

2. $c(\mathcal{I}_v^*(R)) < \infty$, $\mathcal{I}_v^*(R)$ is locally tame, and $\mathcal{I}_v^*(R)$ is tame if and only if $s_{\mathfrak{p}} = 1$ for all $\mathfrak{p} \in \mathcal{P}^*$.
3. If $\mathcal{C}_v(R)$ is finite, then $c(R) < \infty$, $\Delta(R)$ is finite, R is locally tame, and the following statements are equivalent:
 - (a) R is tame.
 - (b) $\rho(R) < \infty$.
 - (c) For every $a \in R^\bullet \setminus R^\times$, the set $\{\min \mathbf{L}(a^n) \mid n \in \mathbb{N}\}$ is infinite.
 - (d) $s_{\mathfrak{p}} = 1$ for all $\mathfrak{p} \in \mathcal{P}^*$.

Exercise 2.25. Apply the above theorem to $\mathbb{Z}[\sqrt{-7}]$.

Theorem 2.26. If R is an order in a quadratic number field, then $c(\mathcal{I}_v^*(R)) \leq 5$.

3. MORE FINITENESS RESULTS - THE NON-KRULL CASE

Class semigroups

Motivation: Let R be the ring of integers of an algebraic number field.

Let D be the monoid of non-zero ideals and H the monoid of non-zero principal ideals.

Two non-zero ideals $I, I' \triangleleft R$ are called *equivalent* if, for all non-zero ideals $J \triangleleft R$ we have

IJ is a principal ideal if and only if $I'J$ is a principal ideal.

Clearly, this defines a congruence relation on D .

Since $H \subset D$ is saturated, the set of congruence classes coincides with the usual ideal class group.

Definition 3.1.

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

$$ya \in H \quad \text{if and only if} \quad y'a \in H.$$

Clearly, H -equivalence defines a congruence relation on D .

For $y \in D$ we denote by $[y]_H^D$ the congruence class of y .

We define the *class semigroup*

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

and is called the *reduced class semigroup*.

Exercise 3.2.

Let D be a monoid and $H \subset D$ a cofinal submonoid.

1. There are epimorphisms

$$\theta: \mathcal{C}(H, D) \rightarrow \mathfrak{q}(D)/\mathfrak{q}(H) \quad \text{and} \quad \theta^*: \mathcal{C}^*(H, D) \rightarrow \mathfrak{q}(D)/D^\times \mathfrak{q}(H),$$

given by

$$\theta([y]_H^D) = [y]_{D/H} = y\mathfrak{q}(H) \quad \text{for all } y \in D,$$

and

$$\theta^*([y]_H^D) = [y]_{D/D^\times H} \quad \text{for all } y \in (D \setminus D^\times) \cup \{1\}.$$

2. $[1]_H^D \subset H \subset [1]_{D/H} \cap D$.

3. The following statements are equivalent:

(a) $H \subset D$ is saturated.

(b) $[y]_H^D = [y]_{D/H} \cap D$ for all $y \in D$.

(c) $[1]_H^D = [1]_{D/H} \cap D$.

(d) $[1]_H^D = H$.

(e) The epimorphism $\theta: \mathcal{C}(H, D) \rightarrow \mathfrak{q}(D)/\mathfrak{q}(H)$ defined in 1. is an isomorphism.

Exercise 3.3. Let $H \subset D$ be a submonoid.

1. If $\mathcal{C}^*(H, D)$ is a group, then $\mathcal{C}(H, D)$ is a group and either $D = D^\times$ or $\mathcal{C}(H, D) = \mathcal{C}^*(H, D)$.

2. If $\mathcal{C}(H, D)$ is a group, then $H \subset D$ is cofinal, and if $\mathcal{C}(H, D)$ is a torsion group, then $H \subset D$ is also saturated.

BE CAREFUL there are simple examples where

$$\mathfrak{q}(D)/\mathfrak{q}(H) = 0 \quad \text{BUT} \quad \mathcal{C}(H, D) \text{ is infinite.}$$

PHILOSOPHY

If $\mathcal{C}^*(H, D)$ is finite, then the arithmetic of H and D are related

A first example

- For an additive abelian semigroup C , let $\mathbf{d}(C)$ denote the smallest $d \in \mathbb{N}_0 \cup \{\infty\}$ with the following property:
For any $m \in \mathbb{N}$ and $c_1, \dots, c_m \in C$ there exists a subset $J \subset [1, m]$ such that $|J| \leq d$ and

$$\sum_{j=1}^m c_j = \sum_{j \in J} c_j.$$

- Finite semigroups have finite Davenport constants.
- If $b \in H$, then $\omega_H(H, b) \leq \omega_D(D, b) + \mathbf{d}(\mathcal{C}^*(H, D))$.

CLASS SEMIGROUPS HAVE NICE TECHNICAL PROPERTIES

- $$\mathcal{C}(H_1 \times H_2, D_1 \times D_2) \xrightarrow{\sim} \mathcal{C}(H_1, D_1) \times \mathcal{C}(H_2, D_2)$$
- Let $S \subset H$ be saturated.

If both $\mathbf{q}(H)/\mathbf{q}(S)$ and $\mathcal{C}^*(H, D)$ are finite,

then $\mathcal{C}^*(S, D)$ is finite.

C-monoids

Definition 3.4. H is called a *C-monoid* if it is a submonoid of a factorial monoid F such that $H \cap F^\times = H^\times$ and $\mathcal{C}^*(H, F)$ is finite.

Main Example 3.5. Let R be a Mori domain with non-trivial conductor $\mathfrak{f} = (R:\widehat{R})$. If $\mathcal{C}(\widehat{R})$ and R/\mathfrak{f} are both finite, then R^\bullet is a C-monoid.

Proof. Let $\widehat{R}^\bullet = \widehat{R}^\times \times R_0$ with a reduced Krull monoid R_0 . Then

$$\varphi: \widehat{R}^\bullet \rightarrow F_0 = \mathcal{I}_v^*(\widehat{R}) = \mathcal{F}(\mathfrak{x}(\widehat{R}))$$

is a divisor theory. If $F = R^\times \times F_0$, then R^\bullet is a C-monoid defined in F . The main task is to deduce the finiteness of $\mathcal{C}^*(R^\bullet, F)$ from that of \widehat{R}/\mathfrak{f} and $\mathcal{C}(\widehat{R})$.

Note, that even in the special case where R is a non-principal order in an algebraic number field, the class semigroup $\mathcal{C}^*(R^\bullet, F)$ does not coincide with the Picard group $\text{Pic}(R)$ or any other class group. Indeed, $\mathcal{C}^*(R^\bullet, F)$ is finite but not even a group. \square

PHILOSOPHY

- If H is Krull, then the class group $\mathcal{C}(H, D) = \mathcal{C}(H)$ measures the distance between the monoid of principal ideals and the monoid of ideals of H .
- If H is not Krull, then the class semigroup $\mathcal{C}(H, D)$ measures the distance between the monoid of principal ideals and the monoid of ideals of the complete integral closure \widehat{H} .

COMPARISON WITH FORMER CONCEPTS

KRULL MONOIDS

Proposition 3.6.

1. *Let H be a Krull monoid with finite class group. Then H is a C-monoid.*
2. *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.*

FINITELY GENERATED MONOIDS

Proposition 3.7. *Let H_{red} be finitely generated.*

Then H is a C-monoid if and only if $\mathcal{C}(\widehat{H})$ is finite.

FINITELY PRIMARY MONOIDS

Proposition 3.8.

Let H be finitely primary and $\widehat{H} = \widehat{H}^\times \times [p_1, \dots, p_s]$, where $s \in \mathbb{N}$ and p_1, \dots, p_s are pairwise non-associated prime elements of \widehat{H} .

Then H is a C-monoid defined in \widehat{H} if and only if the following two conditions are fulfilled:

- (a) *There exists a subgroup $V \subset \widehat{H}^\times$ of finite index such that $V(H \setminus H^\times) \subset H$.*
- (b) *There exists some $\alpha \in \mathbb{N}$ such that, for every $j \in [1, s]$ and $a \in p_j^\alpha \widehat{H}$, we have $a \in H$ if and only if $p_j^\alpha a \in H$.*

ALGEBRAIC PROPERTIES OF C-MONONIDS

Let F be a factorial monoid, P a maximal set of pairwise non-associated primes of F and H a C-monoid defined in F .

H is called *dense* in F if $\mathbf{v}_p(H) \subset \mathbb{N}_0$ is a numerical monoid for all $p \in P$.

Theorem 3.9. *Let H be a C-monoid defined in $F = F^\times \times \mathcal{F}(P)$ with subgroup V and exponent α .*

1. *For $p \in P$, let $d_p = \gcd(\mathbf{v}_p(H)) \in \mathbb{N}_0$,
 $P_0 = \{p^{d_p} \mid p \in P, d_p \neq 0\} \subset \mathcal{F}(P)$ and*

$$F_0 = \{a \in F \mid \mathbf{v}_p(a) \in d_p \mathbb{N}_0 \text{ for all } p \in P\} = F^\times \times \mathcal{F}(P_0) \subset F.$$

Then H is a C-monoid defined in F_0 with subgroup V and exponent α , and H is dense in F_0 .

2. *H is v -noetherian with $(H : \widehat{H}) \neq \emptyset$ and \widehat{H} is a Krull monoid with finite class group $\mathcal{C}(\widehat{H})$, whose exponent divides α .*

REMARK: There are v -noetherian monoids H with $(H : \widehat{H}) \neq \emptyset$ such that $\mathcal{C}(\widehat{H})$ is finite, which are not C-monoids.

This may happen for finitely primary monoids and for one-dimensional local domains.

3. If H is dense in F , then the following assertions hold:

- (a) H is cofinal in F .
- (b) $\widehat{H} = \mathfrak{q}(H) \cap F$, and if $\{p_1, \dots, p_d\} \subset P$ is an H -essential subset satisfying $\{[p_1]_H^F, \dots, [p_d]_H^F\} = \{[p]_H^F \mid p \in P\}$, then $(p_1 \cdot \dots \cdot p_d)^\alpha \widehat{H} \subset H$.
- (c) For every $q \in F \setminus F^\times$, we have $q^\alpha \in \widehat{H}$.
- (d) The map $\partial: \widehat{H} \rightarrow \mathcal{F}(P)$, defined by

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

is a divisor theory, and there is an epimorphism

$$\mathcal{C}^*(H, F) \rightarrow \mathcal{C}(\widehat{H}).$$

- (e) Let H be defined in another factorial monoid F' such that H is dense in F' . Then there exists a $\Phi: F_{\text{red}} \rightarrow F'_{\text{red}}$ such that $\Phi(aF^\times) = aF'^\times$ for all $a \in H$.

In particular, if H is dense in F , then F_{red} is uniquely determined by H (up to isomorphism).

- 4. If $\widehat{H} = \widehat{H}^\times \times H_0$ with a reduced Krull monoid H_0 , and if $H_0 \hookrightarrow \mathcal{F}(P)$ is a divisor theory, then H is a \mathbb{C} -monoid defined in $F_1 = \widehat{H}^\times \times \mathcal{F}(P)$, H is dense in F_1 , and if H is a \mathbb{C}_0 -monoid, then P is finite.

WHEN IS R^\bullet a C-monoid ?

- By the previous result,
 R has to be a Mori domain with non-trivial conductor $\mathfrak{f} = (R:\widehat{R})$
 and finite class group $\mathcal{C}(\widehat{R})$.
- If in addition R/\mathfrak{f} is finite, then R^\bullet is a C-monoid.
- Clearly, a noetherian domain R where \overline{R} is a finitely generated R -module, is a Mori domain with non-trivial conductor.
- Let R be a finitely generated \mathbb{Z} -algebra.
 Then R is noetherian and \overline{R} is a finitely generated R -module.
 If $\mathcal{C}(\widehat{R})$ is finite, then

$$R/\mathfrak{f} \text{ is finite if and only if } \mathcal{C}(R) \text{ is finite}$$
 For examples of this type see Hassler [23].
- Let R be a one-dimensional local noetherian domain with
 non-trivial conductor \mathfrak{f} and maximal ideal \mathfrak{m} .
 Then the following statements are equivalent:
 - R^\bullet is a C-monoid.
 - R/\mathfrak{m} is finite or $\mathfrak{f} = \mathfrak{m}$.

The notion of C-monoids has recently be generalized to study a wider class of Mori domains (see [19]).

ARITHMETIC PROPERTIES OF C-MONONIDS

Theorem 3.10.

Let H be a C-monoid defined in $F = F^\times \times \mathcal{F}(P)$.

1. H is locally tame with finite set of distances $\Delta(H)$ and finite catenary degree $\mathfrak{c}(H) < \infty$.
2. H has finite elasticity if and only if every minimal H -essential subset of P is a singleton.
A subset $E \subset P$ is called H -essential if $E = \text{supp}_P(x)$ for some $x \in H \setminus F^\times$.

3. There exists a constant $M \in \mathbb{N}$ having the following property:

For every $a \in H$, each two factorizations $z, z' \in \mathbf{Z}(a)$ can be concatenated by an M -chain $z = z_0, z_1, \dots, z_k, z_{k+1} = z'$ such that

$$\text{either } |z_1| \leq \dots \leq |z_k| \quad \text{or} \quad |z_1| \geq \dots \geq |z_k|.$$

4. There exist $M \in \mathbb{N}_0$ and a (well-defined) finite set $\Delta^* \subset \Delta(H)$ such that the following holds:
Every $L \in \mathcal{L}(H)$ is an AAMP with difference $d \in \Delta^*$ and bound M .

Compare with the Realization Theorem in Section 1.

A transfer principle

Theorem 3.11. *Let $F = F^\times \times \mathcal{F}(P)$ be a factorial monoid and H a C-monoid defined in F with subgroup $V \subset F^\times$.*

Let $P_0 \subset \{p \in P \mid p^{-1}H \cap F = H \setminus H^\times\}$ be a subset, $\tilde{P} = \{[p]_H^F \mid p \in P \setminus P_0\}$, and

$$\tilde{F} = (F^\times / V) \times \mathcal{F}(\tilde{P}),$$

where $\mathcal{F}(\tilde{P})$ is the free monoid with basis \tilde{P} . Let $\tilde{\beta}: F \rightarrow \tilde{F}$ be the unique homomorphism satisfying $\tilde{\beta}(p) = [p]_H^F$ for all $p \in P \setminus P_0$, $\tilde{\beta}(p) = 1$ for all $p \in P_0$, and $\tilde{\beta}(e) = eV$ for all $e \in F^\times$. Finally, we define

$$\tilde{H} = \tilde{\beta}(H) \quad \text{and} \quad \beta = \tilde{\beta} \mid H: H \rightarrow \tilde{H}.$$

1. \tilde{H} is a C_0 -monoid defined in \tilde{F} and $\tilde{F}^\times = F^\times / V$ is finite.
2. β is a transfer homomorphism, $\mathbf{c}(H, \beta) \leq 2$ and $\mathbf{t}(a, uH^\times, \beta) \leq \omega(a, u) + 1$ for all $a \in H$ and $u \in \mathcal{A}(H)$.
3. H is locally tame, and $\mathbf{c}(H) < \infty$.

Summary

It is sufficient to prove the arithmetical properties for C-monoids H which are defined in a factorial monoid \tilde{F} having only finitely many pairwise non-associated primes and for which \tilde{F}^\times is finite.

Theorem 3.12.

Let $F = F^\times \times [p_1, \dots, p_s]$ be a factorial monoid with pairwise non-associated prime elements p_1, \dots, p_s , and let $H \subset F$ be a submonoid such that $H \cap F^\times = H^\times$. Then the following statements are equivalent:

- (a) H is a C-monoid defined in F .
- (b) There exist some $\alpha \in \mathbb{N}$ and a subgroup $V \subset F^\times$ such that the following two conditions are satisfied:
 - (C1) $(F^\times : V) \mid \alpha$ and $V \cdot (H \setminus H^\times) \subset H$.
 - (C2) For all $j \in [1, s]$ and $a \in p_j^\alpha F$ we have

$$a \in H \quad \text{if and only if} \quad p_j^\alpha a \in H.$$

Let H be as above, and for a subset $Q \subset P$ let

$$H_Q = \{x \in H \mid \text{supp}_P(x) \subset Q\} = (F^\times \times \mathcal{F}(Q)) \cap H.$$

Then we have

- $\{H_Q \mid Q \subset P\}$ is the set of all divisor-closed submonoids of H . In particular, every divisor-closed submonoid of a C-monoid is a C-monoid.
- H has only finitely many divisor-closed submonoids and thus H has only finitely many prime s -ideals.

The Structure Theorem For Sets of Lengths

Sketch of the Proof

1. THE STATEMENT AGAIN

There is an $M \in \mathbb{N}$ such that for all $a \in H$

there is a $d \in \Delta^* \subset \Delta(H)$ such that

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

where

- The central part L^* is large and nice, shifted such that $\min L^* = 0$
- The initial part L' and the end part L'' are universally bounded, that is $L' \subset [-M, -1]$ and $L'' \subset \max L^* + [1, M]$

Note

- If $\mathbf{L}(a) \subset \min \mathbf{L}(a) + [0, 2M]$, then choose $L^* = \{0\}$, and the assertion follows.
- Thus we have to prove something for "large" sets $\mathbf{L}(a)$ arising from "large" elements a .

2. A SIMPLE CONSTRUCTION

- Let $d = \min \Delta(H)$ and choose $a_0 \in H$ such that $d \in \Delta(\mathbf{L}(a))$, that is
there is some $m \in \mathbb{N}$ such that $\{m, m + d\} \subset \mathbf{L}(a)$.
- Clearly, $\{2m, 2m + d, 2m + 2d\} \subset \mathbf{L}(a) + \mathbf{L}(a) \subset \mathbf{L}(a^2)$
whence for all $k \in \mathbb{N}$ there is a z such that
$$\{z, z + d, \dots, z + kd\} \subset \mathbf{L}(a^k).$$

- Let $b \in H$ be arbitrary, and let $a^* \in H$ such that
 $L_1 = \{z, z + d, \dots, z + kd\} \subset \mathbf{L}(a^*)$ with $k \geq d^{-1} \max \Delta(H)$.
Then

$$L^* := L_1 + \mathbf{L}(b) \subset \mathbf{L}(a^*) + \mathbf{L}(b) \subset \mathbf{L}(a^*b) =: L' \cup L^* \cup L''$$

Because $\max \Delta(\mathbf{L}(b)) \subset \max \Delta(H)$ and $d = \min \Delta(H) = \gcd \Delta(H)$, it follows that L^* is an arithmetical progression with difference d .

$$\begin{aligned} \min(L_1 + \mathbf{L}(b)) - \min \mathbf{L}(a^*b) &\leq? =: M \\ \max \mathbf{L}(a^*b) - \max(L_1 + \mathbf{L}(b)) &\leq? =: M \end{aligned}$$

- *Local tameness gives us the $M := \mathbf{t}(H, \mathbf{Z}(a^*))$*
For every $z \in \mathbf{Z}(a = a^*b)$ and $x \in \mathbf{Z}(a^*)$, there exists some $z' \in \mathbf{Z}(a) \cap x\mathbf{Z}(H)$ such that $\mathbf{d}(z, z') \leq M$, and then $x^{-1}z' \in \mathbf{Z}(b)$.

If $|z| = \min \mathbf{L}(a)$ and $|x| = \max \mathbf{L}(a^*)$, then

$$\begin{aligned} \min \mathbf{L}(b) + \max \mathbf{L}(a^*) - \min \mathbf{L}(a) \\ \leq |x^{-1}z'| + |x| - |z| = |z'| - |z| \leq \mathbf{d}(z, z') \leq M, \end{aligned}$$

and therefore

$$\max \mathbf{L}(a^*) + \min \mathbf{L}(b) - M \leq \min \mathbf{L}(a).$$

3. THE SIMPLEST CLASS OF MONOIDS: PRIMARY MONOIDS

Suppose that H is v -noetherian and primary.

Pick an element a^* having the properties as before.

Now let $a \in H$ be arbitrary: there are two cases:

CASE1: $a^* \nmid a$: Then $\mathbf{L}(a)$ is small (universally bounded by M)

CASE2 : $a^* \mid a$: Then $a = a^*b$ and $\mathbf{L}(a)$ has the required form

4. GENERAL SITUATION:

PROBLEM:

Even if $H = H_1 \times H_2$, where H_i is primary with $\min \Delta(H_i) = d_i$, there are elements $a = a_1 a_2$ whose set of lengths $\mathbf{L}(a)$ is large but a is not divisible by an element $a^* = a^*(H)$ as above.

IDEA:

- For every divisor-closed submonoid S pick an element $a^*(S)$
- For an arbitrary element $a \in H$ find a suitable divisor-closed submonoid S set $a = a^*(S)b$ (Ideal theoretic part)
- Study $\mathbf{L}(a^*(S)) + \mathbf{L}(b) \subset \mathbf{L}(a)$ (Additive part)

4. ADDITIVE PART

Definition 3.13. Let H be atomic and $\mathfrak{a} \subset H$.

1. Let $A \subset \mathbb{Z}$ be a finite non-empty subset and $a \in H$. We say that $\mathbf{L}(a)$ *contains the pattern* A if there exists some $y \in \mathbb{Z}$ such that $y + A \subset \mathbf{L}(a)$. We denote by $\Phi(A) = \Phi_H(A)$ the set of all $a \in H$ for which $\mathbf{L}(a)$ contains the pattern A .
2. \mathfrak{a} is called a *pattern ideal* if $\mathfrak{a} = \Phi(A)$ for some finite non-empty subset $A \subset \mathbb{Z}$.
3. A subset $E \subset H$ is called a *tame generating set* of \mathfrak{a} if $E \subset \mathfrak{a}$ and if there exists some $N \in \mathbb{N}$ with the following property:
For every $a \in \mathfrak{a}$ there exists some $e \in E$ such that

$$e \mid a, \quad \sup \mathbf{L}(e) \leq N \quad \text{and} \quad \mathfrak{t}(a, \mathbf{Z}(e)) \leq N.$$

In this case we call E a *tame generating set with bound* N .

4. \mathfrak{a} is called *tamely generated* if \mathfrak{a} has a tame generating set. Then we denote by $\varphi(\mathfrak{a})$ the smallest $N \in \mathbb{N}_0$ such that \mathfrak{a} has a tame generating set with bound N .

The following statements are equivalent :

1. H is locally tame.
2. Every principal ideal of H is tamely generated.
3. Every s -finite s -ideal of H is tamely generated.

In particular, if H_{red} is finitely generated, then every s -ideal of H is tamely generated.

THE STRUCTURE THEOREM IN AN ABSTRACT SETTING

Theorem 3.14.

Let H be a BF-monoid with finite non-empty set of distances $\Delta(H)$, and suppose that all pattern ideals of H are tamely generated.

Then 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 .

Remark 3.15.

- Suppose that H_{red} is finitely generated.
Then H is locally tame and every s -ideal is finitely generated.
Thus the Structure Theorem for Sets of Lengths holds for H .
- Suppose that H is a C-monoid defined in a finitely generated factorial monoid.
It remains to show that pattern ideals are tamely generated
(ideal theoretic part)
- In general, pattern ideals are not s -finite.
- There are finitely primary monoids H_1 and H_2 such that
 $H = H_1 \times H_2$ contains ideals which are not tamely generated.

5. IDEAL THEORETIC PART

Definition 3.16.

1. A subset $U \subset H$ is called an *almost generating set* of H if $U \cap H^\times = \emptyset$ and if there exists some $n \in \mathbb{N}$ such that $(H \setminus H^\times)^n \subset UH$.

We denote by $\mathcal{M}(U)$ the smallest $n \in \mathbb{N}$ with this property, and if $U = \{u\}$ we set $\mathcal{M}(u) = \mathcal{M}(U)$.

2. H is called *finitary* if H is a BF-monoid and has a finite almost generating set.
3. Let H be finitary, $\mathfrak{a} \subset H$ an s -ideal and $U \subset H$ a finite almost generating set.

For $u \in U$, we denote by $\mathfrak{a}(U, u)$ the set of all elements $a \in \mathfrak{a} \cap u^2H$ such that $\llbracket u \rrbracket$ is maximal in the set $\{\llbracket v \rrbracket \mid v \in U, a \in v^2H\}$.

Notation: for a subset $U \subset H$, $\llbracket U \rrbracket$ is the smallest divisor-closed submonoid containing U . In particular, if $u \in H$, then $\llbracket \{u\} \rrbracket = \llbracket u \rrbracket$ consists of all $a \in H$ dividing some power u^n of u .

Theorem 3.17.

Let H be finitary and $U \subset H$ an almost generating set.

1. $H = UH \cup \{a \in H \mid \max \mathsf{L}(a) < \mathcal{M}(U)\}$.
2. Every s -ideal \mathfrak{a} has the decomposition

$$\mathfrak{a} = \bigcup_{u \in U} \mathfrak{a}(U, u) \cup (\mathfrak{a} \setminus U^{[2]}H).$$

Lemma 3.18. *The following statements are equivalent:*

1. *H is finitary and primary.*
2. *For every $a \in H \setminus H^\times$ the singleton $\{a\}$ is an almost generating set of H .*

Definition 3.19. *H is a G -monoid if and only if*

$$\bigcap_{\substack{\mathfrak{p} \in s\text{-spec}(H) \\ \mathfrak{p} \neq \emptyset}} \mathfrak{p} \neq \emptyset.$$

Lemma 3.20.

A domain R is a G -domain if and only if R^\bullet is a G -monoid.

Lemma 3.21. *Every C -monoid defined in a finitely generated factorial monoid is a v -noetherian G -monoid.*

Theorem 3.22. *Let H be a v -noetherian G -monoid.*

1. *H is finitary and $s\text{-spec}(H)$ is finite.*
2. *If $(H : \widehat{H}) \neq \emptyset$, then \widehat{H} is a Krull monoid, $s\text{-spec}(\widehat{H})$ is finite and \widehat{H}_{red} is finitely generated.*

Definition 3.23. Let H be finitary and U a finite almost generating set of H .

1. For $u \in U$, let H_u be the set of all $a \in H$ without a divisor in $\llbracket u \rrbracket \setminus H^\times$.
2. Let $\mathfrak{a} \subset H$ be an s -ideal. For $u \in U$, we set $\mathfrak{a}[U, u] = H_u \cap (u \llbracket u \rrbracket)^{-1} \mathfrak{a}(U, u)$.
3. U is called a *full almost generating set* of H if there exists some $m \in \mathbb{N}$ such that $H[U, u] \subset H \setminus U^{[m]}H$ for all $u \in U$.
4. An s -ideal $\mathfrak{a} \subset H$ is called
 - (a) *U -generated* if $u \llbracket u \rrbracket \mathfrak{a}[U, u] \subset \mathfrak{a}$ for all $u \in U$.
 - (b) *U -tame* if there exists some $M \in \mathbb{N}$ such that for every $u \in U$ and $a \in \mathfrak{a}(U, u)$ there exists a decomposition $a = a^*b$, where $a^* \in u \llbracket u \rrbracket$, $b \in \mathfrak{a}[U, u]$ and $\mathfrak{t}(a, \mathfrak{Z}(b)) \leq M$.

Lemma 3.24. \mathfrak{a} is U -generated if and only if

$$\mathfrak{a} = \left(\bigcup_{u \in U} u \llbracket u \rrbracket \mathfrak{a}[U, u] \right) \cup (\mathfrak{a} \setminus U^{[2]}H).$$

Theorem 3.25. Let H be locally tame and finitary, U a finite full almost generating set of H and $\mathfrak{a} \subset H$ an s -ideal. Then the following statements are equivalent:

- (a) \mathfrak{a} is U -generated and U -tame.
- (b) There exists some $N \in \mathbb{N}$ such that, for every $u \in U$ and $a \in \mathfrak{a}(U, u)$, there exists some $e \in u\mathfrak{a}[U, u]$ such that $e \mid a$, $e^{-1}a \in \llbracket u \rrbracket$, $\max \mathfrak{L}(e) \leq N$, $\mathfrak{t}(a, \mathfrak{Z}(e)) \leq N$, and the set

$$E = \bigcup_{u \in U} u\mathfrak{a}[U, u] \cup (\mathfrak{a} \setminus U^{[2]}H)$$

is a tame generating set of \mathfrak{a} .

Theorem 3.26. *Let H be a C -monoid defined in $F = F^\times \times \mathcal{F}(P)$ for some finite set P .*

Then pattern ideals are U -generated and U -tame, and thus they are tamely generated.

Proof. Since $\mathcal{C}^*(H, D)$ is finite, it follows that $\mathcal{C}^*(\mathcal{A}(H), D)$ is finite.

□

4. ZERO-SUM SEQUENCES AND ADDITIVE GROUP THEORY

Some notations

Throughout this section, let G be an additive finite abelian group. If not stated otherwise, we suppose that $|G| \geq 3$, in order to exclude trivial cases.

An s -tuple (e_1, \dots, e_s) of elements of G is said to be *independent* if $e_i \neq 0$ for all $i \in [1, s]$ and, for every s -tuple $(m_1, \dots, m_s) \in \mathbb{Z}^s$,

$$\sum_{i=1}^s m_i e_i = 0 \quad \text{implies} \quad m_1 e_1 = \dots = m_s e_s = 0.$$

An s -tuple (e_1, \dots, e_s) of elements of G is called a *basis* if it is independent and $G = \langle e_1 \rangle \oplus \dots \oplus \langle e_s \rangle$. Furthermore,

$$\exp(G) = \text{lcm}\{\text{ord}(g) \mid g \in G\} \in \mathbb{N}$$

is called the *exponent* of G , and

$$r(G) = \max\{r_p(G) \mid p \in \mathbb{P}\}$$

is called the *rank* of G .

For $n \in \mathbb{N}$, let C_n denote a cyclic group with n elements. By the Fundamental Theorem of Finite Abelian Groups we have

$$G = C_{n_1} \oplus \dots \oplus C_{n_r} \quad \text{with} \quad 1 < n_1 \mid \dots \mid n_r,$$

where $r = r(G)$ and $\exp(G) = n_r = n$.

Results from Additive Group Theory

Definition 4.1.

Let A, B be non-empty subsets of G and $g \in G$.

- $A + B = \{a + b \mid a \in A, b \in B\}$
denotes the *sumset* of A and B . We set $g + A = \{g\} + A$.

- $A \dot{+} B = \{a + b \mid a \in A, b \in B, a \neq b\}$
denotes the *restricted sumset* of A and B .

- If $A = \{g_1, \dots, g_l\}$, then

$$\Sigma_k(A) = \left\{ \sum_{i \in I} g_i \mid I \subset [1, l] \text{ with } |I| = k \right\}$$

denotes the *set of k -term subsums* of A . Note that

$$\Sigma_2(A) = A \dot{+} A.$$

- $\text{Stab}(A) = \{x \in G \mid x + A = A\}$
is called the *stabilizer* of A . Note that $\text{Stab}(A)$ is a subgroup of G , and $A = A + \text{Stab}(A)$.
- $r_{A,B}(g) = |\{(a, b) \in A \times B \mid g = a + b\}| = |A \cap (g - B)|$
denotes the *number of representations of g*
as a sum of an element of A and an element of B .

Theorem 4.2 (Cauchy-Davenport).

If $G = \mathbb{Z}/p\mathbb{Z}$ for some prime $p \in \mathbb{P}$, then

$$|A + B| \geq \min\{p, |A| + |B| - 1\}.$$

Theorem 4.3 (Kneser, 1956).

Let $K = \text{Stab}(A + B)$ be the stabilizer of $A + B$.

1. There exists a subgroup $H \subset K$ such that

$$|A + B| \geq |A| + |B| - |H|.$$

2. There exists a subgroup $H \subset K$ such that

$$|A + B| \geq |A + H| + |B + H| - |H|.$$

3. $|A + B| \geq |A + K| + |B + K| - |K|$.

4. Either $|A + B| \geq |A| + |B|$ or $|A + B| = |A + K| + |B + K| - |K|$.

Theorem 4.4 (Kemperman-Scherk, 1960).

If $K = \text{Stab}(A + B)$ be the stabilizer of $A + B$, then

$$|A + B| \geq |A| + |B| -$$

$$\min\{r_{(a+K) \cap A, (b+K) \cap B}(g) \mid a \in A, b \in B, g \in a + b + K\} \\ \geq |A| + |B| - \min\{r_{A,B}(g) \mid g \in A + B\}.$$

Corollary 4.5.

If $l \in \mathbb{N}$ and $S = S_1 \cdot \dots \cdot S_l \in \mathcal{F}(G)$ is a zero-sumfree sequence, then

$$|\Sigma(S)| \geq |\Sigma(S_1)| + \dots + |\Sigma(S_l)|.$$

Proof. Exercise: Suppose $l = 2$, set $A = \Sigma(S_1) \cup \{0\}$, $B = \Sigma(S_2) \cup \{0\}$ and use the Theorem of Kemperman-Scherk. \square

Conjecture 4.6 (Lev, 2005, [29]).

If A and B are finite non-empty subsets of ANY abelian group G , then

$$|A \dot{+} B| \geq \min\{|A + B| - 2, |A| + |B| - 3\}.$$

This conjecture unifies various other conjectures in this area.

In particular, it contains the

Erdős-Heilbronn Conjecture, 1964:

If A and B are non-empty subsets of $\mathbb{Z}/p\mathbb{Z}$, for some prime $p \in \mathbb{P}$, then

$$|A \dot{+} B| \geq \min\{p, |A| + |B| - 3\}.$$

This conjecture was open for 30 years till

Theorem 4.7 (Diaz da Silva-Hamidoune, 1994, [5]).

The Erdős-Heilbronn Conjecture holds true, and moreover, for every $k \in [1, |A|]$ we have

$$|\Sigma_k(A)| \geq \min\{p, k(|A| - k) + 1\}.$$

For a proof see also the book of Nathanson [32].

Group Algebras

Let R be a commutative ring (by a ring, we always mean a ring with unit element).

The *group algebra* $R[G]$ of the group G over the ring R is a free R -module with basis $\{X^g \mid g \in G\}$ (built with a symbol X), where multiplication is defined by

$$\left(\sum_{g \in G} a_g X^g\right) \left(\sum_{g \in G} b_g X^g\right) = \sum_{g \in G} \left(\sum_{h \in G} a_h b_{g-h}\right) X^g.$$

We view R as a subset of $R[G]$ by means of $a = aX^0$ for all $a \in R$.

We denote by $\text{Hom}(G, K^\times)$ the *character group* of G with values in K . The constant character with value 1 is denoted by χ_0 and is called the *trivial character*.

Every character $\chi \in \text{Hom}(G, K^\times)$ has a unique extension to a K -algebra homomorphism $\chi: K[G] \rightarrow K$ (again denoted by χ) acting by means of

$$\chi\left(\sum_{g \in G} a_g X^g\right) = \sum_{g \in G} a_g \chi(g).$$

For $n \in \mathbb{N}$, let $\mu_n(K) = \{\zeta \in K \mid \zeta^n = 1\} \subset K^\times$ denote the group of n -th roots of unity of K . $\mu_n(K)$ is a cyclic subgroup of K^\times . If $\exp(G) = n$, then $\text{Hom}(G, K^\times) = \text{Hom}(G, \mu_n(K))$, and K is called a *splitting field* of G if $|\mu_n(K)| = n$.

Lemma 4.8. *If $k \in \mathbb{N}_0$, $g_1, \dots, g_k \in G$ and $X \subset \text{Hom}(G, K^\times)$ is a subset, then there exist $a_1, \dots, a_k \in K^\times$ such that*

$$|\{\chi \in X \mid \chi(g_i) \neq a_i \text{ for all } i \in [1, k]\}| \leq |X| \prod_{i=1}^k \left(1 - \frac{1}{\text{ord}(g_i)}\right).$$

Proposition 4.9.

Let $S = g_1 \cdot \dots \cdot g_l \in \mathcal{F}(G)$ be a sequence, $k \in [1, l]$ and $a_1, \dots, a_k \in K^\times$.

1. *If $0 \notin \Sigma(S)$ and*

$$f = \prod_{i=1}^k (a_i - X^{g_i}) = \sum_{g \in G} c_g X^g \in K[G] \quad \text{with } c_g \in K \text{ for all } g \in G,$$

then $c_0 \neq 0$, and in particular $f \neq 0$.

2. *Let K be a splitting field of G and*

$$s = |\{\chi \in \text{Hom}(G, K^\times) \mid \chi(g_i) \neq a_i \text{ for all } i \in [1, k]\}| \leq l - k.$$

Then there exist $a_{k+1}, \dots, a_{k+s} \in K^\times$ such that

$$f = \prod_{i=1}^{k+s} (a_i - X^{g_i}) = 0.$$

In particular, $0 \in \Sigma(S)$.

Idea of Olson and Kruyswijk, 1969, see [12, 15]

Definition 4.10. Let $S = g_1 \cdot \dots \cdot g_l \in \mathcal{F}(G)$ be a sequence of length $|S| = l \in \mathbb{N}_0$ and let $g \in G$.

1. For every $k \in \mathbb{N}_0$ let

$$\mathbf{N}_g^k(S) = \left| \left\{ I \subset [1, l] \mid \sum_{i \in I} g_i = g \text{ and } |I| = k \right\} \right|$$

denote the number of subsequences T of S having sum $\sigma(T) = g$ and length $|T| = k$.

2. We define

$$\mathbf{N}_g(S) = \sum_{k \geq 0} \mathbf{N}_g^k(S), \quad \mathbf{N}_g^+(S) = \sum_{k \geq 0} \mathbf{N}_g^{2k}(S) \quad \text{and} \quad \mathbf{N}_g^-(S) = \sum_{k \geq 0} \mathbf{N}_g^{2k+1}(S).$$

Proposition 4.11. *Let G be a p -group, $S = g_1 \cdot \dots \cdot g_l \in \mathcal{F}(G)$, and*

$$f = \prod_{i=1}^l (1 - X^{g_i}) = \sum_{g \in G} c_g(S) X^g \in \mathbb{F}_p[G].$$

For every $g \in G$, we have $c_g(S) = \mathbf{N}_g^+(S) - \mathbf{N}_g^-(S) + p\mathbb{Z} \in \mathbb{F}_p$. In particular, if $c_0(S) = 0$, then $0 \in \Sigma(S)$, and if $g \in G^\bullet$ and $c_g(S) \neq 0$, then $g \in \Sigma(S)$.

Proof. For $g \in G$, we set

$$\Omega_g = \left\{ I \subset [1, l] \mid \sum_{i \in I} g_i = g \right\}.$$

Then $\emptyset \in \Omega_0$ and

$$c_g(S) = \sum_{J \in \Omega_g} (-1)^{|J|} + p\mathbb{Z} = \mathbf{N}_g^+(S) - \mathbf{N}_g^-(S) + p\mathbb{Z} \in \mathbb{F}_p.$$

Hence $c_0(S) = 0$ implies $0 \in \Sigma(S)$, and if $g \in G^\bullet$ is such that $c_g(S) \neq 0$, then $g \in \Sigma(S)$. \square

The Davenport constant

If (e_1, \dots, e_r) is a basis of G with $\text{ord}(e_i) = n_i$ for all $i \in [1, r]$, then

$$S = \prod_{i=1}^r e_i^{n_i-1} \in \mathcal{F}(G)$$

is zero-sumfree and hence

$$\mathbf{d}^*(G) := \sum_{i=1}^r (n_i - 1) \leq \mathbf{d}(G).$$

It is easy to check that $\mathbf{D}(G) \leq |G|$ whence we get $\mathbf{D}(C_n) = n$.

Theorem 4.12 (Olson and Kruyswijk, 1969).

If G is a p -group or $r(G) \leq 2$, then $\mathbf{d}(G) = \mathbf{d}^(G)$.*

Theorem 4.13. *We have $\mathbf{d}(G) > \mathbf{d}^*(G)$ in each of the foll. cases:*

1. $G = C_m \oplus C_n^2 \oplus C_{2n}$ where $m, n \in \mathbb{N}_{\geq 3}$ are odd and $m \mid n$.
2. $G = C_2^i \oplus C_{2n}^{5-i}$ where $n \in \mathbb{N}_{\geq 3}$ is odd and $i \in [2, 4]$.

Theorem 4.14. *Let $\exp(G) = n \geq 2$ and $H \subset G$ be a subgroup.*

- $\mathbf{d}(G) \leq (n - 1) + n \log \frac{|G|}{n}$.
- $\mathbf{d}(G) \leq \mathbf{d}(H) \exp(G/H) + \max\{\mathbf{d}(G/H), \eta(G/H) - \exp(G/H)\}$.

Conjecture 4.15.

1. *If $r(G) = 3$ or $G = C_n^r$ with $n, r \in \mathbb{N}_{\geq 3}$, then $\mathbf{d}(G) = \mathbf{d}^*(G)$.*
2. *If $|G| > 1$, then $\mathbf{D}(G) \leq \mathbf{d}^*(G) + r(G)$.*
3. *Every zero-sumfree sequence $S \in \mathcal{F}(G)$ of length $|S| = \mathbf{d}(G)$ has some element $g \in \text{supp}(S)$ with $\text{ord}(g) = \exp(G)$.*

On $\mathbf{d}(C_n^r)$: this is connected with covering the non-zero vertices of the unit-cube in $(\mathbb{Z}/n\mathbb{Z})^r$ with proper cosets.

Conjecture 4.8.3 could be simple

Generalized Davenport constants

Definition 4.16. Let $k \in \mathbb{N}$. We define

$$\mathcal{M}_k(G) = \{B \in \mathcal{B}(G) \mid \max \mathbf{L}(B) \leq k\},$$

and we denote by $\mathcal{M}_k^*(G)$ the set of all sequences $S \in \mathcal{F}(G)$ which are not divisible by a product of k non-empty zero-sum subsequences. We define

$$\mathbf{D}_k(G) = \sup\{|B| \mid B \in \mathcal{M}_k(G)\} \in \mathbb{N}_0 \cup \{\infty\}$$

and

$$\mathbf{d}_k(G) = \sup\{|S| \mid S \in \mathcal{M}_k^*(G)\} \in \mathbb{N}_0 \cup \{\infty\}.$$

Theorem 4.17. *Let G be finite, $\exp(G) = n$ and $k \in \mathbb{N}$.*

1. *Let $H \subset G$ be a subgroup such that $G = H \oplus C_n$. Then*

$$\mathbf{d}(H) + kn - 1 \leq \mathbf{d}_k(G) \leq (k-1)n + \max\{\mathbf{d}(G), \eta(G) - n - 1\}.$$

In particular, if $\mathbf{d}(G) = \mathbf{d}(H) + n - 1$ and $\eta(G) \leq \mathbf{d}(G) + n + 1$, then $\mathbf{d}_k(G) = \mathbf{d}(G) + (k-1)n$.

2. *If $\mathbf{r}(G) \leq 2$, then $\mathbf{d}_k(G) = \mathbf{d}(G) + (k-1)n$.*

3. *If G a p -group and $\mathbf{D}(G) \leq 2n - 1$, then $\mathbf{d}_k(G) = \mathbf{d}(G) + (k-1)n$.*

M. Freeze proved that

$$\mathbf{d}_2(C_2^r) > r + \lfloor \log_2 r \rfloor.$$

Inverse Problem:

Describe the structure of a minimal zero-sum sequence of length $D(G)$.

Theorem 4.18. *Let G be cyclic of order $n \geq 3$, $S \in \mathcal{F}(G)$ a zero-sumfree sequence of length*

$$|S| \geq \frac{n+1}{2}.$$

1. *For all $g \in \text{supp}(S)$ we have $\text{ord}(g) \geq 3$.*
2. *There exists some $g \in \text{supp}(S)$ with $\mathbf{v}_g(S) \geq 2|S| - n + 1$.*
3. *There exists some $g \in \text{supp}(S)$ with $\text{ord}(g) = n$ such that*
 $\mathbf{v}_g(S) \geq \frac{n+5}{6}$ *if n is odd, and $\mathbf{v}_g(S) \geq 3$ if n is even.*

Recent progress (keyword: index of a sequence) due to: Chapman and Smith [4], P. Yuan [40], S. Savchev and F. Chen [37, 36].

Theorem 4.19. *Let $G = C_n \oplus C_n$ with $n \geq 2$.*

Then the following statements are equivalent:

- (a) *If $S \in \mathcal{F}(G)$, $|S| = 3n - 3$ and S has no zero-sum subsequence T of length $|T| \geq n$, then there exists some $a \in G$ such that $0^{n-1}a^{n-2} \mid S$.*
- (b) *If $S \in \mathcal{F}(G)$ is zero-sumfree and $|S| = 2n - 2$, then $a^{n-2} \mid S$ for some $a \in G$.*
- (c) *If $S \in \mathcal{A}(G)$ and $|S| = 2n - 1$, then $a^{n-1} \mid S$ for some $a \in G$.*
- (d) *If $S \in \mathcal{A}(G)$ and $|S| = 2n - 1$, then there exists a basis (e_1, e_2) of G and integers $x_1, \dots, x_n \in [0, n - 1]$ with $x_1 + \dots + x_n \equiv 1 \pmod{n}$ such that*

$$S = e_1^{n-1} \prod_{\nu=1}^n (x_\nu e_1 + e_2).$$

Conjecture 4.20. *Let $G = C_n \oplus C_n$ with $n \geq 2$.
Every $S \in \mathcal{A}(G)$ satisfies the above conditions.*

The Conjecture holds true

- For small values of n (see G. Bhowmik and J.-C. Schlage-Puchta).
- for $|\text{supp}(S)| = 3$ (see G. Lettl and W.A. Schmid, [28])

Moreover, if it holds true for $G = C_n \oplus C_n$, then it holds true for $G = C_{2n} \oplus C_{2n}$ (see [13]).

Theorem 4.21. *Let $G = C_n \oplus C_n$ with $n \geq 2$, and $S \in \mathcal{A}(G)$ with $|S| = 2n - 1$.*

1. *We have $\text{ord}(g) = n$ for every $g \in \text{supp}(S)$.*
2. *If n is a prime, then $|\text{supp}(S)| \in [3, n]$.
Conversely, for every $j \in [3, n]$ there is an $U_j \in \mathcal{A}(G)$ with $|U_j| = 2n - 1$ and $|\text{supp}(U_j)| \in j$.*
3. *If $\varepsilon > 0$ and n is a sufficiently large prime (in dependence of ε), then there is some $g \in \text{supp}(S)$ with multiplicity $\mathbf{v}_g(S) > p^{\frac{1}{4}-\varepsilon}$ (Gao+Geroldinger+Schmid, Acta Arith. 2007, [16])*

The last result is based on the Theorem of Diaz da Silva-Hamidoune.

The cross number

This invariant was introduced by U. Krause.

Definition 4.22.

1. If $S = g_1 \cdot \dots \cdot g_l \in \mathcal{F}(G)$, then

$k(S) = \sum_{i=1}^l \frac{1}{\text{ord}g_i} \in \mathbb{Q}_{\geq 0}$ is called the *cross number* of S .

2. For $G = C_{q_1} \oplus \dots \oplus C_{q_s}$, where q_1, \dots, q_s are prime powers, we set

$$k^*(G) = \sum_{i=1}^s \frac{q_i - 1}{q_i}.$$

Note that $s = r^*(G)$ is the *total rank* of G (that is the maximal number of independent elements).

3. The invariant

$$K(G) = \max\{k(S) \mid S \in \mathcal{A}(G)\}$$

is called the *cross number* of G and

$$k(G) = \max\{k(S) \mid S \in \mathcal{F}(G) \text{ is zero-sumfree}\}$$

is called the *little cross number* of G .

If q is the smallest prime divisor of n , then an easy argument shows that

$$\frac{1}{n} + k^*(G) \leq \frac{1}{n} + k(G) \leq K(G) \leq \frac{1}{q} + k(G).$$

Conjecture 4.23. $\frac{1}{n} + k^*(G) = K(G)$.

Theorem 4.24. *If G is a p -group or $r^*(G) \leq 2$, then $\frac{1}{n} + k^*(G) = K(G)$.*

The elasticity and its refinements

For $k \in \mathbb{N}$ we have

$$\begin{aligned}\rho_k(G) &= \sup\{\sup L \mid L \in \mathcal{L}(G), \min L \leq k\} \\ &= \sup\{\sup L \mid L \in \mathcal{L}(G), k \in L\} \\ &= \sup\{\sup L \mid L \in \mathcal{L}(G), k = \min L\}.\end{aligned}$$

Exercise 4.25. Let $k, l \in \mathbb{N}$.

1. We have

$$\rho(G) = \sup\left\{\frac{\rho_m(G)}{m} \mid m \in \mathbb{N}\right\} = \lim_{m \rightarrow \infty} \frac{\rho_m(G)}{m},$$

$$k \leq \rho_k(G) \leq k\rho(G) = \frac{kD(G)}{2}, \quad \rho_{2k}(G) = kD(G)$$

2. $k + l \leq \rho_k(G) + \rho_l(G) \leq \rho_{k+l}(G)$.

3. For all $k \in \mathbb{N}$ we have

$$1 \leq \rho_{2k+1}(G) - kD(G) \leq \left\lfloor \frac{D(G)}{2} \right\rfloor.$$

4. Let $m \in \mathbb{N}$ with

$$\rho_{2m+1}(G) - mD(G) = \max\{\rho_{2k+1}(G) - kD(G) \mid k \in \mathbb{N}\}.$$

Then

$$\rho_{2m+2i+1}(G) = \rho_{2m+1}(G) + iD(G) \quad \text{for all } i \in \mathbb{N}_0.$$

In particular,

$$\rho_3(G) \geq \left\lfloor \frac{3D(G)}{2} \right\rfloor \quad \text{implies} \quad \rho_k(G) = \left\lfloor k \frac{D(G)}{2} \right\rfloor \quad \text{for all } k \geq 2.$$

Theorem 4.26 (Chapman, Freeze, Smith).

1. Let $G = G_1 \oplus G_2$ with subgroups $G_1, G_2 \subset G$ such that $d(G) = d(G_1) + d(G_2)$ and $d(G_2) = d(G_1) + \varepsilon$ with $\varepsilon \in \{0, 1\}$

Then

$$\rho_k(G) = \left\lfloor k \frac{D(G)}{2} \right\rfloor \quad \text{for all } k \geq 2.$$

2. Let $G = H^{2s}$ with a subgroup $H \subset G$ and $s \in \mathbb{N}$ such that $d^*(G) = d(G)$. Then

$$\rho_k(G) = \left\lfloor k \frac{D(G)}{2} \right\rfloor \quad \text{for all } k \geq 2.$$

3. Let $G = C_n^r$ with $n, r \in \mathbb{N}_{\geq 2}$ and $d^*(G) = d(G)$. Then

$$\rho_{2k+3}(G) \geq \left\lfloor \frac{3D(G) + 2 - n}{2} \right\rfloor + kD(G) \quad \text{for all } k \in \mathbb{N}_0.$$

4. If G is an elementary 2-group or an elementary 3-group, then

$$\rho_k(G) = \left\lfloor k \frac{D(G)}{2} \right\rfloor \quad \text{for all } k \geq 2.$$

PROBLEM: Find more groups having the above properties.

Theorem 4.27. For every $n \geq 4$ we have

$$\rho_3(C_n) \leq \frac{4n - 1}{3}.$$

In particular, $\rho_3(C_n) = n + 1$ for $n \in [3, 6]$.

Conjecture 4.28 (Chapman-Smith).

$\rho_3(C_n) = n + 1$ for all $n \geq 3$.

The set of distances and the catenary degree

Theorem 4.29. *Suppose that $|G| \geq 3$.*

1.

$$-1 + \sum_{i=1}^r \left\lfloor \frac{n_i}{2} \right\rfloor \in \Delta(G) \quad \text{and} \quad \max \left\{ n_r, 1 + \sum_{i=1}^r \left\lfloor \frac{n_i}{2} \right\rfloor \right\} \leq \mathbf{c}(G) \leq \mathbf{D}(G).$$

In particular,

$$\max \{ \exp(G), 1 + r(G) \} \leq \mathbf{c}(G) \leq |G|,$$

2. $\mathbf{c}(G) = \mathbf{D}(G)$ if and only if G is either cyclic or an elementary 2-group.
3. If $G = C_2 \oplus C_{2n}$ with $n \geq 2$ or $G = C_2^{r-1} \oplus C_4$ with $r \geq 2$, then $\mathbf{c}(G) = \mathbf{d}(G)$.
4. $\mathbf{c}(G) = 3$ if and only if $G \in \{C_3, C_2 \oplus C_2, C_3 \oplus C_3\}$.

Theorem 4.30.

1. $\Delta(G) = \emptyset$ if and only if $|G| \leq 2$.
2. We have

$$[1, \max \{ \exp(G) - 2, k - 1 \}] \subset \Delta(G) \subset [1, \mathbf{c}(G) - 2] \quad \text{with} \quad k = \sum_{i=1}^{r(G)} \left\lfloor \frac{n_i}{2} \right\rfloor.$$

3. $\Delta(G) = \{1\}$ if and only if $G \in \{C_3, C_3 \oplus C_3, C_2 \oplus C_2\}$.
4. If $G \in \{C_3, C_3 \oplus C_3, C_n, C_2 \oplus C_{2n}, C_2^r, C_2^{r-1} \oplus C_4 \mid n \geq 3, r \geq 2\}$, then $\Delta(G) = [1, \mathbf{c}(G) - 2]$.

Up to now there is no example with $\Delta(G) \neq [1, \mathbf{c}(G) - 2]$.

Conjecture 4.31. $\max \Delta(G) = \mathbf{c}(G) - 2$.

PROBLEM: Study $\Delta(C_n \oplus C_n)$!!!

Half-factorial and minimal non-half factorial sets

Definition 4.32. A subset $G_0 \subset G$ is called

- *half-factorial* if $\Delta(G_0) = \emptyset$,
- *non-half-factorial* if $\Delta(G_0) \neq \emptyset$.
- *minimal non-half-factorial* if it is non-half-factorial, but every proper subset is half-factorial.
- *weakly half-factorial* if $k(U) \in \mathbb{N}$ for every $U \in \mathcal{A}(G_0 \setminus \{0\})$.

We define

$$\mu(G) = \sup\{|G_0| \mid G_0 \text{ is half-factorial}\},$$

$$\mu_0(G) = \sup\{|G_0| \mid G_0 \text{ is weakly half-factorial}\},$$

and

$$\mu^*(G) = \sup\{|G_0| \mid G_0 \text{ is minimal non-half-factorial}\}.$$

Proposition 4.33. *Let $G_0 \subset G$ be a subset.*

1. *The following statements are equivalent:*

- (a) *G_0 is half-factorial.*
- (b) *$k(U) = 1$ for every $U \in \mathcal{A}(G_0 \setminus \{0\})$.*
- (c) *$L(B) = \{k(B)\}$ for every $B \in \mathcal{B}(G_0)$.*

In particular, G_0 is half-factorial if and only if G_0 is weakly half-factorial and $K(G_0) < 2$.

2. *If $|G_0| \leq 1$, then G_0 is half-factorial.*

3. *$\mu(G) \leq \mu_0(G)$, and equality holds if $K(G) < 2$.*

4. *$\mu^*(G) \leq \mu(G)$, and $\mu^*(G) = 0$ if and only if $|G| \leq 2$.*

5. *If G is finite, then $\mu(G) = |G|$ if and only if $|G| \leq 2$.*

Theorem 4.34 (Radziejewski-Schmid, [34]).

There is an explicit characterization of maximal weakly half-factorial sets by character theory. In particular, we have

$$\mu_0(G) = \sum_{1 \leq d | n_r} \prod_{i=1}^{r-1} \gcd(n_i, d).$$

Corollary 4.35. *Let G be cyclic of order $n \geq 2$.*

1. *For a subset $G_0 \subset G$ the following statements are equivalent:*

(a) *G_0 is weakly half-factorial.*

(b) *There exists some $g_0 \in G$ such that*

$$\langle G_0 \rangle = \langle g_0 \rangle \quad \text{and} \quad G_0 \subset \{ag_0 \mid 1 \leq a \mid \text{ord}(g_0)\}.$$

2. *We have*

$$\mu_0(G) = |\{d \in \mathbb{N} \mid 1 \leq d \mid n\}| = \prod_{p \in \mathbb{P}} (\mathbf{v}_p(n) + 1).$$

3. *If $r^*(G) \leq 2$ (that is, if n has at most two distinct prime divisors), then every weakly half-factorial set is half-factorial, and $\mu(G) = \mu_0(G)$.*

Recent results on $\mu(C_n)$ can be found in Plagne-Schmid ([33])

Next we define the set $\Delta^*(G)$ (as a special subset of $\Delta(G)$) which appeared in the Structure Theorem for Sets of Lengths.

Definition 4.36.

$$\Delta^*(G) = \{ \min \Delta(G_0) \mid G_0 \subset G \text{ is a non-half-factorial subset} \}.$$

Exercise 4.37. *Let $|G| \geq 3$.*

1. $1 \in \Delta^*(G) \subset \Delta(G) \subset [1, D(G) - 2]$.
2. *If there exists some $g \in G$ with $3 \leq \text{ord}(g) < \infty$, then $\text{ord}(g) - 2 \in \Delta^*(G)$.*
3. *If $r(G) \geq 2$, then $[1, r(G) - 1] \subset \Delta^*(G)$.*
4. *There exists a minimal non-half-factorial subset $G_0 \subset G$ with $\max \Delta^*(G) = \min \Delta(G_0)$.*

Theorem 4.38. *Let $\exp(G) = n \geq 3$.*

1.

$$\max \Delta^*(G) \leq \max \{ \exp(G) - 2, \min \{ \mu^*(G) - 2, 2k(G) - 1 \} \}.$$

2. *Suppose that*

$$r^*(G) \geq (n - 1) + \frac{1}{2}(n - 1)^2(n - 2).$$

Then $\max \Delta^(G) \leq r^*(G) - 1$, and $\Delta^*(G) = [1, r(G) - 1]$ if G is a p -group.*

3. *If $|G| \leq \max \{ e^{n/2}, n^2 \}$, then $\max \Delta^*(G) = n - 2$.*4. *If G is cyclic of order $n \geq 4$, then*

$$\max \Delta^*(G) = n - 2 \quad \text{and} \quad \max(\Delta^*(G) \setminus \{n - 2\}) = \left\lfloor \frac{n}{2} \right\rfloor - 1.$$

The system of sets of lengths

For $d \in \mathbb{N}$ and $l \in \mathbb{N}_0$ we set

$$P_l(d) = d\mathbb{Z} \cap [0, ld] = \{0, d, 2d, \dots, ld\}.$$

Lemma 4.39.

1. $\mathcal{L}(C_3) = \mathcal{L}(C_2 \oplus C_2) = \{y + 2k + P_k(1) \mid y, k \in \mathbb{N}_0\}$.
2. $\mathcal{L}(C_4) = \{y + k + 1 + P_k(1) \mid y, k \in \mathbb{N}_0\} \cup \{y + 2k + P_k(2) \mid y, k \in \mathbb{N}_0\}$.
3. $\mathcal{L}(C_2^3) = \{y + (k + 1) + P_k(1) \mid y \in \mathbb{N}_0, k \in [0, 2]\} \cup \{y + k + P_k(1) \mid y \in \mathbb{N}_0, k \geq 3\} \cup \{y + 2k + P_k(2) \mid y, k \in \mathbb{N}_0\}$.

PROBLEM: Write down $\mathcal{L}(G)$ for some further small groups !

Exercise 4.40.

1. $\mathcal{L}(G) = \{y + L \mid y \in \mathbb{N}_0, L \in \mathcal{L}(G \setminus \{0\})\} \supset \{\{y\} \mid y \in \mathbb{N}_0\}$,
and equality holds if and only if $|G| \leq 2$.
2. If $G_0 \subset G$ is a subset, then $\mathcal{L}(G_0) \subset \mathcal{L}(G)$.
3. Let G' be an abelian group with $|G'| \geq 3$ such that $\mathcal{L}(G) = \mathcal{L}(G')$. Then we have $\rho_k(G) = \rho_k(G')$ for every $k \in \mathbb{N}$, $\mathbf{D}(G) = \mathbf{D}(G')$, $\Delta_1(G) = \Delta_1(G')$ and $\max \Delta^*(G) = \max \Delta^*(G')$.
4. There exist (up to isomorphisms) only finitely many abelian groups G' such that $\mathcal{L}(G) = \mathcal{L}(G')$, and all of them are finite.

PROBLEM: Find further invariants such that 3. holds !

Conjecture 4.41. *Let G and G' be finite abelian groups with $|G| \geq |G'| \geq 4$ such that $\mathcal{L}(G) = \mathcal{L}(G')$. Then $G \cong G'$.*

Theorem 4.42. *Let G and G' be finite abelian groups such that $\mathcal{L}(G) = \mathcal{L}(G')$, and suppose that $\{G, G'\} \neq \{C_1, C_2\}$ and $\{G, G'\} \neq \{C_3, C_2^2\}$.*

1. *If G is either cyclic or an elementary 2-group or isomorphic to $C_2 \oplus C_{2n}$, then $G \cong G'$.*
2. *If G is an elementary p -group and G' an elementary q -group, then $G \cong G'$.*

The above conjecture is in contrast to the following result,

Theorem 4.43. *If S is a zero-sum sequence such that*

$$\text{supp}(S) \cup \{0\} \quad \text{is a group,}$$

then $c(S) \leq 3$ and therefore

$$L(S) \quad \text{is an arithmetical progression with difference } 1.$$

which is based on

Definition 4.44.

A sequence $S \in \mathcal{F}(G)$ is called *additively closed* with respect to a pair of subsequences (B, C) if $S = BC$ and the following condition is satisfied:

If $g_1, g_2 \in G$ and either $g_1g_2 \mid B$ or $g_1g_2 \mid C$, then $g_1 + g_2 \mid S$.

Theorem 4.45.

Let $S \in \mathcal{F}(G \setminus \{0\})$ be a sequence of length $|S| \geq 4$ which is additively closed with respect to a pair of subsequences (B, C) such that $|B| \geq |C|$.

Then S has a proper zero-sum subsequence, apart from the following exceptions:

1. $|C| = 1$, and we are in one of the following cases:
 - (a) $B = g^k$ and $C = 2g$ for some $k \geq 3$ and $g \in G$ with $\text{ord}(g) \geq k + 2$.
 - (b) $B = g^k(2g)$ and $C = 3g$ for some $k \geq 2$ and $g \in G$ with $\text{ord}(g) \geq k + 5$.
 - (c) $B = g_1g_2(g_1 + g_2)$ and $C = g_1 + 2g_2$ for some $g_1, g_2 \in G$ with $\text{ord}(g_1) = 2$ and $\text{ord}(g_2) \geq 5$.
2. $\{B, C\} = \{g(9g)(10g), (11g)(3g)(14g)\}$ for some $g \in G$ with $\text{ord}(g) = 16$.

REFERENCES

- [1] D.D. Anderson, D.F. Anderson, and M. Zafrullah, *Factorization in integral domains*, J. Pure Appl. Algebra **69** (1990), 1 – 19.
- [2] D.D. Anderson, J. Mott, and M. Zafrullah, *Finite character representations for integral domains*, Boll. Unione Mat. Ital. **6** (1992), 613 – 630.
- [3] D.F. Anderson, S.T. Chapman, and W.W. Smith, *On Krull half-factorial domains with infinite cyclic divisor class group*, Houston J. Math. **20** (1994), 561 – 570.
- [4] S.T. Chapman and W.W. Smith, *A characterization of minimal zero-sequences of index one in finite cyclic groups*, Integers **5(1)** (2005), Paper A27, 5p.
- [5] J.A. Dias da Silva and Y.ould Hamidoune, *Cyclic spaces for Grassmann derivatives and additive theory*, Bull. Lond. Math. Soc. **26** (1994), 140 – 146.
- [6] Y. Edel, *A product construction for sequences in finite abelian groups of odd order without zero-sum subsequences of length $\exp(G)$* , Des. Codes Cryptography, to appear.
- [7] Y. Edel, C. Elsholtz, A. Geroldinger, S. Kubertin, and L. Rackham, *Zero-sum problems in finite abelian groups and affine caps*, Quarterly. J. Math., Oxford II. Ser., 28pp, to appear.
- [8] P. Erdős, A. Ginzburg, and A. Ziv, *Theorem in the additive number theory*, Bull. Research Council Israel **10** (1961), 41 – 43.
- [9] A. Facchini, *Direct sum decomposition of modules, semilocal endomorphism rings, and Krull monoids*, J. Algebra **256** (2002), 280 – 307.
- [10] A. Facchini, W. Hassler, L. Klingler, and R. Wiegand, *Direct-sum decompositions over one-dimensional Cohen-Macaulay local rings*, Multiplicative Ideal Theory in Commutative Algebra (J.W. Brewer, S. Glaz, W. Heinzer, and B. Olberding, eds.), Springer, 2006, pp. 153 – 168.
- [11] A. Facchini and D. Herbera, *K_0 of a semilocal ring*, J. Algebra **225** (2000), 47 – 69.
- [12] W. Gao and A. Geroldinger, *On the number of subsequences with given sum of sequences over finite abelian p -groups*, Rocky Mt. J. Math., to appear.
- [13] ———, *On zero-sum sequences in $\mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$* , Integers **3** (2003), Paper A08, 45p.
- [14] ———, *Zero-sum problems in finite abelian groups: a survey*, Expo. Math. **24** (2006), 337 – 369.
- [15] W. Gao, A. Geroldinger, and F. Halter-Koch, *Group algebras of finite abelian groups and their applications to combinatorial problems*, manuscript.
- [16] W. Gao, A. Geroldinger, and W.A. Schmid, *Inverse zero-sum problems*, Acta Arith., 37pp, to appear.
- [17] A. Geroldinger and R. Göbel, *Half-factorial subsets in infinite abelian groups*, Houston J. Math. **29** (2003), 841 – 858.
- [18] A. Geroldinger and F. Halter-Koch, *Non-Unique Factorizations. Algebraic, Combinatorial and Analytic Theory*, Pure and Applied Mathematics, vol. 278, Chapman & Hall/CRC, 2006.
- [19] A. Geroldinger and W. Hassler, *Arithmetic of Mori domains and monoids*, manuscript.
- [20] ———, *Local tameness of v -noetherian monoids*, manuscript.
- [21] A. Geroldinger, W. Hassler, and G. Lettl, *On the arithmetic of strongly primary monoids*, Semigroup Forum, to appear.
- [22] W. Hassler, *Factorization properties of Krull monoids with infinite class group*, Colloq. Math. **92** (2002), 229 – 242.
- [23] ———, *Factorization in finitely generated domains*, J. Pure Appl. Algebra **186** (2004), 151 – 168.
- [24] J.A. Huckaba, *Commutative rings with zero-divisors*, Pure and Applied Mathematics, vol. 117, Marcel Dekker, 1988.
- [25] F. Kainrath, *Factorization in Krull monoids with infinite class group*, Colloq. Math. **80** (1999), 23 – 30.
- [26] ———, *Elasticity of finitely generated domains*, Houston J. Math. **31** (2005), 43 – 64.
- [27] ———, *On local half-factorial orders*, Arithmetical Properties of Commutative Rings and Monoids, Lect. Notes Pure Appl. Math., vol. 241, Chapman & Hall/CRC, 2005, pp. 316 – 324.
- [28] G. Lettl and W.A. Schmid, *Minimal zero-sum sequences in $C_n \oplus C_n$* , Eur. J. Comb. **28** (2007), 742 – 753.
- [29] V.F. Lev, *Restricted set addition in abelian groups: results and conjectures*, J. Théor. Nombres Bordx. **17** (2005), 181 – 193.

- [30] T.G. Lucas, *The Mori property in rings with zero divisors*, Rings, Modules, Algebras, and Abelian Groups, Lect. Notes Pure Appl. Math., vol. 236, Marcel Dekker, 2004, pp. 379 – 400.
- [31] W. Narkiewicz, *Finite abelian groups and factorization problems*, Colloq. Math. **42** (1979), 319 – 330.
- [32] ———, *A note on elasticity of factorizations*, J. Number Theory **51** (1995), 46 – 47.
- [33] A. Plagne and W.A. Schmid, *On the maximal cardinality of half-factorial sets in cyclic groups*, Math. Ann. **333** (2005), 759 – 785.
- [34] M. Radziejewski and W.A. Schmid, *Weakly half-factorial sets in finite abelian groups*, Forum Math., to appear.
- [35] K. Rogers, *A combinatorial problem in abelian groups*, Proc. Camb. Philos. Soc. **59** (1963), 559 – 562.
- [36] S. Savchev and F. Chen, *Long n -zero-free sequences in finite cyclic groups*, Discrete Math.
- [37] ———, *Long zero-free sequences in finite cyclic groups*, Discrete Math.
- [38] W.A. Schmid, *A realization theorem for sets of lengths*, manuscript.
- [39] R. Wiegand, *Direct-sum decompositions over local rings*, J. Algebra **240** (2001), 83 – 97.
- [40] P. Yuan, *On the index of minimal zero-sum sequences over finite cyclic groups*, J. Comb. Theory, Ser. A, to appear, –.