Graz school of Discrete Mathematics
TU & KFU Graz Austria

UNI GRAZ

Factorization Theory: From Algebra to Additive Combinatorics

PhD-Defense Aqsa Bashir
Advisor: Prof. Geroldinger

University of Graz

June 27, 2024

Outline

Factorization theory

Factorization theory studies decompositions of elements into irreducible elements, known as atoms, in rings and semigroups.

e.g.,

- $6 = 2 \cdot 3 \quad$ (in $\mathbb{Z}$)

Factorization theory

Factorization theory studies decompositions of elements into irreducible elements, known as atoms, in rings and semigroups.

e.g.,

- $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}) \quad (\text{in } \mathbb{Z}[\sqrt{-5}])$

- **Key focus areas:**
  - Multiplicative semigroups of regular elements of a ring.
  - Semigroups of ideals (nonzero, invertible, divisorial).
  - Semigroups of module isomorphism classes.
- **Historical background:**
  - Origin in algebraic number theory.
  - Carlitz's result (1960): $\mathcal{O}_K$ is half-factorial if and only if the class group has at most two elements.

    Philosophy: The class group G controls the arithmetic of $\mathcal{O}_K$.

  - Narkiewicz (1970s) posed the inverse question of whether or not the arithmetical behavior characterize the class group.

Central strategy

$$
\begin{tikzcd}
\text{given } H \arrow[rr, bend left, "\text{transfer hom.}"] & & \text{auxiliary monoid } B
\end{tikzcd}
$$

Key application:

Given an integral domain R with class group G,

$$\begin{tikzcd} R^\bullet = R \setminus \{0\} \arrow[rr, bend left, "\text{transfer hom.}"] & & \mathcal{B}(G) \end{tikzcd}$$

Significance:

- Allows the study of arithmetic properties in rings of integers using methods from additive combinatorics.
- Translates algebraic problems into combinatorial ones.
- Results are pulled back to the original algebraic setting.

Outline

Monoids

Monoid: H, multiplicatively written, commutative, semigroup with identity element

$H^\times$ group of units, $\mathcal{A}(H)$ set of atoms, H is reduced if $H^\times = \{1\}$.

- H is said to be cancellative if $au = bu$ implies $a = b$ for all $a, b, u \in H$ and in that case $\mathsf{q}(H)$ denotes the quotient group.
- If $x = u_1 \ldots u_k$, where $u_1, \ldots, u_k \in \mathcal{A}(H)$, then k is called the length of the factorization.
- $\mathsf{L}(x) = \{k \in \mathbb{N} \mid k \text{ is a factorization length of } x\}$ is the length set.
- H is factorial if every nonunit has unique factorization.
- H is half-factorial if $|\mathsf{L}(x)| = 1$ for every $x \in H$.

Examples: $\mathbb{N}$, $R^\bullet = (R \setminus \{0\}, \cdot)$ for an integral domain R, monoids of ideals $\mathcal{I}(R)$, $\mathcal{I}^*(R)$, ...

Divisor theory

A monoid homomorphism $\varphi\colon H \to D$ is said to be a

- divisor homomorphism if, for all $a, b \in H$,

$$a \,|\, _H b \quad \text{if and only if} \quad \varphi(a) \,|\, _D \varphi(b)\,.$$

- (Skula, 1970) divisor theory if
  - φ is a divisor homomorphism,
  - $D = \mathcal{F}(P)$ is free abelian,
  - For every $p \in P$, there are $a_1, \ldots, a_m \in H$ such that $p = \gcd\big(\varphi(a_1), \ldots, \varphi(a_m)\big)$.

  Then the quotient group $\mathcal{C}(H) = \mathsf{q}(D)/\varphi(\mathsf{q}(H))$ is called the *divisor class group* of H.

Krull monoids

Theorem (Chouinard, Geroldinger+Halter-Koch, 1980s- 90s)

A monoid H is said to be **Krull** *if it satisfies one of the following equivalent conditions:*

1. *H has a divisor theory.*
2. *$\varphi : H \to \mathcal{I}_v^*(H)$ is a divisor theory.*
3. *H is completely integrally closed and satisfies the ascending chain condition on divisorial ideals.*
4. *$H = H^\times \times T$ and T is a saturated submonoid of a free abelian monoid.*
5. *H has a divisor homomorphism into a factorial monoid.*

Theorem (Krause, Wauters, 1990s)

An integral domain R is a Krull domain if and only if its multiplicative monoid $R^\bullet$ is a Krull monoid.

- (Classic) A monoid is factorial if and only if it is Krull with trivial class group.
- (Carlitz 1960) Let H be a Krull monoid with class group G such that every class contains a prime divisor. Then

$$H \quad \text{is half-factorial if and only if} \quad |G| \le 2\,.$$

Classical examples of Krull monoids

Examples

- Integrally closed Noetherian domains, in particular Dedekind domains, e.g., $\mathcal{O}_K^\bullet$.
- Let $0 \neq f \in \mathrm{Int}(\mathbb{Z})$, then

$$[\![f]\!] = \{ g \in \mathrm{Int}(\mathbb{Z}) : g \mid f^n \text{ for some } n \in \mathbb{N} \}$$

is a Krull monoid.

- (Chouinard 1981) Let H be a reduced monoid. Then $R[H]$ is a Krull domain if and only if both R and H are Krull.
  - (Fadinger+Windisch, 2022) If $R[H]$ is Krull then every class of $\mathcal{C}_v(R[H])$ contains infinitely many prime divisors.
- **Monoid of zero-sum sequences.**

Monoid of zero-sum sequences I

Let $(G, +)$ be a finite abelian group, $\emptyset \neq G_0 \subset G$ and let $\mathcal{F}(G_0)$ be the free monoid with basis G_0.

- A sequence $S = g_1 \ldots g_l$ is a finite, unordered sequence with terms from G_0, repetition allowed.
- S is called a zero-sum sequence if $\sigma(S) = g_1 + \ldots + g_l = 0$,
- a minimal zero-sum sequence if no proper subsequence has sum zero.
- and a zero-sum free sequence if $\sum_{i \in I} g_i \neq 0$ for each $\emptyset \neq I \subseteq [1, \ell]$.

▶ $\mathcal{B}(G_0) = \{S \in \mathcal{F}(G) : \sigma(S) = 0\} \subset \mathcal{F}(G_0)$ is the monoid of zero-sum sequences.

- $\mathcal{A}(G_0) := \mathcal{A}(\mathcal{B}(G_0)) = \{\text{minimal zero-sum sequences}\}$.
- $\mathcal{A}^*(G_0) := \mathcal{A}^*(\mathcal{B}(G_0)) = \{\text{zero-sum free sequences}\}$.

Example

Let $G = \{0, e, 2e\}$ and $G_0 = \{e, 2e\}$. Then

- $\mathcal{B}(G_0) = \{e^3, e(2e), (2e)^3, \dots\}$.
- $\mathcal{A}(G_0) = \{e^3, e(2e), (2e)^3\}$.
- $\mathcal{A}^*(G_0) = \{\emptyset, e, e^2, 2e, (2e)^2\}$.

$\mathcal{B}(G_0)$ is Krull

Theorem

The inclusion $\mathcal{B}(G_0) \hookrightarrow \mathcal{F}(G_0)$ is a divisor theory. In particular, $\mathcal{B}(G_0)$ is a Krull monoid.

Indeed,

$$T \mid S \text{ in } \mathcal{B}(G_0) \quad \text{if and only if} \quad T \mid S \text{ in } \mathcal{F}(G_0)\,.$$

Outline

Factorization theory

Krull monoids

Transfer homomorphisms

Structure of sets of lengths with maximal elasticity

Sets of cross numbers

Transfer hom. I

Definition

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

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

(T 2) If $a \in H$, $b_1, b_2 \in B$ and $\theta(a) = b_1 b_2$, then there exist $a_1, a_2 \in H$ such that $a = a_1 a_2$, $\theta(a_1) \simeq b_1$ and $\theta(a_2) \simeq b_2$.

Lemma (Transfer lemma)

Let $\theta \colon H \to B$ be a transfer homomorphism. Then we have:

- *a is irreducible in H if and only if $\theta(a)$ is irreducible in B.*
- $\mathsf{L}_H(a) = \mathsf{L}_B\big(\theta(a)\big)$ *for all $a \in H$.*

  Thus transfer homomorphisms preserve sets of lengths.

Transfer hom. II

Theorem (Narkiewicz, Geroldinger, Halter-Koch 1970s-90s)

Let H be a reduces Krull monoid with class group G. Let $G_p \subset G$ be the set of classes containing prime divisors. Then $\beta : H \to \mathcal{B}(G_p)$ is a transfer homomorphism.

Transfer hom. from a general Krull monoid to $\mathcal{B}(G_P)$

Suppose the embedding $H \hookrightarrow \mathcal{F}(P)$ is a divisor theory.

$$\begin{array}{ccc} H & \longrightarrow & \mathcal{F}(P) \cong \mathcal{I}_v^*(H) \\ \beta \big\downarrow & & \big\downarrow \widetilde{\beta} \\ \mathcal{B}(G_P) & \longrightarrow & \mathcal{F}(G_P) \end{array}$$

Then $\widetilde{\beta}$ and its restriction $\beta = \widetilde{\beta} \mid H$ are transfer homomorphisms mapping

$$a = p_1 \ldots p_l \in \mathcal{F}(P) \quad \text{to} \quad S = \beta(a) = [p_1] \ldots [p_l] \in \mathcal{F}(G_P)$$

In particular,

- a is irreducible in H if and only if S is irreducible in $\mathcal{B}(G_P)$.
- $\mathsf{L}_H(a) = \mathsf{L}_{\mathcal{B}(G_P)}(S)$.

Transfer Krull monoids

Definition

A monoid H is said to be a **transfer Krull monoid** if there is a transfer homomorphism θ to a Krull monoid B.

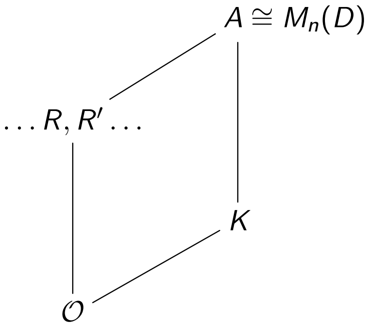
Examples

- Every Krull monoid is transfer Krull.
- Every half-factorial monoid H is transfer Krull.

Beyond Krull I: Classical maximal orders

Let

- K be a global field, A a central simple K-algebra,
- $\mathcal{O}$ a holomorphy ring of K,
- and R a classical maximal $\mathcal{O}$-order in A (R subring of A, $Z(R) = \mathcal{O}$, f.g. as $\mathcal{O}$-module, maximal).
- e.g., $R = M_n(\mathcal{O})$



(Smertnig 2013) If every stably free left R-ideal is free, then there exists a transfer homomorphism

$$\theta \colon R^{\bullet} \to \mathcal{B}(\mathcal{C}_A(\mathcal{O})),$$

with $\mathcal{C}_A(\mathcal{O})$ a ray class group of $\mathcal{O}$.

Method: Theory of one-sided divisorial ideals.

Beyond Krull II: Stable orders in Dedekind domains

A domain R is said to be stable if every nonzero ideal I of R is projective over its ring of endomorphisms.

Theorem (B.+Geroldinger+Reinhart, 2021)

Let R be a stable order in a Dedekind domain. The following statements are equivalent.

(a) $\mathcal{I}(R)$ *is transfer Krull.*

(b) $\mathcal{I}^*(R)$ *is transfer Krull.*

(c) $\mathcal{I}^*(R)$ *is half-factorial.*

(d) $\mathcal{I}(R)$ *is half-factorial.*

Outline

Factorization theory

Krull monoids

Transfer homomorphisms

Structure of sets of lengths with maximal elasticity

Sets of cross numbers

Definition

Monoid: H, $\mathcal{B}(G)$

- $\mathsf{L}(a) = \{k \mid a \text{ has a factorization of length } k\} \subset \mathbb{N}$ is the set of lengths of a.
- $\Delta(L(a)) = \{\text{consecutive differences of } L(a)\}$ is the set of distances of $L(a)$.
- $\Delta(H) = \bigcup_{L \in \mathcal{L}(H)} \Delta(\mathsf{L}) \subset \mathbb{N}$ the set of distances of H.
- The system of all sets of lengths

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

- The elasticity $\rho(H) = \sup\{\max L / \min L \mid L \in \mathcal{L}(H)\}$.

Basic facts

FACT I. H is half-factorial $\Leftrightarrow$ $|L| = 1$ for all $L \in \mathcal{L}(H)$, $\Delta(H) = \emptyset$, $\rho(H) = 1$.

FACT II. An atomic monoid H is

- EITHER half-factorial

  OR

- For all $m \in \mathbb{N}$ there is an $L \in \mathcal{L}(H)$ with $|L| > m$.

Zero-sum sequences II

Notation: $\mathcal{A}(G_0) := \mathcal{A}\big(\mathcal{B}(G_0)\big)$, $\Delta(G_0) := \Delta\big(\mathcal{B}(G_0)\big)$,
$\rho(G_0) := \rho\big(\mathcal{B}(G_0)\big)$, and $\mathcal{L}(G_0) := \mathcal{L}\big(\mathcal{B}(G_0)\big)$.

The Davenport constant

$$\mathsf{D}(G_0) := \sup\{|S| \colon S \in \mathcal{A}(G_0)\}$$

is a well-studied invariant in Additive Combinatorics.

SIMPLE FACTS. Let G be finite abelian.

- $\max \Delta(G) \le \mathsf{D}(G) - 2$.
- $\rho(G) = \mathsf{D}(G)/2$.

Structure theorem for sets of lengths

Long sets of lengths have a well-defined structure: contributions by Freiman, Geroldinger, Halter-Koch, Grynkiewicz, Kainrath

Theorem

There is a constant $M = M(G) \in \mathbb{N}_0$ such that every set of lengths $L \in \mathcal{L}(G)$ is an AAMP with difference $d \in \Delta(G)$ and bound M.

An AAMP is a union of arithmetical progressions

- having the same difference and
- some gaps at the beginning and at the end

Schmid (2009): This description is best possible.

Structure of sets of lengths with max. elasticity

Theorem (B.+Geroldinger+Zhong, 2021)

Let H be a transfer Krull monoid over a finite abelian group G and suppose that $\Delta_\rho(H) = \{1\}$. Then there exists a constant $M \in \mathbb{N}_0$ such that every $L \in \mathcal{L}(H)$ with $\rho(L) = \rho(H)$ has the form

$$L = y + (L' \cup [0, \ell] \cup L'')\,,$$

where $y \in \mathbb{Z}$, $\ell \in \mathbb{N}_0$, $L' \subset [-M, -1]$, and $L'' \subset \ell + [1, M]$.

Conjecture (A)

Let H be a transfer Krull monoid over a finite abelian group G with $|G| > 4$. Then $\Delta_\rho(H) = \{1\}$ if and only if G is neither cyclic nor an elementary 2-group.

$\Delta_\rho(H)$

.......looks rather complicated

Definition

Let $\Delta_\rho(H)$ denote the set of all $d \in \mathbb{N}$ with the following property: for every $k \in \mathbb{N}$, there is some $L_k \in \mathcal{L}(H)$ with $\rho(L_k) = \rho(H)$ and which has the form

$$L_k = y + (L' \cup \{0, d, \ldots, \ell d\} \cup L'') \subset y + d\mathbb{Z}$$

where $y \in \mathbb{Z}$, $\ell \geq k$, $\max L' < 0$, and $\min L'' > \ell D$.

- Clearly $\Delta_\rho(H) \subset \Delta(H)$.

Proof of Conjecture (A)

Theorem (B.+Geroldinger+Zhong 2021)

Let H be a transfer Krull monoid over a finite abelian non-cyclic group G. Then $\Delta_\rho(H) = \{1\}$ for the following groups.

(a) *G is a rank-2 group.*

(b) *G is a p-group such that $\gcd(\exp(G) - 2, \mathsf{D}(G) - 2) = 1$.*

(c) *$G \cong C_{p^{s_1}}^{r_1} \oplus C_{p^{s_2}}^{r_2}$, where p is a prime and $r_1, r_2, s_1, s_2 \in \mathbb{N}$ such that s_1 divides s_2.*

(d) *G is a group with exponent $\exp(G) = pq$, where p, q are distinct primes satisfying one of the four properties.*

  (i) $\gcd(pq - 2, \mathsf{D}(G) - 2) = 1$.
  (ii) $\gcd(pq - 2, p + q - 3) = 1$.
  (iii) $q = 2$ *and* $p - 1$ *is a power of* 2.
  (iv) $q = 2$ *and* $\mathsf{r}_p(G) = 1$.

(e) *G is a group with exponent $\exp(G) \in [3, 11] \setminus \{8\}$.*

Take away & ...

- For transfer Krull monoids with $\Delta_\rho(H) = \{1\}$, all sets of lengths L with maximal elasticity are intervals, apart from their globally bounded initial and end parts.

- The set $\Delta_\rho^*(G) = \{\min \Delta(G_0) \mid G_0 = \mathrm{supp}(A) \text{ for some } A \in \mathcal{B}(G) \text{ with } \rho(L(A)) = \rho(G)\}$ is a crucial invariant to study $\Delta_\rho(H)$ and $\Delta_\rho^*(G)$ is studied via **cross numbers**...

Outline

Cross numbers

Let G be an additive finite abelian group and $\exp(G)$ the exponent of G. Let $S = g_1 \ldots g_\ell \in \mathcal{F}(G)$.

- $\mathsf{k}(S) = \sum_{i=1}^{\ell} \frac{1}{\operatorname{ord}(g_i)} \in \mathbb{Q}_{\ge 0}$ is the **cross number** of S.
- $\mathsf{K}(G) = \max\{\mathsf{k}(S) \mid S \in \mathcal{A}(G)\}$ is the **(large) cross number** of G.
- $\mathsf{k}(G) = \max\{\mathsf{k}(S) \mid S \in \mathcal{A}^*(G)\}$ is the **(small) cross number** of G.

Significance of this invariant

Lemma (Skula+Zaks, 1976)

Let $G_0 \subset G$ be a non-empty subset. Then TFAE.

- *G_0 is half-factorial.*
- $\mathsf{k}(S) = 1$ *for all* $S \in \mathcal{A}(G_0)$.
- $\mathsf{L}(S) = \{\mathsf{k}(S)\}$ *for all* $S \in \mathcal{A}(G_0)$.

Let $G = C_{q_1} \oplus \ldots \oplus C_{q_r}$ be a direct sum decomposition of G into cyclic groups of prime power order.
Set

$$\mathsf{k}^*(G) := \sum_{i=1}^{r} \frac{q_i - 1}{q_i} \quad \textit{and} \quad \mathsf{K}^*(G) := \frac{1}{\exp(G)} + \mathsf{k}^*(G)\,.$$

Then

$$\mathsf{K}^*(G) \le \mathsf{K}(G) \quad \text{and} \quad \mathsf{k}^*(G) \le \mathsf{k}(G) \qquad\qquad (A)$$

EASY!!

Question: When does the equality hold in **(A)**?
So far: Equality holds for p-groups
(not so easy! proof using group algebras).
Open: since decades and there is no group known for which equality does NOT hold.

Theorem (B.+Schmid, 2024)

- *Let H be a finite abelian group of odd order. If $\mathsf{K}(H) = \mathsf{K}^*(H)$ and $\sum_{d \mid \exp(H)} \frac{1}{d} < 2$, then $\mathsf{K}(C_2 \oplus H) = \mathsf{K}^*(C_2 \oplus H)$.*
- *Let $G = C_2^2 \oplus G_p$ where G_p is a p-group for some odd prime p. Then $\mathsf{K}^*(G) = \mathsf{K}(G)$.*

Sets of cross numbers

- $\mathsf{W}(G) = \{\mathsf{k}(S) \mid S \in \mathcal{A}(G)\}$.
- $\mathsf{w}(G) = \{\mathsf{k}(S) \mid S \in \mathcal{A}^*(G)\}$.

▶ Let $g \in G$ with $\operatorname{ord}(g) = \exp(G)$, then $S = g(-g) \in \mathcal{A}(G)$. Therefore,

$$\mathsf{W}(G) \subseteq \frac{1}{\exp(G)}[2, \exp(G)\mathsf{K}(G)]$$

and similarly

$$\mathsf{w}(G) \subseteq \frac{1}{\exp(G)}[1, \exp(G)\mathsf{k}(G)]\,.$$

Question: Are $\mathsf{W} := \exp(G)\mathsf{W}(G)$ and $\mathsf{w} := \exp(G)\mathsf{w}(G)$ intervals? If not, is there a visible gap structure?

Theorem (B.+Schmid, 2024)

Let G be a finite abelian group.

1. $[1, \exp(G) - 1] \subseteq \mathsf{w}$.
2. *If the rank of G is large with respect to the exponent, w is an interval, apart from a globally bounded upper part.*

Theorem (B.+Schmid, 2024)

- *Let $G = C_{n_1} \oplus \ldots \oplus C_{n_r}$ be a finite abelian p-group with* $1 = n_0 < n_1 \mid \ldots \mid n_r = \exp(G) = p^k$.
  1. *Suppose $p = 2$ and $n_{r-1} < n_r$. Then*
  $$\mathrm{W} = 2[1, \frac{p^k}{2}\mathrm{K}(G)] \quad \textit{and} \quad \mathrm{w} = [1, p^k\mathrm{k}(G)]\,.$$
  2. *Otherwise,*
  $$\mathrm{W} = [2, p^k\mathrm{K}(G)] \quad \textit{and} \quad \mathrm{w} = [1, p^k\mathrm{k}(G)]\,.$$
- *Let $G = C_{2p^k}$. Then*
$$\mathrm{W} = 2[1, \frac{3p^k - 1}{2}] \quad \textit{and} \quad \mathrm{w} = [1, 3p^k - 2]\,.$$

Theorem (B.+Schmid, 2024)

Let $G = C_p^r \oplus C_q^s$ for $p > q$ odd primes. Then

- $\mathsf{w} = [1, pq\mathsf{k}^*(G)] \setminus \{\textit{some gaps at the upper end}\}$ *and* $\mathsf{k}(G) = \mathsf{k}^*(G)$.
- $\mathsf{W} = [2, pq\mathsf{K}^*(G)] \setminus \{\textit{some gaps at the upper end}\}$ *and* $\mathsf{K}(G) = \mathsf{K}^*(G)$.

Publications

A. Bashir, A. Geroldinger and A. Reinhart (2021)
On the arithmetic of stable domains
Communications in Algebra 49 , 4763 – 4787.

A. Bashir and A. Geroldinger and Q. Zhong (2021)
On a zero-sum problem arising from factorization theory
Combinatorial and Additive Number Theory IV, Springer.

A. Bashir and A. Reinhart (2022)
On transfer Krull monoids
Semigroup Forum 105 , 73 – 95.

A. Bashir and W. Schmid (2024)
Sets of cross numbers of sequences over finite abelian groups
see https://arxiv.org/pdf/2403.07138.

Thank you!