DOCTORAL PROGRAM
DISCRETE MATHEMATICS
TU & KFU GRAZ • MU LEOBEN
AUSTRIA

UNI GRAZ

Franz Halter-Koch's Contributions to Factorization Theory: The Story of a New Idea

Alfred Geroldinger

Arithmetic and Ideal Theory of
Rings and Semigroups
Graz, 2014

Outline

Rings of Integers in Algebraic Number Fields

Let R be a ring of integers in an algebraic number field with (ideal) class group $G = \mathcal{C}(R)$.

19th Century:

- **Observation:** R is factorial if and only if G is trivial.
- **Philosophy:** The class group G controls the arithmetic of R.

Problem: Describe and classify phenomena of non-uniqueness of factorizations.

Carlitz and Sets of Lengths

If H is a multiplicatively written, cancellative semigroup and $a = u_1 \cdot \ldots \cdot u_k \in H$ where $u_1, \ldots, u_k$ are irreducibles (atoms), then

- k is called the length of the factorization and
- $\mathsf{L}_H(a) = \{k \mid a \text{ has a factorization of length } k\} \subset \mathbb{N}$ is the set of lengths of a.

For $k \in \mathbb{N}$, let $\rho_k(H)$ denote the supremum over all $\ell \in \mathbb{N}$ such that there is an equation $u_1 \cdot \ldots \cdot u_k = v_1 \cdot \ldots \cdot v_\ell$, with u_i, v_j irreducible. Equivalently,

$$\rho_k(H) = \sup\{\sup \mathsf{L}(a) \mid a \in H, k \in \mathsf{L}(a)\} \in \mathbb{N}_{\geq k} \cup \{\infty\}\,.$$

Carlitz (1960): For a ring of integers R there are equivalent:

- $\rho_k(R) = k$ for all $k \geq 2$.
- $|G| \leq 2$.

Blocks and Zero-Sum Sequences: The 1960s and 1970s

Let G be an additive abelian group and $G_0 \subset G$ a subset.
A sequence $S = g_1 \cdot \ldots \cdot g_l$ of group elements from G_0 is called a zero-sum sequence (or a block) if $g_1 + \ldots + g_l = 0$.
The set $\mathcal{B}(G_0)$ of zero-sum sequences over G_0 is a monoid with concatenation as operation. The Davenport constant $\mathsf{D}(G_0)$ is the maximal length of a minimal zero-sum sequence over G_0.

- K. Rogers (1962): If R is a ring of integers, then $\mathsf{D}(\mathcal{C}(R))$ is the maximal number of prime ideals occurring in the prime ideal decomposition of aR for an irreducible element $a \in R$.
- H. Davenport (1965): Midwestern Conference on Group Theory and Number Theory: Study $\mathsf{D}(G)$.
- W. Narkiewicz (1979): *Finite abelian groups and factorization problems*:
  Study the monoid $\mathcal{B}(G)$ instead of the ring of integers R !

Studies on $\rho_k(R)$: The 1980s

For small values of k and small class groups, a study of $\rho_k(R)$ was started by

- A. Czogała (1981): *Arithmetic characterization of algebraic number fields with small class number*
- L. Salce and P. Zanardo (1982): *Arithmetical characterization of rings of algebraic integers with cyclic ideal class group*
- F. Di Franco and F. Pace (1985)
- K. Feng (1985)

  continued later by

- S.T. Chapman, W.W. Smith, and others

Outline

Conference and Special Session
on
Factorization in Integral Domains,
in
Iowa City (1996)
organized by
Daniel D. Anderson

F. Halter-Koch:

Finitely Generated Monoids, Finitely Primary Monoids, and Factorization Properties of Integral Domains

Transfer Homomorphisms

Definition (Transfer Homomorphism)

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:

- $\mathsf{L}_H(a) = \mathsf{L}_B\big(\theta(a)\big)$ *for all $a \in H$.*

  Thus transfer homomorphisms preserve sets of lengths.
- *In particular, $\rho_k(H) = \rho_k(B)$ for all $k \geq 2$.*

Strategy for studying the arithmetic

In order to study the arithmetic (e.g, the invariants $\rho_k(H)$) of a domain or monoid H,

Proceed as follows:

- Study the ideal theory of H.
- Construct a transfer homomorphism $\theta \colon H \to B$.
- Study the arithmetic of B (e.g., study $\rho_k(B)$).

Then

$$\rho_k(H) = \rho_k(B) \quad \text{for all} \quad k \ge 2\,.$$

Outline

Krull monoids: Definition

A monoid H is a Krull monoid if one of the equiv. statements hold:

(a) H is completely integrally closed and v-noetherian.

(b) There is a divisor homomorphism $\varphi\colon H \to F = \mathcal{F}(P)$
(For all $a, b \in H$: $a \mid b$ in $H \iff \varphi(a) \mid \varphi(b)$ in F)

(c) There is a divisor theory $\varphi\colon H \to F = \mathcal{F}(P)$

- For (a): Choinard (1981), P.Wauters (1984): noncommutative
- For (c): Borevic-Safarevic, L. Skula (1970), Gundlach (1972)
- If (a) holds, then $\mathcal{I}_v^*(H)$ is free abelian with basis $\mathfrak{X}(H)$.
- (a) $\iff$ (c): F. Halter-Koch (1990):
  Halbgruppen mit Divisorentheorie

Krull monoids: Examples

- Krause (1990): A domain R is Krull iff $R^\bullet$ is Krull.
- Halter-Koch (1993): Analogue for rings with zero-divisors.
- Halter-Koch: Regular congruence submonoids of Krull domains
- Frisch, Reinhart: Monadic submonoids of $\mathrm{Int}(R)$, R Krull.
- Wiegand, Herbera, Facchini ($\sim$ 2000): Monoids of modules
  If $\mathcal{C}$ is a nice class of modules, then $\mathcal{V}(\mathcal{C}) = \{[M] \mid M \in \mathcal{C}\}$ is Krull (operation stems from the direct sum decomposition)
- Monoids $\mathcal{B}(G_0)$ of zero-sum sequences over G_0:
  If G_0 is a subset of an additive abelian group G,
  then the embedding

$$\mathcal{B}(G_0) \hookrightarrow \mathcal{F}(G_0)$$

  is a divisor homomorphism, and hence $\mathcal{B}(G_0)$ is Krull.

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

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

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

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

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

such that

- a is irreducible in H if and only if S is irreducible in $\mathcal{B}(G_P)$.
- $\mathsf{L}_H(a) = \mathsf{L}_{\mathcal{B}(G_P)}(S)$.
- In particular, $\rho_k(H) = \rho_k\big(\mathcal{B}(G_P)\big) =: \rho_k(G_P)$ for all $k \geq 2$.

First Results

Let G be an abelian group.

- If $G_0 \subset G$ is finite, then $\mathcal{B}(G_0)$ is finitely generated whence

$$\rho_k(H) = \rho_k(G_0) < \infty \quad \text{for all } k \ge 2\,.$$

- Carlitz (1960): If $|G| \le 2$, then $\rho_k(G) = k$ for all $k \ge 2$.
- If G is infinite, then $\rho_k(G) = \infty$ for all $k \ge 2$.
- If $2 < |G| < \infty$, then
  - $\rho_{2k}(G) = k\mathsf{D}(G)$ for all $k \ge 2$.
  - $k\mathsf{D}(G) + 1 \le \rho_{2k+1}(G) \le k\mathsf{D}(G) + \mathsf{D}(G)/2$.
  - Problem 38 in S.T. Chapman and S. Glaz *Non-Noetherian Commutative Ring Theory* (2000):

$$\text{Do we have} \quad k\mathsf{D}(G) + 1 = \rho_{2k+1}(G) \quad \text{for cyclic groups ?}$$

A Result involving Additive Number Theory

Theorem (Savchev-Chen, 2007)

Let G be a cyclic group of order $|G| = n$.
Let $U \in \mathcal{B}(G)$ be a minimal zero-sum sequence of length $l \geq \lfloor \frac{n}{2} \rfloor + 2$. Then there is some $g \in G$ with $G = \langle g \rangle$ such that, with $1 = n_1 \leq n_2 \leq \ldots \leq n_l$,

$$S = (n_1 g)(n_2 g) \cdot \ldots \cdot (n_l g) \quad \text{and} \quad n_1 + \ldots + n_l = n \,.$$

Theorem (Gao+G., 2009)

Let H be a Krull monoid with cyclic class group G such that each class contains a prime divisor. Then for every $k \in \mathbb{N}$, we have

$$\rho_{2k+1}(H) = \rho_{2k+1}(G) = k\mathsf{D}(G) + 1 \,.$$

Outline

Weakly Krull monoids and domains

A monoid H is weakly Krull if

$$H = \bigcap_{\mathfrak{p} \in \mathfrak{X}(H)} H_{\mathfrak{p}} \quad \text{and} \quad \{\mathfrak{p} \in \mathfrak{X}(H) \mid a \in \mathfrak{p}\} \quad \text{is finite for all } a \in H \,,$$

Weakly Krull domains: D.D. Anderson, Mott, Zafrullah (1992)
Weakly Krull monoids: F. Halter-Koch (1995)

- A domain R is weakly Krull iff $R^\bullet$ is a weakly Krull monoid.
- H v-noetherian: H weakly Krull $\iff$ $v\text{-max}(H) = \mathfrak{X}(H)$.

Examples:

- 1-dim. noeth. domains R s.t. $\overline{R}$ is a f.g. R-module
- In particular: Non-principal orders in algebraic number fields

Main Result

F. Halter-Koch:

- *Elasticity of factorizations in atomic monoids and integral domains* (1995)
- *Finitely generated monoids, finitely primary monoids and factorization properties of integral domains* (1997)

Theorem

Let H be a weakly Krull monoid that the class group $G = \mathcal{C}(H)$ is finite and each class contains a $\mathfrak{p} \in \mathfrak{X}(H)$ with $\mathfrak{p} \not\supset \mathfrak{f} = (H : \widehat{H})$. Then the following statements are equivalent:

(a) $\rho_k(H) < \infty$ *for all* $k \in \mathbb{N}$.

(b) *The natural map* $\mathfrak{X}(\widehat{H}) \to \mathfrak{X}(H)$, $\mathfrak{P} \mapsto \mathfrak{P} \cap H$, *is bijective.*

Transfer Homomorphisms

Consider

$$\begin{array}{ccc} H & \longrightarrow & D = \mathcal{F}(P) \times T \cong \mathcal{I}_v^*(H) \\ \beta \big\downarrow & & \widetilde{\beta} \big\downarrow \\ B = \mathcal{B}(G, T, \iota) & \longrightarrow & F = \mathcal{F}(G) \times T \end{array}$$

where

- $T = \prod_{\mathfrak{p} \in \mathcal{P}^*} (H_\mathfrak{p})_{\mathrm{red}}$ and $\mathcal{P}^* = \{\mathfrak{p} \in \mathfrak{X}(H) \mid \mathfrak{p} \supset \mathfrak{f}\}$.
- $\iota \colon T \to G$ is defined by $\iota(t) = [t]$.
- $\widetilde{\beta} \colon D \to F$ be the unique homomorphism satisfying $\widetilde{\beta}(p) = [p]$ for all $p \in P$ and $\widetilde{\beta} \mid T = \mathrm{id}_T$.

Then

- B is weakly Krull again, and
- $\beta = \widetilde{\beta} \mid H$ is a transfer homomorphism.

Combinatorial weakly Krull monoids: $\mathcal{B}(G, T, \iota)$

Let G be a finite abelian group and $T = D_1 \times \ldots \times D_n$ a monoid. Let

- $\iota \colon T \to G$ a homomorphism, and
- $\sigma \colon \mathcal{F}(G) \to G$ satisfying $\sigma(g) = g$.

Then

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

the T-block monoid over G defined by ι.

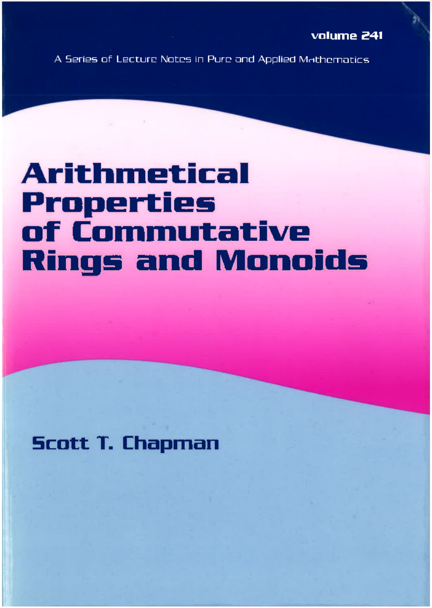
Special Cases:

- If $G = \{0\}$, then $\mathcal{B}(G, T, \iota) = T = D_1 \times \ldots \times D_n$ is a finite product of finitely primary monoids.
- If $T = \{1\}$, then

$$\mathcal{B}(G, T, \iota) = \mathcal{B}(G) = \{S \in \mathcal{F}(G) \mid \sigma(S) = 0\} \subset \mathcal{F}(G)$$

is the monoid of zero-sum sequences over G.

Outline



Conference and Special Session
on
Factorization Properties of
Commutative Rings and Monoids,
in
Chapel Hill (2003)
organized by
Scott T. Chapman

F. Halter-Koch:
C-monoids and congruence monoids in Krull domains

Definition and Examples

A monoid H is called a C-monoid if it is a submonoid of a factorial monoid F such that

$$H \cap F^\times = H^\times \quad \text{and the class semigroup} \quad \mathcal{C}^*(H,F) \quad \text{is finite.}$$

Examples:

1. Let R be a Mori domain such that $\mathfrak{f} = (R : \widehat{R}) \neq \{0\}$.
   (a) If $\mathcal{C}(\widehat{R})$ and $\widehat{R}/\mathfrak{f}$ are finite, then R is a C-monoid.
   (b) In special cases the converse holds (Reinhart)
   (c) There is an analogue to (a) in Mori rings with zero-divisors
2. Many congruence monoids, in particular arithmetical congruence monoids as studied by Chapman, Baginski et al.

C-Monoids: Comments and Strategy

Let H be a Mori monoid such that $\mathfrak{f} = (H : \widehat{H}) \neq \{0\}$.

- $\widehat{H}$ is Krull, $\mathcal{I}_v^*(\widehat{H})$ is free abelian with (infinite) basis $v\text{-spec}(\widehat{H}) = \mathfrak{X}(\widehat{H})$, and we have a map $\varphi \colon H \to \mathcal{I}_v^*(\widehat{H})$.
- Thus there is a factorial monoid $F = F^\times \times \mathcal{F}(P)$ with (**infinite**) basis P such that $H \subset F$.
- The finiteness of the class semigroup $\mathcal{C}^*(H, F)$ allows to construct a transfer homomorphism $\theta \colon H \to B$

$$\begin{array}{ccc} H & \longrightarrow & F = F^\times \times \mathcal{F}(P) \\ \theta \big\downarrow & & \big\downarrow \\ B & \longrightarrow & F_0 = F_0^\times \times \mathcal{F}(P_0) \end{array}$$

where B is a C-monoid again and P_0 is **finite**.

Main Arithmetical Result for C-Monoids

Studying the C-monoid B and using that $\rho_k(B) = \rho_k(H)$ we obtain

Theorem

Let H be a C-monoid.
Then the following statements are equivalent:

(a) $\rho_k(H) < \infty$ *for all* $k \in \mathbb{N}$.

(b) *H is simple*
(i.e., each minimal H-essential subset of P is a singleton).

Outline

Weak Transfer Homomorphisms

D. Smertnig (2013): *Sets of lengths in maximal orders in central simple algebras*

N. Baeth et al. (2014): *Factorization of upper triangular matrices*

N. Baeth and D. Smertnig: *Factorization Theory in Non-Commutative Settings*

Definition

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

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

(WT 2) If $a \in H$ and $b_1, \ldots, b_n$ are atoms in B such that $\theta(a) = b_1 \cdot \ldots \cdot b_n$, then there exist atoms $a_1, \ldots, a_n \in H$ and a permutation $\sigma \in \mathfrak{S}_n$ such that $a = a_1 \cdot \ldots \cdot a_n$ and $\theta(a_i) = b_{\sigma(i)}$ for each $i \in [1, n]$.

Transfer and Weak Transfer Homomorphisms

Facts:

- Each transfer homomorphism is a weak transfer homomorphism but not conversely.
- Weak transfer homomorphisms respect sets of lengths.

Theorem (N. Baeth et al., 2014)

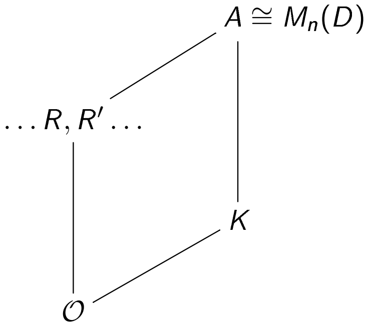
Let R be a commutative BF-domain and $T_n(R)$ the semigroup of upper triangular matrices with nonzero determinant.

1. $\det\colon T_n(R) \to R^\bullet$ *is a transfer homomorphism if and only if R is a principal ideal domain.*
2. *There is a weak transfer hom.* $\theta\colon T_n(R) \to R^\bullet \times \ldots \times R^\bullet$.
3. *Under a weak assumption on R there is no transfer homomorphism from $T_2(R)$ to any commutative semigroup.*

Classical Maximal Orders: D. Smertnig (2013)

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).



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 $\mathcal{O}$.

Summary

Based on a solid understanding of the respective ideal theories
transfer homomorphisms
provide a strategy for studying the arithmetic of

- Dedekind domains including rings of integers in number fields
- Krull domains including integrally closed noetherian domains
- Weakly Krull domains including 1-dimensional noetherian domains
- C-domains including higher-dimensional noetherian domains R where $R/\mathfrak{f}$ and $\mathcal{C}(\widehat{R})$ are finite
- Maximal orders in central simple algebras over global fields (these are non-commutative Dedekind prime rings)
- much much more .... going to come ....