Non-unique factorizations in bounded hereditary noetherian prime rings

Daniel Smertnig

University of Waterloo

Conference on Rings and Factorizations
Graz, Feb 21, 2018

UNIVERSITY OF WATERLOO

FWF Der Wissenschaftsfonds.

Outline

- Factorizations in noncommutative rings
- Non-unique factorizations
- Bounded hereditary noetherian prime (HNP) rings
- Beyond bounded HNP rings

Factorizations

R (unital) ring, $H = R^\bullet$ its monoid of non-zero-divisors.

Assume: $R^\bullet$ is divisor-closed in R.

- A non-unit $u \in H$ is an **atom** if

$$u = ab \text{ with } a,\ b \in H \ \Rightarrow\ a \in H^\times \text{ or } b \in H^\times.$$

- $\mathcal{A}(H)$ ... set of all atoms.

Definition

H is **atomic** if for every $a \in H \setminus H^\times$, there exist atoms $u_1, \ldots, u_k$, such that

$$a = u_1 \cdots u_k.$$

Factorizations

Question

What is a factorization, precisely?

First attempt: an element of $\mathcal{F}^*(\mathcal{A}(H))$ ... free monoid on atoms.

Two problems:

1. In H, we have $uv = (u\varepsilon)(\varepsilon^{-1}v)$ for $\varepsilon \in H^\times$
2. Units should have a trivial factorization.

Note: Cannot reduce $H/H^\times$ in general.

Factorizations

On $H^\times \times \mathcal{F}^*(\mathcal{A}(H))$ define $(\varepsilon, u_1 * \cdots * u_k) \sim (\eta, v_1 * \cdots * v_l)$ if

1. $\varepsilon u_1 \cdots u_k = \eta v_1 \cdots v_l$ in H,
2. $k = l$, and
3. there exist $\delta_i \in H^\times$ s.t.

$$\varepsilon u_1 = \eta v_1 \delta_1, \quad u_i = \delta_{i-1}^{-1} v_i \delta_i, \quad u_k = \delta_{k-1}^{-1} v_k.$$

Definition

$\mathsf{Z}^*(H) = \big(H^\times \times \mathcal{F}^*(\mathcal{A}(H))\big)/\sim$ is the **monoid of (rigid) factorizations**.

- There is a homomorphism $\pi\colon \mathsf{Z}^*(H) \to H$
- $\mathsf{Z}^*(a) = \pi^{-1}(\{a\})$ is the set of **(rigid) factorizations of** a.

Factor posets

The **Factor poset** is

$$[aR, R] = \{bR \mid b \in R^\bullet,\ aR \subseteq bR \subseteq R\}$$

Then

$$\mathsf{Z}^*(a) \quad \longleftrightarrow \quad \textbf{maximal}, \textbf{ finite} \text{ chains in } [aR, R].$$

$u_1 * \cdots * u_k$ corresponds to

$$R \supsetneq u_1 R \supsetneq u_1 u_2 R \supsetneq \cdots \supsetneq u_1 \cdots u_k R = aR.$$

ACCP $\Rightarrow$ atomic

By taking cofactors, ACC on the left implies DCC on $[aR, R]$!

Lemma

If R satisfies ACCP, that is ACC on principal left and right ideals, then $R^\bullet$ is atomic.

Note: ACC on one side is not sufficient.

Similiarity factoriality

Question

What should it mean for R to be factorial?

Suppose R is atomic, and if $bR, cR \in [aR, R]$ then $bR + cR$ and $bR \cap cR$ are principal (e.g., R a PID).

$\Rightarrow [aR, R]$ is a finite length modular lattice

$\Rightarrow$ If $u_1 * \cdots * u_k$, $v_1 * \cdots * v_l \in \mathsf{Z}^*(a)$, then

- $k = l$, and
- there exists a permutation σ s.t. $R/u_iR \cong R/v_{\sigma(i)}R$.

We say R is **similarity factorial**.

Limitations...

Remark

- $[aR, R]$ need not be distributive, e.g., $R = M_2(\mathbb{Z})$.
- $K\langle x, y\rangle$ has distributive factor lattices, but all finite distributive lattices appear as factor lattices.
- $\mathbb{Z}\langle x, y\rangle$ is not similarity factorial (but subsimilarity factorial).
- Let $\mathbb{H}$ be the $\mathbb{Q}$-division algebra of Hamilton quaternions. Then $\mathbb{H}[x]$ is Euclidean ($\Rightarrow$ PID), but $\mathbb{H}[x, y]$ is not half-factorial!

Non-unique factorizations

Arithmetical Invariants

Definition

Let $a \in R^\bullet$. The **set of lengths** of a is

$$\begin{aligned}\mathsf{L}(a) &= \{\, |z| \mid z \in \mathsf{Z}^*(a) \,\} \\ &= \{\, k \in \mathbb{N}_0 \mid a = u_1 \cdots u_k \text{ with } u_1, \ldots, u_k \in R^\bullet \text{ atoms} \,\}.\end{aligned}$$

System of sets of lengths: $\mathcal{L}(R) = \{\, \mathsf{L}(a) \mid a \in R^\bullet \,\}$.

- R is **half-factorial** if $|\mathsf{L}(a)| = 1$ for all $a \in R^\bullet$.
- $|\mathsf{L}(a)| \geq 2 \quad \Rightarrow \quad |\mathsf{L}(a^n)| \geq n + 1$.
- **Elasticity**:

$$\begin{aligned}\rho(a) &= \frac{\sup \mathsf{L}(a)}{\min \mathsf{L}(a)} \in \mathbb{Q}_{\geq 1} \cup \{\infty\}, \\ \rho(R) &= \sup\{\, \rho(a) \mid a \in R^\bullet \,\} \in \mathbb{R}_{\geq 1} \cup \{\infty\}.\end{aligned}$$

Distances

Let $D = \{ (z, z') \in \mathsf{Z}^*(H) \times \mathsf{Z}^*(H) : \pi(z) = \pi(z') \}$.

Definition

A **distance on** $R^\bullet$ is a map $\mathsf{d}\colon D \to \mathbb{N}_0$ s.t.

1. $\mathsf{d}(z, z) = 0$
2. $\mathsf{d}(z, z') = \mathsf{d}(z', z)$
3. $\mathsf{d}(z, z') \le \mathsf{d}(z, z'') + \mathsf{d}(z'', z')$
4. $\mathsf{d}(x * z, x * z') = \mathsf{d}(z, z') = \mathsf{d}(z * x, z' * x)$
5. $||z| - |z'|| \le \mathsf{d}(z, z') \le \max\{|z|, |z'|, 1\}$.

E.g. $\mathsf{d}_{\mathsf{sim}}$, compare factors up to similarity, ...

Catenary degrees

Fix a distance d; let z, $z' \in \mathsf{Z}^*(a)$.
An N-**chain** is a sequence $z = z_0, z_1, \ldots, z_l = z'$ in $\mathsf{Z}^*(a)$, such that

$$\mathsf{d}(z_{i-1}, z_i) \le N \quad \text{for } i \in [1, l].$$

Definition

The **catenary degree** $\mathsf{c}_\mathsf{d}(a)$ is the smallest N such that for all z, $z' \in \mathsf{Z}^*(a)$, there exists an N-chain between z and z'.

$$\mathsf{c}_\mathsf{d}(H) = \sup\{\, \mathsf{c}_\mathsf{d}(a) \mid a \in H \,\}.$$

Transfer homomorphisms

Definition

Let H, T be cancellative monoids, $T^\times = \{1\}$. A homomorphism $\theta\colon H \to T$ is a **transfer homomorphism** if

1. $\theta(H) = T$ and $\theta^{-1}(\{1\}) = H^\times$.
2. Whenever $\theta(a) = st$, there exist b, $c \in H$ such that

$$a = bc, \quad \theta(b) = s, \quad \text{and} \quad \theta(c) = t.$$

Transfer homomorphisms

Theorem

If $\theta\colon H \to T$ is a transfer homomorphism, it induces a homomorphism θ^*,

$$\begin{array}{ccc} \mathsf{Z}^*(H) & \xrightarrow{\theta^*} & \mathsf{Z}^*(T) \\ \downarrow & & \downarrow \\ H & \xrightarrow{\theta} & T, \end{array}$$

with $\theta^*(\mathsf{Z}^*(a)) = \mathsf{Z}^*(\theta(a))$.

- $\mathcal{L}(H) = \mathcal{L}(T)$.
- If T is commutative

$$\mathsf{c}_{\mathsf{d}}(H) \le \max\{\mathsf{c}_p(T), \mathsf{c}(\theta)\}.$$

Monoid of zero-sum sequences

Let $(G, +)$ be an abelian group, $G_0 \subseteq G$, $(\mathcal{F}(G_0), \cdot)$ the free abelian monoid with basis G_0.

- $S = g_1 \cdots g_l \in \mathcal{F}(G_0)$ is called a **sequence** (formal product!).
- $\sigma(S) = g_1 + \cdots + g_l \in G$ is its sum.
- S is a **zero-sum sequence** if $\sigma(S) = 0$.

Definition

The submonoid

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

is the **monoid of zero-sum sequences** over G_0.

If G_0 is finite, then $\mathcal{B}(G_0)$ is a finitely generated Krull monoid (finitely many atoms, arithmetical invariants finite, ...)

Reminder: Commutative Dedekind domains

Theorem

Let R be a commutative Dedekind domain, $(G, +)$ its class group,

$$G_0 = \{\, [\mathfrak{p}] \mid \mathfrak{p} \in \operatorname{spec}(R) \,\}.$$

There is a transfer homomorphism $\theta\colon R^\bullet \to \mathcal{B}(G_0)$:

$$\begin{array}{ccccc}
a & \longmapsto & aR & & \\
R^\bullet & \longrightarrow & \mathcal{F}(\operatorname{spec}(R)) & & \mathfrak{p}_1 \cdots \mathfrak{p}_r \\
\downarrow \theta & & \downarrow & & \downarrow \\
\mathcal{B}(G_0) & \hookrightarrow & \mathcal{F}(G_0) & & [\mathfrak{p}_1] \cdots [\mathfrak{p}_r]
\end{array}$$

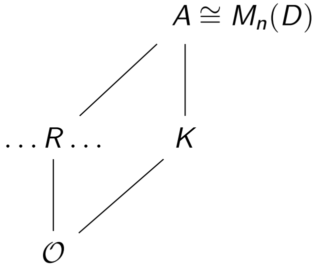
Moreover, $\mathsf{c}(\theta) \le 2$.

Hereditary noetherian prime (HNP) rings

Hereditary orders

Let

- K be a number field,
- $\mathcal{O}$ its ring of algebraic integers,
- A a central simple K-algebra,
- $\mathcal{O} \subset R \subset A$ an order in A (subring, $R_{\mathcal{O}}$ finitely generated, $KR = A$).



Definition

- R is a **maximal order** if it is not contained in a strictly larger order.
- Maximal orders are **hereditary** (right ideals are projective).

Examples...

- Hurwitz quaternions

$$\mathbb{Z}\left[1, i, j, \frac{1+i+j+k}{2}\right]$$

with $i^2 = j^2 = k^2 = -1$, $ij = -ji = k$.

- With p a prime,

$$\begin{bmatrix} \mathbb{Z} & p\mathbb{Z} \\ \mathbb{Z} & \mathbb{Z} \end{bmatrix}.$$

HNP rings

- (Noncommutative) **hereditary noetherian prime (HNP) rings** are analogues of commutative Dedekind domains.
- Structure theory for f. g. projective modules and for finite-length modules (Levy–Robson 2011).
- Examples:
  - Hereditary orders over commutative Dedekind domains.
  - Endomorphism rings of f. g. projective modules over Dedekind domains.
  - Some skew polynomial rings over commutative Dedekind domains, e.g.,

$$A = A_1(K) = K[y][x; \tfrac{d}{dy}], \quad K[x^{\pm 1}][y^{\pm 1}; \sigma] \text{ with } yx = qxy.$$

- R is **right bounded**, if for every $a \in R^\bullet$, there exists a nonzero ideal $I \subseteq R$ with $I \subseteq aR$.

From factor lattices to modules

$$Z^*(a) \longleftrightarrow [aR, R] \longleftrightarrow ?\ R/aR.$$

How to go from R/aR back to $[aR, R]$?
Commutative: $\mathrm{ann}(R/I) = I$; if R is a Dedekind domain:

$$R/\prod_{i=1}^{r} \mathfrak{p}_i^{e_i} \cong \bigoplus_{i=1}^{r} R/\mathfrak{p}_i^{e_i}.$$

Noncommutative: $R/aR \cong R/I \Rightarrow$?

$$\begin{array}{ccccccccc} 0 & \longrightarrow & I & \longrightarrow & R & \longrightarrow & R/aR & \longrightarrow & 0 \\ & & & & \| & & \| & & \\ 0 & \longrightarrow & aR & \longrightarrow & R & \longrightarrow & R/aR & \longrightarrow & 0 \end{array}$$

$\Rightarrow I \oplus R \cong aR \oplus R.$ I is **stably free**.

Problem!

There can be non-principal, stably free right ideals I.

Hermite rings

Definition

R is a **(right) Hermite ring** if every stably free right R-module is free.

- Commutative Dedekind domains are Hermite.
- HNP rings R with $\operatorname{udim} R \geq 2$ are Hermite.
- Indefinite hereditary orders over rings of algebraic integers are Hermite (by **strong approximation**).
- Definite (quaternion) orders over rings of algebraic integers are **usually not** Hermite.
- $A_1(K)$ is not Hermite.

Modules over HNP rings

Let V, W be simple modules.

Definition

W is a **successor** of V if $\mathrm{Ext}^1_R(V, W) \neq 0$.

Isomorphism classes of simple modules are organized into **cycle towers** and **faithful towers**.

$W_1, \ldots, W_n$ pairwise non-isomorphic simple modules.

- **Cycle tower**: All W_i are unfaithful. W_{i+1} is a successor of W_i, and W_1 is a successor of W_n.
- **Faithful tower**: W_1 is faithful, $W_2, \ldots, W_n$ are unfaithful. W_i is a successor of W_{i-1}, and W_n has no unfaithful successor.

In a bounded HNP ring, all simple modules are unfaithful.

Modules over HNP rings

If $a \in R^\bullet$, then R/aR has finite length.

If R is bounded, every finite length module M is a direct sum of **uniserial** modules,

$$M \cong U_1 \oplus \cdots \oplus U_n.$$

The composition factors of U_i form a slice of a repetition of the modules of a cycle tower T.

A class group

$\mathcal{S}(R)$ ... isomorphism classes of simple modules.

$\mathcal{T}(R) \subset \mathcal{F}(\mathcal{S}(R))$ ... towers (as sums of their simple modules),

$$K_0 \operatorname{\mathbf{mod}}_{\mathrm{fl}}(R) = \mathbf{q}\mathcal{F}(\mathcal{S}(R)) \supseteq \mathbf{q}\mathcal{F}(\mathcal{T}(R))$$

For M a module of finite length with composition factors W_1, $\ldots$, W_n, have

$$(M) = (W_1) + \cdots + (W_n) \in \mathcal{F}(\mathcal{S}(R)).$$

Proposition

If $a \in R^\bullet$, then $(R/aR) \in \mathcal{F}(\mathcal{T}(R))$

A class group

Set $\mathcal{P}(R) = \{\, (R/aR) \mid a \in R^{\bullet} \,\} \subseteq \mathcal{F}(\mathcal{T}(R))$.

Definition

The **class group** of R is

$$\mathcal{C}(R) = \mathbf{q}\mathcal{F}(\mathcal{T}(R)) \,/\, \langle \mathcal{P}(R) \rangle.$$

Set $\mathcal{C}_{\mathsf{max}}(R) = \{\, [T] \in \mathcal{C}(R) \mid T \in \mathcal{T}(R) \,\}$.

- $\mathcal{C}(R) \cong G(R) = \ker(\Psi^{+})$.
- $\mathcal{C}(R)$ and $\mathcal{C}_{\mathsf{max}}(R)$ are Morita invariant.

Main result for HNP rings

Theorem

Let R be a bounded HNP ring. Suppose R is a Hermite ring.

- $\mathcal{P}(R) = \{ (R/aR) \mid a \in R^\bullet \}$ is a commutative Krull monoid, and $\mathcal{P}(R) \to \mathcal{F}(\mathcal{T}(R))$ is a cofinal divisor homomorphism.
- There exists a transfer homomorphism

$$\theta\colon R^\bullet \to \mathcal{P}(R),$$

  and a transfer homomorphism to the monoid of zero-sum sequences

$$\overline{\theta}\colon R^\bullet \to \mathcal{B}(\mathcal{C}_{\mathsf{max}}(R)).$$

- $\mathsf{c_d}(\theta) \le 2$ and $\mathsf{c_d}(\overline{\theta}) \le 2$.

Hereditary orders

Theorem

Let R be a hereditary order over a ring of algebraic integers $\mathcal{O}$. Then $\mathcal{C}(R) \cong \mathcal{C}_A(\mathcal{O})$ is a ray class group of $\mathcal{O}$, hence finite, and $\mathcal{C}_{\max}(R) = \mathcal{C}(R)$.

1. If R is a Hermite ring, there exists a transfer homomorphism to $\mathcal{B}(\mathcal{C}_A(\mathcal{O}))$, all arithmetical invariants are finite.
2. If R is maximal and **not** Hermite, then $\rho(R^\bullet) = \infty$, $\Delta(R^\bullet) = \mathbb{N}$, ...

Remark

(1) is the usual case; (2) only happens in definite quaternion algebras.

A corollary

Corollary

Let R be a bounded Hermite HNP ring. Suppose further that $\mathcal{C}_{\mathsf{max}}(R) = \mathcal{C}(R)$, and that, if $\mathcal{C}(R) \cong \mathsf{C}_2$, there exist at least two distinct towers T_1 and T_2 with $\langle T_1 \rangle = \langle T_2 \rangle \neq \mathbf{0}$. Then

1. *$R^\bullet$ is composition series factorial if and only if $\mathcal{C}(R) = \mathbf{0}$. Otherwise, $\mathsf{c}_{\mathsf{cs}}(R^\bullet) \geq 2$.*
2. *$R^\bullet$ is similarity factorial if and only if R is a principal ideal ring. Otherwise, $\mathsf{c}_{\mathsf{sim}}(R^\bullet) \geq 2$.*
3. *$R^\bullet$ is rigidly factorial if and only if R is a local principal ideal ring. Otherwise, $\mathsf{c}^*(R^\bullet) \geq 2$.*

Beyond boundedness: The Weyl algebra

Let K be a field, $\mathrm{char}(K) = 0$,

$$A = K[y][x; \tfrac{d}{dy}] = K\langle x, y\rangle / \langle xy - yx - 1\rangle.$$

A is ....

- a simple HNP ring, all towers are trivial, $\mathcal{C}(A) = 0$
- **not** Hermite.
- not half-factorial,
$$x^2 y = (1 + xy)x$$
$\Rightarrow \; \rho(A^\bullet) \geq 3/2$, in fact $\rho(A^\bullet) = \infty$.
- $M_2(A)$ is a prime PIR, in particular Hermite, similarity factorial.

$$\begin{bmatrix} 1+xy & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} x^2 & 1+xy \\ x & y \end{bmatrix} \begin{bmatrix} -y^2 & y \\ xy+1 & -x \end{bmatrix}.$$

Beyond boundedness

We can still rescue the conclusions of the main theorem as long as

- faithful towers are trivial,
- $\mathrm{Ext}^1_R(V, W) = 0$ if V, W are faithful simple modules in different classes of $\mathcal{C}(R)$.

Let $R = \mathbf{I}_A(xA) = K + xA$ be the idealizer of the maximal right A-ideal xA.

- R has a single faithful tower of length 2: A/R, R/xA.
- $\mathcal{C}(R) = 0$, all other towers of R are trivial & faithful.
- Same is true for $M_2(R)$ and it is Hermite, but not half-factorial.

For

$$a = \begin{bmatrix} x(x-y)(x-yx) & x(x-y)(-xy+xy^2) \\ x^2-(1+xy)x & (1+xy)(1-x)+x^2y^2 \end{bmatrix}$$

we have

$$a = \underbrace{\begin{bmatrix} x(x-y) & 0 \\ 0 & 1 \end{bmatrix}}_{u_1} \underbrace{\begin{bmatrix} x-yx & -xy+xy^2 \\ x^2-(1+xy)x & (1+xy)(1-x)+x^2y^2 \end{bmatrix}}_{u_2}$$

$$= \underbrace{\begin{bmatrix} x & xy \\ x & 1+xy \end{bmatrix}}_{w_1} \underbrace{\begin{bmatrix} -xy^2+x^2y-xy-x+1 & -xy^3+x^2y^2-xy^2-xy \\ xy-x^2+x & xy^2-x^2y+xy+1 \end{bmatrix}}_{w_2} \underbrace{\begin{bmatrix} x & -xy \\ -x & 1+xy \end{bmatrix}}_{w_3}$$

Non-hereditary orders

Non-uniqueness of factorizations in orders due to: non-trivial class group, non-Hermite, local obstructions.

Theorem

Let K be the quotient field of a DVR, let A be a quaternion algebra over K, and let R be a ***non-hereditary*** *order in A. Then*

$$\rho(R^\bullet) < \infty \quad \Longleftrightarrow \quad \widehat{A} \text{ is a division ring.}$$