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

UNI GRAZ

Sets of lengths in maximal orders in central simple algebras

Daniel Smertnig

Institute of Mathematics and Scientific Computing
University of Graz, Austria

Noncommutative rings and their applications III
Lens, July 2nd, 2013

What is this about?

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.

$$\begin{tikzcd}
 & A \cong M_n(D) \arrow[dd, dash] \\
R \arrow[ur, dash] \arrow[dd, dash] & \\
 & K \\
\mathcal{O} \arrow[ur, dash] &
\end{tikzcd}$$

Investigate factorizations of elements in R:

- Every $a \in R^\bullet \setminus R^\times$ can be represented as a finite product of atoms (irreducibles).
- In general, this is far from being unique.
- $\Rightarrow$ Study non-uniqueness of factorizations by means of arithmetical invariants.

Outline

1. Recall: Non-unique factorizations in commutative Krull domains [monoids].

2. Main results for maximal orders.

3. Abstract setting for these results and some sketch of their proof.

Non-unique factorizations

Consider factorizations of elements into atoms.

Goals

Use arithmetical invariants to

- describe the extent of non-uniqueness,
- describe features occuring as part of this non-uniqueness,
- and possible characterize rings [monoids] inside a class by their arithmetic.

Has a rich history and well-developed theory & machinery in the commutative setting: In particular in Krull domains [monoids].

(Commutative) Krull domains

Definition

A *Krull monoid* is a commutative, cancellative monoid H that is

1. completely integrally closed, and
2. v-noetherian.

Equivalently, it is a saturated submonoid of a factorial monoid.

- A commutative domain R is a Krull domain $\Leftrightarrow$ $R^\bullet$ is a Krull monoid.
- $\mathcal{I}_v^*(R)$ is a free abelian monoid on the (non-zero) divisorial prime ideals.
- $R_{\mathrm{red}}^\bullet = \{aR \mid a \in R^\bullet\} \subset \mathcal{I}_v^*(R)$ is a saturated submonoid.

Idea

Study factorizations of $a \in R^\bullet$ using the unique factorization of aR into divisorial prime ideals in $\mathcal{I}_v^*(R)$.

Monoid of zero-sum sequences, I

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

- $S = g_1 \cdot \ldots \cdot g_l \in \mathcal{F}(G_0)$ is called a **sequence**.
- $\sigma(S) = g_1 + \ldots + g_l \in G$ 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 called the **monoid of zero-sum sequences** over G_0.

- $\mathcal{B}(G)$ is a Krull monoid with divisor class group G, and every class contains a prime divisor.
- If G_0 is finite, then $\mathcal{B}(G_0)$ is a finitely generated Krull monoid (finitely many atoms, arithmetical invariants finite, ...)

Some arithmetical invariants

Let $a \in R^\bullet \setminus R^\times$.

- $l \in \mathbb{N}$ is a **length** of a if there exist atoms $u_1, \ldots, u_l$ s.t.:

$$a = u_1 \cdot \ldots \cdot u_l.$$

- $\mathsf{L}(a) \subset \mathbb{N}_0$ denotes the **set of lengths** of a.
- If $\mathsf{L}(a) = \{l_1 < l_2 < \ldots\}$, then

$$\Delta(a) = \{\, l_i - l_{i-1} \mid \text{for all } i \,\}$$

  is the **set of distances of** a.
- $\Delta(R^\bullet) = \bigcup_{a \in R^\bullet} \Delta(a)$ is the **set of distances of** $R^\bullet$.

Sets of lengths

- R is **half-factorial** if $\mathsf{L}(a)$ is a singleton for all $a \in R^\bullet$.
- If R is not half-factorial, sets of lengths are **not uniformly bounded**.
  Proof: Let $a \in R^\bullet$, such that $\{\, k < l \,\} \subset \mathsf{L}(a)$, say

$$a = u_1 \cdot \ldots \cdot u_k = v_1 \cdot \ldots \cdot v_l.$$

  Then, for all $n \in \mathbb{N}$, $\nu \in [0, n]$,

$$a^n = (u_1 \cdot \ldots \cdot u_k)^\nu (v_1 \cdot \ldots \cdot v_l)^{n-\nu},$$

  hence

$$\{\, k\nu + (l-k)(n-\nu) \mid \nu \in [1, n] \,\} \ \subset\ \mathsf{L}(a^n).$$

Remark

$R^\bullet$ is a **BF-Monoid** if $\mathsf{L}(a)$ is finite for all $a \in R^\bullet$. If R is a commutative domain [monoid] and v-noetherian, then it is BF.

Transfer homomorphism

- Useful tool: Transfer homomorphism to a simpler monoid.
- Transfer homomorphisms preserve sets of lengths (and other arithmetical invariants).

Theorem

Let H be a Krull monoid (e.g. $H = R^\bullet$ where R is a Krull domain), G its divisor class group, and $G_P = \{\, [\mathfrak{p}] \mid \mathfrak{p} \in \text{v-max}(H) \,\} \subset G$ the set of classes containing prime divisors.
There is a **transfer homomorphism** $\theta\colon H \to \mathcal{B}(G_P)$*:*

$$\begin{tikzcd} H_{red} \arrow[r, hook] \arrow[d, "\theta_{red}"'] & \mathcal{I}_v^*(H) = \mathcal{F}(\text{v-max}(H)) \arrow[d] \\ \mathcal{B}(G_P) \arrow[r, hook] & \mathcal{F}(G_P) \end{tikzcd} \qquad \begin{tikzcd} aH^\times \arrow[r, mapsto] \arrow[d, mapsto, "\theta_{red}"'] & aH = \mathfrak{p}_1 \cdot_v \ldots \cdot_v \mathfrak{p}_k \arrow[d, mapsto] \\ {[\mathfrak{p}_1] \cdot \ldots \cdot [\mathfrak{p}_k]} \arrow[r, hook] & {[\mathfrak{p}_1] \cdot \ldots \cdot [\mathfrak{p}_k]} \end{tikzcd}$$

Monoid of zero-sum sequences, II

$\mathcal{B}(G)$ provies an easier to study model for the factorization in $R^\bullet$. We get (for example):

Corollary

Let R be a Krull domain with divisor class group G in which every class contains a prime divisor.

1. *R is half-factorial $\Leftrightarrow |G| \le 2$.*
2. *$\Delta(R^\bullet)$ is a finite interval with $\min \Delta(R^\bullet) = 1$ (if non-empty).*
3. *$\mathcal{U}_k(R^\bullet)$ is a finite interval.*
4. *Structure theorem for sets of lengths holds (sets of lengths are AAMPs with uniform bound $M \in \mathbb{N}_0$ and difference $d \in \Delta(R^\bullet)$).*

Maximal orders: Main result, part I

Let K be a global field, $\mathcal{O}$ a holomorphy ring in K, A a central simple K-algebra and let R be a classical maximal $\mathcal{O}$-order in A.

$\mathcal{P}_A = \{\, a\mathcal{O} \mid a \in K^\times,\ a_v > 0 \text{ for all arch. places } v \text{ of } K \text{ with } A_v \text{ ramified.} \,\}$

Theorem 1

Suppose that **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 $\mathcal{C}_A(\mathcal{O}) = \mathcal{F}^\times(\mathcal{O}) \,/\, \mathcal{P}_A$ a ray class group of $\mathcal{O}$.

Maximal orders: Main result, part II

Let K be a number field, $\mathcal{O} = \mathcal{O}_K$ its ring of algebraic integers.

Theorem 2

Suppose that **there exist a stably free left R-ideal that is not free.** Then there exists no transfer homomorphism $\theta\colon R^\bullet \to \mathcal{B}(G_0)$, where G_0 is any subset of of an abelian group. Moreover,

1. $\Delta(R^\bullet) = \mathbb{N}$,
2. For every $k \geq 3$, $\mathbb{N}_{\geq 3} \subset \mathcal{U}_k(R^\bullet) \subset \mathbb{N}_{\geq 2}$.

The condition of the theorems

By Eichler's Theorem, the condition of Theorem 1 can only be violated if:

- K is an algebraic number field, $(A : K) = 4$, and A is ramified at every place of K not arising from $\mathcal{O}$, **or**
- K is a function field, and A is ramified every place of K not arising from $\mathcal{O}$,

Restrict to K a number field, $\mathcal{O} = \mathcal{O}_K$ its ring of algebraic integers:

- If A is not a totally definite quaternion algebra, then Theorem 1 applies.
- If A is a totally definite quaternion algebra, in all but finitely many cases (all classified), Theorem 2 applies.

Abstract setup (for rings)

Remark

An approach with two-sided ideals seems to be limited to normalizing Krull monoids.

- Let Q be a quotient ring, and R a maximal order in Q.
- Write α for the Asano-equivalence class of maximal orders equivalent to R.
- Let $S \in \alpha$, I a fractional left [right] S-ideal:

$$\mathcal{O}_l(I) = \{ x \in Q \mid xI \subset I \} = S \quad \mathcal{O}_r(I) = \{ x \in Q \mid Ix \subset I \}[= S]$$

Set

$$I^{-1} = (\mathcal{O}_l(I) :_r I) = (\mathcal{O}_r(I) :_l I) = \{ x \in Q \mid IxI \subset I \}.$$

I is **divisorial** if

$$I = I_v := (I^{-1})^{-1}.$$

Groupoid of divisorial fractional ideals

- Write $\mathcal{F}_v(\alpha)$ for the set of all such divisorial fractional ideals, $\mathcal{I}_v(\alpha)$ for the divisorial **integral** ideals.
- If $I, J \in \mathcal{F}_v(\alpha)$ with $\mathcal{O}_r(I) = \mathcal{O}_l(J)$,

$$I \cdot_v J := (IJ)_v.$$

- Maximality of $\mathcal{O}_l(I)$, $\mathcal{O}_r(I)$ implies

$$I \cdot_v I^{-1} = \mathcal{O}_l(I) \text{ and } I^{-1} \cdot_v I = \mathcal{O}_r(I).$$

Theorem

$\mathcal{F}_v(\alpha)$ with $\cdot_v$ as partial operation forms a **groupoid** *(=category in which every morphism is an isomorphism), $\mathcal{I}_v(\alpha)$ is a subcategory.*

Groupoid of divisorial fractional ideals

Assume

1. R satisfies the ACC on divisorial left [right] R-ideals;
2. R is bounded;
3. The lattice of divisorial fractional left [right] R-ideals is modular.

Then $\mathcal{F}_v(\alpha)$ is “nice”.

Strategy

To study $a \in R^\bullet$, study instead Ra in the subcategory

$$\mathcal{H}_{R^\bullet} = \{\, d(Rb)d^{-1} \mid b \in R^\bullet, d \in Q^\times \,\}$$

of $\mathcal{I}_v(\alpha)$.

Abstract norm

Provides an invariant for the factorizations of elements of $\mathcal{I}_v(\alpha)$ into maximal ones.

- The divisorial fractional two-sided R-ideals form a free abelian group on the maximal divisorial two-sided R-ideals.
- If $S \in \alpha$, there is a canonical isomorphism between divisorial fractional two-sided R-ideals and divisorial fractional two-sided S-ideals. (vertex groups of the groupoid $G = \mathcal{F}_v(\alpha)$): If I is a divisorial (R, S)-ideal,

$$\{\text{div. frac. } R\text{-ideals}\} \xrightarrow{\sim} \{\text{div. frac. } S\text{-ideals}\}$$
$$X \mapsto I^{-1} \cdot_v X \cdot_v I$$

- Form $\mathbb{G}$, a "universal vertex group" by identifying these groups.

Abstract norm, II

- Let $M \in G$ be maximal integral, X the largest div. frac. two-sided $\mathcal{O}_l(M)$-ideal contained in M.
- Set $\eta(M) = (X) \in \mathbb{G}$.
- Extend multiplicatively to a homorphism $\eta\colon G \to \mathbb{G}$.

Remark

If R is a classical maximal $\mathcal{O}$-order in a CSA A over a global field K, there is a bijection $\mathrm{spec}(R) \xrightarrow{\sim} \mathrm{spec}(\mathcal{O})$, under which η corresponds to the usual reduced norm.

Factorization of divisorial one-sided ideals

Asano, Murata (1953)

Let $I \in \mathcal{I}_v(\alpha)$. Then:

$$I = M_1 \cdot_v \ldots \cdot_v M_m \quad \text{with } M_1, \ldots, M_m \in \mathcal{I}_v(\alpha) \text{ maximal integral.}$$

1. If also $M_1 \cdot_v \ldots \cdot_v M_m = N_1 \cdot_v \ldots \cdot_v N_n$ then $m = n$.
2. There exist a permutation $\sigma \in \mathfrak{S}_m$ s.t. $(\,\eta(M_1), \ldots, \eta(M_m)\,) = (\,\eta(N_{\sigma(1)}), \ldots, \eta(N_{\sigma(n)})\,)$.
3. For every $\tau \in \mathfrak{S}_m$ there exist max. integral $M_1', \ldots, M_m'$ with $\eta(M_i') = \eta(M_{\tau(i)})$ and

$$I = M_1' \cdot_v \ldots \cdot_v M_m'$$

Thus $\mathcal{I}_v(\alpha)$ takes the place of the free abelian monoid, $\mathcal{H}_{R^\bullet}$ the place of $R^\bullet_{\text{red}} = \{\, aR \mid a \in R^\bullet \,\}$.

Abstract main result (for rings)

Theorem

Let Q be a quotient ring, and R a maximal order in Q such that

1. *R satisfies the ACC on divisorial left [right] R-ideals;*
2. *R is bounded;*
3. *The lattice of divisorial fractional left [right] R-ideals is modular.*

Then $\mathsf{L}(a)$ is finite and non-empty for all $a \in R^\bullet$.

Let $\mathcal{P} = \{\eta(Ra) \mid a \in Q^\bullet\} \subset \mathbb{G}$, $C = \mathbb{G}/\mathcal{P}$,

$$C_M = \{[\eta(I)] \in C \mid I \text{ a maximal integral left } S\text{-ideal}, S \in \alpha\}.$$

Assume further:

4. *A divisorial fractional left R-ideal I is principal $\Leftrightarrow \eta(I) \in \mathcal{P}$.*
5. *For all $S \in \alpha$, and all $g \in C_M$, there exists a maximal divisorial left S-ideal I with $[\eta(I)] = g$.*

Then there exists a transfer homomorphism $R^\bullet \to \mathcal{B}(C_M)$.

Obtaining Theorem 1

Let K be a global field, $\mathcal{O}$ a holomorphy ring in K, A a central simple K-algebra, and R a classical maximal $\mathcal{O}$-order.

1. R noetherian $\Rightarrow$ ACC on divisorial left [right] R-ideals.
2. Every left [right] R-ideal contains an element of $\mathcal{O}^\bullet \Rightarrow R$ is bounded.
3. Every left [right] R-ideal is divisorial $\Rightarrow$ modularity.
4. Bijection between projective class group and $\mathcal{C}_A(\mathcal{O})$ implies

   $$I \text{ stably free} \quad \Leftrightarrow \quad \mathrm{nr}(I) \in \mathcal{P}_A \quad \Leftrightarrow \quad \eta(I) \in \mathcal{P}.$$

   Stably free $\Rightarrow$ free implies that the required condition holds.
5. Analytic number theory: Every class of $\mathcal{C}_A(\mathcal{O})$ contains infinitely many prime ideals $\Rightarrow$ last condition satisfied, and $C_M = C$.

On the proof of Theorem 2

If K is a number field, R a maximal order in a totally definite quaternion algebra, Theorem 2 is proven by a combinatorial construction of a left R-ideal I with suitable factorizations.

Ingredients:

- A result on the distribution maximal left R-ideals within the isomorphism classes of left R-ideals (Kirschmer, Voight; 2010).
- A result on representation numbers of totally definite quadratic forms (over totally real number fields).

Proposition

There exists a totally positive prime element $p \in \mathcal{O}_K$, a non-empty subset $E \subset \{2, 3, 4\}$ and for every $l \in \mathbb{N}_0$ an atom $y_l \in R^\bullet$ such that

$$\mathsf{L}_{R^\bullet}(y_l p) = \{3\} \cup (l + E).$$