On half-factorial orders in algebraic number fields

Balint Rago

University of Graz

Conference on Rings and Factorizations

July 14, 2023

Outline

1. Preliminaries
2. The arithmetic of $\mathcal{O}$
3. Previous results
4. Half-factoriality of $\mathcal{O}$

Basic facts about orders

- Let K be an algebraic number field with ring of integers $\mathcal{O}_K$. An *order* in K is a subring $\mathcal{O} \subsetneq \mathcal{O}_K$, such that $\mathsf{q}(\mathcal{O}) = \mathsf{q}(\mathcal{O}_K)$.

Basic facts about orders

- Let K be an algebraic number field with ring of integers $\mathcal{O}_K$. An *order* in K is a subring $\mathcal{O} \subsetneq \mathcal{O}_K$, such that $\mathrm{q}(\mathcal{O}) = \mathrm{q}(\mathcal{O}_K)$.
- Orders are 1-dimensional and noetherian.

Basic facts about orders

- Let K be an algebraic number field with ring of integers $\mathcal{O}_K$. An *order* in K is a subring $\mathcal{O} \subsetneq \mathcal{O}_K$, such that $\mathsf{q}(\mathcal{O}) = \mathsf{q}(\mathcal{O}_K)$.
- Orders are 1-dimensional and noetherian.
- The *conductor* of $\mathcal{O}$

$$\mathfrak{f} = \{x \in \mathcal{O}_K \mid x\mathcal{O}_K \subseteq \mathcal{O}\}$$

is the largest ideal of $\mathcal{O}_K$, contained in $\mathcal{O}$.

Basic facts about orders

- Let K be an algebraic number field with ring of integers $\mathcal{O}_K$. An *order* in K is a subring $\mathcal{O} \subsetneq \mathcal{O}_K$, such that $\mathsf{q}(\mathcal{O}) = \mathsf{q}(\mathcal{O}_K)$.
- Orders are 1-dimensional and noetherian.
- The *conductor* of $\mathcal{O}$

$$\mathfrak{f} = \{x \in \mathcal{O}_K \mid x\mathcal{O}_K \subseteq \mathcal{O}\}$$

  is the largest ideal of $\mathcal{O}_K$, contained in $\mathcal{O}$.
- Let $\mathfrak{p} \in \operatorname{Spec}(\mathcal{O})$. Then $\mathcal{O}_\mathfrak{p}$ is integrally closed (a DVR) if and only if $\mathfrak{p} \not\supseteq \mathfrak{f}$.

Basic facts about orders

- Let K be an algebraic number field with ring of integers $\mathcal{O}_K$. An *order* in K is a subring $\mathcal{O} \subsetneq \mathcal{O}_K$, such that $\mathsf{q}(\mathcal{O}) = \mathsf{q}(\mathcal{O}_K)$.
- Orders are 1-dimensional and noetherian.
- The *conductor* of $\mathcal{O}$

$$\mathfrak{f} = \{x \in \mathcal{O}_K \mid x\mathcal{O}_K \subseteq \mathcal{O}\}$$

  is the largest ideal of $\mathcal{O}_K$, contained in $\mathcal{O}$.
- Let $\mathfrak{p} \in \mathrm{Spec}(\mathcal{O})$. Then $\mathcal{O}_\mathfrak{p}$ is integrally closed (a DVR) if and only if $\mathfrak{p} \not\supseteq \mathfrak{f}$.
- The finitely many $\mathfrak{p} \in \mathrm{Spec}(\mathcal{O})$ with $\mathfrak{p} \supseteq \mathfrak{f}$ are called *irregular* prime ideals.

Basic facts about orders

- Let K be an algebraic number field with ring of integers $\mathcal{O}_K$. An *order* in K is a subring $\mathcal{O} \subsetneq \mathcal{O}_K$, such that $\mathsf{q}(\mathcal{O}) = \mathsf{q}(\mathcal{O}_K)$.
- Orders are 1-dimensional and noetherian.
- The *conductor* of $\mathcal{O}$

$$\mathfrak{f} = \{x \in \mathcal{O}_K \mid x\mathcal{O}_K \subseteq \mathcal{O}\}$$

  is the largest ideal of $\mathcal{O}_K$, contained in $\mathcal{O}$.
- Let $\mathfrak{p} \in \mathrm{Spec}(\mathcal{O})$. Then $\mathcal{O}_\mathfrak{p}$ is integrally closed (a DVR) if and only if $\mathfrak{p} \not\supseteq \mathfrak{f}$.
- The finitely many $\mathfrak{p} \in \mathrm{Spec}(\mathcal{O})$ with $\mathfrak{p} \supseteq \mathfrak{f}$ are called *irregular* prime ideals.
- $\mathcal{O}$ is not integrally closed and hence not a UFD.

Basic facts about orders

- Let K be an algebraic number field with ring of integers $\mathcal{O}_K$. An *order* in K is a subring $\mathcal{O} \subsetneq \mathcal{O}_K$, such that $\mathsf{q}(\mathcal{O}) = \mathsf{q}(\mathcal{O}_K)$.
- Orders are 1-dimensional and noetherian.
- The *conductor* of $\mathcal{O}$

$$\mathfrak{f} = \{x \in \mathcal{O}_K \mid x\mathcal{O}_K \subseteq \mathcal{O}\}$$

  is the largest ideal of $\mathcal{O}_K$, contained in $\mathcal{O}$.
- Let $\mathfrak{p} \in \mathrm{Spec}(\mathcal{O})$. Then $\mathcal{O}_\mathfrak{p}$ is integrally closed (a DVR) if and only if $\mathfrak{p} \not\supseteq \mathfrak{f}$.
- The finitely many $\mathfrak{p} \in \mathrm{Spec}(\mathcal{O})$ with $\mathfrak{p} \supseteq \mathfrak{f}$ are called *irregular* prime ideals.
- $\mathcal{O}$ is not integrally closed and hence not a UFD.
- How close can $\mathcal{O}$ get to being a UFD?

Notions from factorization theory

- Let R be an integral domain. A nonzero element $x \in R$ is *irreducible* (an atom) if $x = ab$ implies that $a \in R^\times$ or $b \in R^\times$.

Notions from factorization theory

- Let R be an integral domain. A nonzero element $x \in R$ is *irreducible* (an atom) if $x = ab$ implies that $a \in R^\times$ or $b \in R^\times$.
- If $x = a_1 \dots a_k$ is a factorization into atoms, then k is the factorization length of the factorization.

Notions from factorization theory

- Let R be an integral domain. A nonzero element $x \in R$ is *irreducible* (an atom) if $x = ab$ implies that $a \in R^\times$ or $b \in R^\times$.
- If $x = a_1 \dots a_k$ is a factorization into atoms, then k is the factorization length of the factorization.
- The *set of lengths* of x:

$$\mathsf{L}(x) = \{k \in \mathbb{N} \mid k \text{ is a factorization length of } x\}.$$

Notions from factorization theory

- Let R be an integral domain. A nonzero element $x \in R$ is *irreducible* (an atom) if $x = ab$ implies that $a \in R^\times$ or $b \in R^\times$.
- If $x = a_1 \ldots a_k$ is a factorization into atoms, then k is the factorization length of the factorization.
- The *set of lengths* of x:

$$\mathsf{L}(x) = \{k \in \mathbb{N} \mid k \text{ is a factorization length of } x\}.$$

- R is *half-factorial* if for every nonzero nonunit $x \in R$, we have $|\mathsf{L}(x)| = 1$.

Notions from factorization theory

- Let $x \in R$, $x \neq 0$. The *elasticity* of x is defined as

$$\rho(x) = \frac{\sup \mathsf{L}(x)}{\min \mathsf{L}(x)}$$

and the elasticity of R as

$$\rho(R) = \sup_{x \in R, x \neq 0} \rho(x).$$

Notions from factorization theory

- Let $x \in R$, $x \neq 0$. The *elasticity* of x is defined as

$$\rho(x) = \frac{\sup \mathsf{L}(x)}{\min \mathsf{L}(x)}$$

  and the elasticity of R as

$$\rho(R) = \sup_{x \in R, x \neq 0} \rho(x).$$

- R is half-factorial if and only if $\rho(R) = 1$.

The arithmetic of $\mathcal{O}_K$

- The arithmetic of $\mathcal{O}_K$ is completely described by the ideal class group $(\mathrm{Cl}(\mathcal{O}_K), +)$, a finite abelian group with infinitely many prime ideals in every class.

The arithmetic of $\mathcal{O}_K$

- The arithmetic of $\mathcal{O}_K$ is completely described by the ideal class group $(\mathrm{Cl}(\mathcal{O}_K), +)$, a finite abelian group with infinitely many prime ideals in every class.
- Let $x \in \mathcal{O}_K$ and let $x\mathcal{O}_K = \mathfrak{P}_1 \dots \mathfrak{P}_k$. Then $[\mathfrak{P}_1] + \ldots + [\mathfrak{P}_k] = 0$.

The arithmetic of $\mathcal{O}_K$

- The arithmetic of $\mathcal{O}_K$ is completely described by the ideal class group $(\mathrm{Cl}(\mathcal{O}_K), +)$, a finite abelian group with infinitely many prime ideals in every class.
- Let $x \in \mathcal{O}_K$ and let $x\mathcal{O}_K = \mathfrak{P}_1 \dots \mathfrak{P}_k$. Then $[\mathfrak{P}_1] + \ldots + [\mathfrak{P}_k] = 0$.
- The arithmetic of $\mathcal{O}_K$ is equivalent to the arithmetic of $\mathcal{B}(\mathrm{Cl}(\mathcal{O}_K))$, the monoid of zero-sum sequences over $\mathrm{Cl}(\mathcal{O}_K)$.

The arithmetic of $\mathcal{O}_K$

- The arithmetic of $\mathcal{O}_K$ is completely described by the ideal class group $(\mathrm{Cl}(\mathcal{O}_K), +)$, a finite abelian group with infinitely many prime ideals in every class.
- Let $x \in \mathcal{O}_K$ and let $x\mathcal{O}_K = \mathfrak{P}_1 \dots \mathfrak{P}_k$. Then $[\mathfrak{P}_1] + \ldots + [\mathfrak{P}_k] = 0$.
- The arithmetic of $\mathcal{O}_K$ is equivalent to the arithmetic of $\mathcal{B}(\mathrm{Cl}(\mathcal{O}_K))$, the monoid of zero-sum sequences over $\mathrm{Cl}(\mathcal{O}_K)$.

Theorem

Let G be an abelian group. Then $\mathcal{B}(G)$ is half-factorial if and only if $|G| \leq 2$.

The arithmetic of $\mathcal{O}_K$

- The arithmetic of $\mathcal{O}_K$ is completely described by the ideal class group $(\mathrm{Cl}(\mathcal{O}_K), +)$, a finite abelian group with infinitely many prime ideals in every class.
- Let $x \in \mathcal{O}_K$ and let $x\mathcal{O}_K = \mathfrak{P}_1 \dots \mathfrak{P}_k$. Then $[\mathfrak{P}_1] + \ldots + [\mathfrak{P}_k] = 0$.
- The arithmetic of $\mathcal{O}_K$ is equivalent to the arithmetic of $\mathcal{B}(\mathrm{Cl}(\mathcal{O}_K))$, the monoid of zero-sum sequences over $\mathrm{Cl}(\mathcal{O}_K)$.

Theorem

Let G be an abelian group. Then $\mathcal{B}(G)$ is half-factorial if and only if $|G| \leq 2$.

Theorem (Carlitz, 1960)

$\mathcal{O}_K$ is half-factorial if and only if $|\mathrm{Cl}(\mathcal{O}_K)| \leq 2$.

The arithmetic of $\mathcal{O}$

- The arithmetic of $\mathcal{O}$ is equivalent to the arithmetic of $\mathcal{B}(G, T, \iota)$, where $G = \mathrm{Pic}(\mathcal{O})$,

$$T = \prod_{\mathfrak{p} \supseteq \mathfrak{f}} \mathcal{O}_{\mathfrak{p}}^{\bullet} / \mathcal{O}_{\mathfrak{p}}^{\times}$$

and $\iota : T \to G$ is the canonical homomorphism.

The arithmetic of $\mathcal{O}$

- The arithmetic of $\mathcal{O}$ is equivalent to the arithmetic of $\mathcal{B}(G, T, \iota)$, where $G = \mathrm{Pic}(\mathcal{O})$,

$$T = \prod_{\mathfrak{p} \supseteq \mathfrak{f}} \mathcal{O}_{\mathfrak{p}}^{\bullet} / \mathcal{O}_{\mathfrak{p}}^{\times}$$

  and $\iota : T \to G$ is the canonical homomorphism.
- $\mathcal{B}(\mathrm{Pic}(\mathcal{O}))$ is a divisor closed submonoid of $\mathcal{B}(G, T, \iota)$.

The arithmetic of $\mathcal{O}$

- The arithmetic of $\mathcal{O}$ is equivalent to the arithmetic of $\mathcal{B}(G, T, \iota)$, where $G = \mathrm{Pic}(\mathcal{O})$,

$$T = \prod_{\mathfrak{p} \supseteq \mathfrak{f}} \mathcal{O}_{\mathfrak{p}}^{\bullet} / \mathcal{O}_{\mathfrak{p}}^{\times}$$

  and $\iota : T \to G$ is the canonical homomorphism.
- $\mathcal{B}(\mathrm{Pic}(\mathcal{O}))$ is a divisor closed submonoid of $\mathcal{B}(G, T, \iota)$.
- $\mathcal{O}$ half-factorial $\implies |\mathrm{Cl}(\mathcal{O}_K)| \leq |\mathrm{Pic}(\mathcal{O})| \leq 2 \implies \mathcal{O}_K$ is half-factorial.

The arithmetic of $\mathcal{O}$

- The arithmetic of $\mathcal{O}$ is equivalent to the arithmetic of $\mathcal{B}(G, T, \iota)$, where $G = \mathrm{Pic}(\mathcal{O})$,

$$T = \prod_{\mathfrak{p} \supseteq \mathfrak{f}} \mathcal{O}_{\mathfrak{p}}^{\bullet} / \mathcal{O}_{\mathfrak{p}}^{\times}$$

  and $\iota : T \to G$ is the canonical homomorphism.
- $\mathcal{B}(\mathrm{Pic}(\mathcal{O}))$ is a divisor closed submonoid of $\mathcal{B}(G, T, \iota)$.
- $\mathcal{O}$ half-factorial $\implies |\mathrm{Cl}(\mathcal{O}_K)| \leq |\mathrm{Pic}(\mathcal{O})| \leq 2 \implies \mathcal{O}_K$ is half-factorial.
- If $\mathcal{O}$ is half-factorial, then $\mathcal{O}$ and $\mathcal{O}_K$ are close arithmetically. Are they also close algebraically?

Half-factoriality of $\mathcal{O}_\mathfrak{p}$

- An order $\mathcal{O}$ is *locally half-factorial* if $\mathcal{O}_\mathfrak{p}$ is half-factorial for all $\mathfrak{p} \in \mathrm{Spec}(\mathcal{O})$.

Half-factoriality of $\mathcal{O}_\mathfrak{p}$

- An order $\mathcal{O}$ is *locally half-factorial* if $\mathcal{O}_\mathfrak{p}$ is half-factorial for all $\mathfrak{p} \in \mathrm{Spec}(\mathcal{O})$.

Theorem (Philipp, 2012)

Let K be an algebraic number field and let $\mathcal{O}$ be a locally half-factorial order in K with $|\mathrm{Pic}(\mathcal{O})| = 1$. Then $\mathcal{O}$ is half-factorial.

Half-factoriality of $\mathcal{O}_\mathfrak{p}$

- An order $\mathcal{O}$ is *locally half-factorial* if $\mathcal{O}_\mathfrak{p}$ is half-factorial for all $\mathfrak{p} \in \mathrm{Spec}(\mathcal{O})$.

Theorem (Philipp, 2012)

Let K be an algebraic number field and let $\mathcal{O}$ be a locally half-factorial order in K with $|\mathrm{Pic}(\mathcal{O})| = 1$. Then $\mathcal{O}$ is half-factorial.

- Is every half-factorial order locally half-factorial?

Half-factoriality of $\mathcal{O}_\mathfrak{p}$

- An order $\mathcal{O}$ is *locally half-factorial* if $\mathcal{O}_\mathfrak{p}$ is half-factorial for all $\mathfrak{p} \in \mathrm{Spec}(\mathcal{O})$.

Theorem (Philipp, 2012)

Let K be an algebraic number field and let $\mathcal{O}$ be a locally half-factorial order in K with $|\mathrm{Pic}(\mathcal{O})| = 1$. Then $\mathcal{O}$ is half-factorial.

- Is every half-factorial order locally half-factorial?
- $\mathcal{O}_\mathfrak{p}$ is half-factorial if and only if $\overline{\mathcal{O}_\mathfrak{p}}$ is a DVR and $\mathsf{v}_p(\mathcal{A}(\mathcal{O}_\mathfrak{p})) = \{1\}$, where p is a prime element of $\overline{\mathcal{O}_\mathfrak{p}}$.

Quadratic orders

- Let K be a quadratic number field. Every conductor ideal $\mathfrak{f}$ is of the form $\mathfrak{f} = f\mathcal{O}_K$ for some $f \in \mathbb{N}_{\geq 2}$ and the only order with conductor f is the minimal order $\mathbb{Z} + f\mathcal{O}_K$.

Quadratic orders

- Let K be a quadratic number field. Every conductor ideal $\mathfrak{f}$ is of the form $\mathfrak{f} = f\mathcal{O}_K$ for some $f \in \mathbb{N}_{\geq 2}$ and the only order with conductor f is the minimal order $\mathbb{Z} + f\mathcal{O}_K$.

Theorem (Halter-Koch, 1983)

Let K be a quadratic number field with ring of integers $\mathcal{O}_K$ and let $\mathcal{O}$ be an order in K with conductor $f \in \mathbb{N}_{\geq 2}$. Then $\mathcal{O}$ is half-factorial if and only if the following conditions are satisfied.

(i) $\mathcal{O}_K$ is half-factorial.

(ii) $\mathcal{O} \cdot \mathcal{O}_K^\times = \mathcal{O}_K$.

(iii) f is either a prime or twice an odd prime.

If this is the case, then $\mathcal{O}$ is locally half-factorial.

Seminormal orders

- Let R be a noetherian domain. We call R *seminormal* if for all $x \in \overline{R} \setminus R$, there are infintely many $n \in \mathbb{N}$ with $x^n \notin R$.

Seminormal orders

- Let R be a noetherian domain. We call R *seminormal* if for all $x \in \overline{R} \setminus R$, there are infintely many $n \in \mathbb{N}$ with $x^n \notin R$.

Lemma

$\mathcal{O}$ is seminormal if and only if $\mathfrak{f}$ is squarefree if and only if $\mathfrak{f}$ is a radical ideal.

Seminormal orders

Theorem (Geroldinger-Kainrath-Reinhart, 2015)

Let K be an algebraic number field with ring of integers $\mathcal{O}_K$ and let $\mathcal{O}$ be a seminormal order in K. Then $\mathcal{O}$ is half-factorial if and only if the following conditions are satisfied.

(i) $\mathcal{O}_K$ is half-factorial.

(ii) The map

$$\mathrm{Spec}(\mathcal{O}_K) \to \mathrm{Spec}(\mathcal{O}),$$

$$\mathfrak{P} \mapsto \mathfrak{P} \cap \mathcal{O}$$

is bijective.

(iii) $|\,\mathrm{Pic}(\mathcal{O})| = |\,\mathrm{Cl}(\mathcal{O}_K)|$.

If this is the case, then $\mathcal{O}$ is locally half-factorial.

The Spec-map

Theorem (Halter-Koch, 1995)

Let K be an algebraic number field with ring of integers $\mathcal{O}_K$ and let $\mathcal{O}$ be an order in K. Then $\rho(\mathcal{O}) < \infty$ if and only if the map $\mathfrak{P} \mapsto \mathfrak{P} \cap \mathcal{O}$ is bijective.

The Spec-map

Theorem (Halter-Koch, 1995)

Let K be an algebraic number field with ring of integers $\mathcal{O}_K$ and let $\mathcal{O}$ be an order in K. Then $\rho(\mathcal{O}) < \infty$ if and only if the map $\mathfrak{P} \mapsto \mathfrak{P} \cap \mathcal{O}$ is bijective.

Let $\mathfrak{p} \in \mathrm{Spec}(\mathcal{O})$ with $\mathfrak{P}_1, \ldots, \mathfrak{P}_s \in \mathrm{Spec}(\mathcal{O}_K)$ lying over $\mathfrak{p}$ and $s \geq 2$. Let p be a prime element of $\overline{\mathcal{O}_\mathfrak{p}}$. Then $|\mathsf{v}_p(\mathcal{A}(\mathcal{O}_\mathfrak{p}))| = \infty$. A product of few atoms of high valuation can have long factorizations with atoms of small valuation. On the other hand, if $s = 1$, then $\mathsf{v}_p(\mathcal{A}(\mathcal{O}_\mathfrak{p}))$ is finite.

The Spec-map

Theorem (Halter-Koch, 1995)

Let K be an algebraic number field with ring of integers $\mathcal{O}_K$ and let $\mathcal{O}$ be an order in K. Then $\rho(\mathcal{O}) < \infty$ if and only if the map $\mathfrak{P} \mapsto \mathfrak{P} \cap \mathcal{O}$ is bijective.

Let $\mathfrak{p} \in \mathrm{Spec}(\mathcal{O})$ with $\mathfrak{P}_1, \ldots, \mathfrak{P}_s \in \mathrm{Spec}(\mathcal{O}_K)$ lying over $\mathfrak{p}$ and $s \geq 2$. Let p be a prime element of $\overline{\mathcal{O}_\mathfrak{p}}$. Then $|\mathrm{v}_p(\mathcal{A}(\mathcal{O}_\mathfrak{p}))| = \infty$. A product of few atoms of high valuation can have long factorizations with atoms of small valuation. On the other hand, if $s = 1$, then $\mathrm{v}_p(\mathcal{A}(\mathcal{O}_\mathfrak{p}))$ is finite.

Corollary

If $\mathcal{O}$ is half-factorial, then the map $\mathfrak{P} \mapsto \mathfrak{P} \cap \mathcal{O}$ is bijective.

Half-factoriality of $\mathcal{O}$

Theorem (R., 2023)

Let K be an algebraic number field with ring of integers $\mathcal{O}_K$, let $\mathcal{O}$ be an order in K with conductor $\mathfrak{f} = \mathfrak{P}_1^{k_1} \dots \mathfrak{P}_s^{k_s}$ and let $\mathfrak{p}_i = \mathfrak{P}_i \cap \mathcal{O}$. Then $\mathcal{O}$ is half-factorial if and only if the following conditions are satisfied.

(i) $\mathcal{O}_K$ is half-factorial.

(ii) $\mathcal{O} \cdot \mathcal{O}_K^\times = \mathcal{O}_K$.

(iii) For all $i \in [1, s]$, we have $k_i \leq 4$ and $\mathsf{v}_{p_i}(\mathcal{A}(\mathcal{O}_{\mathfrak{p}_i})) \subseteq \{1, 2\}$, where p_i is an arbitrary prime element of $\overline{\mathcal{O}}_{\mathfrak{p}_i}$. If $\mathfrak{P}_i$ is principal, we have $k_i \leq 2$ and $\mathsf{v}_{p_i}(\mathcal{A}(\mathcal{O}_{\mathfrak{p}_i})) = \{1\}$.

Implications and possible generalizations

Conjecture (Philipp, 2012)

Every half-factorial order is locally half-factorial.

Implications and possible generalizations

Conjecture (Philipp, 2012)

Every half-factorial order is locally half-factorial.

Conjecture (Kainrath, 2005)

Let $\mathcal{O}$ be a half-factorial order and let $\mathcal{O}'$ be an order, containing $\mathcal{O}$. Then $\mathcal{O}'$ is half-factorial.

Implications and possible generalizations

Conjecture (Philipp, 2012)

Every half-factorial order is locally half-factorial.

Conjecture (Kainrath, 2005)

Let $\mathcal{O}$ be a half-factorial order and let $\mathcal{O}'$ be an order, containing $\mathcal{O}$. Then $\mathcal{O}'$ is half-factorial.

- The Theorem suggests that the conjectures can be disproven. However, it is unknown, how much can be realized.

Implications and possible generalizations

Conjecture (Philipp, 2012)

Every half-factorial order is locally half-factorial.

Conjecture (Kainrath, 2005)

Let $\mathcal{O}$ be a half-factorial order and let $\mathcal{O}'$ be an order, containing $\mathcal{O}$. Then $\mathcal{O}'$ is half-factorial.

- The Theorem suggests that the conjectures can be disproven. However, it is unknown, how much can be realized.
- What about the half-factoriality of other classes of 1-dimensional noetherian domains?

Thank you for your attention!