# Non-principal orders in algebraic number fields with half-factorial localizations

Andreas Philipp

Institute for Mathematics and Scientific Computing
Karl-Franzens University Graz

9th July 2009
26èmes Journées Arithmétiques
Université de Saint-Étienne

FWF Der Wissenschaftsfonds. NAWI Graz UNI GRAZ

This work is supported by the FWF Austrian Science Found (FWF Grant P18779-N13).

# Table of contents

# Example of non-unique factorization

Factorization in rings of algebraic integers is not necessarily unique.
Example: $\mathbb{Z}[3i] \subset \mathbb{Q}(i)$
The elements $3+6i$, $3-6i$, $3$, $5$ are all irreducible.

$$(3+6i)(3-6i) = 3^2 \cdot 5$$

This phaenomenon is called non-unique factorization.

The phaenomenon of non-unique factorization is purely multiplicative.

# Non-unique factorization in maximal orders

Let $K$ be an algebraic number field, $\mathcal{O}_K$ be the ring of integers, i.e. the maximal order, of $K$.
Despite for the integers $\mathbb{Z}$ factorization in such a ring $\mathcal{O}_K$ needs no longer to be unique.
But these rings $\mathcal{O}_K$ are integrally closed and therefore so called Dedekind domains. Thus their (arithmetic) structure can be described well in the terms of classical ideal theory.

# Non-unique factorization in non-principal orders

Non-principal orders (subrings $\mathcal{O} \subset \mathcal{O}_K$) are not integrally closed anymore. In particular, $\mathcal{O}$ is never factorial.

The arithmetic of a non-prinicipal order depends on the Picard group, on the localizations at singular primes and on a yet not understood interplay between these data.

# Introduction

Let $K$ be an algebraic number field, $\mathcal{O}_K$ be the maximal order in $K$, and let $\mathcal{P} = \{p_1, \ldots, p_s\}$ be a set of primes that are inert in $\mathcal{O}_K$ (that is, $p_1, \ldots, p_s$ are prime in $\mathcal{O}_K$).
Then

$$\mathcal{O} = \mathbb{Z} + p_1 \cdot \ldots \cdot p_s \mathcal{O}_K$$

is a non-principal order in $K$ such that all localizations are half-factorial.

**What about the arithmetic of such a non-principal order?**

$$\left.\begin{array}{ll} \triangle(\mathcal{O}) & \min \triangle(\mathcal{O}) \\ \rho(\mathcal{O}) & \mathsf{c}(\mathcal{O}) \end{array}\right\} \quad \text{invariants characterizing the arithmetic}$$

These invariants measure the deviation from unique-factorization.

unique-factorization $\Leftrightarrow$ $\triangle(\mathcal{O}) = \emptyset$, $\min \triangle(\mathcal{O}) = 0$, $\rho(\mathcal{O}) = 1$, $\mathsf{c}(\mathcal{O}) = 0$

# Some definitions

By a *monoid* we always mean a commutative semigroup with identity which satisfies the cancellation law (that is, if $a$, $b$, $c \in H$ with $ab = ac$, then $b = c$ follows).

Let $H$ be a monoid. We denote by $H^\times$ the set of invertible elements of $H$, and we say that $H$ is *reduced* if $H^\times = \{1\}$.
Let $H_{\mathrm{red}} = H/H^\times = \{aH^\times | a \in H\}$ be the associated reduced monoid, and $\mathsf{q}(H)$ a (the) quotient group of $H$.

Let $R$ be a domain. Then $(R^\bullet = R\setminus\{0\}, \cdot)$ is a monoid, and $(R^\bullet)_{\mathrm{red}}$ is isomorphic to the monoid of nonzero principal ideals $\mathcal{H}(R) = \{aR | a \in R^\bullet\}$.

# Some definitions

Let $H$ and $D$ be monoids.
A homomorphism $\varphi : H \to D$ is called a *divisor homomorphism* if $\varphi(u)|\varphi(v)$ implies $u|v$ for all $u, v \in H$.
$H \subset D$ is called *saturated* if the embedding $H \hookrightarrow D$ is a divisor homomorphism (that is, if $u|_D v$ implies $u|_H v$ for all $u, v \in H$).

A homomorphism $\theta : H \to D$ is called *cofinal* if for every $a \in D$ there exists $u \in H$ such that $a \mid \theta(u)$.
$H \subset D$ is called *cofinal* if the embedding $H \hookrightarrow D$ is cofinal (that is, for every $a \in D$ there exists $u \in H$ such that $a \mid u$).

A monoid $F$ is called *free* (*abelian*, with basis $P \subset F$) if every $a \in F$ has a unique representation of the form

$$a = \prod_{p \in P} p^{\mathsf{v}_p(a)} \quad \text{with } \mathsf{v}_p(a) \in \mathbb{N}_0 \text{ and } \mathsf{v}_p(a) = 0 \text{ for almost all } p \in P$$

We set $F = \mathcal{F}(P)$.

# Factorizations

Let $H$ be an atomic monoid and $a \in H \backslash H^\times$.
A *factorization* of $a$ (in $H$) is a decomposition of $a$ into a product of irreducible elements (atoms), that is

$$a = u_1 \cdot \ldots \cdot u_n \quad \text{for } n \in \mathbb{N} \text{ and } u_1, \ldots, u_n \in \mathcal{A}(H)$$

Then this $n$ is called a *length* of $a$ (in $H$).

The set

$$\mathsf{L}(a) = \{n \in \mathbb{N} | n \text{ is a length of } a\}$$

is called the *set of lengths (of $a$)*.

We call $H$ *half-factorial* if $|\mathsf{L}(a)| = 1$ for all $a \in H \backslash H^\times$.

# Set of distances

For a finite subset $L = \{a_1, \ldots, a_t\} \subset \mathbb{Z}$ ($a_1 < a_2 < \ldots < a_t$) let

$$\triangle(L) = \{a_{\nu+1} - a_\nu | \nu \in [1, t-1]\} \subset \mathbb{N}$$

denote the *set of (successive) distances* of $L$. Then

$$\triangle(H) = \bigcup_{a \in H} \triangle(\mathsf{L}(a)) \subset \mathbb{N}$$

denotes the *set of distances of $H$*.
Clearly, $H$ is half-factorial if and only if $\triangle(H) = \emptyset$.

We call $\min \triangle(H)$ the *minimum distance* of $H$ and we set $\min \triangle(H) = 0$ if $\triangle(H) = \emptyset$.

# Orders with “big” class groups

**Theorem**

*Let $\mathcal{O}$ be an order in an algebraic number field and $|\operatorname{Pic}\mathcal{O}| \geq 3$. Then we have*

- $\min \triangle(\mathcal{O}) = 1$
- $\mathsf{c}(\mathcal{O}) \geq 3$
- $\rho(\mathcal{O}) > 1$, *i.e.* $\mathcal{O}$ *is not half-factorial.*

**But:** What can we say about these invariants if $|\operatorname{Pic}(\mathcal{O})| \leq 2$?

# Maximal orders

**Theorem**

*Let $\mathcal{O}_K$ be the maximal order of an algebraic number field $K$. Then*

- *$\mathcal{O}_K$ is factorial if and only if $|\operatorname{Pic}(\mathcal{O}_K)| = 1$.*
- *$\mathcal{O}_K$ is half-factorial if and only if $|\operatorname{Pic}(\mathcal{O}_K)| \leq 2$.*

**Proof.**

This was shown in [Carlitz, 1960]. □

**But:** This does not carry over to non-principal orders.

# Maximal orders

**Corollary**

*Let $\mathcal{O}_K$ be the maximal order of an algebraic number field K. Then*

$$\min \triangle(\mathcal{O}_K) \leq 1$$

**But:** This does not carry over to non-principal orders.

# Our situation

Let $\mathcal{O}$ be a non-principal order in an algebraic number field $K$, $\mathcal{O}_K$ be the corresponding maximal order, $\mathfrak{f} = (\mathcal{O} : \mathcal{O}_K)$ be the conductor, $\mathcal{P} = \{\mathfrak{p} \in \mathfrak{X}(\mathcal{O}) | \mathfrak{p} \not\supset \mathfrak{f}\}$, $\mathcal{P}^* = \{\mathfrak{p} \in \mathfrak{X}(\mathcal{O}) | \mathfrak{p} \supset \mathfrak{f}\}$ and $T = \prod_{\mathfrak{p} \in \mathcal{P}^*} (\mathcal{O}_\mathfrak{p}^\bullet)_{\mathrm{red}}$.
We have the following isomorphisms

$$\mathcal{I}^*(\mathcal{O}) \tilde{\to} \coprod_{\mathfrak{p} \in \mathfrak{X}(\mathcal{O})} (\mathcal{O}_\mathfrak{p}^\bullet)_{\mathrm{red}} \tilde{\to} \mathcal{F}(\mathcal{P}) \times T$$

The diagonal embedding induces a cofinal divisor homomorphism

$$\varphi : \mathcal{O}^\bullet \to \coprod_{\mathfrak{p} \in \mathfrak{X}(\mathcal{O})} (\mathcal{O}_\mathfrak{p}^\bullet)_{\mathrm{red}} \tilde{\to} \mathcal{F}(\mathcal{P}) \times T$$

and we set $H = \varphi(\mathcal{O}^\bullet)$.
Then $H \cong (\mathcal{O}^\bullet)_{\mathrm{red}}$ and $H \subset \mathcal{F}(\mathcal{P}) \times T$ is a saturated and cofinal submonoid and $\mathrm{Pic}(\mathcal{O}) = \mathcal{C}(\varphi) = (\mathcal{F}(\mathcal{P}) \times T)/H$.
We identify these groups.

# Block monoids

$$\mathcal{B}(H) = \mathcal{B}(\mathcal{O}) \subset \mathcal{F}(\mathrm{Pic}(\mathcal{O})) \times T = \mathcal{F}(\mathcal{P}) \times T$$

The canonical map

$$\beta_{\mathcal{O}} : \begin{cases} \mathcal{O}^\bullet & \rightarrow & \mathcal{B}(H) \\ a & \mapsto & \left(\prod_{\mathfrak{p}\in\mathcal{P}}[\mathfrak{p}]^{\mathsf{v}_\mathfrak{p}(a)}\right)(a\mathcal{O}_\mathfrak{p}^\times)_{\mathfrak{p}\in\mathcal{P}^*} \end{cases}$$

is a transfer homomorphism.

Thus the arithmetic of $\mathcal{O}^\bullet$ and $\mathcal{B}(H)$ is *"identical"*.

# $\mathcal{B}(\mathrm{Pic}(\mathcal{O})) \subset \mathcal{B}(H)$

Denote by $\mathcal{B}(\mathrm{Pic}(\mathcal{O}))$ the block monoid over $\mathrm{Pic}(\mathcal{O})$.
Then $\mathcal{B}(\mathrm{Pic}(\mathcal{O})) \subset \mathcal{B}(H)$ is a divisor closed submonoid.

## Immediate consequences

- $\mathcal{A}(\mathcal{B}(\mathrm{Pic}(\mathcal{O}))) \subset \mathcal{A}(\mathcal{B}(H))$, i.e. each atom of $\mathcal{B}(\mathrm{Pic}(\mathcal{O}))$ is an atom of $\mathcal{B}(H)$.
- $\triangle(\mathcal{B}(\mathrm{Pic}(\mathcal{O}))) \subset \triangle(\mathcal{B}(H))$.
- If $|\mathrm{Pic}(\mathcal{O})| \geq 3$ then $1 \in \triangle(\mathcal{B}(\mathrm{Pic}(\mathcal{O})))$ and thus
  - $\min \triangle(\mathcal{B}(H)) = 1$
  - $\mathsf{c}(H) \geq 3$
  - $\rho(H) > 1$

# Strategy

$$H \subset \mathcal{F}(\mathcal{P}) \times T \quad \text{saturated}$$

For an order $\mathcal{O}$ with half-factorial localizations let $\mathcal{P}^* = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$.

$$D_i \cong (\mathcal{O}_{\mathfrak{p}_i}^\bullet)_{\mathrm{red}} \quad \text{for all } i = 1, \ldots, r$$

$\Rightarrow \quad D_i$ are half-factorial finitely primary monoids, i.e. they have a nice structure.

**Strategy:** Use their structure and $G = \mathsf{q}(D/H)$ (=class group) to determine the arithmetic of $H$.

## Theorem

*Let $\mathcal{O}$ be an order in an algebraic number field such that all localizations are half-factorial and $|\operatorname{Pic}(\mathcal{O})| \le 2$.*
*Then we have*

1. $\rho(\mathcal{O}) \in \{1, \frac{3}{2}, 2\}$.
2. $\mathsf{c}(\mathcal{O}) \in \{2, 3\}$ *if* $\rho(\mathcal{O}) = 1$.
3. $\mathsf{c}(\mathcal{O}) = 3$ *and* $\triangle(\mathcal{O}) = \{1\}$ *if* $\rho(\mathcal{O}) = \frac{3}{2}$.
4. $\mathsf{c}(\mathcal{O}) = 4$ *and* $\triangle(\mathcal{O}) = \{1, 2\}$ *if and only of* $\rho(\mathcal{O}) = 2$.
5. $\min \triangle(\mathcal{O}) \le 1$.

*In particular, if all localizations of $\mathcal{O}$ are finitely primary monoids of exponent $1$ then we have $\mathsf{c}(\mathcal{O}) = 2$ if $\rho(\mathcal{O}) = 1$, and therefore*

$$\mathsf{c}(\mathcal{O}) = 2\rho(\mathcal{O}) \in \{2, 3, 4\}$$

*For orders in quadratic or cubic number fields this condition is always fulfilled.*

## Corollary

*Let $\mathcal{O}$ be an order in an algebraic number field such that all localizations are half-factorial.*
*If all localizations of $\mathcal{O}$ are finitely primary monoids of exponent $1$ then the following are equivalent:*

1. *$\mathcal{O}$ is half-factorial.*
2. $\mathsf{c}(\mathcal{O}) = 2$.

*In particular, for quadratic or cubic number fields the condition is always fulfilled.*

## Corollary

*Let $\mathcal{O}$ be an order in an algebraic number field such that all localizations are half-factorial.*
*Then*

$$\min \triangle(\mathcal{O}) \leq 1$$

# References


Carlitz, L. (1960).
In Proc. Amer. Math. Soc. number 11 pp. 391–392,.

Geroldinger, A. & Halter-Koch, F. (2006).
Non-Unique Factorizations: Algebraic, Combinatorial and Analytic Theory.
Pure and Applied Mathematics, Chapman & Hall.