Arithmetic of non-principal orders in algebraic number fields

Andreas Philipp

Institute for Mathematics and Scientific Computing
Karl-Franzens University Graz

Third international meeting on IVP and problems in commutative algrebra

Marseille, 30 November 2010

Let K be an algebraic number field,
$\mathcal{O}_K$ the principal (maximal) order in K, i.e. the ring of integers,
$\mathcal{O}$ a non-principal (non-maximal) order in K.

In this talk, we deal with various arithmetical invariants. These are

- the elasticity $\rho(\cdot)$,
- the catenary degree $\mathsf{c}(\cdot)$,
- the tame degree $\mathsf{t}(\cdot)$, and
- the set of distances $\triangle(\cdot)$.

(No definitions for the last two invariants will be given; these two invariants are just included for the sake of completeness.)

Definitions I

A *monoid* H is a commutative, cancellative ($ab = ac$ implies $b = c$ for all $a, b, c \in H$) semi-group. For example, $\mathcal{O} \setminus \{0\} = \mathcal{O}^\bullet$.

H is reduced, if the only unit element is the identity element (1). If H is not reduced, then there is a reduced monoid associated to H, we write H_{red}. From now on, let H be reduced.

Let $\mathcal{A}(H)$ be the *set of atoms* of H. The free (abelian) monoid $\mathsf{Z}(H) = \mathcal{F}(\mathcal{A}(H))$ is called the *factorization monoid* of H, the unique homomorphism

$$\pi : \mathsf{Z}(H) \to H \text{ satisfying } \pi(u) = u \text{ for all } u \in \mathcal{A}(H)$$

is called the *factorization homomorphism* of H and

$$\sim_H = \{(x, y) \in \mathsf{Z}(H) \times \mathsf{Z}(H) \mid \pi(x) = \pi(y)\}$$

the *monoid of relations* of H.
For $a \in H$, $\mathsf{Z}(a) = \pi^{-1}(a)$ is the *set of factorizations* of a.
$\sim_H$ has itself (as a monoid) a set of atoms $\mathcal{A}(\sim_H)$.

Definitions II

Let $a \in H$ and $z = u_1 \cdot \ldots \cdot u_n$, $z' = u'_1 \cdot \ldots \cdot u'_m \in \mathsf{Z}(a)$.

Then $|z| = n$ is the *length* of z and

$$\mathsf{d}(z, z') = \max\{n, m\} - |\gcd(z, z')|$$

is the *distance* of z and z'.

Factorizations $z_0, \ldots, z_n \in \mathsf{Z}(a)$ with $\mathsf{d}(z_{i-1}, z_i) \le N_0$ for some $N \in \mathbb{N}$ and $i \in [1, n]$ are called an N-*chain* (in $\mathsf{Z}(H)$).

The *catenary degree* $\mathsf{c}(H)$ denotes the smallest $N \in \mathbb{N}_0 \cup \{\infty\}$ such that for all $a \in H$ and for all z, $z' \in \mathsf{Z}(a)$ there is an N-chain concatenating z and z' (i.e. $z_0 = z$ and $z_n = z'$).

Definitions III

Let $a \in H$.

We denote by

$$\mathsf{L}(a) = \{|z| \mid z \in \mathsf{Z}(a)\}$$

the *set of lengths* of a.

Then we set

$$\rho(H) = \sup \left\{ \frac{\sup \mathsf{L}(a)}{\min \mathsf{L}(a)} \middle| a \in H \right\} \in \mathbb{R} \cup \{\infty\}$$

for the *elasticity* of H.

We call H *half-factorial* if and only if $\rho(H) = 1$.

Definition IV

Let O be an order in an algebraic number field K and $\mathcal{O}_K$ the corresponding principal order.

Then we set $\mathfrak{X}(\mathcal{O})$ for its *set of prime ideals of height 1*, i.e. for the set of non-zero prime ideals.

We denote by $\mathfrak{f} = (\mathcal{O} : \mathcal{O}_K)$ the *conductor* of $\mathcal{O}$.

By $\mathcal{I}^*(\mathcal{O})$, we denote the *monoid of invertible ideals* of $\mathcal{O}$.

We set $\mathcal{H}(\mathcal{O})$ for the *monoid of principal ideals*. Then

$$\mathrm{Pic}(\mathcal{O}) = \mathcal{I}^*(\mathcal{O})/\mathcal{H}(\mathcal{O})$$

is the *Picard group* of $\mathcal{O}$.

Abstract finiteness results

Theorem

Let $\mathcal{O}$ be an order (principal or non-principal) in an algebraic number field K and $\mathcal{O}_K$ the corresponding principal order.

- $\mathsf{c}(\mathcal{O}) < \infty$.
- $\rho(\mathcal{O}) < \infty \quad \Leftrightarrow \quad \begin{array}{l} \forall \mathfrak{p} \in \mathfrak{X}(\mathcal{O}) : \mathfrak{p} \supset \mathfrak{f} \\ \exists! \, \bar{\mathfrak{p}} \in \mathfrak{X}(\mathcal{O}_K) : \bar{\mathfrak{p}} \cap \mathcal{O} = \mathfrak{p}. \end{array}$

These results are

- well-known and
- "relatively easy" to prove.

There is a generalization to finitely generated domains.

Precise results

Theorem

Let $\mathcal{O}_K$ be a principal order.

1. $\rho(\mathcal{O}_K) = \max\{\frac{1}{2}\mathsf{D}(\mathrm{Pic}(\mathcal{O}_K)), 1\}$.
2. *(characterization of half-factorial principal orders) The following are equivalent.*
   - *$\mathcal{O}_K$ is half-factorial, i.e. $\rho(\mathcal{O}_K) = 1$.*
   - $|\mathrm{Pic}(\mathcal{O}_K)| \leq 2$.
   - $\mathsf{c}(\mathcal{O}) \leq 2$.
   - $\mathsf{t}(\mathcal{O}) \leq 2$.

Parts of the second part was first shown in [Carlitz, 1960].

There are (nearly) no such results for non-principal orders!

Note

If, for an order $\mathcal{O}$ (principal of non-principal), $|\mathrm{Pic}(\mathcal{O})| \geq 3$, then $\mathcal{O}$ is never half-factorial and $\mathsf{t}(\mathcal{O}) \geq \mathsf{c}(\mathcal{O}) \geq 3$. Thus the only interesting situation is $|\mathrm{Pic}(\mathcal{O})| \leq 2$.

Transfer principles I — Situation for non-principal orders

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.

Transfer principles II — Block monoids

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

The canonical map

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

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

In our situation

$$T = \prod_{\mathfrak{p}\in\mathcal{P}^*} (\mathcal{O}_\mathfrak{p}^\bullet)_{\mathrm{red}} = D_1 \times \cdot \ldots \cdot \times D_r.$$

Special structure of the monoids $D_1, \ldots, D_r$

We assume that $\mathcal{I}^*(\mathcal{O})$ is half-factorial.

$$\mathcal{I}^*(\mathcal{O}) \cong \mathcal{F}(\mathcal{P}) \times D_1 \times \ldots \times D_r$$

Thus $D_1, \ldots, D_r$ are half-factorial.
Additionally, the monoids $D_1, \ldots, D_r$ are known to be finitely primary monoids of rank 1.

The monoids $D_1, \ldots, D_r$ have a very special structure *and* their structure is well known, e.g. the sets of atoms $\mathcal{A}(D_i)$ are known explicitely.
This knowledge will be used to apply the methods from the next step.

Semi-group theoretical characterization of arithmetical invariants

Let H be a monoid (not necessarily finitely generated in our setting!).
Then we can obtain the following bound on the catenary degree and on the tame degree in terms of the monoid of relations.

$$\mathsf{c}(H) \le \mathsf{t}(H) \le \sup\{|y| \mid (x,y) \in \sim_H\}$$

Additionally, we get a similar result for the elasticity.

$$\rho(H) = \sup\left\{ \frac{|x|}{|y|} \middle| (x,y) \in \sim_H \right\}.$$

Note that the result on the catenary degree and the tame degree is slightly weaker than the corresponding result in the talk from P. García-Sánchez. This is caused by the fact that H is not finitely generated.

Putting everything together

Let $\mathcal{O}$ be an order in an algebraic number field K.

Unfortunately, $\mathcal{O}^\bullet$ is much too complicated as a monoid to apply the semi-group theoretic results directly (to $\sim_{\mathcal{O}^\bullet}$).

We can avoid this problem by a 2-step strategy.

Step 1 Apply transfer principles and "move" problem from $\mathcal{O}$ to the block monoid $\mathcal{B}(\mathcal{O})$.

Step 2 Apply the semi-group theoretic results to the block monoid $\mathcal{B}(\mathcal{O})$, which has a much simpler structure.

Theorem

Let $\mathcal{O}$ be a non-principal order in an algebraic number field such that $\mathcal{I}^*(\mathcal{O})$ is half-factorial and set $\mathcal{P}^* = \{\mathfrak{p} \in \mathfrak{X}(\mathcal{O}) \mid \mathfrak{p} \supset (\mathcal{O} : \mathcal{O}_K)\}$. Then we have

1. *If $|\mathrm{Pic}(\mathcal{O})| = 1$, then $\mathcal{O}$ is half-factorial.*
2. *If $|\mathrm{Pic}(\mathcal{O})| \ge 3$, then $(\mathsf{D}(\mathrm{Pic}(\mathcal{O})))^2 \ge \mathsf{c}(\mathcal{O}) \ge 3$ and $\rho(\mathcal{O}) > 1$.*
3. *If $|\mathrm{Pic}(\mathcal{O})| = 2$, then $\rho(\mathcal{O}) \le 2$ and $2 \le \mathsf{c}(\mathcal{O}) \le 4$.*
   If, additionally, all localizations of $\mathcal{O}$ are finitely primary monoids of exponent 1, then, setting $k = |\{\mathfrak{p} \in \mathcal{P}^* \mid [\bar{\mathcal{O}}_{\mathfrak{p}}^{\times}/\mathcal{O}_{\mathfrak{p}}^{\times}]_{\mathrm{Pic}(\mathcal{O})} = \mathrm{Pic}(\mathcal{O})\}|$, it follows that $\mathsf{c}(\mathcal{O}) = 2\rho(\mathcal{O}) = 2 + \min\{2, k\} \in \{2, 3, 4\}$ and $\triangle(\mathcal{O}) = [1, \mathsf{c}(\mathcal{O}) - 2]$; and the following are equivalent:
   - *$\mathsf{c}(\mathcal{O}) = 2$.*
   - *$\mathcal{O}$ is half-factorial, i.e. $\rho(\mathcal{O}) = 1$.*

   If, additionally, $[\mathfrak{p}] = \mathbf{0}_{\mathrm{Pic}(\mathcal{O})}$ for all $\mathfrak{p} \in \mathcal{P}^*$, then the following is also equivalent:
   - *$\mathsf{t}(\mathcal{O}) = 2$.*

References


Carlitz, L. (1960).
A characterization of algebraic number fields with class number two.
In Proc. Amer. Math. Soc. number 11 pp. 391–392,.


Geroldinger, A. and Halter-Koch, F. (2006).
Non-unique factorizations, vol. 278, of Pure and Applied Mathematics (Boca Raton).
Chapman & Hall/CRC, Boca Raton, FL.
Algebraic, combinatorial and analytic theory.


Philipp, A. (2010).
A characterization of arithmetical invariants by the monoid of relations.
Semigroup Forum *81*, 424–434.