Troisième Rencontre Internationale sur les Polynômes à Valeurs Entières

Rencontre organisée par :
Sabine Evrard

29 novembre-3 décembre 2010

Andreas Philipp

Arithmetic of non-principal orders in algebraic number fields

Vol. 2, n° 2 (2010), p. 99-102.

<http://acirm.cedram.org/item?id=ACIRM_2010__2_2_99_0>

Centre international de rencontres mathématiques
U.M.S. 822 C.N.R.S./S.M.F.
Luminy (Marseille) France

Actes des rencontres du C.I.R.M.
Vol. **2** n° 2 (2010) 99-102

Arithmetic of non-principal orders in algebraic number fields

Andreas Philipp

Abstract

Let R be an order in an algebraic number field. If R is a principal order, then many explicit results on its arithmetic are available. Among others, R is half-factorial if and only if the class group of R has at most two elements. Much less is known for non-principal orders. Using a new semigroup theoretical approach, we study half-factoriality and further arithmetical properties for non-principal orders in algebraic number fields.

1. Introduction

This is an extended abstract of the papers [19] and [20]. Its main results were presented in a talk at the *Third International Meeting on Integer Valued Polynomials and Problems in Commutative Algebra, December 2010, Marseilles*. I thank the organizers for the kind invitation.

Let R be a noetherian domain. Then every non-zero non-unit $a \in R$ can be written as a finite product of atoms, say $a = u_1 \cdot \ldots \cdot u_k$. In general, a has many essentially different factorizations into atoms. The non-uniqueness of factorizations of elements in R is measured by arithmetical invariants. For convenience, we briefly recall the definition of two classical invariants, the elasticity and the set of distances. In a factorization of an element $a \in R$ as above, the number of factors k is called the length of the factorization. Then the elasticity $\rho(a) \in \mathbb{R}_{\ge 1} \cup \{\infty\}$ is defined as the supremum over all k/l where k and l are lengths of factorizations of a. Suppose that $a = u_1 \cdot \ldots \cdot u_k = v_1 \cdot \ldots \cdot v_l$, where $k < l$ and all u_i and all v_j are atoms of R. If a has no factorizations of length m with $k < m < l$, then $l - k$ is said to be a distance of two (successive) factorization lengths, and $\Delta(a) \subset \mathbb{N}$ is the set of all such distances. The elasticity $\rho(R)$ is the supremum over all $\rho(a)$, and the set of distances $\Delta(R)$ is the union of all $\Delta(a)$. Then $\rho(R) = 1$ if and only if $\Delta(R) = \emptyset$, and in this case R is said to be half-factorial.

In the last decade, abstract finiteness results for arithmetical invariants have been derived for large classes of noetherian domains (see [11, Theorem 2.11.9], or [14, 15] for recent progress). If the noetherian domain is integrally closed, then it is a Krull domain, and if in addition every divisor class contains a prime divisor, then methods from additive and combinatorial number theory allow one to obtain precise results on the arithmetic (see [12] for the role of combinatorial number theory in this context). By a precise result, we mean an explicit formula, say for the elasticity, in terms of the group invariants of the class group, or an explicit characterization of the extremal cases, say $\rho(R) = 1$, which asks, in other words, for an explicit characterization of half-factoriality.

Half-factoriality has been a central topic ever since the beginning of factorization theory (see the surveys [5, 8, 22], and [6, 7, 9, 17] for some recent results). A classical result due to Carlitz states that a ring of integers, i.e., a principal order, is half-factorial if and only if its class group has at most two elements (see [2]; there are analogous results for Krull monoids, but for simplicity we restrict our discussion here to rings of integers). If R is a ring of integers in an algebraic number field, then, for almost all elements $a \in R$, we have $\Delta(a) = \{1\}$, and hence their sets of lengths are arithmetical progressions with difference 1 (see [11, Theorem 9.4.11]). Precise results of such a type for non-principal orders are extremely rare. In contrast to the above density result for principal orders, it is even open whether a non-principal order contains a single element a with $1 \in \Delta(a)$. In 1984, F. Halter-Koch gave a characterization of half-factoriality for

Text presented during the meeting "Third International Meeting on Integer-Valued Polynomials" organized by Sabine Evrard. 29 novembre-3 décembre 2010, C.I.R.M. (Luminy).
2000 *Mathematics Subject Classification.* 11R27, 13A05, 13F15, 20M13.
Key words. non-unique factorizations, half-factoriality, non-principal orders, algebraic number fields.
I thank my Ph.D. thesis advisors Prof. Franz Halter-Koch and Prof. Alfred Geroldinger for all the help, advice, and mathematical discussions during my thesis which led to all results in this article.

non-principal orders in quadratic number fields (see [11, Theorem 3.7.15], or [13]), but the general case remained wide open ([16, 21]).

2. Terminology

Before we can state our results in the forthcoming sections we have to gather some terminology mainly about orders in algebraic number fields and various invariants of non-unique factorization theory. All introduced notions will coincide with [11].

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

- $\overline{\mathcal{O}}$ its *integral closure* (in K); i.e. the *maximal order* in K.
- $(\mathcal{O} : \overline{\mathcal{O}})$ the *conductor* of $\mathcal{O}$ in $\overline{\mathcal{O}}$.
- $\mathfrak{X}(\mathcal{O})$ the *set of non-zero minimal prime ideals* of $\mathcal{O}$.
- $\mathcal{I}^*(\mathcal{O})$ the *set of invertible ideals* of $\mathcal{O}$.
- $\mathrm{Pic}(\mathcal{O})$ the *Picard group* of $\mathcal{O}$.
- $\mathcal{O}^\times$ the *group of units* of $\mathcal{O}$.
- $\mathcal{O}_\mathfrak{p}$ the *localization* of $\mathcal{O}$ at its prime ideal $\mathfrak{p}$.
- $[\mathfrak{p}]$ the *class* of the ideal $\mathfrak{p}$ of $\mathcal{O}$ in $\mathrm{Pic}(\mathcal{O})$.
- $\mathsf{D}(\mathrm{Pic}(\mathcal{O}))$ the *Davenport constant* of $\mathrm{Pic}(\mathcal{O})$.

We denote by $\mathcal{A}(\mathcal{O})$ the *set of atoms* of $\mathcal{O}$, by $\mathsf{Z}(\mathcal{O}) = \mathcal{F}(\mathcal{A}(\mathcal{O}/\mathcal{O}^\times))$ the free (abelian) monoid with basis $\mathcal{A}(\mathcal{O}/\mathcal{O}^\times)$, and by $\pi_\mathcal{O} : \mathsf{Z}(\mathcal{O}) \to \mathcal{O}/\mathcal{O}^\times$ the unique homomorphism such that $\pi_\mathcal{O}|\mathcal{A}(\mathcal{O}/\mathcal{O}^\times) = \mathrm{id}$. We call $\mathsf{Z}(\mathcal{O})$ the *factorization monoid* and $\pi_\mathcal{O}$ the *factorization homomorphism* of $\mathcal{O}$. For $a \in \mathcal{O}$, we denote by $\mathsf{Z}(a) = \pi_\mathcal{O}^{-1}(a\mathcal{O}^\times)$ the *set of factorizations* of a and denote by $\mathsf{L}(a) = \{|z| \mid z \in \mathsf{Z}(a)\}$ the *set of lengths* of a, where $|\cdot|$ is the ordinary length function in the free monoid $\mathsf{Z}(\mathcal{O})$. In this terminology, $\mathcal{O}$ is called *half-factorial* if $|\mathsf{L}(a)| = 1$ for all $a \in \mathcal{O} \setminus \mathcal{O}^\times$—this coincides with the classical definition of being half-factorial, since then every two factorizations of an element have the same length—and *factorial* if $|\mathsf{Z}(a)| = 1$ for all $a \in \mathcal{O} \setminus \mathcal{O}^\times$.

With all these notions at hand, for $a \in \mathcal{O}$, we set

$$\rho(a) = \frac{\sup \mathsf{L}(a)}{\min \mathsf{L}(a)} \text{ and call } \rho(\mathcal{O}) = \sup\{\rho(a) \mid a \in \mathcal{O}\} \text{ the } \textit{elasticity} \text{ of } \mathcal{O}.$$

Note that $\mathcal{O}$ is half-factorial if and only if $\rho(\mathcal{O}) = 1$.

For two factorizations z, $z' \in \mathsf{Z}(\mathcal{O})$, we call

$$\mathsf{d}(z, z') = \max\left\{\left|\frac{z}{\gcd(z, z')}\right|, \left|\frac{z'}{\gcd(z, z')}\right|\right\} \quad \text{the } \textit{distance} \text{ between } z \text{ and } z'$$

and, for two subset X, $Y \subset \mathsf{Z}(\mathcal{O})$, we call

$$\mathsf{d}(X, Y) = \min\{\mathsf{d}(x, y) \mid x \in X,\, y \in Y\} \quad \text{the } \textit{distance} \text{ between } X \text{ and } Y.$$

If one of the sets is a singleton, say $X = \{x\}$, we write $\mathsf{d}(\{x\}, Y) = \mathsf{d}(x, Y)$.
Let $a \in H$. We call two lengths k, $l \in \mathsf{L}(a)$ with $k < l$ *adjacent* if $[k, l] \cap \mathsf{L}(a) = \{k, l\}$ and, for $M \subset \mathbb{N}$, we set $\mathsf{Z}_M(a) = \{x \in \mathsf{Z}(a) \mid |x| \in M\}$. If the set is a singleton, say $M = \{k\}$, then we write $\mathsf{Z}_{\{k\}}(a) = \mathsf{Z}_k(a)$.

Definition 2.1. Let $a \in \mathcal{O}$.

1. Factorizations $z_0, \ldots, z_n \in \mathsf{Z}(a)$ with $n \in \mathbb{N}$ and $\mathsf{d}(z_{i-1}, z_i) \le N$ for some $N \in \mathbb{N}$ and $i \in [1, n]$ are called
   - an *N-chain* concatenating z_0 and z_n (in $\mathsf{Z}(\mathcal{O})$).
   - a *monotone N-chain* concatenating z_0 and z_n (in $\mathsf{Z}(\mathcal{O})$) if $|z_{i-1}| \le |z_i|$ for all $i \in [1, n]$.
2. The
   - *catenary degree* $\mathsf{c}(a)$
   - *monotone catenary degree* $\mathsf{c}_{\mathrm{mon}}(a)$

   denotes the smallest $N \in \mathbb{N}_0 \cup \{\infty\}$ such that, for all z, $z' \in \mathsf{Z}(a)$ with $|z| \le |z'|$, there is
   - an N-chain concatenating z and z'.
   - a monotone N-chain concatenating z and z'.

   Then we call
   - $\mathsf{c}(\mathcal{O}) = \sup\{\mathsf{c}(a) \mid a \in \mathcal{O}\}$ the *catenary degree* of $\mathcal{O}$.
   - $\mathsf{c}_{\mathrm{mon}}(\mathcal{O}) = \sup\{\mathsf{c}_{\mathrm{mon}}(a) \mid a \in \mathcal{O}\}$ the *monotone catenary degree* of $\mathcal{O}$.

Note that $\mathsf{c}(\mathcal{O}) \le \mathsf{c}_{\mathrm{mon}}(\mathcal{O})$ and that equality holds if $\mathcal{O}$ is half-factorial by [19, Lemma 4.4.1].

Definition 2.2. For $a \in \mathcal{O}$ and $x \in \mathsf{Z}(\mathcal{O})$, let $\mathsf{t}(a, x)$ denote the smallest $N \in \mathbb{N}_0 \cup \{\infty\}$ with the following property:

If $\mathsf{Z}(a) \cap x\mathsf{Z}(\mathcal{O}) \neq \emptyset$ and $z \in \mathsf{Z}(a)$, then there exists some $z' \in \mathsf{Z}(a) \cap x\mathsf{Z}(\mathcal{O})$ such that $\mathsf{d}(z, z') \le N$. For subsets $Y \subset \mathcal{O}$ and $X \subset \mathsf{Z}(\mathcal{O})$, we define

$$\mathsf{t}(Y, X) = \sup\{\mathsf{t}(a, x) \mid a \in Y,\, x \in X\},$$

and we define $\mathsf{t}(\mathcal{O}) = \mathsf{t}(\mathcal{O}, \mathcal{A}(\mathcal{O}/\mathcal{O}^\times))$. This is called the *tame degree* of $\mathcal{O}$.

3. The main result

The paper, [20], is devoted to non-principal orders in algebraic number fields and studies half-factoriality and the question whether 1 occurs in the set of distances.

Theorem 3.1. *Let $\mathcal{O}$ be a non-principal, locally half-factorial order in an algebraic number field and set $\mathcal{P}^* = \{\mathfrak{p} \in \mathfrak{X}(\mathcal{O}) \mid \mathfrak{p} \supset (\mathcal{O} : \overline{\mathcal{O}})\}$.*

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

   and the following are equivalent:
   - $\mathsf{c}_{\mathrm{mon}}(\mathcal{O}) = 2$.
   - $\mathsf{c}(\mathcal{O}) = 2$.
   - *$\mathcal{O}$ is half-factorial.*

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

In particular, $\min \triangle(\mathcal{O}) \le 1$ always holds.

Recall that $\mathcal{O}$ is called locally half-factorial if the localizations $\mathcal{O}_\mathfrak{p}$ are half-factorial for all non-zero prime ideals $\mathfrak{p}$ of $\mathcal{O}$. It is the standing conjecture that all half-factorial orders are locally half-factorial, and this holds true for orders in quadratic and cubic number fields. In particular, the above theorem yields the classical result of F. Halter-Koch as the following corollary. It turns out that the most difficult case is $|\operatorname{Pic}(\mathcal{O})| = 2$, and that the other ones are quite easy.

Corollary 3.2. *Let $\mathcal{O}$ be a non-principal order in a quadratic number field K, let $\overline{\mathcal{O}}$ be its integral closure, and let $\mathcal{P}^* = \{\mathfrak{p} \in \mathfrak{X}(\mathcal{O}) \mid \mathfrak{p} \supset (\mathcal{O} : \overline{\mathcal{O}})\}$.*
Then the following are equivalent:

1. *$\mathcal{O}$ is half-factorial.*
2. $\mathsf{c}(\mathcal{O}) = 2$.
3. *$|\operatorname{Pic}(\mathcal{O})| \le 2$, $\mathcal{O}$ is locally half-factorial and, for all $\mathfrak{p} \in \mathcal{P}^*$, $[(\overline{\mathcal{O}})_\mathfrak{p}^\times / \mathcal{O}_\mathfrak{p}^\times]_{\operatorname{Pic}(\mathcal{O})} = [\mathbf{0}]_{\operatorname{Pic}(\mathcal{O})}$.*
4. *$|\operatorname{Pic}(\mathcal{O})| \le 2$ and, for all $\mathfrak{p} \in \mathcal{P}^*$,*
   - *$[(\overline{\mathcal{O}})_\mathfrak{p}^\times / \mathcal{O}_\mathfrak{p}^\times]_{\operatorname{Pic}(\mathcal{O})} = [\mathbf{0}]_{\operatorname{Pic}(\mathcal{O})}$,*
   - *$\mathfrak{p}$ is inert in $\overline{\mathcal{O}}$, and*
   - *$\mathfrak{p}^2 \not\supset (\mathcal{O} : \overline{\mathcal{O}})$.*

4. Our approach

We briefly sketch our approach. We proceed in two steps. The first one is fairly standard in this area. We consider $\mathcal{O}$, the set of invertible ideals $\mathcal{I}^*(\mathcal{O})$, and construct the associated T-block monoid $\mathcal{B}(G, T, \iota)$. Then all questions under consideration can be studied in the T-block monoid instead of in $\mathcal{O}$ (see [20, Section 3] for this transfer process and [11, Chapter 3] for the detailed definition of T-block monoids). The second step contains the main new idea behind the present progress. In a series of recent papers (see for example [1, 3, 4]) and a talk at this conference [10], arithmetical invariants of a monoid have been characterized in abstract semigroup theoretical terms, such as the monoid of relations and presentations. Of course, these semigroup theoretical invariants are far beyond reach in the case of non-principal orders. However, the T-block monoid $\mathcal{B}(G, T, \iota)$ has such simple constituents that these characterizations can

be used to determine the arithmetical invariants exactly. These local results can be put together to get information for the whole T-block monoid $\mathcal{B}(G, T, \iota)$, and then all this is shifted to $\mathcal{O}$. The two crucial technical results on this are based on [18] and [19] and can be found in [20, Lemma 3.16 and Proposition 3.17].

References

[1] V. Blanco, P. A. García-Sánchez, and A. Geroldinger. Semigroup-theoretical characterizations of arithmetical invariants with applications to numerical monoids and Krull monoids. manuscript.

[2] L. Carlitz. A characterization of algebraic number fields with class number two. *Proc. Amer. Math. Soc.*, 11:391–392, 1960.

[3] S. T. Chapman, P. A. García-Sánchez, and D. Llena. The catenary and tame degree of numerical monoids. *Forum Math.*, 21(1):117–129, 2009.

[4] S. T. Chapman, Pedro A. García-Sánchez, D. Llena, Vadin Ponomarenko, and J. C. Rosales. The catenary and tame degree in finitely generated commutative cancellative monoids. *Manuscripta Math.*, 120(3):253–264, 2006.

[5] Scott T. Chapman and Jim Coykendall. Half-factorial domains, a survey. In *Non-Noetherian commutative ring theory*, volume 520 of *Math. Appl.*, pages 97–115. Kluwer Acad. Publ., Dordrecht, 2000.

[6] J. Coykendall. A characterization of polynomial rings with the half-factorial property. In *Factorization in integral domains (Iowa City, IA, 1996)*, volume 189 of *Lecture Notes in Pure and Appl. Math.*, pages 291–294. Dekker, New York, 1997.

[7] J. Coykendall. On the integral closure of a half-factorial domain. *J. Pure Appl. Algebra*, 180(1-2):25–34, 2003.

[8] J. Coykendall. Extensions of half-factorial domains: a survey. In *Arithmetical properties of commutative rings and monoids*, volume 241 of *Lect. Notes Pure Appl. Math.*, pages 46–70. Chapman & Hall/CRC, Boca Raton, FL, 2005.

[9] J. Coykendall, T. Dumitrescu, and M. Zafrullah. The half-factorial property and domains of the form $A + XB[X]$. *Houston J. Math.*, 32(1):33–46 (electronic), 2006.

[10] P.A. García-Sánchez. Semigroup-theoretical characterizations of arithmetical invariants with applications to numerical monoids and Krull monoids. *Talk at the Third International Meeting on Integer Valued Polynomials and Problems in Commutative Algebra*, December 2010, Marseilles

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

[12] A. Geroldinger and I. Z. Ruzsa. *Combinatorial number theory and additive group theory*. Advanced Courses in Mathematics. CRM Barcelona. Birkhäuser Verlag, Basel, 2009. Courses and seminars from the DocCourse in Combinatorics and Geometry held in Barcelona, 2008.

[13] F. Halter-Koch. On the factorization of algebraic integers into irreducibles. In *Topics in classical number theory, Vol. I, II (Budapest, 1981)*, volume 34 of *Colloq. Math. Soc. János Bolyai*, pages 699–707. North-Holland, Amsterdam, 1984.

[14] F. Kainrath. Arithmetic of Mori domains and monoids : the Global Case. manuscript.

[15] F. Kainrath. Elasticity of finitely generated domains. *Houston J. Math.*, 31(1):43–64 (electronic), 2005.

[16] F. Kainrath. On local half-factorial orders. In *Arithmetical properties of commutative rings and monoids*, volume 241 of *Lect. Notes Pure Appl. Math.*, pages 316–324. Chapman & Hall/CRC, Boca Raton, FL, 2005.

[17] P. Malcolmson and F. Okoh. Power series extensions of half-factorial domains. *J. Pure Appl. Algebra*, 213(4):493–495, 2009.

[18] A. Philipp. A characterization of arithmetical invariants by the monoid of relations. *Semigroup Forum*, 81:424–434, 2010.

[19] A. Philipp. A characterization of arithmetical invariants by the monoid of relations ii: The monotone catenary degree and applications to semigroup rings. manuscript, 2011.

[20] A. Philipp. A precise result on the arithmetic of non-principal orders in algebraic number fields. manuscript, 2011.

[21] M. Picavet-L'Hermitte. Factorization in some orders with a PID as integral closure. In *Algebraic number theory and Diophantine analysis (Graz, 1998)*, pages 365–390. de Gruyter, Berlin, 2000.

[22] W. A. Schmid. Half-factorial sets in finite abelian groups: a survey. In *XI. Mathematikertreffen Zagreb-Graz*, volume 348 of *Grazer Math. Ber.*, pages 41–64. Karl-Franzens-Univ. Graz, Graz, 2005.

Institut für Mathematik und Wissenschaftliches Rechnen
Karl-Franzens-Universität Graz
Heinrichstraße 36
8010 Graz, Austria • andreas.philipp@uni-graz.at