NON-UNIQUE FACTORIZATIONS OF ALGEBRAIC INTEGERS

FRANZ HALTER-KOCH

Dedicated to Professor Władisław Narkiewicz on the occasion of his 70th birthday

Abstract. We present the main results of the theory of non-unique factorizations as far as they deal with algebraic integers. We specify the philosophy that the class group of an algebraic number field measures to what extent its ring of integers fails to have unique factorization. On the other hand, if the ring of integers fails to have unique factorization then (in a sense to be made precise) almost all integers have many distinct factorizations, but also almost all integers have a clearly arranged set of factorizations.

1. Introduction

Let K be an algebraic number field (of finite degree over $\mathbb{Q}$) and $\mathcal{O}_K$ its ring of integers. Every non-zero non-unit of $\mathcal{O}_K$ has a factorization into a product of (finitely many) irreducible elements of $\mathcal{O}_K$. However, contrary to the ring $\mathbb{Z}$ of rational integers, there may be several essentially distinct such factorizations. In detail these facts are explained in §176 of Dedekind's Supplement XI to Dirichlet's "Vorlesungen über Zahlentheorie" (Chelsea Reprint 1968).

It was one of the important achievements of the mathematicians of the 19th century to overcome this deficiency, both by means of Kummer's theory of ideal numbers and by Dedekind's ideal theory. Based on these concepts, algebraic number theory grew into a powerful theory in the 20th century, culminating in class field theory and the higher reciprocity laws.

Astonishingly, questions concerning the non-uniqueness of factorizations were almost neglected in the course of this development. Since the very beginning of the theory, it was well known that $\mathcal{O}_K$ has unique factorization if and only if the class group is trivial, and it was traditional in algebraic number theory to say that the class group is a measure for the lack of unique factorization. Only in 1960. L. Carlitz [2] characterized algebraic number fields with class number 2 by arithmetical properties. In 1974, W. Narkiewicz posed the problem to characterize the class number of an algebraic number field by arithmetical properties (see [14, Problem 32]), that is, by phenomena of non-unique factorizations. In the sequel several such characterizations were given, and there is also a variety of characterizations of algebraic number fields with special class groups. The reader is referred to [14] for a concise bibliography concerning this development.

Already in 1964, W. Narkiewicz started a systematic study of phenomena of non-unique factorizations in rings of integers of algebraic number fields. In a series of papers which appeared over a period of almost 20 years (see the papers [10] to [13]) he investigated the analytic and combinatorial theory of non-unique factorizations. The most striking results of this period are presented in his book on algebraic number theory ([14, Chapter 9]).

In the sequel, the investigation of non-unique factorizations attracted the interest of many mathematicians, not only from algebraic number theory, but also from commutative ring theory, semigroup theory and additive combinatorics. An impression concerning the more recent developments dealing with general

Supported by the Austrian Science Fund FWF (Project 18779-N13).

integral domains and monoids may be obtained from the proceedings [1] and [3] of two Mini-Conferences on Factorization Theory (held 1996 in Iowa City and 2004 in Chapel Hill) and the articles contained in [4]. A survey on recent developments in zero-sum theory may be found in [5]. Only recently, the author together with A. Geroldinger completed the monograph [7] which contains a thorough presentation of the algebraic, combinatorial and analytic aspects of the theory of non-unique factorizations, together with self-contained introductions into additive group theory, the theory of v-ideals and abstract analytical number theory.

The above-mentioned monograph pursues a very broad and general point of view of the theory with possible applications not only in number theory, but also in commutative ring theory, semigroup theory, zero-sum theory and module theory. Maybe, somebody who is mainly interested in results on algebraic numbers may got lost in this generality. For this reason, the present article focusses on the results concerning algebraic integers and shows the progress of the theory since it was initiated by W. Narkiewicz. Accordingly we will concentrate on the presentation of the concepts and results. For proofs and details we refer to [8].

Besides standard notations, we denote by $\mathbb{N}$ the set of all positive integers, we set $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$, and for r, $s \in \mathbb{Z}$, we set $[r, s] = \{x \in \mathbb{Z} \mid r \le x \le s\}$.

2. Factorizations

If $a = u_1 \cdot \ldots \cdot u_r = v_1 \cdot \ldots \cdot v_s$ are two distinct factorizations of an algebraic integer a into irreducibles, then these two factorizations are considered as being not essentially different if $r = s$ and there is some permutation $\sigma \in \mathfrak{S}_r$ such that u_i and $v_{\sigma(i)}$ are associates for all $i \in [1, r]$. Thus the appropriate structure for the investigation of non-unique factorizations in the ring of integers $\mathcal{O}_K$ of an algebraic number field K is the monoid $\mathcal{H}(\mathcal{O}_K)$ of its non-zero principal ideals. It was proved by L. Redei and O. Steinfeld [15] that the structure of $\mathcal{H}(\mathcal{O}_K)$ is uniquely determined by the class group $\mathcal{C}_K$ of K (see [8, Theorem 1.7.1]). Consequently, the structure of $\mathcal{C}_K$ is responsible for all phenomena of non-unique factorizations in $\mathcal{H}(\mathcal{O}_K)$ (and consequently in $\mathcal{O}_K$).

It turns out to be convenient to describe phenomena of non-unique factorizations in an abstract cancellative reduced monoid and to investigate the monoid $\mathcal{H}(\mathcal{O}_K)$ of an algebraic number field K by means of the block monoid $\mathcal{B}(\mathcal{C}_K)$ (to be desribed in Section 3 below). This was alredy noticed by W. Narkiewicz and goes probably back to a remark of H. Davenport. In order to do it in a systematic way, we have to introduce some terminology from semigroup theory.

By a *monoid* H we always mean a multiplicatively written commutative cancellative semigroup with unit element $1 \in H$. In H, we use the notion of divisibility: For a, $b \in H$, we write $a \mid b$ (in H) if $b = ac$ for some $c \in H$. We denote by $H^\times$ the set of invertible elements of H, and we call H *reduced* if $H^\times = \{1\}$.

Let H be a reduced monoid. An element $u \in H$ is called an *atom* if, for all a, $b \in H$, $u = ab$ implies that $a = 1$ or $b = 1$. By a *factorization* z of an element $a \in H$ we mean an equation of the form

$$z\colon\ a = u_1 \cdot \ldots \cdot u_r \quad \text{with} \quad r \in \mathbb{N}_0 \quad \text{and atoms} \quad u_1, \ldots, u_r\,.$$

We call $r = |z|$ the *length* of the factorization z. Two factorizations which differ only in the order of their factors are considered as being equal. Let $\mathsf{Z}(a)$ be the set of all factorizations of a and $\mathsf{L}(a)$ the set of all lengths of factorizations of a. The monoid H is called

- *atomic* if $\mathsf{Z}(a) \ne \emptyset$ for all $a \in H$
- *factorial* if $|\mathsf{Z}(a)| = 1$ for all $a \in H$
- *half-factorial* if $|\mathsf{L}(a)| = 1$ for all $a \in H$.

If H is not factorial, then there are elements $a \in H$ for which $|\mathsf Z(a)|$ is arbitrarily large. Indeed, if $a \in H$ is an element with two distinct factorizations $a = u_1 \cdot \ldots \cdot u_r = v_1 \cdot \ldots \cdot v_s$, $n \in \mathbb N$ and $i \in [0, n]$, then $a^n = (u_1 \cdot \ldots \cdot u_r)^i (v_1 \cdot \ldots \cdot v_s)^{n-i}$, and thus $|\mathsf Z(a^n)| \ge n + 1$. The same argument shows that if H is not half-factorial, then there are elements $a \in H$ for which $|L(a)|$ becomes arbitrarily large.

The monoid $\mathcal H(D)$ of non-zero principal ideals of any noetherian domain D is an atomic monoid in which all sets of length are finite.

A monoid F is called *free* with basis $P \subset F$ if every $a \in F$ is a product of elements of P in a unique way. By definition, a monoid is free if and only if it is reduced and factorial.

From now on, we always assume that H is a reduced atomic monoid. Let $a \in H$, and let

$$z\colon\ a = u_1 \cdot \ldots \cdot u_n v_1 \cdot \ldots \cdot v_r \quad \text{and} \quad z'\colon\ u_1 \cdot \ldots \cdot u_n w_1 \cdot \ldots \cdot w_s$$

be factorizations of a into atoms such that $\{v_1, \ldots, v_r\} \cap \{w_1, \ldots, w_s\} = \emptyset$. Then we call

$$\mathsf d(z,\, z') = \max\{r, s\}$$

the *distance* between z and z'. The distance is a metric on the set of all factorizations. Based on this metric, we define the *catenary degree* $\mathsf c(a)$ for $a \in H$ to be the smallest $N \in \mathbb N_0 \cup \{\infty\}$ such that, for any two factorizations z, z' of a, there exists a finite sequence $z = z_0\,, z_1\,, \ldots, z_k = z'$ of factorizations of a satisfying that $\mathsf d(z_{i-1}, z_i) \le N$ for all $i \in [1, k]$.

The concept of distances and the catenary degree were introduced by A. Geroldinger [6] in order to measure the complexity of the set $\mathsf Z(a)$. Clearly, $\mathsf c(a) = 0$ holds if and only if $|\mathsf Z(a)| = 1$ (that is, if a has unique factorization). If $\mathsf c(a) \ne 0$, then $\mathsf c(a) \ge 2$, if $\mathsf c(a) = 2$, then $|\mathsf L(a)| = 1$, and if $\mathsf c(a) = 3$, then $\mathsf L(a)$ is an arithmetical progression with difference 1. Globally, we define

$$\mathsf c(H) = \sup\{\mathsf c(a) \mid a \in H\} \in \mathbb N_0 \cup \{\infty\}\,,$$

and we call $\mathsf c(H)$ the *catenary degree* of H. By definition, $\mathsf c(H) = 0$ if and only if H is factorial, and if $\mathsf c(H) \le 2$, then H is half-factorial. The size of $\mathsf c(H)$ is a measure for the deviation of H from being factorial: The larger $\mathsf c(H)$, the more complex phenomena of non-unique factorizations appear in H.

The catenary degree $\mathsf c(a)$ gives information about the structure of the sets of lengths $\mathsf L(a)$ for $a \in H$ as follows. For a non-empty subset $L \subset \mathbb Z$, we define its *set of distances* $\Delta(L)$ to be the set of all differences $r - s$, where r, $s \in L$, $r < s$, and $L \cap [r, s] = \{r, s\}$. We define

$$\mathcal L(H) = \{\mathsf L(a) \mid a \in H\} \quad \text{and} \quad \Delta(H) = \bigcup_{L \in \mathcal L(H)} \Delta(L)\,.$$

If H is not half-factorial, then $\Delta(H) \ne \emptyset$, and it is not difficult to prove that $\min \Delta(H) = \gcd \Delta(H)$ and $\sup \Delta(H) \le \mathsf c(H) - 2$.

Sets of lengths are the best investigated objects in the theory of non-unique factorizations. A crude measure for their structure is the elasticity. For a non-empty subset $L \subset \mathbb N$ we define

$$\rho(L) = \frac{\sup(L)}{\min(L)}\,, \quad \text{and we set} \quad \rho(\{0\}) = 1\,.$$

We call $\rho(H) = \sup\{\rho(\mathsf L(a)) \mid a \in H\}$ the *elasticity* of H. By definition H is half-factorial if and only if $\rho(H) = 1$.

Note that the elasticity gives information on the size, but not on the inner structure of the sets of lengths. This inner structure is more precisely described by the following statement.

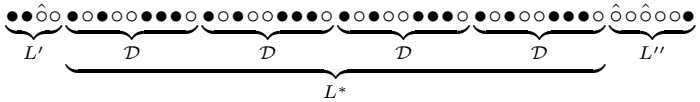
- We say that the *Structure Theorem for Sets of Lengths* holds for H if H is atomic and there exist some $M^* \in \mathbb N$ and a finite set $\Delta^* \subset \mathbb N$ with the following property: For every $L \in \mathcal L(H)$ there exists some $d \in \Delta^*$ and a "pattern" $\{0, d\} \subset \mathcal D \subset [0, d]$ such that L is of the form

  $$L = y + \big[L' \cup L^* \cup (\max L^* + L'')\big] \ \subset\ y + \mathcal D + d\mathbb Z$$

  with $y \in \mathbb Z$, $L^* = (\mathcal D + d\mathbb Z) \cap [0, \max L^*]$, $L' \subset [-M, -1]$ and $L'' \subset [1, M]$.

In this definition, L^* is the long periodic part of L consisting of the union of $|\mathcal{D}|-1$ nested arithmetical progressions. L' and L'' are the (universally bounded) initial and end pieces of L in which the pattern $\mathcal{D}$ may have holes. Such a set L is called *almost arithmetical multiprogression with distance* d *and bound* M.

A typical picture of such a set L (with $M = 6$, $d = 9$ and $\mathcal{D} = \{0, 2, 5, 6, 7, 9\}$) looks as follows (where $\hat{\circ}$ denotes a hole in the pattern):



The most important concept for the investigation of the structure of sets of lengths is that of local tameness. For an atom $u \in H$, we denote by $\mathsf{t}(u)$ the smallest $N \in \mathbb{N}_0 \cup \{\infty\}$ with the following property:

> For every $a \in uH$ and $z \in \mathsf{Z}(a)$ there exists a factorization $z' \in \mathsf{Z}(a)$ containing u as a factor and satisfying $\mathsf{d}(z, z') \le N$.

H is called *locally tame* if $\mathsf{t}(u) < \infty$ for all atoms u of H. We call $\mathsf{t}(H) = \sup\{\mathsf{t}(u) \mid u \text{ is an atom of } H\}$ the *tame degree* of H. The tame degree is a very strong invariant. Indeed we always have $\mathsf{c}(H) \le \mathsf{t}(H)$, and if H is not factorial, then $\max\{2, \rho(H)\} \le \mathsf{t}(H)$.

We are now in position to formulate the basic finiteness properties **F** of non-unique factorizations.

F. H is atomic and locally tame, $\mathsf{c}(H) < \infty$, and the Structure Theorem for Sets of Lengths holds for H.

Theorem 2.1. *Let $\mathcal{O}$ be any order in an algebraic number field K with maximal order $\mathcal{O}_K$, and let $\mathcal{H} = \mathcal{H}(\mathcal{O})$ be the monoid of non-zero principal ideals of $\mathcal{O}$.*

Then $\mathcal{H}$ satisfies **F**, *and the following assertions are equivalent*:

(a) $\rho(\mathcal{H}) < \infty$.

(b) $\mathsf{t}(\mathcal{H}) < \infty$.

(c) *The canonical map* $\operatorname{spec}(\mathcal{O}_K) \to \operatorname{spec}(\mathcal{O})$ *is injective.*

(d) *For every $a \in \mathcal{H}$, there are (up to associates) only finitely many atoms in $\mathcal{H}$ dividing some power a^n of a.*

In particular, these conditions are satisfied if $\mathcal{O} = \mathcal{O}_K$.

3. Block monoids and block homomorphisms

In the theory of non-unique factorizations, block monoids were introduced in a non-formalized way by W. Narkiewicz [12]. Later on, they proved to be not only a powerful tool in this theory, but they also are responsible for the fruitful connections between factorization theory and additive group theory.

Let G be a finite additive abelian group and denote by $\mathcal{F}(G)$ the free monoid with basis G. The elements of $\mathcal{F}(G)$ are finite sequences

$$S = g_1 \cdot \ldots \cdot g_l \quad \text{with} \quad g_1, \ldots, g_l \in G\,,$$

disregarding the order. For S as above, we define its *size* by $|S| = l$, its *sum* by $\sigma(S) = g_1 + \ldots + g_l$ and its support by $\operatorname{supp}(S) = \{g_1, \ldots, g_l\}$. For $A, B \in \mathcal{F}(G)$, we write $A \,|\, B$ if $B = AC$ for some $C \in \mathcal{F}(G)$.

The monoid

$$\mathcal{B}(G) = \{S \in \mathcal{F}(G) \mid \sigma(S) = 0\}$$

of all zero-sum sequences is called the *block monoid* over G. It is a finitely generated monoid possessing a divisor theory, it satisfies **F** and also $\mathsf t(H) < \infty$. In particular, $\mathcal B(G)$ is atomic with only finitely many atoms, and we set

$$\mathsf D(G) = \sup\big\{|U| \bigm| U \text{ is an atom of } \mathcal B(G)\big\}.$$

$\mathsf D(G)$ is called *Davenport's constant*. It is one of the best investigated and not yet completely understood constants of additive group theory. It is easily seen that $\mathsf D(G) \le |G|$ with equality if and only if G is cyclic. For brevity, we set $\mathsf c(G) = \mathsf c\big(\mathcal B(G)\big)$ and $\mathsf t(G) = \mathsf t\big(\mathcal B(G)\big)$ in order to investigate the arithmetic of the block monoid.

The significance of the block monoid for the arithmetic of algebraic number fields comes from the following transfer result.

Theorem 3.1 (Transfer Theorem for block monoids)**.** *Let K be an algebraic number field, $\mathcal O_K$ its ring of integers, $\mathcal H = \mathcal H(\mathcal O_K)$ the monoid of principal ideals of $\mathcal O_K$ and $\mathcal C_K$ the class group of $\mathcal O_K$ (written additively). For a non-zero ideal $\mathfrak a$ of $\mathcal O_K$, we denote by $[\mathfrak a] \in \mathcal C_K$ its class.*

If $\mathfrak c \in \mathcal H$ and $\mathfrak c = \mathfrak p_1 \cdot \ldots \cdot \mathfrak p_l$ is its factorization into prime ideals, then we define

$$\beta(\mathfrak c) = [\mathfrak p_1] \cdot \ldots \cdot [\mathfrak p_l] \in \mathcal B(\mathcal C_K).$$

The map $\beta\colon \mathcal H \to \mathcal B(\mathcal C_K)$ is a monoid homomorphism, and for all $\mathfrak c \in \mathcal H$ the following assertions hold:

1. $\mathsf L\big(\beta(\mathfrak c)\big) = \mathsf L(\mathfrak c)$. *In particular, $\mathfrak c$ is an atom of $\mathcal H$ if and only if $\beta(\mathfrak c)$ is an atom of $\mathcal B(\mathcal C_K)$.*
2. $\mathsf c\big(\beta(\mathfrak c)\big) \le \beta(\mathfrak c) \le \max\big\{\mathsf c\big(\beta(\mathfrak c)\big), 2\big\}$. *In particular, $\mathsf c(G) \le \mathsf c(\mathcal H) \le \max\big\{\mathsf c(G), 2\big\}$.*
3. *If $\mathfrak c$ is an atom of $\mathcal H$, then $\mathsf t\big(\beta(\mathfrak c)\big) \le \mathsf t(\mathfrak c) \le \mathsf t\big(\beta(\mathfrak c)\big) + \mathsf D(\mathcal C_K) + 1$.*

Due to Theorem 3.1, a great part of the investigations of non-unique factorizations in $\mathcal H(\mathcal O_K)$ reduces to that in $\mathcal B(\mathcal C_K)$. In particular, it has been proved in this way, that **F** holde for $\mathcal H(\mathcal O_K)$.

We continue with the investigation of factorizations in $\mathcal B(G)$ for a finite abelian group G. For $n \in \mathbb N$, we denote by C_n the (additive) cylic group with n elements.

Theorem 3.2 (Geroldinger)**.**

1. *Let $G = C_{n_1} \oplus \ldots \oplus C_{n_r}$ with $r = \mathsf r(G)$, $1 < n_1 | \ldots | n_r$, and suppose that $|G| \ge 3$. Then*
$$\max\Big\{n_r, 1 + \sum_{i=1}^{r} \Big\lfloor \frac{n_i}{2} \Big\rfloor\Big\} \le \mathsf c(G) \le \mathsf D(G). \quad \text{In particular,} \quad \max\big\{\exp(G), 1 + \mathsf r(G)\big\} \le \mathsf c(G) \le |G|.$$
2. *$\mathsf c(G) = \mathsf D(G)$ if and only if G is cyclic or an elementary 2-group.*
3. *$\mathsf c(G) = \mathsf r(G) + 1$ if G is an elementary 2-group.*
4. *$\mathsf c(G) = 3$ if and only if $G \in \big\{C_3, C_3 \oplus C_3, C_2 \oplus C_2\big\}$.*

Theorem 3.2 asserts in particular that if a finite abelian group G becomes large, then there exist elements with more and more complicated sets of factorizations in $\mathcal B(G)$. Together with Theorem 3.1, this supports the philosophy of classical algebraic number theory that the class group is a measure for the deviation from unique factorization.

Next we consider sequences with well-behaved factorizations in $\mathcal B(G)$. Two factorizations z and z' of a sequence $A \in \mathcal B(G)$ are called *adjacent* if they are of one of the following types:

A. $\quad z\colon\ A = \underbrace{(g_1g_2U_1')}_{U_1}\underbrace{\big((g_1+g_2)U_2'\big)}_{U_2} U_3 \cdot \ldots \cdot U_l, \quad \text{and} \quad z'\colon\ A = \underbrace{\big((g_1+g_2)U_1'\big)}_{V_1}\underbrace{(g_1g_2U_2')}_{V_2 \text{ or } V_2V_3} U_3 \cdot \ldots U_l$

B. $\quad z\colon\ A = \underbrace{(g_1U_1')}_{U_1}\underbrace{(g_2U_2')}_{U_2}\underbrace{\big((g_1+g_2)U_3'\big)}_{U_3} U_4 \cdot \ldots \cdot U_l \quad \text{and} \quad z'\colon\ A = \underbrace{\big((g_1+g_2)U_1'U_2'\big)}_{V_1}\underbrace{(g_1g_2U_3')}_{V_2 \text{ or } V_2V_3} U_4 \cdot \ldots U_l$

Note that if a sequence $U_1 = g_1g_2U_1'$ (with $g_1, g_2 \in G$ and $U_1' \in \mathcal{F}(G)$) is an atom of $\mathcal{B}(G)$, then the sequence $V_1 = (g_1 + g_2)U_1'$ is also an atom of $\mathcal{B}(G)$. If two sequences $U_1 = g_1U_1'$ and $U_2 = g_2U_2'$ (with $g_1, g_2 \in G$ and $U_1', U_2' \in \mathcal{F}(G)$) are atoms of $\mathcal{B}(G)$, then the sequence $V_1 = (g_1 + g_2)U_1'U_2'$ is also an atom of $\mathcal{B}(G)$. If a sequence $U_2 = (g_1 + g_2)U_2'$ (with $g_1, g_2 \in G$ and $U_2' \in \mathcal{F}(G)$) is an atom of $\mathcal{B}(G)$, then the sequence $g_1g_2U_2' \in \mathcal{B}(G)$ is either an atom or a product of two atoms of $\mathcal{B}(G)$. By definition, two adjacent factorizations z, z' satisfy $\mathsf{d}(z, z') \le 3$.

Theorem 3.3 (Connection Theorem). *Let G be a finite abelian group, $A \in \mathcal{B}(G)$ a sequence be such that $\mathrm{supp}(A) \cup \{0\} \subset G$ is a subgroup, and let z, z' be factorizations of A. Then there exist factorizations $z = z_0, z_1, \ldots, z_k = z'$ of A such that z_{i-1} and z_i are adjacent for all $i \in [1, k]$. In particular, we have $\mathsf{c}(A) \le 3$.*

The assertion of Theorem 3.3 can be rephrased by saying that "z and z' can be concatenated by a sequence of successively adjacent factorizations". The proof of the Connecting Theorem is complicated and takes up 30 pages in [8]. The main tool in its proof is the following theorem on the structure of additively closed sequences, due to W. Gao and A. Geroldinger.

Proposition 3.4. *Let G be a finite abelian group, $B, C \in \mathcal{F}(G)$, $|B| \ge |C|$, $S = BC$, $|S| \ge 4$, $0 \notin \mathrm{supp}(C)$, and suppose that, for all $g_1, g_2 \in G$,*

$$\text{if } \ g_1g_2 \,|\, B \ \text{ or } \ g_1g_2 \,|\, C \ \ (\text{in } \mathcal{F}(G)), \text{ then } \ g_1 + g_2 \in \mathrm{supp}(S)\,.$$

Then S has a proper zero-sum subsequence, apart from the following exceptions:

1. *$|C| = 1$, and we are in one of the following cases:*
   - *$B = g^k$ and $C = 2g$ for some $k \ge 3$ and $g \in G$ with $\mathrm{ord}(g) \ge k + 2$.*
   - *$B = g^k(2g)$ and $C = 3g$ for some $k \ge 2$ and $g \in G$ with $\mathrm{ord}(g) \ge k + 5$.*
   - *$B = g_1g_2(g_1+g_2)$ and $C = g_1+2g_2$ for some $g_1, g_2 \in G$ with $\mathrm{ord}(g_1) = 2$ and $\mathrm{ord}(g_2) \ge 5$.*
2. *$\{B, C\} = \{\, g(9g)(10g)\,,\ (11g)(3g)(14g)\,\}$ for some $g \in G$ with $\mathrm{ord}(g) = 16$.*

From Theorem 3.3 it is now not difficult to derive, that "almost all" zero-sum sequences $B \in \mathcal{B}(G)$ have a clearly arranged set of factorizations and in particular satisfy $\mathsf{c}(B) \le 3$. To be precise, we have the following result.

Theorem 3.5 (Theorem on nice factorizations of zero-sum sequences). *Let G be a finite abelian group.*

1. *If $B \in \mathcal{B}(G)$ and $\mathrm{supp}(B) = G \setminus \{0\}$, then $\mathsf{c}(B) \le 3$.*
2. *For every $A \in \mathcal{F}(G)$ we have*

$$\frac{\big|\big\{B \in \mathcal{B}(G) \ \big|\ B = AC \text{ for some } C \in \mathcal{F}(G)\,,\ |B| \le N\big\}\big|}{\big|\big\{B \in \mathcal{B}(G) \ \big|\ |B| \le N\big\}\big|} = 1 + O\Big(\frac{1}{N}\Big)\,.$$

In particular,

$$\frac{\big|\big\{B \in \mathcal{B}(G) \ \big|\ \mathsf{c}(B) \le 3\,,\ |B| \le N\big\}\big|}{\big|\big\{B \in \mathcal{B}(G) \ \big|\ |B| \le N\big\}\big|} = 1 + O\Big(\frac{1}{N}\Big)\,.$$

4. Quantitative theory of factorizations

Let again K be an algebraic number field, $\mathcal{O}_K$ its ring of integers, $\mathcal{H}_K$ the monoid of non-zero principal ideals of $\mathcal{O}_K$, $\mathcal{C}_K$ the class group of $\mathcal{O}_K$ and $h_K = |\mathcal{C}_K|$. For a non-zero ideal $\mathfrak{a}$ of $\mathcal{O}_K$ we denote its norm by $|\mathfrak{a}| = (\mathcal{O}_K : \mathfrak{a})$. We start with two results, first proved by W. Narkiewicz [11] and J. Śliwa [16]. Recall that for $\mathfrak{c} \in \mathcal{H}_K$ we denote by $\mathsf{Z}(\mathfrak{c})$ the set of all factorizations and by $\mathsf{L}(\mathfrak{c})$ the set of all lengths of factorizations of $\mathfrak{c}$.

Theorem 4.1. *For $x \to \infty$, we have*

$$\big|\big\{\mathfrak{c} \in \mathcal{H}_K \mid |\mathsf{Z}(\mathfrak{c})| \le k\,,\ |\mathfrak{c}| \le x\big\}\big| \sim C_1 x (\log x)^{-1+1/h_K} (\log\log x)^{\mathsf{N}_k(\mathcal{C}_K)}$$

and

$$\big|\big\{\mathfrak{c} \in \mathcal{H}_K \mid |\mathsf{L}(\mathfrak{c})| \le k\,,\ |\mathfrak{c}| \le x\big\}\big| \sim C_2 x (\log x)^{-1+\mu(\mathcal{C}_K)/h_K} (\log\log x)^{\psi_k(\mathcal{C}_K)}\,,$$

where C_1, C_2 are positive constants and $\mu(\mathcal{C}_K)$, $\mathsf{N}_k(\mathcal{C}_K)$ and $\psi_k(\mathcal{C}_K)$ are positive integers only depending on $\mathcal{C}_K$. In particular, it follows that

$$\frac{\big|\big\{\mathfrak{c} \in \mathcal{H}_K \mid |\mathsf{Z}(\mathfrak{c})| > k\,,\ |\mathfrak{c}| \le x\big\}\big|}{\big|\big\{\mathfrak{c} \in \mathcal{H}_K \mid |\mathfrak{c}| \le x\big\}\big|} = 1 + O\bigg(\frac{(\log\log x)^{\mathsf{N}_k(\mathcal{C}_K)}}{(\log x)^{1-1/h_K}}\bigg)$$

and

$$\frac{\big|\big\{\mathfrak{c} \in \mathcal{H}_K \mid |\mathsf{L}(\mathfrak{c})| > k\,,\ |\mathfrak{c}| \le x\big\}\big|}{\big|\big\{\mathfrak{c} \in \mathcal{H}_K \mid |\mathfrak{c}| \le x\big\}\big|} = 1 + O\bigg(\frac{(\log\log x)^{\psi_k(\mathcal{C}_K)}}{(\log x)^{1-\mu(\mathcal{C}_K)/h_K}}\bigg)$$

By Theorem 4.1, "almost all" elements have many distinct factorizations and even many distinct lengths. Nonetheless, also "almost all" elements have a clearly arranged set of factorizations as the following theorem shows.

Theorem 4.2. *For $x \to \infty$, we have*

$$\frac{\big|\big\{\mathfrak{c} \in \mathcal{H}_K \mid \mathsf{c}(a) \le 3\,,\ |a| \le x\big\}\big|}{\big|\big\{\mathfrak{c} \in \mathcal{H}_K \mid |a| \le x\big\}\big|} = 1 + O\bigg(\frac{1}{(\log x)^{1/h_K}}\bigg)\,.$$

The proof of Theorem 4.2 is based on the Theorems 3.1 and 3.3, and the connection between them is given by the following Counting Lemma (which also is basic for the proof of Theorem 4.1). For a sequence $S \in \mathcal{F}(\mathcal{C}_K)$ and $g \in \mathcal{C}_K$, we denote by $\mathsf{v}_g(S)$ the number of appearances of g in the sequence S.

Lemma 4.3 (Counting Lemma)**.** *Let $G_0 \subset \mathcal{C}_K$, $S \in \mathcal{F}(\mathcal{C}_K \setminus G_0)$ and $l \in \mathbb{N}_0$. Let $\Omega(G_0, S, l)$ denote the set of all sequences $C \in \mathcal{B}(\mathcal{C}_K)$ with $\mathsf{v}_g(C) = \mathsf{v}_g(S)$ for all $g \in \mathcal{C}_K \setminus G_0$ and $\mathsf{v}_g(C) \ge l$ for all $g \in G_0$, and suppose that $\Omega(G_0, S, 0)$ contains a non-trivial zero-sum sequence. Let $\boldsymbol{\beta}\colon \mathcal{H}_K \to \mathcal{B}(\mathcal{C}_K)$ be the homomorphism defined in* Theorem 3.1*, and for $x \in \mathbb{R}_{\ge 1}$ let*

$$\Omega(G_0, S, l)(x) = \big|\big\{\mathfrak{c} \in \mathcal{H}_K \mid \boldsymbol{\beta}(\mathfrak{c}) \in \Omega(G_0, S, l)\,,\ |\mathfrak{c}| \le x\big\}\big|\,.$$

Then we have, for $x \to \infty$,

$$\Omega_y(G_0, S, l)(x) = Cx\,(\log x)^{\eta}\,(\log\log x)^{\delta}\,,$$

where C is a positive real constant,

$$\eta = -1 + \frac{|G_0|}{|G|} \quad \text{and} \quad \delta = \begin{cases} |S|\,, & \text{if} \quad G_0 \ne \emptyset\,, \\ |S| - 1\,, & \text{if} \quad G_0 = \emptyset\,. \end{cases}$$

The proof of Lemma 4.3 is done by writing down the defining Dirichlet series and using an appropriate Tauberian Theorem. A weaker form of Lemma 4.3 (and consequently of the Theorems 4.1 and 4.2) can be proved in the context of abstract analytic number theory. Then it becomes applicable not only for rings of integers of algebraic number fields, but also more generally for holomorphy rings in algebraic function fields and for regular congruence monoids in such holomorphy rings (see Section 5 for their definition). Moreover, Theorem 4.1 remains valid in non-principal orders of global fields and can be refined in order to investigate factorizations in residue classes and factorizations of elements of subdomains (see [8, Section 8.10 and Chapter 9] and [9]).

In the case of algebraic number fields and algebraic function fields, it is possible to strengthen Lemma 4.3 and Theorem 4.1 and to give a more precise asymptotic formula using a series of decreasing powers of $\log x$ and $\log\log x$. The necessary analytic tools for doing this may be found in [8, Chapter 8] (theory of arithmetical and geometrical formations).

5. Generalizations and Refinements

The finiteness properties **F** and in particular the Structure Theorem for Sets of Lengths are central in the theory of non-unique factorizations. Apart from algebraic integers, these finiteness results hold for monoids and integral domains satisfying some natural finiteness conditions. To prove such more general results, we have to generalize the notions of class groups and of block monoids as follows.

Let $H \subset D$ be monoids. Two elements $a, b \in D$ are called *H-equivalent* if, for all $x \in D$, we have $ax \in H$ if and only if $bx \in H$. The set of all H-equivalence classes of non-invertible elements of D is a semigroup, called the *reduced class semigroup* $\mathcal{C}^*(H, D)$. A monoid H is called a *C-monoid* if H is a submonoid of a factorial monoid F such that $H^\times = H \cap F^\times$ and $\mathcal{C}^*(H, F)$ is finite.

Besides of their arithmetical significance, C-monoids have nice algebraic properties. Without giving details, we mention the most important ones in the following theorem.

Theorem 5.1. *Let H be a* C*-monoid. Then H satisfies the finiteness properties* **F** *of non-unique factorizations. Moreover, H satisfies the* ACC *for divisorial ideals, and the complete integral closure of H is a Krull monoid with finite divisor class group.*

Every Krull monoid (that is, every monoid with divisor theory) with finite class group is a C-monoid, and in this case the class group coincides with the reduced class semigroup (when adjoining a unit element). The most important examples of C-monoids are the multiplicative monoids of noetherian integral domains satisfying some natural finiteness conditions and congruence monoids in Dedekind domains.

Theorem 5.2. *Let R be a noetherian integral domain whose integral closure R' is a finitely generated R-module. Let $\mathfrak{f} = \mathrm{Ann}_R(R'/R)$ be its conductor, and suppose that the divisor class group of the Krull domain R' and the residue class ring $R'/\mathfrak{f}$ are both finite. Then the multiplicative monoid $\mathcal{H}(R)$ of non-zero principal ideals of R is a* C*-monoid.*

Next we introduce congruence monoids. Let R be an integral domain and $R^\bullet = R \setminus \{0\}$. Let $w_1, \dots, w_m \colon R \to \mathbb{R}$ be distinct ring monomorphisms (possibly $m = 0$), and define $\sigma \colon R^\bullet \to \{\pm 1\}^m$ by $\sigma(x) = \big(\operatorname{sign} w_1(x), \dots, \operatorname{sign} w_m(x)\big)$. Then we call σ a *sign vector*. For $a, b \in R^\bullet$ and a non-zero ideal $\mathfrak{f} \lhd R$ we define $a \equiv b \bmod \mathfrak{f}\sigma$ if $a \equiv b \bmod \mathfrak{f}$ and $\sigma(a) = \sigma(b)$. This is a congruence relation, and for $a \in R^\bullet$, we denote by $[a]_{\mathfrak{f}\sigma}$ the congruence class of a modulo $\mathfrak{f}\sigma$. The set of all congruence classes modulo $\mathfrak{f}\sigma$ is a multiplicative semigroup denoted by $R^\bullet/\mathfrak{f}\sigma$ (if $m = 0$, then $R^\bullet/\mathfrak{f}\sigma$ is the multiplicative semigroup of the residue class ring $R/\mathfrak{f}$). If $\Gamma \subset R^\bullet/\mathfrak{f}\sigma$ is a subsemigroup, then $H_\Gamma = \{a \in R^\bullet \mid [a]_{\mathfrak{f}\sigma} \in \Gamma\} \cup \{1\}$ is a submonoid of $R^\bullet$, called a *congruence monoid* modulo $\mathfrak{f}\sigma$ in R. A congruence monoid modulo $\mathfrak{f}\sigma$ is called *regular* if it consists only of elements relatively prime to $\mathfrak{f}$.

If $R \subset R'$ are integral domains such that $\mathfrak{f} = \mathrm{Ann}_R(R'/R) \neq \{0\}$, then $R^\bullet$ is a congruence monoid modulo $\mathfrak{f}$ in R. In particular, for every order R in an algebraic number field, its multiplicative monoid $R^\bullet$ is a congruence monoid modulo the conductor in its principal order.

Next let $R = \mathbb{Z}$ and $\sigma\colon \mathbb{Z} \to \{\pm 1\}$ is the ordinary sign. If $f \ge 2$ is an integer and $\Gamma \subset \mathbb{Z}/f\mathbb{Z}$ is a multiplicative subsemigroup, then the monoid $H_\Gamma = \{a \in \mathbb{N} \mid a + f\mathbb{Z} \in \Gamma\} \cup \{1\}$ is a congruence monoid modulo $f\mathbb{Z}\sigma$, usually called a *Hilbert monoid*. Hilbert monoids belong to the oldest examples in order to demonstrate non-unique factorizations.

Theorem 5.3. *Let R be a Dedekind domain with finite ideal class group, $\mathfrak{f}$ an ideal of R such that $R/\mathfrak{f}$ is finite and σ a sign vector of R. Then every congruence monoid modulo $\mathfrak{f}\sigma$ in R is a* C*-monoid.*

From the Theorems 5.1, 5.2 and 5.3 we obtain a large class of monoids and integral domains for which the finiteness results of non-unique factorizations hold. In all cases, the finiteness of the class group or of a related invariant seems to be fundamental in order to obtain finiteness results for non-unique factorizations as cited in this article.

It is an open problem whether Theorem 4.2 also holds for non-principal orders in algebraic number fields. Local investigations support the conjecture that this is not true.

References

[1] D.D. Anderson (ed.), *Factorization in Integral Domains*, Lect. Notes Pure Appl. Math., vol. 189, Marcel Dekker, 1997.
[2] L. Carlitz, *A characterization of algebraic number fields with class number two*, Proc. Am. Math. Soc. **11** (1960), 391 – 392.
[3] S.T. Chapman (ed.), *Arithmetical Properties of Commutative Rings and Monoids*, Lect. Notes Pure Appl. Math., vol. 241, Chapman & Hall/CRC, 2005.
[4] S.T. Chapman and S. Glaz (eds.), *Non-Noetherian Commutative Ring Theory*, Kluwer Academic Publishers, 2000.
[5] W. Gao and A. Geroldinger, *Zero-sum problems in finite abelian groups: a survey*, Expo. Math. **24** (2006), 337 – 369.
[6] A. Geroldinger, *Chains of factorizations and sets of lengths*, J. Algebra **188** (1997), 331 – 363.
[7] A. Geroldinger and F. Halter-Koch, *Non-unique factorizations: a survey*, Multiplicative Ideal Theory in Commutative Algebra (J.W. Brewer, S. Glaz, W. Heinzer, and B. Olberding, eds.), Springer, 2006, pp. 217 – 226.
[8] ———, *Non-Unique Factorizations. Algebraic, Combinatorial and Analytic Theory*, Pure and Applied Mathematics, vol. 278, Chapman & Hall/CRC, 2006.
[9] F. Halter-Koch, *Chebotarev formations and quantitative aspects of non-unique factorizations*, Acta Arith. **62** (1992), 173 – 206.
[10] W. Narkiewicz, *On algebraic number fields with non-unique factorizations*, Colloq. Math. **12** (1964), 59 – 67.
[11] ———, *Numbers with unique factorizations in an algebraic number field*, Acta Arith. **21** (1972), 313 – 322.
[12] ———, *Finite abelian groups and factorization problems*, Colloq. Math. **42** (1979), 319 – 330.
[13] ———, *Numbers with all factorizations of the same length in a quadratic number field*, Colloq. Math. **45** (1981), 71 – 74.
[14] ———, *Elementary and Analytic Theory of Algebraic Numbers, 3rd ed.*, Springer, 2004.
[15] L. Redei and O. Steinfeld, *Uber Ringe mit gemeinsamer multiplikativer Halbgruppe*, Comment. Math. Helv. **26** (1952), 146 – 151.
[16] J. Śliwa, *Factorizations of distinct lengths in algebraic number fields*, Acta Arith. **31** (1976), 399 – 417.

Institut für Mathematik, Karl-FranzensUniversität, Heinrichstrasse 36, 8010 Graz, Austria
E-mail address: franz.halterkoch@uni-graz.at