Alfred Geroldinger; Franz Halter-Koch

Non-unique factorizations in block semigroups and arithmetical applications

Mathematica Slovaca, Vol. 42 (1992), No. 5, 641--661

Persistent URL: http://dml.cz/dmlcz/128623

Math. Slovaca, **42** (1992), No. 5, 641–661

Mathematica Slovaca

NON–UNIQUE FACTORIZATIONS IN BLOCK SEMIGROUPS AND ARITHMETICAL APPLICATIONS

A. GEROLDINGER — F. HALTER KOCH

ABSTRACT. We study the structure of non-unique factorizations in block semigroups over finite abelian groups G with $\#G \geq 3$. As an application we obtain asymptotic formulas for certain functions associated with the non-uniqueness of factorizations in algebraic number fields.

§1. Factorizations in block semigroups

Throughout this paper, let G be an additively written finite abelian group with $\#G \geq 3$.

We recall briefly the notion of block semigroups. Let $\mathcal{F}(G)$ be the multiplicative free abelian monoid with basis G. The elements of $\mathcal{F}(G)$ are of the form

$$S = \prod_{g \in G} g^{v_g(S)},$$

where $v_g(S) \in \mathbb{N}_0$, and we set

$$\mathcal{B}(G) = \Big\{ B \in \mathcal{F}(G) \mid \sum_{g \in G} v_g(B) g = 0 \in G \Big\};$$

$\mathcal{B}(G)$ is called the *block semigroup* over G, the elements of $\mathcal{B}(G)$ are called *blocks*. More generally, for a subset $G_0 \subset G$, we set

$$\mathcal{B}(G_0) = \{ B \in \mathcal{B}(G) \mid v_g(B) = 0 \quad \text{for all} \quad g \in G \setminus G_0 \}.$$

The semigroups $\mathcal{B}(G_0)$ are Krull monoids; if $G_0 = G$, then the embedding $\mathcal{B}(G) \hookrightarrow \mathcal{F}(G)$ is a divisor theory, the divisor class group is isomorphic to G, and every class contains exactly one prime divisor; see [7, Beispiel 6] and [6, §3].

AMS Subject Classification (1991): Primary 11R27, 11R44. Secondary 20M14.
Key words: Factorizations, Block semigroups.

In particular, every $B \in \mathcal{B}(G)$ is a product of (finitely many) irreducible elements of $\mathcal{B}(G)$, which we call *irreducible blocks*.

Block semigroups were first introduced by W. Narkiewicz [12] as a combinatorial tool for the investigation of non-unique factorizations in algebraic number fields. In the sequel, they turned out not only to be an in fact very powerful tool [3] but also to be of structural interest [6].

For a block $B \in \mathcal{B}(G)$, we denote by $\mathbf{f}(B)$ the number of distinct factorizations of B into irreducible blocks (factorizations which differ only in the order of their factors are regarded as being equal). We set

$$\mathcal{B}_k(G) = \{B \in \mathcal{B}(G) \mid \mathbf{f}(B) \leq k\} \quad \text{and}$$
$$\bar{\mathcal{B}}_k(G) = \{B \in \mathcal{B}(G) \mid \mathbf{f}(B) = k\}.$$

Clearly,

$$\mathcal{B}_k(G) = \bigcup_{j=1}^{k} \bar{\mathcal{B}}_j(G),$$

and we are going to describe the structure of the sets $\mathcal{B}_k(G)$ and $\bar{\mathcal{B}}_k(G)$ in some detail. For this, we introduce the notion of independent subsets, cf. [2, §16].

DEFINITION 1. *A subset $Q \subset G$ is called independent, if*

$$\sum_{g \in Q} n_g g = 0 \qquad \textit{with} \quad n_g \in \mathbb{Z}$$

implies $n_g g = 0$ (i.e., $n_g \equiv 0 \mod \operatorname{ord}(g)$) for all $g \in Q$. We set

$$\rho(G) = \max\{\#Q \mid Q \subset G \quad \textit{is independent}\}.$$

A subgroup $H < G$ is called essential, if $H \cap G_1 \neq \{0\}$ for every subgroup $\{0\} \neq G_1 < G$.

The group G is called elementary, if every element of G has square-free order. Obviously, a finite abelian group is elementary, if and only if it is a direct sum of cyclic groups of prime order; then it contains no proper essential subgroups.

For a prime p, we denote by $r_p(G)$ the *p-rank of G*, and for a subset $E \subset G$, we denote by $\langle E \rangle$ the *subgroup generated by E*. For $n \in \mathbb{N}$, let C_n be the *cyclic group of order n*.

The notion of independence as introduced differs slightly from the usual one, where 0 is excluded.

LEMMA 1. *Let $Q \subset G$ be an independent subset.*

i) *Q is a maximal independent subset if and only if $0 \in Q$ and $\langle Q \rangle$ is an essential subgroup.*

ii) *If G is elementary, then Q is maximal independent if and only if $0 \in Q$ and $G = \langle Q \rangle$.*

Proof. [2, §16]. □

PROPOSITION 1. *We have*

$$\rho(G) = 1 + \sum_p r_p(G)$$

(*where the sum is taken over all prime numbers*), *and for an independent subset $Q \subset G$, the following assertions are equivalent:*

i) *$\#Q = \rho(G)$;*

ii) *Q is maximal independent and contains only elements of prime power order.*

Proof. By [2, §16] we have

$$\#Q = 1 + \sum_p r_p(G)$$

for every maximal independent subset $Q \subset G$ containing only elements of prime power order. Therefore it is sufficient to prove that $\#Q < \rho(G)$, if $Q \subset G$ is an independent subset containing an element which is not of prime power order. If $Q = \{g_1, \ldots, g_n\} \subset G$ is independent and $\operatorname{ord}(g_1) = de$, where $d, e \in \mathbb{N}$, $d > 1$, $e > 1$ and $(d,e) = 1$, then the set $Q' = \{dg_1, eg_1, g_2, \ldots, g_n\}$ is also independent, and $\#Q < \#Q' \leq \rho(G)$. □

DEFINITION 2.

i) *A system (in G) is a pair (Q, σ), consisting of a subset $Q \subset G$ and a function $\sigma\colon G \setminus Q \to \mathbb{N}_0$; we set*

$$|\sigma| = \sum_{g \in G \setminus Q} \sigma(g) \in \mathbb{N}_0$$

(*the extremal cases $Q = \emptyset$ and $Q = G$ are not excluded*).

ii) *For a system (Q, σ) and $l \in \mathbb{N}_0$, we set*

$$\Omega(Q,\sigma)(l) = \left\{ B \in \mathcal{B}(G) \;\middle|\; v_g(B) \left\langle \begin{array}{lll} = \sigma(g) & \text{for all} & g \in G \setminus Q, \\ \geq l & \text{for all} & g \in Q. \end{array} \right. \right\}$$

and

$$\Omega(Q,\sigma) = \Omega(Q,\sigma)(0).$$

iii) *Let* (Q,σ) *be a system and* $k \in \mathbb{N}$. (Q,σ) *is called a* k*-system, if* $\emptyset \neq \Omega(Q,\sigma) \subset \mathcal{B}_k(G)$; (Q,σ) *is called a maximal* k*-system, if it is a* k*-system and if there is no* k*-system* (Q',σ') *such that* $Q \subsetneqq Q'$ *and* $\sigma' = \sigma|_{G\setminus Q'}$.

PROPOSITION 2. *Let* $Q \subset G$ *be a maximal independent subset,* $d = \max\{\operatorname{ord}(g) \mid g \in Q\} \geq 2$ *and* $k \in \mathbb{N}$. *Then there exists a function* $\sigma\colon G \setminus Q \to \mathbb{N}_0$ *such that* (Q,σ) *is a* k*-system,* $\Omega(Q,\sigma)(dk-1) \subset \mathcal{B}_k(G)$, *and moreover:*

i) $|\sigma| = 4k$, *if there exists an element* $g_0 \in G$ *such that* $\operatorname{ord}(g_0) = 4$ *and* $2g_0 \in Q$.

ii) $|\sigma| = dk-1$, *if either* $d \geq 3$, *or if there exist elements* $g_1, g_2 \in Q$ *such that* $g_1 \neq g_2$ *and* $d = \operatorname{ord}(g_1) = \operatorname{ord}(g_2) = 2$.

Proof. Since $\#G \geq 3$ and Q is maximal, Q fulfils one of the three conditions stated in i) and ii). We set $Q = \{g_1,\ldots,g_r\}$, where $r \geq 2$, $g_1,\ldots,g_r$ are distinct, $d_i = \operatorname{ord}(g_i)$ and $d_1 = d$. Then the blocks $B_i = g_i^{d_i} \in \mathcal{B}(G)$ are irreducible.

Case 1. $g_1 = 2g_0$, where $g_0 \in G$ and $\operatorname{ord}(g_0) = 4$. We define $\sigma\colon G\setminus Q \to \mathbb{N}_0$ by

$$\sigma(g) = \begin{cases} 4k-1, & \text{if} \quad g = g_0, \\ 1, & \text{if} \quad g = -g_0, \\ 0 & \text{otherwise.} \end{cases}$$

If $B = (2g_0)^{n_1} g_2^{n_2} \cdot \ldots \cdot g_r^{n_r} g_0^{n_0} (-g_0)^{n_0'} \in \mathcal{B}(G)$, then $(2n_1 + n_0 - n_0')g_0 + n_2 g_2 + \cdots + n_r g_r = 0$, and since Q is independent, we infer $2n_1 + n_0 - n_0' \equiv 0 \mod 4$ and $n_i \equiv 0 \mod d_i$ for all $i \in \{2,\ldots,r\}$. Therefore every block $B \in \Omega(Q,\sigma)$ has the form

$$B = (2g_0)^{2m_1-1} g_2^{m_2 d_2} \cdot \ldots \cdot g_r^{m_r d_r} g_0^{4k-1}(-g_0),$$

where $m_1 \in \mathbb{N}$, $m_2,\ldots,m_r \in \mathbb{N}_0$, and the only irreducible blocks which may divide B are $B_1 = (2g_0)^2$, B_2, $\ldots$, B_r, $B_0 = g_0^4$, $B_0' = (2g_0)g_0^2$ and $B_0^* = g_0(-g_0)$. Hence all factorizations of B into irreducible blocks are given by

$$B = B_1^{j_1} B_2^{m_2} \cdot \ldots \cdot B_r^{m_r} B_0^{j_0} B_0'^{\,j_0'} B_0^*,$$

where j_1, j_0, $j_0' \in \mathbb{N}_0$ are such that $2j_1 + j_0' = 2m_1 - 1$ and $4j_0 + 2j_0' = 4k-2$, i.e., $j_0' = 2j-1$, where $1 \leq j \leq \min(m_1,k)$ and $j_1 = m_1 - j, j_0 = k - j$. Consequently, $\mathbf{f}(B) = \min(m_1,k) \leq k$, and $\mathbf{f}(B) = k$ if $m_1 \geq k$, i.e., $B \in \Omega(Q,\sigma)(2k-1)$.

Case 2. $d \geq 3$. We define $\sigma \colon G \setminus Q \to \mathbb{N}_0$ by

$$\sigma(g) = \begin{cases} dk-1, & \text{if} \quad g = -g_1, \\ 0 & \text{otherwise.} \end{cases}$$

If $B = g_1^{n_1} \cdot \ldots \cdot g_r^{n_r}(-g_1)^{n_1'} \in \mathcal{B}(G)$, then $(n_1 - n_1')g_1 + n_2 g_1 + \cdots + n_r g_r = 0$, and since Q is independent, we infer $n_1 - n_1' \equiv 0 \mod d_1$ and $n_i \equiv 0 \mod d_i$ for all $i \in \{2, \ldots, r\}$. Therefore every block $B \in \Omega(Q, \sigma)$ has the form

$$B = g_1^{d_1 m_1 - 1} g_2^{d_2 m_2} \cdot \ldots \cdot g_r^{d_r m_r} (-g_1)^{d_1 k - 1},$$

where $m_1 \in \mathbb{N}$, $m_2, \ldots, m_r \in \mathbb{N}_0$, and the only irreducible blocks which may divide B are $B_1, \ldots, B_r$, $B_1' = (-g_1)^{d_1}$ and $B_0 = g_1(-g_1)$. Hence all factorizations of B into irreducible blocks are given by

$$B = B_1^{j_1} B_2^{m_2} \cdot \ldots \cdot B_r^{m_r} B_1'^{j_1'} B_0^{j_0},$$

where $j_1, j_1', j_0 \in \mathbb{N}_0$ are such that $d_1 j_1 + j_0 = d_1 m_1 - 1$ and $d_1 j_1' + j_0 = d_1 k - 1$, i.e., $j_0 = d_1 j - 1$, where $1 \leq j \leq \min(m_1, k)$ and $j_1 = m_1 - j$, $j_1' = k - j$. Consequently, $\mathbf{f}(B) = \min(m_1, k) \leq k$, and $\mathbf{f}(B) = k$ if $m_1 \geq k$, i.e., $B \in \Omega(Q, \sigma)(dk-1)$.

Case 3. $d_1 = d_2 = 2$. We define $\sigma \colon G \setminus Q \to \mathbb{N}_0$ by

$$\sigma(g) = \begin{cases} 2k-1, & \text{if} \quad g = g_1 + g_2, \\ 0 & \text{otherwise.} \end{cases}$$

If $B = g_1^{n_1} g_2^{n_2} g_3^{n_3} \cdot \ldots \cdot g_r^{n_r}(g_1 + g_2)^n \in \mathcal{B}(G)$, then $(n_1 + n)g_1 + (n_2 + n)g_2 + n_3 g_3 + \cdots + n_r g_r = 0$, and since Q is independent, we infer $n_1 \equiv n_2 \equiv n \mod 2$ and $n_i \equiv 0 \mod d_i$ for all $i \in \{3, \ldots, r\}$. Therefore every block $B \in \Omega(Q, \sigma)$ has the form

$$B = g_1^{2m_1 - 1} g_2^{2m_2 - 1} g_3^{d_3 m_3} \cdot \ldots \cdot g_r^{d_r m_r} (g_1 + g_2)^{2k-1},$$

where $m_1, m_2 \in \mathbb{N}$, $m_3, \ldots, m_r \in \mathbb{N}_0$, and the only irreducible blocks which may divide B are $B_1, \ldots, B_r$, $B_0 = (g_1 + g_2)^2$ and $B_0' = g_1 g_2 (g_1 + g_2)$. Hence all factorizations of B into irreducibles are given by

$$B = B_1^{j_1} B_2^{j_2} B_3^{m_3} \cdot \ldots \cdot B_r^{m_r} B_0^{j_0} B_0'^{j_0'},$$

where $j_1, j_2, j_0, j_0' \in \mathbb{N}_0$ are such that $2j_1 + j_0' = 2m_1 - 1$, $2j_2 + j_0' = 2m_2 - 1$ and $2j_0 + j_0' = 2k - 1$, i.e., $j_0' = 2j - 1$, where $1 \leq j \leq \min(m_1, m_2, k)$ and $j_0 = k - j$, $j_1 = m_1 - j$, $j_2 = m_2 - j$. Consequently, $\mathbf{f}(B) = \min(m_1, m_2, k) \leq k$, and $\mathbf{f}(B) = k$, if $B \in \Omega(Q, \sigma)(2k-1)$. $\square$

DEFINITION 3. *For every maximal independent subset $Q \subset G$ and $k \in \mathbb{N}$, we set*

$$\psi_k(Q) = \max\{|\sigma| \mid (Q,\sigma) \text{ is a } k\text{-system}\},$$
$$\bar{\psi}_k(Q) = \max\{|\sigma| \mid (Q,\sigma) \text{ is a } k\text{-system}, \ \Omega(Q,\sigma) \cap \bar{\mathcal{B}}_k(G) \neq \emptyset\}$$

(by Proposition 2, the sets $\{|\sigma| \mid \dots\}$ are not empty), and

$$\psi_k(G) = \max\{\psi_k(Q) \mid Q \subset G \text{ is independent}, \ \#Q = \rho(G)\},$$
$$\bar{\psi}_k(G) = \max\{\bar{\psi}_k(Q) \mid Q \subset G \text{ is independent}, \ \#Q = \rho(G)\}.$$

We shall investigate the combinatorial invariants $\psi_k(G)$ and $\bar{\psi}_k(G)$ in §3. We shall obtain estimates from above and from below, and in a few cases we shall determine their precise values. Obviously, we have

$$\psi_k(G) = \max\{\bar{\psi}_j(G) \mid 1 \le j \le k\}.$$

In the next Proposition we characterize the independent subsets of G.

PROPOSITION 3. *For a subset $Q \subset G$, the following assertions are equivalent:*

i) *Q is independent.*
ii) *$\mathcal{B}(Q)$ is a free abelian monoid.*
iii) *There exists a function $\sigma\colon G \setminus Q \to \mathbb{N}_0$ and integers $k \in \mathbb{N}$, $l \in \mathbb{N}_0$ such that $\emptyset \neq \Omega(Q,\sigma)(l) \subset \mathcal{B}_k(G)$.*

If Q is independent, $Q = \{g_1, \dots, g_r\}$, where $g_1, \dots, g_r$ are distinct, $d_i = \mathrm{ord}(g_i)$ and $B_i = g_i^{d_i}$, then $\mathcal{B}(Q)$ is the free abelian monoid with basis $B_1, \dots, B_r$.

Proof. We set $Q = \{g_1, \dots, g_r\}$, where $g_1, \dots, g_r$ are distinct and $d_i = \mathrm{ord}(g_i)$; then the blocks $B_i = g_i^{d_i}$ are irreducible.

We prove first that ii) and iii) are violated, if Q is not independent. Indeed, suppose that there is a relation of the form $n_1 g_1 + \dots + n_r g_r = 0$, where $0 \le n_i < d_i$ and $(n_1, \dots, n_r) \neq (0, \dots, 0)$. Then we have $B_0 = g_1^{n_1} \cdot \ldots \cdot g_r^{n_r} \in \mathcal{B}(Q)$, and we may assume that B_0 is irreducible. We set $d = d_1 \cdot \ldots \cdot d_r$, $d_i' = d_i^{-1} d$ and $B = B_0^{kd}(B_1 \cdot \ldots \cdot B_r)^l \in \mathcal{B}(Q)$ (where $l \in \mathbb{N}_0$ is arbitrary). For every $0 \le j \le k$, B has the factorization

$$B = B_0^{jd} \cdot \prod_{i=1}^{r} B_i^{(k-j)n_i d_i' + l}$$

into irreducible blocks, whence $\mathbf{f}(B) \geq k+1$.

i) $\Longrightarrow$ iii) follows from Proposition 2.

If Q is independent, then every $B \in \mathcal{B}(Q)$ has a unique representation in the form $B = B_1^{n_1} \cdot \ldots \cdot B_r^{n_r}$; therefore $\mathcal{B}(Q)$ is free abelian with basis $B_1, \ldots, B_r$. □

The following Theorem uncovers the structure of the sets $\mathcal{B}_k(G)$ and $\bar{\mathcal{B}}_k(G)$.

THEOREM 1. *Let $k \in \mathbb{N}$ be a positive integer.*

i) *There exist only finitely many maximal k-systems $(Q_1, \sigma_1), \ldots, (Q_m, \sigma_m)$, and*

$$\mathcal{B}_k(G) = \bigcup_{j=1}^{m} \Omega(Q_j, \sigma_j). \tag{$*$}$$

ii) *Let (Q, σ) be a k-system. Then we have either*

$$\Omega(Q, \sigma) \cap \bar{\mathcal{B}}_k(G) = \emptyset,$$

or there exists an integer $l \in \mathbb{N}_0$ such that

$$\Omega(Q, \sigma)(l) \subset \bar{\mathcal{B}}_k(G).$$

iii) *There exist (finitely many) k-systems $(\bar{Q}_1, \bar{\sigma}_1), \ldots, (\bar{Q}_r, \bar{\sigma}_r)$ and integers $l_1, \ldots, l_r \in \mathbb{N}_0$ such that*

$$\bar{\mathcal{B}}_k(G) = \bigcup_{i=1}^{r} \Omega(\bar{Q}_i, \bar{\sigma}_i)(l_i). \tag{$**$}$$

iv) *Let $(Q, \sigma), (Q_1, \sigma_1), \ldots, (Q_n, \sigma_n)$ be k-systems, $l \in \mathbb{N}_0$ and*

$$\Omega(Q, \sigma)(l) \subset \bigcup_{i=1}^{n} \Omega(Q_i, \sigma_i).$$

Then we have $Q \subset Q_i$ and $\sigma_i = \sigma\big|_{G \setminus Q_i}$ for some $i \in \{1, \ldots, n\}$.

In particular, in the representations $(*)$ and $(**)$ in i) *and* ii) *above, every maximal independent subset Q of G appears among $Q_1, \ldots, Q_m$ as well as among $\bar{Q}_1, \ldots, \bar{Q}_r$, and the corresponding constituent of the union cannot be left out.*

Proof.

i) If $B \in \mathcal{B}_k(G)$ and $\sigma \colon G \to \mathbb{N}_0$ is defined by $\sigma(g) = v_g(B)$, then $(\emptyset, \sigma)$ is a k-system, and $B \in \Omega(\emptyset, \sigma)$. Since for every k-system (Q, σ) there exists a maximal k-system (Q', σ') such that $\Omega(Q, \sigma) \subset \Omega(Q', \sigma')$ it remains to prove that there are only finitely many maximal k-systems. If not, then there exists an independent subset $Q \subset G$, and there exist infinitely many functions $\sigma \colon G \setminus Q \to \mathbb{N}_0$ for which (Q, σ) is a k-system. In particular, there exists a sequence of functions $\left(\sigma_n : G \setminus Q \to \mathbb{N}_0\right)_{n \geq 0}$ such that all (Q, σ_n) are k-systems, and $\lim\limits_{n \to \infty} \sigma_n(g_1) = \infty$ for some $g_1 \in G \setminus Q$. By extracting subsequences of $(\sigma_n)_{n \geq 0}$, we arrive, in a finite number of steps, at the following situation: there exists a subset $\emptyset \neq Q_1 \subset G \setminus Q$, an integer $M \in \mathbb{N}$ and a sequence of functions $\left(\sigma_n : G \setminus Q \to \mathbb{N}_0\right)_{n \geq 0}$ such that all (Q, σ_n) are k-systems, $\lim\limits_{n \to \infty} \sigma_n(g) = \infty$ for all $g \in Q_1$, and $\sigma_n(g) \leq M$ for all $n \geq 0$ and all $g \in G \setminus (Q \cup Q_1)$. Therefore there exists a function $\sigma \colon G \setminus (Q \cup Q_1) \to \mathbb{N}_0$ and a subsequence $(\sigma_{n_j})_{j \geq 0}$ of $(\sigma_n)_{n \geq 0}$ such that $\sigma_{n_j}(g) = \sigma(g)$ for all $j \geq 0$ and all $g \in G \setminus (Q \cup Q_1)$. We contend that $(Q \cup Q_1, \sigma)$ is a k-system (contradicting the maximality of the k-systems (Q, σ_{n_j})). Indeed, $\emptyset \neq \Omega(Q, \sigma_{n_j}) \subset \Omega(Q \cup Q_1, \sigma)$, and if $B \in \Omega(Q \cup Q_1, \sigma)$, then there exists an index $j \geq 0$ such that $\sigma_{n_j}(g) \geq v_g(B)$ for all $g \in Q_1$, and therefore there exists a block $\bar{B} \in \Omega(Q, \sigma_{n_j})$ such that $\bar{B} = BB'$ for some $B' \in \mathcal{B}(G)$, whence $\mathbf{f}(B) \leq \mathbf{f}(\bar{B}) \leq k$, i.e., $B \in \mathcal{B}_k(G)$.

ii) Fix a block $B_0 \in \Omega(Q, \sigma) \cap \bar{\mathcal{B}}_k(G)$, and set $l = \max\{v_g(B_0) \mid g \in Q\}$. If $B \in \Omega(Q, \sigma)(l)$, then $B = B_0 B'$ for some $B' \in \mathcal{B}(G)$, and therefore we have $k = \mathbf{f}(B_0) \leq \mathbf{f}(B) \leq k$, i.e. $B \in \bar{\mathcal{B}}_k(G)$.

iii) By i), we have

$$\bar{\mathcal{B}}_k(G) = \bigcup_{j=1}^{m} \Omega(Q_j, \sigma_j) \cap \bar{\mathcal{B}}_k(G),$$

and therefore it is sufficient to prove the following statement:

Given a k-system (Q, σ) such that $\Omega(Q, \sigma) \cap \bar{\mathcal{B}}_k(G) \neq \emptyset$, then there exist finitely many k-systems (Q_i, σ_i) $(i = 1, \ldots, n)$ and $l_1, \ldots, l_n \in \mathbb{N}_0$ such that

$$\Omega(Q, \sigma) \cap \bar{\mathcal{B}}_k(G) = \bigcup_{i=1}^{n} \Omega(Q_i, \sigma_i)(l_i).$$

We do this by induction on $\#Q$. For $Q = \emptyset$, there is nothing to prove. Thus suppose $Q \neq \emptyset$; by ii), there exists an integer $l \in \mathbb{N}_0$ such that $\Omega(Q, \sigma)(l) \subset \bar{\mathcal{B}}_k(G)$, and we obtain

$$\Omega(Q, \sigma) = \Omega(Q, \sigma)(l) \cup \bigcup_{(Q', \sigma')} \Omega(Q', \sigma'),$$

where the union is taken over all proper subsets $Q' \subsetneqq Q$ and all functions $\sigma' \colon G \setminus Q' \to \mathbb{N}_0$ satisfying $\sigma'|_{G\setminus Q} = \sigma$, $\sigma'(g) < l$ for all $g \in Q \setminus Q'$ and $\Omega(Q',\sigma') \neq \emptyset$. This implies

$$\Omega(Q,\sigma) \cap \bar{\mathcal{B}}_k(G) = \Omega(Q,\sigma)(l) \cup \bigcup_{(Q',\sigma')} \Omega(Q',\sigma') \cap \bar{\mathcal{B}}_k(G),$$

and the assertion follows by induction hypothesis.

iv) Let $B \in \Omega(Q,\sigma)(l)$ be a block satisfying $v_g(B) > \max\{|\sigma_1|,\dots,|\sigma_n|\}$ for all $g \in Q$. If then $B \in \Omega(Q_i,\sigma_i)$ for some i, we infer $Q \subset Q_i$, and $\sigma_i(g) = v_g(B) = \sigma(g)$ for all $g \in G \setminus Q_i$.

Now let $Q \subset G$ be a maximal independent subset. By Proposition 2, there exists a function $\sigma \colon G \setminus Q \to \mathbb{N}_0$ and $l \in \mathbb{N}_0$ such that

$$\Omega(Q,\sigma) \subset \mathcal{B}_k(G) = \bigcup_{j=1}^{m} \Omega(Q_j,\sigma_j)$$

and

$$\Omega(Q,\sigma)(l) \subset \bar{\mathcal{B}}_k(G) = \bigcup_{j=1}^{r} \Omega(\bar{Q}_i,\bar{\sigma}_i)(l_i).$$

By the above argument, we infer $Q \subset Q_j$, $\sigma_j = \sigma|_{G\setminus Q_j}$ for some $j \in \{1,\dots,n\}$, and $Q \subset \bar{Q}_i$, $\bar{\sigma}_i = \sigma|_{G\setminus \bar{Q}_i}$ for some $i \in \{1,\dots,r\}$. Since Q is a maximal independent subset of G, this implies $Q = Q_j$ and $Q = \bar{Q}_i$, whence the assertion. □

§2. Arithmetical applications

Let K be an algebraic number field, R its ring of integers, $\mathcal{I}$ the semigroup of non-zero ideals of R, $\mathcal{H}$ the semigroup of non-zero principal ideals of R, $G = \mathcal{I}/\mathcal{H}$ the ideal class group, and $h = \#G$ the class number of K. If $\mathcal{P}$ denotes the set of all maximal ideals of R, then $\mathcal{I}$ is the free abelian monoid with basis $\mathcal{P}$. For $\mathfrak{a} \in \mathcal{I}$, we denote by $[\mathfrak{a}] \in G$ the ideal class containing $\mathfrak{a}$, and we write G additively so that $[\mathfrak{a}\mathfrak{b}] = [\mathfrak{a}] + [\mathfrak{b}]$ for all $\mathfrak{a},\mathfrak{b} \in \mathcal{I}$.

Every element $\alpha \in R^{\#} = R \setminus (R^{\times} \cup \{0\})$ has a factorization $\alpha = u_1 \cdot \cdot \ldots \cdot u_r$, where $u_i \in R$ are irreducible elements of R; we call r the length of the factorization. If $h = 1$, then R is factorial, and the factorization of any $\alpha \in R^{\#}$ into irreducibles is essentially unique (i.e., it is unique up to associated irreducibles and the order of the factors). If $h > 1$, then there are elements $\alpha \in R^{\#}$ with several distinct factorizations, and G is said to measure the deviation of R from being factorial. For concrete results supporting this philosophy see [7] and the literature quoted there.

The arithmetic of R is connected with the arithmetic of the block semigroup $\mathcal{B}(G)$ in the following way (cf. [3]):

For $\alpha \in R^{\#}$, we consider the prime ideal decomposition

$$(\alpha) = \mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_m$$

with $\mathfrak{p}_j \in \mathcal{P}$ and set

$$\boldsymbol{\beta}(\alpha) = [\mathfrak{p}_1] \cdot \ldots \cdot [\mathfrak{p}_m] \in \mathcal{B}(G);$$

$\boldsymbol{\beta}(\alpha)$ is called the block of α. An element $\alpha \in R^{\#}$ is irreducible in R if and only if $\boldsymbol{\beta}(\alpha) \in \mathcal{B}(G)$ is an irreducible block. If $\alpha = u_1 \cdot \ldots \cdot u_r$ is a factorization of α into irreducible elements of R, then $\boldsymbol{\beta}(\alpha) = \boldsymbol{\beta}(u_1) \cdot \ldots \cdot \boldsymbol{\beta}(u_r)$ is a factorization of $\boldsymbol{\beta}(\alpha)$ into irreducible blocks, and every factorization of $\boldsymbol{\beta}(\alpha)$ in $\mathcal{B}(G)$ arises in this way.

Two factorizations

$$\alpha = u_1 \cdot \ldots \cdot u_r, \qquad \alpha = u_1' \cdot \ldots \cdot u_s'$$

of α into irreducible elements of R are called *block-equivalent*, if the corresponding factorizations

$$\boldsymbol{\beta}(\alpha) = \boldsymbol{\beta}(u_1) \cdot \ldots \cdot \boldsymbol{\beta}(u_r), \qquad \boldsymbol{\beta}(\alpha) = \boldsymbol{\beta}(u_1') \cdot \ldots \cdot \boldsymbol{\beta}(u_s')$$

in $\mathcal{B}(G)$ differ at most in the order of their factors. We denote by

$$\mathbf{f}^*(\alpha) = \mathbf{f}\big(\boldsymbol{\beta}(\alpha)\big)$$

the number of not block-equivalent factorizations of α.

Using this terminology, we obtain the following extension of a classical result of L. Carlitz [1].

PROPOSITION 4. *For an algebraic number field K, the following assertions are equivalent:*

i) $h \le 2$.

ii) $\mathbf{f}^*(\alpha) = 1$ *for all* $\alpha \in R^{\#}$.

iii) *For every $\alpha \in R^{\#}$, any two factorizations of α into irreducibles have the same length.*

Proof.

i) $\Longrightarrow$ ii): If $h \le 2$, then $G = \{0, g\}$ and $\mathcal{B}(G)$ is factorial (it is the free abelian monoid with basis $\{0, g^2\}$), and therefore $\mathbf{f}^*(\alpha) = 1$ for all $\alpha \in R^{\#}$.

ii) $\Longrightarrow$ iii): follows from the simple observation that any two block-equivalent factorizations of an element $\alpha \in R^{\#}$ have the same length.

iii) $\Longrightarrow$ i): See [1]. $\square$

The quantities $\mathbf{f}^*(\alpha)$ give rise to the following quantitative results. For $k \in \mathbb{N}$ and $x \in \mathbb{R}_{>0}$, we set

$$B_k(x) = \#\{(\alpha) \in \mathcal{H} \mid \alpha \in R^{\#}, \quad |\mathcal{N}(\alpha)| \le x, \quad \mathbf{f}^*(\alpha) \le k\},$$
$$\bar{B}_k(x) = \#\{(\alpha) \in \mathcal{H} \mid \alpha \in R^{\#}, \quad |\mathcal{N}(\alpha)| \le x, \quad \mathbf{f}^*(\alpha) = k\},$$

and we determine the asymptotic behaviour of these functions as follows.

THEOREM 2. *For $k \in \mathbb{N}$ and $x \ge e^e$, we have*

$$B_k(x) = x(\log x)^{-1+\frac{\rho(G)}{h}} \Big[V_k(\log\log x) + O\big((\log x)^{-\gamma_h}(\log\log x)^M\big)\Big],$$
$$\bar{B}_k(x) = x(\log x)^{-1+\frac{\rho(G)}{h}} \Big[\bar{V}_k(\log\log x) + O\big((\log x)^{-\gamma_h}(\log\log x)^M\big)\Big],$$

where $V_k, \bar{V}_k \in \mathbb{C}[X]$ are polynomials with positive leading coefficient, $\deg V_k = \psi_k(G), \deg \bar{V}_k = \bar{\psi}_k(G), \gamma_h = \dfrac{1}{h}\Big(1 - \cos\dfrac{2\pi}{h}\Big)$, and $M \in \mathbb{N}$ depends on k and K.

Proof. By Theorem 1, we have

$$\mathcal{B}_k(G) = \bigcup_{j=1}^{m} \Omega(Q_j, \sigma_j), \qquad \bar{\mathcal{B}}_k(G) = \bigcup_{i=1}^{r} \Omega(Q_i', \sigma_i')(l_i),$$

where (Q_j, σ_j) and (Q_i', σ_i') are k-systems, $l_i \in \mathbb{N}_0$,

$$\rho(G) = \max\{\#Q_j \mid j = 1, \dots, m\} = \max\{\#Q_i' \mid i = 1, \dots, r\},$$

and

$$\psi_k(G) = \max\{|\sigma_j| \mid j = 1, \dots, m, \quad \#Q_j = \rho(G)\},$$
$$\bar{\psi}_k(G) = \max\{|\sigma_i'| \mid i = 1, \dots, r, \quad \#Q_i' = \rho(G)\}.$$

Now the assertion follows from the following Lemma, due to J. Kaczorowski [11] (Lemma 2 and p. 66/67):

LEMMA 2. *Let $(Q_1,\sigma_1),\dots,(Q_n,\sigma_n)$ be systems in G and $l_1,\dots,l_n \in \mathbb{N}_0$ such that $\Omega(Q_i,\sigma_i)(l_i) \neq \emptyset$ for all $i \in \{1,\dots,n\}$, and set*

$$\Omega = \bigcup_{i=1}^{n} \Omega(Q_i,\sigma_i)(l_i).$$

Then we have, for $x \geq e^e$,

$$\begin{aligned}\#\{(\alpha) \in \mathcal{H} \mid \ \alpha \in R^{\#}, \quad |\mathcal{N}(\alpha)| \leq x, \quad \beta(\alpha) \in \Omega\}& \\ = x(\log x)^{-1+\frac{\rho}{h}} \Big[V(\log\log x) + O\big((\log x)^{-\gamma_h}(\log\log x)^M\big)\Big]&,\end{aligned}$$

where

$$\rho = \max\{\#Q_i \mid \ i = 1,\dots,n\},$$

$V \in \mathbb{C}[X]$ is a polynomial with positive leading coefficient and

$$\deg V = \max\{|\sigma_i| \mid \ i = 1,\dots,n, \quad \#Q_i = \rho_i\},$$

$\gamma_h = \dfrac{1}{h}\Big(1 - \cos\dfrac{2\pi}{h}\Big)$ and $M = M(\Omega) \in \mathbb{N}$.

There are several other functions connected with non-unique factorizations in algebraic number fields whose asymptotic behaviour has been investigated. For $\alpha \in R^{\#}$, let $\mathbf{f}(\alpha)$ be the number of essentially distinct factorizations of α into irreducible elements of R and $\mathbf{l}(\alpha)$ the number of distinct lengths of such factorizations. Among others, the following functions were considered:

$$\begin{aligned}
F_k(x) &= \#\{(\alpha) \in \mathcal{H} \mid \ \alpha \in R^{\#}, \quad |\mathcal{N}(\alpha)| \leq x, \quad \mathbf{f}(\alpha) \leq k\},\\
\bar{F}_k(x) &= \#\{(\alpha) \in \mathcal{H} \mid \ \alpha \in R^{\#}, \quad |\mathcal{N}(\alpha)| \leq x, \quad \mathbf{f}(\alpha) = k\},\\
G_k(x) &= \#\{(\alpha) \in \mathcal{H} \mid \ \alpha \in R^{\#}, \quad |\mathcal{N}(\alpha)| \leq x, \quad \mathbf{l}(\alpha) \leq k\},\\
\bar{G}_k(x) &= \#\{(\alpha) \in \mathcal{H} \mid \ \alpha \in R^{\#}, \quad |\mathcal{N}(\alpha)| \leq x, \quad \mathbf{l}(\alpha) = k\}.
\end{aligned}$$

All these functions have, for $x \to \infty$, an asymptotical behaviour of the form

$$\big(C + o(1)\big)x(\log x)^{-1+q}(\log\log x)^d,$$

where $C > 0$, $0 < q < 1$ and $d \in \mathbb{N}$. This was shown

- for F_k in [14] (with $q = \dfrac{1}{h}$); d was investigated in [12] and [15],
- for $\bar{F}_k$ in [5] and [9] (with $q = \dfrac{1}{h}$),
- for G_k and $\bar{G}_k$ in [16] and [4].

In any case, the remainder term $o(1)$ can be made more precise by means of the method of Kaczorowski [11]. All results (also these for B_k and $\bar{B}_k$) remain valid in the general context of formations as introduced in [10].

§3. The invariants $\psi_k(G)$ and $\bar{\psi}_k(G)$

Let again G be a finite abelian group and $\#G \geq 3$. For $k \in \mathbb{N}$, we denote by $D_k(G)$ the generalized Davenport constant [8], which is defined as follows:

$D_k(G)$ is the minimal number such that, for every

$$S = \prod_{g \in G} g^{v_g(S)} \in \mathcal{F}(G)$$

satisfying

$$\sum_{g \in G} v_g(S) \geq D_k(G),$$

there exist irreducible blocks $B_1, \ldots, B_k \in \mathcal{B}(G)$ such that

$$S = B_1 \cdot \ldots \cdot B_k S'$$

for some $S' \in \mathcal{F}(G)$.

Proposition 5.

i) *If e is the exponent of G, then we have, for $k \in \mathbb{N}$,*

$$\psi_k(G) \leq \sum_{0 \neq g \in G} \big(\mathrm{ord}(g) - 1\big) + (k-1)e - \rho(G) + 1 .$$

ii) *If G is an elementary group, then we have, for $k \in \mathbb{N}$,*

$$\psi_k(G) \leq D_k(G) - 1 .$$

Proof. We assume that there exists a subset $Q \subset G$ and a function $\sigma \colon G \setminus Q \to \mathbb{N}_0$ such that (Q, σ) is a k-system, $\#Q = \rho(G)$, and $|\sigma|$ exceeds the bounds given in the Proposition.

i) Suppose that $|\sigma| > \sum_{0 \neq g \in G} \big(\mathrm{ord}(g) - 1\big) + (k-1)e - \rho(G) + 1$, $l \geq ke$ and $B \in \Omega(Q, \sigma)(l) \subset \mathcal{B}_k(G)$. We assert that there exist elements $a_1, \ldots, a_k \in G \setminus Q$ such that $d_i = \mathrm{ord}(a_i)$ and $B = a_1^{d_1} \cdot \ldots \cdot a_k^{d_k} B'$ for some $B' \in \mathcal{B}(G)$. Indeed, if $i \in \{1, \ldots, k\}$ and $a_1, \ldots, a_{i-1} \in G \setminus Q$ are such that $B = a_1^{d_1} \cdot \ldots \cdot a_{i-1}^{d_{i-1}} B_i$ for some $B_i \in \mathcal{B}(G)$, then

$$\begin{aligned} \sum_{g \in G \setminus Q} v_g(B_i) &= \sum_{g \in G \setminus Q} v_g(B) - d_1 - \cdots - d_{i-1} \geq |\sigma| - (i-1)e \\ &> \sum_{0 \neq g \in G} \big(\mathrm{ord}(g) - 1\big) - \big(\rho(G) - 1\big) \geq \sum_{g \in G \setminus Q} \big(\mathrm{ord}(g) - 1\big), \end{aligned}$$

and therefore there exists an element $a_i \in G \setminus Q$ such that $B_i = a_i^{d_i} B_i'$ for some $B_i' \in \mathcal{B}(G)$.

It follows that B is divisible by a block B_0 of the form

$$B_0 = a_1^{d_1} \cdot \ldots \cdot a_k^{d_k} \cdot \prod_{g \in Q} g^{ke},$$

and hence $\mathbf{f}(B_0) \le \mathbf{f}(B) \le k$.

Since Q is a maximal independent subset of G, the subgroup $\langle Q \rangle$ of G is essential (Lemma 1), and therefore we obtain relations

$$-m_i a_i = \sum_{g \in G} n_{g,i} g \qquad (i = 1, \ldots, k),$$

where $1 \le m_i < d_i$ and $0 \le n_{g,i} < \operatorname{ord}(g) \le e$. If we choose these relations so that, for each i, $m_i + \sum\limits_{g \in Q} n_{g,i}$ is minimal, then the blocks

$$C_i = a_i^{m_i} \cdot \prod_{g \in Q} g^{n_{g,i}} \in \mathcal{B}(G)$$

are irreducible. Now we obtain, for $j = 0, 1, \ldots, k$,

$$B_0 = C_1 \cdot \ldots \cdot C_j a_{j+1}^{d_{j+1}} \cdot \ldots \cdot a_k^{d_k} \cdot \prod_{g \in Q} g^{ke - \sum_{i=1}^{j} n_{g,i}} \cdot \prod_{i=1}^{j} a_i^{d_i - m_i},$$

and therefore $\mathbf{f}(B_0) \ge k + 1$, a contradiction.

ii) Let G be elementary, $|\sigma| \ge D_k(G)$, $l \ge ke$ and $B \in \Omega(Q, \sigma)(l) \subset \mathcal{B}_k(G)$. By definition of $D_k(G)$, there exist irreducible blocks $A_1, \ldots, A_k \in \mathcal{B}(G \setminus Q)$ such that $A_1 \cdot \ldots \cdot A_k$ divides B. Therefore B is also divisible by a block B_0 of the form

$$B_0 = A_1 \cdot \ldots \cdot A_k \cdot \prod_{g \in Q} g^{ke},$$

and hence $\mathbf{f}(B_0) \le \mathbf{f}(B) \le k$. For every $i \in \{1, \ldots, k\}$, let $a_i \in G \setminus Q$ be an element satisfying $v_{a_i}(A_i) > 0$, and set $A_i = a_i A_i'$. By Lemma 1, $\langle Q \rangle$ is an essential subgroup of G, and since G is elementary, we have $\langle Q \rangle = G$. Therefore there exist relations of the form

$$-a_i = \sum_{g \in Q} n_{g,i} g \qquad (i = 1, \ldots, k),$$

where $0 \le n_{g,i} < \operatorname{ord}(g) \le e$, and the blocks

$$C_i = a_i \cdot \prod_{g \in Q} g^{n_{g,i}} \in \mathcal{B}(G)$$

are irreducible. Now we obtain, for $j = 0, 1, \ldots, k$,

$$B_0 = C_1 \cdot \ldots \cdot C_j A_{j+1} \cdot \ldots \cdot A_k \cdot \prod_{g \in Q} g^{ke - \sum_{i=1}^{j} n_{g,i}} \cdot A_1' \cdot \ldots \cdot A_j',$$

and therefore $\mathbf{f}(B_0) \ge k + 1$, a contradiction. □

Proposition 5 ii) becomes false if G is not elementary. For $G = C_{p^r}$, this is shown by the next result; by [8], we have $D_k(C_{p^r}) = kp^r$.

PROPOSITION 6. *Let p be a prime, $k, r \in \mathbb{N}$ and $r \ge 2$. Then*

$$\bar{\psi}_k(C_{p^r}) \ge kp^r - 1 + (r-1)(p-1).$$

Proof. For $C_{p^r} = \langle g_0 \rangle$, we set $Q = \{0, p^{r-1} g_0\}$, and we define $\sigma \colon G \setminus Q \to \mathbb{N}_0$ by

$$\sigma(g) = \begin{cases} kp^r - 1, & \text{if } g = -g_0, \\ p - 1, & \text{if } g = p^\nu g_0 \text{ for some } \nu \in \{0, 1, \ldots, r-2\}, \\ 0 & \text{otherwise.} \end{cases}$$

We shall prove that $\Omega(Q, \sigma)(kp - 1) \subset \bar{\mathcal{B}}_k(C_{p^r})$; since $\#Q = 2 = \rho(C_{p^r})$, this implies $\bar{\psi}_k(C_{p^r}) \ge |\sigma| = kp^r - 1 + (r-1)(p-1)$. If $B \in \Omega(Q, \sigma)(kp - 1)$, then

$$B = (-g_0)^{kp^r - 1} \cdot \prod_{\nu=0}^{r-2} (p^\nu g_0)^{p-1} (p^{r-1} g_0)^{np-1} (0)^m,$$

where $m, n \in \mathbb{N}_0$, $m \ge kp - 1$, $n \ge k$. We shall prove that, for every $j \in \{1, \ldots, r\}$, all blocks of the form

$$B_j = (-g_0)^{kp^r - p^{r-j}} \cdot \prod_{\nu=r-j}^{r-2} (p^\nu g_0)^{p-1} (p^{r-1} g_0)^{np-1} (0)^m,$$

($m, n \ge k$) lie in $\bar{\mathcal{B}}_k(C_{p^r})$ (for $j = r$, the assertion follows).

We use induction on j. For $j = 1$, we have

$$B_1 = (-g_0)^{kp^r - p^{r-1}} (p^{r-1} g_0)^{np-1} (0)^m ;$$

the irreducible blocks dividing B_1 are $A_0 = (-g_0)^{p^r}$, $A_1 = (-g_0)^{p^{r-1}} (p^{r-1} g_0)$, $A_2 = (p^{r-1} g_0)^p$ and (0). Therefore all factorizations of B_1 into irreducibles are given by

$$B_1 = A_0^{j_0} A_1^{j_1} A_2^{j_2} (0)^m ,$$

where $j_i \in \mathbb{N}_0$ are such that $p^r j_0 + p^{r-1} j_1 = kp^r - p^{r-1}$ and $j_1 + pj_2 = np - 1$, i.e., $j_1 = jp - 1$ for $1 \le j \le k$ and $j_0 = k - j$, $j_2 = n - j$; this implies $\mathbf{f}(B_1) = k$.

Suppose now that $2 \le j \le r$ and $B_{j-1} \in \bar{\mathcal{B}}_k(G)$. There is only one irreducible block C_j dividing B_j for which $v_{p^{r-j} g_0}(C_j) > 0$, namely $C_j = (p^{r-j} g_0)(-g_0)^{p^{r-j}}$. Therefore C_j^{p-1} occurs in every factorization of B_j, and since $B_j = C_j^{p-1} B_{j-1}$, we infer $\mathbf{f}(B_j) = \mathbf{f}(B_{j-1}) = k$. □

PROPOSITION 7.

i) *If* $G = G_1 \oplus G_2$, $\#G_i \ge 3$ *and* $k_i \in \mathbb{N}$ *for* $i = 1, 2$, *then*

$$\bar{\psi}_{k_1 k_2}(G_1 \oplus G_2) \ge \bar{\psi}_{k_1}(G_1) + \bar{\psi}_{k_2}(G_2) \quad \textit{and}$$
$$\psi_{k_1 k_2}(G_1 \oplus G_2) \ge \psi_{k_1}(G_1) + \psi_{k_2}(G_2) .$$

ii) *If* $G_0 < G$ *is a subgroup and* $k \in \mathbb{N}$, *then*

$$\bar{\psi}_k(G) \ge \bar{\psi}_k(G_0) \qquad \textit{and} \qquad \psi_k(G) \ge \psi_k(G_0) .$$

Proof.

i) It is sufficient to prove the assertion for $\bar{\psi}$, since then we have

$$\begin{aligned} \psi_{k_1 k_2}(G_1 \oplus G_2) &= \max\{\bar{\psi}_j(G_1 \oplus G_2) \mid 1 \le j \le k_1 k_2\} \\ &\ge \max\{\bar{\psi}_{j_1 j_2}(G_1 \oplus G_2) \mid 1 \le j_1 \le k_1 , 1 \le j_2 \le k_2\} \\ &\ge \max\{\bar{\psi}_{j_1}(G_1) + \bar{\psi}_{j_2}(G_2) \mid 1 \le j_1 \le k_1 , 1 \le j_2 \le k_2\} \\ &= \sum_{i=1}^{2} \max\{\bar{\psi}_{j_i}(G_i) \mid 1 \le j_i \le k_i\} = \psi_{k_1}(G_1) + \psi_{k_2}(G_2) . \end{aligned}$$

We may suppose that $G_1 \subset G$ and $G_2 \subset G$. For $i = 1, 2$ let $Q_i \subset G_i$ be an independent subset and $\sigma_i : G_i \setminus Q_i \to \mathbb{N}_0$ a function such that $\#Q_i = \rho(G_i)$,

$|\sigma_i| = \bar{\psi}_{k_i}(G_i)$ and (Q_i, σ_i) is a k_i-system with $\Omega(Q_i, \sigma_i) \cap \bar{\mathcal{B}}_{k_i}(G_i) \neq \emptyset$. Then $Q_1 \cup Q_2$ is an independent subset of G, and $\#(Q_1 \cup Q_2) = \#Q_1 + \#Q_2 - 1 = \rho(G)$. We define $\sigma\colon G \setminus (Q_1 \cup Q_2) \to \mathbb{N}_0$ by

$$\sigma(g) = \begin{cases} \sigma_1(g), & \text{if } \; g \in G_1 \setminus Q_1, \\ \sigma_2(g), & \text{if } \; g \in G_2 \setminus Q_2, \\ 0 & \text{otherwise.} \end{cases}$$

Then we have $|\sigma| = |\sigma_1| + |\sigma_2|$, and every block $B \in \Omega(Q_1 \cup Q_2, \sigma)$ has the form $B = B_1 B_2$, where $B_i \in \Omega(Q_i, \sigma_i)$. This implies $\mathbf{f}(B) = \mathbf{f}(B_1)\mathbf{f}(B_2)$ and therefore $\Omega(Q_1 \cup Q_2, \sigma)$ is a $k_1 k_2$-system with

$$\Omega(Q_1 \cup Q_2, \sigma) \cap \bar{\mathcal{B}}_{k_1 k_2}(G_1 \oplus G_2) \neq \emptyset \qquad \text{and}$$
$$\bar{\psi}_{k_1 k_2}(G) \geq |\sigma| = \bar{\psi}_{k_1}(G_1) + \bar{\psi}_{k_2}(G_2).$$

ii) Again it suffices to show the assertion for $\bar{\psi}$. Let $Q_0 \subset G_0$ be an independent subset and $\sigma_0\colon G_0 \setminus Q_0 \to \mathbb{N}_0$ a function such that $\#Q_0 = \rho(G_0)$, $|\sigma_0| = \bar{\psi}_k(G_0)$ and $\Omega(Q_0, \sigma_0) \cap \bar{\mathcal{B}}_k(G_0) \neq \emptyset$. By Proposition 1, Q_0 contains only elements of prime power order. Let $Q_0 \subset Q \subset G$ be such that Q is a maximal independent subset containing only elements of prime power order, and define $\sigma\colon G \setminus Q \to \mathbb{N}_0$ by $\sigma|_{G_0 \setminus Q_0} = \sigma_0$ and $\sigma|_{G \setminus (G_0 \cup Q)} = 0$. Then $\#Q = \rho(G)$ by Proposition 1, and every block $B \in \Omega(Q, \sigma)$ has the form

$$B = \prod_{g \in Q} g^{n_g} \cdot \prod_{g \in G_0 \setminus Q_0} g^{\sigma_0(g)},$$

where $n_g \in \mathbb{N}_0$.

We contend that an element

$$B_1 = \prod_{g \in Q} g^{n_g} \cdot \prod_{g \in G_0 \setminus Q_0} g^{m_g} \in \mathcal{F}(G)$$

(where $m_g, n_g \in \mathbb{N}_0$) is a block if and only if

$$B_1^* = \prod_{g \in Q_0} g^{n_g} \cdot \prod_{g \in G_0 \setminus Q_0} g^{m_g} \in \mathcal{B}(G_0), \qquad \text{and} \quad n_g \equiv 0 \mod \operatorname{ord}(g)$$

for all $g \in Q \setminus Q_0$. Indeed, if B_1 is of the indicated form, then it is a block. Conversely, if

$$\sum_{g \in Q} n_g g + \sum_{g \in G_0 \setminus Q_0} m_g g = 0,$$

then we obtain

$$g^* = \sum_{g \in Q \setminus Q_0} n_g g \in G_0 \,.$$

If $g^* = 0$, then $n_g \equiv 0 \mod \operatorname{ord}(g)$ for all $g \in Q \setminus Q_0$, and the assertion follows. If $g^* \neq 0$, then there exists an integer $d \in \mathbb{N}$ such that $0 \neq dg^* \in \langle Q_0 \rangle$, since $\langle Q_0 \rangle$ is an essential subgroup of G_0. This implies

$$\sum_{g \in Q \setminus Q_0} dn_g g = \sum_{g \in Q_0} e_g g \neq 0$$

(where $e_g \in \mathbb{N}_0$), which contradicts the independence of Q.

Now every block $B \in \Omega(Q, \sigma)$ is of the form

$$B = \prod_{g \in Q \setminus Q_0} g^{m_g \operatorname{ord}(g)} \cdot B_0 \,,$$

where $B_0 \in \Omega(Q_0, \sigma_0)$ and $m_g \in \mathbb{N}_0$, and for every $g \in Q \setminus Q_0$, $g^{\operatorname{ord}(g)}$ is the only block dividing B and containing g. This implies $\mathbf{f}(B) = \mathbf{f}(B_0)$, and since $B_0 \in \Omega(Q_0, \sigma_0)$ can be prescribed arbitrarily, we infer $\Omega(Q, \sigma) \cap \bar{\mathcal{B}}_k(G) \neq \emptyset$, whence $\bar{\psi}_k(G) \geq |\sigma| = |\sigma_0| = \bar{\psi}_k(G_0)$. □

COROLLARY 1.

i) *If p is a prime dividing $\#G$, e the exponent of G and $k \in \mathbb{N}$, then*

$$-1 + kp \leq \bar{\psi}_k(G) \leq \psi_k(G) \leq a + ke$$

for some $a \in \mathbb{N}$.

ii) $\psi_k(G) = \bar{\psi}_k(G)$ *for infinitely many $k \in \mathbb{N}$.*

Proof.

i) We start with the left inequality. By Proposition 7 ii) it is sufficient to prove that $\bar{\psi}_k(C_p) \geq kp - 1$, if $p > 2$, $\bar{\psi}_k(C_4) \geq 2k - 1$ and $\bar{\psi}_k(C_2 \oplus C_2) \geq 2k - 1$. But these inequalities follow immediately from Proposition 2.

Obviously $\bar{\psi}_k(G) \leq \max\{\bar{\psi}_j(G) \mid 1 \leq j \leq k\} = \psi_k(G)$. The right inequality is a consequence of Proposition 5 i).

ii) Since $\bar{\psi}_k(G)$ tends to infinity with k and $\psi_k(G) = \max\{\bar{\psi}_j(G) \mid 1 \leq j \leq k\}$, we infer $\psi_k(G) = \bar{\psi}_k(G)$ for infinitely many $k \in \mathbb{N}$. □

PROPOSITION 8. *Let $k, r \in \mathbb{N}$ and $p > 2$ be a prime.*

i) $\psi_k(C_p^r) \geq \bar{\psi}_k(C_p^r) \geq (k + r - 1)p - r$.

ii) *If $k = 1$ or $r \leq 2$, then*

$$\psi_k(C_p^r) = \bar{\psi}_k(C_p^r) = (k + r - 1)p - r.$$

Proof.

i) We do the proof by induction on r. For $r = 1$ Corollary 1 implies $\bar{\psi}_k(C_p) \geq kp - 1$. For $r \geq 2$ we obtain by Proposition 7 i) that

$$\bar{\psi}_k(C_p^r) \geq \bar{\psi}_k(C_p^{r-1}) + \bar{\psi}_1(C_p) \geq (k+r-2)p-(r-1)+p-1 = (k+r-1)p-r.$$

ii) By Proposition 5 i) we have $\psi_k(C_p^r) \leq D_k(C_p^r) - 1$. For $k = 1$ or $r \leq 2$ $D_k(C_p^r) = kp + (r - 1)(p - 1)$ ([8]) and so the assertion follows. □

PROPOSITION 9. *For $k, r \in \mathbb{N}$, $r \geq 2$ we have*

i) $\psi_k(C_2^r) \geq \bar{\psi}_k(C_2^r) \geq \left[\frac{r}{2}\right] + 2k - 2$.

ii) *If $k = 1$ or $r = 2$, then*

$$\psi_k(C_2^r) = \bar{\psi}_k(C_2^r) = \left[\frac{r}{2}\right] + 2k - 2.$$

Proof.

i) By Proposition 7 ii) it suffices to show the assertion for even r. We set $r = 2s$ and do the proof by induction on s. Corollary 1 i) gives the assertion for $s = 1$. Let $s \geq 2$; using Proposition 7 i) we obtain

$$\begin{aligned}\bar{\psi}_k(C_2^{2s}) &= \bar{\psi}_k\big((C_2 \oplus C_2)^s\big) \geq \bar{\psi}_k\big((C_2 \oplus C_2)^{s-1}\big) + \bar{\psi}_1(C_2 \oplus C_2) \\ &\geq s - 1 + 2k - 2 + 1 = s + 2k - 2.\end{aligned}$$

ii) *Case* 1. $r = 2$: Let $G = C_2 \oplus C_2$ and $Q = \{0, g_1, g_2\}$ a maximal independent subset of G; then $G \setminus Q = \{g_1 + g_2\}$. Therefore we must prove that a block of the form

$$B = g_1^{n_1} g_2^{n_2} (g_1 + g_2)^m,$$

where $n_1, n_2, m \in \mathbb{N}_0$, $n_1 + m \equiv n_2 + m \equiv 0 \mod 2$ satisfies $\mathbf{f}(B) \leq k$ if and only if $m \leq 2k - 1$. This is done in essentially the same way as Case 3 in the proof of Proposition 2.

Case 2. $k = 1$: Let $Q \subset C_2^r$ be an independent subset such that $\#Q = \rho(C_2^r) = r+1$; then Q is of the form $Q = \{0, g_1, \ldots, g_r\}$, where $\langle g_1, \ldots, g_r \rangle = C_2^r$.

Now let $\sigma \colon G \setminus Q \to \mathbb{N}_0$ be any function such that (Q, σ) is a 1-system, and set $m = |\sigma| \in \mathbb{N}_0$; we shall prove that $m \leq \left[\frac{r}{2}\right]$. For a subset $J \subset \{1, \ldots, r\}$, we set $g_J = \sum\limits_{j \in J} g_j$; then we have

$$G \setminus Q = \{g_J \mid J \subset \{1, \ldots, r\}, \quad \#J \geq 2\}.$$

We contend that $\sigma(g) \leq 1$ for all $g \in G \setminus Q$. Indeed, if $\sigma(g) \geq 2$ and $g = g_J$ for some $J \subset \{1, \ldots, r\}$, $\#J \geq 2$, then there exists a block $B \in \Omega(Q, \sigma)$ which is of the form

$$B = g_J^2 \cdot \prod_{j \in J} g_j^2 \cdot B_0$$

for some $B_0 \in \mathcal{B}(G)$, and since

$$g_J^2 \cdot \prod_{j \in J} g_j^2 = \Big(g_J \cdot \prod_{j \in J} g_j\Big)^2,$$

we obtain $\mathbf{f}(B) \geq 2$.

Therefore there exist subsets $J_1, \ldots, J_m$ of $\{1, \ldots, r\}$ such that $\#J_\mu \geq 2$ for all μ and $\sigma(g) = 1$ if and only if $g = g_{J_\mu}$ for some $\mu \in \{1, \ldots, m\}$. We contend that $J_\mu \cap J_\nu = \emptyset$ for all $\mu \neq \nu$. Indeed, if $\mu \neq \nu$ and $J_0 = J_\mu \cap J_\nu \neq \emptyset$, then there exists a block $B \in \Omega(Q, \sigma)$, which is of the form

$$B = \prod_{j \in J_\mu} g_j \prod_{j \in J_\nu} g_j \cdot g_{J_\mu} g_{J_\nu} \cdot B_0$$

for some $B_0 \in \mathcal{B}(G)$, and since

$$\Big(g_{J_\mu} \cdot \prod_{j \in J_\mu} g_j\Big)\Big(g_{J_\nu} \cdot \prod_{j \in J_\nu} g_j\Big) = \Big(g_{J_\mu} g_{J_\nu} \prod_{j \in J_\mu \setminus J_0} g_j \prod_{j \in J_\nu \setminus J_0} g_j\Big) \cdot \prod_{j \in J_0} g_j^2,$$

we infer $\mathbf{f}(B) \geq 2$.

Now we obtain

$$r \geq \sum_{\mu=1}^{m} \#J_\mu \geq 2m,$$

and hence $m \leq \left[\frac{r}{2}\right]$, as asserted. $\square$

REFERENCES

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

[2] FUCHS, L.: *Infinite Abelian Groups*, Academic Press, Address of publisher, 1970.

[3] GEROLDINGER, A.: *Über nicht-eindeutige Zerlegungen in irreduzible Elemente*, Math. Z. **197** (1988), 505–529.

[4] GEROLDINGER, A.: *Ein quantitatives Resultat über Faktorisierungen verschiedener Länge in algebraischen Zahlkörpern*, Math. Z. **205** (1990), 159–162.

[5] GEROLDINGER, A.: *Factorization of natural numbers in algebraic number fields*, Acta Arith. **57** (1991), 365–373.

[6] GEROLDINGER, A.—HALTER-KOCH, F.: *Realization Theorems for semigroups with divisor theory*, Semigroup Forum **44** (1992), 229–237.

[7] HALTER-KOCH, F.: *Halbgruppen mit Divisorentheorie*, Exposition. Math. **8** (1990), 27–66.

[8] HALTER-KOCH, F.: *A generalization of Davenport's constant and its arithmetical applications*, Colloq. Math. **63** (1992), 203–210.

[9] HALTER-KOCH, F.: *Typenhalbgruppen und Faktorisierungsprobleme*, Resultate Math. **22** (1992), 545–559.

[10] HALTER-KOCH, F.—MÜLLER, W.: *Quantitative aspects of non-unique factorization: A general theory with applications to algebraic function fields*, J. Reine Angew. Math. **421** (1991), 159–188.

[11] KACZOROWSKI, J.: *Some remarks on factorization in algebraic number fields*, Acta Arith. **43** (1983), 53–68.

[12] NARKIEWICZ, W.: *Finite abelian groups and factorization problems*, Colloq. Math. **42** (1979), 319–330.

[13] NARKIEWICZ, W.: *Elementary and Analytic Theory of Algebraic Numbers*, Springer, Address of Publisher, 1990.

[14] NARKIEWICZ, W.: *Numbers with unique factorization in an algebraic number field*, Acta Arith. **21** (1972), 313–322.

[15] NARKIEWICZ, W.—ŚLIWA, J.: *Finite abelian groups and factorization problems, II*, Colloq. Math. **46** (1982), 115–122.

[16] ŚLIWA, J.: *Factorizations of distinct lenghts in algebraic number fields*, Acta Arith. **31** (1976), 399–417.

Received September 6, 1991

Institut für Mathematik
Karl-Franzens-Universität
Heinrichstraße 36/IV
A-8010 Graz
Österreich