# C OLLOQUIUM MATHEMATICUM <br> VOL. LXIII $1992 \quad$ FASC. 2 

## a generalization of davenport's Constant AND ITS ARITHMETICAL APPLICATIONS

BY
FRANZ HALTER-KOCH (GRAZ)

1. For an additively written finite abelian group $G$, Davenport's constant $D(G)$ is defined as the maximal length $d$ of a sequence $\left(g_{1}, \ldots, g_{d}\right)$ in $G$ such that $\sum_{j=1}^{d} g_{j}=0$, and $\sum_{j \in J} g_{j} \neq 0$ for all $\emptyset \neq J \varsubsetneqq\{1, \ldots, d\}$. It has the following arithmetical meaning:

Let $K$ be an algebraic number field, $R$ its ring of integers and $G$ the ideal class group of $R$. Then $D(G)$ is the maximal number of prime ideals (counted with multiplicity) which can divide an irreducible element of $R$. This fact was first observed by H. Davenport (1966) and worked out by W. Narkiewicz [8] and A. Geroldinger [4].

For a subset $Z \subset R$ and $x>1$ we denote by $Z(x)$ the number of principal ideals $(\alpha)$ of $R$ with $\alpha \in Z$ and $(R:(\alpha)) \leq x$. If $M$ denotes the set of irreducible integers of $R$, then it was proved by P. Rémond [12] that, as $x \rightarrow \infty$,

$$
M(x) \sim C x(\log x)^{-1}(\log \log x)^{D(G)-1}
$$

where $C>0$ depends on $K$; the error term in this asymptotic formula was investigated by J. Kaczorowski [7].

If an element $\alpha \in R \backslash\left(R^{\times} \cup\{0\}\right)$ has a factorization $\alpha=u_{1} \cdot \ldots \cdot u_{r}$ into irreducible elements $u_{j} \in R$, we call $r$ the length of that factorization and denote by $L(\alpha)$ the set of all lengths of factorizations of $\alpha$. For $k \geq 1$, we define sets $M_{k}$ and $M_{k}^{\prime}$ (depending on $K$ ) as follows:
$M_{k}$ consists of all $\alpha \in R \backslash\left(R^{\times} \cup\{0\}\right)$ for which $\max L(\alpha) \leq k$ (i.e., $\alpha$ has no factorization of length $r>k)$;
$M_{k}^{\prime}$ consists of all $\alpha \in R \backslash\left(R^{\times} \cup\{0\}\right)$ for which $\min L(\alpha) \leq k$ (i.e., $\alpha$ has a factorization of length $r \leq k)$.

If $G=\{0\}$, then $M_{k}=M_{k}^{\prime}$ for all $k$; in the general case, we have $M_{1}=M_{1}^{\prime}=M$ and $M_{k} \subset M_{k}^{\prime}$ for all $k$.

In this paper, we generalize the results of Rémond and Kaczorowski and obtain asymptotic formulas for $M_{k}(x)$ and $M_{k}^{\prime}(x)$. To do this, we shall define a sequence of combinatorial constants $D_{k}(G)(k \geq 1)$ generalizing $D(G)=D_{1}(G)$, and we shall obtain the following result.

Theorem. For $x \geq e^{e}$ and $q \in \mathbb{Z}, 0 \leq q \leq c_{0} \frac{\sqrt{\log x}}{\log \log x}$, we have

$$
M_{k}(x)=\frac{x}{\log x}\left[\sum_{\mu=0}^{q} \frac{W_{\mu}(\log \log x)}{(\log x)^{\mu}}+O\left(\left(c_{1} q\right)^{q} \frac{(\log \log x)^{D_{k}(G)}}{(\log x)^{q+1}}\right)\right]
$$

and

$$
M_{k}^{\prime}(x)=\frac{x}{\log x}\left[\sum_{\mu=0}^{q} \frac{W_{\mu}^{\prime}(\log \log x)}{(\log x)^{\mu}}+O\left(\left(c_{1} q\right)^{q} \frac{(\log \log x)^{k D(G)}}{(\log x)^{q+1}}\right)\right]
$$

where $c_{0}, c_{1}$ are positive constants, and $W_{\mu}, W_{\mu}^{\prime} \in \mathbb{C}[X]$ are polynomials such that $\operatorname{deg} W_{\mu} \leq D_{k}(G), \operatorname{deg} W_{\mu}^{\prime} \leq k D(G), \operatorname{deg} W_{0}=D_{k}(G)-1, \operatorname{deg} W_{0}^{\prime}=$ $k D(G)-1$, and $W_{0}$, $W_{0}^{\prime}$ have positive leading coefficients.

Remarks. 1) For $k=1$, this is [7, Theorem 1].
2) For $G=\{0\}$, we shall see that $D_{k}(G)=k$, and we rediscover $[9$, Ch. IX, § 1, Corollary 1].
3) In another context, the number $M_{k}^{\prime}(x)$ was studied in [6].

The main part of this paper is devoted to the definition and the investigation of the invariants $D_{k}(G)$ and is of purely combinatorial nature. Only in the final section shall we present a proof of the above Theorem using the work of Kaczorowski.
2. Let $G$ be an additively written finite abelian group. We denote by $\mathcal{F}(G)$ the (multiplicatively written) free abelian semigroup with basis $G$. In $\mathcal{F}(G)$, we use the concept of divisibility in the usual way: $S^{\prime} \mid S$ if $S=S^{\prime} S^{\prime \prime}$ for some $S^{\prime \prime} \in \mathcal{F}(G)$. Every $S \in \mathcal{F}(G)$ has a unique representation

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

with $v_{g}(S) \in \mathbb{N}_{0}$; we call

$$
\sigma(S)=\sum_{g \in G} v_{g}(S) \in \mathbb{N}_{0}
$$

the size and

$$
\iota(S)=\sum_{g \in G} v_{g}(S) \cdot g \in G
$$

the content of $S$. The semigroup

$$
\mathcal{B}(G)=\{B \in \mathcal{F}(G) \mid \iota(B)=0\} \subset \mathcal{F}(G)
$$

is called the block semigroup of $G$; we set $\mathcal{B}(G)^{\prime}=\mathcal{B}(G) \backslash\{1\}$ where $1 \in \mathcal{F}(G)$ denotes the unit element. Every $B \in \mathcal{B}(G)^{\prime}$ has a factorization $B=B_{1} \cdot \ldots \cdot B_{r}$ into irreducible blocks $B_{i} \in \mathcal{B}(G)^{\prime} ;$ again, we call $r$ the length
of the factorization and denote by $L(B)$ the set of all lengths of factorizations of $B$ in $\mathcal{B}(G)$. Obviously, $B$ is irreducible if and only if $L(B)=\{1\}$, and $D(G)=\max \left\{\sigma(B) \mid B \in \mathcal{B}(G)^{\prime}\right.$ is irreducible $\}$.

Now we define, for $k \geq 1$,

$$
D_{k}(G)=\sup \left\{\sigma(B) \mid B \in \mathcal{B}(G)^{\prime}, \max L(B) \leq k\right\}
$$

Obviously, $D_{1}(G)=D(G)$, and we shall see in a moment that $D_{k}(G)<\infty$ for all $k \geq 1$.

Proposition 1. Let $G$ be a finite abelian group and $k \in \mathbb{N}$.
(i) $k D(G)=\max \left\{\sigma(B) \mid B \in \mathcal{B}(G)^{\prime}, \min L(B) \leq k\right\}$

$$
=\max \left\{\sigma(B) \mid B \in \mathcal{B}(G)^{\prime}, k \in L(B)\right\} .
$$

(ii) $D_{k}(G) \leq k D(G)<\infty$.
(iii) $D_{k}(G)=\max \left\{\sigma(B) \mid B \in \mathcal{B}(G)^{\prime}, \max L(B)=k\right\}$.
(iv) $D_{k}(G)$ is the smallest number $d \in \mathbb{N}$ with the property that, for every $S \in \mathcal{F}(G)$ with $\sigma(S) \geq d$, there exist blocks $B_{1}, \ldots, B_{k} \in \mathcal{B}(G)^{\prime}$ such that $B_{1} \cdot \ldots \cdot B_{k} \mid S$.
(v) If $B \in \mathcal{B}(G)$ is a block satisfying $\sigma(B)>k D(G)$, then there exist blocks $B_{1}, \ldots, B_{k+1} \in \mathcal{B}(G)^{\prime}$ such that $B=B_{1} \cdot \ldots \cdot B_{k+1}$.
(vi) If $G_{1} \nsubseteq G$ is a proper subgroup, then $D_{k}\left(G_{1}\right)<D_{k}(G)$.

Proof. (i) If $B \in \mathcal{B}(G)^{\prime}$ is a block such that $\min L(B) \leq k$, then there exists a factorization $B=B_{1} \cdot \ldots \cdot B_{l}$ into irreducible blocks $B_{j} \in \mathcal{B}(G)^{\prime}$ of length $l \leq k$, and therefore

$$
\sigma(B)=\sum_{j=1}^{l} \sigma\left(B_{j}\right) \leq D(G) \leq k D(G)
$$

Hence it is sufficient to prove that there exists a block $B \in \mathcal{B}(G)$ such that $\sigma(B)=k D(G)$ and $k \in L(B)$. But if $B_{0} \in \mathcal{B}(G)^{\prime}$ is an irreducible block with $\sigma\left(B_{0}\right)=D(G)$, then $B=B_{0}^{k}$ has the required property.
(ii) follows immediately from (i) and the definition of $D_{k}(G)$.
(iii) Let $l$ be the maximal length of a factorization of a block $B \in \mathcal{B}(G)^{\prime}$ with $\max L(B) \leq k$ and $\sigma(B)=D_{k}(G)$. If $l<k$, then the block $\bar{B}=B \cdot 0$ satisfies $\sigma(\bar{B})=D_{k}(G)+1$ and $\max L(\bar{B})=l+1 \leq k$, which contradicts the definition of $D_{k}(G)$.
(iv) In order to prove that $D_{k}(G)$ has the indicated property, let $S \in$ $\mathcal{F}(G)$ be such that $\sigma(S) \geq D_{k}(G)$, set $g=-\iota(S) \in G$ and consider the block $S_{g} \in \mathcal{B}(G)^{\prime}$. Since $\sigma(S g)>D_{k}(G)$, the block $S g$ has a factorization of length $\nu>k$, say $S g=B_{1} \cdot \ldots \cdot B_{\nu}$ with irreducible $B_{j} \in \mathcal{B}(G)^{\prime}$ and $v_{g}\left(B_{\nu}\right)>0$. This implies $B_{1} \cdot \ldots \cdot B_{k} \mid S$, as asserted.

In order to prove that $D_{k}(G)$ is minimal with this property, let $B \in$ $\mathcal{B}(G)$ be a block satisfying $\sigma(B)=D_{k}(G)$ and max $L(B)=k$, according to (iii). If $B=\prod_{j=1}^{D_{k}(G)} g_{j}$ and $d<D_{k}(G)$, then the element $S_{d}=\prod_{j=1}^{d} g_{j} \in$
$\mathcal{F}(G)$ cannot be divisible by a product of $k$ blocks, for this would imply $\max L(B) \geq k+1$.
(v) If $B=g_{1} \cdot \ldots \cdot g_{\nu}$ with $\nu>k D(G)$ then, by (iv), there exist blocks $B_{1}, \ldots, B_{k} \in \mathcal{B}(G)^{\prime}$ such that $B_{1} \cdot \ldots \cdot B_{k} \mid g_{1} \cdot \ldots \cdot g_{\nu-1}$, and therefore the assertion follows.
(vi) By (iii), there exists a block $B=g_{1} \cdot \ldots \cdot g_{N} \in \mathcal{B}\left(G_{1}\right)$ such that $N=\sigma(B)=D_{k}\left(G_{1}\right)$ and $\max L(B)=k$. We pick an element $g \in G \backslash G_{1}$ and assume that $D_{k}\left(G_{1}\right) \geq D_{k}(G)$. By (iv), there exist blocks $B_{1}, \ldots, B_{k} \in$ $\mathcal{B}(G)^{\prime}$ such that $B_{1} \cdot \ldots \cdot B_{k} \mid g_{1} \cdot \ldots \cdot g_{N-1} g$; this implies $B_{1}, \ldots, B_{k} \in \mathcal{B}\left(G_{1}\right)^{\prime}$, and therefore there exists a block $B_{k+1} \in \mathcal{B}\left(G_{1}\right)^{\prime}$ such that $B=B_{1} \cdot \ldots$ $\ldots \cdot B_{k} B_{k+1}$, a contradiction.
3. The precise value of $D(G)$ is known only for some special types of abelian groups [2], [3]; see [5] for a survey. In the following proposition we collate those results which we shall either use or generalize in the sequel.

For $n \geq 1$, let $C_{n}$ be the cyclic group of order $n$.
Proposition 2. Let $G=\bigoplus_{i=1}^{d} C_{n_{i}}$ be a finite abelian group with $1<$ $n_{d}\left|n_{d-1}\right| \ldots \mid n_{1}$, and set

$$
M(G)=n_{1}+\sum_{i=2}^{d}\left(n_{i}-1\right)
$$

(i) $M(G) \leq D(G) \leq \# G$.
(ii) If either $d \leq 2$ or $G$ is a p-group, then $M(G)=D(G)$.

Proof. [10], [11]; see also [1].
Proposition 3. Let $G$ be a finite abelian group and $k \in \mathbb{N}$.
(i) If $G=G^{\prime} \oplus G^{\prime \prime}$, then $D_{k}(G) \geq D_{k}\left(G^{\prime}\right)+D\left(G^{\prime \prime}\right)-1$.
(ii) If $G=\bigoplus_{i=1}^{d} C_{n_{i}}$ with $1<n_{d}\left|n_{d-1}\right| \ldots \mid n_{1}$, then $D_{k}(G) \geq k n_{1}+$ $\sum_{i=2}^{d}\left(n_{i}-1\right)$.
(iii) $D_{k}\left(C_{n}\right)=k n$.

Proof. (i) By Proposition 1(iv), there exist elements $S^{\prime} \in \mathcal{F}\left(G^{\prime}\right)$ and $S^{\prime \prime} \in \mathcal{F}\left(G^{\prime \prime}\right)$ such that $\sigma\left(S^{\prime}\right)=D_{k}\left(G^{\prime}\right)-1, S^{\prime}$ is not divisible by a product of $k$ blocks from $\mathcal{B}\left(G^{\prime}\right)^{\prime}$ and $\sigma\left(S^{\prime \prime}\right)=D\left(G^{\prime \prime}\right)-1, S^{\prime \prime}$ is not divisible by a block of $\mathcal{B}\left(G^{\prime \prime}\right)^{\prime}$. If $S^{\prime}=\prod_{j=1}^{D_{k}\left(G^{\prime}\right)-1} g_{j}^{\prime}$ and $S^{\prime \prime}=\prod_{j=1}^{D\left(G^{\prime \prime}\right)-1} g_{j}^{\prime \prime}$, then the element

$$
S=\prod_{j=1}^{D_{k}\left(G^{\prime}\right)-1}\left(g_{j}^{\prime}, 0\right) \cdot \prod_{j=1}^{D\left(G^{\prime \prime}\right)-1}\left(0, g_{j}^{\prime \prime}\right) \in \mathcal{F}(G)
$$

is not divisible by a product of $k$ blocks of $\mathcal{B}(G)^{\prime}$, whence

$$
D_{k}(G)>\sigma(S)=D_{k}\left(G^{\prime}\right)+D\left(G^{\prime \prime}\right)-2,
$$

by Proposition 1(iv), as asserted.
(ii) If $G=\left\langle g_{1}, \ldots, g_{d}\right\rangle$ and $\operatorname{ord}\left(g_{i}\right)=n_{i}$, then the block

$$
B=g_{1}^{k n_{1}-1} \cdot\left(g_{1}+\ldots+g_{d}\right) \cdot \prod_{j=2}^{d} g_{j}^{n_{j}-1} \in \mathcal{B}(G)
$$

has a unique factorization into irreducible blocks of length $k$, given by $B=$ $B_{1}^{k-1} B_{0}$, where $B_{1}=g_{1}^{n_{1}}$ and $B_{0}=\left(g_{1}+\ldots+g_{d}\right) \cdot \prod_{j=1}^{d} g_{j}^{n_{j}-1}$. This implies $D_{k}(G) \geq \sigma(B)=k n_{1}+\sum_{j=2}^{d}\left(n_{j}-1\right)$.
(iii) By Propositions 1 and 2, we have $D_{k}\left(C_{n}\right) \leq k D\left(C_{n}\right)=k n$, whereas, by (ii), $D_{k}\left(C_{n}\right) \geq k n$.
4. In this section we generalize the result on groups of rank 2 .

Proposition 4. Let $G=G_{1} \oplus G_{2}$ be a finite abelian group, $\# G_{i}=n_{i}$, $n_{2} \mid n_{1}$ and $k \in \mathbb{N}$. Then

$$
D_{k}\left(C_{n}\right) \leq k n_{1}+n_{2}-1 .
$$

For the proof of Proposition 4 we need two technical lemmas.
Lemma 1. Let $G$ be a finite abelian group, $m \in \mathbb{N}, D(G)<2 m$ and $D\left(G \oplus C_{m}\right)<3 m$. Let $t \in \mathbb{N}$ and $S \in \mathcal{F}(G)$ be such that $\sigma(S) \geq D(G \oplus$ $\left.C_{m}\right)+(t-1) m$. Then there exist blocks $B_{1}, \ldots, B_{t} \in \mathcal{B}(G)^{\prime}$ such that $B_{1} \cdot \ldots \cdot B_{t} \mid S$ and $\sigma\left(B_{i}\right) \leq m$ for all $i \in\{1, \ldots, t\}$.

Proof. It suffices to consider the case $t=1$, for then the general case follows by a trivial induction argument.

Set $N=D\left(G \oplus C_{m}\right)<3 m$, and let $S=g_{1} \cdot \ldots g_{\nu} \in \mathcal{F}(G)$ be an element with $\nu=\sigma(S) \geq N$. Let $e_{m}$ be a generator of $C_{m}$, and consider the element

$$
S^{\prime}=\prod_{j=1}^{N}\left(g_{j}, e_{m}\right) \in \mathcal{F}\left(G \oplus C_{m}\right)
$$

by Proposition 1(iv) there exists an irreducible block $S_{0}^{\prime} \in \mathcal{B}\left(G \oplus C_{m}\right)^{\prime}$ such that $S_{0}^{\prime} \mid S^{\prime}$, and we may assume that $S_{0}^{\prime}=\prod_{j=1}^{N_{0}}\left(g_{j}, e_{m}\right)$ for some $N_{0} \leq N$. Since

$$
\iota\left(S_{0}^{\prime}\right)=\left(\sum_{j=1}^{N_{0}} g_{j}, N_{0} e_{m}\right)=(0,0) \in G \oplus C_{m}
$$

we obtain $S_{0}=\prod_{j=1}^{N_{0}} g_{j} \in \mathcal{B}(G)$ and $m \mid N_{0}$, whence $m=N_{0}$ or $2 m=N_{0}$. If $m=N_{0}$, the assertion follows with $B=S_{0}$; if $2 m=N_{0}>D(G)$, then $S_{0}$ has a decomposition $S_{0}=B B^{\prime}$ with $B, B^{\prime} \in \mathcal{B}(G)$ and $\sigma(B) \leq m$, which again implies the assertion.

Lemma 2. Let $p$ be a prime, $t \in \mathbb{N}$ and $B \in \mathcal{B}\left(C_{p} \oplus C_{p}\right)$ a block satisfying $\sigma(B) \geq t p$. Then there exist blocks $B_{1}, \ldots, B_{t} \in \mathcal{B}\left(C_{p} \oplus C_{p}\right)^{\prime}$ such that $B=B_{1} \cdot \ldots \cdot B_{t}$.

Proof. The assertion is true for $t=1$ and also for $t=2$, as $D\left(C_{p} \oplus C_{p}\right)$ $=2 p-1<2 p$. Therefore we assume that $t \geq 3$ and $B=g_{1} \cdot \ldots \cdot g_{\nu}$ for some $\nu \geq t p$. We apply Lemma 1 with $G=C_{p} \oplus C_{p}, m=p$ and $S=g_{1} \cdot \ldots$ $\ldots \cdot g_{t p-1}$. Since $\sigma(S)=t p-1>(3 p-2)+(t-3) p=D\left(C_{p} \oplus C_{p} \oplus C_{p}\right)+(t-3) p$, there exist blocks $B_{1}, \ldots, B_{t-2}, B^{\prime} \in \mathcal{B}(G)^{\prime}$ such that $B=B_{1} \cdot \ldots \cdot B_{t-2} B^{\prime}$ and $\sigma\left(B_{j}\right) \leq p$ for all $j \in\{1, \ldots, t-2\}$. This implies

$$
\sigma\left(B^{\prime}\right)=\sigma(B)-\sum_{j=1}^{t-2} \sigma\left(B_{j}\right) \geq t p-(t-2) p=2 p>D(G)
$$

whence $B^{\prime}=B_{t-1} B_{t}$ with blocks $B_{t-1}, B_{t} \in \mathcal{B}(G)^{\prime}$.
Proof of Proposition 4. By induction on $n_{2}$; if $n_{2}=1$, then $D_{k}(G)=D_{k}\left(G_{1}\right) \leq k D\left(G_{1}\right) \leq k n_{1}$ by Proposition 1(ii) and Proposition 2(i).

If $n_{2}>1$, let $p$ be a prime with $p \mid n_{2}$ and choose subgroups $G_{i}^{\prime} \subset G_{i}$ $(i=1,2)$ with $\left(G_{i}: G_{i}^{\prime}\right)=p$. Set

$$
t=k n_{1} / p+n_{2} / p
$$

and assume that the assertion is true for the subgroup $G^{\prime}=G_{1}^{\prime} \oplus G_{2}^{\prime} \subset G$, i.e., $D_{k}\left(G^{\prime}\right) \leq t-1$. We must prove that every block $B \in \mathcal{B}(G)$ with $\sigma(B)=N \geq k n_{1}+n_{2}$ has a factorization of length $l \geq k+1$. We set $B=g_{1} \cdot \ldots \cdot g_{N}$ and consider the canonical epimorphism $\pi: G \rightarrow C_{p} \oplus C_{p}$ with $\operatorname{ker}(\pi)=G^{\prime}$. The block $B^{*}=\pi\left(g_{1}\right) \cdot \ldots \cdot \pi\left(g_{N}\right) \in \mathcal{B}\left(C_{p} \oplus C_{p}\right)$ satisfies $\sigma\left(B^{*}\right)=N \geq t p$ and therefore, by Lemma $2, B^{*}$ is a product of $t$ blocks from $\mathcal{B}\left(C_{p} \oplus C_{p}\right)^{\prime}$. Taking preimages in $G$, we obtain a decomposition $B=S_{1} \cdot \ldots \cdot S_{t}$ with $S_{i} \in \mathcal{F}(G)^{\prime}$ and $\iota\left(S_{i}\right)=g_{i}^{\prime} \in G^{\prime}$. Since $t>D_{k}\left(G^{\prime}\right)$ and $g_{1}^{\prime} \cdot \ldots \cdot g_{t}^{\prime} \in \mathcal{B}\left(G^{\prime}\right)$, there exist blocks $B_{1}^{\prime}, \ldots, B_{k+1}^{\prime} \in \mathcal{B}\left(G^{\prime}\right)^{\prime}$ with $B_{1}^{\prime}, \ldots, B_{k+1}^{\prime} \mid g_{1}^{\prime} \cdot \ldots \cdot g_{t}^{\prime}$ by Proposition 1(v). Hence there exists a decomposition

$$
\{1, \ldots, t\}=\bigcup_{\nu=1}^{k+1} J_{n} \quad \text { (disjoint union) }
$$

such that $B_{\nu}^{\prime}=\prod_{j \in J_{\nu}} g_{j}^{\prime}$ for all $\nu \in\{1, \ldots, k+1\}$. Putting $B_{\nu}=\prod_{j \in J_{\nu}} S_{j} \in$ $\mathcal{B}(G)$, we obtain $B_{1} \cdot \ldots \cdot B_{k+1} \mid B$, and therefore $B$ has a factorization of length $l \geq k+1$.

Proposition 5. If $G=C_{n_{1}} \oplus C_{n_{2}}$ with $n_{2} \mid n_{1}$, then $D_{k}(G)=k n_{1}+$ $n_{2}-1$.

Proof. Obvious by Propositions 3 and 4 .
5. Proof of the Theorem. Let $K$ be an algebraic number field, $R$ its ring of integers, $G$ the ideal class group, $\mathcal{I}$ the semigroup of nonzero ideals and $\mathcal{H}$ the subsemigroup of non-zero principal ideals of $R$. We write $G$ additively, and for $J \in \mathcal{I}$ we denote by $[J] \in G$ the ideal class of $J$. Let $\theta: \mathcal{I} \rightarrow \mathcal{F}(G)$ be the unique semigroup homomorphism satisfying $\theta(P)=[P]$ for every maximal $P$ of $R$. For $J \in \mathcal{I}$, we have $\theta(J) \in \mathcal{B}(G)$ if and only if $J \in \mathcal{H}$. If $\alpha \in R \backslash\left(R^{\times} \cup\{0\}\right)$, then $L(\alpha)=L(\theta((\alpha)))$.

Let $\mathcal{M}_{k}$ be the set of all blocks $B \in \mathcal{B}(G)$ such that $\max L(B) \leq k$, and let $\mathcal{M}_{k}^{\prime}$ be the set of all blocks $B \in \mathcal{B}(G)$ such that $\min L(B) \leq k$. Then

$$
M_{k}^{\prime}=\left\{\alpha \in R \backslash\left(R^{\times} \cup\{0\}\right) \mid \theta((\alpha)) \in \mathcal{M}_{k}^{\prime}\right\}
$$

and, by Proposition 1,

$$
k D(G)=\max \left\{\sigma(B) \mid B \in \mathcal{M}_{k}^{\prime}\right\}, \quad D_{k}(G)=\max \left\{\sigma(B) \mid B \in \mathcal{M}_{k}\right\}
$$

In particular, the sets $\mathcal{M}_{k}$ and $\mathcal{M}_{k}^{\prime}$ are finite.
After these observations, the Theorem is an immediate consequence of the following Lemma, due to Kaczorowski [7, Lemma 1].

Lemma 3. For $1 \neq S \in \mathcal{F}(G), x \geq e^{e}$ and $q \in \mathbb{Z}, 0 \leq q \leq c_{0} \frac{\sqrt{\log x}}{\log \log x}$, we have

$$
\begin{aligned}
& \#\{J \in \mathcal{I} \mid(R: J) \leq x, \theta(J)=S\} \\
& \quad=\frac{x}{\log x}\left[\sum_{\mu=0}^{q} \frac{W_{\mu}(\log \log x)}{(\log x)^{\mu}}+O\left(\left(c_{1} q\right)^{q} \frac{(\log \log x)^{\sigma(S)}}{(\log x)^{q+1}}\right)\right]
\end{aligned}
$$

with constants $c_{0}, c_{1} \in \mathbb{R}_{+}$and polynomials $W_{\mu} \in \mathbb{C}[X]$ such that $\operatorname{deg} W_{\mu} \leq$ $\sigma(S), \operatorname{deg} W_{0}=\sigma(S)-1$, and $W_{0}$ has a positive leading coefficient.

## REFERENCES

[1] P. C. Baayen, Een combinatorisch problem voor eindige Abelse groepen, Math. Centrum Syllabus 5, Coll. Discrete Wiskunde Caput 3, Math. Centre Amsterdam, 1968.
[2] P.van Emde Boas, A combinatorial problem on finite Abelian groups II, Stichting Mathematisch Centrum Amsterdam, Report ZW 1969-007, 1969.
[3] P.van Emde Boas and D. Kruyswijk, A combinatorial problem on finite abelian groups III, Stichting Mathematisch Centrum Amsterdam, Report ZW 1969-008, 1969.
[4] A. Geroldinger, Über nicht-eindeutige Zerlegungen in irreduzible Elemente, Math. Z. 197 (1988), 505-529.
[5] F. Halter-Koch, Factorization of algebraic integers, Ber. Math.-Stat. Sektion Forschungszentrum Graz 191 (1983).
[6] F. Halter-Koch and W. Müller, Quantitative aspects of non-unique factorization: A general theory with applications to algebraic function fields, J. Reine Angew. Math. 421 (1991), 159-188.
[7] J. Kaczorowski, Some remarks on factorization in algebraic number fields, Acta Arith. 43 (1983), 53-68.
[8] W. Narkiewicz, Finite abelian groups and factorization problems, Colloq. Math. 42 (1979), 319-330.
[9] -, Elementary and Analytic Theory of Algebraic Numbers, Springer, 1990.
[10] J. E. Olson, A combinatorial problem on finite Abelian groups, I, J. Number Theory 1 (1969), 8-10.
[11] -, A combinatorial problem on finite Abelian groups, II, ibid., 195-199.
[12] P. Rémond, Étude asymptotique de certaines partitions dans certaines semigroupes, Ann. Sci. École Norm. Sup. 83 (1966), 343-410.

INSTITUT FÜR MATHEMATIK
KARL-FRANZENS-UNIVERSITÄT
HEINRICHSTRASSE 36
A-8010 GRAZ, AUSTRIA

