Franz Halter-Koch
Relative block semigroups and their arithmetical applications

Commentationes Mathematicae Universitatis Carolinae, Vol. 33 (1992), No. 3, 373--381

Persistent URL: http://dml.cz/dmlcz/118506

Terms of use:
© Charles University in Prague, Faculty of Mathematics and Physics, 1992

Institute of Mathematics of the Academy of Sciences of the Czech Republic provides access to digitized documents strictly for personal use. Each copy of any part of this document must contain these Terms of use.

This paper has been digitized, optimized for electronic delivery and stamped with digital signature within the project DML-CZ: The Czech Digital Mathematics Library http://project.dml.cz
Relative block semigroups and their arithmetical applications

FRANZ HALTER-KOCH

Abstract. We introduce relative block semigroups as an appropriate tool for the study of certain phenomena of non-unique factorizations in residue classes. Thereby the main interest lies in rings of integers of algebraic number fields, where certain asymptotic results are obtained.

Keywords: factorization problems, Krull semigroups

Classification: 11R27, 11R47, 20M14

In a series of papers A. Geroldinger, W. Narkiewicz and myself investigated phenomena of non-unique factorizations in an abstract context but mainly with emphasis to rings of integers of algebraic number fields. If we are merely interested in the different lengths of factorizations of a given integer, the concept of block semigroups turned out to be the appropriate combinatorial tool for this question. It was introduced in [8] and investigated in a systematical way in [1], [2] and [3]. In this paper we shall refine this tool: we introduce relative blocks; with the aid of them we shall study lengths of factorizations of elements in given residue classes.

In §1 we introduce relative block semigroups and determine their algebraic structure; in §2 we apply them to the arithmetic of arbitrary Krull semigroups. In §3 we recall some abstract analytic number theory in the context of arithmetical formations, and we determine an asymptotic formula for the number of elements with a given block. Finally, in §4 we give some arithmetical applications for algebraic number fields.

§1. Relative block semigroups

Throughout this paper, a semigroup is a multiplicatively written commutative and cancellative monoid. We shall use the concept of divisor theories and Krull semigroups, cf. [4] and [3]. For a set $P$, we denote by $\mathcal{F}(P)$ the free abelian monoid with basis $P$, and we write the elements of $\mathcal{F}(P)$ in the form

$$a = \prod_{p \in P} p^{v_p(a)}$$

with (uniquely determined) exponents $v_p(a) \in \mathbb{N}_0$, $v_p(a) = 0$ for all but finitely many $p \in P$. 
**Definition 1.** Let $G$ be an (additively written) abelian group. For an element
\[ S = \prod_{g \in G} g^{v_g(S)} \in \mathcal{F}(G) \]
we call
\[ \sigma(S) = \sum_{g \in G} v_g(S) \in \mathbb{N}_0 \quad \text{the size of } S, \]
\[ \iota(S) = \sum_{g \in G} v_g(S)g \in G \quad \text{the content of } S \quad \text{and} \]
\[ \chi(S) = \prod_{g \in G} \frac{1}{v_g(S)!} \quad \text{the characteristic of } S. \]

For a subgroup $G^* < G$, we set
\[ B(G, G^*) = \{ S \in \mathcal{F}(G) \mid \iota(S) \in G^* \}; \]
the elements of $B(G, G^*)$ are called relative blocks over $G$ with respect to $G^*$. In particular, $B(G, G) = \mathcal{F}(G)$, and
\[ B(G) = B(G, \{0\}) \]
is the ordinary block semigroup investigated in [2] and [3].

**Proposition 1.** Let $G$ be an abelian group and $G^* < G$ a subgroup.

i) $B(G, G^*)$ is a Krull semigroup.

ii) Suppose that either $G^* \neq \{0\}$ or $\#G > 2$. Then the injection $B(G, G^*) \hookrightarrow \mathcal{F}(G)$ is a divisor theory; the divisor class group $C = \mathcal{F}(G)/B(G, G^*)$ is isomorphic to $G/G^*$. If $[S] \in C$ denotes the divisor class of an element $S \in \mathcal{F}(G)$, then an isomorphism $\iota^* : C \to G/G^*$ is given by $\iota^*([S]) = \iota(S) + G^*$. For every $g \in G$, the set $g + G^* \subset [g] = \iota^*^{-1}(g + G^*)$ is the set of prime elements contained in $[g] \in C$.

**Proof:** If $G^* = \{0\}$, all this is well known, cf. [4, Beispiel 5]. If $G^* \neq \{0\}$, we consider the unique semigroup homomorphism $\varphi : \mathcal{F}(G) \to G/G^*$ satisfying $\varphi(g) = g + G^*$ for all $g \in G$, and apply [4, Satz 4].

**Definition 2.** Let $G$ be an abelian group and $G^* < G$ a subgroup. Then
\[ \theta : \mathcal{F}(G) \to \mathcal{F}(G/G^*) \]
denotes the unique semigroup epimorphism satisfying $\theta(g) = g + G^*$ for all $g \in G$, i.e.
\[ \theta\left( \prod_{g \in G} g^{n(g)} \right) = \prod_{g \in G} (g + G^*)^{n(g)}. \]
Proposition 2. Let $G$ be an abelian group and $G^* < G$ a subgroup.

i) If $S \in \mathcal{F}(G)$, then

$$\iota(\theta(S)) = \iota(S) + G^* \in G/G^*;$$

in particular: $S \in \mathcal{B}(G, G^*)$ if and only if $\theta(S) \in \mathcal{B}(G/G^*)$.

ii) Given $S^* \in \mathcal{F}(G/G^*)$ and $g \in G$ such that $\sigma(S^*) > 0$ and $\iota(S^*) = g + G$, there exists some $S \in \mathcal{F}(G)$ satisfying $\theta(S) = S^*$ and $\iota(S) = g$.

iii) Let $G$ be finite, $S^* \in \mathcal{F}(G/G^*)$ and $g \in G$ such that $\sigma(S^*) > 0$ and $\iota(S^*) = g + G^*$; then

$$\sum_{S \in \mathcal{F}(G)} \chi(S) = d^{\sigma(S^*) - 1} \chi(S^*),$$

where $d = \#G^*$.

Proof: i) Let $\pi: G \to G/G^*$ be the canonical epimorphism. Then $\pi \circ \iota: \mathcal{F}(G) \to G/G^*$ and $\iota \circ \theta: \mathcal{F}(G) \to G/G^*$ are semigroup homomorphisms which coincide on $G$; this implies $\pi \circ \iota = \iota \circ \theta$, i.e. $\iota(S) + G^* = \iota \circ \theta(S)$ for all $S \in \mathcal{F}(G)$.

ii) Since $\sigma(S^*) > 0$, we have $S^* = (g_1 + G)\bar{S}$, where $\bar{S} \in \mathcal{F}(G/G^*)$ and $g_1 \in G$, which implies $\iota(\bar{S}) = g - g_1 + G^* \in G/G^*$. Let $S' \in \mathcal{F}(G)$ be arbitrary such that $\theta(S') = \bar{S}$. By i), $\iota(S') = g - g_1 + g^*$ for some $g^* \in G^*$, and the element $S = (g_1 - g^*)S' \in \mathcal{F}(G)$ fulfills our requirements.

iii) Suppose that $G^* = \{g_1, \ldots, g_d\}$. We use induction on $\sigma(S^*)$ and consider first the case where

$$S^* = (g^* + G^*)^n \in \mathcal{F}(G/G^*)$$

for some $g^* \in G$ and $n \in \mathbb{N}$. In this case we have $g + G^* = \iota(S^*) = ng^* + G^*$, and

$$\{S \in \mathcal{F}(G) \mid \theta(S) = S^*, \ iota(S) = g\}$$

$$= \left\{ \prod_{i=1}^{d} (g^* + g_i)^{n_i} \mid (n_1, \ldots, n_d) \in \mathbb{N}_0^d, \sum_{i=1}^{d} n_i = n, \sum_{i=1}^{d} n_i (g^* + g_i) = g \right\}.$$

If $\bar{g} = g - ng^* \in G^*$, this implies

$$\sum_{S \in \mathcal{F}(G)} \chi(S) = \sum_{\bar{g} = n_1g_1 + \cdots + n_dg_d} \frac{1}{n_1! \cdots n_d!} = N^* \text{ (say)}.$$

Let $\hat{G}^*$ be a multiplicative abelian group isomorphic to $G^*$, fix an isomorphism

$$\begin{cases} G^* \xrightarrow{\sim} \hat{G}^* \\ g_j \mapsto \hat{g}_j \end{cases}$$
and consider the group ring $\mathbb{Z}[\hat{G}^*]$; here the multinomial formula yields
\[
(\hat{g}_1 + \cdots + \hat{g}_d)^n = \sum_{(n_1, \ldots, n_d) \in \mathbb{N}_0^d \atop n_1 + \cdots + n_d = n} \frac{n!}{n_1! \cdots n_d!} \hat{g}_1^{n_1} \cdots \hat{g}_d^{n_d}.
\]
Writing the right-hand side in the canonical form
\[
\sum_{\hat{g} \in \hat{G}^*} N(\hat{g})\hat{g}, \text{ where } N(\hat{g}) \in \mathbb{Z},
\]
and comparing the coefficient of $\hat{g}$, yields
\[
N(\hat{g}) = n!N^*.
\]
On the other hand, induction on $n$ gives
\[
(\hat{g}_1 + \cdots + \hat{g}_d)^n = d^{n-1}(\hat{g}_1 + \cdots + \hat{g}_d),
\]
and consequently
\[
N^* = \frac{d^{n-1}}{n!} = d^{\sigma(S^*)-1}\chi(S^*).
\]
For the general case, let $h_1, \ldots, h_m \in G$ be a system of representatives for $G/G^*$; then
\[
S^* = \prod_{j=1}^m (h_j + G^*)^{n_j},
\]
where $n_j \in \mathbb{N}_0$, and since $\sigma(S^*) = n_1 + \cdots + n_m > 0$, we may assume that $n_m > 0$. We set
\[
S_0^* = \prod_{j=1}^{m-1} (h_j + G^*)^{n_j}
\]
and obtain
\[
\{S \in \mathcal{F}(G) \mid \theta(S) = S^*, \ \iota(S) = g\} = \{S_0S' \mid S_0, S' \in \mathcal{F}(G), \ \theta(S_0) = S_0^*, \ \theta(S') = (h_m + G^*)^{n_m}, \ \iota(S') = g - \iota(S_0)\}.
\]
If $S_0, S' \in \mathcal{F}(G), \ \theta(S_0) = S_0^*$ and $\theta(S') = (h_m + G^*)^{n_m}$, then $S_0$ and $S'$ are relatively prime, and therefore $\chi(S) = \chi(S_0)\chi(S')$. This implies
\[
\sum_{S_0 \in \mathcal{F}(G)} \chi(S_0) = \sum_{S' \in \mathcal{F}(G)} \chi(S') = \sum_{S' \in \mathcal{F}(G)} \chi(S') = \sum_{\iota(S') = g - \iota(S_0)} \chi(S_0)\chi(S') = \sum_{\theta(S_0) = S_0^*} \chi(S_0)\chi(S_0^*) = \chi(S_0)\chi(S_0^*).
\]
by the special case considered above we obtain
\[
\sum_{S' \in \mathcal{F}(G)} \chi(S') = \frac{d^{n_m - 1}}{n_m}. 
\]

By induction hypothesis,
\[
\sum_{S_0 \in \mathcal{F}(G)} \chi(S_0) = d \cdot d^{\sigma(S_0^*) - 1} \chi(S_0^*) = d^{\sigma(S_0^*)} \chi(S_0^*);
\]

since \( \chi(S^*) = \chi(S_0^*)/n_m! \) and \( \sigma(S^*) = \sigma(S_0^*) + n_m, \) the assertion follows. \( \qed \)

\section{Relative blocks and Krull semigroups}

If \( H \) is a Krull semigroup and \( \partial: H \rightarrow \mathcal{F}(P) \) is a divisor theory, then \( \partial \) induces an injective divisor theory \( \partial: H/H^\times \rightarrow \mathcal{F}(P) \) (where \( H^\times \) denotes the group of invertible elements of \( H \)). If \( H \) is reduced (i.e., \( H^\times = \{1\} \)), then we may assume that \( H \subset \mathcal{F}(P) \) and \( H \hookrightarrow \mathcal{F}(P) \) is a divisor theory. We shall adopt this viewpoint in the sequel.

**Definition 3.** Let \( H \) be a reduced Krull semigroup, \( H \hookrightarrow \mathcal{F}(P) \) a divisor theory and \( G \) its divisor class group. We write \( G \) additively, and for \( a \in \mathcal{F}(P) \) we denote by \([a] \in G\) the class containing \( a \). The unique semigroup homomorphism \( \beta^H: \mathcal{F}(P) \rightarrow \mathcal{F}(G) \) satisfying \( \beta^H(p) = [p] \) for all \( p \in P \) is called the \( H \)-block homomorphism. For \( a \in \mathcal{F}(P) \), the element \( \beta^H(a) \in \mathcal{F}(G) \) is called the \( H \)-block of \( a \).

Clearly, \( \iota(\beta^H(a)) = [a] \in G; \) in particular, \( a \in H \) if and only if \( \beta^H(a) \in \mathcal{B}(G) \).

The significance of the block homomorphism \( \beta^H \) for the arithmetic of \( H \) is given as follows (cf. [1, Prop. 1]):

An element \( a \in H \) is irreducible in \( H \) if and only if \( \beta^H(a) \) is irreducible in \( \mathcal{B}(G) \). If \( a \in H \) and \( a = u_1 \cdot \ldots \cdot u_r \) is a factorization of \( a \) into irreducible elements \( u_i \in H \), then \( \beta^H(a) = \beta^H(u_1) \cdot \ldots \cdot \beta^H(u_r) \) is a factorization of \( \beta^H(a) \) into irreducible elements of \( \mathcal{B}(G) \), and every factorization of \( \beta^H(a) \) into irreducible elements of \( \mathcal{B}(G) \) arises in this way. In particular, if \( \mathcal{L}(a) \) denotes the set of all lengths of factorizations of \( a \) in \( H \), i.e.,
\[
\mathcal{L}(a) = \{ r \in \mathbb{N} | a = u_1 \cdot \ldots \cdot u_r \text{ with irreducible } u_i \in H \},
\]
then \( \mathcal{L}(a) = \mathcal{L}(\beta^H(a)) \). If every class \( g \in G \) contains at least one prime \( p \in P \), then \( \beta^H(H) = \mathcal{B}(G) \) and \( \beta^H(\mathcal{F}(P)) = \mathcal{F}(G) \).

We need the following relative construction.
Proposition 3. Let $H$ be a reduced Krull semigroup, $H \hookrightarrow \mathcal{F}(P)$ a divisor theory, $G$ its divisor class group and $G^* < G$ a subgroup. We assume that $g \cap P \neq \emptyset$ for every $g \in G$, and we set

$$H^* = \{a \in \mathcal{F}(P) \mid [a] \in G^*\}$$

where $[a] \in G$ denotes the divisor class of an element $a \in \mathcal{F}(P)$ under $H \hookrightarrow \mathcal{F}(P)$.

i) $H^* \hookrightarrow \mathcal{F}(P)$ is a divisor theory with divisor class group $G/G^*$. If $a \in \mathcal{F}(P)$, then $[a] + G^* \in G/G^*$ is the divisor class of $a$ under $H^* \hookrightarrow \mathcal{F}(P)$, $\theta(\beta^H(a)) = \beta^{H^*}(a)$, and $a \in H^*$ if and only if $\beta^H(a) \in \mathcal{B}(G, G^*)$.

ii) Given $S^* \in \mathcal{B}(G/G^*)$ such that $\sigma(S^*) > 0$ and $g^* \in G^*$, there exists an element $a \in H^*$ such that $\beta^{H^*}(a) = S^*$ and $[a] = g^*$.

Proof: i) It suffices to consider the case $G^* \neq \{0\}$. If $\varphi: \mathcal{F}(P) \rightarrow G/G^*$ is defined by $\varphi(a) = [a] + G^*$, then $H^* = \varphi^{-1}(G^*)$ and $#P \cap \varphi^{-1}(g + G^*) \geq #G^* \geq 2$ for every $g \in G$. Therefore $H^* \hookrightarrow \mathcal{F}(P)$ is a divisor theory by [4, Satz 4]. Clearly, $G/G^*$ is the associated divisor class group, and $[a] + G^* \in G/G^*$ is the divisor class of an element $a \in \mathcal{F}(P)$. The mappings $\theta \circ \beta^H$ and $\beta^{H^*}$ are semigroup homomorphisms $\mathcal{F}(P) \rightarrow \mathcal{F}(G/G^*)$; for $p \in P$, we have $\theta \circ \beta^H(p) = \theta([p]) = [p] + G^* = \beta^{H^*}(p)$, which implies $\theta \circ \beta^H = \beta^{H^*}$. Since $\iota(\beta^H(a)) = [a] \in G$, we have $a \in H^*$ if and only if $\beta^H(a) \in \mathcal{B}(G, G^*)$.

ii) By Proposition 2, there exists an element $S \in \mathcal{F}(G)$ satisfying $\theta(S) = S^*$ and $\iota(S) = g^*$, whence $S \in \mathcal{B}(G, G^*)$. Since $g \cap P \neq \emptyset$ for every $g \in G$, there exists an element $a \in H^*$ such that $\beta^H(a) = S$; this implies $\beta^{H^*}(a) = \theta(S) = S^*$ and $[a] = \iota(S) = g^*$. □

Main Example. Let $R$ be a Dedekind domain and $\mathfrak{f}$ a non-zero ideal of $R$ (more generally, $\mathfrak{f}$ may be a cycle; see [5]). Let $H$ be the semigroup of all principal ideals $aR$ of $R$ generated by elements $a \equiv 1 \mod \mathfrak{f}$, and let $H^*$ be the semigroup of all principal ideals of $R$ which are relatively prime to $\mathfrak{f}$. If $P$ denotes the set of all maximal ideals $\mathfrak{p}$ of $R$ not containing $\mathfrak{f}$, then $D = \mathcal{F}(P)$ is the semigroup of all ideals of $R$ which are relatively prime to $\mathfrak{f}$, and

$$H \hookrightarrow H^* \hookrightarrow D = \mathcal{F}(P)$$

satisfies the assumption of Proposition 3; here $G$ is the ray class group modulo $\mathfrak{f}$ in $R$, and $G^*$ is the subgroup of all ray classes represented by principal ideals. Consequently, $C = G/G^*$ is isomorphic to the ideal class group of $R$ (we identify!), and there is a canonical isomorphism

$$G^* \cong (R/\mathfrak{f})^\times /U(\mathfrak{f}),$$

where $U(\mathfrak{f})$ denotes the subgroup of all prime residue classes modulo $\mathfrak{f}$ which are represented by elements of $R^\times$. 
With an element \( a \in R \setminus (R^\times \cup \{0\}) \) we associate its block
\[
\beta(a) = \beta^{H^*}(aR) \in \mathcal{B}(C);
\]
then we have \( \mathcal{L}(a) = \mathcal{L}(\beta(a)) \subset \mathbb{N} \). Therefore Proposition 3, ii) describes the distribution of the elements \( a \in R \) having the same block in \( \mathcal{B}(C) \) in the various prime residue classes modulo \( \mathfrak{f} \), provided that each ray class modulo \( \mathfrak{f} \) contains at least one prime ideal of \( R \). In fact, it is sufficient to assume that every ideal class of \( R \) which contains a prime ideal splits into ray classes each of which contains a prime ideal; details are left to the reader.

§ 3. Formations

We develop the quantitative theory in an abstract setting following [6]. Let \( \Lambda \) be the set of all complex functions which are regular in the closed half-plane \( \Re s > 1 \).

We denote by \( \log \) that branch of the complex logarithm which is real for positive arguments, and we set \( z^s = \exp(z \log s) \).

**Definition 4.** An arithmetical formation \( \mathfrak{D} \) consists of

1) a reduced Krull monoid \( H \), together with a divisor theory \( H \hookrightarrow D = \mathcal{F}(P) \) such that the divisor class group \( G = D/H \) is of finite order \( N \in \mathbb{N} \);

2) a completely multiplicative function \( |\cdot| : D \to \mathbb{N}_0 \) satisfying \( |a| > 1 \) for all \( a \neq 1 \) such that, for every \( g \in G \),
\[
\sum_{p \in P \cap g} |p|^{-s} = \frac{1}{N} \log \frac{1}{s-1} + h(s)
\]
holds in the half-plane \( \Re s > 1 \) for some function \( h \in \Lambda \).

Whenever we deal with an arithmetical formation \( \mathfrak{D} \), we use all notations as introduced above. We write \( G \) additively, and for \( a \in D \) we denote by \( [a] \in G \) the divisor class containing \( a \). By 2), \( g \cap P \) is infinite for every \( g \in G \).

**Main Example (continued).** We pick up again the main example discussed in § 2 and let now \( R \) be the ring of integers of an algebraic number field. For \( a \in D \) (an ideal of \( R \) which is relatively prime to \( \mathfrak{f} \)), we set \( |a| = (R : a) \); then \( |\cdot| : D \to \mathbb{N} \) is completely multiplicative and defines on \( D \) the structure of an arithmetical formation (with respect to \( H^* \) as well as with respect to \( H \)), see [10, Ch. VII, § 2]. For \( 0 \neq a \in R \), we have \( |aR| = |N(a)| \), where \( N \) denotes the ordinary norm to \( \mathbb{Q} \).

**Proposition 4.** Let \( \mathfrak{D} \) be an arithmetical formation as in Definition 4 and \( S \in \mathcal{F}(G) \) such that \( \sigma(S) > 0 \). Then we have, as \( x \to \infty \),
\[
\#\{a \in D \mid \beta^H(a) = S\} \sim \frac{\sigma(S)\chi(S)}{N^\sigma(S)} \frac{x}{(\log \log x)^\sigma(S) - 1}.
\]

**Proof:** It is sufficient to prove that
\[
(*) \quad \sum_{a \in D \atop \beta^H(a) = S} |a|^{-s} = \chi(S) \frac{\sigma(S)}{N^\sigma(S)} \left( \log \frac{1}{s-1} \right)^\sigma(S) + P\left( \log \frac{1}{s-1} \right)
\]
for $\Re s > 1$, where $P \in \Lambda[X]$ is a polynomial of degree less than $\sigma(S)$. Then we apply the Tauberian Theorem of Ikehara and Delange, see [9, Ch. III, § 3]. The proof of (*) can be given in two different ways: one may either follow the arguments in the proof of [10, Theorem 9.4] or those in the proof of [6, Proposition 4]; details are left to the reader.

**Theorem.** Let $\mathcal{D}$ be an arithmetical formation as in Definition 4, $G^* < G$ a subgroup and $H^* = \{a \in D \mid [a] \in G^*\}$. Let $S^* \in \mathcal{B}(G/G^*)$ be a block satisfying $\sigma(S^*) > 0$, and $g^* \in G^*$. Then we have, as $x \to \infty$,

$$
\#\{a \in g^* \mid |a| \leq x, \ \beta^{H^*}(a) = S^*\} \sim \frac{1}{\#G^*} \frac{\sigma(S^*)\chi(S^*)}{(G: G^*)^{\sigma(S^*)}} \frac{x}{\log x} (\log \log x)^{\sigma(S^*)-1}.
$$

**Proof:** Since

$$
\{a \in g^* \mid \beta^{H^*}(a) = S^*\} = \bigcup_{S \in \mathcal{F}(G)} \{a \in D \mid \beta^H(a) = S\}
$$

(disjoint union), Proposition 4 implies, observing $\sigma(\theta(S)) = \sigma(S)$,

$$
\#\{a \in g^* \mid |a| \leq x, \ \beta^{H^*}(a) = S^*\} \sim c \frac{x}{\log x} (\log \log x)^{\sigma(S^*)-1},
$$

where

$$
c = \frac{\sigma(S^*)}{N\sigma(S^*)} \sum_{S \in \mathcal{F}(G)} \chi(S^*);
$$

now the assertion follows from Proposition 2, iii).

§ 4. ARITHMETICAL APPLICATIONS

**Proposition 5.** Let $R$ be the ring of integers of an algebraic number field with class group $C$ and $B \in \mathcal{B}(C)$ such that $\sigma(B) > 0$. Let $\mathfrak{f}$ be a cycle of $R$, and $a_0 \in R$ an element relatively prime to $\mathfrak{f}$. Then we have, as $x \to \infty$,

$$
\#\{aR \mid a \in R, \ a \equiv a_0 \mod \mathfrak{f}, \ |N(a)| \leq x, \ \beta(a) = B\} \sim \frac{\sigma(B)\chi(B)}{\phi^*(\mathfrak{f})^{h\sigma(B)}} \frac{x}{\log x} (\log \log x)^{\sigma(B)-1},
$$

where $h = \#C$ and $\phi^*(\mathfrak{f}) = \#(R/\mathfrak{f})^\times / \mathcal{U}(\mathfrak{f})$.

**Proof:** Obvious by Proposition 4, applied to the Main Example.

**Remark.** The case $B = 0$ in Proposition 5 yields the prime ideal theorem for principal primes in residue classes modulo $\mathfrak{f}$. 
Corollary. Let $R$ be the ring of integers of an algebraic number field with class group $C$ and $L \subset \mathbb{N}$ such that there exists a block $B \in B(C)$ satisfying $\mathcal{L}(B) = L$. Let $\mathfrak{f}$ be a cycle of $R$ and $a_0 \in R$ an element relatively prime to $\mathfrak{f}$. Then we have, as $x \to \infty$,

$$
\# \{ aR \mid a \in R, \ a \equiv a_0 \mod \mathfrak{f}, \ |N(a)| \leq x, \ \mathcal{L}(a) = L \} \sim c \frac{\sigma}{\phi^*(\mathfrak{f})} \frac{x}{\log x} (\log \log x)^{\sigma-1},
$$

where $\phi^*(f) = \#(R/\mathfrak{f})^\times / U(f)$, $h = \#C$, and $c \in \mathbb{Q}_{>0}$, $\sigma \in \mathbb{N}$ are given as follows:

$$
\sigma = \max \{ \sigma(B) \mid B \in B(C), \ \mathcal{L}(B) = L \}, \quad c = \sum_{\substack{B \in B(C) \\mathcal{L}(B)=L, \ \sigma(B)=\sigma}} \chi(B);
$$

in particular, $c$ and $\sigma$ depend only on $C$ and $L$.

Proof: The set $\mathcal{L} = \{ B \in B(C) \mid \mathcal{L}(B) = L \}$ is finite, and for $a \in R \setminus (R^\times \cup \{0\})$ we have $\mathcal{L}(a) = L$ if and only if $\beta(a) \in \mathcal{L}$. Now the assertion follows from Proposition 5. \(\square\)

Remarks. 1) Using the methods of J. Kaczorowski [7], it is possible to obtain more precise asymptotic formulas, from which we presented only the main term.

2) Using the methods developed in [6], it is possible to derive analogous results for algebraic function fields.

REFERENCES


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

(Received March 10, 1992)