ACTA ARITHMETICA
LXII.2 (1992)

Chebotarev formations and quantitative aspects of non-unique factorizations

by

Franz Halter-Koch (Graz)

Introduction. Let K be an algebraic number field, R its ring of integers and G its ideal class group. Every non-zero non-unit of R is a product of (finitely many) irreducible elements of R, but this factorization need not be unique (unless G is trivial). The deviation of R from being a unique factorization domain is measured by G. In recent years, several papers appeared describing the connection between phenomena of non-unique factorization and the structure of G; see [6], [8], [11] and the literature cited there.

Quantitative aspects of non-unique factorizations in algebraic number fields were first considered by E. Fogels [2], and then studied in detail by W. Narkiewicz, J. Śliwa, A. Geroldinger, J. Kaczorowski and the author. For a non-zero non-unit $\alpha \in R$, let $\mathbf{f}(\alpha)$ be the number of essentially distinct factorizations of α in R and $\mathbf{l}(\alpha)$ the number of lengths of such factorizations. Consider the functions

$$\begin{aligned}
F_k(x) &= \#\{(\alpha) \mid \alpha \in R,\ |N(\alpha)| \le x,\ \mathbf{f}(\alpha) \le k\},\\
F'_k(x) &= \#\{n \in \mathbb{N} \mid n \le x,\ \mathbf{f}(n) \le k\},\\
G_k(x) &= \#\{(\alpha) \mid \alpha \in R,\ |N(\alpha)| \le x,\ \mathbf{l}(\alpha) \le k\},\\
G'_k(x) &= \#\{n \in \mathbb{N} \mid n \le x,\ \mathbf{l}(n) \le k\}\,;
\end{aligned}$$

all these functions have, as $x \to \infty$, an asymptotic behaviour of the form

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

where $C > 0,\ 0 < q < 1$ and $d \in \mathbb{N}_0$. This was shown

— for F_k by W. Narkiewicz [28]; he showed that $q = 1/\#G$ and gave a combinatorial description of d [29], [33];

— for F'_k by J. Śliwa [37] (using a method of R. W. K. Odoni [34] who dealt with the case $k = 1$); here q does not depend on k;

— for G_k and G'_k by J. Śliwa [38]; in both cases the exponents were investigated by A. Geroldinger [5], [7].

For quadratic number fields, W. Narkiewicz [24], [26], [27] proved substantially stronger results: He determined C explicitly and considered the functions F_k' and G_k' for residue classes of an arbitrary rational modulus. Several other functions connected with non-unique factorizations were studied in [9], [14], [15].

In this paper we give a common generalization of all these results. We consider an arbitrary finite extension $\overline{K}/K$ of algebraic number fields, a cycle $\mathfrak{f}$ of K, and we investigate factorization properties in $\overline{K}$ of integers $\alpha \in K$ from a given residue class modulo $\mathfrak{f}$. To do this, we proceed axiomatically; we introduce the concept of a Chebotarev formation which turns out to be the appropriate setting for problems of this kind. The results proved in this abstract setting apply not only to algebraic number fields, but also to algebraic function fields and, even more generally, to generalized Hilbert semigroups in holomorphy rings of global fields.

In Section 1 we introduce Chebotarev formations and discuss the relevant examples which are built from the above-mentioned Hilbert semigroups. In Section 2 we develop the combinatorial and analytical machinery used later on. The main results of this paper are contained in Sections 3 and 4: In Section 3 we deal with functions connected with the number of distinct factorizations, which fall into the category of so-called type-dependent factorization properties. In Section 4 we deal with functions connected with the number of different lengths of factorizations, which fall into the category of so-called valuation-dependent factorization properties.

Since our basic results are of abstract nature, their applications to number fields and function fields do not give as precise asymptotic results as could be obtained in the special context; this fact will be discussed in Section 5.

1. Formations.

By a *semigroup* H we always mean a commutative multiplicative monoid with unit element $1 \in H$ satisfying the cancellation law; in such a semigroup we have the usual notions of divisibility theory as developed in [19; Ch. 2.14]. H is called *atomic* if every non-unit $a \in H$ has a *factorization* of the form $a = u_1 \ldots u_r$, where $u_i \in H$ are irreducible elements. r is called the *length* of that factorization. In this paper, we shall study among others the following quantities:

$\mathbf{l}_H(a)$, the number of different lengths of factorizations of a;

$\mathbf{f}_H(a)$, the number of essentially different factorizations of a (two factorizations which agree up to the order of their factors and up to associated irreducible elements are not essentially different).

For a set P, we denote by $\mathcal{F}(P)$ the free abelian monoid with basis P;

every $a \in \mathcal{F}(P)$ has a unique representation in the form

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

where $v_p(a) \in \mathbb{N}_0$, $v_p(a) = 0$ for almost all $p \in P$. Every submonoid $H \subset \mathcal{F}(P)$ is atomic, and for $1 \neq a \in H$ the quantities $\mathbf{l}_H(a)$ and $\mathbf{f}_H(a)$ are finite [13].

If D is a semigroup and $H \subset D$ a subsemigroup, we define congruence modulo H by

$$a \equiv b \bmod H \quad \text{if and only if} \quad aH \cap bH \neq \emptyset\,;$$

this is a congruence relation on D, and we denote the quotient monoid (consisting of all congruence classes $g \subset D$) by D/H. A subsemigroup $H \subset D$ is called *saturated* if $H = \{a \in D \mid a \equiv 1 \bmod H\}$ (equivalently: $a, b \in H$ and $a \mid b$ in D implies $a \mid b$ in H).

Definition 1. A *formation* $[D, H]$ consists of a free abelian monoid $D = \mathcal{F}(P)$, together with a saturated subsemigroup $H \subset D$ such that $G = D/H$ is a finite abelian group, and $g \cap P \neq \emptyset$ for every $g \in G$. The elements of P are called *primes*, the elements of g are called (*divisor*) *classes*, and G is called the (*divisor*) *class group*.

We write G additively, and for $a \in D$ we denote by $[a] \in G$ the class containing a; the principal class $H = [1]$ is the zero of G.

The notion of a formation is closely connected with the notion of a divisor theory (cf. [11]): If $\partial : H \to D$ is a divisor theory with finite divisor class group, and every class contains at least one prime divisor, then $[D, \partial H]$ is a formation. As to the converse, we have the following simple result.

Lemma 1. *Let* $[D, H]$ *be a formation*, $D = \mathcal{F}(P)$ *and* $G = D/H$. *If* $\#G = 2$ *we assume that the non-principal class* $g \neq H$ *of* G *contains at least two primes. Then every* $p \in P$ *is a g.c.d. of two elements of* H. *In particular*, $H \hookrightarrow D$ *is a divisor theory.*

Proof. We may assume that $p \in P \setminus H$. If $\#G = 2$, $G = \{H, g\}$, then there exists $p' \in P \cap g$ such that $p \neq p'$, and $p = \gcd(p^2, pp')$. If $\#G \geq 3$, let $g \in G \setminus \{[p], H\}$ and let $p_1, p_2, p_3 \in P$ be such that $p_1 \in -[p]$, $p_2 \in -g$ and $p_3 \in g - [p]$; then $p = \gcd(pp_1, pp_2p_3)$. ∎

Usually the concept of a formation is accompanied by a norm function giving rise to abstract analytic number theory (cf. [17], [22]); we introduce this as an additional structure and call the corresponding objects *arithmetical formations*.

We denote by $\varLambda$ the algebra of all complex functions which are regular in the half-plane $\Re s > 1$ and also in some neighbourhood of $s = 1$. We shall always denote by log that branch of the complex logarithm which is real for positive arguments. As usual, we set $z^s = \exp(z \log s)$. We write $f \ll g$ for $f = O(g)$, and $f \asymp g$ for $f \ll g$ and $g \ll f$.

DEFINITION 2. Let $[D, H]$ be a formation, $D = \mathcal{F}(P)$ and $G = D/H$.

(a) A *norm* $|\cdot| : D \to \mathbb{N}$ is a completely multiplicative function satisfying $|a| > 1$ for all $a \in D \setminus \{1\}$.

(b) Let $|\cdot| : D \to \mathbb{N}$ be a norm. A subset $Q \subset P$ is called *regular* (for $|\cdot|$) if the Dirichlet series $\sum_{p\in Q} |p|^{-s}$ converges in the half-plane $\Re s > 1$, and if we have

$$\sum_{p\in Q} |p|^{-s} = \varrho \log \frac{1}{s-1} + h(s)\,,$$

where $h \in \varLambda$, $\varrho \in [0,1]$ and Q is finite if $\varrho = 0$; $\varrho = \varrho(Q)$ is called the *density* of Q.

(c) Let $|\cdot| : D \to \mathbb{N}$ be a norm. The triple $[D, H, |\cdot|]$ is called an *arithmetical formation* if for every $g \in G$ the set $P \cap g$ is regular with density $1/\#G$.

PROPOSITION 1 (Abstract Prime Number Theorem). *Let $[D, H, |\cdot|]$ be an arithmetical formation, $D = \mathcal{F}(P)$, and let $Q \subset P$ be a regular subset with density $\varrho > 0$. Then Q is infinite and, as $x \to \infty$,*

$$\#\{p \in Q \mid |p| \le x\} \asymp \frac{x}{\log x}\,.$$

Proof. Apply the Tauberian Theorem of Ikehara–Delange (cf. [1], Theorem IV and Remark 4.2). ■

BASIC EXAMPLES. 1. Hilbert semigroups: For $f \in \mathbb{N}$, $f \ge 2$, and a subgroup $\varGamma < (\mathbb{Z}/f\mathbb{Z})^\times$, we set

$$H_{f,\varGamma} = \{a \in \mathbb{N} \mid a + f\mathbb{Z} \in \varGamma\}\,.$$

If $\mathbb{N}^{(f)}$ denotes the set of all positive integers relatively prime to f, and $|a| = a$, then $[\mathbb{N}^{(f)}, H_{f,\varGamma}, |\cdot|]$ is an arithmetical formation with class group $(\mathbb{Z}/f\mathbb{Z})^\times/\varGamma$; this follows from Dirichlet's Theorem (cf. [31; Th. 3.17]).

2. Algebraic integers: Let R be the ring of integers in an algebraic number field K of finite degree, H the semigroup of non-zero principal ideals of R and D the semigroup of all non-zero ideals of R. For $\mathfrak{a} \in D$, we set $|\mathfrak{a}| = (R : \mathfrak{a})$; then $[D, H, |\cdot|]$ is an arithmetical formation by [32; Ch. VII, §2] whose class group is just the ordinary ideal class group of R. Note that H is isomorphic to the multiplicative semigroup $R \setminus \{0\}$ modulo units, and thus H reflects the arithmetic of R.

In the sequel we introduce Hilbert semigroups in holomorphy rings of global fields; these form a common generalization of the above-mentioned two basic examples.

A *global field* K is either an algebraic number field or an algebraic function field in one variable over a finite field. Let $\mathcal{S}(K)$ denote the set of all non-archimedean places of K. For $v \in \mathcal{S}(K)$, let R_v be the valuation ring, $\mathfrak{P}_v$ the valuation ideal, k_v the residue field and $|v| = \# k_v$ the norm of v; we shall identify v with the associated normalized additive valuation $v : K \to \mathbb{Z} \cup \{\infty\}$. If $\overline{K}/K$ is a finite Galois extension with Galois group G, if $v \in \mathcal{S}(K)$ is unramified in $\overline{K}$, and $\overline{v} \in \mathcal{S}(\overline{K})$ lies above v, then $\left[\frac{\overline{K}/K}{\overline{v}}\right] \in G$ denotes the Frobenius automorphism for $\overline{v} \mid v$, and $\left(\frac{\overline{K}/K}{v}\right) \subset G$ its conjugacy class, the Artin symbol; see [3; Ch. 5]. If G is abelian, we identify $\left(\frac{\overline{K}/K}{v}\right) = \left[\frac{\overline{K}/K}{\overline{v}}\right]$. We make use of Chebotarev's density theorem in the following form.

PROPOSITION 2. *Let $\overline{K}/K$ be a finite Galois extension of global fields with Galois group G and $c \subset G$ a conjugacy class. Then we have*, *for $\Re s > 1$*,

$$\sum_{\substack{v \in \mathcal{S}(K) \\ \left(\frac{\overline{K}/K}{v}\right) = c}} |v|^{-s} = \frac{\# c}{[\overline{K} : K]} \log \frac{1}{s-1} + f(s)$$

for some $f \in \Lambda$.

Proof. See [3; Ch. 5]; there they have $O(1)$ instead of $f(s)$, but going through the proofs gives the result as asserted. A proof using L-series is sketched in [36]. Note that in the function field case $f(s)$ has infinitely many poles on the line $\Re s = 1$. ■

Let now K be a global field and $S \subset \mathcal{S}(K)$ a finite set, $S \neq \emptyset$ in function field case. Then

$$R = R_S = \bigcap_{v \in \mathcal{S}(K) \setminus S} R_v \subset K$$

is called the *holomorphy ring associated with S*. The ring R is a Dedekind domain with quotient field K and finite ideal class group. The set of maximal ideals of R is given by

$$\mathcal{P}_R = \{\mathfrak{P}_v \cap R \mid v \in \mathcal{S}(K) \setminus S\}.$$

We denote by $\mathcal{I}_R$ the semigroup of all non-zero ideals and by $\mathcal{H}_R$ the semigroup of all non-zero principal ideals of R. For $\mathfrak{a} \in \mathcal{I}_R$, we set $|\mathfrak{a}| = (R : \mathfrak{a})$; then we have $|\mathfrak{P}_v \cap R| = |v|$ for all $v \in \mathcal{S}(K) \setminus S$. Proofs of these facts may be found in [39; Ch. 4] for the number field case and in [3; Ch. 2.7] for the function field case.

Next we introduce S-ray class groups. Let $R = R_S$ be a holomorphy ring in a global field K as above. By a *cycle* of R we mean a formal product $\mathfrak{f} = \mathfrak{f}_0 v_1 \ldots v_m$, where $\mathfrak{f}_0 \in \mathcal{I}_R$, $m \geq 0$ and $v_1, \ldots, v_m : K \to \mathbb{R}$ are real embeddings ($m=0$ in the function field case). Associated with such a cycle $\mathfrak{f}$, we introduce the following semigroups:

$\mathcal{I}_R^{(\mathfrak{f})}$, the semigroup of all $\mathfrak{a}\in\mathcal{I}_R$ which are relatively prime to $\mathfrak{f}_0$; in particular, $\mathcal{I}_R^{(1)}=\mathcal{I}_R$. If $\mathcal{P}_R^{(\mathfrak{f})}=\mathcal{P}_R\cap\mathcal{I}_R^{(\mathfrak{f})}$, then $\mathcal{I}_R^{(\mathfrak{f})}=\mathcal{F}(\mathcal{P}_R^{(\mathfrak{f})})\subset\mathcal{I}_R$.

$\mathcal{H}_R^{(\mathfrak{f})}=\mathcal{H}_R\cap\mathcal{I}_R^{(\mathfrak{f})}$; in particular $\mathcal{H}_R^{(1)}=\mathcal{H}_R$. $\mathcal{H}_R^{(\mathfrak{f})}\subset\mathcal{I}_R^{(\mathfrak{f})}$ is a saturated subsemigroup, and $\mathcal{I}_R^{(\mathfrak{f})}/\mathcal{H}_R^{(\mathfrak{f})}=\mathcal{I}_R/\mathcal{H}_R$ is the ideal class group of R.

$\mathcal{S}_R^{(\mathfrak{f})}=\{(\alpha)\in\mathcal{H}_R^{(\mathfrak{f})}\mid\alpha\in R,\ \alpha\equiv 1 \bmod \mathfrak{f}\}$, the principal ray modulo $\mathfrak{f}$ in R; here $\alpha\equiv 1\bmod\mathfrak{f}$ means as usual $v(\alpha-1)\geq v(\mathfrak{f})$ for all $v\in\mathcal{S}(K)\setminus S$ and $v_\mu(\alpha)>0$ for all $\mu\in\{1,\dots,m\}$. $\mathcal{S}_R^{(\mathfrak{f})}\subset\mathcal{I}_R^{(\mathfrak{f})}$ is a saturated subsemigroup, and $\mathcal{I}_R^{(\mathfrak{f})}/\mathcal{S}_R^{(\mathfrak{f})}$ is a finite abelian group, called the *S-ray class group modulo* $\mathfrak{f}$ (cf. [12]). It gives rise to the following exact sequence of finite abelian groups:

$$0\to\mathcal{H}_R^{(\mathfrak{f})}/\mathcal{S}_R^{(\mathfrak{f})}\to\mathcal{I}_R^{(\mathfrak{f})}/\mathcal{S}_R^{(\mathfrak{f})}\to\mathcal{I}_R/\mathcal{H}_R\to 0\,.$$

By a *generalized Hilbert semigroup in R defined modulo* $\mathfrak{f}$ we mean a saturated subsemigroup $H\subset\mathcal{H}_R^{(\mathfrak{f})}$ such that $\mathcal{S}_R^{(\mathfrak{f})}\subset H$. Obviously, $H=\mathcal{H}_R$ is the simplest example of a Hilbert semigroup in R.

If $K=\mathbb{Q}$, $R=\mathbb{Z}$ and $\mathfrak{f}=f\infty$ for some $f\in\mathbb{N}$, then we recover the classical Hilbert semigroups by means of the identifications $\mathcal{I}_{\mathbb{Z}}^{(f\infty)}=\mathbb{N}^{(f)}$ and $\mathcal{S}_{\mathbb{Z}}^{(f\infty)}=H_{f,\{1+f\mathbb{Z}\}}$.

PROPOSITION 3. *Let H be a generalized Hilbert semigroup in a holomorphy ring R of a global field defined modulo a cycle $\mathfrak{f}$ of R. Then $[\mathcal{I}_R^{(\mathfrak{f})},H,|\cdot|]$ is an arithmetical formation.*

Proof. Obviously, $H\subset\mathcal{I}_R^{(\mathfrak{f})}=\mathcal{F}(\mathcal{P}_R^{(\mathfrak{f})})$ is a saturated subsemigroup. Since $\mathcal{I}_R^{(\mathfrak{f})}/\mathcal{S}_R^{(\mathfrak{f})}$ is a group, $\mathcal{I}_R^{(\mathfrak{f})}/H$ and $H/\mathcal{S}_R^{(\mathfrak{f})}$ are also groups, and every class $g_0\in\mathcal{I}_R^{(\mathfrak{f})}/H$ is the union of $\#H/\mathcal{S}_R^{(\mathfrak{f})}$ ordinary ray classes $g\in\mathcal{I}_R^{(\mathfrak{f})}/\mathcal{S}_R^{(\mathfrak{f})}$. Therefore it is sufficient to prove that, for every $g\in\mathcal{I}_R^{(\mathfrak{f})}/\mathcal{S}_R^{(\mathfrak{f})}$, there exists $h_g\in\varLambda$ such that

$$\sum_{\mathfrak{p}\in g\cap\mathcal{P}_R^{(\mathfrak{f})}}|\mathfrak{p}|^{-s}=\frac{1}{(\mathcal{I}_R^{(\mathfrak{f})}:\mathcal{S}_R^{(\mathfrak{f})})}\log\frac{1}{s-1}+h_g(s)$$

for $\Re s>1$.

Let K be the quotient field of R and $S\subset\mathcal{S}(K)$ a finite subset such that $R=R_S$. Let $K^{S,\mathfrak{f}}$ be the S-ray class field modulo $\mathfrak{f}$ of K as introduced in [12]. $K^{S,\mathfrak{f}}/K$ is abelian, unramified outside S, and the Artin symbol induces an isomorphism

$$\theta:\mathcal{I}_R^{(\mathfrak{f})}/\mathcal{S}_R^{(\mathfrak{f})}\xrightarrow{\sim}\mathrm{Gal}\,(K^{S,\mathfrak{f}}/K)\,,$$

given by

$$\theta([\mathfrak{P}_v\cap R])=\left(\frac{K^{S,\mathfrak{f}}/K}{v}\right).$$

If $g \in \mathcal{I}_R^{(\mathfrak{f})}/\mathcal{S}_R^{(\mathfrak{f})}$ and $\Re s > 1$, then

$$\sum_{\mathfrak{p} \in g \cap \mathcal{P}_R^{(\mathfrak{f})}} |\mathfrak{p}|^{-s} = \sum_{\substack{v \in \mathcal{S}(K) \setminus S \\ \left(\frac{K^{S,\mathfrak{f}}/K}{v}\right) = \theta(g)}} |v|^{-s}\,,$$

and the assertion follows from Proposition 2. ∎

Definition 3. Let $[D, H, |\cdot|]$ be an arithmetical formation, $D = \mathcal{F}(P)$ and $G = D/H$. Let $[\overline{D}, \overline{H}]$ be a formation, $\overline{D} = \mathcal{F}(\overline{P})$, $\overline{G} = \overline{D}/\overline{H}$, and let $\varphi : D \to \overline{D}$ be a semigroup homomorphism satisfying $\varphi(H) \subset \overline{H}$.

Two primes $p, p' \in P$ are called *φ-equivalent* if $[p] = [p'] \in G$, and a factorization of the form

$$\varphi(p) = \prod_{i=1}^{r} \overline{p}_i^{\,e_i}$$

with $r \in \mathbb{N}_0$, distinct $\overline{p}_1, \ldots, \overline{p}_r \in \overline{P}$ and $e_i \in \mathbb{N}$ implies

$$\varphi(p') = \prod_{i=1}^{r} \overline{p}_i'^{\,e_i}$$

with distinct $\overline{p}_1', \ldots, \overline{p}_r' \in \overline{P}$ such that $[\overline{p}_i] = [\overline{p}_i'] \in \overline{G}$ for all $i \in \{1, \ldots, r\}$.

The triple $([D, H, |\cdot|], [\overline{D}, \overline{H}], \varphi)$ is called a *Chebotarev formation* (with *base formation* $[D, H, |\cdot|]$, *top formation* $[\overline{D}, \overline{H}]$ and *embedding* φ) if there are only finitely many φ-equivalence classes in P, and these are regular subsets of P.

There is a trivial example: If $[D, H, |\cdot|]$ is an arithmetical formation, then $([D, H, |\cdot|], [D, H], \mathrm{id})$ is a Chebotarev formation. Less trivial examples of arithmetical importance are furnished by the following proposition which generalizes the method of Odoni [34].

Proposition 4. *Let $\overline{K}/K$ be a finite separable extension of global fields. Let $R \subset K$ and $\overline{R} \subset \overline{K}$ be holomorphy rings such that $R \subset \overline{R}$, and let $H \subset R$* (*resp.* $\overline{H} \subset \overline{R}$) *be generalized Hilbert semigroups defined modulo a cycle $\mathfrak{f}$ of R* (*resp.* $\overline{\mathfrak{f}}$ *of* $\overline{R}$). *Define $\varphi : \mathcal{I}_R \to \mathcal{I}_{\overline{R}}$ by $\varphi(\mathfrak{a}) = \mathfrak{a}\overline{R}$ and suppose that $\varphi(H) \subset \overline{H}$. Then we also have $\varphi(\mathcal{I}_R^{(\mathfrak{f})}) \subset \mathcal{I}_{\overline{R}}^{(\overline{\mathfrak{f}})}$, and $([\mathcal{I}_R^{(\mathfrak{f})}, H, |\cdot|], [\mathcal{I}_{\overline{R}}^{(\overline{\mathfrak{f}})}, \overline{H}], \varphi)$ is a Chebotarev formation.*

Proof. Let $S \subset \mathcal{S}(K), \overline{S} \subset \mathcal{S}(\overline{K})$ be finite sets such that $R = R_S$ and $\overline{R} = R_{\overline{S}}$. If $\mathfrak{a} \in \mathcal{I}_R^{(\mathfrak{f})}$ then $\mathfrak{a}^m \in H$ for some $m \in \mathbb{N}$, whence $\varphi(\mathfrak{a})^m \in \overline{H} \subset \mathcal{I}_{\overline{R}}^{(\overline{\mathfrak{f}})}$ and therefore $\varphi(\mathfrak{a}) \in \mathcal{I}_{\overline{R}}^{(\overline{\mathfrak{f}})}$.

Therefore it remains to show that the φ-equivalence classes in $\mathcal{P}_R^{(\mathfrak{f})}$ are finitely many regular sets. Let $K^{S,\mathfrak{f}}$ be the S-ray class field modulo $\mathfrak{f}$ of

K, $\overline{K}^{\overline{S},\bar{\mathfrak{f}}}$ the $\overline{S}$-ray class field modulo $\bar{\mathfrak{f}}$ of $\overline{K}$, $L = K^{S,\mathfrak{f}}\overline{K}^{\overline{S},\bar{\mathfrak{f}}}$ and N/K the normal hull of L/K (inside a fixed algebraic closure of K). The primes $\mathfrak{p} \in \mathcal{P}_R^{(\mathfrak{f})}$ are of the form $\mathfrak{p} = \mathfrak{P}_v \cap R$, where $v \in \mathcal{S}(K) \setminus S$. Let $\mathcal{P}^*$ be the set of all $\mathfrak{p} = \mathfrak{P}_v \cap R \in \mathcal{P}_R^{(\mathfrak{f})}$ for which either v ramifies in N or there exists some $w \in \overline{S}$ satisfying $w \,|\, v$. The set $\mathcal{P}^*$ is finite and therefore it splits into finitely many regular φ-equivalence classes.

We claim that two primes $\mathfrak{p} = \mathfrak{P}_v \cap R$, $\mathfrak{p}' = \mathfrak{P}_{v'} \cap R \in \mathcal{P}_R^{(\mathfrak{f})} \setminus \mathcal{P}^*$ (where $v, v' \in \mathcal{S}(K) \setminus S$) are φ-equivalent if $\left(\frac{N/K}{v}\right) = \left(\frac{N/K}{v'}\right)$; then the assertion follows from Proposition 2. So let $\mathfrak{p} = \mathfrak{P}_v \cap R$ and $\mathfrak{p}' = \mathfrak{P}_{v'} \cap R \in \mathcal{P}_R^{(\mathfrak{f})} \setminus \mathcal{P}^*$ be primes satisfying $\left(\frac{N/K}{v}\right) = \left(\frac{N/K}{v'}\right)$; by [18; §23], v and v' have the same splitting type in every intermediate field $K \subset M \subset N$. In particular, $\left(\frac{K^{S,\mathfrak{f}}/K}{v}\right) = \left(\frac{K^{S,\mathfrak{f}}/K}{v'}\right)$, and therefore $\mathfrak{p}$ and $\mathfrak{p}'$ lie in the same S-ray class $g \in \mathcal{I}_R^{(\mathfrak{f})}/\mathcal{S}_R^{(\mathfrak{f})}$. This implies $[\mathfrak{p}] = [\mathfrak{p}'] \in \mathcal{I}_R^{(\mathfrak{f})}/H$, since every class of $\mathcal{I}_R^{(\mathfrak{f})}/H$ is a union of classes $g \in \mathcal{I}_R^{(\mathfrak{f})}/\mathcal{S}_R^{(\mathfrak{f})}$. Now let $\bar{v}_1, \ldots, \bar{v}_r$ (resp. $\bar{v}_1', \ldots, \bar{v}_r'$) be the places of $\overline{K}$ above v (resp. v'); by assumption, they do not lie in $\overline{S}$, and therefore

$$\varphi(\mathfrak{p}) = \prod_{i=1}^{r} \mathfrak{P}_i, \qquad \varphi(\mathfrak{p}') = \prod_{i=1}^{r} \mathfrak{P}_i',$$

where $\mathfrak{P}_i = \mathfrak{P}_{\bar{v}_i} \cap \overline{R}$ and $\mathfrak{P}_i' = \mathfrak{P}_{\bar{v}_i'} \cap \overline{R} \in \mathcal{P}_{\overline{R}}^{(\bar{\mathfrak{f}})}$. Since every divisor class of $[\mathcal{I}_{\overline{R}}^{(\bar{\mathfrak{f}})}, \overline{H}]$ is a union of $\overline{S}$-ray classes $\bar{g} \in \mathcal{I}_{\overline{R}}^{(\bar{\mathfrak{f}})}/\mathcal{S}_{\overline{R}}^{(\bar{\mathfrak{f}})}$, it is sufficient to prove that the $\overline{S}$-ray classes $\bar{g}_i \in \mathcal{I}_{\overline{R}}^{(\bar{\mathfrak{f}})}/\mathcal{S}_{\overline{R}}^{(\bar{\mathfrak{f}})}$ containing $\mathfrak{P}_i$ coincide with those containing the primes $\mathfrak{P}_i'$. By Artin reciprocity, the $\overline{S}$-ray classes modulo $\bar{\mathfrak{f}}$ containing $\mathfrak{P}_i$ (resp. $\mathfrak{P}_i'$) are uniquely determined by $\left(\frac{\overline{K}^{\overline{S},\bar{\mathfrak{f}}}/\overline{K}}{\bar{v}_i}\right)$ (resp. $\left(\frac{\overline{K}^{\overline{S},\bar{\mathfrak{f}}}/\overline{K}}{\bar{v}_i'}\right)$) and therefore it is sufficient to prove that

$$\left\{\left(\frac{\overline{K}^{\overline{S},\bar{\mathfrak{f}}}/\overline{K}}{\bar{v}_i}\right) \,\middle|\, i = 1, \ldots, r\right\} = \left\{\left(\frac{\overline{K}^{\overline{S},\bar{\mathfrak{f}}}/\overline{K}}{\bar{v}_i'}\right) \,\middle|\, i = 1, \ldots, r\right\}.$$

In fact, we shall prove that the set $\left\{\left(\frac{\overline{K}^{\overline{S},\bar{\mathfrak{f}}}/\overline{K}}{\bar{v}_i}\right) \,\middle|\, i = 1, \ldots, r\right\} \subset \operatorname{Gal}(\overline{K}^{\overline{S},\bar{\mathfrak{f}}}/\overline{K})$ is uniquely determined by the conjugacy class $\left(\frac{N/K}{v}\right) \subset \operatorname{Gal}(N/K)$. To do this, let $w_i \in \mathcal{S}(N)$ be a place above $\bar{v}_i$; then

$$\left(\frac{\overline{K}^{\overline{S},\bar{\mathfrak{f}}}/\overline{K}}{\bar{v}_i}\right) = \left[\frac{N/\overline{K}}{w_i}\right]\Big|\overline{K}^{\overline{S},\bar{\mathfrak{f}}} \quad \text{and} \quad \left[\frac{N/\overline{K}}{w_i}\right] = \left[\frac{N/K}{w_i}\right]^{f_i},$$

where f_i is the residue class degree of $\bar{v}_i \mid v_i$. Since $\left(\frac{N/K}{v}\right)$ consists of the elements $\left[\frac{N/K}{w_i}\right]$ and its conjugates in $\mathrm{Gal}(N/K)$, and since $\mathrm{Gal}(\overline{K}^{\overline{S},\bar{\mathfrak{f}}}/\overline{K})$ is abelian, the assertion follows. ∎

2. Combinatorial and analytical tools. We start by generalizing the concept of types as introduced in [28] and [37] (cf. [14]).

Definition 4. Let $\mathfrak{D} = [D, H, |\cdot|]$ be an arithmetical formation, $D = \mathcal{F}(P)$ and $G = D/H$.

(a) A *partition* of P (with respect to $\mathfrak{D}$) is a finite sequence

$$\mathcal{P} = (P_0, P_1, \ldots, P_m) \quad (m \in \mathbb{N})$$

of mutually disjoint subsets $P_j \subset P$ possessing the following properties:

(P1) $P = P_0 \cup P_1 \cup \ldots \cup P_m$.

(P2) For every $g \in G$, the set $P_0 \cap g$ is regular.

(P3) For every $j \in \{1, \ldots, m\}$, P_j is regular, and there exists $g_j \in G$ such that $P_j \subset g_j$.

For $a \in D$, we call

$$\delta^{\mathcal{P}}(a) = \sum_{\substack{j=1 \\ \varrho(P_j)>0}}^{m} \#\{p \in P_j \mid v_p(a) = 1\}$$

the $\mathcal{P}$-*depth* of a.

(b) Let $\mathcal{P} = (P_0, P_1, \ldots, P_m)$ be a partition of P. A $\mathcal{P}$-*type* is a sequence $t = ((t_{j,\nu})_{\nu\in\mathbb{N}})_{j=1,\ldots,m}$ of integers $t_{j,\nu} \in \mathbb{N}_0$ such that $t_{j,\nu} = 0$ for all but finitely many pairs (j, ν). Let $\mathcal{T}(\mathcal{P})$ be the set of all $\mathcal{P}$-types. Under componentwise addition, $\mathcal{T}(\mathcal{P})$ is a free abelian monoid.

(c) A $\mathcal{P}$-type $t = ((t_{j,\nu})_{\nu\in\mathbb{N}})_{j=1,\ldots,m}$ is called *normalized* if for every $j \in \{1, \ldots, m\}$ there exists $\lambda_j(t) \in \mathbb{N}_0$ such that $t_{j,\nu} = 0$ if $\nu > \lambda_j(t)$, and $1 \le t_{j,1} \le t_{j,2} \le \ldots \le t_{j,\lambda_j(t)}$ if $\lambda_j(t) \ge 1$; in this case we write $t = ((t_{j,\nu})_{\nu\le\lambda_j(t)})_{j=1,\ldots,m}$. Let $\mathcal{T}^*(\mathcal{P})$ be the set of all normalized $\mathcal{P}$-types.

For every $t = ((t_{j,\nu})_{\nu\in\mathbb{N}})_{j=1,\ldots,m} \in \mathcal{T}(\mathcal{P})$ there is a family of bijective maps $(\psi_j : \mathbb{N} \to \mathbb{N})_{j=1,\ldots,m}$ such that the $\mathcal{P}$-type $t^* = ((t_{j,\psi_j(\nu)})_{\nu\in\mathbb{N}})_{j=1,\ldots,m}$ is normalized; $t^* \in \mathcal{T}^*(\mathcal{P})$ is uniquely determined by t; it is called the *normalization* of t.

(d) For $t = ((t_{j,\nu})_{\nu\le\lambda_j(t)})_{j=1,\ldots,m} \in \mathcal{T}^*(\mathcal{P})$ and $j \in \{1, \ldots, m\}$, we denote by $\kappa_j(t)$ the number of permutations $\sigma \in \mathfrak{S}_{\lambda_j(t)}$ satisfying $t_{j,\sigma(\nu)} = t_{j,\nu}$ for all $\nu \in \{1, \ldots, \lambda_j(t)\}$, and we set

$$\kappa(t) = \prod_{j=1}^{m} \kappa_j(t)^{-1}\,.$$

(e) For $t = ((t_{j,\nu})_{\nu\in\mathbb{N}})_{j=1,\ldots,m} \in \mathcal{T}^*(\mathcal{P})$ and $j \in \{1, \ldots, m\}$, we denote by $\delta_j(t)$ the number of $\nu \in \mathbb{N}$ for which $t_{j,\nu} = 1$, and we call

$$\delta(t) = \sum_{\substack{j=1 \\ \varrho(P_j)>0}}^{m} \delta_j(t)$$

the *depth* of t (depending on $\mathfrak{D}$ and $\mathcal{P}$).

(f) For $a \in D$ and $t = ((t_{j,\nu})_{\nu\le\lambda_j})_{j=1,\ldots,m} \in \mathcal{T}^*(\mathcal{P})$, we say that *$a$ has the $\mathcal{P}$-type t, $\boldsymbol{\tau}^{\mathcal{P}}(a) = t$*, if

$$a = a_0 \cdot \prod_{j=1}^{m} \prod_{\nu=1}^{\lambda_j} p_{j,\nu}^{t_{j,\nu}}\,,$$

where $a_0 \in \mathcal{F}(P_0)$, and $p_{j,\nu} \in P_j$ are distinct. Obviously, $\boldsymbol{\tau}^{\mathcal{P}}(a) = t$ implies $\delta^{\mathcal{P}}(a) = \delta(t)$.

Theorem 1. *Let $[D, H, |\cdot|]$ be an arithmetical formation, $D = \mathcal{F}(P)$ and $\mathcal{P} = (P_0, P_1, \ldots, P_m)$ a partition of P. Let $\emptyset \ne \mathfrak{T} \subset \mathcal{T}^*(\mathcal{P})$ and suppose that*

$$d = \max\{\delta(t) \mid t \in \mathfrak{T}\} < \infty\,.$$

Let $y \in G$ and let $a_1 \in y$ satisfy $\boldsymbol{\tau}^{\mathcal{P}}(a_1) \in \mathfrak{T}$ and $\delta^{\mathcal{P}}(a_1) = d$. If $\varrho_0 = \varrho(P_0)$ and $\varrho_0 + d > 0$, then we have, as $x \to \infty$,

$$\#\{a \in y \mid |a| \le x, \boldsymbol{\tau}^{\mathcal{P}}(a) \in \mathfrak{T}\} \asymp x(\log x)^{-1+\varrho_0}(\log\log x)^{d'}\,,$$

where

$$d' = \begin{cases} d & \text{if } \varrho_0 > 0, \\ d-1 & \text{if } \varrho_0 = 0. \end{cases}$$

If $\varrho_0 = d = 0$, then

$$\#\{a \in y \mid |a| \le x,\ \boldsymbol{\tau}^{\mathcal{P}}(a) \in \mathfrak{T}\} \ll x^{\eta}$$

for some $0 < \eta < 1$.

Proof. 1. We first show that it is sufficient to prove Theorem 1 under the additional assumption

$$(+) \qquad \text{If } g \in G \text{ and } P_0 \cap g \ne \emptyset\,, \text{ then } \varrho(P_0 \cap g) > 0\,.$$

Assume that Theorem 1 is true whenever (+) holds. We set $\{g_1, \ldots, g_k\} = \{g \in G \mid P_0 \cap g \ne \emptyset,\ \varrho(P_0 \cap g) = 0\}$, $P_0' = P_0 \setminus (g_1 \cup \ldots \cup g_k)$, $P_{m+i} = P_0 \cap g_i$

for $i = 1, \ldots, k$ and $\mathcal{P}' = (P_0', P_1, \ldots, P_m, P_{m+1}, \ldots, P_{m+k})$. Then $\mathcal{P}'$ is a partition of P satisfying (+). We define $\theta : \mathcal{T}^*(\mathcal{P}') \to \mathcal{T}^*(\mathcal{P})$ by

$$\theta(((t'_{j,\nu})_{\nu \le \lambda_j})_{j=1,\ldots,m+k} = ((t'_{j,\nu})_{\nu \le \lambda_j})_{j=1,\ldots,m}\,,$$

and we set

$$\mathfrak{T}' = \{t' \in \mathcal{T}^*(\mathcal{P}') \mid \theta(t') \in \mathfrak{T}\}\,.$$

For $a \in D$, we have $\boldsymbol{\tau}^{\mathcal{P}}(a) = \theta(\boldsymbol{\tau}^{\mathcal{P}'}(a))$, and therefore $\boldsymbol{\tau}^{\mathcal{P}}(a) \in \mathfrak{T}$ if and only if $\boldsymbol{\tau}^{\mathcal{P}'}(a) \in \mathfrak{T}'$. Since moreover $\delta(t') = \delta(\theta(t'))$ for all $t' \in \mathfrak{T}'$, the assertion of the theorem follows with $\mathcal{P}'$ and $\mathfrak{T}'$ instead of $\mathcal{P}$ and $\mathfrak{T}$.

2. The proof of Theorem 1 uses a Tauberian theorem for Dirichlet series, essentially due to H. Delange [1]. For convenience, we state it as the following lemma.

LEMMA 2. *Let*

$$f_0(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

be a Dirichlet series with real coefficients $a_n \ge 0$, *converging for* $\Re s > 1$, *and suppose that*

$$f_0(s) = \sum_{j=1}^{m} \left(\frac{1}{s-1}\right)^{w_j} \sum_{\nu=0}^{d_j} g_{j,\nu}(s) \left(\log \frac{1}{s-1}\right)^{\nu} + g_0(s)\,,$$

where $m \in \mathbb{N}$, $d_j \in \mathbb{N}_0$, $g_{j,\nu} \in \mathit{\Lambda}$, $g_{1,d_1}(1) > 0$, $g_0 \in \mathit{\Lambda}$, $w_1 \in \mathbb{R}$, $w_2, \ldots, w_m \in \mathbb{C}$ *and either* $m = 1$, $w_1 = 0$ *or* $m \ge 2$, $w_1 > \Re w_j \ge 0$ *for* $2 \le j \le m$. *Then the function*

$$A(x) = \sum_{n \le x} a_n$$

behaves as follows (*for* $x \to \infty$):

(i) *If* $w_1 = d_1 = 0$, *then* $A(x) = O(x^{\eta})$ *for some* $0 < \eta < 1$.

(ii) *If* $w_1 + d_1 > 0$, *then*

$$A(x) \asymp \begin{cases} x(\log x)^{-1+w_1}(\log\log x)^{d_1} & \text{if } w_1 > 0, \\ x(\log x)^{-1}(\log\log x)^{d_1-1} & \text{if } w_1 = 0. \end{cases}$$

Proof. (i) If $w_1 = d_1 = 0$, then f_0 is regular at $s = 1$, and therefore the defining Dirichlet series has an abscissa of absolute convergence $\sigma_0 < 1$. For $\sigma_0 < \eta < 1$, we have

$$\sum_{n \le x} \frac{a_n}{x^{\eta}} \le \sum_{n=1}^{\infty} \frac{a_n}{n^{\eta}} < \infty\,,$$

whence the assertion.

(ii) See [1] (Theorem IV and Remark 4.2); there the arguments are given for $w_j \in \mathbb{R}$, but they remain valid in the general case. ■

3. The following proposition embodies the crucial point in the proof of Theorem 1. We denote by $G^* = \operatorname{Hom}(G, \mathbb{C}^\times)$ the character group of G and by $\chi_0 \in G^*$ the principal character. For $\chi \in G^*$, we denote by $\bar{\chi}$ the conjugate character, and for $a \in D$ we set $\chi(a) = \chi([a])$. We denote by $G^*(P_0)$ the set of all $\chi \in G^*$ satisfying $\chi(p) = 1$ for all $p \in P_0$. We set $G_0 = \langle [p] \mid p \in P_0 \rangle$, and we identify $G^*(P_0)$ with $(G/G_0)^*$.

Proposition 5. *Under the hypothesis of Theorem* 1 *and the assumption* (+) *we have*, *for* $\chi \in G^*$ *and* $\Re s > 1$,

$$S_\chi = \sum_{\substack{a \in D \\ \boldsymbol{\tau}^{\mathcal{P}}(a) \in \mathfrak{T}}} \frac{\chi(a)}{|a|^s} = \left(\frac{1}{s-1}\right)^{\varrho_\chi} R_\chi\left(\log \frac{1}{s-1}\right),$$

where

$$\varrho_\chi = \sum_{g \in G} \chi(g) \varrho(P_0 \cap g),$$

and $R_\chi \in \Lambda[X]$ *is a polynomial of degree* $\deg R_\chi \le d$. *The coefficient of* X^d *in* R_χ *is of the form*

$$A_\chi(s) = \sum_{\gamma \in G/G_0} A_{\chi,\gamma}(s),$$

where $A_{\chi,\gamma} \in \Lambda$ *are functions with the following property*:

If there exists $g \in G$ *such that* $\gamma = g + G_0$, *and* $a_1 \in g$ *such that* $\boldsymbol{\tau}^{\mathcal{P}}(a_1) \in \mathfrak{T}$ *and* $\delta^{\mathcal{P}}(a_1) = d$, *then*

$$\bar{\chi}(g) A_{\chi,\gamma}(1) = A_{\chi_0,\gamma}(1) > 0$$

for all $\chi \in G^*(P_0)$; *otherwise* $A_{\chi,\gamma} = 0$ *for all* $\chi \in G^*$.

Proof of Theorem 1 (by means of Proposition 5 and Lemma 2). The orthogonality relations for characters imply

$$\begin{aligned}\sum_{\substack{a \in y \\ \boldsymbol{\tau}^{\mathcal{P}}(a) \in \mathfrak{T}}} |a|^{-s} &= \sum_{\substack{a \in D \\ \boldsymbol{\tau}^{\mathcal{P}}(a) \in \mathfrak{T}}} \frac{1}{\#G} \sum_{\chi \in G^*} \bar{\chi}(y) \frac{\chi(a)}{|a|^s} = \frac{1}{\#G} \sum_{\chi \in G^*} \bar{\chi}(y) S_\chi \\ &= \left(\frac{1}{s-1}\right)^{\varrho_0} R_0\left(\log \frac{1}{s-1}\right) \\ &\quad + \sum_{\chi \in G^* \setminus G^*(P_0)} \left(\frac{1}{s-1}\right)^{\varrho_\chi} \frac{\bar{\chi}(y)}{\#G} R_\chi\left(\log \frac{1}{s-1}\right),\end{aligned}$$

where

$$R_0 = \sum_{\chi \in G^*(P_0)} \frac{\bar{\chi}(y)}{\#G} R_\chi \in \Lambda[X] \,.$$

By Proposition 5, all R_χ (and hence also R_0) are polynomials of degree at most d, and the coefficient of X^d in R_0 is given by

$$A_0(s) = \sum_{\chi \in G^*(P_0)} \frac{\bar{\chi}(y)}{\#G} \sum_{\gamma \in G/G_0} A_{\chi,\gamma}(s) \,.$$

If $\Gamma = \{\gamma \in G/G_0 \mid A_{\chi_0,\gamma}(1) > 0\}$, then $y_0 + G \in \Gamma$ by assumption, and Proposition 5 implies

$$\begin{aligned} A_0(1) &= \sum_{\chi \in G^*(P_0)} \frac{\bar{\chi}(y)}{\#G} \sum_{\gamma \in \Gamma} \chi(\gamma) A_{\chi_0,\gamma}(1) \\ &= \sum_{\gamma \in \Gamma} \frac{A_{\chi_0,\gamma}(1)}{\#G} \sum_{\chi \in G^*(P_0)} \bar{\chi}(y)\chi(\gamma) > 0 \,, \end{aligned}$$

by the orthogonality relations. For $\chi \in G^* \setminus G^*(P_0)$, we have $\Re \varrho_\chi < \varrho_0$, and therefore the assertion follows from Lemma 2. ∎

4. Proof of Proposition 5. Every $a \in D$ has a unique decomposition $a = a_0 a_1$, where $a_0 \in \mathcal{F}(P_0)$ and $a_1 \in \mathcal{F}(P \setminus P_0)$, and we have $\boldsymbol{\tau}^{\mathcal{P}}(a) = \boldsymbol{\tau}^{\mathcal{P}}(a_1)$. This implies

$$S_\chi = \Bigg(\sum_{a_0 \in \mathcal{F}(P_0)} \frac{\chi(a_0)}{|a_0|^s} \Bigg) \Bigg(\sum_{\substack{a \in \mathcal{F}(P \setminus P_0) \\ \boldsymbol{\tau}^{\mathcal{P}}(a) \in \mathfrak{T}}} \frac{\chi(a)}{|a|^s} \Bigg) \,,$$

and Proposition 5 is a consequence of the following two lemmata dealing with the two factors.

LEMMA 3. *Under the assumptions of Proposition* 5 *we have*, *for every* $\chi \in G^*$ *and* $\Re s > 1$,

$$\sum_{a_0 \in \mathcal{F}(P_0)} \frac{\chi(a_0)}{|a_0|^s} = \left(\frac{1}{s-1} \right)^{\varrho_\chi} F_\chi(s) \,,$$

where $F_\chi \in \Lambda$. *If* $\chi \in G^*(P_0)$, *then* $F_\chi = F_{\chi_0}$, *and* $F_{\chi_0}(1) > 0$.

LEMMA 4. *Under the assumptions of Proposition* 5 *we have*, *for every* $\chi \in G^*$ *and* $\Re s > 1$,

$$S'_\chi = \sum_{\substack{a \in \mathcal{F}(P \setminus P_0) \\ \boldsymbol{\tau}^{\mathcal{P}}(a) \in \mathfrak{T}}} \frac{\chi(a)}{|a|^s} = R'_\chi \bigg(\log \frac{1}{s-1} \bigg) \,,$$

where $R'_\chi \in \Lambda[X]$ *and* $\deg R'_\chi \le d$. *The coefficient* $A'_\chi(s)$ *of* X^d *in* R'_χ *is of the form*

$$A'_\chi(s) = \sum_{\gamma \in G/G_0} A'_{\chi,\gamma}(s)\,,$$

where $A'_{\chi,\gamma} \in \Lambda$ *are functions with the following property*:

If there exist $g \in G$ *and* $a_1 \in g$ *such that* $\gamma = g + G_0, \boldsymbol{\tau}^{\mathcal{P}}(a_1) \in \mathfrak{T}$ *and* $\delta^{\mathcal{P}}(a_1) = d$, *then*

$$\overline{\chi}(g) A_{\chi,\gamma}(1) = A_{\chi_0,\gamma}(1) > 0$$

for every $\chi \in G^*(P_0)$; *otherwise* $A_{\chi,\gamma} = 0$ *for all* $\chi \in G^*$.

5. Proof of Lemma 3. For $\chi \in G^*$ and $\Re s > 1$, we make use of the identity

$$\sum_{a_0 \in \mathcal{F}(P_0)} \frac{\chi(a_0)}{|a_0|^s} = \prod_{p \in P_0} \left(1 - \frac{\chi(p)}{|p|^s}\right)^{-1} = \exp\left\{\sum_{p \in P_0} -\log\left(1 - \frac{\chi(p)}{|p|^s}\right)\right\}$$
$$= \exp\left\{\sum_{p \in P_0} \frac{\chi(p)}{|p|^s} + \sum_{p \in P_0} \sum_{\nu=2}^{\infty} \frac{\chi(p)^\nu}{\nu |p|^{\nu s}}\right\}.$$

By assumption, we have

$$\sum_{p \in P_0} \frac{\chi(p)}{|p|^s} = \sum_{g \in G} \chi(g) \left\{\varrho(P_0 \cap g) \log \frac{1}{s-1} + h_{g,0}(s)\right\}$$
$$= \varrho_\chi \log \frac{1}{s-1} + \sum_{g \in G} \chi(g) h_{g,0}(s)\,,$$

where $h_{g,0} \in \Lambda$; the assertion follows with

$$F_\chi(s) = \exp\left\{\sum_{p \in P_0} \sum_{\nu=2}^{\infty} \frac{\chi(p)^\nu}{\nu |p|^{\nu s}} + \sum_{g \in G} \chi(g) h_{g,0}(s)\right\}. \ \blacksquare$$

6. Proof of Lemma 4. Let $1 \le l \le m$ be such that $\varrho_j = \varrho(P_j) > 0$ for $1 \le j \le l$ and $\varrho_j = 0$ for $l < j \le m$. For $t \in \mathcal{T}^*(\mathcal{P})$, we set $\boldsymbol{\delta}(t) = (\delta_1(t), \ldots, \delta_l(t)) \in \mathbb{N}_0^l$, and for $\mathbf{d} = (d_1, \ldots, d_l) \in \mathbb{N}_0^l$, we set $|\mathbf{d}| = d_1 + \ldots + d_l$; this implies $\delta(t) = |\boldsymbol{\delta}(t)|$.

We proceed by induction on d and suppose that the assertion is true for all sets of types with depths less than d. We consider the decomposition

$$\mathfrak{T} = \biguplus_{\substack{\mathbf{d} \in \mathbb{N}_0^l \\ |\mathbf{d}| = d}} \mathfrak{T}(\mathbf{d}) \uplus \mathfrak{T}' \qquad \text{(disjoint union)}\,,$$

where $\mathfrak{T}(\mathbf{d}) = \{t \in \mathfrak{T} \mid \boldsymbol{\delta}(t) = \mathbf{d}\}$ and $\mathfrak{T}' = \{t \in \mathfrak{T} \mid \delta(t) < d\}$. By additivity and induction hypothesis, we may suppose that $\mathfrak{T} = \mathfrak{T}(\mathbf{d})$ for some $\mathbf{d} \in \mathbb{N}_0^l$.

Under this assumption, every $t \in \mathfrak{T}$ is of the form $t = ((t_{j,\nu})_{\nu \le \lambda_j(t)})_{j=1,\dots,m}$, where $t_{j,\nu} = 1$ for $\nu \le d_j$ and $t_{j,\nu} \ge 2$ for $d_j < \nu \le \lambda_j(t)$, and we obtain

$$S'_\chi = \sum_{(\mathbf{p})} \Big[\Big(\prod_{j=1}^{l} \prod_{\nu=1}^{d_j} \frac{\chi(g_j)}{|p_{j,\nu}|^s} \Big) \sum_{t \in \mathfrak{T}} \kappa(t) \sum_{(\mathbf{q},\mathbf{p},t)} \Big(\prod_{j=1}^{l} \prod_{\nu=d_j+1}^{\lambda_j(t)} \frac{\chi(g_j)^{t_{j,\nu}}}{|q_{j,\nu}|^{t_{j,\nu}s}} \Big) \times \sum_{(\mathbf{q},t)^*} \Big(\prod_{j=l+1}^{m} \prod_{\nu=1}^{\lambda_j(t)} \frac{\chi(g_j)^{t_{j,\nu}}}{|q_{j,\nu}|^{t_{j,\nu}s}} \Big) \Big],$$

where $(\mathbf{p})$ denotes the sum over all $(p_{j,1},\dots,p_{j,d_j})_{j=1,\dots,l}$ with distinct $p_{j,\nu} \in P_j$; if $d_j = 0$, the corresponding factor has to be given the value 1. The symbol $(\mathbf{q},\mathbf{p},t)$ denotes the sum over all $(q_{j,d_j+1},\dots,q_{j,\lambda_j(t)})_{j=1,\dots,l}$ with distinct $q_{j,\nu} \in P_j$ such that $\{p_{j,1},\dots,p_{j,d_j}\} \cap \{q_{j,d_j+1},\dots,q_{j,\lambda_j(t)}\} = \emptyset$ for all j; again, if $d_j = \lambda_j(t)$, the corresponding factor has to be given the value 1. The symbol $(\mathbf{q},t)^*$ denotes the sum over all $(q_{j,1},\dots,q_{j,\lambda_j(t)})_{j=l+1,\dots,m}$ with distinct $q_{j,\nu} \in P_j$; again, if $\lambda_j(t) = 0$, the corresponding factor has to be given the value 1.

For every $(\mathbf{p})$ and $t \in \mathfrak{T}$, we consider the decomposition

$$\sum_{(\mathbf{q},\mathbf{p},t)} (\dots) = \sum_{(\mathbf{q},t)} (\dots) - \sum_{(\mathbf{E})} \sum_{(\mathbf{q},\mathbf{p},t,\mathbf{E})} (\dots),$$

where $(\mathbf{q},t)$ denotes the sum over all $(q_{j,d_j+1},\dots,q_{j,\lambda_j(t)})_{j=1,\dots,l}$ with distinct $q_{j,\nu} \in P_j$. The symbol $(\mathbf{E})$ denotes the sum over all sequences $\mathbf{E} = (E_1,\dots,E_l) \ne (\emptyset,\dots,\emptyset)$ of subsets $E_j \subset \{1,\dots,d_j\}$, and for any such $\mathbf{E}$, the symbol $(\mathbf{q},\mathbf{p},t,\mathbf{E})$ denotes the sum over all $(q_{j,d_j+1},\dots,q_{j,\lambda_j(t)})_{j=1,\dots,l}$ with distinct $q_{j,\nu} \in P_j$ such that $\{q_{j,d_j+1},\dots,q_{j,\lambda_j(t)}\} \cap \{p_{j,1},\dots,p_{j,d_j}\} = \{p_{j,\nu} \mid \nu \in E_j\}$ for all j. For each $\mathbf{E}$, we apply the induction hypothesis for the sum

$$\overline{S}'_\chi = \sum_{(\mathbf{p})} \Big[(\dots) \sum_{t \in \mathfrak{T}} \kappa(t) \sum_{(\mathbf{q},\mathbf{p},t,\mathbf{E})} (\dots) \sum_{(\mathbf{q},t)^*} (\dots) \Big]$$

which is in fact a sum over types t' with $\delta(t') < d$; this implies $\overline{S}'_\chi = R(\log \frac{1}{s-1})$ for some polynomial $R \in \Lambda[X]$ with $\deg R < d$, and we are left with the sum

$$S''_\chi = \sum_{(\mathbf{p})} (\dots) \sum_{t \in \mathfrak{T}} \kappa(t) \sum_{(\mathbf{q},t)} (\dots) \sum_{(\mathbf{q},t)^*} (\dots),$$

where the second factor is independent of $(\mathbf{p})$. We must prove that S''_χ has the properties asserted for S'_χ.

The first factor of S''_χ is investigated by means of the decomposition

$$\sum_{(\mathbf{p})} (\dots) = \sum_{(\mathbf{p})^*} (\dots) - \sum_{(\mathbf{F})} \sum_{(\mathbf{p},\mathbf{F})} (\dots),$$

where $(\mathbf{p})^*$ denotes the sum over all $(p_{j,1},\ldots,p_{j,d_j})_{j=1,\ldots,l}$ with $p_{j,\nu}\in P_j$. The symbol $(\mathbf{F})$ denotes the sum over all sequences $\mathbf{F}=(F_1,\ldots,F_l)$ of subsets $F_j\subset\{1,\ldots,d_j\}$ such that $\#(F_1\times\ldots\times F_l)\ge 2$; for any such $\mathbf{F}$, the symbol $(\mathbf{p},\mathbf{F})$ denotes the sum over all $(p_{j,1},\ldots,p_{j,d_j})_{j=1,\ldots,l}$ with $p_{j,\nu}\in P_j$ satisfying $p_{j,\nu}=p_{j,\mu}$ for some j and $\mu\ne\nu$ if and only if $\{\mu,\nu\}\subset F_j$. For each $\mathbf{F}$, the induction hypothesis applies for the sum

$$\overline{S}''_\chi=\sum_{(\mathbf{F})}\sum_{(\mathbf{p},\mathbf{F})}(\ldots)\sum_{t\in\mathfrak{T}}\kappa(t)\sum_{(\mathbf{q},t)}(\ldots)\sum_{(\mathbf{q},t)^*}(\ldots)\,,$$

and we must prove that the sum

$$S^*_\chi=\sum_{(\mathbf{p})^*}(\ldots)\sum_{t\in\mathfrak{T}}\kappa(t)\sum_{(\mathbf{q},t)}(\ldots)\sum_{(\mathbf{q},t)^*}(\ldots)$$

has the properties asserted for S'_χ.

The first factor of S^*_χ is evaluated in the form

$$\begin{aligned}\sum_{(\mathbf{p})^*}(\ldots)&=\prod_{j=1}^{l}\Big[\sum_{p\in P_j}\frac{\chi(p)}{|p|^s}\Big]^{d_j}\\&=\prod_{j=1}^{l}\Big[\chi(g_j)\Big(\varrho_j\log\frac{1}{s-1}+h_j(s)\Big)\Big]^{d_j}=R_{0,\chi}\Big(\log\frac{1}{s-1}\Big)\,,\end{aligned}$$

where $h_j\in\Lambda$ and $R_{0,\chi}\in\Lambda[X]$ is a polynomial of degree d and leading coefficient

$$A_{0,\chi}=\prod_{j=1}^{l}[\chi(g_j)\varrho_j]^{d_j}\,.$$

For the calculation of the second factor of S^*_χ, we set $P_{l+1}\cup\ldots\cup P_m=\{r_1,\ldots,r_M\}$ (for some $M\in\mathbb{N}_0$) and find

$$\Big|\sum_{(\mathbf{q},t)^*}(\ldots)\Big|\le\prod_{j=1}^{M}\frac{1}{1-|r_j|^{-1}}\,,$$

whence

$$\Big|\sum_{t\in\mathfrak{T}}\kappa(t)\sum_{(\mathbf{q},t)}(\ldots)\sum_{(\mathbf{q},t)^*}(\ldots)\Big|\ll\sum_{a\in D_2}|a|^{-1}<\infty\,,$$

uniformly for $\Re s>1$, where $D_2=\{a\in D\mid v_p(a)\ne 1\text{ for all }p\in P\}$ (observe that the Dirichlet series $\sum_{a\in D_2}|a|^{-s}$ converges for $\Re s\ge 1$). We thus conclude that the second factor of S''_χ belongs to Λ.

Putting all together, we have proved that

$$S'_\chi=R'_\chi\Big(\log\frac{1}{s-1}\Big)\,,$$

where $R'_\chi \in \Lambda[X], \deg R'_\chi \le d$, and the coefficient of X^d in R'_χ is given by

$$A'_\chi(s) = \sum_{\substack{\mathbf{d}\in\mathbb{N}_0^l\\ |\mathbf{d}|=d}} \prod_{j=1}^{l} [\chi(g_j)\varrho_j]^{d_j} \sum_{t\in\mathfrak{T}(\mathbf{d})} \kappa(t) \sum_{(\mathbf{q},t)} \Bigg(\prod_{j=1}^{l} \prod_{\nu=d_j+1}^{\lambda_j(t)} \frac{\chi(g_j)^{t_{j,\nu}}}{|q_{j,\nu}|^{t_{j,\nu}s}} \Bigg)$$
$$\times \sum_{(\mathbf{q},t)^*} \Bigg(\prod_{j=l+1}^{m} \prod_{\nu=1}^{\lambda_j(t)} \frac{\chi(g_j)^{t_{j,\nu}}}{|q_{j,\nu}|^{t_{j,\nu}s}} \Bigg).$$

For $t = ((t_{j,\nu})_{\nu\le\lambda_j(t)})_{j=1,\ldots,m} \in \mathcal{T}^*(\mathcal{P})$, we set

$$\iota(t) = \sum_{j=1}^{m} \sum_{\nu=1}^{\lambda_j(t)} t_{j,\nu} g_j \in G\,;$$

if $a \in \mathcal{F}(P \setminus P_0)$ and $\boldsymbol{\tau}^{\mathcal{P}}(a) = t$, then $[a] = \iota(t)$. Now we consider the decomposition

$$A'_\chi(s) = \sum_{\gamma\in G/G_0} A'_{\chi,\gamma}(s)\,,$$

where

$$A'_{\chi,\gamma}(s) = \sum_{\substack{\mathbf{d}\in\mathbb{N}_0^l\\ |\mathbf{d}|=d}} \prod_{j=1}^{l} [\chi(g_j)\varrho_j]^{d_j} \sum_{\substack{t\in\mathfrak{T}(\mathbf{d})\\ \iota(t)+G_0=\gamma}} \kappa(t) \sum_{(\mathbf{q},t)} (\ldots) \sum_{(\mathbf{q},t)^*} (\ldots)\,.$$

If $A'_{\chi,\gamma} \ne 0$, then there exist some $\mathbf{d} \in \mathbb{N}_0^l$ with $|\mathbf{d}| = d$, $t \in \mathfrak{T}(\mathbf{d})$ such that $\iota(t) + G_0 = \gamma$ and $a_1 \in \mathcal{F}(P \setminus P_0)$ such that $\boldsymbol{\tau}^{\mathcal{P}}(a_1) = t$; this implies $\delta^{\mathcal{P}}(a_1) = d$ and $[a_1] + G_0 = \gamma$.

Now let $\gamma = g + G_0 \in G/G_0$ and $a_1 \in g$ be such that $\boldsymbol{\tau}^{\mathcal{P}}(a_1) = t \in \mathfrak{T}$ and $\delta^{\mathcal{P}}(a_1) = d$. We set $a_1 = a_0 a'_1$, where $a_0 \in \mathcal{F}(P_0)$ and $a'_1 \in \mathcal{F}(P \setminus P_0)$; then $\boldsymbol{\tau}^{\mathcal{P}}(a'_1) = t$ and $[a'_1] + G_0 = [a_1] + G_0 = \gamma$. If $\mathbf{d} = \boldsymbol{\delta}(t)$, then $|\mathbf{d}| = d$, $t \in \mathfrak{T}(\mathbf{d})$, $\iota(t) + G_0 = \gamma$ and $\bar{\chi}(a'_1) A_{\chi,\gamma}(1) = A_{\chi_0,\gamma}(1) > 0$ for all $\chi \in G^*$. If moreover $\chi \in G^*(P_0)$, then $\bar{\chi}(a'_1) = \bar{\chi}(a_1)$, and the assertion follows. ∎

3. Type-dependent factorization properties. The nature of type-dependent factorization properties is described by the following (rather formal) Theorem 2. The subsequent arithmetical applications are partitioned into three groups dealt with in subsections 3.1–3.3. These latter results should be regarded as examples. It is of course possible to derive dozens of similar statements.

Theorem 2. *Let* $([D, H, |\cdot|], [\overline{D}, \overline{H}], \varphi)$ *be a Chebotarev formation*, $D = \mathcal{F}(P)$, $\mathfrak{M} = \{P_1, \ldots, P_m, P_{m+1}, \ldots, P_{m+l}\}$ *the set of* φ*-equivalence classes* *(for some $m \in \mathbb{N}$ and $l \in \mathbb{N}_0$), $P_0 = P_{m+1} \cup \ldots \cup P_{m+l}$, $\varrho_0 = \varrho(P_0)$ and $\mathcal{P} = (P_0, P_1, \ldots, P_m)$. Let $\emptyset \neq Z \subset D$ have the following two properties*:

(1) *If $a, b \in D$, $a \in Z$ and $\boldsymbol{\tau}^{\mathcal{P}}(a) = \boldsymbol{\tau}^{\mathcal{P}}(b)$, then $b \in Z$.*

(2) $d = \sup\{\delta^{\mathcal{P}}(a) \mid a \in Z\} < \infty$.

Let $y \in G = D/H$ and let $a_1 \in Z \cap y$ be such that $\delta^{\mathcal{P}}(a_1) = d$. If $d + \varrho_0 > 0$, then we have, as $x \to \infty$,

$$\#\{a \in Z \cap y \mid |a| \le x\} \asymp x(\log x)^{-1+\varrho_0}(\log\log x)^{d'}$$

where

$$d' = \begin{cases} d & \text{if } \varrho_0 > 0, \\ d-1 & \text{if } \varrho_0 = 0. \end{cases}$$

Proof. Apply Theorem 1 with $\mathfrak{T} = \{\boldsymbol{\tau}^{\mathcal{P}}(a) \mid a \in Z\} \subset \mathcal{T}^*(\mathcal{P})$. ∎

3.1. *Elements with a given number of distinct factorizations*

Proposition 6. *Let $([D, H, |\cdot|], [\overline{D}, \overline{H}], \varphi)$ be a Chebotarev formation, $D = \mathcal{F}(P)$, $\overline{D} = \mathcal{F}(\overline{P}) \neq \overline{H}$, and suppose that there is a finite subset $P^* \subset P$ such that $p \in P \setminus P^*$ implies $\varphi(p) = \overline{p}_1 \ldots \overline{p}_s$ with $s \ge 1$ distinct primes $\overline{p}_j \in \overline{P}$ and $p, q \in P \setminus P^*, p \neq q$ implies $\gcd(\varphi(p), \varphi(q)) = 1$. Let $\overline{e} \in \overline{D}$ be such that $\gcd(\varphi(a), \overline{e}) = 1$ for all $a \in D$. Let $y \in G = D/H$, $k \in \mathbb{N}$, and suppose that there exists $a_1 \in y$ satisfying $\varphi(a_1)\overline{e} \in \overline{H}$ and $\mathbf{f}_{\overline{H}}(\varphi(a_1)\overline{e}) \le k$. Let P_0 be the set of all $p \in P$ satisfying $v_{\overline{p}}(\varphi(p)) = 0$ for all $\overline{p} \in \overline{P} \setminus \overline{H}$ and assume that $\varrho_0 = \varrho(P_0) > 0$. Then we have, as $x \to \infty$,*

$$\#\{a \in y \mid |a| \le x,\ \mathbf{f}_{\overline{H}}(\varphi(a)\overline{e}) \le k\} \asymp x(\log x)^{-1+\varrho_0}(\log\log x)^{d};$$

the exponent d is given by

$$d = \max\{\delta(a) \mid a \in y,\ \mathbf{f}_{\overline{H}}(\varphi(a)\overline{e}) \le k\},$$

where $\delta(a)$ is the number of $p \in P \setminus P_0$ lying in a φ-equivalence class of positive density and satisfying $v_p(a) = 1$.

Proof. We set $\overline{G} = \overline{D}/\overline{H} = \{\overline{H}, \overline{g}_2, \ldots, \overline{g}_N\}$, where $N = \#\overline{G} \ge 2$ and consider the partition $\overline{\mathcal{P}} = (\overline{P} \cap \overline{H}, \overline{P} \cap \overline{g}_2, \ldots, \overline{P} \cap \overline{g}_N)$. If $\overline{a}, \overline{b} \in \overline{H}$, then $\boldsymbol{\tau}^{\overline{\mathcal{P}}}(\overline{a}) = \boldsymbol{\tau}^{\overline{\mathcal{P}}}(\overline{b})$ implies $\mathbf{f}_{\overline{H}}(\overline{a}) = \mathbf{f}_{\overline{H}}(\overline{b})$ by [14; Satz 6], and $a_k(\overline{G}) = \sup\{\delta(\boldsymbol{\tau}^{\overline{\mathcal{P}}}(\overline{a})) \mid \overline{a} \in \overline{H},\ \mathbf{f}_{\overline{H}}(\overline{a}) \le k\} < \infty$ by [14; Satz 9].

Let $\mathfrak{M} = \{P_1, \ldots, P_m, P_{m+1}, \ldots, P_{m+l}\}$ be the set of all φ-equivalence classes ($m \in \mathbb{N}$, $l \in \mathbb{N}_0$), and suppose that $P_0 = P_{m+1} \cup \ldots \cup P_{m+l}$ consists of all $p \in P$ satisfying $v_{\overline{p}}(\varphi(p)) = 0$ for all $\overline{p} \in \overline{P} \setminus \overline{H}$ (i.e., $\varphi(p) \in \overline{D}$ is a product of principal primes). If $\mathcal{P} = (P_0, P_1, \ldots, P_m)$, then $\boldsymbol{\tau}^{\mathcal{P}}(a) = \boldsymbol{\tau}^{\mathcal{P}}(b)$ implies $\boldsymbol{\tau}^{\overline{\mathcal{P}}}(\varphi(a)\overline{e}) = \boldsymbol{\tau}^{\overline{\mathcal{P}}}(\varphi(b)\overline{e})$ and hence $\mathbf{f}_{\overline{H}}(\varphi(a)\overline{e}) = \mathbf{f}_{\overline{H}}(\varphi(b)\overline{e})$ for all $a, b \in \varphi^{-1}(\overline{H}) \subset D$. We apply Theorem 2, setting

$$Z = \{a \in \varphi^{-1}(\overline{H}) \mid \mathbf{f}_{\overline{H}}(\varphi(a)\overline{e}) \le k\}.$$

We have just proved that Z has property (1) of Theorem 2. For the proof of property (2), set $M = \#P^*$; then, for any $a \in Z$, we obtain

$$\delta(\boldsymbol{\tau}^{\mathcal{P}}(a)) \le \delta(\boldsymbol{\tau}^{\overline{\mathcal{P}}}(\varphi(a))) + M \le \delta(\boldsymbol{\tau}^{\overline{\mathcal{P}}}(\varphi(a)\bar{e})) + M \le a_k(\overline{G}) + M\,,$$

and the assertion follows. ∎

Proposition 6A. *Let R be a holomorphy ring in a global field, G its ideal class group, $N = \#G \ge 2$ and $k \in \mathbb{N}$. Let $\mathfrak{f}$ be a cycle of R and $\alpha_0 \in R$ such that* $\gcd(\alpha_0, \mathfrak{f}) = 1$. *Then we have, as $x \to \infty$,*

$$\#\{(\alpha) \in \mathcal{H}_R \mid \alpha \in R,\ |(\alpha)| \le x,\ \alpha \equiv \alpha_0 \bmod \mathfrak{f},\ \mathbf{f}_{\mathcal{H}_R}((\alpha)) \le k\} \asymp x(\log x)^{-1+1/N}(\log\log x)^{a_k(G)}\,,$$

where $a_k(G) \in \mathbb{N}$ is the constant introduced by W. Narkiewicz in [29]; *it depends only on k and G.*

Proof. We apply Proposition 6 with the Chebotarev formation $([\mathcal{I}_R^{(\mathfrak{f})}, \mathcal{S}_R^{(\mathfrak{f})}, |\cdot|], [\mathcal{I}_R, \mathcal{H}_R], \varphi)$, where $\varphi = (\mathcal{I}_R^{(\mathfrak{f})} \hookrightarrow \mathcal{I}_R)$, $y = \{(\alpha) \in \mathcal{H}_R^{(\mathfrak{f})} \mid \alpha \in R,\ \alpha \equiv \alpha_0 \bmod \mathfrak{f}\} \in \mathcal{I}_R^{(\mathfrak{f})}/\mathcal{S}_R^{(\mathfrak{f})}$ and $\bar{e} = 1$. Then we have $P_0 = \mathcal{P}_R^{(\mathfrak{f})} \cap \mathcal{H}_R$ and $\varrho_0 = 1/N$; Proposition 6 implies

$$\#\{\ldots\} \asymp x(\log x)^{-1+1/N}(\log\log x)^d,$$

where $d = \max\{\delta(a) \mid a \in y,\ \mathbf{f}_{\mathcal{H}_R}(a) \le k\}$, and $\delta(a)$ is the number of prime ideals $\mathfrak{p} \in \mathcal{P}_R^{(\mathfrak{f})} \setminus \mathcal{H}_R$ satisfying $v_{\mathfrak{p}}(a) = 1$. It was proved in [14; Satz 9] that $a_k(G) = \max\{\delta(a) \mid a \in \mathcal{H}_R,\ \mathbf{f}_{\mathcal{H}_R}(a) \le k\}$. Now let $a^* = (\alpha^*) \in \mathcal{H}_R$ satisfy $\mathbf{f}_{\mathcal{H}_R}(a^*) \le k$ and $\delta(a^*) = a_k(G)$. If $a^* = \mathfrak{p}_1^{m_1} \ldots \mathfrak{p}_r^{m_r}\mathfrak{a}_0^*$ where $\mathfrak{p}_1, \ldots, \mathfrak{p}_r \in \mathcal{P}_R$ are distinct prime ideals dividing $\mathfrak{f}$ and $\mathfrak{a}_0^* \in \mathcal{I}_R^{(\mathfrak{f})}$, choose distinct prime ideals $\bar{\mathfrak{p}}_1, \ldots, \bar{\mathfrak{p}}_r \in \mathcal{P}_R^{(\mathfrak{f})}$ such that $[\mathfrak{p}_i] = [\bar{\mathfrak{p}}_i] \in \mathcal{I}_R/\mathcal{H}_R$, consider the principal ideal $\bar{\mathfrak{p}}_1^{m_1} \ldots \bar{\mathfrak{p}}_r^{m_r}\mathfrak{a}_0^* = (\alpha) \in \mathcal{H}_R^{(\mathfrak{f})}$, and let $(\pi) \in \mathcal{P}_R^{(\mathfrak{f})} \cap \mathcal{H}_R$ be a principal prime ideal satisfying $\alpha\pi \equiv \alpha_0 \bmod \mathfrak{f}$. Then the ideal $a = (\alpha\pi)$ has the desired properties: $a \in y$, $\mathbf{f}_{\mathcal{H}_R}(a) \le k$ and $\delta(a) = a_k(G)$. ∎

Remark. If R is the ring of integers of an algebraic number field and $\mathfrak{f} = 1$, the assertion of Proposition 6A was proved in [28]; for more general cases with $\mathfrak{f} = 1$ see [17].

Proposition 6B. *Let $\overline{K}/K$ be a finite extension of algebraic number fields, $R, \overline{R}$ their rings of integers, $\mathfrak{f}$ a cycle of R and $\alpha_0 \in R$ such that $\mathbf{f}_{\mathcal{H}_{\overline{R}}}(\alpha_0\overline{R}) \le k$ for some $k \in \mathbb{N}$. If $\overline{R}$ is not a principal ideal domain, then we have, as $x \to \infty$,*

$$\#\{(\alpha) \in \mathcal{H}_R \mid \alpha \in R,\ |(\alpha)| \le x,\ \alpha \equiv \alpha_0 \bmod \mathfrak{f},\ \mathbf{f}_{\mathcal{H}_{\overline{R}}}(\alpha\overline{R}) \le k\} \asymp x(\log x)^{-\varrho}(\log\log x)^d$$

for some $0 < \varrho < 1$ and $d \in \mathbb{N}_0$.

Proof. Suppose that $\mathfrak{f} = \mathfrak{f}_0 w_1 \ldots w_r$, where $\mathfrak{f}_0 \in \mathcal{I}_R$ and $w_1, \ldots, w_r : K \to \mathbb{R}$ are distinct real imbeddings. We set $\mathfrak{a}_0 = \gcd(\alpha_0 R, \mathfrak{f}_0) \in \mathcal{I}_R$ and $\mathfrak{f}' = \mathfrak{a}_0^{-1}\mathfrak{f}$; $\mathfrak{f}'$ is a cycle of R, and $\gcd(\mathfrak{a}_0^{-1}\alpha_0 R, \mathfrak{f}') = 1$. Let $y \in \mathcal{I}_R^{(\mathfrak{f}')}/\mathcal{S}_R^{(\mathfrak{f}')}$ be the ray class modulo $\mathfrak{f}'$ containing the ideal $\mathfrak{a}_0^{-1}\alpha_0 R$. If $a \in \mathcal{H}_R$, then we have $a = (\alpha)$ for some $\alpha \in R$ satisfying $\alpha \equiv \alpha_0 \bmod \mathfrak{f}$ if and only if $a = \mathfrak{a}_0\mathfrak{c}$ for some $\mathfrak{c} \in y$. This implies

$$\begin{aligned}\#\{(\alpha) \in \mathcal{H}_R \mid \alpha \in R, |(\alpha)| \le x,\ \alpha \equiv \alpha_0 \bmod \mathfrak{f},\ \mathbf{f}_{\mathcal{H}_{\overline{R}}}(\alpha\overline{R}) \le k\}& \\ = \#\{\mathfrak{c} \in y \mid |\mathfrak{c}| \le x/|\mathfrak{a}_0|,\ \mathbf{f}_{\mathcal{H}_{\overline{R}}}(\mathfrak{a}_0\mathfrak{c}\overline{R}) \le k\}&\,,\end{aligned}$$

and therefore it is sufficient to prove that

$$\#\{\mathfrak{c} \in y \mid\ |\mathfrak{c}| \le x,\ \mathbf{f}_{\mathcal{H}_{\overline{R}}}(\mathfrak{a}_0\mathfrak{c}\overline{R}) \le k\} \asymp x(\log x)^{-\varrho}(\log\log x)^d$$

for some $0 < \varrho < 1$ and $d \in \mathbb{N}_0$. We apply Proposition 6 with the Chebotarev formation $([\mathcal{I}_R^{(\mathfrak{f}')}, \mathcal{S}_R^{(\mathfrak{f}')}, |\cdot|], [\mathcal{I}_{\overline{R}}, \mathcal{H}_{\overline{R}}], \varphi)$, $\bar{e} = \mathfrak{a}_0\overline{R}$ and $a_1 = \mathfrak{a}_0^{-1}\alpha_0 R$. The set P_0 consists of all $\mathfrak{p} \in \mathcal{P}_R^{(\mathfrak{f}')}$ for which $\mathfrak{p}\overline{R}$ is a product of principal prime ideals. In particular, P_0 contains all $\mathfrak{p}$ splitting completely in the Hilbert class field of $\overline{K}$, and therefore $\varrho(P_0) > 0$. If $\bar{g}$ is a non-principal ideal class of $\overline{R}$, then the set of prime ideals $\mathfrak{p} \in \mathcal{P}_R$ having a prime factor in $\bar{g}$ has positive density, and therefore $\varrho(P_0) < 1$. On putting $\varrho = 1 - \varrho(P_0)$, the assertion follows. ■

Remarks. The special case $K = \overline{K}$ and $\gcd(\alpha_0, \mathfrak{f}) = 1$ of Proposition 6B is contained in Proposition 6A; the case $K = \mathbb{Q}$ and $\mathfrak{f} = 1$ was settled in [37]. In general, it seems to be very complicated to determine ϱ and d. If $K = \mathbb{Q}$, $\overline{K}/\mathbb{Q}$ is cyclic of prime degree $l, \mathfrak{f} = 1$ and h is the class number of $\overline{K}$, we have $\varrho = 1/l - 1/(lh)$ [32; Theorem 9.7]. If $K = \mathbb{Q}$ and $\overline{K}$ is a quadratic number field, there are precise results due to W. Narkiewicz [24], [25], [26].

The following Proposition 6C is a variant of Proposition 6B in the case $K = \mathbb{Q}$ which avoids the hypothesis $\mathbf{f}_{\mathcal{H}_{\overline{R}}}(\alpha_0\overline{R}) \le k$.

Proposition 6C. *Let L be an algebraic number field whose ring of integers R is not a principal ideal domain. Let $f \ge 2$ and $a_0 \ge 1$ be coprime integers, and suppose that either f is relatively prime to the discriminant of L, or $L/\mathbb{Q}$ is cyclic of prime degree. Then we have, as $x \to \infty$,*

$$\#\{a \in \mathbb{N} \mid a \le x,\ a \equiv a_0 \bmod f,\ \mathbf{f}_{\mathcal{H}_R}(aR) \le k\} \asymp x(\log x)^{-\varrho}(\log\log x)^d$$

for some $0 < \varrho < 1$ and $d \in \mathbb{N}_0$.

Proof. We apply Proposition 6B with $K = \mathbb{Q}$, $\overline{K} = L$ and $\mathfrak{f} = f\infty$; it is sufficient to prove that there exists an integer $a_1 \ge 2$ such that $a_1 \equiv a_0 \bmod f$, and $a_1 R$ is a product of principal prime ideals of R.

Suppose first that f is relatively prime to the discriminant of L, let $\bar{L}$ be the Hilbert class field of L and ζ a primitive fth root of unity. Since $\mathbb{Q}(\zeta)\cap\bar{L}=\mathbb{Q}$, it follows from Chebotarev's theorem that every residue class $g\in(\mathbb{Z}/f\mathbb{Z})^{\times}$ contains a prime p splitting completely in $\bar{L}$, whence pR is a product of principal prime ideals of R.

Now suppose that $L/\mathbb{Q}$ is cyclic of prime degree, and let m be the conductor of L. Assume first that $m\,|\,f$; then L is defined by a character $\chi:(\mathbb{Z}/f\mathbb{Z})^{\times}\to\mathbb{C}^{\times}$. Let $\bar{L}$ be the Hilbert class field of L and L^* its absolute genus field [23], i.e., L^* is the maximal absolutely abelian subfield of $\bar{L}$. If $\chi=\chi_1\ldots\chi_r$ is the decomposition of χ into characters χ_i of prime power conductor, then L^* is defined by $\chi_1,\ldots,\chi_r$, and therefore a class $g\in(\mathbb{Z}/f\mathbb{Z})^{\times}$ contains a prime p splitting completely in $\bar{L}$ if and only if $\chi_i(g)=1$ for all $i\in\{1,\ldots,r\}$.

Let $g_1,\ldots,g_r\in(\mathbb{Z}/f\mathbb{Z})^{\times}$ be classes satisfying

$$\chi_\nu(g_i)=\begin{cases}\chi_i(a_0+f\mathbb{Z}) & \text{if } \nu=i,\\ 1 & \text{if } \nu\neq i,\end{cases}$$

for all $i,\nu\in\{1,\ldots,r\}$, and let $g_0\in(\mathbb{Z}/f\mathbb{Z})^{\times}$ be such that $a_0+f\mathbb{Z}=g_0g_1\ldots g_r$. Then, for any $i\in\{0,1,\ldots,r\}$, either $\chi(g_i)\neq 1$ or $\chi_\nu(g_i)=1$ for all $\nu\in\{1,\ldots,r\}$. If $\chi(g_i)\neq 1$, take any prime $p_i\in g_i$; it is inert in L, whence $p_iR\in\mathcal{P}_R$. If $\chi_\nu(g_i)=1$ for all $\nu\in\{1,\ldots,r\}$, then there exists a prime $p_i\in g_i$ splitting completely in $\bar{L}$, and then, by class field theory, p_iR is a product of principal prime ideals of R. Setting $a_1=p_0p_1\ldots p_r$, we obtain $a_1\equiv a_0 \bmod f$, and a_1R is a product of principal prime ideals of R.

If $m\nmid f$, we set $\bar{f}=\operatorname{lcm}(f,m)$ and determine integers $a_0^{(1)},\ldots,a_0^{(r)}\geq 2$ such that

$$a_0+f\mathbb{Z}=\biguplus_{i=1}^{r}(a_0^{(i)}+\bar{f}\mathbb{Z})\,,$$

and $\gcd(a_0^{(i)},\bar{f})=1$. Then the result follows by applying the above arguments for $\bar{f}$ and $a_0^{(i)}$ instead of f and a_0. ∎

Remark. Proposition 6 and its followers have their counterparts for sets defined by the property $\mathbf{f}(\ldots)=k$ instead of $\mathbf{f}(\ldots)\leq k$; for classical cases see [14].

3.2. *Elements with a given factorization scheme.* We recall the concept of a factorization scheme from [14]: Let H be an atomic semigroup and $E=(e_{ij})_{i=1,\ldots,r,j=1,\ldots,m}$ a matrix of non-negative integers. We say that $a\in H$ *allows the factorization scheme* E if there exist irreducible elements $u_1,\ldots,u_r\in H$ such that $a\simeq u_1^{e_{1j}}\ldots u_r^{e_{rj}}$ for all $j\in\{1,\ldots,m\}$.

Proposition 7. *Let* $([D,H,|\cdot|],[\overline{D},\overline{H}],\varphi)$ *be a Chebotarev formation*, $D=\mathcal{F}(P)$, *and suppose that the set* $P^*=\{p\in P\mid \varphi(p)=1\}$ *is finite. Let* $\bar{e}\in\overline{D}$ *satisfy* $\gcd(\varphi(a),\bar{e})=1$ *for all* $a\in D$. *Let* E *be a matrix of non-negative integers*, *and let* $y\in G=D/H$ *and* $a_1\in y$ *have the following properties*: $\varphi(a_1)\bar{e}\in\overline{H}$, $\varphi(a_1)\bar{e}$ *allows the factorization scheme* E, *and there exists* $p\in P$ *lying in a* φ*-equivalence class of positive density and satisfying* $v_p(a_1)=1$. *Then we have*, *as* $x\to\infty$,

$$\#\{a\in y\mid |a|\le x,\varphi(a)\bar{e}\text{ allows }E\}\asymp x(\log x)^{-1}(\log\log x)^d$$

for some $d\in\mathbb{N}_0$.

Proof. We set $\overline{G}=\overline{D}/\overline{H}=\{\overline{H}=\bar{g}_1,\bar{g}_2,\ldots,\bar{g}_N\}$, where $N=\#G$ and consider the partition $\overline{\mathcal{P}}=(\emptyset,\overline{P}\cap\bar{g}_1,\ldots,\overline{P}\cap\bar{g}_N\}$. If $\bar{a},\bar{b}\in\overline{H}$ and $\boldsymbol{\tau}^{\overline{\mathcal{P}}}(\bar{a})=\boldsymbol{\tau}^{\overline{\mathcal{P}}}(\bar{b})$, then $\bar{a}$ and $\bar{b}$ allow the same factorization schemes by [14; Satz 5]. Let $\mathfrak{M}=\{P_1,\ldots,P_m\}$ be the set of all φ-equivalence classes and $\mathcal{P}=(\emptyset,P_1,\ldots,P_m)$. If $a,b\in D$ and $\boldsymbol{\tau}^{\mathcal{P}}(a)=\boldsymbol{\tau}^{\mathcal{P}}(b)$, then $\boldsymbol{\tau}^{\overline{\mathcal{P}}}(\varphi(a)\bar{e})=\boldsymbol{\tau}^{\overline{\mathcal{P}}}(\varphi(b)\bar{e})$, and therefore $\varphi(a)\bar{e}$ and $\varphi(b)\bar{e}$ allow the same factorization schemes if they lie in $\overline{H}$.

There is an integer $r=r(E)$ such that every $\bar{a}\in\overline{H}$ allowing the factorization scheme E is a product of at most r irreducible elements of $\overline{H}$, and therefore

$$\delta(\boldsymbol{\tau}^{\overline{\mathcal{P}}}(\bar{a}))\le rD(\overline{G})<\infty$$

by [14; Satz 7] (where $D(\overline{G})$ is Davenport's constant). If $a\in D,\varphi(a)\bar{e}\in\overline{H}$ and $\varphi(a)\bar{e}$ allows the factorization scheme E, then $\delta(\boldsymbol{\tau}^{\mathcal{P}}(a))\le\delta(\boldsymbol{\tau}^{\overline{\mathcal{P}}}(\varphi(a)\bar{e}))+\#P^*\le rD(\overline{G})+\#P^*<\infty$. By assumption, $\delta(\boldsymbol{\tau}^{\mathcal{P}}(a_1))\ge1$, and therefore the assertion follows from Theorem 2. ■

Proposition 7A. *Let* K *be an algebraic number field*, R *its ring of integers and* E *a matrix of non-negative integers. Let* $f\ge2$ *and* a_0 *be integers*, *and suppose that there exists an integer* $a_1\ge2$ *with the following properties*: a_1R *allows the factorization scheme* E *in* $\mathcal{H}_R$, $a_1\equiv a_0\bmod f$, *and there exists a prime* p *such that* $p\mid a_1$, $p^2\nmid a_1$, $p\nmid f$, *and* p *is unramified in* K. *Then we have*, *as* $x\to\infty$,

$$\#\{a\in\mathbb{N}\mid a\le x,\ a\equiv a_0\bmod f,\ aR\text{ allows }E\}\asymp x(\log x)^{-1}(\log\log x)^d$$

for some $d\in\mathbb{N}_0$.

Proof. We set $c=\gcd(a_0,f)$, $f'=c^{-1}f$, $a_0'=c^{-1}a_0$, and we must prove that

$$\#\{a\in\mathbb{N}\mid a\le x,\ a\equiv a_0'\bmod f',\ acR\text{ allows }E\}\asymp x(\log x)^{-1}(\log\log x)^d$$

for some $d\in\mathbb{N}_0$.

We observe that $[\mathbb{N}^{(f')}, H_{f',\{1+f'\mathbb{Z}\}}, |\cdot|] = [\mathcal{I}_{\mathbb{Z}}^{(f'\infty)}, \mathcal{S}_{\mathbb{Z}}^{(f'\infty)}, |\cdot|]$, and we consider the Chebotarev formation $([\mathbb{N}^{(f')}, H_{f',\{1+f'\mathbb{Z}\}}, |\cdot|], [\mathcal{I}_R, \mathcal{H}_R], \varphi)$, where $\varphi(a) = aR$. We apply Proposition 7 with $\bar{e} = cR$. Since unramified primes fall into φ-equivalence classes of positive density, the result follows. ∎

3.3. *Elements with prime factors in a given class.* In this subsection we content ourselves with one characteristic example.

PROPOSITION 8. *Let R be a holomorphy ring in a global field, G its ideal class group and $N = \#G$. For $\mathfrak{a} \in \mathcal{I}_R$ and $y \in G$, we set*

$$\omega_y(\mathfrak{a}) = \#\{\mathfrak{p} \in \mathcal{P}_R \cap y \mid v_{\mathfrak{p}}(\mathfrak{a}) > 0\}.$$

Let $y \in G$, $\mathfrak{f}$ a cycle of R, $c \in \mathcal{I}_R^{(\mathfrak{f})}/\mathcal{S}_R^{(\mathfrak{f})}$, $\widehat{c} \in G$ the absolute class containing c and $k \in \mathbb{N}$. Then we have, as $x \to \infty$,

$$\#\{\mathfrak{a} \in c \mid |\mathfrak{a}| \le x,\ \omega_y(\mathfrak{a}) = k\} \asymp x(\log x)^{-1/N}(\log\log x)^{k'},$$

where

$$k' = \begin{cases} k-1 & \textit{if either } N = 1 \textit{ or } N = 2,\ y \ne 0,\ ky \ne \widehat{c}, \\ k & \textit{otherwise.} \end{cases}$$

Proof. We consider the Chebotarev formation $([\mathcal{I}_R^{(\mathfrak{f})}, \mathcal{S}_R^{(\mathfrak{f})}, |\cdot|], [\mathcal{I}_R, \mathcal{H}_R], \varphi)$, where φ is the inclusion map. Then $\mathfrak{M} = \{\mathcal{P}_R \cap b \mid b \in \mathcal{I}_R^{(\mathfrak{f})}/\mathcal{S}_R^{(\mathfrak{f})}\}$ is the set of φ-equivalence classes, and we set $\mathfrak{M} = \{P_1, \ldots, P_m, P_{m+1}, \ldots, P_{m+l}\}$, where $P_0 = P_{m+1} \cup \ldots \cup P_{m+l} = \mathcal{P}_R^{(\mathfrak{f})} \setminus y$, and $\mathcal{P} = (P_0, P_1, \ldots, P_m)$. Then $\varrho(P_0) = 1 - 1/N$, and if $\mathfrak{a}, \mathfrak{b} \in \mathcal{I}_R^{(\mathfrak{f})}$ satisfy $\boldsymbol{\tau}^{\mathcal{P}}(\mathfrak{a}) = \boldsymbol{\tau}^{\mathcal{P}}(\mathfrak{b})$, then $\omega_y(\mathfrak{a}) = \omega_y(\mathfrak{b})$. We set

$$Z = \{\mathfrak{a} \in \mathcal{I}_R^{(\mathfrak{f})} \mid \omega_y(\mathfrak{a}) = k\},$$

and we are going to apply Theorem 2; for $\mathfrak{a} \in \mathcal{I}_R^{(\mathfrak{f})}$, we have $\mathfrak{a} \in Z$ if and only if $\mathfrak{a} = \mathfrak{p}_1^{m_1} \ldots \mathfrak{p}_k^{m_k}\mathfrak{a}_0$, where $\mathfrak{p}_1, \ldots, \mathfrak{p}_k \in \mathcal{P}_R \cap y$ are distinct, $m_i \in \mathbb{N}$ and $\mathfrak{a}_0 \in \mathcal{I}_R^{(\mathfrak{f})}$, $\omega_y(\mathfrak{a}_0) = 0$; obviously, $\delta(\boldsymbol{\tau}^{\mathcal{P}}(\mathfrak{a})) = \#\{1 \le i \le k \mid m_i = 1\} \le k$, and $[\mathfrak{a}] = (m_1 + \ldots + m_k)y + [\mathfrak{a}_0] \in G$. We must prove that there exists an ideal $\mathfrak{a}_1 \in Z \cap c$ such that $\delta(\boldsymbol{\tau}^{\mathcal{P}}(\mathfrak{a}_1)) = k$ except in the special case $N = 2$, $y \ne 0$, $ky \ne \widehat{c}$; in this special case we must prove that there exists an ideal $\mathfrak{a}_2 \in Z \cap c$ such that $\delta(\boldsymbol{\tau}^{\mathcal{P}}(\mathfrak{a}_2)) = k - 1$, but no ideal $\mathfrak{a}_1 \in Z \cap c$ such that $\delta(\boldsymbol{\tau}^{\mathcal{P}}(\mathfrak{a}_1)) = k$.

Case 1: $\widehat{c} = ky$. Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_{k-1} \in y$ be arbitrary distinct prime ideals, and choose a further prime ideal $\mathfrak{p}_k \in y$ such that $\mathfrak{a}_1 = \mathfrak{p}_1 \ldots \mathfrak{p}_k \in c$.

Case 2: $\widehat{c} \ne ky$, $\widehat{c} \ne (k+1)y$. Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_k \in y$ be arbitrary distinct prime ideals, and choose a prime ideal $\mathfrak{p}_{k+1} \in \mathcal{P}_R^{(\mathfrak{f})}$ such that $\mathfrak{a}_1 = \mathfrak{p}_1 \ldots \mathfrak{p}_k\mathfrak{p}_{k+1} \in c$; since $\widehat{c} - ky \ne y$, we infer $\mathfrak{p}_{k+1} \notin y$.

Case 3: $\widehat{c} \neq ky$, $\widehat{c} = (k+1)y$, $N \geq 3$. Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_k \in y$ be arbitrary distinct prime ideals. Since $N \geq 3$, there exist $y', y'' \in G \setminus \{y\}$ such that $y = y' + y''$; we choose distinct prime ideals $\mathfrak{p}' \in y' \cap \mathcal{P}_R^{(\mathrm{f})}$ and $\mathfrak{p}'' \in y'' \cap \mathcal{P}_R^{(\mathrm{f})}$ such that $\mathfrak{a}_1 = \mathfrak{p}_1 \ldots \mathfrak{p}_k \mathfrak{p}' \mathfrak{p}'' \in c$.

Case 4: $\widehat{c} \neq ky$, $\widehat{c} = (k+1)y$, $N = 2$. This is exactly the exceptional case $N = 2$, $y \neq 0$, $ky \neq \widehat{c}$. Suppose that $\mathfrak{a}_1 = \mathfrak{p}_1 \ldots \mathfrak{p}_k \mathfrak{a}_0 \in Z \cap c$, where $\mathfrak{p}_1, \ldots, \mathfrak{p}_k \in \mathcal{P}_R \cap y$ are distinct and $\omega_y(\mathfrak{a}_0) = 0$; then $\mathfrak{a}_0 \in \mathcal{H}_R$, and therefore $\widehat{c} = [\mathfrak{a}_1] = ky$, a contradiction. If $\mathfrak{p}_1, \ldots, \mathfrak{p}_k \in \mathcal{P}_R \cap y$ are distinct, there exists a principal prime ideal $\mathfrak{p}_0 \in \mathcal{P}_R^{(\mathrm{f})} \cap \mathcal{H}_R$ such that $\mathfrak{a}_2 = \mathfrak{p}_1 \ldots \mathfrak{p}_{k-1} \mathfrak{p}_k^2 \mathfrak{a}_0 \in c$. ■

4. Valuation-dependent factorization properties. The methods developed so far are not suitable for the study of the functions G_k and related functions. We are now going to describe a formalism which is able to produce very general quantitative results concerning lengths. We start with a description of the combinatorial setting (Definition 5 and Proposition 9) and a very general analytical result. After that we recall the formalism of block semigroups and give several arithmetical applications.

The combinatorial formalism has its prototype in [9].

Definition 5. Let $[D, H]$ be a formation, $D = \mathcal{F}(P)$ and $G = D/H$.

(a) By a *decomposition* of P we mean a finite set $\mathcal{R} = \{P_1, \ldots, P_m\}$ of mutually disjoint subsets $P_j \subset P$ such that $P = P_1 \cup \ldots \cup P_m$. For $j \in \{1, \ldots, m\}$, we define

$$v_j = v_{P_j} : D \to \mathbb{N}_0 \quad \text{by} \quad v_j(a) = \sum_{p \in P_j} v_p(a)\,.$$

For a subset $I \subset \{1, \ldots, m\}$, we set $I^{\mathrm{c}} = \{1, \ldots, m\} \setminus I$; for a function $\sigma : I^{\mathrm{c}} \to \mathbb{N}_0$ and $l \in \mathbb{N}_0$, we set

$$\Omega^{\mathcal{R}}(I, \sigma)(l) = \left\{ a \in D \;\middle|\; \begin{matrix} v_j(a) = \sigma(j) & \text{for } j \in I^{\mathrm{c}} \\ v_j(a) \geq l & \text{for } j \in I \end{matrix} \right\},$$

and

$$\Omega^{\mathcal{R}}(I, \sigma) = \Omega^{\mathcal{R}}(I, \sigma)(0)\,.$$

(b) Let $\mathcal{R} = \{P_1, \ldots, P_m\}$ be a decomposition of P. A subset $\emptyset \neq Z \subset D$ is called *$\mathcal{R}$-valuation-dependent* if there exists $y \in G$ such that

(V) $Z \subset y$, and if $a, c \in Z$, $b \in y$ and $v_j(a) \leq v_j(b) \leq v_j(c)$ for all $j \in \{1, \ldots, m\}$, then $b \in Z$.

(c) Let $\mathcal{R} = \{P_1, \ldots, P_m\}$ be a decomposition of P, $y \in G$ and $Z \subset y$ an

$\mathcal{R}$-valuation-dependent subset; we set

$$Z^{\#} = \left\{ a \in y \;\middle|\; \begin{array}{l} \text{there exists } c \in Z \ \text{ such that} \\ v_j(a) \le v_j(c) \ \text{ for all } 1 \le j \le m \end{array} \right\} \supset Z\,.$$

By a *Z-system* (I, σ) we mean a subset $I \subset \{1, \ldots, m\}$ together with a function $\sigma : I^{\mathrm{c}} \to \mathbb{N}_0$ such that $\emptyset \ne y \cap \Omega^{\mathcal{R}}(I, \sigma) \subset Z^{\#}$. A Z-system (I, σ) is called a *maximal Z-system* if there is no Z-system $(\bar{I}, \bar{\sigma})$ such that $I \subsetneq \bar{I}$ and $\bar{\sigma} = \sigma | \bar{I}^{\mathrm{c}}$. A subset $I \subset \{1, \ldots, m\}$ is called a *Z-set* if there exists $\sigma : I^{\mathrm{c}} \to \mathbb{N}_0$ such that (I, σ) is a Z-system.

If I is a maximal Z-set and $\sigma : I^{\mathrm{c}} \to \mathbb{N}_0$ is such that (I, σ) is a Z-system, then (I, σ) is a maximal Z-system; on the other hand, if (I, σ) is a maximal Z-system, then I need not be a maximal Z-set.

The following simple lemma will be useful.

Lemma 5. *Let $[D, H]$ be a formation, $D = \mathcal{F}(P)$ and $y \in G = D/H$. Let $\mathcal{R} = \{P_1, \ldots, P_m\}$ be a decomposition of P, $I \subset \{1, \ldots, m\}$, $\sigma : I^{\mathrm{c}} \to \mathbb{N}_0$ and $y \cap \Omega^{\mathcal{R}}(I, \sigma) \ne \emptyset$. Then $y \cap \Omega^{\mathcal{R}}(I, \sigma)(l) \ne \emptyset$ for all $l \in \mathbb{N}_0$.*

Proof. For any $i \in I$, fix $p_i \in P_i$, and set $q = \prod_{i \in I} p_i$. If $a \in y \cap \Omega^{\mathcal{R}}(I, \sigma)$ and $N = \#G$, then we clearly obtain $aq^{Nl} \in y \cap \Omega^{\mathcal{R}}(I, \sigma)(l)$ for all $l \in \mathbb{N}_0$. ∎

Proposition 9. *Let $[D, H]$ be a formation, $D = \mathcal{F}(P)$ and $y \in G = D/H$. Let $\mathcal{R} = \{P_1, \ldots, P_m\}$ be a decomposition of P, and let $Z \subset y$ be an $\mathcal{R}$-valuation-dependent subset.*

(i) *There exist only finitely many maximal Z-systems*; *if these are $(I_1, \sigma_1), \ldots, (I_m, \sigma_m)$, then*

$$(*) \qquad Z^{\#} = \bigcup_{j=1}^{m} y \cap \Omega^{\mathcal{R}}(I_j, \sigma_j)\,.$$

(ii) *If (I, σ) is a Z-system, then either $\Omega^{\mathcal{R}}(I, \sigma) \cap Z = \emptyset$, or there exists some $l \in \mathbb{N}_0$ such that $y \cap \Omega^{\mathcal{R}}(I, \sigma)(l) \subset Z$.*

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

$$(**) \qquad Z = \bigcup_{i=1}^{r} y \cap \Omega^{\mathcal{R}}(\bar{I}_i, \bar{\sigma}_i)(l_i)\,.$$

(iv) *Let $(I, \sigma), (I_1, \sigma_1), \ldots, (I_n, \sigma_n)$ be Z-systems, $l \in \mathbb{N}_0$ and*

$$y \cap \Omega^{\mathcal{R}}(I, \sigma)(l) \subset \bigcup_{\nu=1}^{n} \Omega^{\mathcal{R}}(I_\nu, \sigma_\nu)\,.$$

Then there exists some $\nu \in \{1, \ldots, n\}$ such that $I \subset I_\nu$ and $\sigma_\nu = \sigma | I_\nu^{\mathrm{c}}$.

In particular, the representation $(*)$ *above is unique. If the representation* $(**)$ *is incontractible, i.e., if there are no inclusions* $y \cap \Omega^{\mathcal{R}}(\bar{I}_i, \bar{\sigma}_i) \subset y \cap \Omega^{\mathcal{R}}(\bar{I}_k, \bar{\sigma}_k)$ *for* $i \neq k$, *then* $(**)$ *is also unique.*

Proof. (i) If $a \in Z^{\#}$ and $\sigma : \{1, \ldots, m\} \to \mathbb{N}_0$ is defined by $\sigma(j) = v_j(a)$, then $(\emptyset, \sigma)$ is a Z-system and $a \in y \cap \Omega^{\mathcal{R}}(\emptyset, \sigma)$. For every Z-system (I, σ), there exists a maximal Z-system $(\bar{I}, \bar{\sigma})$ such that $\Omega^{\mathcal{R}}(I, \sigma) \subset \Omega^{\mathcal{R}}(\bar{I}, \bar{\sigma})$; therefore it remains to prove that there are only finitely many maximal Z-systems. If not, then there exists a Z-set $I \subset \{1, \ldots, m\}$ and there exist infinitely many functions $\sigma : I^{\mathrm{c}} \to \mathbb{N}_0$ such that (I, σ) is a Z-system. In particular, there exists a sequence of functions $(\sigma_\nu : I^{\mathrm{c}} \to \mathbb{N}_0)_{\nu \geq 0}$ such that all (I, σ_ν) are Z-systems, and $\lim_{\nu \to \infty} \sigma_\nu(i_1) = \infty$ for some $i_1 \in I^{\mathrm{c}}$. By extracting subsequences of $(\sigma_\nu)_{\nu \geq 0}$ we arrive, in a finite number of steps, at the following situation: there exists a subset $\emptyset \neq I_1 \subset I^{\mathrm{c}}$, an integer $M \in \mathbb{N}$ and a sequence of functions $(\sigma_\nu : I^{\mathrm{c}} \to \mathbb{N}_0)_{\nu \geq 0}$ such that all (I, σ_ν) are Z-systems, $\lim_{\nu \to \infty} \sigma_\nu(i) = \infty$ for all $i \in I_1$, and $\sigma_\nu(i) \leq M$ for all $\nu \geq 0$ and $i \in I^{\mathrm{c}} \setminus I_1$. Therefore there exists $\sigma : I^{\mathrm{c}} \setminus I_1 \to \mathbb{N}_0$ and a subsequence $(\sigma_{\nu_k})_{k \geq 0}$ of $(\sigma_\nu)_{\nu \geq 0}$ such that $\sigma_{\nu_k}(i) = \sigma(i)$ for all $k \geq 0$ and $i \in I^{\mathrm{c}} \setminus I_1$. We assert that $(I \cup I_1, \sigma)$ is a Z-system, contrary to the maximality of the Z-systems (I, σ_ν). Indeed, $\emptyset \neq y \cap \Omega^{\mathcal{R}}(I, \sigma_{\nu_k}) \subset y \cap \Omega^{\mathcal{R}}(I \cup I_1, \sigma)$, and if $a \in y \cap \Omega^{\mathcal{R}}(I \cup I_1, \sigma)$, then there exists $k \in \mathbb{N}$ such that $\sigma_{\nu_k}(i) \geq v_i(a)$ for all $i \in I_1$; obviously, $\sigma_{\nu_k}(i) = \sigma(i) = v_i(a)$ for all $i \in I^{\mathrm{c}} \setminus I_1$. If $l = \max\{v_i(a) \mid i \in I\}$, then $y \cap \Omega^{\mathcal{R}}(I, \sigma_{\nu_k}) \neq \emptyset$ implies $y \cap \Omega^{\mathcal{R}}(I, \sigma_{\nu_k})(l) \neq \emptyset$ by Lemma 5; if $b \in y \cap \Omega^{\mathcal{R}}(I, \sigma_{\nu_k})(l)$, then we infer $b \in Z^{\#}$, and $v_i(a) \leq v_i(b)$ for all $i \in \{1, \ldots, m\}$ implies $a \in Z^{\#}$.

(ii) Suppose that there exists some $c \in \Omega^{\mathcal{R}}(I, \sigma) \cap Z$, and set $l = \max\{v_i(c) \mid i \in I\}$. If $a \in y \cap \Omega^{\mathcal{R}}(I, \sigma)(l)$, then $v_i(a) \geq v_i(c)$ for all $i \in \{1, \ldots, m\}$. Since $a \in Z^{\#}$, there exists $b \in Z$ such that $v_i(a) \leq v_i(b)$ for all $i \in \{1, \ldots, m\}$, and therefore (V) implies $a \in Z$.

(iii) By (i), we have

$$Z = \bigcup_{j=1}^{m} \Omega^{\mathcal{R}}(I_j, \sigma_j) \cap Z\,;$$

therefore it is sufficient to prove the following statement:

Given a Z-system such that $\Omega^{\mathcal{R}}(I, \sigma) \cap Z \neq \emptyset$, there exist finitely many Z-systems (I_ν, σ_ν) $(\nu = 1, \ldots, n)$ and $l_1, \ldots, l_n \in \mathbb{N}_0$ such that

$$\Omega^{\mathcal{R}}(I, \sigma) \cap Z = \bigcup_{\nu=1}^{n} y \cap \Omega^{\mathcal{R}}(I_\nu, \sigma_\nu)(l_\nu)\,.$$

We do this by induction on $\#I$. For $I = \emptyset$, there is nothing to prove; thus we suppose $I \neq \emptyset$. By (ii), there exists some $l \in \mathbb{N}_0$ such that $y \cap$

$\Omega^{\mathcal{R}}(I,\sigma)(l) \subset Z$, and

$$\Omega^{\mathcal{R}}(I,\sigma) = \Omega^{\mathcal{R}}(I,\sigma)(l) \cup \bigcup_{(I',\sigma')} \Omega^{\mathcal{R}}(I',\sigma'),$$

where the union is taken over all proper subsets $I' \subsetneq I$ and all functions $\sigma' : I'^{\mathrm{c}} \to \mathbb{N}_0$ satisfying $\sigma'|I^{\mathrm{c}} = \sigma$ and $\sigma'(i) < l$ for all $i \in I \setminus I'$. This implies

$$\Omega^{\mathcal{R}}(I,\sigma) \cap Z = y \cap \Omega^{\mathcal{R}}(I,\sigma)(l) \cup \bigcup_{(I',\sigma')} \Omega^{\mathcal{R}}(I',\sigma') \cap Z\,,$$

and the assertion follows by induction hypothesis.

(iv) Since $y \cap \Omega^{\mathcal{R}}(I,\sigma) \neq \emptyset$, Lemma 5 implies the existence of $a \in y \cap \Omega^{\mathcal{R}}(I,\sigma)(l)$ satisfying $v_i(a) > \max\{\sigma_\nu(j) \mid j \in I_\nu, 1 \le \nu \le n\}$ for all $i \in I$. If $\nu \in \{1,\ldots,n\}$ is such that $a \in \Omega^{\mathcal{R}}(I_\nu,\sigma_\nu)$, then we obtain $I \subset I_\nu$ and $\sigma_\nu = \sigma|I_\nu^{\mathrm{c}}$. The uniqueness assertions are now obvious. ■

The following proposition is fundamental for a quantitative investigation of valuation-dependent sets (cf. Theorem 3 below).

PROPOSITION 10. *Let $[D,H,|\cdot|]$ be an arithmetical formation, $D = \mathcal{F}(P)$, $G = D/H$ and $\mathcal{R} = \{P_1,\ldots,P_m\}$ a decomposition of P with the property that for every $j \in \{1,\ldots,m\}$, there exists $g_j \in G$ such that $P_j \subset g_j$, and P_j is regular with density ϱ_j. Let $I \subset \{1,\ldots,m\}$, $\varrho = \sum_{i\in I} \varrho_i$, $\sigma : I^{\mathrm{c}} \to \mathbb{N}_0$,*

$$d = \sum_{\substack{j\in I^{\mathrm{c}}\\ \varrho_j>0}} \sigma(j) \quad \text{and} \quad \varrho + d > 0\,.$$

Let $y \in G$, $y \cap \Omega^{\mathcal{R}}(I,\sigma) \neq \emptyset$ and $l \in \mathbb{N}_0$. Then we have, as $x \to \infty$,

$$\#\{a \in y \cap \Omega^{\mathcal{R}}(I,\sigma)(l) \mid |a| \le x\} \asymp x(\log x)^{-1+\varrho}(\log\log x)^{d'}\,,$$

where

$$d' = \begin{cases} d & \text{if } \varrho > 0, \\ d-1 & \text{if } \varrho = 0. \end{cases}$$

Proof. It suffices to consider the case $l = 0$; then the general case follows by means of the identity

$$\Omega^{\mathcal{R}}(I,\sigma)(l) = \Omega^{\mathcal{R}}(I,\sigma) \setminus \biguplus_{\substack{(e_i)_{i\in I}\\ 0\le e_i<l}} \{a \in \Omega^{\mathcal{R}}(I,\sigma) \mid v_i(a) = e_i \ \text{ for all } \ i \in I\}\,.$$

We may suppose that $I = \{n+1,\ldots,m\}$ and $I^{\mathrm{c}} = \{1,\ldots,n\}$ for some $0 \le n \le m$. We set $P_0 = P_{n+1} \cup \ldots \cup P_m$, and we consider the partition $\mathcal{P} = (P_0, P_1, \ldots, P_m)$ of P. Let $\mathfrak{T} \subset \mathcal{T}^*(\mathcal{P})$ be the set of all $\mathcal{P}$-types

$((t_{j,\nu})_{\nu\le\lambda_j})_{j=1,\ldots,n}$ satisfying

$$\sum_{\nu=1}^{\lambda_j} t_{j,\nu} = \sigma(j) \quad \text{for all } j \in I^{\mathrm{c}}.$$

For $a \in D$, we have $a \in \Omega^{\mathcal{R}}(I,\sigma)$ if and only if $\boldsymbol{\tau}^{\mathcal{P}}(a) \in \mathfrak{T}$. Now the assertion follows from Theorem 1. ∎

THEOREM 3. *Let $[D, H, |\cdot|]$ be an arithmetical formation, $D = \mathcal{F}(P)$, $G = D/H$ and $\mathcal{R} = \{P_1, \ldots, P_m\}$ a decomposition of P with the property that for every $j \in \{1, \ldots, m\}$, there exists a class $g_j \in G$ such that $P_j \subset g_j$, and P_j is regular with density ϱ_j. Let $Z \subset D$ be $\mathcal{R}$-valuation-dependent.*

(i) *If*

$$\varrho = \max\Big\{\sum_{i\in I}\varrho_i \;\Big|\; I \subset \{1,\ldots,m\} \ \text{ is a } Z\text{-set}\Big\},$$

$$d = \max\Big\{\sum_{\substack{j\in I^{\mathrm{c}}\\ \varrho_j>0}}\sigma(j) \;\Big|\; (I,\sigma) \ \text{ is a } Z\text{-system}, \ \sum_{i\in I}\varrho_i = \varrho\Big\}$$

and $\varrho + d > 0$, then we have, as $x \to \infty$,

$$\#\{a \in Z^{\#} \mid |a| \le x\} \asymp x(\log x)^{-1+\varrho}(\log\log x)^{d'},$$

where

$$d' = \begin{cases} d & \text{if } \varrho > 0,\\ d-1 & \text{if } \varrho = 0.\end{cases}$$

(ii) *If*

$$\bar\varrho = \max\left\{\sum_{i\in I}\varrho_i \;\middle|\; \begin{array}{l} I \subset \{1,\ldots,m\} \text{ is a } Z\text{-set such that}\\ y \cap \Omega(I,\sigma)(l) \subset Z \text{ for some } \sigma : I^{\mathrm{c}} \to \mathbb{N}_0 \text{ and } l \in \mathbb{N}_0\end{array}\right\},$$

$$\bar d = \max\left\{\sum_{\substack{j\in I^{\mathrm{c}}\\ \varrho_j>0}}\sigma(j) \;\middle|\; \begin{array}{l} (I,\sigma) \text{ is a } Z\text{-system such that}\\ y \cap \Omega(I,\sigma)(l) \subset Z \text{ for some } l \in \mathbb{N}_0 \text{ and } \sum_{i\in I}\varrho_i = \varrho\end{array}\right\}$$

and $\bar\varrho + \bar d > 0$, then we have, as $x \to \infty$,

$$\#\{a \in Z \mid |a| \le x\} \asymp x(\log x)^{-1+\bar\varrho}(\log\log x)^{\bar d'},$$

where

$$\bar d' = \begin{cases} \bar d & \text{if } \bar\varrho > 0,\\ \bar d-1 & \text{if } \bar\varrho = 0.\end{cases}$$

Proof. By Proposition 9(i),

$$Z^{\#} = \bigcup_{\mu=1}^{m} y \cap \Omega^{\mathcal{R}}(I_\mu, \sigma_\mu),$$

where the union is taken over all maximal Z-systems (I_μ, σ_μ), and Proposition 9(iv) implies

$$\varrho = \max\Big\{\sum_{i\in I_\mu} \varrho_i \;\Big|\; \mu = 1,\dots,m\Big\}$$

and

$$d = \max\Big\{\sum_{\substack{j\in I_\mu^{\mathrm{c}}\\ \varrho_j>0}} \sigma_\mu(j) \;\Big|\; \mu \in \{1,\dots,m\},\ \sum_{i\in I_\mu} \varrho_i = \varrho\Big\}\,.$$

Similarly, again by Proposition 9,

$$Z = \bigcup_{\nu=1}^{r} y \cap \Omega^{\mathcal{R}}(\bar I_\nu, \bar\sigma_\nu)(l_\nu)$$

where the union is taken over all Z-systems $(\bar I_\nu, \bar\sigma_\nu)$ and $l_\nu \in \mathbb{N}_0$ such that $y \cap \Omega^{\mathcal{R}}(\bar I_\nu, \bar\sigma_\nu)(l_\nu) \subset Z$ which are maximal with this property (then the representation is incontractible and thus unique). Therefore

$$\bar\varrho = \max\Big\{\sum_{i\in \bar I_\nu} \varrho_i \;\Big|\; \nu = 1,\dots,r\Big\}$$

and

$$\bar d = \max\Big\{\sum_{\substack{j\in \bar I_\nu^{\mathrm{c}}\\ \varrho_j>0}} \bar\sigma_\nu(j) \;\Big|\; \nu \in \{1,\dots,r\}, \sum_{i\in \bar I_\nu} \varrho_i = \bar\varrho\Big\}\,.$$

Now the assertion follows from Proposition 10 and the observation that, for any Z-systems (I_1,σ_1), (I_2,σ_2) and $l_1, l_2 \in \mathbb{N}_0$ we have either $\Omega^{\mathcal{R}}(I_1,\sigma_1)(l_1) \cap \Omega^{\mathcal{R}}(I_2,\sigma_2)(l_2) = \emptyset$, or $\Omega^{\mathcal{R}}(I_1,\sigma_1)(l_1) \cap \Omega^{\mathcal{R}}(I_2,\sigma_2)(l_2) = \Omega^{\mathcal{R}}(I_1\cap I_2,\sigma)(l)$, where $\sigma|I_1^{\mathrm{c}} = \sigma_1$, $\sigma|I_2^{\mathrm{c}} = \sigma_2$ and $l = \max(l_1, l_2)$. ■

For subsequent arithmetical applications of Theorem 3 we recall the concept of block semigroups (cf. [11; Beispiel 6]). For an additive finite abelian group G, let $\mathcal{F}(G)$ be the (multiplicative) free abelian monoid with basis G. For $B = \prod_{g\in G} g^{v_g(B)} \in \mathcal{F}(G)$, the element

$$\iota(B) = \sum_{g\in G} v_g(B) g \in G$$

is called the *content* of B, and

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

is called the *block semigroup* over G. If $\#G \ge 3$, then $[\mathcal{F}(G), \mathcal{B}(G)]$ is a formation, and $\iota : \mathcal{F}(G) \to G$ induces a group isomorphism $\iota^* : \mathcal{F}(G)/\mathcal{B}(G) \overset{\sim}{\to} G$. We identify the class group of $[\mathcal{F}(G),\ \mathcal{B}(G)]$ with G by means of ι^*.

If $[D, H]$ is a formation, $D = \mathcal{F}(P)$ and $G = D/H$, then there is a unique semigroup homomorphism $\boldsymbol{\beta} : D \to \mathcal{F}(G)$ such that $\boldsymbol{\beta}(p) = [p] \in G$ for all

$p \in P$. We have $\iota \circ \boldsymbol{\beta}(a) = [a]$ for all $a \in D$, and hence $H = \boldsymbol{\beta}^{-1}(\mathcal{B}(G))$. $\boldsymbol{\beta}$ is called the *block homomorphism* of $[D, H]$; it has the following arithmetical significance (cf. [4; Prop. 1]):

If $a \in H$, and $a = u_1 \ldots u_r$ is a factorization into irreducible elements $u_i \in H$, then $\boldsymbol{\beta}(a) = \boldsymbol{\beta}(u_1) \ldots \boldsymbol{\beta}(u_r)$ is a factorization of $\boldsymbol{\beta}(a)$ into irreducible blocks in $\mathcal{B}(G)$, and every factorization of $\boldsymbol{\beta}(a)$ into irreducible elements of $\mathcal{B}(G)$ arises in this way. In particular, $\mathbf{l}_H(a) = \mathbf{l}_{\mathcal{B}(G)}(\boldsymbol{\beta}(a))$.

Now let $([D, H, |\cdot|], [\overline{D}, \overline{H}], \varphi)$ be a Chebotarev formation, $\overline{G} = \overline{D}/\overline{H}$, and let $\boldsymbol{\beta} : \overline{D} \to \mathcal{F}(\overline{G})$ be the block homomorphism of $[\overline{D}, \overline{H}]$. If $D = \mathcal{F}(P)$ and $p, p' \in P$ are φ-equivalent, then $\boldsymbol{\beta} \circ \varphi(p) = \boldsymbol{\beta} \circ \varphi(p')$. If $\#\overline{G} \geq 3$, then $([D, H, |\cdot|], [\mathcal{F}(\overline{G}), \mathcal{B}(\overline{G})], \boldsymbol{\beta} \circ \varphi)$ is a Chebotarev formation, and the $(\boldsymbol{\beta} \circ \varphi)$-equivalence classes coincide with the φ-equivalence classes.

As in Section 3, we continue with two subsections dealing with arithmetical applications.

4.1. *Elements with a given block*

Proposition 11. *Let $([D, H, |\cdot|], [\overline{D}, \overline{H}], \varphi)$ be a Chebotarev formation, $D = \mathcal{F}(P)$, $G = D/H$, $\overline{D} = \mathcal{F}(\overline{P})$, $\overline{G} = \overline{D}/\overline{H}$, $\boldsymbol{\beta} : \overline{D} \to \mathcal{F}(\overline{G})$ the block homomorphism, and suppose that the set $P^* = \{p \in P \mid \varphi(p) = 1\}$ is finite. Let $\bar{e} \in \overline{D}$ and $y \in G$ be fixed. Let $\overline{B} \in \mathcal{F}(\overline{G})$ be given, and suppose that there exists $a_1 \in y$ having a prime factor in a φ-equivalence class of positive density and satisfying $\boldsymbol{\beta}(\varphi(a_1)\bar{e}) = \overline{B}$. Then we have, as $x \to \infty$,*

$$\#\{a \in y \mid |a| \leq x,\ \boldsymbol{\beta}(\varphi(a)\bar{e}) = \overline{B}\} \asymp x(\log x)^{-1}(\log\log x)^d$$

for some $d \in \mathbb{N}_0$.

Proof. Let $\mathcal{R} = \{P_1, \ldots, P_m\}$ be the set of all φ-equivalence classes, and $Z = \{a \in y \mid \boldsymbol{\beta}(\varphi(a)\bar{e}) = \overline{B}\}$. If $a, b \in D$, then $v_j(a) \leq v_j(b)$ for all $j \in \{1, \ldots, m\}$ implies $\boldsymbol{\beta}(\varphi(a)\bar{e}) \mid \boldsymbol{\beta}(\varphi(b)\bar{e})$ in $\mathcal{F}(\overline{G})$. Therefore Z is $\mathcal{R}$-valuation dependent. A subset $I \subset \{1, \ldots, m\}$ is a Z-set if and only if $\bigcup_{i \in I} P_i \subset P^*$. We apply Theorem 3; obviously, $\bar{\varrho} = 0$, and our assumption on a_1 guarantees $d = \bar{d} - 1 \geq 0$. ■

Remarks. 1. In Proposition 11, $Z^{\#} = \{a \in y \mid \boldsymbol{\beta}(\varphi(a)\bar{e}) \mid \overline{B}\}$, and Theorem 3 yields a similar asymptotic behaviour of $\#\{a \in Z^{\#} \mid |a| \leq x\}$.

2. In concrete arithmetical examples the exponent d can be determined very precisely (cf. [32; Theorem 9.4]).

As an application of Proposition 11, we determine the number of irreducible elements in residue classes of a holomorphy ring.

Proposition 11A. *Let R be a holomorphy ring in a global field. Let $\mathfrak{f}$ be a cycle of R, $\alpha_0 \in R$, and suppose that there exists an irreducible element*

$u \in R$ such that $u \equiv \alpha_0 \bmod \mathfrak{f}$ and $(u) \neq \gcd(\alpha_0, \mathfrak{f})$. Then we have, as $x \to \infty$,

$$\#\{(\alpha) \in \mathcal{H}_R \mid \alpha \in R,\ |(\alpha)| \le x,\ \alpha \equiv \alpha_0 \bmod \mathfrak{f},\ \alpha \textit{ is irreducible in } R\} \asymp x(\log x)^{-1}(\log\log x)^{d'}$$

for some $d' \in \mathbb{N}_0$.

Proof. If $\boldsymbol{\beta} : \mathcal{I}_R \to \mathcal{F}(G)$ is the block homomorphism of the formation $[\mathcal{I}_R, \mathcal{H}_R]$, then an element $\alpha \in R$ is irreducible if and only if $(\alpha) \neq (1) \in \mathcal{H}_R$, and $\boldsymbol{\beta}((\alpha))$ is irreducible in $\mathcal{B}(G)$. Since there exist only finitely many irreducible blocks in $\mathcal{B}(G)$, the problem is reduced to that of counting elements with a given block. Therefore Proposition 11 applies, and the result is derived by the same methods as used in the proofs of Propositions 6A and 6B. ■

Remarks. 1. Proposition 11A can be strengthened if $\gcd(\alpha_0, \mathfrak{f}) = 1$. Then the existence of an element u with the indicated properties is obvious; moreover, we obtain $d' = D(G) - 1$, where $D(G)$ is Davenport's constant of the ideal class group G of R.

2. The first special case of Proposition 11A was proved in [35]; for generalizations see [15].

4.2. *Elements with a given number of lengths*

Proposition 12. *Let $([D, H, |\cdot|], [\overline{D}, \overline{H}], \varphi)$ be a Chebotarev formation, $D = \mathcal{F}(P)$, $\overline{D} = \mathcal{F}(\overline{P})$, $G = D/H$, $\overline{G} = \overline{D}/\overline{H}$ and $\#\overline{G} \ge 3$. Suppose that for every $\bar{g} \in \overline{G}$ there exists $p \in P$, lying in a φ-equivalence class of positive density, such that $\varphi(p)$ has a prime factor in $\bar{g}$. We set*

$$P_0 = \{p \in P \mid v_{\bar{p}}(\varphi(p)) = 0 \textit{ for all } \bar{p} \in \overline{P} \setminus \overline{H}\}$$

and suppose that $\varrho_0 = \varrho(P_0) > 0$. Let $\bar{e} \in \overline{D}$ satisfy $\gcd(\varphi(a), \bar{e}) = 1$ for all $a \in D$. Let $y \in G$, $k \in \mathbb{N}$, and suppose that there exists $a_1 \in y$ such that $\varphi(a_1)\bar{e} \in \overline{H}$ and $\mathbf{l}_{\overline{H}}(\varphi(a_1)\bar{e}) \le k$. Then we have, as $x \to \infty$,

$$\#\{a \in y \mid |a| \le x,\ \mathbf{l}_{\overline{H}}(\varphi(a)\bar{e}) \le k\} \asymp x(\log x)^{-1+\varrho}(\log\log x)^{d},$$

where $\varrho_0 \le \varrho < 1$ and $d \in \mathbb{N}_0$.

Proof. Let $\mathcal{R} = \{P_1, \ldots, P_m\}$ be the set of all φ-equivalence classes. Since $\varphi(H) \subset \overline{H}$, we obtain $\varphi(a)\bar{e} \in \overline{H}$ for all $a \in y$, and we consider the set $Z = \{a \in y \mid \mathbf{l}_{\overline{H}}(\varphi(a)\bar{e}) \le k\}$. If $\boldsymbol{\beta} : \overline{D} \to \mathcal{F}(\overline{G})$ is the block homomorphism, then $\mathbf{l}_{\overline{H}}(\varphi(a)\bar{e}) = \mathbf{l}_{\mathcal{B}(\overline{G})}(\boldsymbol{\beta}(\varphi(a)\bar{e}))$ for all $a \in y$, and $v_j(a) = v_j(b)$ for all $j \in \{1, \ldots, m\}$ implies $\boldsymbol{\beta}(\varphi(a)\bar{e}) = \boldsymbol{\beta}(\varphi(b)\bar{e})$ for all $a, b \in D$. Therefore Z is valuation-dependent, and even $Z = Z^{\#}$; we shall apply Theorem 3(i).

If $p \in P_0$, then $\boldsymbol{\beta}(\varphi(p)) = (0)^k$ for some $k \in \mathbb{N}$, and $\mathbf{l}_{\mathcal{B}(\overline{G})}(B(0)^k) = \mathbf{l}_{\mathcal{B}(\overline{G})}(B)$ for every $B \in \mathcal{B}(\overline{G})$. Consequently, every set $I \subset \{1, \ldots, m\}$ satisfying $\bigcup_{i \in I} P_i \subset P_0$ is a Z-set, which implies $\varrho \geq \varrho_0$.

It remains to prove that $\varrho < 1$. If, on the contrary, $\varrho = 1$, then there exists a Z-system (I, σ) such that $\sum_{i \in I} \varrho_i = 1$ and consequently $\varrho_j = 0$ for all $j \in I^{\mathrm{c}}$. Since $\#\overline{G} \geq 3$, there exists $\overline{B} \in \mathcal{B}(\overline{G})$ such that $\mathbf{l}_{\mathcal{B}(\overline{G})}(\overline{B}) > k$ (see [4; Lemma 1]). For every $g \in \overline{G}$ there exists (by assumption) $p \in P_i$ (for some $i \in I$) such that $g | \boldsymbol{\beta}(\varphi(p))$ in $\mathcal{F}(\overline{G})$. Therefore there exists $a \in y \cap \Omega(I, \sigma)$ such that $\overline{B} | \boldsymbol{\beta}(\varphi(a)\bar{e})$ in $\mathcal{B}(\overline{G})$, whence $\mathbf{l}_{\overline{H}}(\varphi(a)\bar{e}) > k$, a contradiction. ■

Proposition 12A. *Let $\overline{K}/K$ be a finite extension of algebraic number fields*, R, $\overline{R}$ *their rings of integers*, $\mathfrak{f}$ *a cycle of R and $\alpha_0 \in R$ such that $\mathbf{l}_{\mathcal{H}_{\overline{R}}}(\alpha_0 \overline{R}) \leq k$ for some $k \in \mathbb{N}$. If the class number of $\overline{K}$ is at least* 3, *then we have*, *as $x \to \infty$*,

$$\#\{(\alpha) \in \mathcal{H}_R \mid \alpha \in R,\ |(\alpha)| \leq x,\ \alpha \equiv \alpha_0 \bmod \mathfrak{f},\ \mathbf{l}_{\mathcal{H}_{\overline{R}}}(\alpha \overline{R}) \leq k\} \asymp x(\log x)^{-\varrho}(\log\log x)^d$$

for some $0 < \varrho < 1$ and $d \in \mathbb{N}_0$.

Proof. By Proposition 12, similarly to Proposition 6B. ■

Remark 1. There are several special cases of Proposition 12A in which the exponents ϱ and d can be given more precisely (cf. [37], [38], [5], [10] and [26], [30]).

Remark 2. There are some other properties of non-unique factorization which have been studied in recent years and which can be handled (and generalized) using the method of valuation-dependent sets (cf. [20], [9]).

5. More precise asymptotics. All results of this paper are of the shape

$$A(x) \asymp x(\log x)^{-\varrho}(\log\log x)^d$$

for some $0 < \varrho < 1$ and $d \in \mathbb{N}_0$. The weakness of these results comes from the weak notion of regularity introduced in Definition 2. If there the algebra Λ is replaced by the algebra $\overline{\Lambda}$ of all complex functions which are regular in the closed half-plane $\Re s \geq 1$, then all asymptotic results get the form

$$A(x) \sim Cx(\log x)^{-\varrho}(\log\log x)^d$$

for some positive constant C, which can be explicitly calculated and has been determined in several special cases (cf. [32; Ch. 9], [26], [27], [16]). In particular, in Proposition 1 we obtain $C = \varrho$.

In the case of algebraic number fields, the methods of J. Kaczorowski

[21] yield more precise results, namely

$$A(x) = \sum_{\nu=1}^{r} x(\log x)^{-\varrho_\nu}\Big[\sum_{j=0}^{M}(\log x)^{-j}P_{k,j}(\log\log x) \\ +O((\log x)^{-M-1}(\log\log x)^{N})\Big]$$

for every $M \in \mathbb{N}$; here $N \in \mathbb{N}$ is a fixed exponent, $P_{k,j} \in \mathbb{C}[X]$ are polynomials, $0 < \varrho_1 \le 1$, $\varrho_2, \ldots, \varrho_r \in \mathbb{C}$, $0 \le \Re\varrho_\nu < \varrho_1$ and $r = 1$ in all results of Section 3 and Subsection 4.1. Moreover, it is even possible not to fix M, but to take a suitable $M = M(x) \to \infty \quad (x \to \infty)$, thereby obtaining asymptotics which can be made as precise as zero-free regions of Hecke L-functions are known.

In the case of algebraic function fields, the L-functions have zeros for $\Re s = 1$. Using the methods of [17] it is possible to derive a result which is formally analogous to that of the number field case, but under the restriction that x goes to ∞ through natural powers of q, the cardinality of the constant field.

References

[1] H. Delange, *Généralisation du théorème de Ikehara*, Ann. Sci. École Norm. Sup. 71 (1954), 213–242.

[2] E. Fogels, *Zur Arithmetik quadratischer Zahlenkörper*, Wiss. Abh. Univ. Riga, Kl. Math. Abt. 1 (1943), 23–47.

[3] F. D. Fried and M. Jarden, *Field Arithmetic*, Springer, 1986.

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

[5] —, *Ein quantitatives Resultat über Faktorisierungen verschiedener Länge in algebraischen Zahlkörpern*, ibid. 205 (1990), 159–162.

[6] —, *Arithmetical characterizations of divisor class groups*, Arch. Math. (Basel) 54 (1990), 455–464.

[7] —, *Factorization of natural numbers in algebraic number fields*, Acta Arith. 57 (1991), 365–373.

[8] —, *Arithmetical characterizations of divisor class groups, II*, to appear.

[9] A. Geroldinger and F. Halter-Koch, *Non-unique factorizations in block semigroups and arithmetical applications*, Math. Slovaca, to appear.

[10] A. Geroldinger and J. Kaczorowski, *Analytic and arithmetic theory of semigroups with divisor theory*, to appear.

[11] F. Halter-Koch, *Halbgruppen mit Divisorentheorie*, Exposition. Math. 8 (1990), 27–66.

[12] —, *A note on ray class fields of global fields*, Nagoya Math. J. 120 (1990), 61–66.

[13] —, *Finiteness theorems for factorizations*, Semigroup Forum 44 (1992), 112–117.

[14] —, *Typenhalbgruppen und Faktorisierungsprobleme*, to appear.

[15] —, *A generalization of Davenport's constant and its arithmetical applications*, Colloq. Math. 63 (1992), to appear.

[16] —, *Factorization problems in formations of class number two*, to appear.

[17] 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.

[18] H. Hasse, *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper*, Teil I, Ia und II, Physica-Verlag, 1965.

[19] N. Jacobson, *Basic Algebra I*, W. H. Freeman & Co., 1985.

[20] J. Kaczorowski, *Completely irreducible numbers in algebraic number fields*, Funct. Approx. 11 (1981), 95–104.

[21] —, *Some remarks on factorization in algebraic number fields*, Acta Arith. 43 (1983), 53–68.

[22] J. Knopfmacher, *Abstract Analytic Number Theory*, North-Holland, 1975.

[23] H. W. Leopoldt, *Zur Geschlechtertheorie in abelschen Zahlkörpern*, Math. Nachr. 9 (1953), 350–362.

[24] W. Narkiewicz, *On natural numbers having unique factorization in a quadratic number field*, Acta Arith. 12 (1966), 1–22.

[25] —, *Factorization of natural numbers in some quadratic number fields*, Colloq. Math. 16 (1967), 257–268.

[26] —, *On natural numbers having unique factorization in a quadratic number field, II*, Acta Arith. 13 (1967), 123–129.

[27] —, *A note on factorizations in quadratic fields*, ibid. 15 (1968), 19–22.

[28] —, *Numbers with unique factorization in an algebraic number field*, ibid. 21 (1972), 313–322.

[29] —, *Finite abelian groups and factorization problems*, Colloq. Math. 42 (1979), 319–330.

[30] —, *Numbers with all factorizations of the same length in a quadratic number field*, ibid. 45 (1981), 71–74.

[31] —, *Number Theory*, World Scientific, 1983.

[32] —, *Elementary and Analytic Theory of Algebraic Numbers*, Springer, 1990.

[33] W. Narkiewicz and J. Śliwa, *Finite abelian groups and factorization problems, II*, Colloq. Math. 46 (1982), 115–122.

[34] R. W. K. Odoni, *On a problem of Narkiewicz*, J. Reine Angew. Math. 288 (1976), 160–167.

[35] P. Rémond, *Étude asymptotique de certaines partitions dans certains semi-groupes*, Ann. Sci. École Norm. Sup. 83 (1966), 343–410.

[36] J. P. Serre, *Zeta and L functions*, in: Arithmetical Algebraic Geometry, Harper and Row, 1965, 82–92.

[37] J. Śliwa, *A note on factorizations in algebraic number fields*, Bull. Acad. Polon. Sci. 24 (1976), 313–314.

[38] —, *Factorizations of distinct lengths in algebraic number fields*, Acta Arith. 31 (1976), 399–417.

[39] E. Weiss, *Algebraic Number Theory*, McGraw-Hill, 1963.

INSTITUT FÜR MATHEMATIK
KARL-FRANZENS-UNIVERSITÄT
HEINRICHSTRASSE 36/IV
A-8010 GRAZ, ÖSTERREICH

Received on 27.1.1992
and in revised form on 16.3.1992 (2219)