J. reine angew. Math. **459** (1995), 89—118

Journal für die reine und
angewandte Mathematik
© Walter de Gruyter
Berlin · New York 1995

Non-unique factorizations in orders of global fields

By *Alfred Geroldinger* and *Franz Halter-Koch* at Graz and *Jerzy Kaczorowski* at Poznan

§ 1. Introduction

Let K be an algebraic number field and $\mathfrak{o}$ a (not necessarily principal) order in K. Then $\mathfrak{o}$ is a one-dimensional noetherian domain and its integral closure is the ring $\mathfrak{o}_K$ of algebraic integers of K. Every non-unit $0 \neq u \in \mathfrak{o}$ possesses a factorization into irreducible elements of $\mathfrak{o}$; in general, there are several distinct such factorizations. If $\mathfrak{o} = \mathfrak{o}_K$, then the class group of K measures the deviation of $\mathfrak{o}$ from unique factorization; cf. [3] or [22], Ch. 9 and the literature cited there for the interdependence of phenomena of non-unique factorizations and the structure of the class group. If $\mathfrak{o} \neq \mathfrak{o}_K$, then the factorization properties in $\mathfrak{o}$ do not depend only on the class group $\mathrm{Pic}(\mathfrak{o})$ of invertible ideals of $\mathfrak{o}$, but also on the structure of the local rings $\mathfrak{o}_\mathfrak{p}$ for the primes $\mathfrak{p}$ dividing the conductor of $\mathfrak{o}$; cf. [1], [4], [5] or [16] for some results in this direction (which are far from being as complete as in the case $\mathfrak{o} = \mathfrak{o}_K$).

Quantitative aspects of non-unique factorizations were first considered by E. Fogels 1943 in a special case and then investigated in greater generality by W. Narkiewicz, J. Śliwa and the authors; see [13], [17], [18] or [22], Ch. 9 for detailed references. In this paper we shall extend these quantitative investigations to non-principal orders. For $\mathfrak{o}$ as above and $k \in \mathbb{N}$, we shall investigate the following sets (which are well-studied in the case $\mathfrak{o} = \mathfrak{o}_K$):

$\mathbf{M}_k(\mathfrak{o})$, the set of all $u \in \mathfrak{o}$ having only factorizations of lengths $l \leqq k$;

$\mathbf{G}_k(\mathfrak{o})$, the set of all $u \in \mathfrak{o}$ having factorizations of at most k different lengths;

$\mathbf{F}_k(\mathfrak{o})$, the set of all $u \in \mathfrak{o}$ having at most k distinct factorizations.

If Z is one of these sets and $x \geqq 1$, then $Z(x)$ denotes the number of principal ideals $u\mathfrak{o}$ of $\mathfrak{o}$ such that $u \in Z$ and $(\mathfrak{o} : u\mathfrak{o}) \leqq x$. It turns out that $Z(x)$ has, for $x \to \infty$, the same type of asymptotic behaviour as in the case $\mathfrak{o} = \mathfrak{o}_K$, namely

$$Z(x) \sim Cx(\log x)^{-A}(\log\log x)^{B},$$

where C is a positive constant, $0 \leqq A \leqq 1$ and $B \in \mathbb{N}_0$. The reason for this behaviour lies in the fact, that besides of the finitely many prime ideals dividing the conductor of $\mathfrak{o}$ the arithmetic behaves exactly as in $\mathfrak{o}_K$. The point is to show that the influence of these finitely many prime ideals is small enough to obtain the same asymptotic results as in the case $\mathfrak{o} = \mathfrak{o}_K$. In fact, we shall prove stronger results, giving not only the main term but also the remainder term of the asymptotic behaviour; see Theorems 1$\mathfrak{o}$, 2$\mathfrak{o}$ and 3$\mathfrak{o}$ (for $\mathfrak{o} = \mathfrak{o}_K$ this was done in [18]).

It turns out that the asymptotic behaviour of $Z(x)$ is not a typical result of algebraic number theory. It holds for more general structures including orders in holomorphy rings of global fields and certain types of submonoids defined by congruences (so-called generalized Hilbert semigroups); the main results in this general context are Theorems 1, 2 and 3. We proceed axiomatically, a method which already proved its worth in [7], [13] and [17]. The main argument for the use of the axiomatic method in this context comes from the fact that it allows us to describe and investigate the combinatorial structures which are responsible for the various phenomena of non-unique factorization. Only in a second step we show how to realize these combinatorial structures in one-dimensional domains, and in a third step we use some (rather simple) arguments from (abstract) analytic number theory to derive the main results for arbitrary orders from those of principal orders.

In § 2 we start with some preliminaries on monoids; then we introduce the notion of an arithmetical order formation which is fundamental for the whole paper. In § 3 we discuss congruence monoids in Dedekind domains and in particular in holomorphy rings of global fields, which are in the center of our interest. § 4 contains the main results of our analytical theory; these will be applied in § 5 to obtain asymptotic results for the sets $\mathbf{M}_k$, $\mathbf{G}_k$ and $\mathbf{F}_k$ in order formations.

In the asymptotic analysis, we use simultaneously the notions $f \ll g$ and $f = O(g)$ and we write $f \asymp g$ for $f \ll g$ and $g \ll f$. Whenever a complex logarithm appears, we mean that branch which is real for positive arguments, and we put $z^{\varrho} = \exp(\varrho \log z)$. $\mathbb{N}$ denotes the set of positive integers, and $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$.

§ 2. Preliminaries. Order formations

Throughout this paper, a monoid is a multiplicatively written commutative and cancellative semigroup H with unit element $1 \in H$. We denote by $H^{\times}$ the group of invertible elements of H, and we call H reduced if $H^{\times} = \{1\}$. We use the standard notions of divisibility theory as developed in [9], § 6.

If H_1 and H_2 are monoids, then $H_1 \times H_2$ denotes the direct product of H_1 and H_2; we view H_1 and H_2 as submonoids of $H_1 \times H_2$ so that every $u \in H_1 \times H_2$ has a unique decomposition $u = u_1 u_2$, where $u_i \in H_i$. For a family $(H_\lambda)_{\lambda \in \Lambda}$ of monoids, we denote as usual by $\prod_{\lambda \in \Lambda} H_\lambda$ their (outer) direct product consisting of all families $(a_\lambda)_{\lambda \in \Lambda}$, where $a_\lambda \in H_\lambda$, and we set

$$\coprod_{\lambda \in \Lambda} H_\lambda = \{(a_\lambda)_{\lambda \in \Lambda} \in \prod_{\lambda \in \Lambda} H_\lambda \mid a_\lambda = 1 \text{ for almost all } \lambda \in \Lambda\}.$$

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

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

where $v_p(a) \in \mathbb{N}_0$ and $v_p(a) = 0$ for almost all $p \in P$.

Let D be a monoid and $H \subset D$ a submonoid. On D, we define the 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 by D/H the factor monoid (consisting of all congruence classes $g \subset D$); H is called saturated (in D), if $H = \{a \in D \mid a \equiv 1 \bmod H\}$ (equivalently: $a, b \in H$ and $a|b$ in D implies $a|b$ in H).

For the following notions concerning monoid homomorphisms, we refer to [6]. A monoid homomorphism $\varphi : H \to D$ is said to be

1. *cofinal*, if for every $a \in D$ there exists some $u \in H$ such that $a|\varphi(u)$ (equivalently: $D/\varphi H$ is a group);

2. a *divisor homomorphism*, if $u, v \in H$ and $\varphi(u)|\varphi(v)$ implies $u|v$ (equivalently: $\varphi H \subset D$ is a saturated submonoid, and φ induces an isomorphism $H/H^\times \xrightarrow{\sim} \varphi H$);

3. a *divisor theory*, if $D = \mathcal{F}(P)$ is free abelian, φ is a divisor homomorphism, and for every $p \in P$ there exist $u_1, \ldots, u_m \in H$ such that $p = \gcd\{\varphi(u_1), \ldots, \varphi(u_m)\}$ (then φ is also cofinal).

Definition 1. An *order formation* $[\mathcal{F}(P), T, H]$ consists of a free abelian monoid $\mathcal{F}(P)$, a reduced monoid T and a saturated submonoid $H \subset \mathcal{F}(P) \times T$, such that

$$G = (\mathcal{F}(P) \times T)/H$$

is a group. We write G additively and call it the *class group* of the order formation $[\mathcal{F}(P), T, H]$; for $\mathfrak{a} \in \mathcal{F}(P) \times T$, we denote by $[\mathfrak{a}] \in G$ the class containing the element $\mathfrak{a}$.

The idea behind the above definition is the following: we intend to investigate the arithmetic of the monoid H by means of $\mathcal{F}(P) \times T$, where T is assumed to be small. The most important examples of order formations arise from congruence monoids in Dedekind domains and in particular from the multiplicative monoids of one-dimensional noetherian domains. These will be discussed in § 3. Here we present some examples in the context of general monoids.

Examples. 1. If $\partial : H \to \mathcal{F}(P)$ is a divisor theory, then $[\mathcal{F}(P), \{1\}, \partial H]$ is an order formation.

2. If $\varphi : H \to T$ is a cofinal divisor homomorphism, then $[\{1\}, T, \varphi H]$ is an order formation.

3. Let G be a finite abelian group, T a reduced monoid and $\iota : \mathscr{F}(G) \times T \to G$ a monoid homomorphism such that $\iota(g) = g$ for all $g \in G$. Let

$$\mathscr{B}(G, T, \iota) = \{\mathfrak{a} \in \mathscr{F}(G) \times T \mid \iota(\mathfrak{a}) = 0\}$$

be the T-block monoid; then $[\mathscr{F}(G), T, \mathscr{B}(G, T, \iota)]$ is an order formation by [5], Prop. 1.

The following lemma strengthens the conception that an order formation is like a divisor theory with some obstruction.

Lemma 1. *Let $[\mathscr{F}(P), T, H]$ be an order formation with class group G. Then the embedding $i : H \cap \mathscr{F}(P) \to \mathscr{F}(P)$ is a divisor homomorphism. If $g \cap \mathscr{F}(P) \neq \emptyset$ for all $g \in G$, then i is cofinal and $G \simeq \mathscr{F}(P)/\big(H \cap \mathscr{F}(P)\big)$. If furthermore $g \cap P \neq \emptyset$ for all $g \in G$, and if in the case $\# G = 2$ the non-principal class $g \in G$ satisfies $\#(g \cap P) \geqq 2$, then i is a divisor theory.*

Proof. Since $H \subset \mathscr{F}(P) \times T$ is saturated, $H \cap \mathscr{F}(P) \subset \mathscr{F}(P)$ is also saturated, i.e., i is a divisor homomorphism. If $g \cap \mathscr{F}(P) \neq \emptyset$ for all $g \in G$, the canonical homomorphism $\mathscr{F}(P) \to \mathscr{F}(P) \times T \to G$ is surjective and induces an isomorphism $\mathscr{F}(P)/\big(H \cap \mathscr{F}(P)\big) \xrightarrow{\sim} G$. If we identify the two groups by means of this isomorphism the final assertion follows from [13], Lemma 1. □

Next we introduce norms on order formations in order to develop analytical results.

Definition 2. Let T be a reduced monoid. By a *norm function* on T we mean a monoid homomorphism $|\cdot| : T \to \mathbb{N}$ satisfying $|t| = 1$ if and only if $t = 1$.

Definition 3. By a *small arithmetical monoid* $[T, |\cdot|]$ *of rank* $r \in \mathbb{N}$ we mean a reduced monoid T, together with a norm function $|\cdot|$ on T satisfying

$$\# \{t \in T \mid |t| \leqq x\} \ll (\log x)^r$$

for every $x \geqq 2$.

Definition 4. An *arithmetical order formation* $[\mathscr{F}(P), T, H, |\cdot|]$ (*of rank* $r \in \mathbb{N}$) consists of an order formation $[\mathscr{F}(P), T, H]$ with finite class group $G = \big(\mathscr{F}(P) \times T\big)/H$, together with a norm function $|\cdot| : \mathscr{F}(P) \times T \to \mathbb{N}$ satisfying the following two properties:

1. For every $g \in G$, there is a complex function $h_g(s)$, regular in the half-plane $\Re s > 1$ and also in some neighbourhood of $s = 1$ such that

$$\sum_{p \in P \cap g} |p|^{-s} = \frac{1}{\# G} \log \frac{1}{s-1} + h_g(s)$$

holds for $\Re s > 1$.

2. $[T, |\cdot|]$ is a small arithmetical monoid (of rank r).

Remark. If $[\mathscr{F}(P), T, H, |\cdot|]$ is an arithmetical order formation, then

$$[\mathcal{F}(P), \mathcal{F}(P) \cap H, |\cdot|]$$

is an arithmetical formation in the sense of [13], Def. 2, with the same class group.

§ 3. Congruence monoids

For an integral domain R, let $R^\bullet = R \setminus \{0\}$ be its multiplicative monoid, $R^\times = R^{\bullet\times}$ its group of units, $\mathcal{P}(R)$ the set of all maximal ideals of R and $\mathcal{I}(R)$ the monoid of integral invertible ideals of R. Our standard references for ideal theory are [19] and [20].

Now let R be a Dedekind domain; then $\mathcal{I}(R) = \mathcal{F}(\mathcal{P}(R))$. Let

$$\mathfrak{f}^* = \mathfrak{f}\omega_1 \cdot \ldots \cdot \omega_m$$

be a cycle of R, i.e., $\mathfrak{f}^*$ is a formal product of an ideal $\mathfrak{f} \in \mathcal{I}(R)$ and $m \geqq 0$ distinct ring monomorphisms $\omega_1, \ldots, \omega_m : R \to \mathbb{R}$; see [11], Def. 4. For $1 \leqq i \leqq m$ we set $\sigma_i = \operatorname{sgn} \circ \omega_i$ where $\operatorname{sgn} : \mathbb{R} \to \{0, \pm 1\}$ denotes the signum function. Let

$$\Gamma^* \subset (R/\mathfrak{f}) \times \{\pm 1\}^m$$

be a multiplicatively closed subset, and let $\Gamma \subset R/\mathfrak{f}$ be the image of Γ^* under the projection $(R/\mathfrak{f}) \times \{\pm 1\}^m \to R/\mathfrak{f}$. We suppose that $\Gamma \cap (R/\mathfrak{f})^\times$ is a subgroup of $(R/\mathfrak{f})^\times$; if $R/\mathfrak{f}$ is finite, this is equivalent with $\Gamma \cap (R/\mathfrak{f})^\times \neq \emptyset$ or $1 + \mathfrak{f} \in \Gamma$. Then we call

$$H = \{a \in R^\bullet \mid (a + \mathfrak{f}, \sigma_1(a), \ldots, \sigma_m(a)) \in \Gamma^*\}$$

the *congruence monoid of R modulo $\mathfrak{f}^*$ defined by Γ^**.

With H as above, we associate a divisor homomorphism ∂ as follows:

Suppose that $\mathfrak{f} = \mathfrak{p}_1^{e_1} \cdot \ldots \cdot \mathfrak{p}_r^{e_r}$, where $r \geqq 0$, $\mathfrak{p}_1, \ldots, \mathfrak{p}_r \in \mathcal{P}(R)$ are distinct and $e_1, \ldots, e_r \in \mathbb{N}$. We set $P = \mathcal{P}(R) \setminus \{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$; then $\mathcal{F}(P) = \mathcal{I}_\mathfrak{f}(R) \subset \mathcal{I}(R)$ is the monoid of integral ideals relatively prime to $\mathfrak{f}$. By localization and the Chinese remainder theorem, we obtain a surjective mapping

$$\pi : \prod_{i=1}^r R_{\mathfrak{p}_i}^\bullet \to \prod_{i=1}^r R_{\mathfrak{p}_i}/\mathfrak{p}_i^{e_i} R_{\mathfrak{p}_i} \xrightarrow{\sim} \prod_{i=1}^r R/\mathfrak{p}_i^{e_i} \xrightarrow{\sim} R/\mathfrak{f}.$$

We set

$$U = \pi^{-1}(\Gamma) \subset \prod_{i=1}^r R_{\mathfrak{p}_i}^\bullet \quad \text{and} \quad T = U/U^\times.$$

For later use, we observe that

$$U^\times = U \cap \prod_{i=1}^r R_{\mathfrak{p}_i}^\times = \pi^{-1}(\Gamma^\times) = \pi^{-1}(\Gamma \cap (R/\mathfrak{f})^\times),$$

and therefore

$$\prod_{i=1}^{r} (1+\mathfrak{p}_i^{e_i} R_{\mathfrak{p}_i}) \subset U^{\times}\,.$$

For $a \in H$, we have $a + \mathfrak{f} \in \Gamma$, and consequently $(a, \dots, a) \in U \subset \prod_{i=1}^{r} R_{\mathfrak{p}_i}^{\bullet}$; we set

$$\Delta(a) = (a, \dots, a)\, U^{\times} \in T\,,$$

and we define $\partial : H \to \mathcal{F}(P) \times T$ by

$$\partial(a) = \Big(\prod_{\mathfrak{p} \in P} \mathfrak{p}^{v_{\mathfrak{p}}(a)}\Big)\,\Delta(a) \in \mathcal{F}(P) \times T\,.$$

We call ∂ the *canonical divisor homomorphism associated with H.*

Proposition 1. *The canonical divisor homomorphism $\partial : H \to \mathcal{F}(P) \times T$, associated with a congruence monoid H as above, has the following properties*:

(i) *∂ is a divisor homomorphism.*

(ii) *For every $\mathfrak{a} \in \mathcal{F}(P) \times T$, there exists some $c \in \mathcal{F}(P)$ such that $\mathfrak{a} c \in \partial H$.*

(iii) *$G = (\mathcal{F}(P) \times T)/\partial H$ is a group, and for every $g \in G$ we have $g \cap \mathcal{F}(P) \neq \emptyset$.*

(iv) *$\Delta(H) = T$.*

(v) *$[\mathcal{F}(P), T, \partial H]$ is an order formation.*

Proof. (i) If $a, b \in H$ and $\partial(a) \mid \partial(b)$, then $v_{\mathfrak{p}}(a) \leqq v_{\mathfrak{p}}(b)$ for all $\mathfrak{p} \in P$ and $\Delta(a) \mid \Delta(b)$; the latter relation implies $v_{\mathfrak{p}_i}(a) \leqq v_{\mathfrak{p}_i}(b)$ for $1 \leqq i \leqq r$, and therefore $a \mid b$.

(ii) Let

$$\mathfrak{a} = \Big(\prod_{\mathfrak{p} \in P} \mathfrak{p}^{e_{\mathfrak{p}}}\Big) \cdot (a_1, \dots, a_r)\, U^{\times} \in \mathcal{F}(P) \times T$$

be given, where $e_{\mathfrak{p}} \in \mathbb{N}_0$, $e_{\mathfrak{p}} = 0$ for almost all $\mathfrak{p} \in P$ and $(a_1, \dots, a_r) \in U \subset \prod_{i=1}^{r} R_{\mathfrak{p}_i}^{\bullet}$. If $a_i = u_i^{-1} c_i$ (where $c_i \in R^{\bullet}$ and $u_i \in R \backslash \mathfrak{p}_i$), let $y_i \in R$ be such that $u_i y_i \equiv 1 \bmod \mathfrak{p}_i^{e_i}$; then we have $(u_1 y_1, \dots, u_r y_r) \in \prod_{i=1}^{r} (1 + \mathfrak{p}_i^{e_i} R_{\mathfrak{p}_i}) \subset U^{\times}$, which implies

$$(c_1 y_1, \dots, c_r y_r)\, U^{\times} = (a_1, \dots, a_r)\, U^{\times} \subset U$$

and therefore $\pi(c_1 y_1, \dots, c_r y_r) \in \Gamma$. Let $\varepsilon_1, \dots, \varepsilon_m \in \{\pm 1\}$ be such that

$$(\pi(c_1 y_1, \dots, c_r y_r), \varepsilon_1, \dots, \varepsilon_m) \in \Gamma^{*}\,;$$

by [11], Satz 6, there is some $a \in R^{\bullet}$ satisfying

$$a \equiv c_i y_i \bmod \mathfrak{p}_i^{e_i + v_{\mathfrak{p}_i}(c_i)} \quad \text{for} \quad 1 \leqq i \leqq r,$$

$$v_{\mathfrak{p}}(a) \geqq e_{\mathfrak{p}} \quad \text{for all} \quad \mathfrak{p} \in P \quad \text{and}$$

$$\sigma_j(a) = \varepsilon_j \quad \text{for} \quad 1 \leqq j \leqq m.$$

Since $a + \mathfrak{f} = \pi(a, \ldots, a) = \pi(c_1 y_1, \ldots, c_r y_r)$, we infer $a \in H$. Moreover,

$$a \equiv c_i y_i \bmod \mathfrak{p}_i^{e_i + v_{\mathfrak{p}_i}(c_i)}$$

implies $a \in c_i y_i (1 + \mathfrak{p}_i^{e_i} R_{\mathfrak{p}_i})$, and hence

$$\Delta(a) = (a, \ldots, a) U^\times = (c_1 y_1, \ldots, c_r y_r) U^\times = (a_1, \ldots, a_r) U^\times.$$

If $c = \prod_{\mathfrak{p} \in P} \mathfrak{p}^{v_{\mathfrak{p}}(a) - e_{\mathfrak{p}}} \in \mathscr{F}(P)$, then $\mathfrak{a} c = \partial(a) \in \partial H$.

(iii) Let $g = [\mathfrak{a}] \in G$ be given, where $\mathfrak{a} \in \mathscr{F}(P) \times T$. By (ii), there exists some $c \in \mathscr{F}(P)$ such that $\mathfrak{a} c \in \partial H$, whence $[c] + g = 0$ and $c \in (-g) \cap \mathscr{F}(P)$.

(iv) If $t \in T$, then (ii) implies the existence of some $c \in \mathscr{F}(P)$ and $a \in H$ such that $tc = \partial(a)$, whence $t = \Delta(a)$.

(v) is obvious by (i), (ii) and (iii). □

Corollary 1. *Let H be a congruence monoid and $\partial : H \to \mathscr{F}(P) \times T$ the canonical divisor homomorphism as above. Then*

$$H_{\mathfrak{f}} = \{a \in H \mid aR + \mathfrak{f} = R\}$$

is a submonoid of H,

$$H_{\mathfrak{f}} = \{a \in R^\bullet \mid (a + \mathfrak{f}, \sigma_1(a), \ldots, \sigma_m(a)) \in \Gamma^* \cap ((R/\mathfrak{f})^\times \times \{\pm 1\}^m)\} = \partial^{-1}(\mathscr{F}(P)),$$

$\partial | H_{\mathfrak{f}} : H_{\mathfrak{f}} \to \mathscr{F}(P)$ is a divisor homomorphism, and there is a natural isomorphism

$$\mathscr{F}(P) / \partial H_{\mathfrak{f}} \xrightarrow{\sim} (\mathscr{F}(P) \times T) / \partial H.$$

Proof. Since $\partial H \cap \mathscr{F}(P) = \partial H_{\mathfrak{f}}$, the assertion follows from Proposition 1 and Lemma 1. □

Remark. In Corollary 1, $H_{\mathfrak{f}}$ is a generalized Hilbert semigroup in the sense of [11]; if $\Gamma \subset (R/\mathfrak{f})^\times$, then $H = H_{\mathfrak{f}}$. If R is a holomorphy ring in some global field, then $H_{\mathfrak{f}} / H_{\mathfrak{f}}^\times$ is a generalized Hilbert semigroup in the sense of [13].

Examples. 1. The most important examples (in fact the impulse for that theory) arise from orders in global fields and will be discussed in detail later on; cf. Definition 5 and Proposition 4.

2. Suppose that $R = \mathbb{Z}$, $\mathfrak{f} = f\mathbb{Z}$, where $f \in \mathbb{N}$, $f \geqq 2$, and $\mathfrak{f}^* = \mathfrak{f}\infty$, where $\infty = (\mathbb{Z} \hookrightarrow \mathbb{R})$. If $\Gamma \subset \mathbb{Z}/f\mathbb{Z}$ is multiplicatively closed, $1 + f\mathbb{Z} \in \Gamma$ and $\Gamma^* = \Gamma \times \{1\} \subset \mathbb{Z}/f\mathbb{Z} \times \{\pm 1\}$, then

$$H = \{a \in \mathbb{N} \mid a + f\mathbb{Z} \in \Gamma\}\,.$$

We identify $\mathscr{P}(\mathbb{Z})$ with the set $\mathbb{P}$ of all prime numbers; then we obtain

$$P = \{p \in \mathbb{P} \mid p \nmid f\}, \quad \mathscr{F}(P) = \mathbb{N}^{(f)} = \{a \in \mathbb{N} \mid (a, f) = 1\}$$

and $H_{f\mathbb{Z}} = \{a \in H \mid (a, f) = 1\}$. If $\partial : H \to \mathbb{N}^{(f)} \times T$ is the canonical divisor homomorphism associated with H, then $\partial \mid H_{f\mathbb{Z}} = (H_{f\mathbb{Z}} \hookrightarrow \mathbb{N}^{(f)})$; it is well known that this is a divisor theory with class group

$$G \simeq (\mathbb{Z}/f\mathbb{Z})^\times / (\Gamma \cap (\mathbb{Z}/f\mathbb{Z})^\times)$$

cf. [10], Beispiel 2. By Corollary 1, G is also the class group of the order formation $[\mathbb{N}^{(f)}, T, H]$.

As a simple example, let us discuss the case

$$f = 3, \quad \Gamma = \{3\mathbb{Z}, 1 + 3\mathbb{Z}\} \subset \mathbb{Z}/3\mathbb{Z}, \quad H = \{a \in \mathbb{N} \mid a \not\equiv -1 \bmod 3\}.$$

We have $U = \{a \in \mathbb{Z}_{(3)} \mid a \not\equiv -1 \bmod 3\mathbb{Z}_{(3)}\}$, and

$$\{\pm 3^n \mid n \in \mathbb{N}\} \cup \{1\} \subset U$$

is a set of representatives for $U/U^\times$. Since this is multiplicatively closed, we may identify T with this set of representatives and obtain $T = [3, -3]$ (the multiplicative submonoid of $\mathbb{Z}$ generated by 3 and -3). The divisor homomorphism $\partial : H \to \mathbb{N}^{(3)} \times T$ is given by

$$\partial(3^n b) = \begin{cases} b, & \text{if } n = 0, \\ b \cdot 3^n, & \text{if } n > 0,\ b \equiv 1 \bmod 3, \\ b \cdot (-3^n), & \text{if } n > 0,\ b \equiv -1 \bmod 3 \end{cases}$$

(where $n \in \mathbb{N}_0$ and $b \in \mathbb{N}^{(3)}$). The class group G satisfies

$$G \simeq (\mathbb{Z}/3\mathbb{Z})^\times / (\Gamma \cap (\mathbb{Z}/3\mathbb{Z})^\times) = (\mathbb{Z}/3\mathbb{Z})^\times\,,$$

hence $\# G = 2$, and if we identify G with $\mathbb{Z}/2\mathbb{Z}$, then the canonical epimorphism

$$[\cdot] : \mathscr{F}(P) \times T = \mathbb{N}^{(3)} \times [-3, 3] \to G = \mathbb{Z}/2\mathbb{Z}$$

is given by

$$[(\prod_{3 \nmid p \in \mathbb{P}} p^{e_p})((-1)^e 3^n)] = e + \sum_{\substack{p \in \mathbb{P} \\ p \equiv -1 \bmod 3}} e_p + 2\mathbb{Z}$$

(where $e_p \in \mathbb{N}_0$, $e_p = 0$ for almost all $p \in \mathbb{P}$, $n \in \mathbb{N}$ and $e \in \{\pm 1\}$).

Now we continue our general investigations and suppose that R is a Dedekind domain satisfying $(R:\mathfrak{p}) < \infty$ for all $\mathfrak{p} \in \mathscr{P}(R)$. Then we have $(R:I) < \infty$ for all $I \in \mathscr{I}(R)$, and $(R:IJ) = (R:I)(R:J)$ for all $I, J \in \mathscr{I}(R)$, cf. [22], Ch. 1, § 1. Moreover, if $\mathfrak{p} \in \mathscr{P}(R)$ and $a \in R_\mathfrak{p}$, then $(R_\mathfrak{p} : aR_\mathfrak{p}) = (R:\mathfrak{p})^{v_\mathfrak{p}(a)} < \infty$. Let $H \subset R^\bullet$ be a congruence monoid and $\partial : H \to \mathscr{F}(P) \times T$ the canonical divisor homomorphism as before. We define a size function (called canonical in the sequel)

$$|\cdot| : \mathscr{F}(P) \times T \to \mathbb{N}$$

by

$$|(\prod_{\mathfrak{p}\in P} \mathfrak{p}^{a_\mathfrak{p}})((a_1, \dots, a_r)U^\times)| = \prod_{\mathfrak{p}\in P} (R:\mathfrak{p})^{a_\mathfrak{p}} \cdot \prod_{i=1}^{r} (R_{\mathfrak{p}_i} : a_i R_{\mathfrak{p}_i})$$

(since $U^\times \subset \prod_{i=1}^{r} R_{\mathfrak{p}_i}^\times$, this definition does not depend on the representative $(a_1, \dots, a_r)$ of $(a_1, \dots, a_r)\, U^\times \in T$).

Proposition 2. *Let R be a Dedekind domain satisfying $(R:\mathfrak{p}) < \infty$ for all $\mathfrak{p} \in \mathscr{P}(R)$. Let $H \subset R^\bullet$ be a congruence monoid and $\partial : H \to \mathscr{F}(P) \times T$ the canonical divisor homomorphism as above. Then the size function $|\cdot| : \mathscr{F}(P) \times T \to \mathbb{N}$ has the following properties*:

(i) *$|\cdot| : \mathscr{F}(P) \times T \to \mathbb{N}$ is a norm.*

(ii) *For $I \in \mathscr{I}_\mathfrak{f}(R) = \mathscr{F}(P)$, we have $|I| = (R:I)$.*

(iii) *For $a \in H$, we have $|\partial(a)| = (R:aR)$.*

(iv) *$[T, |\cdot|]$ is a small arithmetical monoid of rank r.*

Proof. (i) and (ii) are obvious.

(iii) For $a \in H$, we have

$$|\partial(a)| = \left|(\prod_{\mathfrak{p}\in P} \mathfrak{p}^{v_\mathfrak{p}(a)})((a, \dots, a)U^\times)\right| = \prod_{\mathfrak{p}\in P} (R:\mathfrak{p})^{v_\mathfrak{p}(a)} \cdot \prod_{i=1}^{r} (R_{\mathfrak{p}_i} : aR_{\mathfrak{p}_i})$$
$$= \prod_{\mathfrak{p}\in\mathscr{P}(R)} (R:\mathfrak{p})^{v_\mathfrak{p}(a)} = (R:aR).$$

(iv) For $1 \leqq i \leqq r$, the group $R_{\mathfrak{p}_i}^\times/(1 + \mathfrak{p}_i^{e_i} R_{\mathfrak{p}_i})$ is finite, since $R_{\mathfrak{p}_i}/\mathfrak{p}_i^{e_i} R_{\mathfrak{p}_i} \simeq R/\mathfrak{p}_i^{e_i}$ is (cf. [23], Kap. II, 3.10). Let $\alpha_{i,1}, \dots, \alpha_{i,N_i} \in R_{\mathfrak{p}_i}^\times$ be a set of representatives of

$$R_{\mathfrak{p}_i}^\times/(1 + \mathfrak{p}_i^{e_i} R_{\mathfrak{p}_i}),$$

and let $\pi_i \in R_{\mathfrak{p}_i}$ be a prime element. Since

$$\prod_{i=1}^{r} (1 + \mathfrak{p}_i^{e_i} R_{\mathfrak{p}_i}) \subset U^\times \subset U \subset \prod_{i=1}^{r} R_{\mathfrak{p}_i}^\bullet,$$

every $t \in T$ is of the form

$$t = (\pi_1^{n_1}\alpha_{1,\nu_1}, \ldots, \pi_r^{n_r}\alpha_{r,\nu_r})\, U^\times$$

(where $n_1, \ldots, n_r \in \mathbb{N}_0$ and $1 \leqq \nu_i \leqq N_i$), which implies

$$|t| = \prod_{i=1}^{r} (R_{\mathfrak{p}_i} : \pi_i^{n_i} R_{\mathfrak{p}_i}) = \prod_{i=1}^{r} (R : \mathfrak{p}_i)^{n_i}\,.$$

If $|t| \leqq x$, then $n_i \leqq [\log(R : \mathfrak{p}_i)]^{-1} \log x$, and consequently

$$\# \{t \in T \,|\, |t| \leqq x\} \leqq \left(\prod_{i=1}^{r} \frac{N_i}{\log(R : \mathfrak{p}_i)} \right) (\log x)^r\,. \quad \square$$

A *global field* K is either an algebraic number field or an algebraic function field in one variable over a finite field. Let $\mathscr{S}(K)$ be the set of all non-archimedian places of K. For $v \in \mathscr{S}(K)$, let R_v be the valuation ring, $\mathfrak{P}_v$ the valuation ideal and $|v| = (R_v : \mathfrak{P}_v)$ the cardinality of the residue field of v. Let $S \subset \mathscr{S}(K)$ be a finite set, $S \neq \emptyset$ in the function field case, and set

$$R_S = \bigcap_{v \in \mathscr{S}(K) \backslash S} R_v \subset K\,;$$

R_S is called the *holomorphy ring* of K associated with S. It is a Dedekind domain with quotient field K, $\mathscr{P}(R_S) = \{\mathfrak{P}_v \cap R_S \,|\, v \in \mathscr{S}(K) \backslash S\}$, and for every $v \in \mathscr{S}(K) \backslash S$ we have

$$(R_S : \mathfrak{P}_v \cap R_S) = |v| < \infty\,.$$

(For the function field case cf. [2], Ch. 2.7 or [25], Ch. 3.2; in the number field case $R_\emptyset$ is just the ring of algebraic integers in K and R_S is an overring of $R_\emptyset$, cf. also [26], Ch. 4.)

Proposition 3. *Let R be a holomorphy ring in a global field, $H \subset R^\bullet$ a congruence monoid and $\partial : H \to \mathscr{F}(P) \times T$ the canonical divisor homomorphism. Then $[\mathscr{F}(P), T, \partial H, |\cdot|]$ is an arithmetical order formation.*

Proof. By Proposition 1, $[\mathscr{F}(P), T, \partial H]$ is an order formation. By definition, $\partial H \cap \mathscr{F}(P)$ is a generalized Hilbert semigroup in R in the sense of [13], and therefore $[\mathscr{F}(P), \partial H \cap \mathscr{F}(P), |\cdot|]$ is an arithmetical formation by [13], Proposition 3. Let

$$G = (\mathscr{F}(P) \times T) / \partial H$$

be the class group of $[\mathscr{F}(P), T, \partial H]$. By Corollary 1, we may identify G with

$$\mathscr{F}(P) / (\partial H \cap \mathscr{F}(P))\,.$$

Since $[\mathscr{F}(P), \partial H \cap \mathscr{F}(P), |\cdot|]$ is an arithmetical formation, G is finite and condition 1 of Definition 4 is fulfilled. By Proposition 2, $[T, |\cdot|]$ is a small arithmetical monoid. $\square$

Finally, we are now going to discuss orders in Dedekind domains.

Definition 5. Let R be a Dedekind domain. By an *order* $\mathfrak{o}$ *in* R we mean a subring $\mathfrak{o} \subset R$ such that $R/\mathfrak{o}$ is a finitely generated torsion $\mathfrak{o}$-module. The ideal $\mathfrak{f} = \operatorname{Ann}_{\mathfrak{o}}(R/\mathfrak{o})$ is called the *conductor* of $\mathfrak{o}$ (clearly, $\mathfrak{f} = \{a \in R \mid aR \subset \mathfrak{o}\}$ is the greatest ideal of R lying in $\mathfrak{o}$).

The above definition is very sparse; the following lemma shows that it coincides with the usual concept.

Lemma 2. *Let* $\mathfrak{o} \subset R$ *be integral domains. Then the following two assertions are equivalent*:

(a) *R is a Dedekind domain and $\mathfrak{o}$ is an order in R.*

(b) *$\mathfrak{o}$ is a one-dimensional noetherian domain, R is the integral closure of $\mathfrak{o}$ (in some quotient field of $\mathfrak{o}$), and R is a finitely generated $\mathfrak{o}$-module.*

Proof. (a) $\Rightarrow$ (b) Since $R/\mathfrak{o}$ is a torsion $\mathfrak{o}$-module, the quotient fields of R and $\mathfrak{o}$ coincide, and since $R/\mathfrak{o}$ is a finitely generated $\mathfrak{o}$-module, the same is true for R. Therefore $\mathfrak{o}$ is noetherian by the Eakin-Nagata theorem, R is the integral closure of $\mathfrak{o}$, and in particular we have $\dim(\mathfrak{o}) = \dim(R) = 1$.

(b) $\Rightarrow$ (a) R is a Dedekind domain by the Krull-Akizuki theorem, and obviously $R/\mathfrak{o}$ is a finitely generated torsion $\mathfrak{o}$-module. □

Lemma 3. *Let R be a Dedekind domain and $\mathfrak{o} \subset R$ an order with conductor $\mathfrak{f}$.*

(i) *Let $\mathcal{I}_{\mathfrak{f}}(\mathfrak{o}) = \{I \in \mathcal{I}(\mathfrak{o}) \mid I + \mathfrak{f} = \mathfrak{o}\}$, $\mathcal{P}_{\mathfrak{f}}(\mathfrak{o}) = \{\mathfrak{q} \in \mathcal{P}(\mathfrak{o}) \mid \mathfrak{q} + \mathfrak{f} = \mathfrak{o}\}$ and $\mathcal{T}(\mathfrak{o}) \subset \mathcal{I}(\mathfrak{o})$ the submonoid generated by the multiplicative irreducible elements $\mathfrak{q} \in \mathcal{I}(\mathfrak{o})$ with*

$$\sqrt{\mathfrak{q}} \in \mathcal{P}(\mathfrak{o}) \setminus \mathcal{P}_{\mathfrak{f}}(\mathfrak{o}) .$$

Then $\mathcal{I}(\mathfrak{o}) = \mathcal{I}_{\mathfrak{f}}(\mathfrak{o}) \times \mathcal{T}(\mathfrak{o})$ and $\mathcal{I}_{\mathfrak{f}}(\mathfrak{o}) = \mathcal{F}(\mathcal{P}_{\mathfrak{f}}(\mathfrak{o}))$.

(ii) *If $(R : \mathfrak{p}) < \infty$ for all $\mathfrak{p} \in \mathcal{P}(R)$, then we have, for all $J \in \mathcal{I}(\mathfrak{o})$,*

$$(R : JR) = (\mathfrak{o} : J) .$$

Proof. (i) Since $\mathfrak{o}$ is a one-dimensional noetherian domain, the monoid $\mathcal{I}(\mathfrak{o})$ is generated by its irreducible elements, and every irreducible element $\mathfrak{q} \in \mathcal{I}(\mathfrak{o})$ is a primary ideal. The set of prime elements of $\mathcal{I}(\mathfrak{o})$ is just $\mathcal{P}(\mathfrak{o}) \cap \mathcal{I}(\mathfrak{o})$ and from [23], Kap. I, 12.10 and Aufgabe 5, it follows that $\mathcal{P}(\mathfrak{o}) \cap \mathcal{I}(\mathfrak{o}) = \mathcal{P}_{\mathfrak{f}}(\mathfrak{o})$. Obviously, $\mathcal{I}_{\mathfrak{f}}(\mathfrak{o})$ is generated by $\mathcal{P}_{\mathfrak{f}}(\mathfrak{o})$ and hence $\mathcal{I}_{\mathfrak{f}}(\mathfrak{o}) = \mathcal{F}(\mathcal{P}_{\mathfrak{f}}(\mathfrak{o}))$. Finally we infer $\mathcal{I}(\mathfrak{o}) = \mathcal{I}_{\mathfrak{f}}(\mathfrak{o}) \times \mathcal{T}(\mathfrak{o})$.

(ii) Suppose first that $J = a\mathfrak{o}$ for some $a \in \mathfrak{o}$. Then $JR = aR$, and multiplication with a induces an isomorphism $R/\mathfrak{o} \xrightarrow{\sim} aR/a\mathfrak{o}$. Let $\mathfrak{f}$ be the conductor of $\mathfrak{o}$; since $\mathfrak{f} \subset \mathfrak{o} \subset R$ and $(R : \mathfrak{f}) < \infty$, we infer $(R : \mathfrak{o}) < \infty$ and therefore

$$(R : aR)(aR : a\mathfrak{o}) = (R : a\mathfrak{o}) = (R : \mathfrak{o})(\mathfrak{o} : a\mathfrak{o}) ,$$

which implies $(\mathfrak{o} : a\mathfrak{o}) = (R : aR)$.

Now we turn to the general case. By [23], Kap. I, (12.3), we have

$$\mathfrak{o}/J \simeq \coprod_{\mathfrak{q}\in\mathscr{P}(\mathfrak{o})} \mathfrak{o}_{\mathfrak{q}}/J\mathfrak{o}_{\mathfrak{q}},$$

and consequently

$$R/JR \simeq \mathfrak{o}/J \underset{\mathfrak{o}}{\otimes} R \simeq \coprod_{\mathfrak{q}\in\mathscr{P}(\mathfrak{o})} \mathfrak{o}_{\mathfrak{q}}/J\mathfrak{o}_{\mathfrak{q}} \underset{\mathfrak{o}}{\otimes} R.$$

For $\mathfrak{q}\in\mathscr{P}(\mathfrak{o})$, $\mathfrak{o}_{\mathfrak{q}}$ is an order in $R_{\mathfrak{q}}$, and $J\mathfrak{o}_{\mathfrak{q}} = a_{\mathfrak{q}}\mathfrak{o}_{\mathfrak{q}}$ for some $a_{\mathfrak{q}}\in J$, which implies

$$\mathfrak{o}_{\mathfrak{q}}/J\mathfrak{o}_{\mathfrak{q}} \underset{\mathfrak{o}}{\otimes} R \simeq R_{\mathfrak{q}}/a_{\mathfrak{q}}R_{\mathfrak{q}},$$

and consequently

$$(R:JR) = \prod_{\mathfrak{q}\in\mathscr{P}(\mathfrak{o})} (R_{\mathfrak{q}}:a_{\mathfrak{q}}R_{\mathfrak{q}}) = \prod_{\mathfrak{q}\in\mathscr{P}(\mathfrak{o})} (\mathfrak{o}_{\mathfrak{q}}:a_{\mathfrak{q}}\mathfrak{o}_{\mathfrak{q}}) = (\mathfrak{o}:J). \quad \square$$

Remark. In general $\mathfrak{o}/J$ is not isomorphic to R/JR as can be seen from the following example: consider $\mathfrak{o} = \mathbb{Z}[\sqrt{-3}]$, $R = \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$ and $J = (1+\sqrt{-3})\mathfrak{o}$; then $JR = 2R$, $R/JR \simeq \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ but $\mathfrak{o}/J \simeq \mathbb{Z}/4\mathbb{Z}$ since $2\notin J$.

Proposition 4. *Let R be a Dedekind domain and $\mathfrak{o}\subset R$ an order with conductor $\mathfrak{f}$.*

(i) *$\mathfrak{o}^\bullet$ is the congruence monoid of R modulo $\mathfrak{f}$ defined by $\mathfrak{o}/\mathfrak{f}\subset R/\mathfrak{f}$.*

(ii) *Let $\mathscr{I}(\mathfrak{o})$ be the monoid of integral invertible ideals of $\mathfrak{o}$, and let $\partial:\mathfrak{o}^\bullet\to\mathscr{F}(P)\times T$ be the canonical divisor homomorphism. Then there exists a (natural) isomorphism*

$$\varphi:\mathscr{I}(\mathfrak{o}) \xrightarrow{\sim} \mathscr{F}(P)\times T$$

such that $\varphi(a\mathfrak{o}) = \partial(a)$ for all $a\in\mathfrak{o}^\bullet$ and $\varphi(J) = JR$ for all $J\in\mathscr{I}_{\mathfrak{f}}(\mathfrak{o})$. Moreover, φ induces an isomorphism $\varphi^*:\mathrm{Pic}(\mathfrak{o})\simeq G$ between the Picard group of $\mathfrak{o}$ and the class group $G = (\mathscr{F}(P)\times T)/\partial\mathfrak{o}^\bullet$.

(iii) *Suppose that $(R:\mathfrak{p})<\infty$ for all $\mathfrak{p}\in\mathscr{P}(R)$; then we have*

$$|\varphi(J)| = (\mathfrak{o}:J) = (R:JR)$$

for all $J\in\mathscr{I}(\mathfrak{o})$.

Proof. (i) is obvious.

(ii) We set $\mathfrak{f} = \mathfrak{p}_1^{e_1}\dots\mathfrak{p}_r^{e_r}$ and use all notations introduced at the beginning of § 3 and in Lemma 3. We set $\{\mathfrak{p}_1\cap\mathfrak{o},\dots,\mathfrak{p}_r\cap\mathfrak{o}\} = \{\mathfrak{q}_1,\dots,\mathfrak{q}_s\}$ and obtain

$$\mathscr{P}_{\mathfrak{f}}(\mathfrak{o}) = \{\mathfrak{p}\cap\mathfrak{o}\mid\mathfrak{p}\in P\} = \mathscr{P}(\mathfrak{o})\backslash\{\mathfrak{q}_1,\dots,\mathfrak{q}_s\}.$$

For $\mathfrak{q} \in \mathscr{P}_{\mathfrak{f}}(\mathfrak{o})$ there is exactly one $\mathfrak{p} \in \mathscr{P}(R)$ satisfying $\mathfrak{p} \cap \mathfrak{o} = \mathfrak{q}$; it satisfies $\mathfrak{p} \in P$ and $R_{\mathfrak{p}} = \mathfrak{o}_{\mathfrak{q}}$.

We are going to establish the following commutative diagram with all mappings being isomorphisms:

$$\begin{tikzcd}
\mathscr{I}(\mathfrak{o}) = \mathscr{I}_{\mathfrak{f}}(\mathfrak{o}) \times \mathscr{T}(\mathfrak{o}) \arrow[r, "\varphi = \varphi_1 \times \varphi_2"] \arrow[d, "\varrho = \varrho_1 \times \varrho_2"] & \mathscr{F}(P) \times T \\
\coprod\limits_{\mathfrak{q} \in \mathscr{P}(\mathfrak{o})} \mathfrak{o}_{\mathfrak{q}}^{\bullet}/\mathfrak{o}_{\mathfrak{q}}^{\times} = \coprod\limits_{\mathfrak{q} \in \mathscr{P}_{\mathfrak{f}}(\mathfrak{o})} \mathfrak{o}_{\mathfrak{q}}^{\bullet}/\mathfrak{o}_{\mathfrak{q}}^{\times} \times \prod\limits_{j=1}^{s} \mathfrak{o}_{\mathfrak{q}_j}^{\bullet}/\mathfrak{o}_{\mathfrak{q}_j}^{\times} \arrow[r, phantom, "="] & \coprod\limits_{\mathfrak{p} \in P} R_{\mathfrak{p}}^{\bullet}/R_{\mathfrak{p}}^{\times} \times \prod\limits_{j=1}^{s} \mathfrak{o}_{\mathfrak{q}_j}^{\bullet}/\mathfrak{o}_{\mathfrak{q}_j}^{\times} . \arrow[u, "\sigma \times \psi"]
\end{tikzcd}$$

For $J \in \mathscr{I}(\mathfrak{o})$, with $J\mathfrak{o}_{\mathfrak{q}} = a_{\mathfrak{q}}\mathfrak{o}_{\mathfrak{q}}$ for $\mathfrak{q} \in \mathscr{P}(\mathfrak{o})$, we set $\varrho(J) = (a_{\mathfrak{q}}\mathfrak{o}_{\mathfrak{q}}^{\times})_{\mathfrak{q} \in \mathscr{P}(\mathfrak{o})}$. Then ϱ is an isomorphism by [23], Kap. I, 12.6, and obviously $\varrho_1(\mathscr{I}_{\mathfrak{f}}(\mathfrak{o})) = \coprod\limits_{\mathfrak{q} \in \mathscr{P}_{\mathfrak{f}}(\mathfrak{o})} \mathfrak{o}_{\mathfrak{q}}^{\bullet}/\mathfrak{o}_{\mathfrak{q}}^{\times}$ where $\varrho_1 = \varrho \,|\, \mathscr{I}_{\mathfrak{f}}(\mathfrak{o})$.

Clearly $\sigma : \coprod\limits_{\mathfrak{p} \in P} R_{\mathfrak{p}}^{\bullet}/R_{\mathfrak{p}}^{\times} \to \mathscr{F}(P)$, given by $\sigma((a_{\mathfrak{p}}R_{\mathfrak{p}}^{\times})_{\mathfrak{p} \in P}) = \prod\limits_{\mathfrak{p} \in P} \mathfrak{p}^{v_{\mathfrak{p}}(a_{\mathfrak{p}})}$, is an isomorphism. If we define $\varphi_1 : \mathscr{I}_{\mathfrak{f}}(\mathfrak{o}) \to \mathscr{F}(P)$ by $\varphi_1 = \sigma \circ \varrho_1$, then φ_1 is an isomorphism and

$$\varphi_1(J) = \prod_{\mathfrak{p} \in P} \mathfrak{p}^{v_{\mathfrak{p}}(a_{\mathfrak{p} \cap \mathfrak{o}})} = JR$$

for $J \in \mathscr{I}_{\mathfrak{f}}(\mathfrak{o})$ with $J\mathfrak{o}_{\mathfrak{q}} = a_{\mathfrak{q}}\mathfrak{o}_{\mathfrak{q}}$ for $\mathfrak{q} \in \mathscr{P}_{\mathfrak{f}}(\mathfrak{o})$.

It remains to construct an isomorphism

$$\psi : \prod_{j=1}^{s} \mathfrak{o}_{\mathfrak{q}_j}^{\bullet}/\mathfrak{o}_{\mathfrak{q}_j}^{\times} \to T$$

satisfying

$$\psi(a\mathfrak{o}_{\mathfrak{q}_1}^{\times}, \ldots, a\mathfrak{o}_{\mathfrak{q}_s}^{\times}) = \Delta(a)$$

for all $a \in \mathfrak{o}^{\bullet}$. Then in particular $\varphi(a\mathfrak{o}) = \partial(a)$ and φ induces an isomorphism

$$\varphi^* : \mathrm{Pic}(\mathfrak{o}) \to G$$

sending the ideal class $[J] \in \mathrm{Pic}(\mathfrak{o})$ of some $J \in \mathscr{I}(\mathfrak{o})$ onto the class $[\varphi(J)] \in G$.

Remember that $T = U/U^{\times}$ and $U = \pi^{-1}(\mathfrak{o}/\mathfrak{f})$, where

$$\pi : \prod_{i=1}^{r} R_{\mathfrak{p}_i}^{\bullet} \to \prod_{i=1}^{r} R_{\mathfrak{p}_i}/\mathfrak{p}_i^{e_i}R_{\mathfrak{p}_i} \xrightarrow{\sim} \prod_{i=1}^{r} R/\mathfrak{p}_i^{e_i} \xrightarrow{\sim} R/\mathfrak{f} .$$

Let

$$\psi_0 : \prod_{j=1}^{s} \mathfrak{o}_{\mathfrak{q}_j}^{\bullet} \to \prod_{i=1}^{r} R_{\mathfrak{p}_i}^{\bullet}$$

be defined by $\psi_0(b_1, \ldots, b_s) = (a_1, \ldots, a_r)$, where $a_i = b_j$ if $\mathfrak{p}_i \cap \mathfrak{o} = \mathfrak{q}_j$. We assert that $\mathrm{Im}(\psi_0) \subset U$. Indeed, let $(a_1, \ldots, a_r) \in \mathrm{Im}(\psi_0)$ be given, $a_i = u_i^{-1} c_i$, where $c_i \in \mathfrak{o}^\bullet$, $u_i \in \mathfrak{o} \backslash \mathfrak{p}_i$ and $(c_i, u_i) = (c_\nu, u_\nu)$ if $\mathfrak{p}_i \cap \mathfrak{o} = \mathfrak{p}_\nu \cap \mathfrak{o}$. From $u_i \mathfrak{o} + (\mathfrak{p}_i \cap \mathfrak{o}) = \mathfrak{o}$ we infer

$$u_i \mathfrak{o} + (\mathfrak{p}_i^{e_i} \cap \mathfrak{o}) = \mathfrak{o}\,,$$

and therefore there exist $y_i \in \mathfrak{o}$ such that $u_i y_i \equiv 1 \bmod \mathfrak{p}_i^{e_i}$; again, we may assume that $y_i = y_\nu$ if $\mathfrak{p}_i \cap \mathfrak{o} = \mathfrak{p}_\nu \cap \mathfrak{o}$. If $\mathfrak{p}_i \cap \mathfrak{o} \neq \mathfrak{p}_\nu \cap \mathfrak{o}$, then $(\mathfrak{p}_i \cap \mathfrak{o}) + (\mathfrak{p}_\nu \cap \mathfrak{o}) = \mathfrak{o}$, hence

$$(\mathfrak{p}_i^{e_i} \cap \mathfrak{o}) + (\mathfrak{p}_\nu^{e_\nu} \cap \mathfrak{o}) = \mathfrak{o}\,,$$

and therefore the Chinese remainder theorem implies the existence of some $a \in \mathfrak{o}$ satisfying $a \equiv c_i y_i \bmod \mathfrak{p}_i^{e_i}$ for all $1 \leqq i \leqq r$. Consequently we obtain

$$\pi(a_1, \ldots, a_r) = \pi(c_1 y_1, \ldots, c_r y_r) = \pi(a, \ldots, a) \in \mathfrak{o}/\mathfrak{f}$$

and hence $(a_1, \ldots, a_r) \in U$ as asserted.

Now $\psi_0 : \prod_{j=1}^{s} \mathfrak{o}_{\mathfrak{q}_j}^\bullet \to U$ induces an injective monoid homomorphism

$$\psi : \prod_{j=1}^{s} \mathfrak{o}_{\mathfrak{q}_j}^\bullet / \mathfrak{o}_{\mathfrak{q}_j}^\times \to U/(U \cap \prod_{i=1}^{r} R_{\mathfrak{p}_i}^\times) = U/U^\times = T\,,$$

given by $\psi(b_1 \mathfrak{o}_{\mathfrak{q}_1}^\times, \ldots, b_s \mathfrak{o}_{\mathfrak{q}_s}^\times) = (a_1, \ldots, a_r) U^\times$, where $a_i = b_j$ if $\mathfrak{p}_i \cap \mathfrak{o} = \mathfrak{q}_j$; in particular, we have $\psi(a\mathfrak{o}_{\mathfrak{q}_1}^\times, \ldots, a\mathfrak{o}_{\mathfrak{q}_s}^\times) = \Delta(a)$ for all $a \in \mathfrak{o}^\bullet$. Since $\Delta(\mathfrak{o}^\bullet) = T$ by Proposition 1, ψ is an isomorphism.

(iii) From (ii) and Proposition 2 it follows that $|\varphi(J)| = (R : JR)$ for all $J \in \mathscr{I}_\mathfrak{f}(\mathfrak{o})$ and all $J = a\mathfrak{o}$ with $a \in \mathfrak{o}$. If $J \in \mathscr{I}(\mathfrak{o})$ is arbitrary, then by Proposition 1 there is an $I \in \mathscr{I}_\mathfrak{f}(\mathfrak{o})$ such that $\varphi(J)\varphi(I) = \partial(a)$ for some $a \in \mathfrak{o}^\bullet$, and hence we infer

$$|\varphi(J)| = |\varphi(I)|^{-1} |\partial(a)| = (R : IR)^{-1} (R : aR) = (R : JR)\,;$$

the equality $(\mathfrak{o} : J) = (R : JR)$ follows from Lemma 3. □

§ 4. Counting elements in arithmetical order formations

This paragraph contains our main result concerning analytic number theory in order formations. We start with two preliminary lemmata. Then we prove a general counting result (Proposition 5) which reduces the task of counting certain elements in an arithmetical order formation $[\mathscr{F}(P), T, H, |\cdot|]$ to that in the arithmetical formation

$$[\mathscr{F}(P), \mathscr{F}(P) \cap H, |\cdot|]\,.$$

Lemma 4. *Let $[T, |\cdot|]$ be a small arithmetical monoid of rank $r \in \mathbb{N}$ and $\varepsilon > 0$. Then we have, for all $y \geqq 2$ and $u \geqq 0$,*

$$\sum_{\substack{t \in T \\ |t| > y}} (u + |t|)^{-\varepsilon} \ll (u + y)^{-\varepsilon} (\log y)^r .$$

Proof. Putting $A(x) = \# \{t \in T \,|\, |t| \leqq x\}$, we obtain for any $z > y$

$$\sum_{\substack{t \in T \\ y < |t| \leqq z}} (u + |t|)^{-\varepsilon} = \int_y^z (u + \xi)^{-\varepsilon} dA(\xi)$$

$$= \frac{A(z)}{(u+z)^{\varepsilon}} - \frac{A(y)}{(u+y)^{\varepsilon}} + \varepsilon \int_y^z \frac{A(\xi)}{(u+\xi)^{\varepsilon+1}} d\xi .$$

Observing $A(x) \ll (\log x)^r$, the assertion follows as z tends to infinity. □

Lemma 5. *Let T be a non-empty set, $\gamma \in (0, 1]$, $d \in \mathbb{N}_0$, and for $0 \leqq \nu \leqq d+1$ let $c_\nu : T \to \mathbb{C}$ be complex functions. Suppose that*

$$C(t, x) = \sum_{\nu=0}^{d} c_\nu(t) x^\nu + c_{d+1}(t) e^{-\gamma/x} \frac{1}{x}$$

is bounded for $(t, x) \in T \times (0, 1]$. Then the functions c_ν for $0 \leqq \nu \leqq d+1$ are bounded as well.

Proof. Let $x_1, \ldots, x_{d+1} \in (0, 1]$ be pairwise distinct numbers. For $u \in (0, 1]$, we set

$$\varphi(u) = e^{-\gamma/u} \frac{1}{u}$$

and

$$f(u) = \det \begin{pmatrix} 1 & u & u^2 & \cdots & u^d & \varphi(u) \\ 1 & x_1 & x_1^2 & \cdots & x_1^d & \varphi(x_1) \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & x_{d+1} & x_{d+1}^2 & \cdots & x_{d+1}^d & \varphi(x_{d+1}) \end{pmatrix} .$$

Then

$$f^{(d+1)}(u) = (-1)^{d+1} \varphi^{(d+1)}(u) \cdot V(x_1, \ldots, x_{d+1}) ,$$

where

$$V(x_1, \ldots, x_{d+1}) = \det \begin{pmatrix} 1 & x_1 & \cdots & x_1^d \\ \vdots & \vdots & \vdots & \vdots \\ 1 & x_{d+1} & \cdots & x_{d+1}^d \end{pmatrix} \neq 0$$

denotes Vandermonde's determinant. For every $\nu \geqq 0$, $\varphi^{(\nu)}(u) = u^{-\nu-1} \psi_\nu(u) e^{-\gamma/u}$; therefore $\varphi^{(d+1)}$ and hence also $f^{(d+1)}$ has at most $d+1$ zeroes. This means in particular that f is not constant in $(0, 1]$; hence we can find some $x_0 \in (0, 1]$ for which $f(x_0) \neq 0$.

Let us suppose now that $|C(t,x)| \leqq C^*$ for all $(t,x) \in T \times (0,1]$. Then, for

$$0 \leqq j \leqq d+1\,,$$

we have

$$(*) \qquad \sum_{\nu=0}^{d} c_\nu(t)\, x_j^\nu + c_{d+1}(t)\, \varphi(x_j) = \Theta_j(t)\, C^*$$

with certain $\Theta_j : T \to \mathbb{C}$ satisfying $|\Theta_j(t)| \leqq 1$. Since $f(x_0) \neq 0$ we can determine $c_\nu(t)$ from $(*)$ by means of Cramer's rule; finally Hadamard's inequality shows that $c_\nu(t)$ is bounded. □

Proposition 5. *Let $[\mathscr{F}(P), T, H, |\cdot|]$ be an arithmetical order formation of rank r. Let $E \subset \mathscr{F}(P) \times T$ be a subset, and for $t \in T$ set*

$$E_t = \{a \in \mathscr{F}(P) \,|\, at \in E\}\,.$$

Let $C : T \times (0,\infty) \to [0,\infty)$ be a bounded function, $\eta \in \mathbb{R}_{\geqq 0}$ and $d \in \mathbb{N}_0$ such that, for any $t \in T$ and $x \geqq 3$,

$$\#\{a \in E_t \,|\, |a| \leqq x\} = C(t,x)\, x (\log x)^{-\eta} (\log\log x)^d\,.$$

Then we obtain (again for $x \geqq 3$)

$$\#\{c \in E \,|\, |c| \leqq x\} = C^*(x)\, x (\log x)^{-\eta} (\log\log x)^d\,,$$

where

$$C^*(x) = \sum_{t \in T} \frac{1}{|t|}\, C\left(t, \frac{x}{|t|}\right) + O\left(\frac{(\log\log x)^r}{\log x}\right).$$

In particular:

(i) *Suppose that there is some $t \in T$ and $x_0 > 0$ such that $C(t,x) \gg 1$ for $x \geqq x_0$; then we have $C^*(x) \asymp 1$ for all $x \geqq x_0$.*

(ii) *Suppose that for $x \geqq 3$*

$$C(t,x) = \sum_{\nu=0}^{d} c_\nu(t) (\log\log x)^{-\nu} + O\left(\frac{\log\log x}{(\log x)^\gamma}\right)$$

with functions $c_\nu : T \to \mathbb{R}$, $0 \leqq \nu \leqq d$, and $\gamma \in \mathbb{R}$ with $0 < \gamma \leqq 1$; then we have

$$C^*(x) = \sum_{\nu=0}^{d} c_\nu^* (\log\log x)^{-\nu} + O\left(\frac{(\log\log x)^N}{(\log x)^\gamma}\right),$$

where $c_\nu^* = \sum_{t \in T} \dfrac{c_\nu(t)}{|t|}$, $N = 1$ for $\gamma < 1$ and $N = r$ for $\gamma = 1$.

Proof. For $x \geqq 3$ we have

$$\begin{aligned}
\# \{c \in E \,||c| \leqq x\} &= \sum_{t \in T} \# \left\{a \in E_t \,||a| \leqq \frac{x}{|t|}\right\} \\
&= \Big(\sum_{\substack{t \in T \\ |t| \leqq \log x}} + \sum_{\substack{t \in T \\ \log x < |t| \leqq \sqrt{x}}} + \sum_{\substack{t \in T \\ \sqrt{x} < |t| \leqq \frac{x}{3}}} + \sum_{\substack{t \in T \\ \frac{x}{3} < |t| \leqq x}} \Big) \# \left\{a \in E_t \,||a| \leqq \frac{x}{|t|}\right\} \\
&= \sum_{j=1}^{4} S_j, \quad \text{say}.
\end{aligned}$$

We treat the sums S_j separately. If $|t| \leqq \log x$ we have

$$\left(\log \frac{x}{|t|}\right)^{-\eta} = (\log x)^{-\eta} \left(1 + O\left(\frac{\log\log x}{\log x}\right)\right),$$

$$\left(\log\log \frac{x}{|t|}\right)^{d} = (\log\log x)^{d} \left(1 + O\left(\frac{\log\log x}{\log x}\right)\right)$$

and hence

$$\begin{aligned}
S_1 &= \sum_{\substack{t \in T \\ |t| \leqq \log x}} C\left(t, \frac{x}{|t|}\right) \frac{x}{|t|} (\log x)^{-\eta} (\log\log x)^{d} \left(1 + O\left(\frac{\log\log x}{\log x}\right)\right) \\
&= x (\log x)^{-\eta} (\log\log x)^{d} \left(\sum_{\substack{t \in T \\ |t| \leqq \log x}} \frac{1}{|t|} C\left(t, \frac{x}{|t|}\right) + O\left(\frac{\log\log x}{\log x}\right)\right) \\
&= x (\log x)^{-\eta} (\log\log x)^{d} \left(\sum_{t \in T} \frac{1}{|t|} C\left(t, \frac{x}{|t|}\right) + O\left(\frac{(\log\log x)^{r}}{\log x}\right)\right)
\end{aligned}$$

because T is a small arithmetical monoid of rank r and therefore, by Lemma 4,

$$\sum_{\substack{t \in T \\ |t| > \log x}} \frac{1}{|t|} C\left(t, \frac{x}{|t|}\right) \ll \frac{(\log\log x)^{r}}{\log x}.$$

For $\log x < |t| \leqq \sqrt{x}$ we have

$$\left(\log \frac{x}{|t|}\right)^{-\eta} \left(\log\log \frac{x}{|t|}\right)^{d} \ll (\log x)^{-\eta} (\log\log x)^{d}$$

and hence

$$S_2 \ll \sum_{\substack{t \in T \\ \log x < |t| \leqq \sqrt{x}}} C\left(t, \frac{x}{|t|}\right) \frac{x}{|t|} (\log x)^{-\eta} (\log\log x)^{d} \ll x (\log x)^{-\eta-1} (\log\log x)^{d+r}.$$

For $\sqrt{x} < |t| \leqq \frac{x}{3}$ we have

$$\left(\log \frac{x}{|t|}\right)^{-\eta} \left(\log\log \frac{x}{|t|}\right)^{d} \ll 1$$

and thus

$$S_3 \ll x \sum_{\substack{t \in T \\ \sqrt{x} < |t| \leqq \frac{x}{3}}} \frac{1}{|t|} C\left(t, \frac{x}{|t|}\right) \ll \sqrt{x} (\log x)^r .$$

Finally we infer

$$S_4 \ll \Big(\sum_{\substack{t \in T \\ \frac{x}{3} < |t| \leqq x}} 1\Big) \# \{a \in \mathscr{F}(P) \,|\, |a| \leqq 3\} \ll (\log x)^r .$$

Hence

$$\sum_{j=1}^{4} S_j = \left(\sum_{t \in T} \frac{1}{|t|} C\left(t, \frac{x}{|t|}\right) + O\left(\frac{(\log\log x)^r}{\log x}\right)\right) x (\log x)^{-\eta} (\log\log x)^d$$

and the main formula is proved.

Since $C(t, x) \ll 1$ uniformly in t, we obtain $C^*(x) \ll 1$, and (i) follows.

For the proof of (ii), let us write $C(t, x)$ in the form

$$C(t, x) = \sum_{\nu=0}^{d} c_\nu(t) (\log\log x)^{-\nu} + c_{d+1}(t) \frac{\log\log x}{(\log x)^\gamma} .$$

Lemma 5 implies that the functions c_ν, $0 \leqq \nu \leqq d+1$, are bounded. Inserting this expression into the main formula for $C^*(x)$ we obtain

$$\begin{aligned} C^*(x) &= \sum_{t \in T} \frac{1}{|t|} \left(\sum_{\nu=0}^{d} c_\nu(t) (\log\log x)^{-\nu} + c_{d+1}(t) \frac{\log\log x}{(\log x)^\gamma}\right) + O\left(\frac{(\log\log x)^r}{\log x}\right) \\ &= \sum_{\nu=0}^{d} c_\nu^* (\log\log x)^{-\nu} + O\left(\frac{\log\log x}{(\log x)^\gamma} + \frac{(\log\log x)^r}{\log x}\right), \end{aligned}$$

as required. □

§ 5. Factorization properties

We start with some preliminaries concerning factorizations in arbitrary monoids. Then we consider arbitrary order formations, and finally we derive analytical results for arithmetical order formations. A general reference for factorization properties in arbitrary monoids is [14].

A monoid H is called atomic, if every $a \in H \backslash H^\times$ possesses a factorization

$$a = u_1 \cdot \ldots \cdot u_r ,$$

where $r \in \mathbb{N}$ and $u_1, \ldots, u_r \in H$ are irreducible; we call r the length of that factorization, and we denote by $\mathscr{L}(a) \subset \mathbb{N}$ the set of all lengths of factorizations of a. For $a \in H^\times$, we set $\mathscr{L}(a) = \{0\}$. An atomic monoid H is called a BF-monoid (bounded factorization monoid) if $\mathscr{L}(a)$ is finite for all $a \in H$.

Let H be an atomic monoid. Two factorizations $a = u_1 \cdot \ldots \cdot u_r = v_1 \cdot \ldots \cdot v_s$ of an element $a \in H \backslash H^\times$ are said to be not essentially different if $r = s$ and there exists some permutation $\sigma \in \mathfrak{S}_r$ such that u_i and $v_{\sigma(i)}$ are associated for $1 \leqq i \leqq r$. Let $\mathbf{f}(a) \in \mathbb{N} \cup \{\infty\}$ be the number of essentially different factorizations of an element $a \in H \backslash H^\times$; for $a \in H^\times$, set $\mathbf{f}(a) = 1$. For $k \in \mathbb{N}$, we consider the following sets:

$$\mathbf{M}_k(H) = \{a \in H \mid \max \mathscr{L}(a) \leqq k\} ,$$

$$\mathbf{G}_k(H) = \{a \in H \mid \# \mathscr{L}(a) \leqq k\} ,$$

$$\mathbf{F}_k(H) = \{a \in H \mid \mathbf{f}(a) \leqq k\} .$$

If $\pi : H \to H/H^\times$ is the canonical epimorphism of H onto the associated reduced monoid $H/H^\times$, then $a \in H$ and $\pi(a) \in H/H^\times$ have the same factorization properties. Therefore there is no loss of generality if we assume H to be reduced.

We start with an algebraic description of the sets $\mathbf{M}_k(H)$ and $\mathbf{G}_k(H)$ if H belongs to an order formation $[\mathscr{F}(P), T, H]$. The following lemma gives a simple criterion for H to be a BF-monoid and consequently atomic.

Lemma 6. (i) *Let $[\mathscr{F}(P), T, H]$ be an order formation. If T is a* BF*-monoid, then H is also a* BF*-monoid.*

(ii) *Let R be a Dedekind domain, $H \subset R^\bullet$ a congruence monoid and $\partial : H \to \mathscr{F}(P) \times T$ its canonical divisor homomorphism. Then T and H are* BF*-monoids.*

Proof. (i) If T is a BF-monoid, then clearly $\mathscr{F}(P) \times T$ is also a BF-monoid, and the assertion follows from [14], Theorem 3.

(ii) We use the notations introduced at the beginning of § 3. The rings $R_{\mathfrak{p}_i}$ are Dedekind domains; therefore all $R^\bullet_{\mathfrak{p}_i}$ and $\prod_{i=1}^{r} R^\bullet_{\mathfrak{p}_i}$ are BF-monoids. Since $U \subset \prod_{i=1}^{r} R^\bullet_{\mathfrak{p}_i}$ and $U^\times = U \cap \left(\prod_{i=1}^{r} R^\bullet_{\mathfrak{p}_i} \right)^\times$, it follows that U is a BF-monoid by [14], Theorem 3; hence $T = U/U^\times$ is a BF-monoid. Since $[\mathscr{F}(P), T, \partial H]$ is an order formation, ∂H is a BF-monoid by (i), and from $\partial H \simeq H/H^\times$ it follows that H is also a BF-monoid. □

Now let $[\mathscr{F}(P), T, H]$ be an order formation and $G = \mathscr{F}(P) \times T/H$ its class group. We assume that H is atomic, G is finite and $g \cap P \neq \emptyset$ for all $g \in G$ (i.e., every class contains a prime).

For $k \in \mathbb{N}$, we set

$$\mathbf{M}_k(H,t) = \{a \in \mathscr{F}(P) \mid at \in \mathbf{M}_k(H)\}\,,$$
$$\mathbf{G}_k(H,t) = \{a \in \mathscr{F}(P) \mid at \in \mathbf{G}_k(H)\}\,,$$
$$\mathbf{F}_k(H,t) = \{a \in \mathscr{F}(P) \mid at \in \mathbf{F}_k(H)\}\,,$$

and we shall give a combinatorial description of these sets. Let $\mathscr{F}(G)$ be the (multiplicative) free abelian monoid with basis G, define $\iota : \mathscr{F}(G) \times T \to G$ by

$$\iota(g_1 \cdot \ldots \cdot g_n t) = g_1 + \cdots + g_n + [t]$$

and consider the T-block monoid

$$\mathscr{B} = \mathscr{B}(G,T,\iota) = \{\mathfrak{w} \in \mathscr{F}(G) \times T \mid \iota(\mathfrak{w}) = 0\}\,,$$

cf. [5]. By §2, Example 3, $[\mathscr{F}(G), T, \mathscr{B}]$ is an order formation. We define the T-block homomorphism $\beta : \mathscr{F}(P) \times T \to \mathscr{F}(G) \times T$ by

$$\beta(p_1 \cdot \ldots \cdot p_n t) = ([p_1] \cdot \ldots \cdot [p_n])\, t\,;$$

then $\beta(\mathscr{F}(P)) = \mathscr{F}(G)$, $\beta^{-1}(\mathscr{B}) = H$, $\mathscr{B}$ is atomic and $\beta | H : H \to \mathscr{B}$ is length-preserving, i.e., $\mathscr{L}(\beta(a)) = \mathscr{L}(a)$ for all $a \in H$ by [5], Prop. 4. This implies

$$\mathbf{M}_k(H,t) = \{a \in \mathscr{F}(P) \mid \beta(a) \in \mathbf{M}_k(\mathscr{B}, t)\}\,,$$
$$\mathbf{G}_k(H,t) = \{a \in \mathscr{F}(P) \mid \beta(a) \in \mathbf{G}_k(\mathscr{B}, t)\}\,,$$

and we have to consider the order formation $[\mathscr{F}(G), T, \mathscr{B}]$.

For an (additive) abelian group G and a non-empty subset $Q \subset G$ we denote by

$$\mathscr{B}(Q) = \{g_1 \cdot \ldots \cdot g_n \in \mathscr{F}(Q) \mid g_1 + \cdots + g_n = 0\} \subset \mathscr{F}(Q)$$

the ordinary block monoid over Q; for $S = g_1 \cdot \ldots \cdot g_n \in \mathscr{F}(Q)$, we call $\sigma(S) = n$ the size of S. If G is finite we define the generalized Davenport constants $D_k(G)$ (for $k \in \mathbb{N}$), following [12], by

$$D_k(G) = \max\{\sigma(B) \mid B \in \mathbf{M}_k(\mathscr{B}(G))\} \in \mathbb{N}\,.$$

In particular, $D_1(G) = D(G)$ is Davenport's constant. For recent results concerning $D(G)$, see [8].

Let $[\mathscr{F}(G), T, \mathscr{B}]$ be an order formation with T-block monoid

$$\mathscr{B} = \mathscr{B}(G,T,\iota) \subset \mathscr{F}(G) \times T\,;$$

then $\mathscr{B}(G) = \mathscr{B} \cap \mathscr{F}(G) \subset \mathscr{B}$. Suppose $\# G \neq 2$; then $\mathscr{B}(G) \hookrightarrow \mathscr{F}(G)$ is a divisor theory with class group $\mathscr{F}(G)/\mathscr{B}(G) \simeq G$ and every class contains exactly one prime divisor (cf. [10], Beispiel 6). Let

$$\lambda : \mathscr{F}(G) \to \mathscr{F}(G)/\mathscr{B}(G) \xrightarrow{\sim} G$$

denote the canonical epimorphism satisfying $\lambda(g) = g$. Then, for every $g \in G$,

$$\lambda^{-1}(-g) = \{S \in \mathscr{F}(G) \mid Sg \in \mathscr{B}(G)\},$$

and we set $\lambda^{-1}(-g) = \mathscr{B}_g(G)$; in particular we have $\mathscr{B}_0(G) = \mathscr{B}(G)$.

Proposition 6. *Let G be a finite abelian group, T a reduced monoid, $\iota : \mathscr{F}(G) \times T \to G$ a monoid homomorphism satisfying $\iota(g) = g$ for all $g \in G$, and assume that the T-block monoid $\mathscr{B} = \mathscr{B}(G, T, \iota) \subset \mathscr{F}(G) \times T$ is atomic.*

(i) $\mathbf{M}_k(\mathscr{B}, 1) = \mathbf{M}_k(\mathscr{B}(G))$ *and* $\max\{\sigma(S) \mid S \in \mathbf{M}_k(\mathscr{B}, 1)\} = D_k(G)$.

(ii) *If $1 \neq t \in T$, then $\sigma(S) < D_k(G)$ for all $S \in \mathbf{M}_k(\mathscr{B}, t)$.*

Proof. (i) is obvious by definition.

(ii) Let $S \in \mathscr{F}(G)$ be such that $\sigma(S) \geqq D_k(G)$. By [12], Prop. 1, there exist

$$B_1, \dots, B_k \in \mathscr{B}(G) \setminus \{1\}$$

and $S_0 \in \mathscr{F}(G)$ such that $S = B_1 \cdot \ldots \cdot B_k S_0$. If $1 \neq t \in T$ and $St \in \mathscr{B}$, then

$$St = B_1 \cdot \ldots \cdot B_k (S_0 t)$$

implies $\max \mathscr{L}(St) > k$ and hence $S \notin \mathbf{M}_k(\mathscr{B}, t)$. □

For the description of the sets $\mathbf{G}_k(\mathscr{B}, t)$ we recall the notion of Z-systems from [13], sec. 4. Let G be a finite abelian group. By a system in G we mean a pair (Q, σ), consisting of a subset $Q \subset G$ and a function $\sigma : G \setminus Q \to \mathbb{N}_0$. If (Q, σ) and (Q', σ') are systems in G, $(Q, \sigma) \leqq (Q', \sigma')$ means $Q \subset Q'$ and $\sigma' = \sigma \mid G \setminus Q'$. For a system (Q, σ), we set

$$\Omega(Q, \sigma) = \{S \in \mathscr{F}(G) \mid v_g(S) = \sigma(g) \text{ for all } g \in G \setminus Q\}$$

($v_g(S)$ denotes the exponent of g in S), and

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

(for $Q = G$, set $\sigma = \emptyset$ and $|\sigma| = 0$). A subset $Q \subset G$ is said to be half-factorial, if the block monoid $\mathscr{B}(Q)$ is half-factorial i.e., $\# \mathscr{L}(B) = 1$ for every $B \in \mathscr{B}(Q)$. Half-factorial sets were first studied by L. Skula, who called them c-sets (see [24]); for further properties we refer to [7], §13 (there they are the sets with $\Delta(Q) = \emptyset$), in particular remember that

$$\mu(G) = \max\{\# Q \mid Q \subset G \text{ is half-factorial}\}.$$

Proposition 7. *Let assumptions be as in Proposition* 6, $k \in \mathbb{N}$ *and suppose* $\# G \geqq 3$.

(i) *For every* $t \in T$, *we have*

$$\mathbf{G}_k(\mathscr{B}, t) = \bigcup_{j=1}^{m(t)} \Omega(Q_j^{(t)}, \sigma_j^{(t)}) \cap \mathscr{B}_{\iota(t)}(G),$$

where $(Q_1^{(t)}, \sigma_1^{(t)}), \ldots, (Q_{m(t)}^{(t)}, \sigma_{m(t)}^{(t)})$ *are mutually incomparable systems of* G *such that* $\Omega(Q_j^{(t)}, \sigma_j^{(t)}) \cap \mathscr{B}_{\iota(t)}(G) \neq \emptyset$. *Moreover, this decomposition is unique, the sets* $Q_1^{(1)}, \ldots, Q_{m(1)}^{(1)}$ *are half-factorial, and every maximal half-factorial set is among* $Q_1^{(1)}, \ldots, Q_{m(1)}^{(1)}$.

(ii) *For every* $t \in T$ *and* $j \in \{1, \ldots, m(t)\}$, *there exists some* $l \in \{1, \ldots, m(1)\}$ *and a function* $\varphi : G \setminus Q_l^{(1)} \to \mathbb{N}_0$ *such that* $|\varphi| \leqq D(G) - 1$ *and* $(Q_j^{(t)}, \sigma_j^{(t)}) \leqq (Q_l^{(l)}, \sigma_l^{(1)} + \varphi)$.

Proof. (i) Let $t \in T$ be given; then clearly $\mathbf{G}_k(\mathscr{B}, t) \subset \mathscr{B}_{\iota(t)}(G)$, and if

$$A \in \mathbf{G}_k(\mathscr{B}, t), \quad B \in \mathscr{B}_{\iota(t)}(G) \quad \text{and} \quad v_g(B) \leqq v_g(A) \quad \text{for all } g \in G,$$

then $B \in \mathbf{G}_k(\mathscr{B}, t)$. Therefore the set $Z = \mathbf{G}_k(\mathscr{B}, t) \subset \mathscr{B}_{\iota(t)}(G)$ is valuation dependent and $Z = Z^*$ in the sense of [13], Def. 5. Therefore [13], Prop. 9 implies existence and uniqueness of a decomposition as asserted. Comparison with [7], Prop. 9 shows that $Q_1^{(1)}, \ldots, Q_{m(1)}^{(1)}$ are half-factorial. If $Q \subset G$ is a maximal half-factorial set, then

$$\Omega(Q, 0) \subset \mathbf{G}_k(\mathscr{B}, 1)$$

implies $Q \in \{Q_1^{(1)}, \ldots, Q_{m(1)}^{(1)}\}$.

(ii) Suppose that $t \in T, j \in \{1, \ldots, m(t)\}$ and $S \in \Omega(Q_j^{(t)}, \sigma_j^{t)}) \cap \mathscr{B}_{\iota(t)}(G)$. By [12], Prop. 1 there is a decomposition $S = BS'$, where $B \in \mathscr{B}(G)$, $S' \in \mathscr{B}_{\iota(t)}(G)$ and $\sigma(S') \leqq D(G) - 1$. From $S \in \mathbf{G}_k(\mathscr{B}, t)$ we infer $B \in \mathbf{G}_k(\mathscr{B}, 1)$, and hence

$$S = BS' \in \bigcup_{l=1}^{m(1)} \bigcup_{\substack{\varphi : G \setminus Q_l^{(1)} \to \mathbb{N}_0 \\ |\varphi| \leqq D(G) - 1}} \Omega(Q_l^{(l)}, \sigma_l^{(1)} + \varphi) \cap \mathscr{B}_{\iota(t)}(G);$$

now the assertion follows from [13], Prop. 9. □

Now we are ready to state our quantitative results concerning $\mathbf{M}_k$ and $\mathbf{G}_k$; they are based on the following analytical result.

Proposition 8. *Let* $[\mathscr{F}(P), T, H, |\cdot|]$ *be an arithmetical order formation with class group* $G = \mathscr{F}(P) \times T/H$, $Q \subset G$, $\sigma : G \setminus Q \to \mathbb{N}_0$, $|\sigma| > 0$ *if* $Q = \emptyset$, *and* $g \in G$ *such that* $\Omega(Q, \sigma) \cap \mathscr{B}_g(G) \neq \emptyset$. *Then we have*

$$\# \{a \in \mathscr{F}(P) \mid \beta(a) \in \Omega(Q, \sigma) \cap \mathscr{B}_g(G), |a| \leqq x\} = C(x)\, x (\log x)^{-\eta} (\log \log x)^d,$$

where

$$\eta = \frac{\#(G \setminus Q)}{\# G}, \quad d = \begin{cases} |\sigma|, & \text{if } Q \neq \emptyset, \\ |\sigma| - 1, & \text{if } Q = \emptyset \end{cases}$$

and $C(x) \asymp 1$ *as* $x \to \infty$.

Suppose moreover that H_0 is a congruence monoid in a holomorphy ring of some algebraic number field, $\partial : H_0 \to \mathcal{F}(P) \times T$ is the canonical divisor homomorphism associated with H_0, and $H = \partial H_0$. Then we have

$$C(x) = \sum_{\nu=0}^{d} c_\nu (\log\log x)^{-\nu} + O\left(\frac{\log\log x}{(\log x)^\gamma}\right),$$

where $c_0, \ldots, c_d \in \mathbb{R}$, $c_0 > 0$ and

$$\gamma = \begin{cases} 1, & \text{if } G = \{0\} \quad \text{or} \quad Q = \emptyset \quad \text{or} \quad Q = G, \\ \dfrac{1}{\# G} \min\left\{1, 1 - \cos \dfrac{2\pi}{\# G}\right\} & \text{otherwise}. \end{cases}$$

Proof. Since $[\mathcal{F}(P), H \cap \mathcal{F}(P), |\cdot|]$ is an arithmetical formation, the first assertion follows from [13], Proposition 10. The stronger result in the number field case is proved exactly as [18], Lemma 2 (compare also [7], Prop. 8 and note the misprints of γ). □

Theorem 1. *Let $[\mathcal{F}(P), T, H, |\cdot|]$ be an arithmetical order formation with class group G, $\beta : \mathcal{F}(P) \to \mathcal{F}(G)$ the block homomorphism and $k \in \mathbb{N}$.*

(i) *There exist $S_1, \ldots, S_m \in \mathcal{F}(G)$ and subsets $T_1, \ldots, T_m$ of T such that*

$$\mathbf{M}_k(H) = \dot{\bigcup_{j=1}^{m}} \beta^{-1}(S_j) \times T_j,$$

and there exists some $1 \leqq n \leqq m$ such that

$$T_1 = \cdots = T_n = \{1\}, \quad \{S_1, \ldots, S_n\} = \{S \in \mathbf{M}_k(\mathcal{B}(G)) \mid \sigma(S) = D_k(G)\},$$

and $\sigma(S_j) < D_k(G)$ for $n + 1 \leqq j \leqq m$.

(ii) *For $x \to \infty$, we have*

$$\# \{a \in \mathbf{M}_k(H) \mid |a| \leqq x\} \asymp x (\log x)^{-1} (\log\log x)^{D_k(G) - 1}.$$

Proof. (i) By Proposition 6,

$$\bigcup_{t \in T} \mathbf{M}_k(\mathcal{B}, t) = \{S_1, \ldots, S_m\} \subset \mathcal{F}(G),$$

and there exists some $1 \leqq n \leqq m$ such that

$$\sigma(S_1) = \cdots = \sigma(S_n) = D_k(G), \quad \{S_1, \ldots, S_n\} \subset \mathbf{M}_k(\mathcal{B}, 1) = \mathbf{M}_k(\mathcal{B}(G)),$$

and $\sigma(S_j) < D_k(G)$ if $S_j \in \mathbf{M}_k(\mathcal{B}, t)$ for some $t \neq 1$. Putting $T_j = \{t \in T \mid S_j \in \mathbf{M}_k(\mathcal{B}, t)\}$, we obtain

$$\mathbf{M}_k(\mathcal{B}) = \dot{\bigcup_{j=1}^{m}} \{S_j\} \times T_j,$$

and consequently

$$\mathbf{M}_k(H) = \dot{\bigcup_{j=1}^{m}} \beta^{-1}(S_j) \times T_j .$$

(ii) For $S \in \mathscr{F}(G)$, we define $\sigma_S : G \to \mathbb{N}_0$ by $\sigma_S(g) = v_g(S)$; then we have $|\sigma_S| = \sigma(S)$ and $\Omega(\emptyset, \sigma_S) = \{S\}$. Now the result follows from (i), Proposition 8 and Proposition 5. □

Remarks. 1. Since $\mathbf{M}_1(H)$ is the set of irreducible elements of H, Theorem 1 contains a generalization of the prime number theorem.

2. There are similar results for the sets

$$\mathbf{M}_k'(H) = \{a \in H \mid k \in \mathscr{L}(a)\} ,$$
$$\mathbf{M}_k''(H) = \{a \in H \mid \min \mathscr{L}(a) \leqq k\} ,$$

see [7], Theorem 5.

3. If H arises from a congruence monoid in some holomorphy ring of an algebraic number field or algebraic function field, we get essentially stronger asymptotic results. For the number field case this follows from Proposition 8, for the function field case from [17].

Let us state Theorem 1, provided with a strong asymptotics, for orders in algebraic number fields.

Theorem 1 $\mathfrak{o}$. *Let $\mathfrak{o}$ be an order in an algebraic number field K, $G = \mathrm{Pic}(\mathfrak{o})$, r the number of distinct prime ideals of $\mathfrak{o}_K$ dividing the conductor of $\mathfrak{o}$ and $k \in \mathbb{N}$. Then we have, for all $x \geqq 3$,*

$$\# \{a\mathfrak{o} \mid a \in \mathbf{M}_k(\mathfrak{o}),\ (\mathfrak{o} : a\mathfrak{o}) \leqq x\} = \frac{x}{\log x}\left[V(\log\log x) + O\left(\frac{(\log\log x)^N}{\log x}\right)\right],$$

where $V \in \mathbb{R}[X]$ is a polynomial of degree $D_k(G) - 1$ with positive leading coefficient and $N = D_k(G)$ if $r = 0$ and $N = D_k(G) + r - 1$ otherwise.

Proof. If $r = 0$, then $\mathfrak{o}$ is a principal order and the assertion follows from Proposition 8. Suppose $r \geqq 1$; by Proposition 4, $\mathfrak{o}^\bullet$ is a congruence monoid of $\mathfrak{o}_K$. Let

$$\partial : \mathfrak{o}^\bullet \to \mathscr{F}(P) \times T$$

be the canonical divisor homomorphism; then $[\mathscr{F}(P), T, \partial\mathfrak{o}^\bullet, |\cdot|]$ is an arithmetical order formation by Proposition 3, and for $a \in \mathfrak{o}^\bullet$ we have $|\partial a| = (\mathfrak{o} : a\mathfrak{o})$ by Proposition 4. Since ∂ induces an isomorphism $\partial^* : \mathfrak{o}^\bullet / \mathfrak{o}^\times \xrightarrow{\sim} \partial\mathfrak{o}^\bullet$ the assertion follows as in Theorem 1, using the stronger asymptotics given in Proposition 5 and in Proposition 8. □

Theorem 2. *Let $[\mathscr{F}(P), T, H, |\cdot|]$ be an arithmetical order formation with class group G, $\beta : \mathscr{F}(P) \to \mathscr{F}(G)$ the block homomorphism and $k \in \mathbb{N}$.*

(i) *Suppose* $\#G \geqq 3$; *then there exist systems* $(\Omega_1, \sigma_1), \dots, (\Omega_m, \sigma_m)$ *of* G, *classes* $g_1, \dots, g_m \in G$ *and subsets* $T_1, \dots, T_m$ *of* T *such that*

$$\mathbf{G}_k(H) = \bigcup_{j=1}^{m} \beta^{-1}[\Omega(Q_j, \sigma_j) \cap \mathscr{B}_{g_j}(G)] \times T_j \, ;$$

we have $\max\{\#Q_j \mid 1 \leqq j \leqq m\} = \mu(G)$, *and there is a constant* $\mathbf{c}_k(G)$ *depending only on* G *such that* $|\sigma_j| \leqq \mathbf{c}_k(G)$ *for all* $1 \leqq j \leqq m$.

(ii) *For* $x \to \infty$, *we have*

$$\#\{a \in \mathbf{G}_k(H) \,|\, |a| \leqq x\} \asymp x(\log x)^{-1+\mu(G)/\#G}(\log\log x)^c$$

where $c \in \mathbb{N}_0$ *with* $c \leqq \mathbf{c}_k(G)$ *if* $\#G \geqq 3$, *and* $c = 0$ *if* $\#G \leqq 2$.

Proof. (i) By Proposition 7, there exist systems $(Q_1, \sigma_1), \dots, (Q_m, \sigma_m)$ of G and classes $g_1, \dots, g_m \in G$ such that

$$\bigcup_{t \in T} \mathbf{G}_k(\mathscr{B}, t) = \bigcup_{j=1}^{m} \Omega(Q_j, \sigma_j) \cap \mathscr{B}_{g_j}(G) \, ,$$

and there exists a constant $\mathbf{c}_k(G)$ depending only on G such that $|\sigma_j| \leqq \mathbf{c}_k(G)$ for all $1 \leqq j \leqq m$. Moreover, for each $1 \leqq j \leqq m$, there is some $t \in T$ such that

$$\Omega(Q_j, \sigma_j) \cap \mathscr{B}_{g_j}(G) \subset \mathbf{G}_k(\mathscr{B}, t) \, ,$$

and the maximal half-factorial sets of G are amongst $Q_1, \dots, Q_m$, whence

$$\max\{\#Q_j \mid 1 \leqq j \leqq m\} = \mu(G) \, .$$

Putting

$$T_j = \{t \in T \mid \Omega(Q_j, \sigma_j) \cap \mathscr{B}_{g_j}(G) \subset \mathbf{G}_k(\mathscr{B}, t)\} \, ,$$

we obtain

$$\mathbf{G}_k(\mathscr{B}) = \bigcup_{j=1}^{m} [\Omega(Q_j, \sigma_j) \cap \mathscr{B}_{g_j}(G)] \times T_j \, ,$$

and consequently

$$\mathbf{G}_k(H) = \bigcup_{j=1}^{m} \beta^{-1}[\Omega(Q_j, \sigma_j) \cap \mathscr{B}_{g_j}(G)] \times T_j \, .$$

(ii) First suppose $\#G \leqq 2$. In this case, G is half-factorial, and therefore we have for every $t \in T$ either $\mathbf{G}_k(\mathscr{B}, t) = \emptyset$ or $\mathbf{G}_k(\mathscr{B}, t) = \mathscr{B}_{\iota(t)}(G)$; this implies

$$\#\{a \in \mathbf{G}_k(H) \,|\, |a| \leqq x\} \asymp x$$

though in general $\mathbf{G}_k(H) \neq H$.

Now let $\# G \geqq 3$; then the assertion follows from (i), Proposition 8 and Proposition 5 if we observe that for $1 \leqq j, \mu \leqq m$ the intersection

$$[\Omega(Q_j, \sigma_j) \cap \mathscr{B}_{g_j}(G)] \cap [\Omega(Q_\mu, \sigma_\mu) \cap \mathscr{B}_{g_\mu}(G)]$$

is either empty or of the form $\Omega(Q_j \cap Q_\mu, \sigma) \cap \mathscr{B}_{g_j}(G)$ where

$$\sigma | G \setminus Q_j = \sigma_j \quad \text{and} \quad \sigma | G \setminus Q_\mu = \sigma_\mu .$$

Remarks. 1. There is a similar result for the sets $\mathbf{G}'_k(H) = \mathbf{G}_k(H) \setminus \mathbf{G}_{k-1}(H)$ $(k \geqq 2)$.

2. Again, we obtain essentially stronger asymptotic results if we are in the number field or in the function field case.

Let us state Theorem 2, provided with a strong asymptotics, for orders in algebraic number fields.

Theorem 2 $\mathfrak{o}$. *Let $\mathfrak{o}$ be an order in an algebraic number field K, $G = \mathrm{Pic}(\mathfrak{o})$, r the number of distinct prime ideals dividing the conductor of $\mathfrak{o}$ and $k \in \mathbb{N}$. Then we have, for all $x \geqq 3$,*

$$\# \{a\mathfrak{o} \,|\, a \in G_k(\mathfrak{o}), (\mathfrak{o} : a\mathfrak{o}) \leqq x\} = x(\log x)^{-1+\mu(G)/\# G}\left[V(\log\log x) + O\left(\frac{(\log\log x)^N}{(\log x)^\gamma}\right)\right],$$

where $V \in \mathbb{R}[X]$ is a polynomial with positive leading coefficient.

If $\# G \leqq 2$, *then* $\deg(V) = 0$, $N = \max\{1, r\}$ *and* $\gamma = 1$.

If $\# G \geqq 3$, *then* $\deg(V) \leqq \mathsf{c}_k(G)$, $N = \deg(V) + 1$ *and*

$$\gamma = \min\{1, 1 - \cos(2\pi / \# G)\} / \# G .$$

Proof. Combine the proofs of Theorem 1$\mathfrak{o}$ and Theorem 2 and observe that in the case $\# G \leqq 2$ the set G is half-factorial. □

In order to describe the sets $\mathbf{F}_k(H, t)$, we recall from [15] the notion of reduced types. For an abelian group $G \neq \{0\}$, we set $G' = G \setminus \{0\}$; we write the elements $\nu \in \mathscr{F}(G' \times \mathbb{N})$ in the form

$$\nu = \prod_{(g,n) \in G' \times \mathbb{N}} (g, n)^{\nu_{g,n}}$$

where $\nu_{g,n} \in \mathbb{N}_0$, $\nu_{g,n} = 0$ for almost all $(g, n) \in G' \times \mathbb{N}$, and we call

$$\delta(\nu) = \# \{(g, n) \in G' \times \mathbb{N} \,|\, \nu_{g,n} = 1\}$$

the depth of ν.

Now let again $[\mathscr{F}(P), T, H]$ be an order formation with class group G; we assume that H is atomic, $\{0\} \neq G$ is finite and $\#(g \cap P) = \infty$ for all $g \in G$; then $\mathscr{F}(P) \cap H \hookrightarrow \mathscr{F}(P)$

is a divisor theory with class group G by Lemma 1. We write the elements $a \in \mathscr{F}(P)$ in the form

$$a = \prod_{g \in G} \prod_{n=1}^{\lambda_g} p_{g,n}^{\nu_{g,n}},$$

where $\lambda_g \in \mathbb{N}_0$, $p_{g,1}, \dots, p_{g,\lambda_g} \in P \cap g$ are distinct, $\nu_{g,n} \in \mathbb{N}$ and $1 \leqq \nu_{g,1} \leqq \nu_{g,2} \leqq \cdots \leqq \nu_{g,\lambda_g}$; we call

$$\tau_0(a) = \prod_{g \in G'} \prod_{n=1}^{\lambda_g} (g, n)^{\nu_{g,n}} \in \mathscr{F}(G' \times \mathbb{N})$$

the reduced type of a and $\delta(a) = \delta(\tau_0(a))$ the depth of a. For $k \in \mathbb{N}$, Narkiewicz' constant $\mathbf{a}_k(G)$ is defined by

$$\mathbf{a}_k(G) = \max\{\delta(a) \mid a \in \mathbf{F}_k(H \cap \mathscr{F}(P))\}.$$

For $G = \{0\}$ we set $\mathbf{a}_k(G) = 0$. It follows from [15], Satz 6 and Satz 9, that in fact $\mathbf{a}_k(G)$ depends only on G and coincides with the constant of the same name introduced by W. Narkiewicz in [21] (note that $H \cap \mathscr{F}(P) \hookrightarrow \mathscr{F}(P)$ is a divisor theory with class group G, every class contains infinitely many primes and therefore every normalized reduced type is of the form $\tau_0(a)$).

Proposition 9. *Let $[\mathscr{F}(P), T, H]$ be an order formation, where H is atomic,*

$$\{0\} \neq G = \mathscr{F}(P) \times T/H$$

is finite and $\#(g \cap P) = \infty$ for all $g \in G$.

(i) *If $t \in T$, $a \in \mathbf{F}_k(H, t)$, $b \in \mathscr{F}(P)$ and $\tau_0(a) = \tau_0(b)$, then $b \in \mathbf{F}_k(H, t)$.*

(ii) *For every $t \in T$ and $a \in \mathbf{F}_k(H, t)$ we have $\delta(a) \leqq \mathbf{a}_k(G)$.*

Proof. (i) Let $t \in T$ and $a \in \mathscr{F}(P)$ be given,

$$a = \prod_{g \in G} \prod_{n=1}^{\lambda_g} p_{g,n}^{\nu_{g,n}},$$

where $\lambda_g \in \mathbb{N}_0$, $p_{g,i} \in P \cap g$ are distinct and $1 \leqq \nu_{g,1} \leqq \cdots \leqq \nu_{g,\lambda_g}$. Then we have $at \in H$ if and only if

$$\sum_{g \in G'} \sum_{n=1}^{\lambda_g} \nu_{g,n} g + [t] = 0;$$

since $p_{0,1}, \dots, p_{0,\lambda_0}$ are prime elements, the factorizations of at in H correspond bijectively to pairs of decompositions

$$\left(\nu_{g,n} = \sum_{j=1}^{r} \nu_{g,n}^{(j)}\right)_{g \in G'}, \quad t = t_1 \cdot \ldots \cdot t_r$$

where $v_{g,n}^{(j)} \geqq 0$ and $t_j \in T$ are such that

$$\sum_{g \in G'} \sum_{n=1}^{\lambda_g} v_{g,n}^{(j)} g + [t_j] = 0 .$$

Therefore the property of belonging to $\mathbf{F}_k(H, t)$ does not depend on the element $a \in \mathscr{F}(P)$ but only on its reduced type $\tau_0(a)$.

(ii) Suppose that $a \in \mathscr{F}(P)$ satisfies $\delta(a) > \mathbf{a}_k(G)$ and $at \in H$ for some $t \in T$. By assumption, there is some $p \in P \cap [t]$ such that $p \nmid a$; then $c = ap \in H$, and

$$\delta(c) \geqq \delta(a) > \mathbf{a}_k(G) .$$

This implies $\mathbf{f}(c) > k$, and substituting t for p, we obtain $\mathbf{f}(at) \geqq \mathbf{f}(c) > k$, whence

$$a \notin \mathbf{F}_k(H, t) . \quad \square$$

Theorem 3. *Let $[\mathscr{F}(P), T, H, |\cdot|]$ be an arithmetical order formation with class group G and $k \in \mathbb{N}$. Then we have, for $x \to \infty$,*

$$\#\{a \in \mathbf{F}_k(H) \,|\, |a| \leqq x\} \asymp x(\log x)^{-1+1/\#G}(\log\log x)^{\mathbf{a}_k(G)} .$$

Proof. If $G = \{0\}$, then we have for every $t \in T$ either $\mathbf{F}_k(H, t) = \emptyset$ or $\mathbf{F}_k(H, t) = H$ and in particular $\mathbf{F}_k(H, 1) = \mathbf{F}_k(H)$ for all $k \geqq 1$. Thus in this case the assertion follows.

From now on, suppose that $G \neq \{0\}$; for $t \in T$, set

$$\mathfrak{T}(t) = \{\tau_0(a) \,|\, a \in \mathbf{F}_k(H, t)\}$$

and

$$\delta(t) = \max\{\delta(v) \,|\, v \in \mathfrak{T}(t)\} .$$

Proposition 9 implies

$$\mathbf{a}_k(G) = \max\{\delta(t) \,|\, t \in T\} ,$$

and from [13], Theorem 1 we obtain, for every $0 \leqq l \leqq a_k(G)$ and $t \in T$ such that $\delta(t) = l$,

$$(*) \qquad \begin{aligned} \#\{a \in \mathbf{F}_k(H, t) \,|\, |a| \leqq x\} &= \#\{a \in \mathscr{F}(P) \,|\, \tau_0(a) \in \mathfrak{T}(t), |a| \leqq x\} \\ &= C(t, x)\, x(\log x)^{-1+1/\#G}(\log\log x)^l , \end{aligned}$$

where $C(t, x) \asymp 1$ as $x \to \infty$. Also from [13], Theorem 1 we obtain

$$\#\{a \in \mathscr{F}(P) \,|\, \delta(a) = l, |a| \leqq x\} = C_l(x)\, x(\log x)^{-1+1/\#G}(\log\log x)^l$$

where $C_l(x) \asymp 1$ as $x \to \infty$, and since obviously $C(t, x) \leqq C_l(x)$ for all $t \in T$ satisfying $\delta(t) = l$, we see that C is bounded. Thus Proposition 5 applies and yields

$$\# \{a \in \mathbf{F}_k(H) \,|\, |a| \leqq x\} = \sum_{t \in T} \left\{a \in \mathbf{F}_k(H, t) \,|\, |a| \leqq \frac{x}{|t|}\right\}$$
$$= C(x)\, x (\log x)^{-1 + 1/\# G} (\log\log x)^{\mathbf{a}_k(G)},$$

where $C(x) \asymp 1$ as $x \to \infty$. □

Theorem 3 $\mathfrak{o}$. *Let $\mathfrak{o}$ be an order in an algebraic number field K, $G = \operatorname{Pic}(\mathfrak{o})$, r the number of distinct prime ideals dividing the conductor of $\mathfrak{o}$ and $k \in \mathbb{N}$. Then we have, for all $x \geqq 3$,*

$$\# \{a\mathfrak{o} \,|\, a \in F_k(\mathfrak{o}), (\mathfrak{o} : a\mathfrak{o}) \leqq x\} = x (\log x)^{-1 + 1/\# G} \left[V(\log\log x) + O\left(\frac{(\log\log x)^N}{\log x}\right)\right],$$

where $N \in \mathbb{N}$ and $V \in \mathbb{R}[X]$ is a polynomial with positive leading coefficient of degree $\mathbf{a}_k(G)$.

Proof. In case $G = \{0\}$ as well as in case $G \neq \{0\}$ the function $C(t, x)$ in formula (∗) (proof of Theorem 3) has the form given in Proposition 5 (ii) (cf. [13], section 5), which implies the assertion. □

References

[1] *D.D. Anderson* and *D.F. Anderson*, Elasticity of factorizations in integral domains, J. Pure Appl. Algebra **80** (1992), 217–235.

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

[3] *A. Geroldinger*, Arithmetical characterizations of divisor class groups, Arch. Math. **54** (1990), 455–464.

[4] *A. Geroldinger*, On the arithmetic of certain not integrally closed noetherian integral domains, Comm. Algebra **19** (1991), 685–698.

[5] *A. Geroldinger*, *T*-block monoids and their arithmetical applications to certain integral domains, Comm. Algebra **22** (1994), 1603–1615.

[6] *A. Geroldinger* and *F. Halter-Koch*, Arithmetical theory of monoid homomorphisms, Semigroup Forum **48** (1994), 333–362.

[7] *A. Geroldinger* and *J. Kaczorowski*, Analytic and arithmetic theory of semigroups with divisor theory, Sém. Th. Nombres Bordeaux **4** (1992), 199–238.

[8] *A. Geroldinger* and *R. Schneider*, On Davenport's constant, J. Comb. Th. (A) **61** (1992), 147–152.

[9] *R. Gilmer*, Commutative semigroup rings, The University of Chicago Press, 1984.

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

[11] *F. Halter-Koch*, Ein Approximationssatz für Halbgruppen mit Divisorentheorie, Result. Math. **19** (1991), 74–82.

[12] *F. Halter-Koch*, A generalization of Davenport's constant and its arithmetical applications, Colloq. Math. **63** (1992), 203–210.

[13] *F. Halter-Koch*, Chebotarev formations and quantitative aspects of non-unique factorizations, Acta Arith. **62** (1992), 173–206.

[14] *F. Halter-Koch*, Finiteness theorems for factorizations, Semigroup Forum **44** (1992), 112–117.

[15] *F. Halter-Koch*, Typenhalbgruppen und Faktorisierungsprobleme, Result. Math. **22** (1992), 545–559.

[16] *F. Halter-Koch*, Elasticity of factorizations in atomic monoids and integral domains, J. Th. Nomb. Bordeaux.

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

[19] *M.D. Larsen* and *P.J. McCarthy*, Multiplicative theory of ideals, Academic Press, 1971.

[20] *H. Matsumura*, Commutative ring theory, Cambridge University Press, 1986.

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

[22] *W. Narkiewicz*, Elementary and analytic theory of algebraic numbers, Springer, 1990.

[23] *J. Neukirch*, Algebraische Zahlentheorie, Springer, 1992.

[24] *L. Skula*, On *c*-semigroups, Acta Arith. **31** (1976), 247–257.

[25] *H. Stichtenoth*, Algebraic function fields and codes, Springer, 1993.

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

Institut für Mathematik, Karl-Franzens-Universität, Heinrichstraße 36/IV, 8010 Graz, Austria

Wydział Matematyki i Informatyki, Uniwersytet Im. A. Mickiewicza, Ul. Matejki 48/49, 60-769 Poznan, Polen

Eingegangen 13. Juni 1994