C O L L O Q U I U M   M A T H E M A T I C U M

VOL. 72 | 1997 | NO. 1

CHAINS OF FACTORIZATIONS IN ORDERS OF GLOBAL FIELDS

BY

ALFRED GEROLDINGER (GRAZ)

1. Introduction. Let R be the ring of integers in an algebraic number field. Every non-zero non-unit $a \in R$ has a factorization into irreducible elements of R. In general, there are several distinct factorizations. In the qualitative theory of non-unique factorizations one tries to describe the non-uniqueness of factorizations by various arithmetical invariants. A main aim is to understand the interdependence of phenomena of non-unique factorizations and other invariants of R, in particular its class group. In the quantitative theory of non-unique factorizations one considers arithmetically defined subsets $Z \subseteq R$ and the asymptotic behaviour of the corresponding counting function $Z(x)$. Here $Z(x)$ means the number of principal ideals aR such that $a \in Z$ and $(R : aR) \le x$. The classical sets are, for each $k \in \mathbb{N}_+$,

$\mathbf{G}_k(R)$: the set of all $a \in R$ having factorizations of at most k different lengths,

$\mathbf{F}_k(R)$: the set of all $a \in R$ having at most k distinct factorizations

(cf. [Na; Chapter 9]). If Z is one of these sets, it turned out that, apart from trivial cases,

$$\lim_{x\to\infty} \frac{Z(x)}{R(x)} = 0.$$

So one might ask about the typical behaviour of factorizations of elements of R. In other words, the problem is to characterize arithmetically simple subsets $Z \subseteq R$ such that

$$\lim_{x\to\infty} \frac{Z(x)}{R(x)} = 1. \tag{1}$$

By [Ge1; Satz 2], (1) is satisfied by the subset $Z \subseteq R$ consisting of those elements $a \in R$ whose sets of lengths $L(a)$ have the form

$$L(a) = \{y, y+1, \ldots, y+k\} \tag{2}$$

for some $y, k \in \mathbb{N}_+$.

1991 *Mathematics Subject Classification*: Primary 11R27.

In this paper we study chains of factorizations of elements $a \in R$. To be more precise, we consider the subset $Z \subseteq R$ consisting of those elements $a \in R$ for which

$$c(a) \le 3 \tag{3}$$

(i.e., the elements $a \in R$ such that for any two factorizations z, z' of a there exists a 3-chain of factorizations from z to z'). For general properties of chains of factorizations and the significance of the catenary degree we refer to [Ge3]. However, note that, in particular, (3) implies (2).

After fixing notations in Section 2 we show that there exists an element $a^* \in R$ such that for all multiples a of a^*, we have $c(a) \le 3$ (Theorem 3.1). This result is proved in the setting of Krull monoids. Its proof uses the finiteness of the catenary degree and some technical preparations done in [Ge3]. In Section 4 we derive the desired quantitative interpretation of Theorem 3.1:

$$\lim_{x\to\infty} \frac{\#\{aR : (R : aR) \le x,\ c(a) \le 3\}}{\#\{aR : (R : aR) \le x\}} = 1$$

(see Theorem 4.4). To do so, we use the abstract analytic machinery recently established in [G-HK-K]. This allows us to obtain asymptotic results not only for principal orders in algebraic number fields, but also for arbitrary orders in global fields (Theorem 4.3).

2. Preliminaries. 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. H is said to be *reduced* if $H^\times = \{1\}$.

For a set P we denote by $\mathcal{F}(P)$ the free abelian monoid with basis P. Then every $a \in \mathcal{F}(P)$ has a unique representation

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

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

$$\sigma(a) = \sum_{p\in P} v_p(a) \in \mathbb{N}$$

is called the *size* of a.

Let D be a monoid and $H \subseteq D$ a submonoid. We define the congruence modulo H in D by

$$x \equiv y \bmod H \quad \text{if} \quad xH \cap yH \ne \emptyset.$$

The *factor monoid* of D with respect to the congruence modulo H is denoted by D/H. For $a \in D$, $[a] \in D/H$ denotes the class containing a. In particular, we set $D_{\text{red}} = D/D^\times$.

A monoid homomorphism $\varphi : H \to D$ is said to be a

(a) *divisor homomorphism* if $a, b \in H$ and $\varphi(a) \,|\, \varphi(b)$ implies $a \,|\, b$.

(b) *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 $p = \gcd\{\varphi(u_1), \ldots, \varphi(u_m)\}$.

A monoid H is called a *Krull monoid* if it admits a divisor theory $\varphi : H \to D$. The factor monoid $\mathrm{Cl}(H) = D/\varphi(H)$ is an abelian group, which just depends on H. It is called the (*divisor*) *class group* of H; it will be written additively.

Let G be an abelian group. As usual, we say that elements $g_1, \ldots, g_r$ are *linearly independent* if each equation $\sum_{i=1}^{r} n_i g_i = 0$ with integer coefficients n_i implies $n_1 g_1 = \ldots = n_r g_r = 0$.

For a subset $G_0 \subseteq G$ we consider the free abelian monoid $\mathcal{F}(G_0)$ and the submonoid

$$\mathcal{B}(G_0) = \Big\{ \prod_{g \in G_0} g^{n_g} \in \mathcal{F}(G_0) : \sum_{g \in G_0} n_g g = 0 \Big\} \subseteq \mathcal{F}(G_0),$$

called the *block monoid* over G_0. Block monoids are a powerful combinatorial tool for arithmetical investigations of Krull monoids.

Let H be a Krull monoid with divisor class group G. For simplicity, we suppose that H is reduced and the inclusion $H \hookrightarrow \mathcal{F}(P)$ is a divisor theory. Let $G_0 = \{[p] \in G : p \in P\} \subseteq G$ denote the set of classes containing prime divisors. Then the *block homomorphism*

$$\boldsymbol{\beta} : \mathcal{F}(P) \to \mathcal{F}(G_0)$$

defined by $\boldsymbol{\beta}(p) = [p] \in G_0$, for all $p \in P$, carries over essential arithmetical information from H to $\boldsymbol{\beta}(H) = \mathcal{B}(G_0)$ (cf. [Ge3; Section 4]).

We briefly recall some basic notions from the theory of non-unique factorizations.

Let H be a monoid. We denote by $\mathcal{U}(H)$ the set of irreducible elements of H. The *factorization monoid* $\mathcal{Z}(H)$ of H is defined as the free abelian monoid with basis $\mathcal{U}(H_{\mathrm{red}})$. Thus,

$$\mathcal{Z}(H) = \mathcal{F}(\mathcal{U}(H_{\mathrm{red}}))$$

and the elements $z \in \mathcal{Z}(H)$ are written in the form

$$z = \prod_{u \in \mathcal{U}(H_{\mathrm{red}})} u^{v_u(z)}.$$

Let $\pi : \mathcal{Z}(H) \to H_{\mathrm{red}}$ be the canonical homomorphism. We say that H is *atomic* if π is surjective.

For a finite abelian group G let *Davenport's constant* $\mathcal{D}(G)$ be defined as

$$\mathcal{D}(G) = \max\{\sigma(U) : U \in \mathcal{B}(G) \text{ is irreducible}\} \in \mathbb{N}_+.$$

For the significance of Davenport's constant in factorization theory the reader is referred to [Ch].

Suppose that H is an atomic monoid. For $a \in H$ the elements of

$$\mathcal{Z}_H(a) = \mathcal{Z}(a) = \pi^{-1}(aH^\times) \subseteq \mathcal{Z}(H)$$

are called *factorizations of* a and

$$L_H(a) = L(a) = \{\sigma(z) : z \in \mathcal{Z}(a)\} \subseteq \mathbb{N}$$

denotes the *set of lengths* of a. For two factorizations $z, z' \in \mathcal{Z}(H)$ we call

$$d(z,z') = \max\left\{\sigma\left(\frac{z}{\gcd(z,z')}\right),\ \sigma\left(\frac{z'}{\gcd(z,z')}\right)\right\} \in \mathbb{N}$$

the *distance* between z and z'.

Finally, we define the central arithmetical notion of this paper. For a motivation and a broader discussion the reader is referred to [Ge3; Section 3].

Let $a \in H$, $z, z' \in \mathcal{Z}(a)$ and $N \in \mathbb{N} \cup \{\infty\}$; we say that there is an *N-chain* (*of factorizations*) *from z to z'* if there exist factorizations $z = z_0, z_1, \ldots, z_k = z' \in \mathcal{Z}(a)$ such that $d(z_{i-1}, z_i) \le N$ for $1 \le i \le k$.

The *catenary degree*

$$c_H(H') = c(H') \in \mathbb{N} \cup \{\infty\}$$

of a subset $H' \subseteq H$ is the minimal $N \in \mathbb{N} \cup \{\infty\}$ such that for any $a \in H'$ and any two factorizations $z, z' \in \mathcal{Z}(a)$ there exists an N-chain from z to z'. For simplicity, we write $c(a)$ instead of $c(\{a\})$.

By definition, we have $c(a) = 0$ if and only if $\#\mathcal{Z}(a) = 1$. Thus H is factorial if and only if $c(H) = 0$. Furthermore, if $c(a) = 2$, then $\#L(a) = 1$; therefore $c(H) = 2$ implies that H is half-factorial.

3. Chains of factorizations of large elements. Let H be a Krull monoid with finite divisor class group G such that each class contains a prime divisor. Then for all $a \in H$ we have

$$c(a) \le c(G) \le \mathcal{D}(G)$$

(see [Ge3; Propositions 4.2 and 4.3]). In this section we show that if $a \in H$ is sufficiently large, then

$$c(a) \le 3.$$

If $\#G > 2$, then H is not half-factorial and thus "$c(a) \le 3$" is best possible. Furthermore, if $c(a) \le 3$, then $L(a) = \{y, y+1, \ldots, y+k\}$ for some $y, k \in \mathbb{N}$. Hence, the following result will sharpen [Ge1; Proposition 11]; cf. also [Ge2; Theorem 1].

THEOREM 3.1. *Let H be a reduced Krull monoid with divisor theory $H \hookrightarrow \mathcal{F}(P)$ and finite divisor class group G, and suppose that each class contains a prime divisor. Then there exists some element $A^* \in \mathcal{B}(G)$ such that* $c(a) \le 3$

for every $a \in H$ *with* $A^* \mid \boldsymbol{\beta}(a)$, *where* $\boldsymbol{\beta} : \mathcal{F}(P) \to \mathcal{F}(G)$ *denotes the block homomorphism.*

Throughout this section we keep the following notation: G denotes the divisor class group of H, $G' = G \backslash \{0\}$, and $G'' \subseteq G'$ is a half-system (i.e., $G'' \subseteq G'$ is minimal such that $G' = G'' \cup \{-g : g \in G''\}$). In the case where $\# G \le 2$, Theorem 3.1 holds with $A^* = 1$ (cf. [Ge3; Propositions 4.2 and 4.3]). Hence we suppose that $\# G \ge 3$.

Lemma 3.2. *Let* $A \in \mathcal{B}(G')$ *and* $(n_g)_{g \in G''} \in \mathbb{N}^{G''}$ *be such that*

$$(*) \qquad \prod_{g \in G'} g^{\operatorname{ord}(g)} \prod_{g \in G''} (-g \cdot g)^{n_g} \mid A.$$

Then for every $z \in \mathcal{Z}(A)$ *there exists a* 3*-chain of factorizations from* z *to*

$$z' = \prod_{g \in G''} (-g \cdot g)^{n_g} y' \in \mathcal{Z}(A)$$

for some $y' \in \mathcal{Z}(A \prod_{g \in G''} (-g \cdot g)^{-n_g})$.

Proof. We set $N = \sum_{g \in G''} n_g$ and complete the proof by induction on N. If $N = 0$, nothing has to be done. Let $N > 0$ and suppose the lemma is true for all $B \in \mathcal{B}(G')$ and all $(m_g)_{g \in G''} \in \mathbb{N}^{G''}$ satisfying $(*)$ and with $\sum_{g \in G''} m_g < N$.

Now let $A \in \mathcal{B}(G')$, $z \in \mathcal{Z}(A)$ and $(n_g)_{g \in G''}$ be given such that $(*)$ holds and $\sum_{g \in G''} n_g = N$. Since $N > 0$, there is some $g_1 \in G''$ with $n_{g_1} > 0$.

Assertion. *There exists a* 3*-chain of factorizations from* z *to*

$$z' = (-g_1 \cdot g_1) y'$$

for some $y' \in \mathcal{Z}(B)$ *and* $B = A(-g_1 \cdot g_1)^{-1} \in \mathcal{B}(G')$.

Given the assertion, Lemma 3.2 follows by applying the induction hypothesis to B and to $(m_g)_{g \in G''}$ with $m_{g_1} = n_{g_1} - 1$ and $m_g = n_g$ for $g \in G'' \backslash \{g_1\}$.

In order to prove the assertion, suppose $z = \prod_{i=1}^{\varphi} U_i$ with $U_1, \ldots, U_\varphi \in \mathcal{U}(\mathcal{B}(G'))$ and $U_1 = \prod_{j=1}^{k} g_j$. We argue by induction on $k = \sigma(U_1)$. For $k = 2$ we are done. Suppose $k \ge 3$, and set $g_0 = g_{k-1} + g_k$. Since

$$v_{g_0}(A) \ge \operatorname{ord}(g_0) \quad \text{and} \quad v_{g_0}(U_1) < \operatorname{ord}(g_0),$$

it follows that $v_{g_0}(U_2 \ldots U_\varphi) > 0$ and hence we may suppose without restriction of generality that $U_2 = g_0 \prod_{j=k+1}^{l} g_j$.

Then $V_1 = \prod_{j=0}^{k-2} g_j \in \mathcal{U}(\mathcal{B}(G'))$ and $\prod_{j=k-1}^{l} g_j$ is a product of at most two irreducible blocks, say $\prod_{j=k-1}^{l} g_j = \prod_{\nu=2}^{t} V_\nu$ with $t \in \{2, 3\}$ and $V_\nu \in$

$\mathcal{U}(\mathcal{B}(G'))$. Setting

$$y = \prod_{\nu=1}^{t} V_\nu \prod_{\nu=3}^{\varphi} U_\nu$$

we infer that $d(z, y) \le 3$. Since $\sigma(V_1) < \sigma(U_1)$ and $v_{g_1}(V_1) > 0$, the induction hypothesis applies to V_1, which implies the assertion. ∎

For every $A \in \mathcal{B}(G')$ we have $A = \prod_{g \in G'} g^{v_g(A)}$ and we set

$$-A = \prod_{g \in G'} (-g)^{v_g(A)}.$$

Then

$$(-A)A = \prod_{g \in G'} (-g \cdot g)^{v_g(A)}.$$

Whenever in the sequel we consider N-chains of factorizations $z = z_0, z_1, \ldots, z_k = z'$, then of course all z_i are factorizations of some fixed block $B \in \mathcal{B}(G)$.

LEMMA 3.3. *Let* $U_1, \ldots, U_\varphi \in \mathcal{U}(\mathcal{B}(G'))$ *and*

$$z = \prod_{g \in G''} (-g \cdot g)^{\mathcal{D}(G)} \prod_{g \in G'} (-g \cdot g)^{\sum_{i=1}^{\varphi} v_g(U_i)} \in \mathcal{Z}(\mathcal{B}(G)).$$

Then there exists a 3*-chain of factorizations from* z *to*

$$z' = \prod_{g \in G''} (-g \cdot g)^{\mathcal{D}(G)} \prod_{i=1}^{\varphi} (-U_i) U_i.$$

P r o o f. We give a proof for $\varphi = 1$. The general case follows by an inductive argument.

Suppose $U_1 = U = \prod_{j=1}^{k} g_j$. It suffices to find a 3-chain of factorizations from

$$x = \prod_{g \in G'} (-g \cdot g)^{v_g(U)} \prod_{g \in G''} (-g \cdot g)^{\sigma(U)}$$

to

$$x' = (-U)U \prod_{g \in G''} (-g \cdot g)^{\sigma(U)}.$$

We proceed by induction on $\sigma(U) = k$. There is nothing to show for $k = 2$. Let $k \ge 3$ and set $g_0 = g_{k-1} + g_k$ and $V = \prod_{j=0}^{k-2} g_j$. Since $\sigma(V) < \sigma(U)$ and

$$\prod_{g \in G'} (-g \cdot g)^{v_g(V)} \prod_{g \in G''} (-g \cdot g)^{\sigma(V)}$$

divides x (in $\mathcal{Z}(\mathcal{B}(G))$), the induction hypothesis gives a 3-chain of factorizations from x to

$$(-V)V \prod_{g\in G'} (-g\cdot g)^{v_g(U)-v_g(V)} \prod_{g\in G''} (-g\cdot g)^{\sigma(U)}.$$

If $W = (-g_0 \cdot g_{k-1} \cdot g_k)$, then $VW = U(-g_0 \cdot g_0)$ and for all $g \in G'$ we have

$$v_g(U) - v_g(V) - v_g(W) = -v_g(-g_0 \cdot g_0).$$

Thus

$$\prod_{g\in G'} (-g\cdot g)^{v_g(U)-v_g(V)-v_g(W)} \prod_{g\in G''} (-g\cdot g)^{\sigma(U)} \in \mathcal{B}(G)$$

and we obtain

$$\begin{aligned}
&(-V)V \prod_{g\in G'} (-g\cdot g)^{v_g(U)-v_g(V)} \prod_{g\in G''} (-g\cdot g)^{\sigma(U)} \\
&\quad = (-V)V(-W)W \prod_{g\in G'} (-g\cdot g)^{v_g(U)-v_g(V)-v_g(W)} \prod_{g\in G''} (-g\cdot g)^{\sigma(U)} \\
&\quad = (-V)(-W)U(-g_0\cdot g_0) \prod_{g\in G'} (-g\cdot g)^{-v_g(-g_0\cdot g_0)} \prod_{g\in G''} (-g\cdot g)^{\sigma(U)} \\
&\quad = (-U)U \prod_{g\in G''} (-g\cdot g)^{\sigma(U)}.
\end{aligned}$$

Since the distance of any two subsequent factorizations is bounded by 3, the assertion is proved. ∎

Let $e_1, \ldots, e_r \in G''$ be such that $G = \bigoplus_{i=1}^r \mathbb{Z}e_i$. We may choose r as the maximal p-rank of G, which is the minimal possible r. This makes some subsequent invariants small, but the proof works for all $e_1, \ldots, e_r$.

For $1 \le i \le r$ we set $A(e_i) = e_i^{\mathrm{ord}(e_i)} \in \mathcal{B}(G)$ and for $g \in G' \setminus \{e_1, \ldots, e_r\}$, let $A(g)$ denote the irreducible block in $\mathcal{B}(\{g, e_1, \ldots, e_r\})$ with $v_g(A(g)) = 1$.

Let $B = \prod_{j=1}^k g_j \in \mathcal{B}(G)$ and for $1 \le i \le r$ let $\tau_i(B)$ be defined by

$$\prod_{j=1}^k A(g_j) = B \prod_{i=1}^r A(e_i)^{\tau_i(B)}.$$

Let $1 \le i \le r$. Comparing both sides of the equality shows that

$$\tau_i(B) = \frac{1}{\mathrm{ord}(e_i)} \Big(\sum_{j=1}^k v_{e_i}(A(g_j)) - v_{e_i}(B) \Big)$$

and hence

$$\tau_i(B) \le \frac{1}{\operatorname{ord}(e_i)} k \cdot (\operatorname{ord}(e_i) - 1) \le k - 1.$$

Furthermore, we have

$$\tau_i(BC) = \tau_i(B) + \tau_i(C)$$

for every $C \in \mathcal{B}(G)$.

LEMMA 3.4. *For every* $U = \prod_{j=1}^k g_j \in \mathcal{U}(\mathcal{B}(G'))$ *there exists a* 3*-chain of factorizations from*

$$\prod_{g \in G''} (-g \cdot g)^{r\sigma(U)} \prod_{i=1}^r A(e_i)^{(r+1)\sigma(U)} U$$

to

$$\prod_{g \in G''} (-g \cdot g)^{r\sigma(U)} \prod_{i=1}^r A(e_i)^{(r+1)\sigma(U) - \tau_i(U)} \prod_{j=1}^k A(g_j).$$

Proof. We proceed in 3 steps.

Step 1. Suppose $r = 1$ and let $U \in \mathcal{U}(\mathcal{B}(G'))$ be given. We complete the proof by induction on $k = \sigma(U)$.

For $k = 2$ the assertion holds since

$$A(e_1)(-g_1 \cdot g_1) = A(g_1)A(-g_1).$$

Let $k \ge 3$, $U = \prod_{j=1}^k g_j$, and suppose the assertion holds for all irreducible blocks V with $\sigma(V) < k$. We set $g_0 = g_{k-1} + g_k$, $V = \prod_{j=0}^{k-2} g_j$, and $W = (-g_0 \cdot g_{k-1} \cdot g_k)$. Then $V, W \in \mathcal{U}(\mathcal{B}(G))$ and $U(-g_0 \cdot g_0) = VW$. Hence we infer that

$$\begin{aligned}
&\prod_{g \in G''} (-g \cdot g)^{\sigma(U)} A(e_1)^{2\sigma(U)} U \\
&\quad = \prod_{g \in G''} (-g \cdot g)^{\sigma(V)} A(e_1)^{2\sigma(V)} V A(e_1)^2 \prod_{g \in G'' \setminus \{\pm g_0\}} (-g \cdot g) W \\
&\quad = \prod_{g \in G''} (-g \cdot g)^{\sigma(V)} A(e_1)^{2\sigma(V)} V \\
&\qquad \times \prod_{g \in G'' \setminus \{\pm g_0\}} (-g \cdot g) A(e_1)^{2 - \tau_1(W)} A(-g_0) A(g_{k-1}) A(g_k).
\end{aligned}$$

By the induction hypothesis there is a 3-chain of factorizations to

$$\prod_{g\in G''}(-g\cdot g)^{\sigma(V)}A(e_1)^{2\sigma(V)-\tau_1(V)}$$
$$\times\prod_{j=0}^{k-2}A(g_j)\prod_{g\in G''\setminus\{\pm g_0\}}(-g\cdot g)A(e_1)^{2-\tau_1(W)}A(-g_0)A(g_{k-1})A(g_k)$$
$$=\prod_{g\in G''}(-g\cdot g)^{\sigma(V)}A(e_1)^{2\sigma(V)-\tau_1(V)}$$
$$\times\prod_{j=1}^{k}A(g_j)\prod_{g\in G''\setminus\{\pm g_0\}}(-g\cdot g)(-g_0\cdot g_0)A(e_1)^{2-\tau_1(W)+1}$$
$$=\prod_{g\in G''}(-g\cdot g)^{\sigma(U)}A(e_1)^{2\sigma(U)-\tau_1(U)}\prod_{j=1}^{k}A(g_j).$$

The distance of any two subsequent factorizations is bounded by 3, which implies the assertion.

Step 2. We define a special class of irreducible blocks in $\mathcal{B}(G)$. Let $r\ge 2$, $\emptyset\ne I\subseteq\{1,\dots,r\}$, $\#I\ge 2$, $\emptyset\ne J\subseteq I$, and for $i\in I$ let $0\ne h_i\in\mathbb{Z}e_i$. Let

$$A\Big(\sum_{i\in I}h_i,\ -\sum_{i\in J}h_i\Big)\in\mathcal{B}\Big(\Big\{\sum_{i\in I}h_i,\ -\sum_{i\in J}h_i,\ e_1,\dots,e_r\Big\}\Big)$$

denote the irreducible block which contains the elements $\sum_{i\in I}h_i$ and $-\sum_{i\in J}h_i$ exactly once (i.e.,

$$A\Big(\sum_{i\in I}h_i,\ -\sum_{i\in J}h_i\Big)=\Big(\sum_{i\in I}h_i\Big)\cdot\Big(-\sum_{i\in J}h_j\Big)\cdot\prod_{i\in I\setminus J}e_i^{n_i}\in\mathcal{U}(\mathcal{B}(G'))$$

with exponents $0\le n_i<\mathrm{ord}(e_i)$).

We show that Lemma 3.4 holds for irreducible blocks of the above form. In order to simplify notation, we assume without restriction of generality that $I=\{1,\dots,s\}$ with $2\le s\le r$ and $J=\{1,\dots,\nu\}$ with $1\le\nu\le s$.

We verify the following assertion which is stronger than Lemma 3.4. For every $2\le s\le r$ and every $1\le\nu\le s$, there is a 3-chain of factorizations from

$$z=\prod_{i=1}^{\nu-1}\Big(-\sum_{j=1}^{i}h_j\cdot\sum_{j=1}^{i}h_j\Big)\prod_{i=1}^{\nu}A(e_i)A\Big(\sum_{i=1}^{s}h_i,\ -\sum_{i=1}^{\nu}h_i\Big)$$

to

$$z'=\prod_{i=1}^{\nu-1}\Big(-\sum_{j=1}^{i}h_j\cdot\sum_{j=1}^{i}h_j\Big)A\Big(\sum_{i=1}^{s}h_i\Big)A\Big(-\sum_{i=1}^{\nu}h_i\Big).$$

Let $2 \le s \le r$. We proceed by induction on ν. The assertion holds for $\nu = 1$, since the distance of the two given factorizations equals $\max\{\nu+1, 2\} = 2$. Let $\nu \ge 2$. We pass from $\nu - 1$ to ν. The distance from z to

$$x_1 = \prod_{i=1}^{\nu-2} \Big(-\sum_{j=1}^{i} h_j \cdot \sum_{j=1}^{i} h_j\Big) \prod_{i=1}^{\nu-1} A(e_i) A\Big(\sum_{i=1}^{s} h_i,\ -\sum_{i=1}^{\nu-1} h_i\Big) A\Big(-\sum_{i=1}^{\nu} h_i,\ \sum_{i=1}^{\nu-1} h_i\Big)$$

equals 3. By the induction hypothesis there is a 3-chain of factorizations from x_1 to

$$x_2 = \prod_{i=1}^{\nu-2} \Big(-\sum_{j=1}^{i} h_j \cdot \sum_{j=1}^{i} h_j\Big) A\Big(\sum_{i=1}^{s} h_i\Big) A\Big(-\sum_{i=1}^{\nu-1} h_i\Big) A\Big(-\sum_{i=1}^{\nu} h_i,\ \sum_{i=1}^{\nu-1} h_i\Big).$$

Since the distance between x_2 and z' equals 2, the proof is complete.

Step 3. We treat the general case by induction on r. Step 1 settles the problem for $r = 1$. Suppose $r \ge 2$. We pass from $r-1$ to r. Let

$$U = \prod_{\nu=1}^{j} (g_\nu + h_\nu) \prod_{\nu=j+1}^{k} g_\nu \prod_{\nu=j+1}^{l} h_\nu \in \mathcal{U}(\mathcal{B}(G'))$$

be given with $0 \le j \le k$, $0 \le j \le l$, $0 \ne g_\nu \in \bigoplus_{i=1}^{r-1} \mathbb{Z}e_i$, and $0 \ne h_\nu \in \mathbb{Z}e_r$. If $j = 0$, then either $U \in \mathcal{B}(\bigoplus_{i=1}^{r-1} \mathbb{Z}e_i)$ or $U \in \mathcal{B}(\mathbb{Z}e_r)$ and the assertion follows by the induction hypothesis. So now suppose that $j \ge 1$. Then $k \ge 2$ and $l \ge 2$.

Note for all $1 \le i \le r-1$ that

$$\tau_i(A(g_\nu + h_\nu, -g_\nu)) \le 1 \quad \text{and} \quad \tau_r((-h_\nu \cdot h_\nu)) = 1.$$

(i) First we show that there is a 3-chain of factorizations from

$$z_1 = \prod_{g \in G''} (-g \cdot g)^{r\sigma(U)} \prod_{i=1}^{r} A(e_i)^{(r+1)\sigma(U)} U$$

to a factorization z_2 of the form

$$\begin{aligned} z_2 = xy &\prod_{g \in G''} (-g \cdot g)^{r\sigma(U)} \prod_{\nu=1}^{j} (-g_\nu \cdot g_\nu)^{-1} (-h_\nu \cdot h_\nu)^{-1} \\ &\times \prod_{i=1}^{r-1} A(e_i)^{(r+1)\sigma(U) - \sum_{\nu=1}^{j} \tau_i(A(g_\nu + h_\nu, -g_\nu))} A(e_r)^{(r+1)\sigma(U) - j} \\ &\times \prod_{\nu=1}^{j} A(g_\nu + h_\nu) A(-g_\nu) A(-h_\nu) \end{aligned}$$

for some $x \in \mathcal{Z}(V)$, $y \in \mathcal{Z}(W)$ with $V = \prod_{\nu=1}^{l} h_\nu \in \mathcal{B}(\mathbb{Z}e_r)$ and $W = \prod_{\nu=1}^{k} g_\nu \in \mathcal{B}(\bigoplus_{i=1}^{r-1} \mathbb{Z}e_i)$.

To do so, we define a sequence $(z'_\psi)_{\psi=0}^{j}$ with $z'_0 = z_2$ and $z'_j = z_1$. For every $1 \le \psi \le j$ we verify that there is a 3-chain from z'_ψ to $z'_{\psi-1}$. Let $1 \le \psi \le j$. If

$$\varrho_\psi \in \mathcal{Z}\Big(\prod_{\nu=1}^{\psi}(g_\nu + h_\nu) \prod_{\nu=\psi+1}^{k} g_\nu \prod_{\nu=\psi+1}^{l} h_\nu\Big),$$

then

$$\varrho_{\psi-1} \in \mathcal{Z}\Big(\prod_{\nu=1}^{\psi-1}(g_\nu + h_\nu) \prod_{\nu=\psi}^{k} g_\nu \prod_{\nu=\psi}^{l} h_\nu\Big)$$

should be the factorization which arises by replacing $g_\psi + h_\psi$ by $g_\psi \cdot h_\psi$. Obviously, $\varrho_j = U$ and $\varrho_0 \in \mathcal{Z}(VW)$.

Now we define, for all $0 \le \psi \le j$,

$$\begin{aligned} z'_\psi = \varrho_\psi &\prod_{g\in G''} (-g\cdot g)^{r\sigma(U)} \prod_{\nu=\psi+1}^{j} (-g_\nu \cdot g_\nu)^{-1}(-h_\nu \cdot h_\nu)^{-1} \\ &\times \prod_{i=1}^{r-1} A(e_i)^{(r+1)\sigma(U) - \sum_{\nu=\psi+1}^{j} \tau_i(A(g_\nu + h_\nu, -g_\nu))} A(e_r)^{(r+1)\sigma(U)-(j-\psi)} \\ &\times \prod_{\nu=\psi+1}^{j} A(g_\nu + h_\nu) A(-g_\nu) A(-h_\nu). \end{aligned}$$

Let $1 \le \psi \le j$. By definition of ϱ_ψ we have $d(z'_\psi, z''_\psi) \le 3$ with

$$\begin{aligned} z''_\psi = \varrho_{\psi-1}&\big((g_\psi + h_\psi)\cdot(-g_\psi)\cdot(-h_\psi)\big) \\ &\times \prod_{g\in G''} (-g\cdot g)^{r\sigma(U)} \prod_{\nu=\psi}^{j} (-g_\nu \cdot g_\nu)^{-1}(-h_\nu \cdot h_\nu)^{-1} \\ &\times \prod_{i=1}^{r-1} A(e_i)^{(r+1)\sigma(U) - \sum_{\nu=\psi+1}^{j} \tau_i(A(g_\nu + h_\nu, -g_\nu))} A(e_r)^{(r+1)\sigma(U)-(j-\psi)} \\ &\times \prod_{\nu=\psi+1}^{j} A(g_\nu + h_\nu) A(-g_\nu) A(-h_\nu). \end{aligned}$$

Next we have $d(z''_\psi, z'''_\psi) \le 2$ with

$$\begin{aligned} z'''_\psi = \varrho_{\psi-1} &A(g_\psi + h_\psi, -g_\psi) A(-h_\psi) A(e_r)^{-1} \\ &\times \prod_{g\in G''} (-g\cdot g)^{r\sigma(U)} \prod_{\nu=\psi}^{j} (-g_\nu \cdot g_\nu)^{-1}(-h_\nu \cdot h_\nu)^{-1} \end{aligned}$$

$$\times \prod_{i=1}^{r-1} A(e_i)^{(r+1)\sigma(U)-\sum_{\nu=\psi+1}^{j}\tau_i(A(g_\nu+h_\nu,-g_\nu))} A(e_r)^{(r+1)\sigma(U)-(j-\psi)}$$

$$\times \prod_{\nu=\psi+1}^{j} A(g_\nu+h_\nu)A(-g_\nu)A(-h_\nu).$$

By Step 2 there is a 3-chain from z'''_ψ to

$$\begin{aligned} z'_{\psi-1} = {} & \varrho_{\psi-1} A(g_\psi+h_\psi)A(-g_\psi)A(-h_\psi)A(e_r)^{-1} \\ & \times \prod_{g\in G''}(-g\cdot g)^{r\sigma(U)} \prod_{\nu=\psi}^{j}(-g_\nu\cdot g_\nu)^{-1}(-h_\nu\cdot h_\nu)^{-1} \\ & \times \prod_{i=1}^{r-1} A(e_i)^{(r+1)\sigma(U)-\sum_{\nu=\psi}^{j}\tau_i(A(g_\nu+h_\nu,-g_\nu))} A(e_r)^{(r+1)\sigma(U)-(j-\psi)} \\ & \times \prod_{\nu=\psi+1}^{j} A(g_\nu+h_\nu)A(-g_\nu)A(-h_\nu). \end{aligned}$$

(ii) Since

$$A(e_r)^{2\sigma(V)} \mid A(e_r)^{(r+1)\sigma(U)-j}$$

and

$$\prod_{g\in G''\cap\mathbb{Z}e_r}(-g\cdot g)^{\sigma(V)} \mid \prod_{g\in G''}(-g\cdot g)^{r\sigma(U)}\prod_{\nu=1}^{j}(-g_\nu\cdot g_\nu)^{-1}(-h_\nu\cdot h_\nu)^{-1},$$

Step 1 may be applied $\sigma(x)$ times and we obtain a 3-chain of factorizations from z_2 to

$$\begin{aligned} z_3 = {} & \prod_{g\in G''}(-g\cdot g)^{r\sigma(U)}\prod_{\nu=1}^{j}(-g_\nu\cdot g_\nu)^{-1}(-h_\nu\cdot h_\nu)^{-1} \\ & \times \prod_{i=1}^{r-1} A(e_i)^{(r+1)\sigma(U)-\sum_{\nu=1}^{j}\tau_i(A(g_\nu+h_\nu,-g_\nu))} A(e_r)^{(r+1)\sigma(U)-j-\tau_r(V)} \\ & \times \prod_{\nu=1}^{j}[A(g_\nu+h_\nu)A(-g_\nu)A(-h_\nu)]\prod_{\nu=1}^{l}A(h_\nu)y. \end{aligned}$$

(iii) Since

$$\prod_{i=1}^{r-1} A(e_i)^{r\sigma(W)} \mid \prod_{i=1}^{r-1} A(e_i)^{(r+1)\sigma(U)-\sum_{\nu=1}^{j}\tau_i(A(g_\nu+h_\nu,-g_\nu))}$$

and

$$\prod_{g\in G''\cap\bigoplus_{i=1}^{r-1}\mathbb{Z}e_i}(-g\cdot g)^{(r-1)\sigma(W)} \mid \prod_{g\in G''}(-g\cdot g)^{r\sigma(U)}\prod_{\nu=1}^{j}(-g_\nu\cdot g_\nu)^{-1}(-h_\nu\cdot h_\nu)^{-1},$$

we may apply the induction hypothesis $\sigma(y)$ times and obtain a 3-chain of factorizations from z_3 to

$$\begin{aligned}
z_4 = &\prod_{g\in G''}(-g\cdot g)^{r\sigma(U)}\prod_{\nu=1}^{j}(-g_\nu\cdot g_\nu)^{-1}(-h_\nu\cdot h_\nu)^{-1}\\
&\times\prod_{i=1}^{r-1}A(e_i)^{(r+1)\sigma(U)-\sum_{\nu=1}^{j}\tau_i(A(g_\nu+h_\nu,-g_\nu))-\tau_i(W)}\\
&\times A(e_r)^{(r+1)\sigma(U)-j-\tau_r(V)}\\
&\times\prod_{\nu=1}^{j}[A(g_\nu+h_\nu)A(-g_\nu)A(-h_\nu)]\prod_{\nu=1}^{l}A(h_\nu)\prod_{\nu=1}^{k}A(g_\nu).
\end{aligned}$$

(iv) Because (for $1\le\nu\le j$)

$$\begin{aligned}
&2\sigma((-h_\nu\cdot h_\nu))-\tau_r((-h_\nu\cdot h_\nu))\\
&\qquad\qquad= 3\le 3(k+l-j)-j-(l-1)\le 3\sigma(U)-j-\tau_r(V)\\
&\qquad\qquad\le (r+1)\sigma(U)-j-\tau_r(V),
\end{aligned}$$

we have

$$A(e_r)^{2\sigma((-h_\nu\cdot h_\nu))-\tau_r((-h_\nu\cdot h_\nu))}\mid A(e_r)^{(r+1)\sigma(U)-j-\tau_r(V)}$$

and clearly

$$\prod_{g\in G''\cap\mathbb{Z}e_r}(-g\cdot g)^{\sigma((-h_\nu\cdot h_\nu))}\mid\prod_{g\in G''}(-g\cdot g)^{r\sigma(U)}\prod_{\mu=1}^{j}(-g_\mu\cdot g_\mu)^{-1}\prod_{\mu=1}^{j}(-h_\mu\cdot h_\mu)^{-1}.$$

Furthermore (for $1\le\nu\le j$),

$$\begin{aligned}
&r\sigma((-g_\nu\cdot g_\nu))-\tau_i((-g_\nu\cdot g_\nu))\\
&\qquad\qquad= 2r-1\le (r+1)(k+l-j)-j-(k-1)\\
&\qquad\qquad\le (r+1)\sigma(U)-\sum_{\mu=1}^{j}\tau_i(A(g_\mu+h_\mu,-g_\mu))-\tau_i(W)
\end{aligned}$$

and hence

$$\prod_{i=1}^{r-1} A(e_i)^{r\sigma((-g_\nu\cdot g_\nu))-\tau_i((-g_\nu\cdot g_\nu))} \mid$$
$$\prod_{i=1}^{r-1} A(e_i)^{(r+1)\sigma(U)-\sum_{\mu=1}^{j}\tau_i(A(g_\mu+h_\mu,-g_\mu))-\tau_i(W)}.$$

Obviously,

$$\prod_{g\in G''\cap\bigoplus_{i=1}^{r-1}\mathbb{Z}e_i} (-g\cdot g)^{(r-1)\sigma((-g_\nu\cdot g_\nu))} \mid$$
$$\prod_{g\in G''}(-g\cdot g)^{r\sigma(U)}\prod_{\mu=1}^{j}(-g_\mu\cdot g_\mu)^{-1}(-h_\mu\cdot h_\mu)^{-1}.$$

Therefore, by the induction hypothesis there is a 3-chain of factorizations from z_4 to

$$\begin{aligned} z_5 = &\prod_{g\in G''}(-g\cdot g)^{r\sigma(U)}\\ &\times\prod_{i=1}^{r-1}A(e_i)^{(r+1)\sigma(U)-\sum_{\nu=1}^{j}\tau_i(A(g_\nu+h_\nu,-g_\nu))-\tau_i(W)+\sum_{\nu=1}^{j}\tau_i((-g_\nu\cdot g_\nu))}\\ &\times A(e_r)^{(r+1)\sigma(U)-j-\tau_r(V)+\sum_{\nu=1}^{j}\tau_r((-h_\nu\cdot h_\nu))}\\ &\times\prod_{\nu=1}^{j}A(g_\nu+h_\nu)\prod_{\nu=j+1}^{l}A(h_\nu)\prod_{\nu=j+1}^{k}A(g_\nu). \end{aligned}$$

Since, for $1\le i\le r-1$,

$$-\sum_{\nu=1}^{j}\tau_i(A(g_\nu+h_\nu,-g_\nu))-\tau_i(W)+\sum_{\nu=1}^{j}\tau_i((-g_\nu\cdot g_\nu))=-\tau_i(U)$$

and

$$-j-\tau_r(V)+\sum_{\nu=1}^{j}\tau_r((-h_\nu\cdot h_\nu))=-\tau_r(U),$$

the proof of Lemma 3.4 is complete. ■

Proof of Theorem 3.1. By [Ge3; Proposition 4.2] it is sufficient to prove the assertion for $\mathcal{B}(G)$ instead of H. We set

$$A^*=\prod_{g\in G'}g^{\mathrm{ord}(g)}\prod_{g\in G''}(-g\cdot g)^{n_g},$$

where

$$n_g=\begin{cases} r\mathcal{D}(G)+s\,\mathrm{ord}(e_i) & \text{if } g=e_i \text{ for some } 1\le i\le r,\\ r\mathcal{D}(G) & \text{otherwise,}\end{cases}$$

with $s=(r+1)\mathcal{D}(G)+(\mathcal{D}(G)-1)(c(G)-1)$.

Let $A \in \mathcal{B}(G)$ with $A^* \mid A$. Since $(0) \in \mathcal{B}(G)$ is a prime element in $\mathcal{B}(G)$, we may suppose without restriction of generality that $v_0(A) = 0$ (i.e., $A \in \mathcal{B}(G'))$. We have to show that for any two factorizations $z, z' \in \mathcal{Z}(A)$ there is a 3-chain of factorizations from z to z'.

There is some $B \in \mathcal{B}(G)$ such that

$$\prod_{g \in G''} (-g \cdot g)^{r\mathcal{D}(G)} \prod_{i=1}^{r} A(e_i)^s B = A.$$

We define a subset $Z \subseteq \mathcal{Z}(A)$ as

$$Z = \Big\{ \prod_{g \in G''} (-g \cdot g)^{r\mathcal{D}(G)} \prod_{i=1}^{r} A(e_i)^s y : y \in \mathcal{Z}(B) \Big\}.$$

We proceed in two steps which immediately imply the assertion.

Step 1. *For every $z \in \mathcal{Z}(A)$ there is a 3-chain of factorizations to some $z' \in Z$.*

Proof. Let $z \in \mathcal{Z}(A)$ be given. By Lemma 3.2 there is a 3-chain of factorizations from z to

$$z' = \prod_{g \in G''} (-g \cdot g)^{n_g} y' = \prod_{g \in G''} (-g \cdot g)^{r\mathcal{D}(G)} \prod_{i=1}^{r} (-e_i \cdot e_i)^{s \cdot \mathrm{ord}(e_i)} y' \in \mathcal{Z}(A)$$

for some $y' \in \mathcal{Z}(\mathcal{B}(G))$. By Lemma 3.3 there is a 3-chain of factorizations from z' to

$$\begin{aligned} z'' &= \prod_{g \in G''} (-g \cdot g)^{r\mathcal{D}(G)} \prod_{i=1}^{r} (-A(e_i))^s A(e_i)^s y' \\ &= \prod_{g \in G''} (-g \cdot g)^{r\mathcal{D}(G)} \prod_{i=1}^{r} A(e_i)^s y'' \end{aligned}$$

with $y'' \in \mathcal{Z}(B)$, and hence $z'' \in Z$.

Step 2. *For any two factorizations $z, z' \in Z$ there is a 3-chain of factorizations from z to z'.*

Proof. Let

$$z = \prod_{g \in G''} (-g \cdot g)^{r\mathcal{D}(G)} \prod_{i=1}^{r} A(e_i)^s y \in Z$$

and

$$z' = \prod_{g \in G''} (-g \cdot g)^{r\mathcal{D}(G)} \prod_{i=1}^{r} A(e_i)^s y' \in Z$$

be given with $y, y' \in \mathcal{Z}(B)$. There exist factorizations $y = y_0, y_1, \ldots, y_m = y' \in \mathcal{Z}(B)$ with $d(y_l, y_{l+1}) \le c(G)$ for every $0 \le l \le m-1$. Hence we have to verify that there is a 3-chain of factorizations from

$$z_l = \prod_{g \in G''} (-g \cdot g)^{r\mathcal{D}(G)} \prod_{i=1}^{r} A(e_i)^s y_l$$

to

$$z_{l+1} = \prod_{g \in G''} (-g \cdot g)^{r\mathcal{D}(G)} \prod_{i=1}^{r} A(e_i)^s y_{l+1}$$

for every $0 \le l \le m-1$. Let $l \in \{0, \ldots, m-1\}$ and suppose $y_l = xU_1 \ldots U_\lambda$, $y_{l+1} = xV_1 \ldots V_\mu$ with $x \in \mathcal{Z}(\mathcal{B}(G))$, $U_1, \ldots, U_\lambda, V_1, \ldots V_\mu \in \mathcal{U}(\mathcal{B}(G))$, $\lambda \le c(G)$, $\mu \le c(G)$ and

$$U_1 \ldots U_\lambda = V_1 \ldots V_\mu = \prod_{j=1}^{k} g_j.$$

Since for every U_ν we have $\sigma(U_\nu) \le \mathcal{D}(G)$, $\tau_i(U_\nu) \le \mathcal{D}(G) - 1$, and $s = (r+1)\mathcal{D}(G) + (\mathcal{D}(G)-1)(c(G)-1)$, Lemma 3.4 may be applied $\lambda \le c(G)$ times to obtain a 3-chain of factorizations from z_l to

$$z'' = \prod_{g \in G''} (-g \cdot g)^{r\mathcal{D}(G)} \prod_{i=1}^{r} A(e_i)^{s - \tau_i(\prod_{j=1}^{k} g_j)} \prod_{j=1}^{k} A(g_j) x.$$

For the same reasons there is a 3-chain of factorizations from z_{l+1} to z'' and the proof is complete. ■

4. Arithmetical order formations. In this section we give a quantitative interpretation of Theorem 3.1 for orders in global fields (see Theorems 4.3 and 4.4). To do so we rely entirely on the methods developed in [G-HK-K]. We recall the necessary notions and results, for all details we refer to [G-HK-K].

For two real-valued functions f, g we write $f \asymp g$ if $f \ll g$ and $g \ll f$; furthermore, $f \sim g$ means that

$$\lim_{x \to \infty} \frac{f(x)}{g(x)} = 1.$$

We use that branch of the complex logarithm which is real for positive arguments. By a *norm function* on a reduced monoid H, we mean a monoid homomorphism $|\cdot| : H \to \mathbb{N}_+$ satisfying $|a| = 1$ if and only if $a = 1$.

DEFINITION 4.1. An *arithmetical order formation* $[\mathcal{F}(P), T, H, |\cdot|]$ (of rank $r \in \mathbb{N}_+$) consists of a free abelian monoid $\mathcal{F}(P)$, a reduced monoid T, a submonoid $H \subseteq \mathcal{F}(P) \times T$, where the inclusion $H \hookrightarrow \mathcal{F}(P) \times T$ is a divisor homomorphism, and a norm function $|\cdot| : \mathcal{F}(P) \times T \to \mathbb{N}_+$ such that the following conditions are satisfied:

(a) $G = \mathcal{F}(P) \times T/H$ is a finite abelian group, called the *class group* of the formation.

(b) 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 $s = 1$ and such that

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

(c) $\#\{t \in T : |t| \leq x\} \ll (\log x)^r$.

Remark. Let $[\mathcal{F}(P), T, H, |\cdot|]$ be an arithmetical order formation with class group G. Then $H \cap \mathcal{F}(P) \hookrightarrow \mathcal{F}(P)$ is a divisor theory with class group G and each class contains infinitely many prime divisors. In particular, $H \cap \mathcal{F}(P)$ is a reduced Krull monoid (cf. [G-HK-K; Lemma 1]).

The most important examples of arithmetical order formations arise from orders in global fields which we will discuss briefly (for details and for other examples see [G-HK-K; §3]).

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 and for $v \in \mathcal{S}(K)$ let R_v be the corresponding valuation domain. For a finite subset $S \subset \mathcal{S}(K)$, with $S \neq \emptyset$ in the function field case,

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

is called the *holomorphy ring of K associated with S*. R_S is a Dedekind domain with quotient field K. A subring $\mathfrak{o} \subseteq R_S$ is called an *order* in R_S if R_S is a finitely generated $\mathfrak{o}$-module and $\mathfrak{o}$ has quotient field K (equivalently, $R_S/\mathfrak{o}$ is a finitely generated torsion $\mathfrak{o}$-module).

Let K be a global field, $R \subseteq K$ a holomorphy ring and $\mathfrak{o} \subseteq R$ an order. Then $\mathfrak{o}$ is a one-dimensional noetherian domain with finite Picard group, R is the integral closure of $\mathfrak{o}$ in K and R is a finitely generated $\mathfrak{o}$-module. Hence $\mathfrak{o}$ is a weakly Krull domain satisfying all assumptions of [Ge3; Theorem 7.3; see Lemmata 7.6 and 7.7 therein]. Thus $c(\mathfrak{o}^\bullet) < \infty$.

Let $\mathfrak{f}$ denote the conductor of $R/\mathfrak{o}$ and let $r \geq 0$ be the number of distinct prime ideals of R dividing $\mathfrak{f}$. We set $P = \{\mathfrak{p} \in X^{(1)}(\mathfrak{o}) \mid \mathfrak{p} \not\supset \mathfrak{f}\}$ and $T \subseteq \mathcal{I}(\mathfrak{o})$ is the submonoid generated by the sets $\Omega(\mathfrak{p})$ for those $\mathfrak{p} \in X^{(1)}(\mathfrak{o})$ with $\mathfrak{p} \supset \mathfrak{f}$ (see [Ge3; Section 7] for the necessary definitions). Then $\mathcal{I}(\mathfrak{o}) = \mathcal{F}(P) \times T$. For an ideal $I \in \mathcal{I}(\mathfrak{o})$ we set $|I| = (\mathfrak{o} : I)$ and let $H = \mathcal{H}(\mathfrak{o}) \subseteq \mathcal{I}(\mathfrak{o})$ denote the submonoid of principal ideals. Then $[\mathcal{F}(P), T, H, |\cdot|]$ is an arithmetical order formation of rank r.

Let $[\mathcal{F}(P), T, H, |\cdot|]$ be an arithmetical order formation with class group G. Let $\boldsymbol{\beta} : \mathcal{F}(P) \times T \to \mathcal{F}(G) \times T$ denote the block homomorphism and for $g \in G$ let $\mathcal{B}_g(G) = \{S \in \mathcal{F}(G) : Sg \in \mathcal{B}(G)\}$. For a non-empty subset $Q \subseteq G$ and a function $\sigma : G\backslash Q \to \mathbb{N}$ we set

$$\Omega(Q,\sigma) = \{S \in \mathcal{F}(G) : v_g(S) = \sigma(g) \text{ for all } g \in G\backslash Q\}.$$

For any subset $Z \subseteq \mathcal{F}(P) \times T$ and for $x \in \mathbb{R}_{\geq 0}$ let

$$Z(x) = \{a \in Z : |a| \leq x\}.$$

PROPOSITION 4.2. *Let all notations be as above, and let $g \in G$ be such that $\Omega(Q,\sigma) \cap \mathcal{B}_g(G) \neq \emptyset$. Then, for x tending to infinity, we have*

$$\#\{a \in \mathcal{F}(P) : \boldsymbol{\beta}(a) \in \Omega(Q,\sigma) \cap \mathcal{B}_g(G),\ |a| \leq x\} \asymp x(\log x)^{-\eta}(\log\log x)^d$$

with $\eta = \#(G\backslash Q)/\#G$ and $d = \sum_{g \in G\backslash Q} \sigma(g)$.

Proof. This is a special case of Proposition 8 in [G-HK-K]. ∎

THEOREM 4.3. *Let $[\mathcal{F}(P), T, H, |\cdot|]$ be an arithmetical order formation. Then, for x tending to infinity, we have*

$$\#\{a \in H : c(a) \leq 3,\ |a| \leq x\} \asymp x.$$

Proof. Let $G = \mathcal{F}(P) \times T/H$ denote the class group of the formation. By the remark after Definition 4.1, $H \cap \mathcal{F}(P)$ is a reduced Krull monoid and each class contains a prime divisor. Hence by Theorem 3.1 there exists an element $A^* \in \mathcal{B}(G)$ such that

$$\begin{aligned}(1)\qquad H &\supseteq \{a \in H : c(a) \leq 3\}\\ &\supseteq \{a \in H \cap \mathcal{F}(P) : c(a) \leq 3\}\\ &\supseteq \{a \in H \cap \mathcal{F}(P) : A^* \mid \boldsymbol{\beta}(a)\} \qquad \text{(by Theorem 3.1)}\\ &\supseteq (H \cap \mathcal{F}(P)) \backslash \bigcup_{g \in G} \bigcup_{i=0}^{v_g(A^*)-1} \{a \in H \cap \mathcal{F}(P) : v_g(\boldsymbol{\beta}(a)) = i\}.\end{aligned}$$

For $t \in T$ we set

$$H_t = \{a \in \mathcal{F}(P) : at \in H\} = \{a \in \mathcal{F}(P) : \boldsymbol{\beta}(a) \in \Omega(G,0) \cap \mathcal{B}_{\boldsymbol{\beta}(t)}(G)\}$$

and

$$H_t(x) = C(t,x) \cdot x$$

for a function $C : T \times (0,\infty) \to [0,\infty)$. Proposition 4.2 implies that for every $t \in T$ and for x tending to infinity,

$$H_t(x) \asymp x, \tag{2}$$

whence $C(t,x) \asymp 1$. Since for $t, t' \in T$ with $\boldsymbol{\beta}(t) = \boldsymbol{\beta}(t')$ we have $H_t = H_{t'}$, there are at most $\#G$ distinct functions $H_t(x)$. Therefore the function C is bounded. Thus by Proposition 5 of [G-HK-K] it follows that

$$H(x) \asymp x. \tag{3}$$

In case $t = 1$, (2) means that

$$H_1(x) = (H \cap \mathcal{F}(P))(x) \asymp x. \tag{4}$$

If $\#G = 1$, then $\{a \in H \cap \mathcal{F}(P) : c(a) \le 3\} = H \cap \mathcal{F}(P)$, whence the assertion follows from (1), (3) and (4).

Now suppose $\#G > 1$. For $g \in G$ and $i \in \mathbb{N}$ we set $Q = G \setminus \{g\}$ and define the function $\sigma : G \setminus Q = \{g\} \to \mathbb{N}$ by $\sigma(g) = i$. Then $\emptyset \ne Q$ and by Proposition 4.2 we infer that

$$\begin{aligned} (5)\qquad \#\{a \in H \cap \mathcal{F}(P) : v_g(\boldsymbol{\beta}(a)) = i,\ |a| \le x\} \\ = \#\{a \in \mathcal{F}(P) : \boldsymbol{\beta}(a) \in \Omega(Q,\sigma) \cap \mathcal{B}(G),\ |a| \le x\} \\ \asymp x(\log x)^{-1/\#G}(\log\log x)^i. \end{aligned}$$

Thus the assertion follows from (1), (3), (4) and (5). ∎

For rings of integers in algebraic number fields we obtain an essentially stronger asymptotic result.

THEOREM 4.4. *Let K be an algebraic number field, $R \subseteq K$ the ring of integers and G its ideal class group. Then $c(R^\bullet) \le \mathcal{D}(G)$ and*

$$\begin{aligned} \#\{aR : a \in R^\bullet,\ (R : aR) \le x\} \sim \#\{aR : a \in R^\bullet,\ c(a) \le 3,\ (R : aR) \le x\} \\ = \left(\frac{1}{\#G}\varrho_K + O\left(\frac{(\log\log x)^M}{(\log x)^{1/\#G}}\right)\right) \cdot x, \end{aligned}$$

where ϱ_K denotes the residue of Dedekind's zeta function of K at $s = 1$ and $M = \max\{0, v_g(A^*) - 1 : g \in G\}$ with $A^* \in \mathcal{B}(G)$ satisfying the conclusions of Theorem 3.1.

Proof. Clearly, R is a Dedekind domain, $H = \mathcal{H}(R) \hookrightarrow \mathcal{I}(R)$ is a divisor theory with divisor class group G and each class contains a prime ideal. Hence

$$c(R^\bullet) \le \mathcal{D}(G)$$

by [Ge3; Propositions 4.2 and 4.3].

Relation (1) in the proof of Theorem 4.3 reduces to

$$H \supseteq \{a \in H : c(a) \le 3\} \supseteq H \setminus \bigcup_{g \in G} \bigcup_{i=0}^{v_g(A^*)-1} \{a \in H : v_g(\boldsymbol{\beta}(a)) = i\}.$$

Since

$$H(x) = \frac{1}{\#G}\varrho_K x + O(x^{1-1/[K:\mathbb{Q}]})$$

(cf. [La; p. 132 and p. 161]), the assertion follows from relation (5) in the proof of Theorem 4.3. ∎

REFERENCES

[Ch] S. Chapman, *On the Davenport constant*, *the Cross number*, *and their application in factorization theory*, in: Zero-Dimensional Commutative Rings, Lecture Notes in Pure and Appl. Math. 171, Marcel Dekker, 1995, 167–190.

[Ge1] A. Geroldinger, *Über nicht-eindeutige Zerlegungen in irreduzible Elemente*, Math. Z. 197 (1988), 505–529.

[Ge2] —, *Factorizations of algebraic integers*, in: Number Theory, Lecture Notes in Math. 1380, Springer, 1989, 63–74.

[Ge3] —, *Chains of factorizations in weakly Krull domains*, this volume, 53–81.

[G-HK-K] A. Geroldinger, F. Halter-Koch and J. Kaczorowski, *Non-unique factorizations in orders of global fields*, J. Reine Angew. Math. 459 (1995), 89–118.

[La] S. Lang, *Algebraic Number Theory*, Grad. Texts in Math. 110, Springer, 1986.

[Na] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, Springer, 1990.

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

Institut für Mathematik
Karl-Franzens-Universität
Heinrichstraße 36
8010 Graz, Austria
E-mail: alfred.geroldinger@kfunigraz.ac.at

Received 23 October 1995