COLLOQUIUM MATHEMATICUM

VOL. 92 2002 NO. 2

FACTORIZATION PROPERTIES OF KRULL MONOIDS WITH INFINITE CLASS GROUP

BY

WOLFGANG HASSLER (Graz)

Abstract. For a non-unit a of an atomic monoid H we call

$$L_H(a) = \{k \in \mathbb{N} \mid a = u_1 \ldots u_k \text{ with irreducible } u_i \in H\}$$

the set of lengths of a. Let H be a Krull monoid with infinite divisor class group such that each divisor class is the sum of a bounded number of prime divisor classes of H. We investigate factorization properties of H and show that H has sets of lengths containing large gaps. Finally we apply this result to finitely generated algebras over perfect fields with infinite divisor class group.

1. Introduction. In this paper, a *monoid* H is a commutative and cancellative semigroup with unit element. We usually write H multiplicatively and we denote by $H^\times$ the group of units of H.

A monoid H is said to be *atomic* if every $h \in H \setminus H^\times$ has a factorization

$$h = u_1 \ldots u_k \tag{1}$$

into irreducible elements (*atoms*) u_i of H. We say that k is the *length* of the factorization (1) and we call

$$L_H(h) = \{k \in \mathbb{N} \mid k \text{ is the length of some factorization of } h\} \subset \mathbb{N}$$

the *set of lengths* of h. We denote by

$$\mathcal{L}(H) = \{L_H(h) \mid h \in H \setminus H^\times\}$$

the set of all sets of lengths of H.

Clearly, H is factorial if and only if (1) is unique up to associates and up to order for each $h \in H$. If H is not factorial the problem arises to describe and classify the occurring phenomena of non-uniqueness of factorizations. A first coarse measure for this non-uniqueness is the *elasticity*

$$\varrho(H) = \sup\left\{\frac{\sup L_H(h)}{\min L_H(h)} \,\middle|\, h \in H \setminus H^\times\right\} \in \mathbb{R}_{\geq 1} \cup \{\infty\}.$$

This is a frequently investigated invariant and there is an extensive bibliography about it; for a survey see [3]. Unfortunately, the elasticity does not contain any information about the structure of $L_H(h)$ between $\min L_H(h)$

2000 *Mathematics Subject Classification*: 13F05, 13A05, 13C20, 20M14.

and $\sup L_H(h)$. In the following we consider an invariant which measures the size of the "gaps" between elements of $L_H(h)$.

Recall that an atomic monoid H is called a *BF-monoid* if $L_H(h)$ is a finite set for every $h \in H \setminus H^\times$. By [2], Proposition 2.2, every Krull monoid (see for example [4]) and the monoid $R \setminus \{0\}$ of nonzero elements of every noetherian domain R is a BF-monoid.

For an arbitrary set A we denote by $\mathbb{P}_{\mathrm{fin}}(A)$ the set of finite subsets of A.

Let $L = \{l_1, \ldots, l_r\} \in \mathbb{P}_{\mathrm{fin}}(\mathbb{Z})$ where $l_1 < \ldots < l_r$. Then we call

$$\Delta(L) = \{l_i - l_{i-1} \mid 2 \le i \le r\}$$

the *set of differences* of L (note that $\Delta(L)$ is empty if and only if $|L| \le 1$), and we call

$$\Delta(H) = \bigcup_{h \in H \setminus H^\times} \Delta(L_H(h))$$

the *set of differences* of a BF-monoid H (see also [4]).

Let H be a Krull monoid. If the class group of H is finite, then all sets of lengths of H are, up to bounded initial and final segments, arithmetical multiprogressions with bounded sets of differences (see [4], Theorem 2.13). In particular this implies that $\Delta(H)$ is a finite set.

If on the other hand H is a Krull monoid with infinite class group and if each divisor class of H is a prime divisor class, then every non-empty finite set $L \subset \mathbb{N}_{\ge 2}$ is contained in $\mathcal{L}(H)$ (see [7]).

In this paper we study sets of lengths of Krull monoids H with infinite class group such that every class is the sum of a bounded number of prime divisor classes. Such Krull monoids occur in a natural way in the study of finitely generated algebras over perfect fields (see Section 2).

Let G be an abelian group and $G_0 \subset G$ a subset. We set

$$G_0(m) = \{g_1 + \ldots + g_r \mid r \le m,\ g_i \in G_0\}.$$

Our main result where we prove the existence of "thin" sets of lengths (which in particular implies that $\Delta(H)$ is infinite) reads as follows:

THEOREM 1.1. *Let H be a Krull monoid with infinite class group G and let $G_0 \subset G$ denote the set of prime divisor classes. If $G = G_0(m)$ for some $m \in \mathbb{N}$ then there exists some constant $K \in \mathbb{N}$ such that for all $N \in \mathbb{N}$ there exists some $L \in \mathcal{L}(H)$ with* $\min L \le K$, $|L| \le K$ *and* $\max L > N$. *In particular*, $\Delta(H)$ *is an infinite set.*

The organization of the paper is as follows: In Section 2 we apply Theorem 1.1 to finitely generated algebras over perfect fields. Section 3 is entirely devoted to the proof of Theorem 1.1.

2. Finitely generated domains. Let H be a monoid. We denote by $\mathcal{Q}(H)$ the quotient group of H. A monoid homomorphism $\varphi : H \to D$ is called a *divisor homomorphism* if $\varphi(a) \mid \varphi(b)$ implies $a \mid b$ for all $a, b \in H$. In this case φ induces a monomorphism $\mathcal{Q}(H)/H^\times \to \mathcal{Q}(D)/D^\times$ whose cokernel $\mathcal{C}(\varphi)$ is called the (*divisor*) *class group* of φ. It is always written additively. For each $d \in \mathcal{Q}(D)$ we denote by $[d]_\varphi$ its image under the canonical map $\mathcal{Q}(D) \to \mathcal{C}(\varphi)$. We call the elements of $\{[p]_\varphi \mid p \in D \text{ is prime}\}$ the *prime divisor classes* of φ.

For an integral domain R we set $R^\bullet = R \setminus \{0\}$, $R^\# = R^\bullet/R^\times$ and $\Delta(R) = \Delta(R^\bullet)$.

Let R be a noetherian integral domain whose integral closure $\overline{R}$ is a finitely generated R-module. Let

$$S = R^\bullet \setminus \bigcup_{\mathfrak{p} \in A} \mathfrak{p},$$

where $A = \mathrm{Ass}_R(\overline{R}/R)$, denote the set of non-zero divisors of $\overline{R}/R$. Set

$$P(R) = \{\mathfrak{p} \in \mathrm{spec}(R) \mid \mathrm{ht}(\mathfrak{p}) = 1,\ \mathfrak{p} \cap S \neq \emptyset\}.$$

Then $R_\mathfrak{p}$ is a discrete valuation domain for every $\mathfrak{p} \in P(R)$ (see [5], Lemma 2). Thus $\prod_{\mathfrak{p} \in P(R)} R_\mathfrak{p}^\#$ can be canonically identified with the free abelian monoid $\mathcal{F}(P(R))$ with basis $P(R)$ (see also formula (2) in Section 3). The natural maps $R^\bullet \to R_\mathfrak{p}^\#$ and $R^\bullet \to R_S^\#$ induce a divisor homomorphism (see [5], Theorem 1) $\partial_R : R^\bullet \to \mathcal{F}(P(R)) \times R_S^\#$ whose class group $\mathcal{C}(R)$ is called the *divisor class group* of R.

By restricting ∂_R to S we obtain a divisor homomorphism $\partial_R|_S : S \to \mathcal{F}(P(R))$ whose class group and set of prime divisor classes naturally coincide with those of R (see [5], Remark 4 to Theorem 1). In fact, S is a Krull monoid with divisor theory $\partial_R|_S$ and thus the set of prime divisor classes generates the class group of R as a monoid.

THEOREM 2.1. *Let R be a domain which is a finitely generated algebra over some perfect field. If R has infinite divisor class group then there exists some $K \in \mathbb{N}$ such that for all $N \in \mathbb{N}$ there exists some $L \in \mathcal{L}(R)$ with $\min L \le K$, $|L| \le K$ and $\max L > N$. In particular, $\Delta(R)$ is an infinite set.*

Proof. Let G denote the class group of R and let G_0 be the set of prime divisor classes. If R is finitely generated over some infinite perfect field then $G = G_0(m)$ for some $m \in \mathbb{N}$ by [6], Proposition 4.2. If R is a finitely generated algebra over a finite field we again have $G = G_0(m)$ for some $m \in \mathbb{N}$ by the remark after Corollary 4.1 in [6].

Since the set S of non-zero divisors of $\overline{R}/R$ is a divisor closed submonoid of $R^\bullet$, the assertion follows immediately from Theorem 1.1 and the above considerations. ∎

It is well known from [8], Theorem 3, that if a domain R is a finitely generated algebra over an infinite perfect field with $\dim(R) \ge 2$, then each divisor class of R is a prime divisor class. It is conjectured that the same is true if R is finitely generated over $\mathbb{Z}$.

The example $R = k[X^3, X^4, X^5] \subset k[X]$ in [8], where k is an algebraically closed field, shows that the assumption $\dim(R) \geq 2$ for algebras over infinite perfect fields is necessary.

3. Krull monoids. In the following we need the concept of block monoids. Let P be a set. We denote by

$$\mathcal{F}(P) = \Big\{ \prod_{p\in P} p^{n_p} \,\Big|\, n_p \in \mathbb{N}_0,\ n_p = 0 \text{ for almost all } p \in P \Big\} \tag{2}$$

the *free abelian monoid* with basis P. For an element $h = \prod_{p\in P} p^{n_p} \in \mathcal{F}(P)$ we set

$$\sigma(h) = \sigma_{\mathcal{F}(P)}(h) = \sum_{p\in P} n_p \in \mathbb{N}_0.$$

For an abelian group G and an arbitrary subset $G_0 \subset G$ the *block monoid* of G_0 is defined by

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

Let H be a Krull monoid with class group G and let G_0 denote the set of divisor classes containing a prime divisor. Then

$$\mathcal{L}(H) = \mathcal{L}(\mathcal{B}(G_0))$$

(see [4], Section 3).

In order to prove Theorem 1.1 it is thus sufficient to show the following purely group-theoretical theorem.

THEOREM 3.1. *Let G be an infinite abelian group, $m \in \mathbb{N}$ and $G_0 \subset G$ a subset such that $G = G_0(m)$. Then there exists some constant $K \in \mathbb{N}$ such that for all $N \in \mathbb{N}$ there exists some $L \in \mathcal{L}(\mathcal{B}(G_0))$ with $\min L \leq K$, $|L| \leq K$ and $\max L > N$. In particular, $\Delta(H)$ is an infinite set.*

The rest of the paper is devoted to the proof of this theorem.

LEMMA 3.2. *Let G be an abelian group and let $G_0 \subset G$ be a subset. Let $V, W \in \mathcal{F}(G_0)$ be elements such that VW is a block. Suppose that for all divisors $D \mid_{\mathcal{F}(G_0)} W$, $E \mid_{\mathcal{F}(G_0)} V$ and $E' \mid_{\mathcal{F}(G_0)} V$ the following holds true: $\sigma(E) = \sigma(E')$ whenever ED and $E'D$ are irreducible elements of $\mathcal{B}(G_0)$. Then*

$$|L_{\mathcal{B}(G_0)}(VW)| \leq \sigma(W)!.$$

Proof. Let

$$VW = q_1 \ldots q_s$$

be a factorization of VW into irreducible elements q_i of $\mathcal{B}(G_0)$. Then we can decompose each q_i in the form

$$q_i = v_i w_i$$

where $v_i, w_i \in \mathcal{F}(G_0)$, $v_i \,|\, V$, $w_i \,|\, W$ and $w_1 \ldots w_s = W$. We assume that $w_i \neq 1$ for $1 \leq i \leq t$ and $w_i = 1$ for $t+1 \leq i \leq s$.

If we consider a second decomposition

$$VW = q'_1 \ldots q'_{s'}$$

into irreducible elements q'_i of $\mathcal{B}(G_0)$ such that $q'_i = v'_i w_i$ for all $1 \leq i \leq t$, we see that $s = s'$, i.e. $|L_{\mathcal{B}(G_0)}(VW)|$ is bounded by the number of different (up to order) decompositions $w_1 \ldots w_s$ of W into non-trivial elements $w_i \in \mathcal{F}(G_0)$.

Let $W = x_1 \ldots x_n$, where the x_i are prime elements of $\mathcal{F}(G_0)$. Without restriction we assume that the x_i are pairwise distinct (since this just enlarges the number of possible decompositions of W). If we write permutations $\tau \in \mathfrak{S}_n$ as products of disjoint cycles $\tau = \sigma_1 \ldots \sigma_k$ we see that τ determines a decomposition of $\{1, \ldots, n\}$ into non-empty disjoint sets. Hence we get a surjective map from $\mathfrak{S}_n$ to the set of decompositions of W. This implies that the number of decompositions of W is bounded by $\sigma(W)!$. ■

LEMMA 3.3. *Let G be an abelian group which contains an element of infinite order and let $G_0 \subset G$ be a subset which generates G as a monoid. Then there exists a non-trivial block*

$$B = g_1^{t_1} \ldots g_k^{t_k} \in \mathcal{B}(G_0)$$

with pairwise distinct elements $g_i \in G_0$ of infinite order and $t_i > 0$ such that the kernel of the homomorphism

$$\varphi : \mathbb{Z}^k \to G, \qquad (\alpha_1, \ldots, \alpha_k) \mapsto \sum_{i=1}^{k} \alpha_i g_i,$$

is generated by $(t_1, \ldots, t_k) \in \mathbb{N}^k$. In particular, $\mathcal{B}(\{g_1, \ldots, g_k\}) \cong (\mathbb{N}_0, +)$.

Proof. Since G_0 generates G as a monoid, there exists an element $\widetilde{g}_1 \in G_0$ with infinite order. Let $\widetilde{B} = \widetilde{g}_1 \ldots \widetilde{g}_n \in \mathcal{B}(G_0)$. For large $l \in \mathbb{N}$, $\widetilde{B}^l$ has a non-trivial divisor $\widetilde{B}' = \widetilde{g}'_1 \ldots \widetilde{g}'_{n'}$ in $\mathcal{B}(G_0)$ such that each $\widetilde{g}'_i$ has infinite order. We thus assume that all $\widetilde{g}_i$ have infinite order.

Let T be a minimal subset of $\{\widetilde{g}_1, \ldots, \widetilde{g}_n\}$ with respect to inclusion such that $\mathcal{B}(T) \neq \{1\}$. We write $T = \{g_1, \ldots, g_k\}$ with pairwise distinct elements g_i.

Next we show that the kernel of φ is cyclic.

Since $g_1, \ldots, g_k$ are not linearly independent over $\mathbb{Z}$, it suffices to show that every proper subset $T' \subsetneq T$ is linearly independent over $\mathbb{Z}$. Assume the contrary and let $g_1^{r_1} \ldots g_k^{r_k}$ with $r_i > 0$ be a non-trivial block.

Then there exists some $(\beta_1, \dots, \beta_k) \in \mathbb{Z}^k \setminus \{\mathbf{0}\}$ such that $\beta_1 g_1 + \dots + \beta_k g_k = 0$ and $\beta_i = 0$ for at least one $i \in \{1, \dots, k\}$ (note that $k \geq 2$ since all g_i have infinite order). By the minimal choice of T, we have $\beta_j < 0$ for at least one j, and we choose $(\beta_1, \dots, \beta_k)$ with a minimal number of negative components. We may assume that $\beta_k = 0$ and $\beta_{k-1} < 0$. Then we obtain

$$0 = \sum_{i=0}^{k-2} (r_{k-1}\beta_i - \beta_{k-1} r_i) g_i + \beta_{k-1} r_k g_k,$$

a relation with fewer negative coefficients, which is a contradiction.

Let $(t_1, \dots, t_k) = \boldsymbol{t} \in \mathbb{Z}^k$ be a generator of $\ker(\varphi)$. Since there exists a non-trivial block in $\mathcal{B}(T)$ we can choose $\boldsymbol{t} \in \mathbb{N}^k$. We set

$$B = g_1^{t_1} \dots g_k^{t_k}.$$

Since $\boldsymbol{t}$ generates $\ker(\varphi)$, we see that B is the only irreducible element of $\mathcal{B}(T)$ and hence $\mathcal{B}(T) \cong (\mathbb{N}_0, +)$. ∎

From now on let G be always an infinite abelian group, $m \in \mathbb{N}$ and $G_0 \subset G$ a subset such that

$$G = G_0(m).$$

The proof of Theorem 3.1 is divided into three parts:

1. G contains an element of infinite order.
2. G is a torsion group with $\{\mathrm{ord}(g) \mid g \in G\}$ bounded.
3. G is a torsion group with $\{\mathrm{ord}(g) \mid g \in G\}$ unbounded.

3.1. *Case 1: G contains an element of infinite order.* Let

$$B = g_1^{t_1} \dots g_k^{t_k} \in \mathcal{B}(G_0)$$

be a block as in Lemma 3.3. We set $B_1 = g_1^{t_1} \dots g_{k-1}^{t_{k-1}}$ and $B_2 = g_k^{t_k}$ (since all g_i are of infinite order, we have $k \geq 2$).

Let $N \in \mathbb{N}$ be arbitrary and let $\phi_1, \dots, \phi_v, \psi_1, \dots, \psi_w$ be elements of G_0 such that $v \leq m$, $w \leq m$,

$$-N \sum_{i=1}^{k-1} t_i g_i = \phi_1 + \dots + \phi_v$$

and $-N t_k g_k = \psi_1 + \dots + \psi_w$. Set $V = B^N$ and $W = \phi_1 \dots \phi_v \psi_1 \dots \psi_w$. We assert that V and W satisfy the assumptions of Lemma 3.2.

Let D be a divisor of W in $\mathcal{F}(G_0)$. We assume that there are $u_1, \dots, u_k$, $u_1', \dots, u_k' \in \mathbb{N}_0$ such that $Q = g_1^{u_1} \dots g_k^{u_k} D$ and $Q' = g_1^{u_1'} \dots g_k^{u_k'} D$ are irreducible blocks. Then

$$\sum_{i=1}^{k} u_i g_i = \sum_{i=1}^{k} u_i' g_i$$

and thus $(u_1 - u_1', \dots, u_k - u_k') \in \ker(\varphi)$ (where φ is as in Lemma 3.3). Hence $g_1^{u_1-u_1'} \dots g_k^{u_k-u_k'} = B^l$ for some $l \in \mathbb{Z}$ and $Q = B^l Q'$. This implies $l = 0$, since Q and Q' are both irreducible.

If we set $C = VW$, then Lemma 3.2 implies

$$|L_{\mathcal{B}(G_0)}(C)| \leq (2m)!.$$

We immediately see that

$$\max L_{\mathcal{B}(G_0)}(C) \geq N + 1.$$

On the other hand we have

$$\max L_{\mathcal{B}(G_0)}(B_1\phi_1 \dots \phi_v) \leq v \leq m,$$
$$\max L_{\mathcal{B}(G_0)}(B_2\psi_1 \dots \psi_w) \leq w \leq m,$$

since every non-trivial divisor (in $\mathcal{B}(G_0)$) of $B_1\phi_1 \dots \phi_v$ (resp. $B_2\psi_1 \dots \psi_w$) must contain some ϕ_i (resp. ψ_i). Hence we get

$$\min L_{\mathcal{B}(G_0)}(C) \leq 2m.$$

3.2. *Case 2: G is a bounded torsion group.* We now assume that G is a torsion group with $\{\mathrm{ord}(g) \mid g \in G\}$ bounded.

By [9], Theorem 6, we know that G is a direct sum of cyclic groups:

$$G = \bigoplus_{i \in I} \mathbb{Z}/n_i\mathbb{Z}$$

for some bounded family $n_i \geq 2$ of integers. For a subset $T \subset I$ we denote by

$$P_T : \bigoplus_{i \in I} \mathbb{Z}/n_i\mathbb{Z} \to \bigoplus_{i \in T} \mathbb{Z}/n_i\mathbb{Z} \subset G$$

the projection. For any $g \in G$ and $T \subset I$ we set $\mathrm{ord}_T(g) = \mathrm{ord}(P_T(g))$ and we define the *support* of g by

$$\mathrm{supp}(g) = \{i \in I \mid P_i(g) \neq 0\}.$$

We now construct a sequence $(h_i)_{i \in \mathbb{N}}$ in G_0 with the following properties: There exist $t \geq 2$, $a \in G$ and a finite set $\mathcal{E} \subset I$ such that the following assertions hold for all $i \geq 1$:

(i) $P_{\mathcal{E}}(h_i) = a$.
(ii) $\mathrm{ord}_{I \setminus \mathcal{E}}(h_i) = t$.
(iii) If $M = I \setminus (\mathcal{E} \cup \mathrm{supp}(h_1) \cup \ldots \cup \mathrm{supp}(h_{i-1}))$ then $\mathrm{ord}_M(h_i) = t$.

To begin with, let $t \in \mathbb{N}$ be minimal such that there exists a finite subset $\mathcal{E} \subset I$ for which the set

$$T = \{g \in G_0 \mid \mathrm{ord}_{I \setminus \mathcal{E}}(g) = t\}$$

is infinite (since G_0 is infinite and since $\{\mathrm{ord}(g) \mid g \in G\}$ is bounded, such a t exists and $t \geq 2$). Then for every finite set $J \subset I$, the set $\{g \in T \mid$

$\mathrm{ord}_{I\setminus(\mathcal{E}\cup J)}(g) \neq t\}$ is finite since $\mathrm{ord}_{I\setminus(\mathcal{E}\cup J)}(g) \neq t$ implies $\mathrm{ord}_{I\setminus(\mathcal{E}\cup J)}(g) < t$ for all $g \in T$.

Let $\widetilde{T} \subset T$ be an infinite subset with the property

$$P_{\mathcal{E}}(g) = P_{\mathcal{E}}(h) = a \in G \tag{3}$$

for all $g, h \in \widetilde{T}$ and for some $a \in G$ (such a set exists since $\mathcal{E}$ is finite).

Now we construct the sequence h_i. Let $h_1 \in \widetilde{T}$ be arbitrary and assume that $h_1, \ldots, h_{n-1}$ are already constructed. Since the set

$$F = \{g \in \widetilde{T} \mid \mathrm{ord}_{I\setminus(\mathcal{E}\cup \mathrm{supp}(h_1)\cup\ldots\cup \mathrm{supp}(h_{n-1}))}(g) \neq t\}$$

is finite by the above considerations, $\widetilde{T} \setminus F$ is non-empty and we choose $h_n \in \widetilde{T} \setminus F$. We see easily that the sequence h_i satisfies our requirements (i)–(iii). We set

$$r = \mathrm{ord}(ta).$$

Next we show the following

Claim. *Set $H = \{h_i \mid i \in \mathbb{N}\}$. Then:*

(i) *Let $(\alpha_i)_{i\in\mathbb{N}} \in \mathbb{Z}^{(\mathbb{N})}$ be a sequence such that*

$$\sum_{i\in\mathbb{N}} \alpha_i h_i = 0.$$

Then $t \mid \alpha_i$ for all $i \in \mathbb{N}$ and $rt \mid \sum_{i\in\mathbb{N}} \alpha_i$.

(ii) *Let $A = \prod_{i\in\mathbb{N}} h_i^{\alpha_i} \in \mathcal{F}(H)$ and $B = \prod_{i\in\mathbb{N}} h_i^{\beta_i} \in \mathcal{F}(H)$ be such that*

$$\sum_{i\in\mathbb{N}} \alpha_i h_i = \sum_{i\in\mathbb{N}} \beta_i h_i.$$

If $\sum_{i\in\mathbb{N}} \alpha_i > \sum_{i\in\mathbb{N}} \beta_i$ then there exists some $\widetilde{A} \in \mathcal{F}(H)$ and some non-trivial block $C \in \mathcal{B}(H)$ of the form

$$C = c_1^t \ldots c_r^t$$

with $c_i \in H$ such that $A = \widetilde{A}C$.

(iii) *$\{c_1^t \ldots c_r^t \mid c_1, \ldots, c_r \in H\}$ is the set of all irreducible blocks of H. In particular, $\mathcal{B}(H)$ is half-factorial.*

Proof. (i) We show more generally that if

$$pa + \sum_{i\in\mathbb{N}} \alpha_i h_i = 0$$

(for the definition of a see (3)) where $p \in \mathbb{Z}$ and $(\alpha_i)_{i\in\mathbb{N}} \in \mathbb{Z}^{(\mathbb{N})}$ then $t \mid \alpha_i$ for all i. Set

$$i_0 = \max\{i \mid \alpha_i \neq 0\}$$

and define

$$M = \mathcal{E} \cup \mathrm{supp}(h_1) \cup \ldots \cup \mathrm{supp}(h_{i_0-1}) \subset I.$$

Then

$$0 = P_{I\setminus M}\Big(pa + \sum_{i\in\mathbb{N}} \alpha_i h_i\Big) = P_{I\setminus M}(\alpha_{i_0} h_{i_0}) = \alpha_{i_0} P_{I\setminus M}(h_{i_0}).$$

Since the order of $P_{I\setminus M}(h_{i_0})$ equals t, we get $t \mid \alpha_{i_0}$. Thus we have

$$\alpha_{i_0} h_{i_0} = \frac{\alpha_{i_0}}{t} t h_{i_0} = \frac{\alpha_{i_0}}{t} ta = \alpha_{i_0} a,$$

since $th = P_{\mathcal{E}}(th) + P_{I\setminus\mathcal{E}}(th) = P_{\mathcal{E}}(th) = ta$ for all $h \in H$. By induction we now infer that $t \mid \alpha_i$ for all $i \in \mathbb{N}$.

Now let $(\alpha_i)_{i\in\mathbb{N}} \in \mathbb{Z}^{(\mathbb{N})}$ be a sequence such that $\sum_{i\in\mathbb{N}} \alpha_i h_i = 0$. From the above we get

$$\sum_{i\in\mathbb{N}} \alpha_i h_i = \sum_{i\in\mathbb{N}} \frac{\alpha_i}{t} t h_i = \frac{\sum_{i\in\mathbb{N}} \alpha_i}{t} ta.$$

Hence $rt \mid \sum_{i\in\mathbb{N}} \alpha_i$.

(ii) Without loss of generality we may assume that A and B are coprime in $\mathcal{F}(H)$. Then we see from (i) that $t \mid \alpha_i$ and $t \mid \beta_i$ for all $i \in \mathbb{N}$. Moreover, we have

$$\sum_{i\in\mathbb{N}} \alpha_i = \sum_{i\in\mathbb{N}} \beta_i + \gamma r t$$

for some $\gamma \in \mathbb{N}$. Since t divides each α_i there exist $c_1, \ldots, c_r \in H$ such that the block $C = c_1^t \ldots c_r^t$ divides A.

(iii) Let $B \in \mathcal{B}(H)$ be non-trivial. Then $B = \widetilde{B} c_1^t \ldots c_r^t$ where $c_i \in H$ by (ii). If B is irreducible, $\widetilde{B}$ is equal to 1. $\blacksquare_{\text{Claim}}$

For $n \in \mathbb{N}$ we set

$$A_n = h_{(n-1)r+1} \ldots h_{nr} \in \mathcal{F}(G_0).$$

Then A_n^t is a block.

Let $N \in \mathbb{N}$ be arbitrary. Set $B = A_1 \ldots A_N$ and let $\phi_1, \ldots, \phi_v \in G_0$ be such that

$$\phi_1 + \ldots + \phi_v = -\sum_{i=1}^{Nr} h_i$$

and $v \le m$. We set $\Phi = \phi_1 \ldots \phi_v \in \mathcal{F}(G_0)$, $V = B^t$ and $W = \Phi^t$.

From (iii) of the Claim we see that every non-trivial divisor of $B\Phi$ in $\mathcal{B}(G_0)$ must contain at least one ϕ_i (note that $t \ge 2$) and we get $\max L_{\mathcal{B}(G_0)}(B\Phi) \le v$. Let $C = VW$. Then

$$\min L_{\mathcal{B}(G_0)}(C) \le tv \le tm \le \exp(G)m.$$

On the other hand,

$$\max L_{\mathcal{B}(G_0)}(C) \ge N + 1.$$

Let D be a divisor of W in $\mathcal{F}(G_0)$. If $Q = h_1^{\beta_1} \dots h_s^{\beta_s} D$ and $Q' = h_1^{\beta'_1} \dots h_s^{\beta'_s} D$ where $\beta_i, \beta'_i \in \mathbb{N}_0$ are irreducible blocks then $\sum_{i=1}^{s} \beta_i = \sum_{i=1}^{s} \beta'_i$ by (ii) of the Claim. Thus Lemma 3.2 yields

$$|L_{\mathcal{B}(G_0)}(C)| \le (tv)! \le (\exp(G)m)!.$$

3.3. *Case 3: G is an unbounded torsion group.* We now consider the case when G is a torsion group such that $\{\mathrm{ord}(g) \mid g \in G\} \subset \mathbb{N}$ is unbounded.

Let $N \in \mathbb{N}$ be arbitrary. The goal is to construct a block

$$B = g_1^{\gamma_1} \dots g_u^{\gamma_u} \in \mathcal{B}(G_0) \tag{4}$$

with pairwise distinct elements $g_i \in G_0$ such that $2 \le u \le 2m$ and such that there is no relation

$$\sum_{i=0}^{u} \alpha_i g_i = 0$$

(where $\alpha_i \in \mathbb{Z}$) with the following properties:

(i) $|\alpha_i| \le \max\{\gamma_1, \dots, \gamma_u\} N$ for all $1 \le i \le u$.
(ii) $(\alpha_1, \dots, \alpha_u)$ and $(\gamma_1, \dots, \gamma_u)$ are linearly independent over $\mathbb{Z}$.

We set $d = 2m + 1$ and define a sequence $(l_i)_{i \in \mathbb{N}_0}$ of integers as follows:

$$l_0 = 1, \quad l_1 = 2^{d^d} d^{d^d} N^{d^d} \quad \text{and} \quad l_{i+1} = l_1 l_i^{d^{d^d}} \quad \text{for all } i \ge 1.$$

In order to construct the block we start with a sequence $(g_1, \dots, g_r)$ of (not necessarily pairwise distinct) non-zero elements of G_0 such that

(i) $r \le 2m$.
(ii) $g_1 + \dots + g_r = 0$.
(iii) There exists some $g \in \{g_1, \dots, g_r\}$ such that $\mathrm{ord}(g) \ge l_{d+1}$.

(Such a sequence exists since $G_0(m) = G$ and $\{\mathrm{ord}(g) \mid g \in G\} \subset \mathbb{N}$ is unbounded.) Set $I = \{g_1, \dots, g_r\}$.

Our first aim is to get rid of those elements g_i which have "too small" order: We construct a block

$$B_0 = g_1^{\beta_1} \dots g_k^{\beta_k} \in \mathcal{B}(I)$$

of distinct elements g_i and $k \le r$ (after renumbering the g_i if necessary) such that $1 \le \beta_i \le 2m\, l_{t-1}^{2m}$ and $\mathrm{ord}(g_i) > l_t$ for some $1 \le t \le d$ and all $1 \le i \le k$.

For $i \ge 1$ set

$$K_i = \{g \in I \mid l_{i-1} < \mathrm{ord}(g) \le l_i\}.$$

Then $K_i \cap K_j = \emptyset$ if $i \ne j$. This implies that there exists some $1 \le t \le d$ such that $K_t = \emptyset$, since I contains at most $2m$ elements. Since there exists some $g \in I$ such that $\mathrm{ord}(g) \ge l_{d+1}$, the set

$$M_t = \{g \in I \mid \mathrm{ord}(g) > l_t\}$$

is non-empty. Without restriction let $M_t = \{g_1, \ldots, g_k\}$ with pairwise distinct elements g_i. Since for all $g \in I$ we have either $\mathrm{ord}(g) > l_t$ or $\mathrm{ord}(g) \le l_{t-1}$, we see that there exists some $1 \le \kappa \le l_{t-1}^{2m}$ such that $\kappa g = 0$ for all $g \in I \setminus M_t = \{g \in I \mid \mathrm{ord}(g) \le l_{t-1}\}$.

From these considerations we see that there is a block

$$B_0 = g_1^{\beta_1} \ldots g_k^{\beta_k}$$

where $1 \le \beta_i \le 2m\kappa$. (The factor $2m$ arises because the g_i of our original sequence $(g_1, \ldots, g_r)$ are not necessarily pairwise distinct.)

We now define a sequence κ_i by

$$\kappa_0 = 2m\kappa \quad \text{and} \quad \kappa_{i+1} = 2^{2m}\kappa_i^d N.$$

The next step is to use relations $\sum_{i=1}^k \alpha_i g_i = 0$ with "small" coefficients α_i, where $(\alpha_1, \ldots, \alpha_k)$ and $(\beta_1, \ldots, \beta_k)$ are linearly independent (if such relations exist) to obtain blocks

$$B_i = g_1^{\beta_1^{(i)}} \ldots g_{k_i}^{\beta_{k_i}^{(i)}}$$

which contain fewer g_i than B_0 does and where the $\beta_j^{(i)}$ are still "small" (compared with the order of the g_i). We repeat this till there are no such relations and finally obtain the block B in (4).

Hence assume that there is a relation

$$\sum_{i=1}^k \alpha_i g_i = 0$$

(where $\alpha_i \in \mathbb{Z}$) such that $|\alpha_i| \le \kappa_0 N$ for all $1 \le i \le k$ and such that $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_k)$ and $\boldsymbol{\beta} = (\beta_1, \ldots, \beta_k)$ are linearly independent over $\mathbb{Z}$. Without loss of generality we assume that there exists some j with $\alpha_j < 0$ (otherwise we pass to $\sum_{i=1}^k (-\alpha_i) g_i = 0$). The formula

$$\beta_j \boldsymbol{\alpha} + (-\alpha_j)\boldsymbol{\beta} =: \boldsymbol{\alpha}^{(1)} = (\alpha_1^{(1)}, \ldots, \alpha_k^{(1)})$$

defines a new vector $\boldsymbol{\alpha}^{(1)}$ such that $\alpha_j^{(1)} = 0$. If we repeat this procedure with $\boldsymbol{\alpha}^{(1)}$ instead of $\boldsymbol{\alpha}$ (provided there exists some $\alpha_j^{(1)} < 0$), we obtain a vector $\boldsymbol{\alpha}^{(2)}$. After n steps (where $n \le k$) we get a vector $\boldsymbol{\alpha}^{(n)}$ such that all $\alpha_j^{(n)}$ are non-negative and $\alpha_j^{(n)} = 0$ for at least one j. Without restriction let $\alpha_1^{(n)}, \ldots, \alpha_{k_1}^{(n)} > 0$ and $\alpha_{k_1+1}^{(n)} = \ldots = \alpha_k^{(n)} = 0$. We set

$$\beta_i^{(1)} = \alpha_i^{(n)} \quad \text{for all } 1 \le i \le k_1$$

and obtain a block

$$B_1 = g_1^{\beta_1^{(1)}} \ldots g_{k_1}^{\beta_{k_1}^{(1)}} \in \mathcal{B}(G_0)$$

where $k_1 < k$.

In order to estimate the size of the $\beta_i^{(1)}$ we consider the equalities

$$\beta_j \alpha_i^{(l)} - \alpha_j^{(l)} \beta_i = \alpha_j^{(l+1)}$$

which yield

$$\begin{aligned}\max\{|\alpha_j^{(l+1)}| \mid 1 \le j \le k\} &\le 2 \max\{\beta_j \mid 1 \le j \le k\} \max\{|\alpha_j^{(l)}| \mid 1 \le j \le k\} \\ &\le 2\kappa_0 \max\{|\alpha_j^{(l)}| \mid 1 \le j \le k\}.\end{aligned}$$

Since $\max\{|\alpha_j| \mid 1 \le j \le k\} \le \kappa_0 N$ we obtain, by induction on l,

$$\max\{|\alpha_j^{(l)}| \mid 1 \le j \le k\} \le 2^l \kappa_0^{l+1} N \le 2^{2m} \kappa_0^{2m+1} N = \kappa_1.$$

Thus we have $\beta_i^{(1)} \le \kappa_1$ for all $1 \le i \le k_1$.

If we repeat the whole procedure with B_1 (provided there exists some relation

$$\sum_{i=1}^{k_1} \alpha_i g_i = 0$$

such that $|\alpha_i| \le \kappa_1 N$ for all $1 \le i \le k_1$ and such that $(\alpha_1, \dots, \alpha_{k_1})$ and $(\beta_1^{(1)}, \dots, \beta_{k_1}^{(1)})$ are linearly independent over $\mathbb{Z}$), we obtain a block

$$B_2 = g_1^{\beta_1^{(2)}} \dots g_{k_2}^{\beta_{k_2}^{(2)}}$$

such that $\beta_i^{(2)} \le \kappa_2$ for all $1 \le i \le k_2$. After s steps (where $0 \le s \le k \le 2m$) we finally obtain a block

$$B_s = g_1^{\beta_1^{(s)}} \dots g_{k_s}^{\beta_{k_s}^{(s)}}$$

such that there is no equality

$$\sum_{i=1}^{k_s} \alpha_i g_i = 0$$

with the property $|\alpha_i| \le \kappa_s N$ for all $1 \le i \le k_s$ and such that $(\alpha_1, \dots, \alpha_{k_s})$ and $(\beta_1^{(s)}, \dots, \beta_{k_s}^{(s)})$ are linearly independent over $\mathbb{Z}$.

It is clear by construction that B_s is non-trivial and that $\beta_i^{(s)} > 0$ for all $1 \le i \le k_s$. For the following argument it is crucial to see that even $k_s \ge 2$.

One can easily verify that

$$\kappa_i = 2^{d^i - 1} \kappa_0^{d^i} N^{\sum_{j=0}^{i-1} d^j}$$

for every $i \ge 0$. We thus have

$$\kappa_{2m} = 2^{d^{2m}-1} \kappa_0^{d^{2m}} N^{\sum_{j=0}^{2m-1} d^j} = 2^{2d^{2m}-1} m^{d^{2m}} \kappa^{d^{2m}} N^{\sum_{j=0}^{2m-1} d^j} \le 2^{d^d} d^{d^d} \kappa^{d^d} N^{d^d}.$$

Assume that k_s is equal to one. Then

$$\operatorname{ord}(g_1) \le \beta_1^{(s)} \le \kappa_s \le \kappa_{2m} \le 2^{d^d} d^{d^d} \kappa^{d^d} N^{d^d}$$

since B_s is a block. On the other hand, $\mathrm{ord}(g_1) > l_t$. Hence

$$l_t < \mathrm{ord}(g_1) \le 2^{d^d} d^{d^d} \kappa^{d^d} N^{d^d} \le 2^{d^d} d^{d^d} l_{t-1}^{2m^{d^d}} N^{d^d} \le l_t,$$

which is a contradiction.

Thus we have constructed a block as required at the beginning of the subsection if we set $u = k_s$, $\gamma_i = \beta_i^{(s)}$ and $B = B_s$.

We now set $B_1 = g_1^{\gamma_1} \dots g_{u-1}^{\gamma_{u-1}}$ and $B_2 = g_u^{\gamma_u}$ (note that $u \ge 2$).

Let $\phi_1, \dots, \phi_v, \psi_1, \dots, \psi_w \in G_0$ be such that $v \le m$, $w \le m$,

$$-N \sum_{i=1}^{u-1} \gamma_i g_i = \phi_1 + \dots + \phi_v$$

and $-N\gamma_u g_u = \psi_1 + \dots + \psi_w$. Set $V = B^N$, $W = \phi_1 \dots \phi_v \psi_1 \dots \psi_w$ and consider the block $C = VW$. We obviously have

$$\max L_{\mathcal{B}(G_0)}(C) \ge N + 1.$$

On the other hand, $\max L(B_1\phi_1 \dots \phi_v) \le v \le m$ and $\max L(B_2\psi_1 \dots \psi_w) \le w \le m$ because there does not exist a non-trivial block which divides B_1 (resp. B_2). Hence we obtain

$$\min L_{\mathcal{B}(G_0)}(C) \le 2m.$$

Next we check that V and W satisfy the assumptions of Lemma 3.2. Let D be a divisor of W in $\mathcal{F}(G_0)$ and let $E = g_1^{\delta_1} \dots g_u^{\delta_u}$ and $E' = g_1^{\delta'_1} \dots g_u^{\delta'_u}$ be divisors of V in $\mathcal{F}(G_0)$. If $Q = ED$ and $Q' = E'D$ are irreducible blocks we have

$$\sum_{i=1}^{u} (\delta_i - \delta'_i) g_i = 0$$

and thus $(\delta_1 - \delta'_1, \dots, \delta_u - \delta'_u) = x(\gamma_1, \dots, \gamma_u)$ for some $x \in \mathbb{Q}$ because of the properties of B.

Assume that $x \ne 0$. Without loss of generality let $x > 0$. This implies that $\delta_i - \delta'_i > 0$ for all $1 \le i \le u$ and hence

$$Q = Q' g_1^{\delta_1 - \delta'_1} \dots g_u^{\delta_u - \delta'_u}$$

is a non-trivial decomposition, which is a contradiction.

Hence Lemma 3.2 implies

$$|L_{\mathcal{B}(G_0)}(C)| \le (2m)!.$$

REFERENCES

[1] D. D. Anderson (ed.), *Factorization in Integral Domains*, Lecture Notes in Pure and Appl. Math. 189, Marcel Dekker, 1997.

[2] D. D. Anderson, D. F. Anderson and M. Zafrullah, *Factorization in integral domains*, J. Pure Appl. Algebra 69 (1990), 1–19.
[3] D. F. Anderson, *Elasticity of factorizations in integral domains*: *A survey*, in [1], 1–29.
[4] A. Geroldinger and S. Chapman, *Krull domains and monoids*, *their sets of lengths and associated combinatorial problems*, in [1], 73–112.
[5] F. Kainrath, *A divisor-theoretic approach towards the arithmetic of Noetherian domains*, Arch. Math. (Basel) 73 (1999), 347–354.
[6] —, *Elasticity of finitely generated domains*, preprint.
[7] —, *Factorization in Krull monoids with infinite class group*, Colloq. Math. 80 (1999), 23–30.
[8] —, *The distribution of prime divisors in finitely generated domains*, Manuscripta Math. 100 (1999), 203–212.
[9] I. Kaplansky, *Infinite Abelian Groups*, third printing, Univ. of Michigan Press, 1960.

Institut für Mathematik
Karl-Franzens-Universität Graz
Heinrichstraße 36/4
A-8010 Graz, Austria
E-mail: wolfgang.hassler@uni-graz.at

Received 10 September 2001 (4106)