COLLOQUIUM MATHEMATICUM

VOL. 80 1999 NO. 1

FACTORIZATION IN KRULL MONOIDS WITH INFINITE CLASS GROUP

BY

FLORIAN KAINRATH (GRAZ)

Abstract. Let H be a Krull monoid with infinite class group and such that each divisor class of H contains a prime divisor. We show that for each finite set L of integers ≥ 2 there exists some $h \in H$ such that the following are equivalent:

(i) h has a representation $h = u_1 \cdot \ldots \cdot u_k$ for some irreducible elements u_i,
(ii) $k \in L$.

1. Introduction and notations. Let H be a Krull monoid. For an element h of H its set of lengths $\mathcal{L}(h)$ is defined as the set of all integers k such that there exist irreducible $u_1, \ldots, u_k$ with $h = u_1 \cdot \ldots \cdot u_k$. If the class group of H is finite, then the sets $\mathcal{L}(h)$ have a special structure:

$$\begin{array}{lllll}\mathcal{L}(h) = \{x_1, \ldots, x_\alpha, & y_1, & \ldots & y_l, & \\ & y_1 + d, & \ldots & y_l + d, & \\ & \ldots & \ldots & \ldots & \\ & y_1 + kd, & \ldots & y_l + kd, & z_1, \ldots, z_\beta\},\end{array}$$

where $x_1 < \ldots < x_\alpha < y_1 < \ldots < y_l < y_1 + d < y_l + kd < z_1 < \ldots < z_\beta$ and $\alpha, \beta, d \leq M$ for some constant M depending only on the class group of H ([1], Theorem 2.13).

In this paper we look at the sets $\mathcal{L}(h)$ when the class group of H is infinite and each divisor class of H contains a prime divisor. Our main result states that in this case every finite set of integers ≥ 2 occurs as a set of lengths of an element in H. We apply this result also to certain integral domains.

Throughout this paper the following notations will be used. We let $\mathbb{N}$ be the set of all nonnegative integers, $\mathbb{N}_+ = \mathbb{N} \setminus \{0\}$ and $\mathbb{N}_{\geq 2}$ the set of all integers ≥ 2. For a finite set X we denote by $|X|$ the number of elements of X.

2. Sets of lengths. In the following let H be a commutative, cancellative monoid with unit element. By a *factorization* of an element $h \in H$ we mean a representation of the form $h = u_1 \cdot \ldots \cdot u_k$ with irreducible $u_i \in H$. The integer k is called the *length* of the factorization. Two factorizations

1991 *Mathematics Subject Classification*: 11R27, 13G05.

$h = u_1 \cdot \ldots \cdot u_k = v_1 \cdot \ldots \cdot v_l$ are said to be *essentially the same* if $k = l$ and after some renumbering $u_i = e_i \cdot v_i$ for some unit e_i; they are called *essentially different* if they are not essentially the same. We denote by $\mathcal{L}(h) = \mathcal{L}_H(h)$ the set of lengths of factorizations of h and define a function $v_h = v_{H,h} : \mathcal{L}(h) \to \mathbb{N}_+$ by

$$v_h(k) = \text{the number of essentially different factorizations of } h \text{ having length } k.$$

Now let H be Krull monoid (see for example [1]), $\partial : H \to D$ its divisor theory and $G = D/\partial(H)$ its class group. We denote the canonical map $D \to G$ by $d \mapsto [d]$. We say that *every divisor class of H contains a prime divisor* if for every $g \in G$ there exists a prime element $p \in D$ with $[p] = g$. Now we can state our main result.

THEOREM 1. *Let H be a Krull monoid with infinite class group in which every divisor class contains a prime divisor. For a finite subset $L \subset \mathbb{N}_{\geq 2}$ there exists some $h \in H$ such that $\mathcal{L}_H(h) = L$. If the class group of H is not of the form $(\mathbb{Z}/2\mathbb{Z})^{(N)} \oplus \Gamma$ with an infinite set N and a finite group Γ, then there is such an h satisfying $v_h = v$, where v is any given function $L \to \mathbb{N}_+$.*

For the proof of this theorem we need the concept of block monoids. Let G be the class group of H. We let $\mathcal{F}(G)$ be the free abelian monoid with basis G. The block monoid $\mathcal{B}(G)$ over G is the submonoid of $\mathcal{F}(G)$ defined by

$$\mathcal{B}(G) = \Big\{ \prod_{g \in G} g^{n_g} \in \mathcal{F}(G) : \sum_{g \in G} n_g g = 0 \Big\}.$$

We say that a block $g_1 \cdot \ldots \cdot g_n \in \mathcal{B}(G)$ is *square free* if the g_i are pairwise distinct. For an element $h \in H$ define $\beta(h) \in \mathcal{B}(G)$ by $\beta(h) = [p_1] \cdot \ldots \cdot [p_n]$ where $\partial(h) = p_1 \cdot \ldots \cdot p_n$ is the prime factorization of $\partial(h)$ in D. Then we have

$$\mathcal{L}_{\mathcal{B}(G)}(\beta(h)) = \mathcal{L}_H(h)$$

(see [1], Lemma 3.2). Moreover, it is easy to to see that

$$v_{H,h} = v_{\mathcal{B}(G),\beta(h)}$$

if $\beta(h)$ is square free.

For the proof of Theorem 1 we also need the following proposition whose proof will be given in the next section.

PROPOSITION. *Let C be a nonzero cyclic group, $L \subset \mathbb{N}_{\geq 2}$ a finite set and $v : L \to \mathbb{N}_+$ a function. Then there exists a block B in $\mathcal{B}(C^k)$ for some $k \geq 1$ such that $\mathcal{L}(B) = L$. If $C \neq \mathbb{Z}/2\mathbb{Z}$, then there is a square free block $B \in \mathcal{B}(C^k)$ such that $L = \mathcal{L}(B)$ and $v_B = v$.*

Proof of Theorem 1. Let H be as in Theorem 1, G its class group and choose some finite $L \subset \mathbb{N}_{\geq 2}$ and $v : L \to \mathbb{N}_+$. We show that there is a block

$B \in \mathcal{B}(G)$ with $\mathcal{L}(B) = L$. If G is not of the form $(\mathbb{Z}/2\mathbb{Z})^{(N)} \oplus \Gamma$ with an infinite set N and a finite group Γ, then we will choose B such that it is square free and satisfies $v_B = v$. By the above considerations this will prove Theorem 1. We consider three cases.

Case 1: G is not a torsion group. Then G contains a subgroup isomorphic to $\mathbb{Z}$, so we may assume $G = \mathbb{Z}$. By the Proposition (with $C = \mathbb{Z}$) there is a square free block $B \in \mathcal{B}(\mathbb{Z}^k)$ for some k such that $\mathcal{L}(B) = L$ and $v_B = v$, say $B = u_1 \cdot \ldots \cdot u_n$. Choose some homomorphism $f : \mathbb{Z}^k \to \mathbb{Z}$ such that

$$\sum_{i\in I} f(u_i) \neq 0 \quad \text{if } \sum_{i\in I} u_i \neq 0,\ I \subset \{1, \ldots, n\}, \quad \text{and}$$
$$f(u_i) \neq f(u_j) \quad \text{if } i \neq j.$$

Then it is clear that the square free block $C = f(u_1) \cdot \ldots \cdot f(u_n) \in \mathcal{B}(\mathbb{Z})$ satisfies $\mathcal{L}(C) = L$ and $v_C = v$.

Case 2: G is a torsion group which contains elements of arbitrarily high order. Choose first a square free block $B = u_1 \cdot \ldots \cdot u_n \in \mathcal{B}(\mathbb{Z})$ such that $\mathcal{L}(B) = L$ and $v_B = v$. This is possible by Case 1. Define $M \in \mathbb{N}$ by

$$M = \max\Big(\Big\{\Big|\sum_{i\in I} u_i\Big| : I \subset \{1, \ldots, n\}\Big\} \cup \{|u_i - u_j| : i, j = 1, \ldots, n\}\Big).$$

Then it is obvious that for every $N > M$ the square free block $B_N = (u_1 + N\mathbb{Z}) \cdot \ldots \cdot (u_n + N\mathbb{Z}) \in \mathcal{B}(\mathbb{Z}/N\mathbb{Z})$ satisfies $\mathcal{L}(B_N) = L$ and $v_{B_N} = v$ as well. By our hypothesis on G there exists an element of order greater than M, which means that G contains a subgroup isomorphic to $\mathbb{Z}/N\mathbb{Z}$ for some $N > M$. Therefore the theorem is proved in this case.

Case 3: G is a torsion group in which the orders of all elements are bounded. By Theorem 6 of [4], G is a direct sum of cyclic groups

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

for some bounded family of integers $n_i \geq 2$. Since by assumption G is infinite there is an integer m such that G contains a subgroup isomorphic to $(\mathbb{Z}/m\mathbb{Z})^{(\mathbb{N})}$. If G is not of the form $(\mathbb{Z}/2\mathbb{Z})^{(N)} \oplus \Gamma$ with an infinite set N and a finite group Γ, we may suppose $m > 2$. Using the Proposition with $C = \mathbb{Z}/m\mathbb{Z}$, we see that the theorem is proved in this case as well. ■

In the following we want to apply Theorem 1 to certain integral domains. Let R be a noetherian domain whose integral closure $\overline{R}$ is a finitely generated R-module. Denote by H_R the set of all nonzero divisors of $\overline{R}/R$:

$$H_R = \{r \in R \setminus \{0\} : r\bar{r} \notin R \text{ for all } \bar{r} \in \overline{R} \setminus R\}.$$

Then H_R is a divisor closed Krull submonoid of $R^\bullet = R \setminus \{0\}$ whose class group is isomorphic to the v-class group of R (cf. [2]). Therefore

$$\mathcal{L}_{H_R}(r) = \mathcal{L}_{R^\bullet}(r) \quad \text{and} \quad v_{H_R,r} = v_{R^\bullet,r}$$

for all $r \in H_R$. Hence we get the following theorem.

THEOREM 2. *Let R be a noetherian domain with finitely generated integral closure and infinite v-class group. Suppose that in the monoid H_R every divisor class contains a prime divisor. Then for every finite set $L \subset \mathbb{N}_{\geq 2}$ there exists an element $r \in R^\bullet$ such $\mathcal{L}(r) = L$. If the v-class group of R is not of the form $(\mathbb{Z}/2\mathbb{Z})^{(N)} \oplus \Gamma$ with an infinite set N and a finite group Γ, then there is such an r satisfying $v_r = v$, where v is any given function $L \to \mathbb{N}_+$.*

REMARK. Examples of domains satisfying the condition on the divisor classes may be found in [3].

3. Proof of the Proposition. Let $C = \mathbb{Z}/c\mathbb{Z}$, $c \neq 1$, be some cyclic group. In this section we regard C as a ring. Let $X_1, \ldots, X_n$ be finite sets. We suppose that $|X_i| \geq 2$ for all i and that

$$n = 2 \text{ and } |X_i| \geq 3 \text{ for at least one } i \text{ or } n \geq 3 \quad \text{if } C \neq \mathbb{Z}/2\mathbb{Z},$$

and

$$n \geq 3 \quad \text{if } C = \mathbb{Z}/2\mathbb{Z}.$$

For a subset $J \subset \{1, \ldots, n\}$ we put

$$X_J = \prod_{j \in J} X_j$$

and let $X = X_{\{1,\ldots,n\}}$ for short. The points x of X will always be written as $x = (x_1, \ldots, x_n)$. We denote by $p_J : X \to X_J$ the projection mapping. For a point $z \in X$ we define $X_i^{(z)} = X_i \setminus \{z_i\}$ and

$$X_J^{(z)} = \prod_{j \in J} X_j^{(z)}.$$

If $x \in X$ is a second point we let $J_z(x)$ be the set of all indices i with $x_i \neq z_i$. We denote by C^X the C-algebra of all functions $X \to C$. For a subset M of X we let $\chi_M \in C^X$ be its characteristic function. If $A \subset C^X$ then ${}_C\langle A\rangle$ is the C-submodule generated by A.

We now proceed in 10 steps. In Steps 1 to 8 we construct a block in C^X/V for some submodule V and calculate its set of lengths. In Steps 9 and 10 we use this construction to prove the proposition.

STEP 1. For $z \in X$ the set $\{\chi_{p_J^{-1}(y)} : y \in X_J^{(z)},\ J \subset \{1, \ldots, n\}\}$ is a basis of C^X.

For each i the set $\{1\} \cup \{\chi_y : y \in X_i^{(z)}\}$ is obviously a basis of C^{X_i}. Now, by taking tensor products and by using the canonical isomorphism $\alpha : C^{X_1} \otimes \ldots \otimes C^{X_n} \cong C^X$, $\alpha(f_1 \otimes \ldots \otimes f_n)(x_1, \ldots, x_n) = f_1(x_1) \ldots f_n(x_n)$, we prove our claim (note also that $\chi_{p_\emptyset^{-1}(y)} = 1$ if y is the unique element of $X_\emptyset^{(z)}$).

STEP 2. Define submodules V, W_z $(z \in X)$ of C^X by

$$V = {}_C\langle \chi_{p_i^{-1}(y)} : y \in X_i,\ i = 1, \dots, n\rangle,$$

$$W_z = {}_C\langle \chi_{p_J^{-1}(y)} : |J| \geq 2,\ y \in X_J^{(z)}\rangle.$$

Then we have

$$C^X = V \oplus W_z \tag{1}$$

for all $z \in X$.

Note that V is generated by $\{1\} \cup \{\chi_{p_i^{-1}(y)} : y \in X_i^{(z)},\ i = 1, \dots, n\}$ for all $z \in X$. Therefore the assertion follows from Step 1.

STEP 3. Let $z, x \in X$ with $x \neq z$ and $M \subset X$, $z \notin M$. Then there exist $w_k \in W_z$ $(k = 1, 2, 3)$ and $Y_i \subset X_i^{(z)}$ $(i = 1, \dots, n)$ such that:

$$\chi_z = 1 - \sum_{i=1}^{n} \sum_{y \in X_i^{(z)}} \chi_{p_i^{-1}(y)} + w_1, \tag{2}$$

$$\chi_x = \begin{Bmatrix} 0 & \text{if } |J_z(x)| \geq 2 \\ \chi_{p_i^{-1}(x_i)} & \text{if } J_z(x) = \{i\} \end{Bmatrix} + w_2, \tag{3}$$

$$\chi_M = \sum_{i=1}^{n} \sum_{y \in Y_i} \chi_{p_i^{-1}(y)} + w_3. \tag{4}$$

Let $w \in X$. Then we have

$$\begin{aligned} \chi_w = \prod_{i=1}^{n} \chi_{p_i^{-1}(w_i)} &= \prod_{i \in J_z(w)} \chi_{p_i^{-1}(w_i)} \prod_{i \notin J_z(w)} \chi_{p_i^{-1}(z_i)} \\ &= \prod_{i \in J_z(w)} \chi_{p_i^{-1}(w_i)} \prod_{i \notin J_z(w)} \Big(1 - \sum_{y \in X_i^{(z)}} \chi_{p_i^{-1}(y)}\Big). \end{aligned}$$

Expanding the last product for $w = x$ and z yields (2) and (3). Formula (4) is an immediate consequence of (3).

STEP 4. The cosets $\chi_x + V \in C^X/V$ $(x \in X)$ are pairwise distinct.

Let $x, z \in X$ be such that $x \neq z$ and suppose $\chi_z - \chi_x \in V$. By (1)–(3), we obtain

$$\chi_z - \chi_x = 1 - \sum_{i=1}^{n} \sum_{y \in X_i^{(z)}} \chi_{p_i^{-1}(y)} - \chi_M, \tag{5}$$

where $M = \emptyset$ if $|J_z(x)| \geq 2$ and $M = p_i^{-1}(x_i)$ if $J_z(x) = \{i\}$. Assume first $C \neq \mathbb{Z}/2\mathbb{Z}$. Choose $w \in X$ such that $w \neq x$ and $|J_z(w)| = 2$. This is possible by our assumption on n and the X_i. Evaluating both sides of (5) at w we get 0 on the left side and -1 or -2 on the right side. This contradiction proves our assertion in the case $C \neq \mathbb{Z}/2\mathbb{Z}$. Assume now $C = \mathbb{Z}/2\mathbb{Z}$. Since $n \geq 3$ there is some $w \in X$ such that $w \neq x$, $|J_z(w)| = 2$ and, in addition, $i \notin J_z(w)$ if $J_z(x) = \{i\}$. Again evaluating both sides of (5) at w gives a contradiction.

Step 5. Suppose $C \neq \mathbb{Z}/2\mathbb{Z}$ and let M be a subset of X such that $\chi_M \in V$. Then $M = p_i^{-1}(Y_i)$ for some i and some $Y_i \subset X_i$.

If $M = X$ there is nothing to do. So assume $z \in X \setminus M$. By (4) there exist subsets $Y_i \subset X_i^{(z)}$ such that

$$\chi_M = \sum_{i=1}^{n} \sum_{y \in Y_i} \chi_{p_i^{-1}(y)}.$$

Taking squares we get

$$\chi_M = \chi_M^2 = \sum_{i=1}^{n} \sum_{y \in Y_i} \chi_{p_i^{-1}(y)} + 2 \sum_{i<j} \sum_{y \in Y_i \times Y_j} \chi_{p_{\{i,j\}}^{-1}(y)}.$$

Now using Step 1 we infer $Y_i \neq \emptyset$ for at most one i, which implies the assertion.

Step 6. Assume $C = \mathbb{Z}/2\mathbb{Z}$. Let $M \subsetneqq X$ and suppose $\chi_M \in V$. For any $z \in X \setminus M$ there exist $Y_i \subset X_i^{(z)}$ $(i = 1, \ldots, n)$ such that

$$M = \{x \in X : |\{i : x_i \in Y_i\}| \text{ is odd}\}.$$

By (4) there are $Y_i \subset X_i^{(z)}$ such that

$$\chi_M = \sum_{i=1}^{n} \sum_{y \in Y_i} \chi_{p_i^{-1}(y)} = \sum_{i=1}^{n} \chi_{p_i^{-1}(Y_i)}.$$

Now the claim follows from the equation $1 + 1 = 0$ in $\mathbb{Z}/2\mathbb{Z}$.

Step 7. Let $z \in X$ and $Y_i, Y_i' \subset X_i^{(z)}$ $(i = 1, \ldots, n)$. Set

$$M_Y = \{x \in X : |\{i : x_i \in Y_i\}| \text{ is odd}\}$$

and define $M_{Y'}$ in the same manner. Suppose we have $\emptyset \subsetneqq M_Y \subsetneqq M_{Y'}$. Then there exists an index i such that $M_Y = p_i^{-1}(Y_i)$ and $M_{Y'} = p_i^{-1}(Y_i')$, i.e. $Y_j = Y_j' = \emptyset$ for $j \neq i$.

Let $y \in Y_j$ for some j. Then $(z_1, \ldots, z_{j-1}, y, z_{j+1}, \ldots, z_n) \in M_Y \subset M_{Y'}$, which implies $y \in Y_j'$. So we conclude $Y_j \subset Y_j'$ for all j. Since $M_Y \neq M_{Y'}$ there is some i such that $Y_i \neq Y_i'$. Suppose now $Y_j \neq \emptyset$ for some $j \neq i$. Choose $y_j \in Y_j$ and $y_i' \in Y_i' \setminus Y_i$. Then $(z_1, \ldots, y_i', \ldots, y_j, \ldots, z_n) \in M_Y \setminus M_{Y'}$. This contradiction proves $Y_j = \emptyset$ for $j \neq i$. Similary, suppose $y_j' \in Y_j'$. Choose $y_i \in Y_i$. Since $Y_j = \emptyset$ we obtain $(z_1, \ldots, y_i, \ldots, y_j', \ldots, z_n) \in M_Y \setminus M_{Y'}$.

STEP 8. For any subset M of X define

$$B_M = \prod_{x\in M} (\chi_x + V) \in \mathcal{F}(C^X/V).$$

Then B_M is a block if and only if $\chi_M \in V$, in particular $B = B_X \in \mathcal{B}(C^X/V)$. We have

$$\mathcal{L}(B) = \{|X_1|, \dots, |X_n|\}, \quad v_B(|X_i|) = |\{j : |X_j| = |X_i|\}| \quad \text{if } C \neq \mathbb{Z}/2\mathbb{Z}$$

and

$$\mathcal{L}(B) = \{2, |X_1|, \dots, |X_n|\} \quad \text{if } C = \mathbb{Z}/2\mathbb{Z}.$$

By Steps 5–7 the blocks $B_{p_i^{-1}(y)}$, $i = 1, \dots, n$, $y \in X_i$, are irreducible. Therefore B has the following factorizations:

$$B = \prod_{y\in X_i} B_{p_i^{-1}(y)}, \quad i = 1, \dots, n. \tag{6}$$

Suppose first $C \neq \mathbb{Z}/2\mathbb{Z}$. We have to show that the factorizations (6) are the only ones for B. By Step 5 the irreducible divisors of B are given by the $B_{p_i^{-1}(y)}$ with $y \in X_i$ and $i = 1, \dots, n$. Now B is square free and two sets $p_i^{-1}(y)$, $p_j^{-1}(y')$ with $i \neq j$ have nonempty intersection. Hence the assertion follows.

Assume now $C = \mathbb{Z}/2\mathbb{Z}$. Let $z \in X$ and choose subsets $Y_i \subset X_i^{(z)}$ such that $Y_i \neq \emptyset$ for at least two indices i. Set $M_Y = \{x \in X : |\{i : x_i \in Y_i\}| \text{ is odd}\}$. By Steps 6 and 7 the blocks B_{M_Y} and $B_{X\setminus M_Y}$ are irreducible. Hence we obtain $2 \in \mathcal{L}(B)$. Suppose now that $B = B_1 \cdot \ldots \cdot B_k$ is some factorization different from all the ones in (6). We have to show that $k = 2$. Since B is square free there is some partition $X = M_1 \cup \ldots \cup M_k$, $M_s \cap M_t = \emptyset$ for $s \neq t$, such that $B_s = B_{M_s}$ for all s. Since the sets $p_i^{-1}(y)$, $p_j^{-1}(y')$ for $i \neq j$ have nonempty intersection, there exists some s, say $s = 1$, such that M_1 and therefore also $X \setminus M_1$ are not of the form $p_i^{-1}(Y_i)$ (for any $i = 1, \dots, n$, $Y_i \subset X_i$). Hence by Steps 6 and 7 again, $B_{X\setminus M_1}$ is irreducible, and we get $B_2 = B_{X\setminus M_1}$ and $k = 2$.

STEP 9. Suppose that $C \neq \mathbb{Z}/2\mathbb{Z}$ and let $L \subset \mathbb{N}_{\geq 2}$ be a finite subset and $v : L \to \mathbb{N}_+$ a function. We assume first that

$$(L, v) \neq (\{m\}, m \mapsto 1), (\{2\}, 2 \mapsto 2) \tag{7}$$

for all $m \geq 2$. Set $n = \sum_{l\in L} v(l)$ and choose finite sets $X_1, \dots, X_n$ such that for $l \in L$ exactly $v(l)$ of them have cardinality l. Then by our assumption (7) we have $n \geq 3$, or $n = 2$ and $|X_i| \geq 3$ for at least one i. Then the block $B \in \mathcal{B}(C^X/V)$ constructed in Step 8 satisfies $\mathcal{L}(B) = L$ and $v_B = v$. Note also that by Steps 1 and 2, C^X/V is free.

To finish the proof of the proposition in the case $C \neq \mathbb{Z}/2\mathbb{Z}$ we need to check the two remaining cases

(a) $L = \{m\}$, $v(m) = 1$ $(m \geq 2)$, and
(b) $L = \{2\}$, $v(2) = 2$.

In case (a) one may for example take

$$B = \left[\begin{pmatrix}1\\0\\\vdots\\0\end{pmatrix}\cdot\begin{pmatrix}-1\\0\\\vdots\\0\end{pmatrix}\right]\cdot\ldots\cdot\left[\begin{pmatrix}0\\\vdots\\0\\1\end{pmatrix}\cdot\begin{pmatrix}0\\\vdots\\0\\-1\end{pmatrix}\right] \in \mathcal{B}(C^m).$$

For (b) we can choose

$$\begin{aligned} B &= \left[\begin{pmatrix}1\\0\\0\end{pmatrix}\cdot\begin{pmatrix}-1\\0\\0\end{pmatrix}\right]\cdot\left[\begin{pmatrix}0\\1\\0\end{pmatrix}\cdot\begin{pmatrix}0\\0\\1\end{pmatrix}\cdot\begin{pmatrix}1\\0\\-1\end{pmatrix}\cdot\begin{pmatrix}-1\\-1\\0\end{pmatrix}\right]\\ &= \left[\begin{pmatrix}0\\1\\0\end{pmatrix}\cdot\begin{pmatrix}-1\\-1\\0\end{pmatrix}\cdot\begin{pmatrix}1\\0\\0\end{pmatrix}\right]\cdot\left[\begin{pmatrix}-1\\0\\0\end{pmatrix}\cdot\begin{pmatrix}0\\0\\1\end{pmatrix}\cdot\begin{pmatrix}1\\0\\-1\end{pmatrix}\right] \in \mathcal{B}(C^3). \end{aligned}$$

Step 10. Assume now $C = \mathbb{Z}/2\mathbb{Z}$ and let $L \subset \mathbb{N}_{\geq 2}$ be a finite set. Define $m = \min L$. Suppose that, for some $k \geq 1$, we have constructed a block $B \in \mathcal{B}(C^k)$ with $\mathcal{L}(B) = L - m + 2$. Then obviously $\mathcal{L}(0^{m-2}B) = L$. We may therefore assume that $2 \in L$. In this case, choose finite sets $X_1, \ldots, X_n$ with $n \geq 3$ and $L = \{|X_1|, \ldots, |X_n|\}$. Then the block B constructed in Step 8 satisfies $\mathcal{L}(B) = L$.

REFERENCES

[1] S. Chapman and A. Geroldinger, *Krull domains and monoids, their sets of lengths, and associated combinatorial problems*, in: Factorization in Integral Domains, D. D. Anderson (ed.), Lecture Notes in Pure and Appl. Math. 189, Marcel Dekker, 1997, 73–112.

[2] F. Kainrath, *A divisor theoretic approach towards the arithmetic of noetherian domains*, Arch. Math., to appear.

[3] —, *The distribution of prime divisors in finitely generated domains*, preprint.

[4] I. Kaplansky, *Infinite Abelian Groups*, third printing, The University of Michigan Press, 1960.

Institut für Mathematik
Karl-Franzes-Universität
Heinrichstraße 36
A-8010 Graz, Austria
E-mail: florian.kainrath@kfunigraz.ac.at

Received 26 February 1998