MINIMAL GENERATING SETS OF GROUPS, RINGS, AND FIELDS

LORENZ HALBEISEN, MARTIN HAMILTON, AND PAVEL RŮŽIČKA

Abstract. A subset X of a group (or a ring, or a field) is called *generating*, if the smallest subgroup (or subring, or subfield) containing X is the group (ring, field) itself. A generating set X is called *minimal generating*, if X does not properly contain any generating set. The existence and cardinalities of minimal generating sets of various groups, rings, and fields are investigated. In particular it is shown that there are groups, rings, and fields which do not have a minimal generating set. Among other result, the cardinality of minimal generating sets of finite abelian groups and of finite products of $\mathbb{Z}_n$ rings is computed.

Key words: minimal generating sets, cyclic groups, finite rings, field extensions
2000 Mathematics Subject Classification: **12E99** 20F05 12F99 13E15 13M99

0. Introduction

At the end of [1], in which the cardinalities of smallest spanning sets of rings were investigated, the notion of minimal generating sets of rings were introduced and some basic facts about their cardinality were given.

The notion of a minimal generating set of a ring can be generalized in a natural way to groups as well as to fields: A subset X of a group (or a ring, or a field) is called *generating*, if the smallest subgroup (or subring, or subfield) containing X is the group (ring, field) itself. A generating set X is called *minimal generating*, if X does not properly contain any generating set.

In the following we investigate the cardinalities and the existence of minimal generating sets of various groups, rings, and fields. In Section 1 it will be shown for example that there are rings which have minimal generating sets of different cardinalities. In Section 2 examples of groups, rings, and fields are given which do not have a minimal generating set. Finally in Section 3 the cardinality of smallest minimal generating sets of the ring of integer matrices, of finite products of cyclic groups, as well as of finite products of $\mathbb{Z}_n$ rings is computed.

1. The Cardinality of Minimal Generating Sets

In the following we investigate the cardinality of minimal generating sets of groups, rings, and fields. If a minimal generating set is finite, then we can even find a minimal generating set of *smallest* size; otherwise, if a minimal generating set is infinite, then we shall show that it has always the same cardinality as the corresponding group, ring, or field.

First we show that if the group, ring, or field, is infinite, then a minimal generating set is either finite, or has the same cardinality as the group, ring, or field.

In the sequel, the cardinality of a set S is denoted by $|S|$.

FACT 1.1. If S is an infinite group (infinite ring, infinite field) and S does not have a finite generating set, then every generating set of S has the same cardinality as S.

Proof. Let $S' \subseteq S$ be any infinite generating set of S. Since S' is generating, every element of S can be represented by a finite word involving elements of S' as well as of a finite set containing symbols like "(", ")", "+", "−", *etc.* Now, since the cardinality of the set of all such words is the same as the cardinality of S' (*cf.* [1]), this implies that $|S'| = |S|$. ⊣

It is clear that if the group, ring, or field, is finite, then there is always a minimal generating set of least cardinality.

As we have seen so far, the cardinality of a minimal generating set of say a ring is either finite or it has the same cardinality as the ring. In the latter case, the cardinality of a minimal generating set is determined by the cardinality of the ring. However, in the former case it may happen that minimal generating sets of different cardinalities exist. For example $\{1\}$ as well as $\{6, 10, 15\}$ are minimal generating sets of the ring $\mathbb{Z}$. Moreover, $\mathbb{Z}$, both as a ring and as group, has a minimal generating set of size m for every positive integer m (see Section 3).

2. The Existence of Minimal Generating Sets

So far, we did not address the question whether every group, ring, or field, has a minimal generating set. We know that if the group, ring, or field, is finite, then it has a minimal generating set and we already have seen an example of an infinite ring having finite minimal generating sets. On the other hand, there are infinite groups, rings, and fields, which do not have minimal generating sets. Let us start with groups.

Not every Group has a Minimal Generating Set.

THEOREM 2.1. The p-primary group $\mathbb{Z}_{p^\infty}$ does not have a minimal generating set.

Proof. The group $\mathbb{Z}_{p^\infty}$ is not cyclic, and all of its proper subgroups are finite and cyclic ([4, Theorem 10.13]), and the set of all subgroups of $\mathbb{Z}_{p^\infty}$ is well-ordered by inclusion. Hence, for all $a, b \in \mathbb{Z}_{p^\infty}$, either a lies in the subgroup generated by b or vice versa. Therefore, $\mathbb{Z}_{p^\infty}$ cannot have a minimal generating set. ⊣

Not every Field has a Minimal Generating Set. An example of a field which does not have a minimal generating set is the field of real numbers $\mathbb{R}$, but before we can prove this, we have to recall some definitions and results from Field Theory.

If F is a subfield of a field K, then K is called an **extension field** of F, and the dimension of K as an F-vector space is called the **degree** of K over F, and is denoted by $[K : F]$.

The following is a standard result from Field Theory:

PROPOSITION 2.2. (1) If L is an extension field of F and K is an extension field of L, then $[K : F] = [K : L][L : F]$.
(2) If K is an extension field of F and $a \in K$ is algebraic over F, with minimal polynomial $m(x)$ and $\deg m(x) = n$, then $[F(a) : F] = n$.

Let F be a field. We define the **characteristic** of F, $\operatorname{char} F$, to be the minimal number in the set $\{n \in \mathbb{N} : n \cdot 1 = 0\}$, provided the set is non-empty. If the set is empty, we define $\operatorname{char} F = 0$.

The following result [2, A.V. §11, Exercise 11] (see also [3, Theorem VIII.16.7]) will be crucial in order to prove that $\mathbb{R}$ has no minimal generating set:

PROPOSITION 2.3. If K is a field whose algebraic closure Ω is an extension of finite degree > 1, then $\Omega = K(i)$, where $i^2 = -1$. In particular $[\Omega : K] = 2$.

Now we are ready to prove the following:

THEOREM 2.4. $\mathbb{R}$ does not have a minimal generating set.

Proof. Suppose that G is a minimal generating set of $\mathbb{R}$, and let $r \in G$. Without loss of generality assume $r > 0$. Let F be the field generated by $G \setminus \{r\}$, so F is a subfield of $\mathbb{R}$. Then we have $\mathbb{R} = F(r)$ and also $\sqrt{r} \in \mathbb{R}$. Thus $\sqrt{r} \in F(r)$ and there are $f(x), g(x) \in F[x]$ where $g(x) \neq 0$ such that

$$\sqrt{r} = \frac{f(r)}{g(r)} .$$

Thus, $\frac{f(r)^2}{g(r)^2} - r = 0$ and consequently we get

$$f(r)^2 - rg(r)^2 = 0 .$$

Observe that the polynomial $h(x) = f(x)^2 - xg(x)^2$ is nonzero. Indeed, since $g(x)$ is nonzero, the polynomial $xg(x)^2$ has odd degree while the degree of $f(x)^2$ is even. Since $h(r) = 0$, r is algebraic over F. Thus $[F(r) : F]$ is finite. Now $F(r) = \mathbb{R}$, so $[\mathbb{R} : F]$ is finite. Also, we have that $[\mathbb{C} : F] = [\mathbb{C} : \mathbb{R}][\mathbb{R} : F]$, and also we know $[\mathbb{C} : \mathbb{R}] = 2$. Since $\mathbb{C}$ is the algebraic closure of F and $[\mathbb{C} : F] < \infty$, by Proposition 2.3 we have $[\mathbb{C} : F] = 2$ and therefore $[\mathbb{R} : F] = 1$ which implies $F = \mathbb{R}$. So, $G \setminus \{r\}$ generates the field $\mathbb{R}$, which is a contradiction to the fact that G is a minimal generating set of $\mathbb{R}$ and completes the proof. $\dashv$

Rings and Fields which do not have a Minimal Generating Set. With similar arguments as in the proof of Theorem 2.4 we can show the following result:

THEOREM 2.5. An algebraically closed field has not a minimal generating set.

Proof. Let C be an algebraicly closed field with a prime field P. Suppose that M is a minimal generating set of C. The set M is not finite, otherwise $C = P(M)$ would contain only finitely many roots of unity [2, A.V.§14.7 Corollary 2]. There is a finite subset N of M such that the polynomial $x^2 + 1$ splits in $P(N)$. Let $r \in M \setminus N$ and put $F = P(M \setminus \{r\})$. Arguing similarly as in the proof of Theorem 2.4, $\sqrt{r} \in F(r)$, whence

$$\sqrt{r} = \frac{f(r)}{g(r)},$$

for some $f(x), g(x) \in F[x]$, and, consequently, r is a root of a nonzero polynomial $h(x) = f(x)^2 - xg(x)^2$. Thus r is algebraic over F, and so the degree $[C : F]$ is finite. By Proposition 2.3 $C = F(i)$, where $i^2 = -1$. Since $x^2 + 1$ splits in F, $C = F$, which is a contradiction. ⊣

Before we can prove that an algebraic closure of a finite field, considered as a ring, does not have a minimal generating set, we would like to recall the following result from Field Theory:

Proposition 2.6. Let A be the algebraic closure of some field F. Then every subring of A containing F is a subfield of A.

Proof. Let R be a subring of A containing F. Let $r \in R$, $r \neq 0$. As A is algebraic over F, there is a polynomial $f(x) \in F[x]$ such that $f(r) = 0$. That is:

$$r^n + a_{n-1}r^{n-1} + \ldots + a_1 r + a_0 = 0$$

$$r(r^{n-1} + a_{n-2}r^{n-2} + \ldots + a_1) = -a_0$$

Now provided that $-a_0 \neq 0$, it has an inverse, so

$$r(-a_0^{-1}r^{n-1} - a_0^{-1}a_{n-2}r^{n-2} - \cdots - a_0^{-1}a_1) = 1$$

so r has a multiplicative inverse. If $a_0 = 0$, then since $r \neq 0$, we have that $r^{n-1} + a_{n-2}r^{n-2} + \cdots + a_1 = 0$ and we can carry out the same process. Thus R is a subfield. ⊣

Corollary 2.7. Every subring of an algebraic closure of a finite field is its subfield.

Proof. Let A be an algebraic closure of a finite field F of a characteristic p and let R be its subring. Since the prime field $\mathbb{Z}_p$ of A is contained in R and A is an algebraic closure of $\mathbb{Z}_p$, R is a subfield of A by Proposition 2.6. ⊣

Thus a set M generates an algebraic closure A of a finite field as a ring iff it generates A as a field. Theorem 2.5 yields the desired result.

Theorem 2.8. Let A be the algebraic closure of a finite field F. Then A, considered as a ring, does not have a minimal generating set.

3. Examples of Generating Sets

Generating Sets of $\mathbb{Z}$ and $\mathbb{Q}$. Obviously, $\{1\}$ is a minimal generating set of least cardinality of the ring of integers $\mathbb{Z}$. On the other hand, there are also minimal generating sets of $\mathbb{Z}$ like $\{2, 3\}$ which are not smallest. Moreover, for any set of mutually different prime numbers $p_1, \ldots, p_m$, the set $\{\frac{n}{p_1}, \ldots, \frac{n}{p_m}\}$, where $n = \prod_{i=1}^m p_i$, is a minimal generating set of $\mathbb{Z}$.

In contrast, the empty set generates the field of rationals $\mathbb{Q}$, as the smallest field containing the empty set must contain a 1 and a 0, and we can obtain any non-zero rational number from 1 by addition and division. On the other hand, if we consider $\mathbb{Q}$ as a ring, then every generating set must be infinite and an example of a minimal generating set of $\mathbb{Q}$ is $G = \{\frac{1}{p} : p \text{ prime}\}$. To see this, consider any $\frac{m}{n} \in \mathbb{Q}$. Without loss of generality assume that n is positive and write $\frac{m}{n}$ as

$$\frac{m}{n} = \frac{m}{p_1 p_2 \cdot \ldots \cdot p_r} = m\frac{1}{p_1}\frac{1}{p_2}\cdots\frac{1}{p_r}$$

where $n = p_1 p_2 \cdot \ldots \cdot p_r$. To see that G is minimal, notice that $\frac{1}{p}$ (where p is any prime number) cannot be written as a combination of elements of $G \setminus \{\frac{1}{p}\}$.

Minimal Generating Sets of the Ring of Integer Matrices. In the following we investigate minimal generating sets of $M_n(\mathbb{Z})$, the ring of $n \times n$ matrices with integer entries.

Let us consider first the case $n = 2$: For the matrix $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ we have

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} b & a \\ d & c \end{pmatrix}$$

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} c & d \\ a & b \end{pmatrix}$$

Thus, multiplying $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ from the right will swap the columns and multiplying from the left will swap the rows, and therefore, with $\left\{\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\right\}$ we can write the matrices $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$, $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$, $\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$, and $\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$, and hence, the ring $M_2(\mathbb{Z})$. So, since no singleton set can generate the ring, the cardinality of a smallest generating set of $M_2(\mathbb{Z})$ is 2. Similarly one can show that the set

$$\left\{\begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 0 & \cdots & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ 1 & 0 & 0 & \cdots & 0 \end{pmatrix}\right\}$$

generates $M_n(\mathbb{Z})$, and since no singleton will generate the ring, the cardinality of a smallest generating set of $M_n(\mathbb{Z})$ is always 2.

Minimal Generating Sets of Finite Abelian Groups. Notice that every finite abelian group is isomorphic to a finite product of finite cyclic groups (see *e.g.*, [4, Corollary 10.22]). So, in order to investigate finite abelian groups we can just consider finite products of finite cyclic groups.

In the following we show how to compute the cardinality of a smallest minimal generating set of finite products of finite cyclic groups.

Theorem 3.1. Given a product of finite cyclic groups $C = \mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_k}$ where all the n_i's are strictly greater than 1. For every prime p let $d_p = \big|\{i \leq k : p \mid n_i\}\big|$ and let

$$\mu_C = \max\{d_p : \ p \text{ prime}\} .$$

Then the smallest minimal generating set of C is of size μ_C.

Recall the following generalization of the Chinese Remainder Theorem:

Proposition 3.2. Assume $m_1, \ldots, m_r$ are pairwise relatively prime. Let $b_1, \ldots, b_r$ be arbitrary integers and $a_1, \ldots, a_r$ satisfy $(a_k, m_k) = 1$ for $k = 1, \ldots, r$. Then the linear system of congruences

$$\begin{array}{rcll} a_1 x & \equiv & b_1 & \pmod{m_1} \\ a_2 x & \equiv & b_2 & \pmod{m_2} \\ & \vdots & & \\ a_r x & \equiv & b_r & \pmod{m_r} \end{array}$$

has exactly one solution modulo $m_1 \cdot \ldots \cdot m_r$.

The existence of a set of size μ_C which generates C follows from the above Proposition (see also the example below), and that no set of size smaller than μ_C is generating the group C is a consequence of the following:

Lemma 3.3. Let p be any prime number, then the group $\mathbb{Z}_{p^{l_1}} \times \ldots \times \mathbb{Z}_{p^{l_s}}$, where all the l_i's are positive integers, cannot be generated by less than s elements.

Proof. Consider first a product of s copies of $\mathbb{Z}_p$. Then, since p is prime, $(\mathbb{Z}_p)^s$ can be considered as an s-dimensional vector space over $\mathbb{Z}_p$, and therefore, every minimal generating set of a product of s copies of $\mathbb{Z}_p$ has s elements. On the other hand, it is easy to see that there exists a minimal generating set of $\mathbb{Z}_{p^{l_1}} \times \ldots \times \mathbb{Z}_{p^{l_s}}$ containing s elements and every minimal generating set of $\mathbb{Z}_{p^{l_1}} \times \ldots \times \mathbb{Z}_{p^{l_s}}$ induces a generating set of $(\mathbb{Z}_p)^s$. Hence, the the group $\mathbb{Z}_{p^{l_1}} \times \ldots \times \mathbb{Z}_{p^{l_s}}$ cannot be generated by less than s elements and the cardinality of a smallest minimal generating set of this group is equal to s. ⊣

An Example. Consider the group $C = \mathbb{Z}_6 \times \mathbb{Z}_{98} \times \mathbb{Z}_{63} \times \mathbb{Z}_{54}$. The prime numbers involved in representing $6, 98, 63, 54$ are $2, 3, 7$, and we compute $d_2 = d_3 = 3$ and $d_7 = 2$, thus, the size of a smallest minimal generating set is 3. Now, the order of the element $g_1 = (1, 2, 0, 0)$ in C is $6 \cdot 49$ (since 6 and 49 are relatively prime), $49 \cdot g_1 = (1, 0, 0, 0)$ and $246 \cdot g_1 = (0, 2, 0, 0)$. The order of $g_2 = (0, 49, 7, 0)$ is $2 \cdot 9$, $9 \cdot g_2 = (0, 49, 0, 0)$ and $10 \cdot g_2 = (0, 0, 7, 0)$, and $25 \cdot 246 \cdot g_1 + 9 \cdot g_2 = (0, 1, 0, 0)$. Further, the order of $g_3 = (0, 0, 9, 1)$ is $7 \cdot 54$, $162 \cdot g_3 = (0, 0, 3, 0)$ and $217 \cdot g_3 = (0, 0, 0, 1)$, and $10 \cdot g_2 + 5 \cdot 162 \cdot g_3 = (0, 0, 1, 0)$. Thus, the elements $(1, 0, 0, 0)$, $(0, 1, 0, 0)$, $(0, 0, 1, 0)$, and $(0, 0, 0, 1)$ belong to the group generated by g_1, g_2, and g_3, and hence, $\{g_1, g_2, g_3\}$ is a generating set of C.

Minimal Generating Sets of Finite Products of $\mathbb{Z}_n$ Rings. In the following we compute the cardinality of smallest minimal generating sets of finite products of $\mathbb{Z}_n$ rings, where we assume that each of the $\mathbb{Z}_n$ rings contains at least 2 elements; but first let us prove some preliminary results about rings, where we assume that all rings as well as all their subrings contain the unit element.

Let R be a ring. We denote by $n\times 1$ the sum $\underbrace{1+\ldots+1}_{n \text{ times}}$ of n copies of 1 in R. Similarly as for fields, we can define a **characteristic** of a ring R, denoted by $\operatorname{char}(R)$, as the minimal positive integer n such that $n \times 1 = 0$. If $n \times 1 \neq 0$ for all positive integers n, we define $\operatorname{char}(R) = 0$.

For a positive integer n, let $\varphi(n)$ denote the value of the Euler φ-function in n (see *e.g.*, [4, Exercises 2.19–2.23]). Recall that if n and k are relatively prime, then $k^{\varphi(n)} \equiv 1 \pmod{n}$. In particular, in a ring of a characteristic n, $k^{\varphi(n)} \times r = r$, for every k relatively prime to n and every $r \in R$.

Lemma 3.4. Let p be a prime number and let the unital ring $R = R_1 \times \ldots \times R_p$ be a product of rings of characteristics p^{n_i}, $i = 1, \ldots, p$, respectively. If R_i is generated by n elements for every $i = 1, \ldots, p$, then R is generated by $n + 1$ elements.

Proof. We will regard elements of the ring R as p-tuple $\mathbf{r} = (r_1, \ldots, r_p)$. For $i = 1, \ldots, p$ denote by $r_{i,1}, \ldots, r_{i,n}$ the generators of R_i. Now, set $\mathbf{r}_j = (r_{1,j}, \ldots, r_{p,j})$, for every $j = 1, \ldots, n$, and $\mathbf{r} = (1, 2, \ldots, p-1, 0)$. We claim that $\mathbf{r}_j$, $j = 1, \ldots, n$ together with $\mathbf{r}$ generate R. Thus denote by S the subring of R generated by these elements. For $i = 1, \ldots, p-1$ denote by $f_i(x)$ the polynomial

$$f_i(x) = (x-1)\ldots(x-(i-1)\times 1)x(x-(i+1)\times 1)\ldots(x-(p-1)\times 1).$$

Observe that $f_i(\mathbf{r})$ belongs to the subring of R generated by $\mathbf{r}$, and

$$f_i(\mathbf{r})^{\varphi(p^{n_i})} = (0, \ldots, 0, 1, 0, \ldots, 0),$$

where the nonzero element is in the i^{th} coordinate. It follows that

$$\mathbf{r}_j f_i(\mathbf{r})^{\varphi(p^{n_i})} = (0, \ldots, 0, r_{i,j}, 0, \ldots, 0) \in S,$$

for every $i = 1, \ldots, p-1$, $j = 1, \ldots, n$. Finally, since

$$\mathbf{r}_j - \sum_{i=1}^{p-1} \mathbf{r}_j f_i(\mathbf{r})^{\varphi(p^{n_i})} = (0, \ldots, 0, r_{p,j})$$

belongs to S as well, we conclude that $R = S$. ⊣

Given a real number r, we denote by $\lceil r \rceil$ the smallest integer n such that $r \leq n$.

Proposition 3.5. Let p be a prime number. The smallest cardinality of the generating set of the unital ring $R = \mathbb{Z}_{p^{t_1}} \times \ldots \times \mathbb{Z}_{p^{t_n}}$, where $1 \leq t_1, \ldots, t_n$, is $\lceil \log_p n \rceil$.

Proof. Put $k = \lceil \log_p n \rceil$, and let $r_1, \ldots, r_m$ be a generating set of R of the smallest cardinality. Since $\mathbb{Z}_{p^{t_1}}$ is as an abelian group generated by the unit element, it is generated by the empty set as a unital ring. Applying Lemma 3.4, we prove by

induction that the ring $S = \mathbb{Z}_{p^{t_1}} \times \ldots \times \mathbb{Z}_{p^{(t_{p^k})}}$, where $t_{n+1}, \ldots, t_{p^k}$ are arbitrary positive integers, is generated by k elements. Since R is a homomorphic image of S, $m \le k$.
Observe that

$$R/pR \simeq \underbrace{\mathbb{Z}_p \times \ldots \times \mathbb{Z}_p}_{n\times}.$$

The images of $r_1 + pR, \ldots, r_m + pR$ of $r_1, \ldots, r_m$, respectively, in R/pR must generate R/pR. If $m < k$, there would be $1 \le j < k \le n$ such that the j^{th} coordinate of the image of each r_i in R/pR (R/pR is regarded as the product of n copies of $\mathbb{Z}_p$) equals to its k^{th} coordinate. This contradicts the fact that $r_1 + pR, \ldots, r_m + pR$ generate R/pR and so $m \ge k$. ⊣

Lemma 3.6. Let $R = R_1 \times \ldots \times R_t$ be a product of rings of characteristics $p_i^{n_i}$, $i = 1, \ldots, t$, respectively, where $p_1, \ldots, p_t$ are distinct primes. If each of the rings R_i is generated by n elements, then the ring R is generated by n elements as well.

Proof. For $i = 1, \ldots, t$ denote by $r_{i,1}, \ldots, r_{i,n}$ the generators of R_i. For $j = 1, \ldots, n$ set $\mathbf{r}_j = (r_{1,j}, \ldots, r_{t,j})$. We claim that the elements $\mathbf{r}_1, \ldots, \mathbf{r}_n$ generate R. Indeed, for every $i = 1, \ldots, t$ set

$$m_i = \left(\frac{p_1^{n_1} \ldots p_t^{n_t}}{p_i^{n_i}} \right)^{\varphi(p_i^{n_i})},$$

and observe that

$$\underbrace{\mathbf{r}_j + \ldots + \mathbf{r}_j}_{m_i\times} = (0, \ldots, 0, r_{i,j}, 0, \ldots, 0),$$

for every $j = 1, \ldots, n$.

⊣

Theorem 3.7. Given a product $C = \mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_k}$ where all the n_i's are strictly greater than 1. For every prime p let $d_p = \left|\{i \le k : p \mid n_i\}\right|$ and let

$$\nu_C = \max \left\{ \lceil \log_p d_p \rceil : \ p \text{ prime dividing } n_1 \ldots n_k \right\}.$$

Then the smallest minimal generating set of C as a ring is of size ν_C.

Proof. Observe that if $n = p_1^{k_1} \ldots p_t^{k_t}$ is a decomposition of n into a product of primes, then

$$\mathbb{Z}_n \simeq \mathbb{Z}_{p_1^{k_1}} \times \ldots \times \mathbb{Z}_{{p_t}^{k_t}}$$

both as a group and as a ring. It follows that $C \simeq C_1 \times \ldots \times C_s$, where $p_1, \ldots, p_s$ are all (pairwise distinct) primes dividing $n_1 \cdot \ldots \cdot n_k$ and C_i is a ring isomorphic to the product $\mathbb{Z}_{{p_i}^{k_{1,i}}} \times \ldots \times \mathbb{Z}_{{p_i}^{k_{d_p,i}}}$. Now apply Proposition 3.5 and Lemma 3.6. ⊣

References

[1] Nadia Boudi and Lorenz Halbeisen: *The cardinality of smallest spanning sets of rings*, ***Quaestiones Mathematicae***, vol. 26(3) (2003), 321–325.

[2] Nicholas Bourbaki: ***Elements of Mathematics: Algebra II, Chapters 4-7***, (translated by P.M. Cohn & J. Howie), Springer-Verlag (1988).

[3] Ladislav Procházka, Ladislav Bican, Tomáš Kepka, Petr Němec: ***Algebra***, Academia [Publishing House of the Czech Academy of Sciences], Prague (1990).

[4] Joseph J. Rotman: ***An Introduction to the Theory of Groups***, Fourth Edition, Springer-Verlag (New York). 1995

Institut für Informatik und angewandte Mathematik, Universität Bern, Neubrückstrasse 10, CH-3012 Bern, Switzerland, halbeis@iam.unibe.ch

Department of Mathematics, University of Glasgow, Glasgow G12 8QW, Scotland, mh@maths.gla.ac.uk

Katedra Algebry, Univerzita Karlova v Praze, Sokolovská 83, 186 75 Praha 8, Czech Republic, ruzicka@karlin.mff.cuni.cz