

On Existence of Minimal Generating Sets And Maximal Independent Sets In Groups And The Additive Semigroup of Integers

Zsolt, Lipcsey.

Department of Mathematics, University of Calabar, Calabar, CRS, Nigeria.

Sampson, Marshal I.

Department of Mathematics, Akwa Ibom State University, Ikot Akpaden, Nigeria.

ABSTRACT.

There is an existing theorem showing that not every group has a minimal generating set, by relying on a claim that all Proper Subgroups of infinite P – Primary Group (a group G in which the order, $n(g)$ of its element g is the power of some prime p) are finite and cyclic. This paper shows as one of its objectives that not all Proper Subgroups of an infinitely generated P – Primary Group are finite and cyclic. Furthermore, the concepts of Maximal Independent sets and Minimal Generating Set are investigated for condition under which both concepts coincide. It is also shown that in the additive semigroup of integers, there are infinite minimal generating sets with different number of elements. This gives the implication that the dimension of vector spaces do not have analog in semigroups. Equivalently, these same examples serve as examples of infinite inequivalent maximal independent sets.

Keywords: Semigroup, Minimal Generating Set, Maximal Generating Set, Independent Set, Generating set, Ordering, Cyclic Group, p -primary Group, additive semigroup.

Date of Submission: 21-07-2023

Date of Acceptance: 31-07-2023

I. Introduction

This paper focuses on subset of semigroups which determines the whole semigroup through algebraic closure. Such subsets are called generating sets. There may be many such sets but the ones with smallest number of elements are preferred. We call a generating set minimal if it does not have a proper generating subset. The question of whether a finite group, ring, or field, respectively has a minimal generating set has been discussed in some papers. It is presented in a paper by (Halbeisen, L. and Co, 2007) that some infinite groups, rings, and fields, do not have minimal generating sets. We shall be discussing some of these claims. Specifically, in Theorem 2.1. of (Halbeisen, L. and Co, 2007) the infinite p -primary group was used to support their claim that not every Group has a Minimal Generating Set. We study this result with the aim of clarifying some areas of doubt. We are of the opinion that any group should have a generating set however it may be infinite set.

Furthermore, in this paper, we also investigate the conditions under which certain sets called the Maximal independent sets are equivalent to Minimal generating Set. A set is independent if no element of the set can be generated by the remaining members of the set. An independent set in which there is no independent set containing it as proper subset, is called a Maximal Independent set.

Our Approach

To achieve the objectives of this paper, we begin with some definitions of terms and concepts. Next we dwell on the existence of Minimal generating sets in group with regards to a result of (Halbeisen, L. and Co, 2007). In section 2.3.2 we consider proper subgroups of p -primary groups and in section 2.3.3 show that not all Proper Subgroups of the p -primary Group are finite and cyclic. This negates an important requirement in the proof of the theorem (section 2.3.1.) by (Halbeisen, L. and Co, 2007) that the p -primary group Z_{p^∞} does not have a minimal generating set, leaving the theorem yet unverified.

We also present our opinion about existence for the case of a finite group. We show that when a group is finite, there is a simple algorithm to find a generating set.

We also gave Condition for Maximal Independent sets to be Minimal Generating Set. This is stated in the algorithm for determining the generator of a finite group in section 2.3.5.

There is the question of whether the dimension of vector spaces have analogues in other algebraic structures. We present an example to show that the dimension of vector spaces do not have analog in

semigroups since in the additive semigroup of integers as we shall later see, there are infinite minimal generating sets with different number of elements. This becomes a tool for showing that there are infinite inequivalent maximal independent sets in a semigroup.

Remark

We will later state Theorem 2.1. of (Halbeisen, L. and Co, 2007) as an example 2.3.1. here for easier referencing.

Definition of Terms

We define some important terminologies about the subject of the studies. For other terms not defined here, we refer readers to (Gould, V., 2010) and (Howie, 1976).

Definition (Semigroup)

Let S be a set and $*$: $S \times S \rightarrow S$ be a binary operation that maps each ordered pair (x, y) of S into an element of S . S is a Semigroup if $\forall x, y, z \in S$,

$$(x * y) * z = x * (y * z)$$

Definition (Subsemigroup)

Let $\{S, *\}$ be an ordered pair, where S is a semigroup and " $*$ " is the binary operation in S . A subsemigroup of $\{S, *\}$ is a non-empty subset $H \subset S$ of S which is closed under the multiplication of S .

Definition (Generating Set)

Let S be a semigroup and let $H \subset S$ be a nonempty subset of S . Then H is a generating set of S if $S = \langle H \rangle := \left\{ \prod_{j=1}^k a_j \mid \forall \{a_j\}_{j=1}^k \subset H, 1 \leq k < \infty \right\}$

where $\langle H \rangle$ is called the subsemigroup generated by H .

Examples (Generating Sets)

(i) **Generating Sets of \mathbb{Z} and \mathbb{Q}** (Halbeisen and Co, 2007).

Obviously, $\{1\}$ is a minimal generating set of the ring of integers \mathbb{Z} . On the other hand, there are also generating sets of \mathbb{Z} like $\{2, 3\}$ which are not smallest. Moreover, for any set of mutually different prime numbers p_1, \dots, p_m , the set $\left\{ \frac{n}{p_1}, \dots, \frac{n}{p_m} \right\}$ where $n = \prod_{i=1}^m p_i$ is a minimal generating set of \mathbb{Z} . (See also section 1.3.5. for an important observation about this example.)

Moreover, $\{1\}$ is the minimal generating set of \mathbb{Q} ($\langle \{1\} \rangle = \mathbb{Q}$) since we can obtain any non-zero rational number from 1 by addition and division as the field operations. Notice also that $\langle \{0, 1\} \rangle = \mathbb{Q}$.

Important Observation and Questions

From 1.3.4 (i), it is clear that the additive group Z has infinite different generating sets (for example $\{1\}$ and $\{2, 3\}$) with different number of elements, hence the generating set $\{1\}$ has the smallest number of elements. Section 1.3.6. below gives us a clearer understanding of whether to call this the minimal or minimum generating set. This will depend strongly on the comparability of these generating subsets.

Definition (Minimum/maximum):

Let X be a totally ordered set, let H be a nonempty subset of X .

$$\min(H) \leq x \forall x \in H; \quad \max(H) \geq x, \forall x \in H;$$

Definition (Minimal/Maximal)

Let X be a partially ordered set, let H be a nonempty subset of X .

m is a minimal element of H if there is no x in H such that $x < m$.

M is a maximal element of H if there is no x in H such that $x > M$

Remarks

Note that in the Minimal/Maximal case all uncomparable elements are out! In the example 1.3.4 (i) above, $\{1\} \not\subset \{2, 3\}$ and so it would be improper to use the term "Minimal generating set" as the suitable term in this case should be "Minimum generating set".

Definition (Rank of a Semigroup)

Let S be a semigroup, let $B \subset S$ be a subsemigroup of S and let $G_B \subset S$ be such that $G_B \subset S$ is a generating system of $B: B = \langle G_B \rangle$. The rank of a semigroup B is given by

$$\text{rank}(B) := \min_{B=\langle G_B \rangle} \{|G_B|\}$$

Remark

The rank of an algebraic structure is the size of its generating set with the least number of elements.

Definition (Independent Element of a Semigroup)

An element $a \in S$ is independent from a subset $U \subset S$ if $a \notin \langle U \rangle$.

Definition (Independent Subsets of a Semigroup)

Let S be a semigroup and let $U \subset S$. If $\forall u \in U, u \notin \langle U \setminus \{u\} \rangle$, then U is an independent set.

Definition (Dependent Sets of Semigroup)

Let S be a finite semigroup and let $U \subset S$. U is dependent if, $\exists u \in U, u \in \langle U \setminus \{u\} \rangle$.

Definition (Maximal Independent Sets of semigroup)

A Maximal Independent subset $U \in S$ of a semigroup S is that subset $U \in S$ in which including any other element in the set makes it dependent.

Definition (Basis)

A subset $B \subset S$ is a basis in S if B is a minimal generating system in S .

II. Existence of Minimal Generating Sets in Groups

We now focus attention to the question of whether every group has a minimal generator. It is not in doubt here that when a group, ring, or field, is finite then it has a minimal generating set. The theorem(2.2) below by (Halbeisen, L. and Co, 2007) states with the infinite p-primary group as example, that not all groups have minimal generating sets and this is the focus of the next few sections. We begin quickly with the definition of a p-primary group

Definition (p-primary Group)

Let p be a prime number and G be a group. Let $n(g)$ be the order (number of elements) of each $g \in G$. G is p-primary if each $g \in G$ has order $n(g)$ as the power of p .

Theorem (Halbeisen, L. and Co, 2007)

The p-primary group Z_{p^∞} does not have a minimal generating set.

Proof. The proof is as given in Page 2 of (Halbeisen, L. and Co, 2007)

In summary, The group Z_{p^∞} is not cyclic, and all of its proper subgroups are finite and cyclic and the set of all subgroups of Z_{p^∞} is well-ordered by inclusion. Hence, for all $a, b \in Z_{p^\infty}$, either a lies in the subgroup generated by b or vice versa. Therefore, Z_{p^∞} cannot have a minimal generating set.

■

Remarks (About Proper Subgroups of the p-primary Group)

The example 2.2. by (Halbeisen and Co., 2007) relies strongly on the premise that all proper subgroups of the infinite p-primary group, Z_{p^∞} are finite and cyclic. To strengthen our claim against the result in 2.2., it suffices to show with an example that not all proper subgroups of Z_{p^∞} are finite and cyclic. The next sections are devoted to showing this.

Example (Not all Proper Subgroups of the Infinite p-primary Group are finite and cyclic)

Let $\{g_i\}_{i=1}^\infty$ be a group generator such that $g_i^{p^i} = e$. Let us form the p-primary group

$$G := \prod_{i=1}^{\infty} \langle g_i \rangle$$

Then $(e, e, \dots, e, \dots) \in G$ is the unit element.

Let $Gen, 0 := \{h_j | h_j = (e, e, e, g_j, e_{j+1}, \dots, e_n, \dots), 1 \leq j < \infty\}$.

$G \supset Gen, 0$ and $\langle Gen, 0 \rangle \subset G$, (where 0 emphasises that this does not generate G) because if $U \in \langle Gen, 0 \rangle$, then U has e in each of its components except finite components. In other words,

$$U = (e, g_2^3, e, e, g_5^1, 0, \dots, 0, g_{21}^{11}, 0, \dots, 0)$$

Hence $\langle Gen, 0 \rangle \subset G$ is a proper non-cyclic, non-infinite subgroup.

Clearly, there exists a p-primary group $\langle Gen, 0 \rangle$ which is a minimal generator of the subgroup

$$U = (e, g_2^3, e, e, g_5^1, 0, \dots, 0, g_{21}^{11}, 0, \dots, 0)$$

and $\langle Gen, 0 \rangle$ is a proper non-cyclic subgroup and non-infinite subgroup.

One can make to any subset $W \subset N$ a subgroup $U_W = e_j$ if $j \notin W$ and g_j if $j \in W$. This gives as many subgroups as many subsets N has.

Conclusion

Not all proper subgroups of the infinite p-primary group, Z_{p^∞} are finite and cyclic. The attempt to use this idea to prove that the infinite p-primary group do not have minimal generating set fails to be valid for this reason.

III. RELATIONSHIP BETWEEN MINIMAL GENERATING SETS, INDEPENDENT SETS AND MAXIMAL INDEPENDENT SETS.

Introduction

In this section we study the relationship between the minimal generating set, the independent set and the maximal independent set of a semigroup. We give as the main result of this section, the condition under which the minimal generating set coincides with the maximal independent set of any given semigroup.

Theorem (Lipcsey, Z. & Sampson, M. I., 2022)

If a generating set G is independent, then G is minimal Generating Set.

Proof. Let $x \in G$ be any element. Then $x \notin \langle G \setminus \{x\} \rangle$. Hence $\langle G \setminus \{x\} \rangle$ is not a generating set. Let $\emptyset \neq H \subset G \neq H$. Then there is at least one element $x \in G \setminus H \Rightarrow G \setminus \{x\} \supset H$. Since $G \setminus \{x\}$ is not a generating set, its subset H is also not a generating set.

Theorem (Lipcsey, Z. & Sampson, M. I., 2022)

A generating set G of a structure is minimal if G is independent (for any structure like vector spaces, groups, semi-groups, monoids etc.).

Proof.

A generating set G is minimal \Rightarrow it is independent: Let $x \in G$ be any element. If $x \in \langle G \setminus \{x\} \rangle$ then

$$\langle G \setminus \{x\} \rangle \cup \{x\} \subset \langle G \setminus \{x\} \rangle \Rightarrow S = \langle G \rangle = \langle \langle G \setminus \{x\} \rangle \cup \{x\} \rangle \subset \langle \langle G \setminus \{x\} \rangle \rangle$$

Which contradicts with the minimality of G .

Theorem (Condition for Maximal Independent sets to be Minimal Generating Set)

Let S be a semigroup and let $H \subset S$ be a maximal independent set. If $\exists A \subset S$ such that $H \cup A$ is a generating set and $\forall x \in H, x \notin \langle (H \cup A) \setminus \{x\} \rangle$ and $A \cap \langle H \rangle = \emptyset$. Then H is a minimal generating set.

Proof.

1. If H is a generating set then it is minimal by its independence and our theorem (3.2.) about minimal generating sets.

2. Assume that $\langle H \rangle \subset S$ is a proper subset of S . Then $\emptyset \neq A := S \setminus \langle H \rangle$ such that

$\forall x \in H, x \notin \langle (H \cup A) \setminus \{x\} \rangle$. Then let $B := A \cup H \subset S$. Then $A \cup H \subset S$ is a generating set by

$$\langle B \rangle = \langle A \cup H \rangle \supset \langle A \rangle \cup \langle H \rangle \supset (S \setminus \langle H \rangle) \cup \langle H \rangle = S.$$

Let us well order A , and let us select a minimal generating set from B with the generating set selector algorithm as follows:

Let the starting state be as follows: Let $H := A, B := H$ (Elements are to be selected from

H and B is to be the already selected independent elements of the current generating set and

independent from be the starting set H).

Let us select $k := \min H$. Then we remove the selected e_k from H . If $e_k \in \langle H \cup B \rangle$ then we repeat the process from selecting a new element e_k , removing it from H as long as we get one such that $e_k \notin \langle H \cup B \rangle$ from H . Then $B \cup \{e_k\} \supset H$, and it is independent which contradicts with the maximality of H . Therefore H is a minimal generating set.

IV. Cardinality of Minimal Generating Sets and Maximal Independent Sets

Introduction

We ask the question of whether if S is a semigroup, and $G_1, G_2 \subset S$ are minimal generating sets, then $|G_1| = |G_2|$. Also the research targets (following vector spaces) that if $I_1, I_2 \subset S$ are maximal independent sets, then $|I_1| = |I_2|$. We present in this section, an example to show that the dimension of vector spaces do not have analog in semigroups since, as we shall see, in the additive semigroup of integers there are infinite minimal

generating sets with different number of elements. Equivalently, these same examples serve as examples of infinite inequivalent maximal independent sets.

The additive group Z.

Let $\{Z, +, -, 0\}$ be the additive group of integers and let the commutative semigroup – monoid of integers be $\{\hat{Z}, +, 0\}$.

Theorem

Let $\{e_i\}_i^k \subset N$. $\{e_i\}_i^k$ are coprime if and only if $\exists \{x_i\}_i^k \subset Z$ such that

$$\sum_{i=1}^k x_i e_i = 1 \tag{4.3}$$

Proof. (1). If $HCF(\{e_i\}_i^k) = 1$, then by Euclid the statement (4.3) holds.

(2). Let (4.3) be true. Assume that $h = HCF(\{e_i\}_i^k) > 1$. Then $e_i = h e'_i, 1 \leq i \leq k$. Hence

$$1 = \sum_{i=1}^k x_i e_i = \sum_{i=1}^k x_i h e'_i = \left(\sum_{i=1}^k x_i e'_i \right) h \neq 0 \tag{4.4}$$

Hence $(\sum_{i=1}^k x_i e'_i) \neq 0$ which contradicts to $1 = (\sum_{i=1}^k x_i e'_i) h \neq 0$.

Hence $\nexists h > 0$ common factor.

Definition.

A set $G \subset N$ is a generating set if $\langle G \rangle = Z$. G is minimal if $\forall \emptyset \neq H \subset G, H \neq G \implies \langle H \rangle \neq Z$.

Theorem.

A finite set $G \subset Z$ is a generating set of Z iff $HCF(G) = 1$. It is minimal iff $HCF(H) > 1, \forall \emptyset \neq H \subset G, H \neq G$.

Lemma.

Let $\{Z, +, -, 0\}$ be the additive group of integers and let $n, m \in Z$. Then

$$n \times m := \begin{cases} \frac{n + n + n + \dots + n}{m}, & \text{if } m \geq 0 \\ \frac{-n - n - n - \dots - n}{-m}, & \text{if } m < 0 \end{cases} \tag{4.5}$$

hence or otherwise, $n \times m$ can be computed as the equation shows in the group $\{Z, +, 0, 1\}$ for any two integers.

Proof. The proof is left to the reader.

Corollary (On Cardinality of a Minimal Generating Set).

Let $\{p_j\}_{j=1}^n \subset N \subset Z$ be different prime numbers. Then let

$$G_k := \left\{ b_t := \prod_{\substack{s=1 \\ s \neq t}}^k p_s \mid 1 \leq t \leq k \right\} \tag{4.6}$$

Then $G_k \subset Z$ is a minimal generating set, $|G_k| = k$.

Proof. The statement follows from theorem 3.1. $HCF(G_k) = 1$ since $\forall 1 \leq t \leq k, p_t \nmid b_t$ which means no p_t is not a common factor of G_k while each of the elements of G_k are products of the primes $\{p_j\}_{j=1}^k$. Hence G_k is a generating set of Z . For each

$$H_t := G_k \setminus \{b_t\} \implies HCF(H_t) = p_t > 1.$$

Therefore by theorem 3.1, G_k is a minimal generating set of k elements in Z .

Corollary.

There exists a minimal generating set $G_n \subset Z$ such that $|G_n| = n, \forall n \in N$ in the additive group $\{Z, +, -, 0\}$. The generating set G_n is then a maximal independent set. Hence there exists a maximal independent set of n elements $\forall n \in N$ in the additive group Z .

The additive Semigroup \hat{Z} .

Note that in \hat{Z} there are the same elements as in Z hence if $1 \in Z \implies -1 \in Z \implies 1$ and $-1 \in \hat{Z}$.

However, $\langle 1 \rangle_{\mathbb{Z}} = \langle -1 \rangle_{\mathbb{Z}} = \mathbb{Z}$ while $\langle 1 \rangle_{\mathbb{Z}} = \mathbb{N} \subset \hat{\mathbb{Z}}$ and $\langle -1 \rangle_{\mathbb{Z}} = -\mathbb{N} \subset \hat{\mathbb{Z}}$. Even though all elements are available in both structure, in a group we can convert an element to its additive inverse while in a semigroup we cannot. We will convert minimal generating sets of the additive group to minimal generating sets of the semigroup.

Remark.

There is no singleton generating set $\hat{\mathbb{Z}} \supset G = \{e\}$ in $\hat{\mathbb{Z}}$. If $e = 0$ then $\langle 0 \rangle = \{0\} \neq \hat{\mathbb{Z}}$. If $e > 0 \implies \langle e \rangle \subset \mathbb{N} \neq \hat{\mathbb{Z}}$ and similarly if $e < 0 \implies \langle e \rangle \subset -\mathbb{N} \neq \hat{\mathbb{Z}}$. Therefore the additive semigroup $\hat{\mathbb{Z}}$ can be generated by an at least two elements generating set only. It is easy to see that $G = \{-1, 1\}$ is a minimal generating set of $\hat{\mathbb{Z}}$.

Lemma.

Let $\{\hat{\mathbb{Z}}, +, 0, 1\}$ be the additive semigroup of integers and let $n \in \mathbb{Z}$ and $m \in \mathbb{N}$. Then

$$n \times m := \frac{n+n+\dots+n}{m} \tag{4.7}$$

hence or otherwise, $n \times m$ can be computed as the equation shows in the semigroup $\{\hat{\mathbb{Z}}, +, 0, 1\}$ for any integer and any natural number.

Hence the number theoretic statements about HCF remain valid here (Euclidean algorithm and expression of HCF by Euclid) with the statement of lemma as stated (see Theorem 3.2).

Remark

Note that all these operations can be performed in the additive semigroup.

Theorem .

A finite set $G \subset \hat{\mathbb{Z}}$ is a generating set of $\hat{\mathbb{Z}}$ iff $\text{HCF}(G) = 1$. It is minimal iff $\text{HCF}(H) > 1, \forall H \subset G, H \neq G$.

The proof is word for word the same as the proof of theorem 3.1 and left to the reader.

Conversion of group generating sets to Semigroup generating sets.

We have to summarize some preliminaries to formulate the main theorem and prove it.

Operations on the natural numbers: The set of natural numbers \mathbb{N} was defined by Dedekind and Peano. Four axioms define the set \mathbb{N} of natural numbers as follows:

- (1) Zero (0) is a natural number, $0 \in \mathbb{N}$;
- (2) $\forall n \in \mathbb{N} \exists! n' \in \mathbb{N}$ called a unique successor ;
- (3) If $n \in \mathbb{N} \setminus \{0\} \exists! \text{pr}(n) \in \mathbb{N}$ called a unique predecessor $n = \text{pr}(n)'$;
- (4) The mathematical induction principle holds on the set of natural numbers: If $S \subset \mathbb{N}$ is a subset of the natural numbers such that $0 \in S$ and $\forall n \in S \implies n' \in S$ then $S = \mathbb{N}$.

Addition: $+(n, m), \forall n, m \in \mathbb{N}$ is defined as follows:

- A1. $+(n, 0) = n, \forall n \in \mathbb{N}$;
- A2. $+(n, m') = (+ (n, m))', \forall n, m \in \mathbb{N}$;

Theorem.

The addition fulfills:

- AA: $\forall a, b, c \in \mathbb{N}, +(+ (a, b), c) = +(a, +(b, c))$ (associative);
- AC: $\forall a, b \in \mathbb{N}, +(a, b) = +(b, a)$ (commutative);
- AN: $\forall a \in \mathbb{N}, +(a, 0) = +(0, a) = a$ (neutral element);

Multiplication: $*(n, m), \forall n, m \in \mathbb{N}$ is defined as follows:

- M1. $*(n, 0) = 0, \forall n \in \mathbb{N}$;
- M2. $(n, m') = +(* (n, m), n), \forall n, m \in \mathbb{N}$;

Note that M1 and M2 are used in equation (2) of lemma 4.16.10.

Theorem.

The multiplication fulfills:

- MA: $\forall a, b, c \in \mathbb{N}, *(*(a, b), c) = *(a, *(b, c))$ (associative);
- MC: $\forall a, b \in \mathbb{N}, *(a, b) = *(b, a)$ (commutative);
- MN: $\forall a \in \mathbb{N}, *(a, 0) = *(0, a) = 0$ and $*(a, 1) = *(1, a) = a$ (neutral element);
- MD: $\forall a, b, c \in \mathbb{N}, *(a, +(b, c)) = +(* (a, b), *(a, c))$ =(distributive);
- MI: $(-1) \times n = -n, \forall n \in \mathbb{N}$.

The proof is left to the reader.

The sign of an integer:

Any non-zero integer $n \in \mathbb{Z}$ is either $n \in \mathbb{N}$ or $n \in -\mathbb{N}$. Let $\text{sgn}(n) := 1$ if $n \in \mathbb{N}$ and let $\text{sgn}(n) := -1$ if $n \in -\mathbb{N}$. Let $n \in \mathbb{Z}$ be any number. Let $|n| = n$ if $n \in \mathbb{N}$ and let $|n| = -n$ if $n \in -\mathbb{N} \setminus \{0\}$ hence $|n| \in \mathbb{N}$, $\forall n \in \mathbb{Z}$. Then $n = \text{sgn}(n) * |n|$, $\forall n \in \mathbb{Z}$.

4.17. Theorem (An Important Result).

Let $G_k = \{e_t\}_{t=1}^k \subset \mathbb{N} \setminus \{0\}$, $1 < k \in \mathbb{N}$ be a minimal generating set in the additive group \mathbb{Z} . Then $\exists \{x_j\} \subset \mathbb{Z} \setminus \{0\}$ such that

$$1 = \sum_{t=1}^k x_t * e_t$$

Moreover, $\forall H \subset G$, $H \neq G$, $\text{HCF}(H) \neq 1$. Then let $b_t \in \hat{\mathbb{Z}}$ be selected by $b_t = \text{sgn}(x_t) * e_t$, $\forall 1 \leq t \leq k$. Then $G_{k,\hat{\mathbb{Z}}} := \{b_t\}_{t=1}^k$ is a minimal generating set in $\hat{\mathbb{Z}}$.

Proof of theorem 4.17.

Step 1. Let us select $1 \leq t \leq k$ and calculate $x_t \times e_t$ in terms of $\hat{\mathbb{Z}}$:

$x_t \times e_t = \text{sgn}(x_t) \times |x_t| \times e_t = \text{sgn}(x_t) \times e_t \times |x_t| = b_t \times |x_t|$ where the commutativity of multiplication and the definitions of $b_t \in G_{k,\hat{\mathbb{Z}}}$ and $|x_t| \in \mathbb{N} \subset \hat{\mathbb{Z}}$ were used.

Step 2. By formula

$$1 = \sum_{t=1}^k x_t * e_t$$

in the theorem and Step 1. We get that

$$1 = \sum_{t=1}^k x_t * e_t = \sum_{t=1}^k b_t * |x_t| \in \langle G_{k,\hat{\mathbb{Z}}} \rangle \Rightarrow \langle 1 \rangle = \mathbb{N} \subset \langle G_{k,\hat{\mathbb{Z}}} \rangle \text{ holds.}$$

Step 3. Since $k > 1$ and $(e_t \geq 1, x_t \neq 0) \forall 1 \leq t \leq k$ hold in the formula $1 = \sum_{t=1}^k x_t * e_t$ cited in step 2. Therefore at least one $x_{t^*} < 0$, $1 \leq t^* \leq k$ must hold. Then the corresponding $b_t = \text{sgn}(x_{t^*}) * e_{t^*} = (-1) * e_{t^*} < 0$. If $e_{t^*} = 1 \Rightarrow b_{t^*} = -1 \Rightarrow -1 \in \langle G_{k,\hat{\mathbb{Z}}} \rangle$. If $e_{t^*} > 1$ then $1 \leq e_{t^*} - 1 \in \mathbb{N} \subset \langle G_{k,\hat{\mathbb{Z}}} \rangle$ holds and $-1 = b_{t^*} - (e_{t^*} - 1) \in \langle G_{k,\hat{\mathbb{Z}}} \rangle$.

Step 4. In Step 2, We proved that $\langle 1 \rangle = \mathbb{N} \setminus \{0\} \subset \langle G_{k,\hat{\mathbb{Z}}} \rangle$. In Step 3, we proved that $-1 \in \langle G_{k,\hat{\mathbb{Z}}} \rangle$ from which follows that $\langle -1 \rangle = -(\mathbb{N} \setminus \{0\}) \subset \langle G_{k,\hat{\mathbb{Z}}} \rangle$ holds. Moreover, $1, -1 \in \langle G_{k,\hat{\mathbb{Z}}} \rangle \Rightarrow 1 + (-1) = 0 \in \langle G_{k,\hat{\mathbb{Z}}} \rangle$ hence $\langle G_{k,\hat{\mathbb{Z}}} \rangle = \hat{\mathbb{Z}}$. The rest of the proof is left to the reader, it is the same as in the case of the additive group.

Corollary (On Minimal Generating Set of the Additive Group).

Let $\{p_j\}_{j=1}^k \subset \mathbb{N} \subset \mathbb{Z}$, $1 < k \in \mathbb{N}$ be different prime numbers. Then let

$$G_k = \left\{ e_t := \prod_{\substack{s=1 \\ s \neq t}}^k p_s \mid 1 \leq t \leq k \right\}$$

Then $G_k \subset \mathbb{Z}$ is a minimal generating set, $|G_k| = k$. Let $\{x_s\}_{s=1}^k \subset \mathbb{Z}$ fulfill the relation

$$1 = \sum_{t=1}^k x_t * e_t$$

Then the system of elements

$$G_{k,\hat{\mathbb{Z}}} := \{b_t := \text{sgn}(x_t) * e_t \mid 1 \leq t \leq k\}$$

is a minimal generating set of the additive semigroup $\hat{\mathbb{Z}}$.

Proof. The statement follows from theorem 4.17. In theorem 4.13 we proved the statements for the additive group. In the proof of theorem 4.17 the construction of the minimal generating set for the additive semigroup was discussed in details.

Corollary (On Cardinality of Maximal Independent Set of the Additive Semigroup).

There exists a minimal generating set $G_{n,\mathbb{Z}} \subset \hat{\mathbb{Z}}$ such that

$$|G_{n,\mathbb{Z}}| = n, \quad \forall n \in \mathbb{N}$$

in the additive semigroup $\{\mathbb{Z}, +, 0\}$. The generating set $G_{n,\mathbb{Z}}$ is then a maximal independent set. Hence there exists a maximal independent set of n elements $\forall 1 < n \in \mathbb{N}$ in the additive semigroup $G_{k,\mathbb{Z}}$.

Remark

We have given some examples of free semigroup with infinite rank in sections 2.6.3 – 2.6.9 of (Lipcsey and Sampson, 2019a, 2019b). We conclude this with a more general example that generalises that result

Example of a Commutative Semigroup with Infinite Rank

There exist a commutative semigroup S such that $rank(S) = \infty$.

Let $a \in S$, where $\{S, * \}$ is any semigroup. Let $|\langle a \rangle| = \infty$. Then $\langle a \rangle = \{a^j\}_{j=1}^{\infty}$.

Consider $\{a^{p_i}\}_{i=1}^{\infty} \subset \langle a \rangle$, where p_i is a prime for all $1 \leq i \leq \infty$. Select a proper subset

$$H := \{a^{p_{ij}}\}_{j=1}^{\infty} \subset \{a^{p_i}\}_{i=1}^{\infty}$$

Let $S := \langle H \rangle$. S is a commutative semigroup

(1). $H \subset S$ is a minimal generating set of S :

$a^{p_{ij}} \notin \langle H \setminus \{a^{p_{ij}}\} \rangle$. Hence $H \setminus \{a^{p_{ij}}\}$ is not a generating set of S . Hence H is minimal

(2). S cannot be finitely generated:

Assume $\langle G \rangle \supset S$. $G \subset S$, $|G| < \infty$ and G is a generating set.

Then $\exists P \subset H$ where P is finite, such that $G \subset \langle P \rangle$.

Then $S := \langle G \rangle \subseteq \langle P \rangle \subset S \implies S = \langle P \rangle$ which contradicts $P \subset H$, $P \neq H$ by (1) above since $P \supset H$:

$\exists r \in H$ s.t. $P \subset H \setminus \{r\} \implies S = \langle P \rangle \subset H \setminus \{r\} \neq S$.

Thus there is no finite generating subset of S . There is a commutative semigroup where the smallest generating set is infinite. Hence the rank is infinite.

Remark

There is a commutative semigroup where the smallest generating set is infinite. Hence the rank is infinite.

References

- [1] Bukh, Boris. Math Studies Algebra: Axiom OfChoice* (2019), Pages 21 – 237. [Http://Www.Borishbukh.Org/Mathstudiesalgebra1718/Notes_Ac.Pdf](http://www.borishbukh.org/mathstudiesalgebra1718/Notes_Ac.Pdf).
- [2] Gould, V. Semigroup Theory, A Lecture Course (Monograph) (2010), Retrieved From [Www-Users.York.Ac.Uk/~Varg1/Semigrouptheory.Pdf](http://www-users.york.ac.uk/~varg1/Semigrouptheory.Pdf).
- [3] Halbeisen, L., Hamilton, M. & Růžička, P. Minimal Generating Sets Of Groups, Rings, And Fields. *Quaestiones Mathematicae*(2007), Volume 30 - Issue 3.
- [4] Howie, J. M. Introduction ToSemigroup Theory. Academic Press, Elsevier, Cambridge, Massachusetts, United States(1976).
- [5] Lipcsey, Z. &Sampson, M. I. (2019a). Rank Of Semigroup: Generating Sets AndIndependent Sets. Proceedings Of The 236thTheierInternational Conference, 20th – 21stMay, 2019, San Diego, California, USA.
- [6] Lipcsey, Z. &Sampson, M. I. (2019b). Rank Of Semigroup: Generating Sets AndIndependent Sets. Proceedings Of The 3rd International Conference OfMathematics, An Istanbul Meeting Of World Mathematics, Fatih Sultan Memet Foundation University Of Mathematics. Istanbul, Turkey.
- [7] Lipcsey, Z. &Sampson, M. I. (2022). Independence And Minimal Generating Set InSemigroups And Countable Systems Of Semigroups. *International OrganisationOfScientific Research Journal Of Mathematics(IOSR-JM)*. www.iosrjournals.org. Accepted For Publication.
- [8] Nadia B. &Halbeisen, L. (2003). The Cardinality Of Smallest Spanning Sets Of Rings, *Quaestiones Mathematicae*, Vol. 26(3), 321–325.
- [9] Paul, J. Campbell (1978). The Origin Of “Zorn’s Lemma”. *Historica Mathematica* 5, Pages 77 – 89.
- [10] Sampson, M. I. , Nduka W. , Jackson A. On divisibility of Sum of Coprimes of Integers by Integers and Primes, *IOSR Journal of Mathematics (IOSR-JM)*, Volume 17, Issue 1 Ser. III, Pages 54 – 67. Jan.– Feb. 2021. www.iosrjournals.org