Transactions of the Nigerian Association of Mathematical Physics
***Volume 14, (January - March, 2021 Issue*), pp21 – 26**

ON THE GROUP-THEORETIC PROPERTIES OF POWER SET OF FINITE SET UNDER THE OPERATION OF SYMMETRIC DIFFERENCE

Amina M. L. and Abdul Iguda

**Department of Mathematical Sciences, Faculty of Physical Sciences,
Bayero University, Kano, Nigeria.**

Abstract

This study is aimed at finding more results on the algebraic properties of the group of power set $\mathcal{P}(X)$ of finite set $X = \{1, . . . , n\}$, $n \in \mathbb{N}$ under the operation of symmetric difference Δ. We consider the case when $|X| = 1$, $|X| = 2$, $|X| = 3$, $|X| = 4$ one by one as illustrative examples and then generalizes for any finite positive integer n. We determined the order of each non-identity element in $(\mathcal{P}(X), \Delta)$ and found that each is having order two. We checked whether the non-empty subsets of $\mathcal{P}(X)$ form subgroups and then determined the number of such subgroups in each case, and obtained some general results on that. We have shown that there exists bijection between $\mathcal{P}(X)$ and the collection of 2-subgroups of order two together with the trivial subgroup. Since $(\mathcal{P}(X), \Delta)$ is an abelian group, we try to determine whether it is cyclic for any finite set X, we found that $\mathcal{P}(X)$ is non-cyclic when $|X| \geq 2$. Moreover other properties for finite abelian groups such as existence of nontrivial factor group, isomorphism, solubility and nilpotency were determined and provide results on that. Finally we constructed the associated identity graphs of $(\mathcal{P}(X), \Delta)$ when $X = \{1, 2\}$, $X= \{1, 2, 3\}$ and $X = \{1, 2, 3, 4\}$. From the graphs obtained we came up with general property for some types of finite abelian groups.

***Keywords*:** Power set, symmetric difference operation, group-theoretic properties.

1. Introduction

Let $X = \{1, . . ., n\}$ be a finite set. The power set of X is the set of all subsets of X including the empty set and X itself, denoted by $\mathcal{P}(X)$ and has 2^n elements where $|X| = n$. The power set of X known to be an abelian group under the operation of symmetric difference Δ (where empty set $\emptyset$ is the identity element and each subset (element) being its own inverse). Bean [1] proved that Δ can be characterized as the unique group operation $*$ on $\mathcal{P}(X)$ such that $A * B \subseteq A \cup B$; for all $A, B \in \mathcal{P}(X)$. He defined the co-symmetric difference operation ∇ on $\mathcal{P}(X)$ by $A \nabla B = X - (A \Delta B)$ for all $A, B \in \mathcal{P}(X)$. And claimed that $(\mathcal{P}(X), \nabla)$ is also an abelian group. Moreover, he proved that ∇ can be characterized as the unique group operation * on $\mathcal{P}(X)$ such that $A \cap B \subseteq A * B$ for all $A, B \in \mathcal{P}(X)$. Bean [1] additionally proved that $(\mathcal{P}(X), \Delta, \cap)$ and $(\mathcal{P}(X), \nabla, \cup)$ are isomorphic commutative rings with unity. To the best of our knowledge there is no research done on the group theoretic of $(\mathcal{P}(X), \Delta)$. This creates a gap to enable us study more group theoretic properties of this structure, since for any finite set X; $(\mathcal{P}(X), \Delta)$ is a p-group and hence they are easier to understand and classify than arbitrary groups.

The aim of this paper is to study some important properties such as order of elements, subgroups, other abelian groups' properties and graph representation. We would first consider the case when $|X| = 1$, $|X| = 2$, $|X| = 3$, $|X| = 4$ as illustrative examples and then generalized for any finite set X.

2. Preliminaries

In this section we give definitions of some basic terms and relevant theorems needed for the understanding of this paper.

Definition 2.1 [2]**:** Let G be a group and $x \in G$. The order of x is the smallest positive integer m such that $x^m = e$ (where e is the identity in G) and in such case x is said to be of order m. This is denoted by $|x|$.

Correspondence Author: Amina M.L., Email: amlawan.mth@buk.edu.ng, Tel: +2348065025723

Definition 2.2 ([3]**, Definition 8.22):** Let G be a finite group. Then G is said to be torsion group if every non-identity element of G has finite order.
Definition 2.3 [2]**:** A group G is said to be cyclic if there is some g ∈ G such that every element of G can be expressed in the form of g^m for $m \in \mathbb{Z}$ and g is called the generator of G.
Theorem 2.1([4]**, Result 6.4.2):** Let G be a finite group of order *n*. Then G is cyclic if and only if G contains an element of order *n*. And such element is called the generator of G.
Theorem 2.2 ([4], **Theorem 7.2.3):** If G is a finite group and H is a subgroup of G, then the order of H divides the order of G.
Definition 2.4 ([3]**, Definition 7.7):** Let M be a proper normal Subgroup of a group G. Then M is said to be maximal if it is not contained in any other proper normal subgroup of G.
Definition 2.5 ([3]**, Definition 5.8):** Let G be a finite group and let *p* be a prime number. G is said to be a *p*-group if $|G| = p^{\alpha}, \alpha \in Z^+$. A subgroup H of G is called *p*-subgroup if $|H| = p^k$, for some $k \in Z^+$.
Definition 2.6 ([3]**, Definition 7.4):** Let G be a group. A series $G = G_0 \supseteq G_1 \supseteq ... \supseteq G_n = \{e\}$ is said to be normal if each G_i is normal in G.
Definition 2.7 ([3], **Definition 7.5):** A group G is said to be solvable if and only if there exists a normal series for G, whose factor groups are abelian.
Proposition 2.3 ([2], **Proposition 7):** A finite group is nilpotent if and only if every maximal subgroup is normal.
Definition 2.8 [5]**:** An identity graph is a rooted tree consisting of lines or triangles or both where the centre (root) of the graph is representing the identity element of a group and is connected to every other vertex by an edge. Two distinct vertices are joined by an edge if they correspond to mutual inverse elements in the group.

3. Group-theoretic properties of ($\mathcal{P}$(X), Δ)
In this section we investigate some group-theoretic properties of the power set $\mathcal{P}$(X) of finite set X = {1, . . . , *n*} with respect to the symmetric difference operation.

3.1 Order of an element in ($\mathcal{P}$(X), Δ)
In every group, an identity element has order one, let's see for other elements in $\mathcal{P}$(X)**.** By definition of Δ; for any A ∈ $\mathcal{P}$(X), A Δ A = ∅ that is, A^2 = ∅ which is the identity element in $\mathcal{P}$(X). This implies that each non-identity element in $\mathcal{P}$(X) has order two. Hence we have the following results.
Theorem 1: Every non-identity element in ($\mathcal{P}$(X), Δ) has order two.
Proof
Follows from the definition of Δ; since for any non- identity element A ∈ $\mathcal{P}$(X), A Δ A = ∅; that is, A^2 = ∅ which is the identity element in $\mathcal{P}$(X).
Corollary 2: ($\mathcal{P}$(X), Δ) is a torsion group.
Proof
This follows from **Definition 2.2**
Theorem 3: ($\mathcal{P}$(X), Δ) is an elementary abelian group.
Proof
($\mathcal{P}$(X), Δ) is clearly elementary because each non- identity element is of prime order.
Corollary 4: ($\mathcal{P}$(X), Δ) is a 2-group.
Proof
The proof follows from **Definition 2.5**.

3.2 Subgroups of ($\mathcal{P}$(X), Δ)
In this subsection, we try to check whether the non-empty subsets of $\mathcal{P}$(X) form subgroups, and if so we determine number of such subgroups; by considering the case when |X| =1, |X| = 2, |X| = 3, |X| = 4 and then generalize.
Case 1: X={1}, $\mathcal{P}$(X) = {∅, {1}}. Here the possible subgroups of ($\mathcal{P}$(X), Δ) are {∅} and $\mathcal{P}$(X). That is the trivial subgroups.
Case 2: X = {1, 2}, $\mathcal{P}$(X) = {∅, {1}, {2}, {1, 2}}. By definition of Δ, each element is self-inverse. Thus for any A ∈ $\mathcal{P}$(X), a subset of $\mathcal{P}$(X) consisting of ∅ and A forms a normal subgroup. In this case, the non-trivial1 proper normal subgroups are; {∅, {1}}, {∅, {2}}, {∅, {1, 2}} each of order two and there are three of them, which is the same as |$\mathcal{P}$(X)| −1 = 2^2 −1.
Case 3: X = {1, 2, 3}, $\mathcal{P}$(X) = {∅, {1}, {2}, {3}, {1, 2}, {1, 3},{2, 3}, {1, 2, 3}}. By **Theorem 2.2**, ($\mathcal{P}$(X), Δ) may have non-trivial proper subgroups of order two or four. Let us try to determine such subgroups, following the definition of symmetric difference on $\mathcal{P}$(X) observe that {∅, {1}}, {∅, {2}}, {∅, {3}}, {∅, {1, 2}}, {∅, {1, 3}}, {∅, {2, 3}}, {∅, {1, 2,

3}} are proper normal subgroups each of order two and there are seven of them. Similarly, {∅, {1},{2},{1, 2}}, {{∅}, {1},{3},{1, 3}}, {∅, {2},{3},{2, 3}} are three proper normal subgroups each of order four.
From these we can see that, the number of 2-subgroups of order two is the same as $|\mathcal{P}(X)|-1= 2^3-1$ and the number of 2-subgroups of order four can be obtained by combination of any two elements of X. That is $^3C_2 = \frac{3!}{1!2!} = 3$.

Case 4: X= {1, 2, 3, 4}, $\mathcal{P}$(X) = {∅, {1}, {2}, {3}, {4}, {1, 2}, {1, 3}, {1, 4}, {2, 3}, {2,4}, {3, 4}, {1, 2, 3}, {1, 2, 4}, {1, 3, 4}, , {2, 3, 4}, {1, 2, 3, 4}}.
By **Theorem 2.2**, ($\mathcal{P}$(X), Δ) may have non-trivial proper 2-subgroups of order two or four or eight. Let us try to determine such subgroups, following the definition of symmetric difference on $\mathcal{P}$(X) observe that, the non-trivial proper 2-subgroups each of order two are;
{∅, {1}}, {∅, {2}}, {∅, {3}}, {∅, {4}}, {∅, {1, 2}}, {∅, {1, 3}}, {∅, {1, 4}}, {∅, {2, 3}}, {∅, {2, 4}}, {∅, {3, 4}}, {∅, {1, 2, 3}}, {∅, {1, 2, 4}}, {∅, {1, 3, 4}}, {∅, {2, 3, 4}},
{∅ ,{1, 2, 3, 4} }.There are fifteen of them which is the same as $|\mathcal{P}(X)| -1 = 2^4 -1$.
2-Subgroups of order four are; {∅, {1}, {2}, {1, 2}}, {∅, {1}, {3}, {1, 3}}, {∅, {1}, {4}, {1, 4}}, {∅, {2}, {3}, {2, 3}}, {∅, {2}, {4}, {2, 4}}, {∅, {3}, {4}, {3, 4}}. There are six of them. From this we can see that the number of these 2-subgroups of order four can be obtained by combination of any two elements of X. This is the same as $^4C_2 = \frac{4!}{2!2!} = 6$.
2-Subgroups of order eight are; {∅, {1}, {2}, {3}, {1, 2}, {1, 3}, {2, 3}, {1, 2, 3}}; {∅, {1}, {2}, {4}, {1, 2}, {1, 4}, {2, 4}, {1, 2, 4}}; {∅, {1}, {3}, {4}, {1, 3}, {1, 4}, {3, 4}, {1, 3, 4}}; {∅, {2}, {3}, {4}, {2, 3}, {2, 4}, {3, 4}, {2, 3, 4}}. We have four of them, formed as a result of combining any three elements of X. Note that the number can be obtained from $^4C_3 = \frac{4!}{1!3!} = 4$. Based on the observations made on the four cases above, we have the following result.
Theorem 5: Let X={1, 2, . . ., n}. Then (i) a distinct 2-subgroup of $\mathcal{P}$(X) of order two is in the form {∅, A} such that A ∈ $\mathcal{P}$(X) and A ≠ ∅. (ii) the group ($\mathcal{P}$(X), Δ) has $2^n -1$ distinct normal 2-subgroups each of order two. (iii) the group ($\mathcal{P}$(X), Δ) has ^nC_r distinct proper normal subgroups each of order 2^r for $2 \le r \le n$. (iv) every subset of order 2^{r-1} is a maximal Subgroup of ($\mathcal{P}$(X), Δ) for $2 \le r \le n$.
Proof
The proof of (i), (ii), (iii) follows from the discussion made in this subsection and (iv) by **Definition 2.4.**

3.3 Bijection

From **Theorem 5**(ii), for any n∈ℕ, the number of 2-subgoups of order two is $2^n - 1$. Hence we can define a mapping between $\mathcal{P}$(X) and the set consisting of all 2-subgroups of order two including the trivial subgroup. Let us consider the example below:
Example 1: For X={1, 2, 3}, $\mathcal{P}$(X) = {∅, {1}, {2}, {3}, {1, 2}, {1, 3}, {2,3}, {1, 2, 3}} and let S be the set consisting of all 2-subgroups of order two including the trivial subgroup. That is, S= {{∅}, {∅, {1}}, {∅, {2}}, {∅, {3}}, {∅, {1, 2}}, {∅, {1, 3}}, {∅, {2, 3}}, {∅, {1, 2, 3}}. Let π: $\mathcal{P}$(X)⟶ S be a mapping defined by ∅ ↔ {∅}, {1}↔{∅, {1}}, {2}↔{∅, {2}}, {3}↔{∅, {3}}, {1, 2}↔{∅, {1, 2}}, {1, 3}↔{∅, {1, 3}}, {2, 3}↔{∅, {2, 3}}, {1, 2, 3} ↔{∅, {1, 2, 3}}. Clearly this is a bijective map. We now have the following result.
Theorem 6: Let X = {1, . . ., n} and S be the set consisting of all 2-subgroups of order two including the trivial subgroup. Then there exists a bijection π : $\mathcal{P}$(X)→S defined by π(∅) = {∅} and π(A) = {∅ , A} for all A ∈ $\mathcal{P}$(X) such that A ≠ ∅.
Proof
Since $|\mathcal{P}(X)| = |S|$, clearly the definition of the map π: $\mathcal{P}$(X)→S is bijective.
Note: Observe that in **Example 1**, S is not closed under the operation of symmetric difference. For example, {∅}Δ{∅, {1}} = {{1}} which is not an element of S,
3.4 Is ($\mathcal{P}$(X), Δ) cyclic?
($\mathcal{P}$(X), Δ) is an abelian group for any finite set X, here we want to check whether or not it can be cyclic. According to **Theorem 2.1**, When |X| =1, ($\mathcal{P}$(X), Δ) is clearly cyclic, generated by X while ($\mathcal{P}$(X), Δ) is not cyclic when $|X| \ge 2$, since by **Theorem 1**, none of the elements in $\mathcal{P}$(X) is having the same order with $\mathcal{P}$(X). Thus we have this result.
Theorem 7: ($\mathcal{P}$(X), Δ) is non-cyclic group for $|X| \ge 2$.

Proof
This is obvious from **Theorem 1.**

3.5 Other properties of finite abelian groups
In this subsection, we determined some of the general properties of finite abelian groups.
3.5.1Factor Group of ($\mathcal{P}$(X), Δ)
Since all the subgroups N of $\mathcal{P}$(X) are normal, this implies that the quotient set $\mathcal{P}$(X)/N = {AΔN: A ∈ $\mathcal{P}$(X)} forms a factor group with respect to the operation of symmetric difference.
Let us illustrate this using $\mathcal{P}$(X) = {∅, {1}, {2}, {1, 2, 3}} and N = {∅, {1}}. Then $\mathcal{P}$(X)/N = {{∅, {1}}, {{2},{1, 2}}}.
To show that $\mathcal{P}$(X)/N is indeed a group, let us construct Cayley table for ($\mathcal{P}$(X)/N, Δ) as follows (Table 1):

Table 1: Cayley table for

Δ	{∅, {1}}	{{2}, {1, 2}}
{∅, {1}}	{∅, {1}}	{{2}, {1, 2}}
{{2}, {1, 2}}	{{2}, {1, 2}}	{∅, {1}}

Clearly from table 1and property of symmetric difference we have:
(i) Δ is associative on $\mathcal{P}$(X)/N.
(ii) {∅, {1}} is the identity element.
(iii) Each element in $\mathcal{P}$(X)/N is self-inverse.
This showed that $\mathcal{P}$(X)/N is a factor group of $\mathcal{P}$(X).
Theorem 8: Let N be any subgroup of ($\mathcal{P}$(X), Δ). Then the set $\mathcal{P}$(X)/N is a factor group.
Proof
Let N be any subgroup of ($\mathcal{P}$(X), Δ). To prove that $\mathcal{P}$(X)/N = {AΔN: A ∈ $\mathcal{P}$(X) is a group, we are to show that the group axioms are satisfied.
Axiom 1: Closure and associativity
By closure and associative property of Δ, for any A, B, C ∈ $\mathcal{P}$(X),
$(A\Delta N)\Delta(B\Delta N) = (A\Delta B)\Delta N \in \mathcal{P}(X)/N$.
Also $(A\Delta N)\Delta[(B\Delta N)\Delta(C\Delta N)] = (A\Delta N)\Delta[(B\Delta C)\Delta N)]$
$= (A\Delta B\Delta C)\ \Delta N$.
Similarly, $[(A\Delta N)\Delta(B\Delta N)]\Delta(C\Delta N)] = [(A\Delta B)\Delta N]\Delta(C\Delta N)$
$= (A\Delta B\Delta C)\ \Delta N$.
Axiom 2: Existence of an identity element.
Since ∅ is the identity element in $\mathcal{P}$(X) and for any subgroup N of $\mathcal{P}$(X); ∅ΔN = N. Hence N is the identity element in $\mathcal{P}$(X)/N.
Axiom 3: Existence of inverse for each element in $\mathcal{P}$(X)/N.
Since for any $A \in \mathcal{P}(X), A \triangle A = \emptyset$. Hence the inverse of each AΔN∈$\mathcal{P}$(X)/N is AΔN because (AΔN)Δ(AΔN) = (AΔA) ΔN =∅ΔN = N which is the identity in $\mathcal{P}$(X)/N. All the group axioms are satisfied and thus the result follows.

3.5.2 Isomorphism
Observe that, the subgroups of order two are sylow 2-subgroups and hence each is isomorphic to the cyclic group $\mathbb{Z}_2$. By primary decomposition theorem, for any finite set X of order *n*, the group ($\mathcal{P}$(X), Δ), is isomorphic to the direct product $Z_2 \times Z_2 \times ... \times Z_2$ (*n* factors) which is non-cyclic. Thus, we give an illustrative example as follows:
Example 2: Let X={1, 2, 3} and consider the group ($\mathcal{P}$(X), Δ) where $\mathcal{P}$(X) ={∅, {1}, {2}, {3}, {1, 2}, {1, 3}, {2,3}, X} and $Z_2 \times Z_2 \times Z_2$. Define one-to-one correspondence between $\mathcal{P}$(X) and $Z_2 \times Z_2 \times Z_2$ as follows: ∅↔(0, 0, 0), {1}↔(0, 0, 1), {2}↔(0, 1, 0), {3}↔(0, 1, 1), {1, 2}↔(1, 0, 0), {1, 3}↔ (1, 0, 1), {2, 3}↔ (1, 1, 0), X↔ (1, 1, 1).This proved that ($\mathcal{P}$(X), Δ) is indeed non-cyclic since it is isomorphic to the non-cyclic group $Z_2 \times Z_2 \times Z_2$.

3.5.3 Solvability and Nilpotency
Theorem 9: The group ($\mathcal{P}$(X), Δ) is solvable.
Proof
This follows from **Definition 2.7** since all subgroups of $\mathcal{P}$(X) are normal and they form a series whose factor groups are abelian, hence $\mathcal{P}$(X) is solvable for any finite set X.
Theorem10: The group ($\mathcal{P}$(X), Δ) is nilpotent.
Proof
The proof follows from **Proposition 2.3** and **Theorem 5**(iv)

3.6 Identity Graphs of ($\mathcal{P}$(X), Δ)

Here we constructed the associated identity graphs of ($\mathcal{P}$(X), Δ), when X = {1, 2}; X= {1, 2, 3} and X = {1, 2, 3, 4}. From the graphs we came up with general property for some types of finite abelian groups. We present the graphs (Figure 1, 2, 3) below:

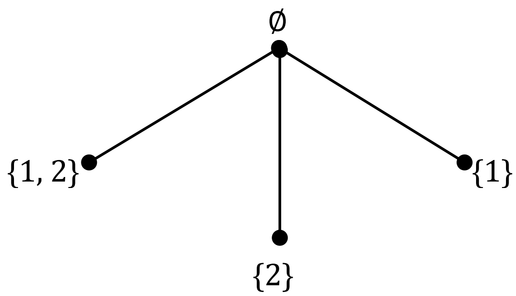

Figure 1: The identity graph of ($\mathcal{P}$(X), Δ) when X = {1, 2}

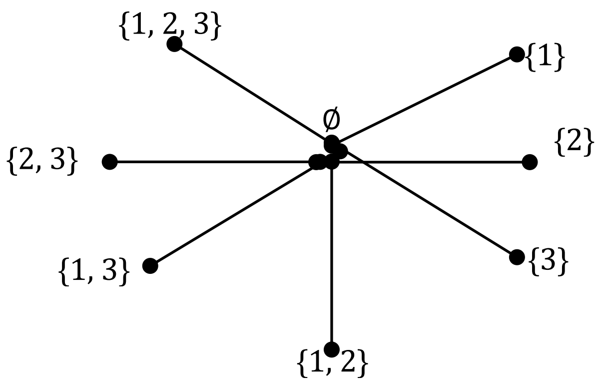

Figure.2: The identity graph of ($\mathcal{P}$(X), Δ) when X = {1, 2, 3}

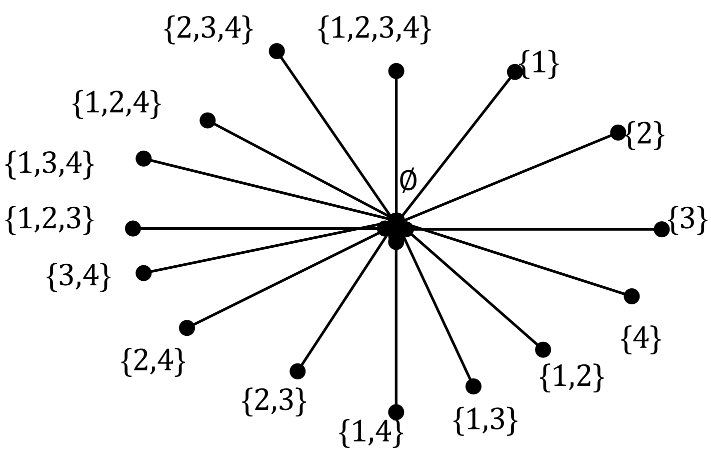

Fig.3: The identity graph of ($\mathcal{P}$(X), Δ) when X = {1, 2, 3, 4}

From the figures above, we can observe that in each case the identity graph consists of lines only and each line (subgraph) is representing the 2- subgroup of order two. We now have the following results.

Theorem 11: The identity graph of ($\mathcal{P}$(X), Δ) is formed only by lines with no triangle(s).

Proof

Since all the elements of $\mathcal{P}$(X) are self-inverse, hence no two distinct vertices will be joined by an edge to obtain a triangle. Therefore the associated identity graphs of ($\mathcal{P}$(X), Δ) cannot consist of triangle(s).except lines only.

Theorem 12: The identity graph of ($\mathcal{P}$(X), Δ) has $2^n - 1$lines only where 2^n is the order of $\mathcal{P}$(X).

Proof

Observe that the vertex corresponding to the identity element in the identity graph associated to $\mathcal{P}$(X) is the centre of the graph. Therefore it is connected by a line to all other vertices corresponding to the non-identity elements in the graph. It follows that there will be

$|\mathcal{P}(X)| - 1 = 2^n - 1$ lines in the graph.

We now give a corollary to **Theorem 12**

Corollary 13: Let p be a prime number. If G is a finite non-cyclic group of order p^k ($k \in \mathbb{N}$) then the identity graph of G consists of $p^k - 1$ lines only. That is its associated identity graph is a triangle free graph.

4. Conclusion

In this study thirteen more results on the group-theoretic properties of power set of a finite set under the operation of symmetric difference were established.

References

[1] Bean, C. (1976). Group operations on the power set, J. of undergraduate math. 8(1) 15-17.
[2] Dummit, D.S. and Foote, R. (2004). Abstract algebra, third ed., John Wiley and sons Inc.
[3] Kuku, A.O. (1993). Abstract algebra. Ibadan university press, Nigeria, SBN 978 121 0699.
[4] Whitehead, C. (1993). Guide to Abstract algebra, fourth ed., the Macmillan press ltd. ISBN 0-333-42657-6.
[5] Vasantha, W. B. and Smarandache, F. (2009). Groups as Graphs, e-book.