IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

Topic – "Concept of cyclic group

Amrish Kumar Srivastav
Research Scholar
Department of Mathematics,
B. N. M. University, Madhepura
Bihar, India

ABSTRACT

Group theory in mathematics refers to the study of a set of different elements present in a group. A group is said to be a collection of several elements or objects which are consolidated together for performing some operation on them. The study of a set of elements present in a group is called a group theory in Mathematics. Its concept is the basic to abstract algebra. Algebraic structures like rings, fields, and vector spaces can be recognized as groups with axioms. Evariste Galois (born October 25, 1811, Bourg-la-Reine near Paris, France, died May 31, 1832, Paris), French mathematician is famous for his contributions to the part of higher algebra i.e., now known as group theory. Cyclic group is a part of group in which every element is in form of indices of an element, that element is known as generator of the cyclic group.

KEY WORDS: structures, generator, abstract, axioms

INTRODUCTION

Binary operation, algebraic structure and some properties are main keys for defining group. A mathematical operation between two digits is known as binary operation. The usual binary operation is addition, subtraction, multiplication and division which are familiar with us. But, in mathematics there are defined many types of binary operation according to need. An algebraic structure has a non empty set whose element is connected with defined binary operation. Normally group has four properties which are closure law, associative law, existence of identity element and existence of inverse element. When group has commutative property also, then it is known as abelian group. On the basis of number of elements in a group it is classified in two categories named finite and infinite groups.

Cyclic group is a group which is generated by single element which is known as generator of cyclic group. Graph of cyclic group is known as Caley graph [1]. Every finite group is virtually cyclic [2].

CONCEPT

A group G is called cyclic, if for some a ∈ G every element x ∈ G is of the form an, where n is some integer. The element a is known as generator of the group G.

A finite abelian group is a direct sum of primary cyclic group [3].

Example: The multiplicative group of unity is cyclic.

Example: The multiplicative group of nth root of unity is cyclic.

Some properties of cyclic group:

Theorem: Every cyclic group is an abelian group.

Proof: Suppose G = (a) be a cyclic group which is generated by element a and x and y are two elements of the group G.

Hence there exists integers r and s such that $x= a^r$, $y=a^s$

Now we take, $x\ y = a^r . a^s$

$\Rightarrow x\ y = a^{r+s}$

$\Rightarrow x\ y = a^{s+r}$

$\Rightarrow x\ y = a^s . a^r$

$\Rightarrow x\ y = y . x$

Hence, G holds commutative law.

Therefore G is abelian.

Theorem: If a is generator of a cyclic group G, then a^{-1} will also be generator of the group G.

Proof: Let G = (a) be a cyclic group which is generated by a and ar be the element of G where r is some integer

Then we can write, $a^r = (a^{-1})^{-r}$

Since –r is some integer; therefore each element of G is generated by a^{-1}

Therefore a^{-1} is also generator of the group G.

Theorem: Every group of prime order is cyclic.

Proof: Let G is a finite group and order of G is a prime number p, then we have to prove that G is cyclic group.

We know that an integer p is said to be prime number if,

$$p \neq 0 , p \neq 1$$

Only divisors of p are ±1, ±p

Since G is a group of prime order, therefore G has at least two elements.

We know that 2 is the least positive prime number. Therefore there exists an element $a \in G$ such that,

$a \neq$ the identity element e

Since the element a is not identity element, hence $o(a) \geq 2$

Now suppose that $o(a) = m$

If H is cyclic subgroup of G generated by a,

Then $o(H) = o(a) = m$

With the help of Lagrange's theorem (order of subgroup is divisor of order of group) which implies m must be divisor of p.

Here we see that p is prime and $m \geq 2$

Hence $m = p$

Therefore $H = G$

Since H is cyclic therefore G will be cyclic and the element a will be generator of G.

Theorem: Every subgroup of a cyclic group is cyclic [5].

Proof: Let G= (a) is a cyclic group which is generated by element a. If H = G or {e}, then H will be cyclic group.

Now let H is proper subgroup of G.

Then the element of H be in multiple power of a.

If $a^r \in H$, then inverse of a^r which is a^{-s}, hence, $a^{-s} \in H$

This shows that H has elements which are positive and negative multiple power of a.

Suppose m is the smallest positive integer, such that

$a^m \in H$

Then we have to prove, $H= \{a^m\}$ i.e.,

The subgroup H is cyclic subgroup and is generated by the element a^m,

Now let $a^t \in H$, with help of division algorithm there exist integer q and r, such that, $t = m\,q + r$, where $0 \leq r < m$

Now, $a^m \in H$

$\Rightarrow (a^m)^q \in H$ (by closure property)

$\Rightarrow a^{mq} \in H$

$\Rightarrow (a^{mq})^{-1} \in H$

$\Rightarrow a^{-mq} \in H$

Since $a^t \in H$ and $a^{-m\,q} \in H \Rightarrow a^t \cdot a^{-m\,q} \in H$

$\Rightarrow a^{t-m\,q} \in H$

$\Rightarrow a^r \in H \quad (\because r = t - m\,q)$

Now m is the smallest positive integer, such that

$a^m \in H$ and $0 \leq r < m$

This shows that value of r should be zero.

Hence $t = m\,q$

$\Rightarrow \quad a^t = a^{mq} = (a^m)^q$

Hence each element $a^t \in H$ is denoted by $(a^m)^q$ which shows that H is cyclic generator element am .

Theorem: If G is finite group of order n which has an element of order n, then the group must be cyclic [4].

Proof: Let G be a finite group of order n and suppose $a \in G$ and the number n be the order of a i.e., n is the least positive integer.

Such that $a^n = e$ the identity element of G

Now, we have to prove that G is cyclic.

If H is cyclic subgroup of G generated by a and $H = \{ a^r : r \in I \}$ then the order of H is n, because the order of generator a of H is n. This shows that H is cyclic subgroup of G and the order of H is equal to the order of G.

Hence H =G and therefore G itself is a cyclic group and a is generator of G.

Theorem: If G is an infinite cyclic group generated by a then show that G has exactly two generators a and a^{-1}.

Proof: Suppose G be an infinite cyclic group which is generated by a. Hence elements of a G is multiple power of a.

First, we show that no two different multiple powers of a can be equal.

If this is true, then suppose, $a^r = a^s$ where $r > s$

$\Rightarrow a^r a^{-s} = a^s a^{-s}$

$\Rightarrow a^{r-s} = a^0$

$\Rightarrow a^{r-s} = e$

Since $r - s > 0$ and $a^{r-s} = e$, this implies that order of a is infinite. This shows that a can not be a generator of infinite cyclic group G.

Hence $a^r \neq a^s$, unless we get r = s

So G can be represent as,

$G = \{\ldots. a^{-2}, a^{-1}, a^0 = e, a^1, a^2, a^3, a^4 \ldots. \}$

If ar is any element of the group G, then, $a^r = (a^{-1})^{-r}$

Therefore, the element a^{-1} is generator of the group G.

Hence the element a and a^{-1} is the generator of the group G.

Now, we show that no element of G be the generator of G.

Suppose b be any generator of G.

$\Rightarrow b = a^m$ for some integer m.

Similarly, we get $a = b^n$ for some integer n.

Now, we have, $a = b^n$

$\Rightarrow a = (a^m)^n = a^{mn}$

$\Rightarrow a^{mn-1} = e$

$\Rightarrow$ o (a) is finite and $0 \leq$ □m n-1

This condition satisfies only when,

$mn - 1 = 0$

$\Rightarrow mn = 1$

$\Rightarrow m = 1/n$

$\Rightarrow m = \pm 1$ as m and n are integers and hence b = a or a-1

Thus G has exactly two generators a and a^{-1}.

Theorem: If a cyclic group G has a subgroup H, then the order of G must be a multiple of order of subgroup H.

Proof: Let order of the cyclic group generated by a is n.

Then $G = \{a, a^2, a^3, a^4 \ldots.., a^n = e\}$

Suppose H be proper subgroup of G.

Since the order of the cyclic group is n, therefore the order of a is also n. i.e., $a^n=e$

$\therefore$ $a^n \in H$ since $e \in H$

Every member of H will evidently be some integral powers of a, positive or negative. Suppose m be the smallest of these positive integers, such that $a^m \in H$.

We know that H is a cyclic subgroup of a^m.

Let the order of a^m i.e., generator of H be q.

Then $(a^m)^q = e = a^n$

$\Rightarrow a^{mq} = a^n$

$\Rightarrow m\,q = n$

$\therefore$ H consist of q distinct elements.

Hence subgroup H of a finite cyclic group G of order of n is a finite cyclic group of order $q = n/m$

$\Rightarrow$ $m = n/q$ i.e., order of H divides the order of G.

Theorem: Prove that every proper subgroup of an infinite cyclic group is infinite.

Proof: Let H be a proper subgroup of G and G is an infinite cyclic group. In this condition H will be cyclic because this is theorem that every subgroup of a cyclic group is cyclic.

If m is the smallest positive integer, such that, $a^m \in H$.

Now we suppose H is a finite group of order p. Since the element am is a generator of H, hence we get, $(a^m)^p = e$

$\Rightarrow$ $a^{mp} = e$, where value of $mp > 0$

This shows that order of p is finite and order of G is also finite, which is against of our hypothesis. Hence the subgroup H must be an infinite cyclic subgroup of the group G.

CONCLUSION

Cyclic group is specific type of group which has generator. A finite abelian group is direct sum of primary cyclic group. The multiplicative group of unity and multiplicative group of nth root of unity is cyclic. We get result that every cyclic group is abelian. If an element is generator of cyclic group then its inverse will also be generator of the group. Every group of prime order is cyclic. Each subgroup of cyclic group will be cyclic. If any finite group of order n has an element of order n, then the group must be cyclic. An infinite cyclic group has two generators

which are generator and its inverse. If a cyclic group has subgroup then order of the group must be multiple of order of subgroup and every proper subgroup of an infinite cyclic group is cyclic.

ACKNOWLEDGEMENT

I would like to express my special thanks of gratitude to my guide Dr M. K. Manoranjan as well as my colleague who encourage me for writing paper for publishing. I am really thankful to them. Secondly, I would also like to thank my parents and friends who helped me a lot in finishing paper writing within the short time. Just because of them I am able to write this paper and make it good and enjoyable experience.

References

1- **Alspach, Brian (1997),** *"Isomorphism and Cayley graphs on abelian groups"*, Graph symmetry (Montreal, PQ, 1996), NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci., vol. 497, Dordrecht: Kluwer Acad. Publ., pp. 1–22, ISBN 978-0-792-34668-5

2- **Kurzweil, Hans; Stellmacher, Bernd (2004),** "*The Theory of Finite Groups: An Introduction, University text",* Springer, ISBN 978-0-387-40510-0

3- **Mahmood Behboodi, Esfahan, Reza Beyranvand, Khoramabad, Amir Hashemi, Hossein Khabazian, Esfahan** *"Classification of finite Rings: Theory and Algorithm",* Czechoslovak Mathematical Journal, Vol. 64 (2014), No. 3,

4-**Jungnickel, Dieter (1992),** "*On the uniqueness of the cyclic group of order n"*, American Mathematical Monthly, doi: 10.2307/2324062,, JSTOR 2324062, MR 1166004

5- **Aluffi, Paolo (2009),** *"Subgroups of Cyclic Groups",* vol. 104, American Mathematical Society, pp. 82–84, ISBN 978-0-8218-4781-7