REVIEW OF RESEARCH

IMPACT FACTOR : 5.7631(UIF) UGC APPROVED JOURNAL NO. 48514 ISSN: 2249-894X

VOLUME - 7 | ISSUE - 12 | SEPTEMBER - 2018

A STUDY ON CYCLIC GROUP AND ITS PROPERTIES

Dr. Sheeja S. S.
Guest Lecturer in Statistics, Govt. Arts and Science College,
Kulathoor, Thiruvananthapuram, Kerala

ABSTRACT

The most important mathematicians associated with abstract algebra are Fermat, Leonhard Euler, and Carl Friedrich Gauss. Among them Gauss was establisher of many theorems associated with cyclic groups. Through this work we study about cyclic groups and various properties associated with them in a detailed manner.

KEYWORDS: *Subgroup, Cyclic Group, Virtually Cyclic Group, Meta Cyclic Group, Polycyclic Group.*

1. INTRODUCTION

In algebra, which is a broad division of Mathematics, abstract algebra is the study of algebraic structures such as groups, rings, field's vector spaces. The branch abstract algebra get evaluated and developed in the latter half of nineteenth century. The attempts to find the solution of general polynomial equations of higher degree that resulted in the discovery of groups were the initial breakthrough in abstract algebra.

Groups and groups theory is considered as the foundation of abstract algebra. Simply a group is an algebraic structure consisting of a set of elements equipped with an operation that combines any two elements to form a third element. Other algebraic structures like rings are defined on the basics of groups. Cyclic group is an important derivative of groups which is defined as the groups which are generated by a single element.

2. FUNDAMENTAL THEOREM OF CYCLIC GROUP

Every subgroup of a cyclic group is cyclic. Moreover if $|<a>|=n$, then the order of every subgroup of $<a>$ is a divisor of n, and for each positive divisor k of n, the group $<a>$has exactly one subgroup of order k namely $<a^{n/k}>$.

Example:

Suppose that $G=<a>$ and $|a|=|G|=30$. The divisors of 30 are 1, 2, 3, 5, 6, 10, 15 and 30. G has one and only one subgroup of order each of these divisors. They are $<a^{30/k}>$ for each k=1, 2, 3, 5, 6, 10, 15 and 30. The table below gives as for each order what the subgroup is and what is its generator is

Order	Generator	Group
1	$<a^{30}>$	$\{e\}$
2	$<a^{15}>$	$\{e,a^{5}\}$
3	$<a^{10}>$	$\{e,a^{10},a^{20}\}$
5	$<a^{6}>$	$\{e,a^{6},.....,a^{24}\}$
6	$<a^{5}>$	$\{e,a^{5},a^{10},.....,a^{25}\}$
10	$<a^{3}>$	$\{e,a^{3},a^{6},.....,a^{27}\}$
15	$<a^{2}>$	$\{e,a^{2},a^{4},.....,a^{28}\}$
30	$<a>$	$\{e,a,a^{2},.....,a^{29}\}$

Corollary (subgroups of Z_n)

For each positive divisor k of n, the set <n/k>is the unique subgroup of Z_n, of k; moreover these are the only subgroups of Z_n.

Example:

Similarly to the above example, we let G =Z_{30}. The table below gives the subgroup of Z_{30} and their generator.

Order	Generator	Group
1	<30>	{0}
2	<15>	{0,15}
3	<10>	{0,10,20}
5	<6>	{0,6,12,18,24}
6	<5>	{0,5,10,15,20,25}
10	<3>	{0,3,6,9,12,18,21,24,27}
15	<2>	{0,2,4,6,8,..........,28}
30	<1>	{0,1,2,3,4,..........,29}

3. Euler phi function

Let n$\in Z^{+}$. The Euler phi function of n, denoted φ(n) is the number of positive integers less than n and relatively prime to n we set $\varphi(1)=1$.

Eg :$\varphi(10)=4$

$\varphi(1)=1$

$\varphi(2)=2$

$\varphi(3)=2$

$\varphi(4)=2$

Theorem:

If d is a positive divisor of n, the number of elements of order d in a cyclic group of n is φ(d).

Proof:

There is exactly one group of such order (sag <a>). Every element of order d also generates <a> so counting the elements of order d is the same as counting the elements which can generate <a>.

We know,

An element a^{-k} generates <a>iffgcd (k,d)=1

This number is precisely (d).

Corollary

In a finite group, the number of elements of order d is divisible by φ(d)

Theorem:

Every infinite cyclic group is isomorphic to Z under addition.

Proof:

Let G be an infinite cyclic group with a generator a.
Let as define the mapping f: Z->G, f(n)=a^n.
We have to prove that f is an isomorphism.
Clearly f is onto since any element g$\in G$ has the form an for some n $\in Z$.
Let us prove that f is one to one.
On contrary we assume that m, n$\in Z$ n>m one has f(n)=f(m)
Denote l=n-m, then

$$a^1=a^{m-n}$$
$$=a^n.(a^m)^{-1}$$
$$=f(n).\ (f(m))^{-1}=e.$$ Where e is an identity.

We claim that G has atmost l elements namely

$$G = \{e,a,a^2 ,\ldots\ldots\ldots\ldots a^{l-1}\}$$

Contrary to the assumption that G infinite. Any element in G has the form a^k for some K$\in Z$ .Using the division algoritm.

K=pl+r, pεZ, $0\leq r < 1$

Thus $a^k=a^{pl+r}=a^{pl} .a^r=(a^l)^p .a^r=a^r\in \{e,a,a^2 ,\ldots\ldots.a^{l-i})$

We have to prove that f preserves the structure.
Ie, f(m+n)=f(m).f(n)
But this is evident
F(m,n)=$a^{m+n}=a^m .a^n$=f(m).f(n)

Theorem:

If G is a cyclic group of a finite order n, then G is isomorphic to Z_n

Proof:

Let a be a generator of G consists of the following distinct elements S=$\{e,a,a^2 ,\ldots\ldots a^{n-1}\}$
Suppose that some of these elements coincide.
$A^k=a^l$ for k,l,$\in Z, k > l$.
Then a^{k-l}=e,
we see that G consists of at most k-l distinct elements
.$e,a,a^2 ,\ldots\ldots\ldots\ldots..a^{k-l-1}$
∴K-l<n, this contradict to the assumption
Since S C G and S consists of n elements.
We see that G=S
Let us define the mapping f:Z_n->G, f(k)=a^k .
f is bijective.
It is remain to prove that f preserves the group structure ie, f(m+n)=f(m).f(n)
F(m+n)=$a^{m+n}=a^m .a^n$ =f(m).f(n)

Corollary

i) A cyclic group generated by an element g is finite iffg^n =e for some n≠0.

II) The order of a finite cyclic group generated by an element g coincides with the minimal positive integer n such that g^n =e

Proof

1) If the group <g>is finite;

We know that g^n=e. If on other hand <g> is infinite, then $g^n \neq e\ for\ any\ n\ \neq 0$

2) Fermats little theorem

Let a be any integer. Then a^p=a mod p. In particular a^{p-1} =1 mod p if a is coprime to p.

Proof:

To prove the fermats theorem in generate. We prove congruent class version write the multiplication table of 2/P_Z we vomit the bracket in the table.

Xp	*1*	*2*	*3…………………a…………………………p-1*
1	1.1	1.2	1.3………………1.a……………………1(p-1)
2	2.1	1.3	2.3………………2.a……………………2(p-1)
.	.	.	.
.	.	.	.
.	.	.	.
a	a.1	a.2	a.3…………………a.a…………………a(p-1)
.	.	.	.
.	.	.	.
.	.	.	.
p-1	(p-1)1	(p-1)2	……………………(p-1)a…………………(p-1)(p-1)

Let u(a) denote the set of non zero element in the row corresponding to the multiplication a form which we get.

U(a)=[a.1] [a.2]…………[a].[a]……[a][p-1]≡1(1.2.3……..p-1)modp

While the product of U_i

U(1)=[1][2]…….[p-1]≡1.2.3…….(p-1)(modp)

But U(a)=U(1)

A^{p-1}(1.2…….p-1)(mod p)≡ 1.2.3……….$(p-1)(mod\ p)$

$A^{p-1} \equiv mod\ p$

Let p be a prime number, then

$\varphi(pk)p^k .p^{k-1}$

eg:

What is the order of u_{5000}?

$5000=5(1000)=5\times10^3 =5^4 .2^3$

Now $\varphi(2^3)=2^3-2^2=4$

$\varphi(5^4)=5^4 -5^3=5^3(5-1)=5^3\times4$

$=125\times4$

∵The Euiler phi function is multiplicative, we get

$\varphi(5000) = \varphi(2^3).\varphi(5^4)$

$=4\times125\times4$

$=2000$

Lemma:

Let a be any integer, which is coprime to the positive integer n.
Then $a^{\square(n)} = 1 \bmod n$

Proof

Let $g=[a]\ \varepsilon\ U_n$. Also $g^{\phi(n)} = e$ But then
$[a^{\square(n)}]=[1]$

Thus

$a^{\square(n)} = 1 \bmod n$

Given this it would be really nice to have a quick way to compute $\varphi(n)$.

4. Related classes of groups

Several other classes of groups have been defined by their relation to the cyclic group.

4.1 Virtually cyclic group.

A group is called virtually cyclic group if it contain a cyclic subgroup of finite index.

<or>

Any element in a virtually group can be arrived at by applying a member of a cyclic subgroup to a member in a certain finite set.

Every cyclic group is virtually cyclic, a as it every finite group. An infinite group is virtually cyclic if it is finitely generated and has exactly two ends.

eg: The product of z/n and z in which the 2 factor has finite index n.
Every abelian sub group of a Gromov hyperbolic group is virtually cyclic.

4.2 Locally cyclic group.

It is a group in which each finitely generated subgroup is cyclic
eg: Additive group of the rational number.
A group is locally cyclic if its lattice of subgroup is a distributive lattice.

4.3 Cyclically ordered group

A cyclically ordered group is a group together with a cyclic order preserved by the group is cyclic
Every finite subgroup of a cyclically ordered group is cyclic.

4.4 Metacyclic group and polycyclic group

A metacyclic group is a group containing a cyclic normal subgroup whose quotient is also cyclic. These groups include the cyclic group the dicyclicgroup and the direct product of two cyclic group.

A polycyclic group generalizes metacyclic groups by allowing more than one level of group extension.
eg; Every finitely generated abelian group or nilpotent group is polycyclic.

5. Associated Objects

5.1. Representation

The representation theory of the cyclic group is a critical base case for the representation theory of more general finite groups. In the complex case, a representation of a cyclic group decomposes into a direct sum of linear characters making the connection between character theory and representation theory transparent. In the positive characteristic case, the indecomposable representation of the cyclic group form a model and inductive basis for the representation theory of groups with cyclic sylow subgroups and more generally the representation theory of blocks of cyclic defect.

5.2. Cyclic graph

A cyclic graph illustrates the various cycles of a group and is particularly useful in visualizing the structure of small finite group. A cycle graph for a cyclic group is simply a circular graph, where the group order is equal to the number of nodes. A single generator defines the group as a directional path on the graph, and the inverse generator defines a backwards path. Trivial path can be drawn as a loop but are usually suppressed Z_2 is sometimes drawn with two curved edges as a multi graph.

Cyclic groups Z_n order n is a single cycle graph simply as an n-side polygon with the elements at the vertices. A cyclic group Z_n can be decomposed into a direct product Z_AXZ_B where n=ab where a and b are relatively prime (gcd ca_1b)=1)

5.3. Cayley graph

A Cayley graph is a graph defined from a pair (G,s) where G is a group and S is a set of generators for the group. It has a vertex for each group element and an edge for each product of an element with a generator. In the case of a finite cyclic group with its single generator, the cayley graph is a cycle graph and for an infinite cyclic group with its generator the cayley graph is a doubly infinite path graph.

However cayley graphs can be defined from other sets of generators as well. The cayley graph of cyclic groups with arbitrary generator sets is called circulent graphs. These graphs may be represented geometrically as a set of equally spaced points on a circle or on a line, with each point connected to neighbors with the same set of distance as each other point. They are exactly the vertex-transitive graphs whose symmetry group includes a transitive cyclic group.

5.4. Endomorphism

The endomorphism ring of the abelian group z/nz is isomorphic to z/nz Itself as a ring under this isomorphism the number r corresponds to the endomorphism of z/nz that maps each element to the sum of r copies of it this is bijection iff r is co-prime with x so the automorphism group of z/nz is isomorphic to the unit group z/nz.

Similarly the endomorphism ring of the additive group of Z is isomorphic to the ring Z. Its automorphism group is ismorphic to the group of units of the ring Z.ie, to ({-1,+1),X)

6. Tensor product and hom of cyclic groups.

The tensor product z/mz z/mz and the group of homomorphism
Hom(z/mz,z/mz) can be shown to both be isomorphic to z/gcd(m,n)z

For the tensor product, this is a consequence of the general fact R/IR (I+J). for the Hom group recall that it is isomorphic to the subgroup of z/nz consisting of the elements of order dividing m. That subgroup is cyclic of order gcd (m,n).

CONCLUSIONS

Through this work we studied about cyclic groups and various properties associated with them in a detailed manner.

REFERENCES

1. Alonso, J. M.; et al. (1991), "Notes on word hyperbolic groups". Group theory from a geometrical viewpoint (Trieste, 1990)(PDF), River Edge, NJ: World Scientific, Corollary 3.6, MR 1170363
2. Alspach,Brian (1997), ISOMORPHISM AND Cayley graphs on abelian groups" . Graph symmetry (Montreal, PQ. 1996). NATO Adv. Sci. Inst. Ser.C Math. Phys. Sci. 497, Dordrecht: Kluwer Acad publ., pp. 1-22, ISBN 978-0-792-34668-5, MR 1468786
3. Alluffi, paolo (2009), "6.4 Example: Subgroups of Cyclic Groups". Algebra, Chapter 0, Graduate Studies in Mathematics 104, American Mathematical Society, pp. 82-84, ISBN 978-0-8218-4781-7

4. Bourbaki, Nicolas (1998-08-03) [1970], Algebra 1: chapters 1-3, Elements of Mathematics 1 (softcover reprient ed.), Springer Science & Business Media, ISBN 978-3-540-64243-5
5. Coxeter, H .S. M.; Moser, W.O.J. (1980), Generators and Relations for Discrete Groups, New York: Springer-Verlag, p. 1, ISBN 0-387-09212-9
6. Lajoie, Caroline: Mura, Roberia (November 2000), "What's ina name? A learning difficulty in connection with cyclic groups" , For the Learning of Mathematics 20(3): 29-33, JSTOR 40248334
7. Cox, David A. (2012), Galois Theory, pure and Applied Mathematics (2nd ed.), John Wiley &Sons, Theorem 11.1.7,p.294, doi: 10. 1002/9781118218457, ISBN 978-1-118-07205-9
8. Gallian, Joseph (2010), Contemporary Abstract Algebra (7th edCengage Learning, Exercise-43, p.84, ISBN 978-0-547-16509-7
9. Gannon, Terry (2006), Moonshine beyond the monster. The bridge connecting algebra, modular forms and physics, Cambridge monograohs on mathematical physics, Cambridge University press, p, 18, ISBN978-0-521-83531-2,$Z_n$is simple iff n is prime.
10. Jungnickel, Dieter (1992), "On the uniqueness of the cyclic group of order n". American Mathematical Monthly 99 (6):545-547, doi: 102307/2324062, MR 1166004
11. Fuchs, Laszlo (2011), partially Ordered Algebraic Systems, International series of monographs in pure and applied mathematics 28, Courier Dover Publications,p. 63, ISBN 978-0-486-48387-0
12. Kurzweil, Hans; Stellmacher, Bernd (2004), The Theory of Finite Groups: An Introduction, Universitext, Springer, p. 50, ISBN 978-0-387-40510-0