A STUDY ON PERMUTATION GROUP

(M.MAHALAKSHMI,Dr.S.SANGEETHA,P.ELAVARASI,R.RAMYA)
(ramya25071987@gmail.com,sangeethasankar2016@gmailcom)
Department of Mathematics
Dhanalakshmi Srinivasan College of
Arts and Science for Women (Autonomous)
Perambalur

ABSTRACT

In this paper we introduced what is meant by a permutation on a given set and showed how they form a group. We discussed the cycle notation of permutation and how it is useful in determining various properties of permutation groups. In fact it is shown that a permutation can be decomposed into disjoint cycles uniquely and that order of the permutation is the l.c.m of the lengths of the cycle in a decomposition of disjoint cycles.

INTRODUCTION

In this paper we started the study of groups by considering planar isometrics. We learnt that finite groups of planar isometrics can only be cyclic or dihedral groups. Furthermore, all the groups we've seen thus far are, up to isomorphisms, either cyclic or dihedral groups! It is thus natural to ponder whether there are finite groups out there which can't be interpreted as isometrics of the plane. Permutations are usually studied as combinatorial objects, we'll see during this chapter that they need a natural group structure, and actually , there's a deep connection between finite groups and permutations! We know intuitively what's a permutation: we've some objects from a group , and that we exchange their positions. However, to figure more precisely, we'd like a proper definition of what's a permutation.

PERMUTATION GROUP

Definition: 1.1

A non-empty G together with the binary operation *. (i.e.) (G,*) is named a gaggle if * satisfies the subsequent

Closure : For every a, b €G, a*b €G.

i) Associative :For every a, b, c €G,

a*(b*c) = (a*b)*c

ii) Identity :For exist an element e €G called

The identity element such that

a *e=e*a=a for all a €G.

iii) Inverse : For exist an element a^{-1}€G called the inverse of 'a' such that $a*a^{-1}=a^{-1}*a=e$ for all a €G.

Definition: 1.2

Let (G,*) be a group and H⊆G (H≠ϕ) is said to be a subgroup (H,*) of (G,*)

i) e €H, where e is the identity of G.

ii) For any a €H, a^{-1}€H

iii) For a, b €H, a*b €H

Definition:1.3

Let A ={a_1,a_2,…,a_n} be a finite set such that |A|=n. A bijective mapping or one-to-one and onto mapping p: A→A is defined as a permutation.

The sets of permutations which form a group under this operation are formed as permutation groups.

Definition: 1.4

A group (G,*) is said to be **cyclic** if there exists a €G such that any x €G can be written as either x=an or x= n a, where n is some integer.

Here the element 'a' is called the 'generator' of the cyclic group G. That is the cyclic group generated by 'a' and we denote if by G= (a).

Example:1

Find the generator in the group (A, *) where * is defined as:

*	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	b	a
d	d	c	a	b

Solution:

Using the table for the * operation, it is readily observed that

$a * a = a$, $b * b = a$,

$c * c = c^2 = b$, $c^3 = d$, $c^4 = ac$

$d * d = d^2 = b$, $d^3 = c$, $c^4 = a$.

Therefore (A, *) is generated by c or d and (A, *) is cyclic.

Theorem: 2

Every cyclic group is abelian.

Proof:

A cyclic group is abelian since for any $p, q \in A$, $p = a^m$ and $q = a^n$ for some $m, n \in Z$ and $p * q = a^m * a^n = a^{m+n} = a^{n-m} = a^n * a^m = q * p$. Thus A is abelian.

Theorem: 3

Let $a \in A$ be the generator of a finite cyclic group (A, *). Then the order of the cyclic group is same as the order of its generator.

Proof:

Case (i):

Let the order of the generator a be finite and equals n. Therefore $a^n = e$.

Therefore A comprises the n elements $e, a, a^2, \ldots, a^{n-1}$. If any two elements in it are equal, say

$a^i = a^j$, with $i > j$,

Then $a^{i-j} = e$. Since $0 < i - j \leq n - 1 < n$, we find that $a^{i-j} = e$ and $i - j < n$. This is a contradiction and thus no two elements can be equal to each other in A.

In other words all elements are distinct and A consists of at least n elements.

Let $x \in A$. We may write $x = a^m$ for some $m \in Z$.

Since $m = nq + r$ for $0 \leq r < n$,

$a^m = a^{nq+r} = (a^n)^q * a^r = e * a^r = a^r$,

We find that $x = a^r$, $0 \leq r < n$. Therefore A consists of only n elements.

Case (ii):

The order of a is infinite. In this case it is possible to show that no two powers of the generator can be equal.

If it is so then $a^n = a^m$ and $n < m$.

This implies that $a^{n-m} = e$. In other words it is possible to find a positive integer n – m such that $a^{n-m} = e$ i.e., the order of a is finite, a contradiction.

Hence no two powers of the generator a could be same. Therefore A has the same order as its generator a.

Theorem: 4

A nonempty subset H of a group (A, *) is a subgroup iff,

(i) $\forall a,b \in H, a * b \in H$ and

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

Proof:

Let H be subgroup of A. Then H must be closed under

* Operation in A i.e., $\forall a, b \in H, a * b \in H$.

Next let $a \in H$ and a^{-1} be the inverse

i.e., $a \in H \Rightarrow a^{-1} \in H$.

Theorem: 5

A nonempty subset H of a group (A, *) is a subgroup iff for any pair a, b ∈ H, a * b^{-1}∈ H.

Proof:

Let H be a subgroup.

Therefore for a, b ∈ H, b^{-1}∈ H and a * b^{-1}∈ H.Next

To prove the converse, let a, b∈ H and a * b^{-1}∈ H.

Taking b = a, we find that a * a^{-1} = e ∈ H.

Since e, a, b ∈ H, we have e * a^{-1} = a^{-1}∈ H.

Similarly b^{-1}∈ H. Finally because a, b^{-1} are in H,

We have a * $(b^{-1})^{-1}$∈ H or a * b ∈ H.

Theorem: 6

The direct product of two or more groups is again **a gaggle** .

Proof:

Let (G, *) and (H,Δ) be two groups with identities e_1 and e_2. The direct product of G and H is defined by G x H = {(a_1, b_1)/ a_1∈ G and b_1∈ H}.

Now define the binary operation ° on G x H by

(a_1, b_1) ° (a_2, b_2) = (a1*a2, b_1Δb_2),

For all (a1, b1), (a2, b2) ∈ G x H

Associative: If (a_1, b_1), (a_2, b_2), (a_3, b_3) ∈ G x H,

(a_1, b_1)° ((a_2, b_2) ° (a_3, b_3) = (a_1, b_1) ° (a_2*a_3, b_2Δb_3)

= [a_1*(a_2*a_3), b_1Δ(b_2Δb_3)]

= [(a_1*a_2) * a_3, (b_1Δb_2) Δb_3]

= [(a_1* a_2), (b_1Δb_2)] ° (a_3, b_3)

= [(a_1, b_1) ° (a_2, b_2)] ° (a_3, b_3)

Identity:

Let e_1 be the identity of G and e_2 be the identity of H and e= (e_1, e_2)

Now $(a_1, b_1) \circ e = (a_1, b_1) \circ (e_1, e_2)$

$= (a_1 * e_1, b_1 \Delta e_2)$

$= (a_1, b_1)$

Similarly, $e \circ (a_1, b_1) = (a_1, b_1)$

Inverse: Let $(a_1, b_1)^{-1} = (a_1^{-1}, b_1^{-1})$

$(a_1, b_1) \circ (a_1, b_1)^{-1} = (a1, b1) \circ (a1\text{-}1, b1\text{-}1)$

$= (a_1 * a_1^{-1}, b_1 \Delta b_2^{-1})$

$= (e_1, e_2) = e$

Similarly $(a_1, b_1)^{-1} \circ (a_1, b_1) = e$

$(G \times H, \circ)$ is a group.

Theorem: 7

The Kernel of a homomorphism f from (A, *) to (b, #) is a subgroup of (A, *).

Proof:

We know that $f(e_A) = e_B$, and $e_A \in \ker(f)$.

For $a, b \in \ker(f)$, we find that $f(a) = f(b) = e_B$ and thus $f(a*b) = f(a) \# f(b)$ $= e_B \# e_B = e_B$.

This implies that $a * b \in \ker(f)$.

Further if $a \in \ker(f)$, $f(a^{-1}) = [f(a)]^{-1} = e_B^{-1} = e_B$.

Thus $a^{-1} \in \ker(f)$ and so Ker (f) is a group.

A group homomorphism f is called monomorphism if it is one-to-one.

If it is onto then it termed as epimorphism and if it is both one-to-one and onto then it is termed as isomorphism.

A homomorphism from (A, *) to (A, *) is termed as endomorphism.

Lagrange's Theorem:

If A is a finite group and H is a subgroup of A then O (H) divides O (A).

Proof:

Let n be the order of the group A.

It is known that for each element in A, a right cosset of H can be defined in A and the number of distinct right cossets of H in A is less than or equal to n.

We may therefore write,

$$A = H \cup Ha_1 \cup \ldots \cup Ha_{m-1}$$

Where m is the number of distinct right cossets of H in A. Note that the order of each cosset is the order of H or O (H).

Thus, $O(A) = O(H) + O(Ha_1) + \ldots + O(Ha_{m-1})$

$= O(H) + O(H) + \ldots + O(H)$.

[Sum taken m-times]

$= mk$

Where O (H) = k. Therefore $m = \frac{O(A)}{O(H)}$.

Example: 8

The subset H = {[0], [2]} is a subgroup of

$(A_4, +_4)$.

Solution:

Following table defines the $+_4$ operation:

$+_4$	[0]	[1]	[2]	[4]
[0]	[0]	[1]	[2]	[3]
[1]	[1]	[2]	[3]	[0]
[2]	[2]	[3]	[0]	[1]
[3]	[3]	[0]	[1]	[2]

The distinct left cossets are respectively

{[0] [2]} and {[1], [3]} which partition Z_4.

Example: 9

*	p_1	p_2	p_3	p_4	p_5	p_6

p_1	p_1	p_2	p_3	p_4	p_5	p_6
p_2	p_2	p_1	p_5	p_6	p_3	p_4
p_3	p_3	p_6	p_1	p_5	p_4	p_2
p_4	p_4	p_5	p_6	p_1	p_2	p_3
p_5	p_5	p_4	p_2	p_3	p_6	p_1
p_6	p_6	p_2	p_4	p_2	p_1	p_5

If H = {p1, p2}, find all left cossets of H in S? Also find i_A (H).

Solution:

It is easy to see that

$$p_1H = \{p_1, p_2\} = p_2H = H;$$

$$p_3H = \{p_3, p_6\} = p_6H;$$

$$p4H = \{p_4, p_5\} = p_5H.$$

Thus number of partitions is i_A (H) = $\frac{O(A)}{O(H)}$ = 3, as expected.

CONCLUSION

In this paper we have learnt that modern algebra is a study of sets with operations defined on them. As the main example we've started a scientific study of groups. Group theory is one among the foremost important areas of up to date mathematics, with applications starting from physics and chemistry to coding and cryptography. Further study of groups can be undertaken in the appropriate honors modules.

REFERENCES

1) KA VENKATESH Department of computer Applications Alliance Business Academy, Bangalore.(edition2003)
2) PS ARUNACHALAM Department of Mathematics, SRM Engineering College, Chennai. (edition 2003)
3) I.N.HERSTEIN, Topics in algebra(Second Edition), Wiley Eastern Limited