e content for students of patliputra university

B. Sc. (Honrs) Part 2paper

Subject:Mathematics

Topic:Permutations group, cayley's theorem

permutations group

We recall that a ***permutation of a set*** A is a function $\phi : A \to A$ that is both one to one and onto.

Consider the operation function composition $\circ$ on the collection of all permutations of a set A (we call this operation as *permutation multiplication*). If σ and τ are any two permutations of a set A, we denote the composition of σ

and τ by $\sigma\tau$ instead of $\sigma \circ \tau$. Note that $\sigma\tau$ is clearly one to one and onto (Prove this!). Thus permutation multiplication is a binary operation on the collection of all permutations of a set A.

Remember that the action of $\sigma\tau$ on A is in right- to -left order; i.e., first apply τ, and then σ.

Theorem .

Let A be a nonempty set , and let S_A denotes the collection of all permutations of A. The S_A is a group under permutation multiplication.

Definition

Let A be the finite set $\{1, 2, 3, ..., n\}$. The group of all permutations of the set A is the **symmetric group on n letters**, and is denoted by S_n.

Note that S_n has $n!$ elements.

Example :

Let $A = \{1, 2, 3\}$. Then we list below the $3! = 6$ elements of the symmetric group on three letters.

$$\rho_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \qquad \mu_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix},$$

$$\rho_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \qquad \mu_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix},$$

$$\rho_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \qquad \mu_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

The multiplication table for S_3 is shown in the table given below.

	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_0	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_1	ρ_1	ρ_2	ρ_0	μ_3	μ_1	μ_2
ρ_2	ρ_2	ρ_0	ρ_1	μ_2	μ_3	μ_1
μ_1	μ_1	μ_2	μ_3	ρ_0	ρ_1	ρ_2
μ_2	μ_2	μ_3	μ_1	ρ_2	ρ_0	ρ_1
μ_3	μ_3	μ_1	μ_2	ρ_1	ρ_2	ρ_0

From the table, it is clear that this group is ***not*** abelian.

It is interesting to note that there is a natural correspondence between the elements of S_3 and the ways in which two copies of an equilateral triangle with vertices 1, 2, and 3 can be placed, one covering the other with vertices on top of vertices. Because of this fact, S_3 is also the ***group D_3 of symmetries of an equilateral triangle.***. D_3 is also called the third dihedral group.

In this context, the permutations ρ_i corresponds to rotations and μ_i corresponds to mirror images in bisectors of angles.

Remark.

Any group of at most 5 elements is abelian.

Lemma

Let G and G' be groups and let $\phi : G \to G'$ be a one-to-one function such that $\phi(xy) = \phi(x)\phi(y)$ for all $x, y \in G$. Then the image of G under ϕ, $\phi[G] = \{\phi(g), g \in G\}$, is a subgroup of G' and ϕ provides an isomorphism of G with $\phi[G]$.

Proof.

Let $x', y' \in \phi[G]$. Then there exists $x, y \in G$ such that $\phi(x) = x'$ and $\phi(y) = y'$. By assumption, $\phi(xy) = \phi(x)\phi(y) = x'y' \implies x'y' \in \phi[G]$. Thus $\phi[G]$ is closed under the operation of G'.

Let e' be the identity element in G'. Then, $e'\phi(e) = \phi(e) = \phi(ee) = \phi(e)\phi(e) \implies e' = \phi(e)$ (by right cancellation in G') $\implies e' \in \phi[G]$.

Let $x' \in G'$. Choose $x \in G$ such that $\phi(x) = x'$. Note that $e' = \phi(e) = \phi(xx^{-1}) = \phi(x)\phi(x^{-1}) = x'\phi(x^{-1}) \implies x'^{-1} = \phi(x)^{-1} \in \phi[G]$. Thus $\phi[G]$ is a subgroup of G'.

Also, ϕ is an isomorphism of G onto $\phi[G]$, because ϕ is a one-to-one map of G onto $\phi[G]$ such that $\phi(xy) = \phi(x)\phi(y), \forall x, y \in G$. □

The following theorem due to the British mathematician, Arthur Cayley (1821 – 1895) illustrates the importance of group of permutations.

Theorem *(Cayley's Theorem)*

Every group is isomorphic to a group of permutations.

Proof.

Let G be a group. We show that G is siomorphic to a subgroup of S_G. By above lemma, we need only to show that there exists a one-to-one function $\phi : G \to S_G$ such that $\phi(xy) = \phi(x)\phi(y), \forall x, y \in G$.

For $x \in G$, let $\lambda_x : G \to G$ be defined by $\lambda_x(g) = xg, \forall g \in G$. Then λ_x is one-to-one, because if $\lambda_x(a) = \lambda_x(b)$, then $xa = xb$, so by left cancellation, $a = b$. Let $c \in G$. Then $x^{-1}c \in G$, and $\lambda_x(x^{-1}c) = x(x^{-1}c) = c$, showing that λ_x maps G onto G. Thus λ_x is a permutation of G.

Define $\phi : G \to S_G$ as $\phi(x) = \lambda_x, \forall x \in G$. Suppose that $\phi(x) = \phi(y)$. Then

$\lambda_x = \lambda_y$ as functions mapping G into G. In particular $\lambda_x(e) = \lambda_y(e) \implies xe = ye \implies x = y$. Thus, ϕ is one-to-one. It remains only to show that $\phi(xy) = \phi(x)\phi(y)$, i.e. to show that $\lambda_{xy} = \lambda_x \lambda_y$. Let $g \in G$. Then, $\lambda_{xy}(g) = (xy)g$. Also, $(\lambda_x \lambda_y)(g) = \lambda_x(\lambda_y(g)) = \lambda_x(yg) = x(yg)$. Thus by associativity, $\lambda_{xy} = \lambda_x \lambda_y$. This completes the proof. $\square$