Department of Mathematics

SEM - 6

Course - BMH6DSE33

Group Theory - II

Notes by Rima Dutta

Group Actions

Definition :- Let $(G, \circ)$ be a group and S be a non-empty set. A left action of G on S is a function $\bullet : G \times S \to S$ such that,

(i) $(g_1 \circ g_2) \bullet x = g_1 \bullet (g_2 \bullet x) \quad \forall\, x \in S,\ \forall\, g_1, g_2 \in G$.

(ii) $e \bullet x = x \quad \forall\, x \in S$ and e being the identity element in G.

If there is a left action of G on S then S is called G-set and in this case we say that G acts on S from the left.

Example :- Let G be a group and H be a subgroup of G. Let $S = \{aH : a \in G\}$. We define $\bullet : G \times S \to S$ by

$g \bullet aH = (ga)H \quad \forall\, g \in G$ and $aH \in S$.

Then S is a G-set.

Verification :- Let $g_1, g_2 \in G$ and $aH \in S$.

Then $(g_1 \circ g_2) \bullet aH = (g_1 g_2)aH = g_1(g_2 a)H = g_1 \bullet (g_2 a)H$

$= g_1 \bullet (g_2 \bullet aH)$.

Also, $e \bullet aH = (ea)H = aH$, e being the identity element in G

Thus, S is a G-set.

Theorem :- Let G be a group and S be a G-set. Then the left action of G on S induces a homomorphism from G into $A(S)$, $A(S)$ is the set of all permutation on S.

Proof:- We define $f : G \to A(S)$ by $f(g) = T_g \ \forall \ g \in G$.

where $T_g : S \to S$ is defined by $T_g(a) = ga \ \forall \ a \in S$.

Let $a, b \in S$ such that

$T_g(a) = T_g(b)$

$\Rightarrow ga = gb$

$\Rightarrow a = b$ [by left cancellation law].

$\therefore T_g$ is injective.

Also let $c \in S$.

Then $g^{-1}c \in S$, and

$T_g(g^{-1}c) = g(g^{-1}c) = (gg^{-1})c = c$.

$\therefore T_g$ is surjective.

Thus, T_g is bijective.

$\therefore T_g \in A(S)$.

Thus, f is well defined.

Let $g_1, g_2 \in G$ and $a \in S$.

Then $\cancel{(g_1 g_2) \cdot a} = T_{g_1 g_2}(a) = (g_1 g_2) a = g_1(g_2 a) = T_{g_1}(T_{g_2}(a))$

$= T_{g_1} \circ T_{g_2}(a)$

$\therefore\ T_{g_1 g_2} = T_{g_1} \circ T_{g_2}$.

Now, $f(g_1 g_2) = T_{g_1 g_2} = T_{g_1} \circ T_{g_2} = f(g_1)\, f(g_2)$.

Thus, f is a homomorphism from G to $A(S)$.

Theorem:– Let G be a group and H be a subgroup of G. Let $S = \{aH : a \in G\}$. Then there exists a homomorphism f from G into $A(S)$ (the group of all permutations on S) such that, $\ker f \subseteq H$.

Proof:- We define $\bullet : G \times S \to S$ by $g \bullet aH = (ga)H\ \forall g \in G$ and $\forall aH \in S$.

Then S is a G-set. [PROVE IT].

Hence left action of G on S induces a homomorphism f from G into $A(S)$. [PROVE IT].

Now, $\ker f = \{g \in G : f(g) = \text{identity element of } A(S)\}$.

$= \{g \in G : f(g) = T_e$, e being the identity element in $G\}$.

$= \{g \in G : T_g = T_e\}$.

$= \{g \in G : T_g(aH) = T_e(aH)\ \forall aH \in S\}$.

$= \{g \in G : (ga)H = (ea)H\ \forall aH \in S\}$.

$= \{g \in G : (ga)H = aH\ \forall aH \in S\}$.

$\subseteq \{g \in G : gH = H$, in particular we take eH for $aH\}$.

$= \{g \in G : g \in H\}$.

$= H$.

Theorem (Caley theorem) :-

Any group G is isomorphic to a subgroup of the permutation group $A(G)$.

Proof:- We define $T_g : G \to G$ by $T_g(a) = ga \quad \forall a \in G$.

Let $a_1, a_2 \in G$. such that

$T_g(a_1) = T_g(a_2)$.

$\Rightarrow ga_1 = ga_2$

$\Rightarrow a_1 = a_2$ [by left cancellation law].

$\therefore T_g$ is injective.

Again let $b \in G$.

Then $g^{-1}b \in G$ and $T_g(g^{-1}b) = g(g^{-1}b) = (gg^{-1})b = b$.

Thus, T_g is surjective.

$\therefore T_g$ is bijective and hence $T_g \in A(G)$.

~~Also,~~ $\cancel{T_g^{-1}(a) = g^{-1}a = T_g}$

Also, $T_{g^{-1}} = (T_g)^{-1}$ and $T_{g_1 g_2} = T_{g_1} \circ T_{g_2}$ for all $g, g_1, g_2 \in G$.

Now we define $f : G \to A(G)$ by $f(g) = T_g \ \forall g \in G$.

Then for $g_1, g_2 \in G$, we have $f(g_1 g_2) = T_{g_1 g_2}$

$$= T_{g_1} \circ T_{g_2}$$

$$= f(g_1) \cdot f(g_2)$$

Thus, f is a homomorphism.

Again let $g_1, g_2 \in G$ such that

$$f(g_1) = f(g_2)$$

$$\Rightarrow T_{g_1} = T_{g_2}$$

$$\Rightarrow T_{g_1}(a) = T_{g_2}(a) \ \forall a \in G.$$

$$\Rightarrow g_1 a = g_2 a \ \forall a \in G.$$

$$\Rightarrow g_1 = g_2 \ [\text{by right cancellation law}].$$

Thus, f is injective.

Thus, G is isomorphic to the subgroup $f(G)$ of $A(G)$.

<u>Theorem</u> :- Let G be a group of order $2m$, m is an odd integer. Show that G has a normal subgroup of order m.

<u>Solution</u> :- Since G is a group of even order, so there exists an element $g \in G$ such that $o(g) = 2$.

Now, by Caley's theorem, G is isomorphic to a subgroup H of $A(G)$ where $f: G \to A(G)$ is given by

$f(x) = T_x \ \forall x \in G$ where $T_x : G \to G$ is given by

$T_x(a) = xa \ \forall a \in G$.

Now, we show that T_g is an odd permutation.

Now, $T_g(ga) = g(ga) = g^2 a = ea = a. \ \forall a \in G$

$\therefore T_g$ is a product of transpositions of the from $(a \ ga)$.

Since $|G| = 2m$, so the number of transpositions appearing in the factorization of T_g is m.

Since m is odd, so T_g is an odd permutation.

$\therefore T_g \in H$.

$\therefore H$ cantains an odd permutation.

Again note that H contains an even permutation. that is identity permutation.

Now, we define a function $\psi : H \to \{-1, 1\}$ by

$$\psi(\sigma) = \begin{cases} -1 & \text{if } \sigma \text{ is an odd permutation.} \\ 1 & \text{if } \sigma \text{ is an even permutation.} \end{cases}$$

where $\{-1, 1\}$ is a group under multiplication.

Then ψ is an onto homomorphism.

Hence by first isomorphism theorem,

$$H/\ker\psi \cong \{-1, 1\}.$$

$$\therefore \left| H/\ker\psi \right| = 2$$

ie. $$\frac{|H|}{|\ker\psi|} = 2$$

ie. $$|\ker\psi| = \frac{|H|}{2} = \frac{2m}{2} = m.$$

So, H has a normal subgroup ie. $\ker\psi$ of order m.

Hence G has a normal subgroup of order m.

Definition :— Let S be a G-set, where G is a group. On S, we define a relation '$\sim$' by for all $a, b \in S$, $a \sim b$ if and only if $ga = b$ for some $g \in G$.

Let $a \in S$.

Then $ea = a$ ($\because S$ is a G-set)

$\therefore a \sim a$ holds.

$\therefore$ '$\sim$' is reflexive.

Again let $a, b \in S$. s.t.

$a \sim b$.

Then $ga = b$ for some $g \in G$.

$\Rightarrow a = g^{-1}b$.

$\Rightarrow b \sim a$ holds.

$\therefore$ '$\sim$' is symmetric.

Again let $a, b, c \in S$ s.t.

$a \sim b$ and $b \sim c$ hold.

i.e. $g_1 a = b$ and $g_2 b = c$ for some $g_1, g_2 \in G$.

$\Rightarrow g_2 g_1 a = g_2 b = c$

$\Rightarrow ga = c$ where $g = g_2 g_1 \in G$.

$\Rightarrow a \sim c$.

Thus, '$\sim$' is transitive.

Hence '$\sim$' is an equivalence relation.

Then S can be partitioned into disjoint equivalence classes. Here each equivalence classes are called orbit and the ~~ord~~ orbit of an element $a \in S$ is denoted by $[a]$ and $[a] = \{ b \in S : ga = b$ for some $g \in G \}$.

$= Ga$.

Definition :- Let G be a group and S be a G-set. Also let $a \in S$ and $g \in G$. Then a is said to fixed by g if $ga = a$. If $ga = a$ for all $g \in G$ then a is called fixed by G.

Definition (Stabilizer group):- Let S be a G-set, where G is a group. We consider the subset G_a of G where

$G_a = \{ g \in G : ga = a \}, a \in S$.

Scanned with CamScanner

Note that $ea = a$ ($\because$ S is a G-set).

$\therefore e \in G_a$.

$\therefore G_a \neq \phi$.

Let $x, y \in G_a$.

Then $xa = a$, $ya = a$.

Now, $ya = a \Rightarrow y^{-1}ya = y^{-1}a \Rightarrow a = y^{-1}a$.

$\therefore (xy^{-1})a = x(y^{-1}a) = xa = a$.

$\therefore xy^{-1} \in G_a$.

Thus, G_a is a subgroup of G.

This subgroup is called fixed subgroup of a or stabilizer of a or isotropy group of a.

Thm : Let G be a group and S be a G-set. Then for all $a \in S$, $[G : G_a] = |[a]|$.

Proof:- Let H be the set of all left cosets of G_a in G.

ie. $H = \{ xG_a : x \in G \}$.

Now, $[a] = \{ b \in S : ga = b \text{ for some } g \in G \}$.

We define a function $\psi : H \to [a]$ by

$\psi(gG_a) = ga$ for $g \in G$.

Now $xG_a,\ yG_a \in H$ and

~~Then~~ $xG_a = yG_a$

$\Leftrightarrow x^{-1}y \in G_a$

$\Leftrightarrow x^{-1}ya = a$

$\Leftrightarrow xa = ya.$

$\cancel{\Rightarrow \psi(xa) = \psi(ya)}.$

$\Leftrightarrow \psi(xG_a) = \psi(yG_a).$

Thus, '$\Rightarrow$' shows that ψ is well defined.

and '$\Leftarrow$' shows that ψ is injective.

Also let $ga \in [a]$ for some $g \in G$.

Then $gG_a \in H$ and $\psi(gG_a) = ga$.

$\therefore$ ψ is surjective.

Hence ψ is bijective.

Therefore, $|H| = |[a]|$ ie. $[G : G_a] = |[a]|$.

Thm: Let G be a group and S be a finite G-set.

Then $|S| = \sum_{a \in A} [G : G_a]$, where A is a finite subset of S containing exactly one element from orbit.

Proof:- Since S is finite, so the number of orbits of S is finite.

Therefore, $S = [a_1] \cup [a_2] \cup \ldots \cup [a_n] = \bigcup_{a \in A} [a]$,

where $A = \{a_1, a_2, \ldots, a_n\}$ containing exactly one element from each orbit.

Hence $|S| = \sum_{a \in A} |[a]|$

Also, $|[a]| = [G : G_a]$.

$\therefore |S| = \sum_{a \in A} [G : G_a]$.

Problem 1 :- Let G be a finite group and H be a subgroup of G of index n such that $|G|$ does not devide $n!$ Then G contains a non-trivial normal subgroup.

Solution :- Let $S = \{aH : a \in G\}$.

Since G is finite, so S is finite also.

Again, $|S| = [G : H] = n$.

Now, we define $\bullet : G \times S \to S$ by $g \bullet aH = (ga)H$ for all $g \in G$ and for all $aH \in S$.

Then under this operation, S is a G-set. and this left action induces a homomorphism $f : G \to A(S)$ such that $\ker f \subseteq H$.

Hence by first isomorphism theorem,

$G/\ker f$ is isomorphic to a subgroup of $A(S)$.

So, $|G/\ker f|$ divides $n!$

But, $|G|$ does not divide $n!$

So, $|\ker f| \neq 1$.

Thus, $\ker f$ is a non-trivial normal subgroup of G.

Problem 2:- Let G be a finite group of order pn where p is prime and $p > n$. If H is a subgroup of G of order p, then prove that H is normal subgroup of G.

Solution:- It is given that, $|H| = p$.

So, $[G:H] = n$.

Let $S = \{aH : a \in G\}$.

Then $|S| = [G:H] = n$.

Now, we define $\cdot : G \times S \to S$ by $g \cdot aH = (ga)H$ for all $g \in G$ and $aH \in S$.

Then under this operation, S is a G-set. and this left action induces a homomorphism $f : G \to A(S)$ such that $\ker f \subseteq H$.

Now, $|H| = p$ and $\ker f \subseteq H$, ~~so ther~~

so by Lagrange's theorem,

$|\ker f| \,\big|\, |H|$.

i.e. $|\ker f| \,\big|\, p$.

i.e. $|\ker f| = 1$ or p ($\because p$ is prime)

If $|\ker f| = 1$, so f is a monomorphism.

Therefore $f : G \to f(G)$ is an isomorphism.

$\therefore |G| = |f(G)|$ and also $|f(G)| \,\big|\, n!$

$\therefore |G|$ divides $n!$

i.e. $pn \,\big|\, n!$ i.e. $p \,\big|\, (n-1)!$

But $p > n$.

So, p does not divide $(n-1)!$, this is a contradiction.

$\therefore |\ker f| \neq 1$.

$\therefore |\ker f| = p$.

Hence $|H| = |\ker f|$.

Since $\ker f$ is a normal subgroup of G, so H is a normal subgroup of G.

Problem 3:– Let G be a finite group. Let H be a subgroup of G of index p, where p is ~~prime~~ the smallest prime dividing $|G|$. Show that H is a normal subgroup of G.

Solution :– Let $S = \{aH : a \in G\}$.

Then $|S| = [G : H] = p$.

Now, we define $\bullet : G \times S \to S$ by $g \bullet aH = (ga)H$ for all $g \in G$ and $aH \in S$.

Then under this operation, S is a G-set. and this left action induces the homomorphism $f : G \to A(S)$ such that $\ker f \subseteq H$.

Then by first isomorphism theorem,

$G/\ker f$ is isomorphic to a subgroup of $A(S)$. and that is $f(G)$.

So, $|G/\ker f|$ divides $p!$

Let $|G/\text{Ker} f| = n$.

Then $n \mid |G|$.

Let $n = p_1 p_2 \cdots p_k$ where p_i's are prime for $i = 1, 2, \ldots, k$.

Now each p_i divides $|G|$ and p is the smallest prime dividing $|G|$.

So, $p \leq p_i \ \forall i = 1, 2, \ldots, k$.

Again n divides $p!$

So each p_i divides $p!$

Since each p_i is prime and $p \leq p_i$ so we must have, $i = 1$ and $p_i = p$.

Thus, $p = n$.

So, $[H : \text{Ker} f] = \dfrac{|H|}{|\text{Ker} f|} = \dfrac{|H|}{|G|} \times \dfrac{|G|}{|\text{Ker} f|} = \dfrac{[G : \text{Ker} f]}{[G : H]}$

$$= \frac{p}{p} = 1.$$

Hence $|H| = |\text{Ker} f|$

Also, $\text{Ker} f \subseteq H$.

Hence $H = \text{Ker} f$.

Since $\text{Ker} f$ is a normal subgroup of G.

Thus, H is a normal subgroup of G.

Problem :- Let H be a subgroup of a group G. Prove that if H ~~is~~ has a finite index n then there is a normal subgroup K of G with $K \subseteq H$ and $[G:K] \leq n!$

Solution :- Let $S = \{aH : a \in G\}$.

Now, we define $\bullet : G \times S \to S$ by $g \bullet aH = (ga)H$ for all $g \in G$ and $aH \in S$.

Then under this operation, S is a G-set and this left action induces a homomorphism $f : G \to A(S)$ such that $\ker f \subseteq H$.

Let $K = \ker f$.

Then K is a normal subgroup of G and hence by first isomorphism theorem, $G/K \cong T$ where $T = f(G)$ is a subgroup of $A(S)$.

since $|S| = [G:H] = n$, so $|A(S)| = n!$.

Therefore, $|T| \leq n!$

$\therefore$ $|G/K| \leq n!$

ie. $[G/K] \leq n!$

Therefore, there is a normal subgroup K of G such that $[G:K] \leq n!$.

Exercise :-

1. Let H be a subgroup of order 11 and index 4 of a group G. Then prove that H is a normal subgroup of G.

2. Let G be a group acting on a set S, containing atleast two elements. Assume that G is transitive, ie. given any $x, y \in S$, there exists $g \in G$ such that $gx = y$. Prove that
   (i) for $x \in S$, the orbit $[x]$ of x is S.
   (ii) all the stabilizer G_x $(x \in S)$ are conjugate.
   (iii) if G has the properly : $\{g \in G : gx = x \text{ for all } x \in S\} = \{e\}$, and if N is a normal subgroup of G and N is a subgroup of G_x for some $x \in S$, then $N = \{e\}$.

3. A normal subgroup H of a group G is said to be direct factor of G if there exists a (normal) subgroup K such that $G = H \times K$. If H is a direct factor of K and K is a direct factor of G then prove that H is normal in G.

4. Let G be a group and let $\pi : G \to A(G)$ be a group homomorphism defined by $(\pi(g))(a) = ga$ for all $g, a \in G$. Prove that if x is an element of G of order n and $|G| = mn$, then $\pi(x)$ is a product of m number of n-cycles.

. Consider the group action of S_5 on the set $X = \{1,2,3,4,5\}$. Also let G be a subgroup of S_5 generated by $\{(1\,2), (3\,4\,5)\}$. Then find all the distinct orbits of X under G. and also find stabilizer subgroup of G.

6. Consider the symmetric group S_3 on the set $I_3 = \{1,2,3\}$. Define the left actions of S_3 on I_3 by $\sigma a = \sigma(a)$ for all $\sigma \in S_3$; $a \in I_3$. Describe all the distinct orbits of I_3. and stabilizer of each element of I_3.

7. Let G be the permutation group $\{(1), (1\,2\,3), (4\,5), (1\,2\,3)(4\,5), (1\,3\,2)(4\,5)\}$ on the set $I_5 = \{1,2,3,4,5\}$. Define the left action of G on I_5 by $\sigma a = \sigma(a)$ for all $\sigma \in G$, $a \in I_5$. Find all distinct orbits and stabilizer of each element of I_5.

8. Consider the left action of the group $G = GL(2,\mathbb{R})$ on $G = GL(2,\mathbb{R})$ by conjugation. Find the orbit and stabilizer of $\begin{bmatrix} 1 & 0 \\ 0 & 4 \end{bmatrix}$.

9. Let G be a group and S be a G-set. For any $x \in S$, G_x denotes the stabilizer of x. Prove that

$$G_{b\cdot x} = b\, G_x\, b^{-1} \text{ for all } b \in G,\ x \in S.$$

10. Consider the action of $GL(2,\mathbb{R})$ on $\mathbb{R}^2$ by matrix multiplication (where elements of $\mathbb{R}^2$ are written as column matrix). Then (i) what is the stabilizer of $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$?

(ii) What is the orbit of $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$?

~~Solved example :-~~

Solved example :-

6. $S_3 = \{e, (1\,2), (1\,3), (2\,3), (1\,2\,3), (1\,3\,2)\}$.

$I_3 = \{1, 2, 3\}$.

Now, orbit of $a = [a] = \{x \in G : gx = a \text{ for some } g \in G\}$.

Now, $e1 = e(1) = 1$	$(1\,2)\,1 = (1\,2)(1) = 2$
$e2 = e(2) = 2$	$(1\,2)\,2 = (1\,2)(2) = 1$
$e3 = e(3) = 3$.	$(1\,2)\,3 = (1\,2)(3) = 3$.
$(1\,3)\,1 = (1\,3)(1) = 3$	$(2\,3)\,1 = (2\,3)(1) = 1$
$(1\,3)\,2 = (1\,3)(2) = 2$	$(2\,3)\,2 = (2\,3)(2) = 3$
$(1\,3)\,3 = (1\,3)(3) = 1$.	$(2\,3)(3) = (2\,3)(3) = 2$.
$(1\,2\,3)\,1 = (1\,2\,3)(1) = 2$	$(1\,3\,2)\,1 = (1\,3\,2)(1) = 3$
$(1\,2\,3)\,2 = (1\,2\,3)(2) = 3$	$(1\,3\,2)\,2 = (1\,3\,2)(2) = 1$.
$(1\,2\,3)(3) = (1\,2\,3)(3) = 1$.	$(1\,3\,2)\,3 = (1\,3\,2)(3) = 2$.

$\therefore$ $[1] = \{1, 2, 3\}$. and $G_1 = \{e, (2\,3)\}$.

$[2] = \{1, 2, 3\}$ and $G_2 = \{e, (1\,3)\}$

$[3] = \{1, 2, 3\}$. and $G_3 = \{e, (1\,2)\}$.

Thus, here the distinct orbit of I_3 is $[1]$. and Stabilizer of 1 is $\{e, (2\,3)\}$, stabilizer of 2 is $\{e, (1\,3)\}$ and stabilizer of 3 is $\{e, (1\,2)\}$.