Subject : MATHEMATICS

Paper 1 : ABSTRACT ALGEBRA

Chapter 3 : Sylow Theorems

Module 1 : Group action

Anjan Kumar Bhuniya
Department of Mathematics
Visva-Bharati; Santiniketan
West Bengal

Group action

Learning outcomes:	1. Group actions.
	2. Some applications of group actions.
	3. Burnside Theorem.

Lagrange's Theorem states that order of every subgroup H of any finite group G divides the order of the group G. Already we have seen that the converse of the Lagrange's Theorem holds for finite commutative groups. If G is a finite non-commutative group, then Cauchy's Theorem implies that for every prime divisor p of $|G|$, G has a subgroup of order p. M. L. Sylow's works on the structure of finite groups are of fundamental importance in this direction. In the next four modules we discuss Sylow Theorems and some of their applications to characterize structure of finite groups. There are several proofs of Sylow Theorems. We use the technique of group action, a concept which generalizes both the notions of automorphism and symmetry. Conjugation of an element of a group is a particular example of group action.

Definition 0.1. *Let G be a group and S a nonempty set. A (left) action of G on S is a function $G \times S \longrightarrow S$, usually denoted by $(g, s) \longmapsto gs$ such that*

1. $(g_1 g_2)s = g_1(g_2 s)$, *and*

2. $es = s$, *where e is the identity of G for all $s \in S, g_1, g_2 \in G$.*

If there is a left action of G on S, we say that G acts on S on the left and S is a G-set.

Example 0.2. *Let G be a group. Then $G \times G \longrightarrow G$ defined by $a \cdot g = aga^{-1}$ is a left action of G on itself.*

Let S be the set of all subgroups of G. Then $G \times S \longrightarrow S$ defined by $a \cdot H = aHa^{-1}$ is a left action of G on S.

Example 0.3. *Let G be a permutation group on a set S. Define a left action $G \times S \longrightarrow S$ of G on S by:*

$$\sigma \cdot s = \sigma(s) \text{ for all } \sigma \in G, s \in S.$$

Denote the identity permutation by e. Then for every $s \in S$, $e \cdot s = e(s) = s$. Let $\sigma_1, \sigma_2 \in G$. Then $(\sigma_1 o \sigma_2) \cdot s = (\sigma_1 o \sigma_2)(s) = \sigma_1(\sigma_2(s)) = \sigma_1 \cdot (\sigma_2(s)) = \sigma_1 \cdot (\sigma_2 \cdot s)$. Hence, S is a G-set.

Example 0.4. *Let G be a group and H be a normal subgroup of G. Define a left action $G \times H \longrightarrow H$ of G on H by*

$$g \cdot h \longrightarrow ghg^{-1} \text{ for all } g \in G, h \in H.$$

For every $h \in H$, $e \cdot h = ehe^{-1} = ehe = h$.

Also for $g_1, g_2 \in G$,

$$\begin{aligned}(g_1g_2) \cdot h &= (g_1g_2)h(g_1g_2)^{-1} \\ &= (g_1g_2)h(g_2^{-1}g_1^{-1}) \\ &= g_1(g_2hg_2^{-1})g_1^{-1} \\ &= g_1(g_2 \cdot h)g_1^{-1} \\ &= g_1 \cdot (g_2 \cdot h).\end{aligned}$$

Hence H is a G-set.

Theorem 0.5. *Let G be a group and S be a G-set. Then the binary relation $\sim$ on S defined by: for all $a, b \in S$,*

$$a \sim b \text{ if } b = ga \text{ for some } g \in G,$$

is an equivalence relation.

Proof. For all $a \in S$, $ea = a$ implies that $a \sim a$. Thus $\sim$ is reflexive. Let $a, b \in S$ be such that $a \sim b$. Then $ga = b$ for some $g \in G$, which implies that $g^{-1}b = g^{-1}(ga) = (g^{-1}g)a = ea = a$. Hence, $b \sim a$, and so $\sim$ is symmetric. Now suppose $a \sim b$ and $b \sim c$. Then there exist $g_1, g_2 \in G$ such that $g_1a = b$ and $g_2b = c$, and it follows that $(g_2g_1)a = g_2(g_1a) = g_2b = c$. Thus $a \sim c$ and so $\sim$ is transitive. Hence, $\sim$ is an equivalence relation on S. □

Definition 0.6. *Let S be a G-set, where G is a group and S is a nonempty set. Then the equivalence classes determined by the equivalence relation $\sim$ are called the orbits of G on S.*

For $a \in S$, the orbit containing a is denoted by $[a]$. Thus

$$\begin{aligned}[a] &= \{b \in S \mid a \sim b\} \\ &= \{b \in S \mid b = ga \text{ for some } g \in G\} \\ &= \{ga \mid g \in G\}.\end{aligned}$$

Lemma 0.7. *Let G be a group and S be a G-set. For all $a \in S$, the subset*

$$G_a = \{g \in G | ga = a\}$$

is a subgroup of G.

Proof. Let $a \in S$. Then $ea = a$ implies that $e \in G_a$, and so $G_a \neq \emptyset$. Let $g, h \in G_a$. Then $ga = a$ and $ha = a$. Now $ha = a$ implies that $h^{-1}a = a$ and it follows that $(gh^{-1})a = g(h^{-1}a) = ga = a$. Thus, $gh^{-1} \in G_a$. Hence, G_a is a subgroup of G. □

The subgroup G_a is called the stabilizer of a or the isotropy group of a.

Example 0.8. *Let G be a group. Consider the action of G on itself by conjugation. Then the equivalence relation $\sim$ is the conjugacy relation. For $a \in G$, the stabilizer of a is*

$$\begin{aligned} G_a &= \{g \in G \mid ga = a\} \\ &= \{g \in G \mid gag^{-1} = a\} \\ &= \{g \in G \mid ga = ag\} \\ &= C(a), \end{aligned}$$

the centralizer of a.

Example 0.9. *Let G be a group and S be the set of all subgroups of G. Consider the action of G on S by conjugation of subgroups, that is, $gH = gHg^{-1}$. For $H \in S$, the stabilizer of H is*

$$\begin{aligned} G_H &= \{g \in G \mid gH = H\} \\ &= \{g \in G \mid gHg^{-1} = H\} \\ &= N(H), \end{aligned}$$

the normalizer of H.

Now we investigate relations between orbit $[a]$ and isotropy group G_a of every $a \in S$.

Lemma 0.10. *Let G be a group and S be a G-set. Then,*

$$[G : G_a] = |[a]| \text{ for all } a \in S.$$

Proof. Let $a \in S$. Denote $\mathcal{L} = \{gG_a \mid g \in G\}$, the set of all left cosets of G_a in G. Also $[a] = \{ga|g \in G\}$. Now define $f : \mathcal{L} \longrightarrow [a]$ by

$$f(gG_a) = ga \text{ for all } gG_a \in \mathcal{L}.$$

Let $g_1, g_2 \in G$. Then $g_1G_a = g_2G_a$ if and only if $g_2^{-1}g_1 \in G_a$ if and only if $g_2^{-1}(g_1a) = (g_2^{-1}g_1)a = a$ if and only if $g_1a = g_2a$. Thus, f is a one-to-one function from $\mathcal{L}$ into $[a]$. Also it follows from the definition of f that it is onto. Hence, $[G : G_a] = |\mathcal{L}| = |[a]|$. □

Theorem 0.11. *Let G be a group and S be a G-set. If S is finite, then*

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

where A is a complete set of distinct representatives of the orbits.

Proof. Let A be a complete set of distinct representatives of the orbits of G on S. Since the orbits yields a partition of S, so $S = \cup_{a \in A}[a]$. Hence,

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

$\square$

Now we give some useful consequences of group action.

Theorem 0.12. *Let G be a group and S be a G-set. Then the action of G on S induces a homomorphism from G into the group $A(S)$ of all permutations of S.*

Proof. Let $g \in G$. Define a mapping $\tau_g : S \longrightarrow S$ by:

$$\tau_g(a) = ga \text{ for all } a \in S.$$

Then for every $a \in S$, $g(g^{-1}a) = (gg^{-1})a = ea = a$ implies that $\tau_g(g^{-1}a) = a$. Thus τ_g is onto. Now for $a, b \in S$,

$$\begin{aligned} \tau_g(a) = \tau_g(b) &\Rightarrow ga = gb \\ &\Rightarrow g^{-1}(ga) = g^{-1}(gb) \\ &\Rightarrow (g^{-1}g)a = (g^{-1}g)b \\ &\Rightarrow a = b, \end{aligned}$$

and so τ_g is one-to-one. Hence $\tau_g \in A(S)$. Also for every $g_1, g_2 \in G$ and $a \in S$,

$$\begin{aligned} \tau_{g_1 g_2}(a) &= (g_1 g_2)a \\ &= g_1(g_2 a) \\ &= \tau_{g_1}(g_2 a) \\ &= \tau_{g_1}(\tau_{g_2}(a)) \\ &= \tau_{g_1} \circ \tau_{g_2}(a) \end{aligned}$$

implies that $\tau_{g_1 g_2} = \tau_{g_1} \circ \tau_{g_2}$. Hence the mapping $\psi : G \longrightarrow A(S)$ defined by

$$\psi(g) = \tau_g \text{ for all } g \in G$$

is a homomorphism from G into $A(S)$. $\square$

Corollary 0.13. *Every group is isomorphic to a group of permutations.*

Proof. Let G be a group. Define an action of G on G by left translation, that is,

$$(g, a) \longmapsto ga.$$

Then $\psi : G \longrightarrow A(G)$ as defined in the previous theorem is a homomorphism of G into $A(G)$.

Thus it remains to show only that ψ is one-to-one. Now for $g_1, g_2 \in G$,

$$\begin{aligned}\psi(g_1) = \psi(g_2) &\Rightarrow \tau_{g_1} = \tau_{g_2}\\ &\Rightarrow \tau_{g_1}(a) = \tau_{g_2}(a) \text{ for all } a \in G\\ &\Rightarrow \tau_{g_1}(e) = \tau_{g_2}(e)\\ &\Rightarrow g_1 = g_2.\end{aligned}$$

Thus it follows that ψ is a monomorphism. $\square$

Corollary 0.14. *Let G be a finite group and p be the smallest prime divisor of $|G|$. Then every subgroup H of G of index p is normal in G.*

Proof. Let H be a subgroup of G such that $[G : H] = p$. Denote $S = \{aH \mid a \in G\}$. Then $G \times S \longrightarrow S$ defined by $(g, aH) \longmapsto (ga)H$ is an action of G on S. So we have a homomorphism $\psi : G \longrightarrow A(S)$ defined by: $\psi(g) = \tau_g$ for all $g \in G$, where $\tau_g : S \longrightarrow S$ is given by:

$$\tau_g(aH) = (ga)H.$$

Let $K = \ker \psi$. Then K is a normal subgroup of G and $K \subseteq H$. Now $|S| = [G : H] = p$ shows that $|A(S)| = p!$. Since G/K is isomorphic to a subgroup of $A(S)$, so $|G/K| \mid p!$. Also $|G| = |K||G/K|$ shows that every divisor of $|G/K|$ is also a divisor of $|G|$. But p is the smallest prime divisor of $|G|$ and so $|G|$ can not have any divisor less than p but 1. hence $|G/K| = p$ or 1. But $|G/K| = [G : K] = [G : H][H : K] \geq p$ shows that $|G/K| = p = [G : H]$. Hence $[H : K] = 1$ and $H = K$. Thus H is a normal subgroup of G. $\square$

The following result has many combinatorial applications.

Theorem 0.15 (Burnside)**.** *Let G be a finite group and S be a finite G-set. Then the number of orbits of G on S is given by*

$$\frac{1}{|G|} \sum_{g \in G} F(g),$$

where $F(g)$ is the number of elements of S fixed by g.

Proof. Consider the set $T = \{(g, a) \in G \times \ S | ga = a\}$. For every $g \in G$, denote the number of elements $a \in S$ such that $ga = a$. Then $F(g)$ is the number of elements $a \in S$ such that $(g, a) \in T$, and it follows that $|T| = \sum_{g \in G} F(g)$. Also, for every $a \in S$, $G_a = \{g \in G \mid (g, a) \in T\}$. Hence, $|T| = \sum_{a \in S} |G_a|$.

Suppose that G has k orbits on S and $[a_1], [a_2], \cdots, [a_k]$ is a complete list of distinct orbits of G on S. Then $S = [a_1] \cup [a_2] \cup \cdots \cup [a_k]$, and hence

$$\sum_{g\in G} F(g) = \sum_{a\in[a_1]} |G_a| + \sum_{a\in[a_2]} |G_a| + \cdots + \sum_{a\in[a_k]} |G_a|.$$

If a, b are in the same orbit, then $[a] = [b]$ and $[G : G_a] = |[a]| = |[b]| = [G : G_b]$. This implies that

$$\frac{|G|}{|G_a|} = \frac{|G|}{|G_b|}$$

and so $|G_a| = |G_b|$. Thus,

$$\begin{aligned}\sum_{g\in G} F(g) &= |[a_1]||G_{a_1}| + |[a_2]||G_{a_2}| + \cdots + |[a_k]||G_{a_k}| \\ &= \frac{|G|}{|G_{a_1}|}|G_{a_1}| + \frac{|G|}{|G_{a_2}|}|G_{a_2}| + \cdots + \frac{|G|}{|G_{a_k}|}|G_{a_k}| \\ &= k|G|,\end{aligned}$$

Consequently, the number of orbits of G on S is

$$k = \frac{1}{|G|}\sum_{g\in G} F(g).$$

□

1 Summary

- Let G be a group and S a nonempty set. A (left) action of G on S is a function $G \times S \longrightarrow S$, usually denoted by $(g, s) \longmapsto gs$ such that

  (i) $(g_1g_2)s = g_1(g_2s)$, and

  (ii) $es = s$, where e is the identity of G for all $s \in S, g_1, g_2 \in G$.

  If there is a left action of G on S, we say that G acts on S on the left and S is a G-set.

- Let G be a group and S be a G-set. Then the binary relation $\sim$ on S defined by: for all $a, b \in S$,

  $$a \sim b \text{ if } b = ga \text{ for some } g \in G,$$

  is an equivalence relation. The equivalence classes determined by the equivalence relation $\sim$ are called the orbits of G on S.

  For $a \in S$, the orbit containing a is denoted by $[a]$. Thus $[a] = \{ga \mid g \in G\}$.

- Let G be a group and S be a G-set. For all $a \in S$, the subset

$$G_a = \{g \in G | ga = a\}$$

is a subgroup of G which is called the stabilizer of a or the isotropy group of a.

- Let G be a group. For every $a \in G$, the stabilizer of a under conjugation is $C(a)$, the centralizer of a.

- Let G be a group and H be a subgroup of H. Then the stabilizer of H under conjugation is $N(H)$, the normalizer of H.

- Let G be a group and S be a G-set. Then,

$$[G : G_a] = |[a]| \text{ for all } a \in S.$$

- Let G be a group and S be a G-set. If S is finite, then

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

where A is a complete set of distinct representatives of the orbits.

- Let G be a group and S be a G-set. Then the action of G on S induces a homomorphism from G into the group $A(S)$ of all permutations of S.

- Every group is isomorphic to a group of permutations.

- Let G be a finite group and p be the smallest prime divisor of $|G|$. Then every subgroup H of G of index p is normal in G.

- (Burnside) Let G be a finite group and S be a finite G-set. Then the number of orbits of G on S is given by

$$\frac{1}{|G|} \sum_{g \in G} F(g),$$

where $F(g)$ is the number of elements of S fixed by g.