Group action and some of its Applications

Pavinder Singh

Department of Mathematics

Central University of Jammu

Jammu, INDIA

5 February, 2016

- $\mathbb{Z}$, the set of integers
- $\mathbb{R}$, the set of real numbers
- $\mathbb{C}$, the set of complex numbers.
- $\mathbb{S}^1 = \{z \in \mathbb{C} : |z| = 1\}$, the set of complex numbers of modulus 1
- $\mathbb{R}^*$, the set of non-zero real numbers.
- $\mathbb{R}_{>0}$, the set of positive real numbers.
- $\mathbb{C}^*$, the set of non-zero complex numbers.
- $GL_n(\mathbb{R})$, the set of $n \times n$ invertible matrices over $\mathbb{R}$.
- $SL_n(\mathbb{R})$, the set of $n \times n$ invertible matrices over $\mathbb{R}$ whose determinant is 1.

- A group is a non-empty set G together with a binary operation

$$\cdot : G \times G \longrightarrow G,$$

  we shall write $a \cdot b$ for $\cdot(a, b)$, such that the following conditions are satisfied:

  - $a \cdot (b \cdot c) = a \cdot (b \cdot c), \forall a, b, c \in G$, i.e., the binary operation on G is associative.

  - **Existence of identity**: There exist an element $e \in G$ such that $a \cdot e = a = e \cdot a, \forall a \in G$. Such an element in G is called the identity element of G.

  - **Existence of inverse**: For each element $a \in G$ there exists an element $b \in G$ such that $a \cdot b = e = b \cdot a$. Such an element b is called inverse of a.

- **Abelian group**: A group G is Abelian if $a \cdot b = b \cdot a, \forall a, b \in G$.

- $(\mathbb{Z}, +)$, the set of integers under the usual operation of addition '$+$' is a group.

- Let X be a non-empty set. Consider
$$S_X := \{f : X \longrightarrow X : f \text{ is a bijective function on } X\}$$
The set S_X together with the operation of Composition of functions forms a group, known as symmetric group on X. If $X = \{1, 2, \ldots, n\}$, then S_X is known as symmetric group on n symbols, and denoted by S_n.

- Consider $GL_n(\mathbb{R})$ the set of $n \times n$ invertible matrices over $\mathbb{R}$. Then $GL_n(\mathbb{R})$ together with the operation of matrix multiplication forms a group known as general linear group.

- Consider
$$U_n = \{e^{k\frac{2\pi\iota}{n}} : 0 \leq k \leq n-1\} \subset \mathbb{C}^*$$
the set of nth roots of unity. Then U_n together with the usual multiplication of complex numbers forms a group, known as group of nth roots of unity.

- Let G and G' be groups. A function $\psi : G \longrightarrow G'$ is called group homomorphism if ψ is compatible with group operations, i.e.,

$$\psi(ab) = \psi(a)\psi(b); \ \forall a, b \in G.$$

- If a group homomorphism $\psi : G \longrightarrow G'$ is bijective function, then we call homomorphism ψ an isomorphism and write $G \simeq G'$.

- Examples
  - Consider the map $\psi : (\mathbb{R}, +) \longrightarrow (S^1, \cdot)$ given by $\psi(t) = e^{\iota t}, \ t \in \mathbb{R}$.
  - Consider the map $\psi : (\mathbb{R}, +) \longrightarrow (\mathbb{R}_{>0}, \cdot)$ given by $\psi(t) = e^{t}, \ t \in \mathbb{R}$.
  - Consider the map $\psi : (\mathbb{Z}, +) \longrightarrow (U_n, \cdot)$ given by $\psi(k) = e^{\frac{k2\pi\iota}{n}}, \ k \in \mathbb{Z}$.
  - Consider the map $\psi : (GL_n(\mathbb{R}), \cdot) \longrightarrow (\mathbb{R}^*, \cdot)$ given by

$$\psi(A) = det(A), \ A \in GL_n(\mathbb{R}).$$

- Let $\psi : G \longrightarrow G'$ be a homomorphism. Then
  - $\psi(e) = e'$, e the identity of G and e' the identity of G'.
  - $\psi(a^{-1}) = \psi(a)^{-1}, \ a \in G$.
  - $Ker(\psi) = \{a \in G : \psi(a) = e'\}$ is a normal subgroup of G.
  - $Im(\psi)$ is a subgroup of G'.
  - ψ is monomorphism if and only if $Ker(\psi) = \{e\}$,

- **Group Action**: Let G be a group and X be a non-empty set. By an action of G on X, we mean a group homomorphism $\Phi : G \longrightarrow S_X$. In other words, there exist a function Φ which maps each element $g \in G$ to a bijective function $\Phi(g)$ on X such that $\Phi(g \cdot h) = \Phi(g)\Phi(h)$, for all $g, h \in G$.

- **Notation**: If a group G act on a set X through Φ, then for $g \in G$ and $x \in X$, we shall write gx for $\Phi(g)(x)$.

- With this notation, for $x \in X$, we see that $(gh)x = g(hx)$ for all $g, h \in G$ and $ex = x$, where e is the identity element of G.

- Let the group G act on a set X. Then to each $x \in X$, we associate a suset of X, denoted by Gx, as:

  $$Gx = \{gx : g \in G\}$$

  and, a subset of G, denoted by $G(x)$, as:

  $$G(x) = \{g \in G : gx = x\}.$$

  We call the subset $Gx \subset X$ the orbit of x, and $G(x) \subset G$ the stablizer of x.

Lemma

If a group G act on a set X, then for each $x \in X$, $G(x)$ the stablizer of x is a subgroup of G.

Lemma

If a group G act on a set X, then for $x, y \in X$, either $Gx \cap Gy = \emptyset$ or $Gx = Gy$.

Lemma (Orbit-Stablizer Formula)

If a group G act on a finite set X, then

$$|Gx| = [G : G(x)]$$

for each $x \in X$.

Lemma (Generalised Class Equation)

If a group G act on a finite set X, then

$$|X| = \sum [G : G(x)]$$

where the sum is taken over a set consisting of one representative of each orbit of G.

- Let G be a group and $X = G$. Define a map $\Phi : G \longrightarrow S_G$ given by sending
$$g \rightsquigarrow \Phi(g)$$
where $\Phi(g)(x) := g \cdot x$, for all $x \in G$, the left multiplication by g. Since the left multiplication by g to each element of G is a bijective function on G, we see that Φ is a function. Also, $\Phi(g \cdot h)(x) = (\Phi(g)\Phi(h))(x)$. Thus, G act on itself, and this action is known as action of G on itself by left translation.

- The above map Φ is a monomorphism.

Theorem (Cayley Theorem)

Let G be a group. Then G is isomorphic to a subgroup of symmetric S_G.

- Let H be a subgroup of a finite group G. Define a map $\Phi : H \longrightarrow S_G$ given by sending

$$h \rightsquigarrow \Phi(h)$$

where $\Phi(h)(x) := h \cdot x$, for all $x \in G$, the left multiplication by h. Since the left multiplication by h to each element of G is a bijective function on G, we see that Φ is a function. Also, $\Phi(g \cdot h)(x) = (\Phi(g)\Phi(h))(x)$. Thus, H act on G by left translation.

- For $x \in G$, the orbit of x under the above action is

$$Hx = \{hx : h \in H\}$$

the right coset of H in G.

- $|H| = |Hx|, \ \forall x \in G$.

Conjugate action of G on itself

- Let G be a group and $X = G$. Define a map $\Phi : G \longrightarrow S_G$ given by sending
$$g \rightsquigarrow \Phi(g)$$
where $\Phi(g)(x) := g \cdot x \cdot g^{-1}$, for all $x \in G$. Now, we see that $\Phi(g)$ is bijective function on G, for each $g \in G$, and $\Phi(g \cdot h)(x) = (g \cdot h) \cdot x \cdot (g \cdot h)^{-1} = (g \cdot h) \cdot x \cdot (h^{-1} \cdot g^{-1}) = g \cdot (h \cdot x \cdot h^{-1}) \cdot g^{-1} = \Phi(g)(\Phi(h)(x))$, which means that G act on itself, and this action is known as *conjugate action* of G on itself.

- Under above action, Orbit of x
$$Gx = \{gxg^{-1} : g \in G\}$$
known as conjugacy class of x, commonly denoted by $C(x)$.

- Stablizer of x
$$G(x) = \{gxg^{-1} = x : g \in G\}$$
also known as normalizer of x, commonly denoted by $N(x)$.

- $C(x) = \{x\}$ if and only if $x \in Z(G)$, the center of G.

Theorem (Cauchy)

Let p be a prime and G be a finite group such that p divides $|G|$. Then G has an element of order p, i.e., there exist $g \in G$ such that $g \neq e$ and $g^p = e$.

Consider

$$X = \{(g_0, g_1, \dots, g_{p-1}) : \ g_0 g_1 \dots g_{p-1} = e\} \subset G^p.$$

and action of $\mathbb{Z}/p\mathbb{Z}$ on X by left cyclic translation as

$$\bar{1} \cdot (g_0, g_1, \dots, g_{p-1}) = (g_1, g_2, \dots, g_{p-1}, g_0)$$

Theorem

Let p be a prime and G be a finite group such that p^n divides $|G|$, but p^{n+1} does not divides $|G|$. Then

1. *G has a subgroup H of order p^n. Such a subgroup is known as p-Sylow subgroup.*
2. *The p-Sylow subgroups of G are conjugate.*
3. *The number of p-Sylow subgroups of G is congruent to 1 modulo p and divides $|G|$.*

Theorem

Let G be a finite abelian group of order n and $n = p_1^{m_1} p_2^{m_2} \dots p_r^{m_r}$ is the prime factorization. Then

$$G \simeq G_1 \times G_2 \times \dots \times G_r$$

where G_i is an abelian group of order $p_i^{m_i}$ for $i = 1, 2, \dots, r$

Theorem

Let G be a finite abelian group of order p^n; p a prime. Then

$$G \simeq C_{p^{n_1}} \times C_{p^{n_2}} \times \ldots \times C_{p^{n_k}}$$

with $n_1 \geq n_2 \geq \ldots \geq n_k \geq 1$, $\sum_{i=1}^{k} n_i = n$ and $C_{p^{n_i}}$ is a cyclic group of order p^{n_i} for $i = 1, 2, \ldots, k$