Progressive Education Society's
Modern College of Arts, Science and Commerce(Autonomuous), Shivajinagar, Pune-5
M.Sc.(Mathematics) Part-I
Department of Mathematics
Subject: Group Theory
Prof.Smita Gajul

Chapter 4: Group Homomorphism and Isomorphism

Group Homomorphism:
Definition: A group homomorphism is a function ϕ from group G to $\bar{G}$ that preserves the group operation. that is $\phi(ab) = \phi(a)\phi(b)$ for all $a, b \in G$

Group Isomorphism:
Definition: A group isomorphism is a function ϕ from group G to $\bar{G}$ that is one- one, onto and that preserves the group operation. that is $\phi(ab) = \phi(a)\phi(b)$ for all $a, b \in G$
If there is an isomorhism from G and $\bar{G}$, we say that G and $\bar{G}$ are isomorphic. and we denote it by $G \approx \bar{G}$.

Example:
1. Let $\phi : R \to R^+$ defined by $\phi(x) = 2^x$
One-one: $\phi(x) = \phi(y) \Rightarrow 2^x = 2^y \Rightarrow \log 2^x = \log 2^y \Rightarrow x = y$. So ϕ is one-one.
Onto: For $y \in R^+$ we need to find $x \in R$ such that
$\phi(x) = y \Rightarrow 2^x = y \Rightarrow \log 2^x = \log y \Rightarrow x = \log_2 y$
So ϕ is onto.
Operation Preserving: $\phi(x + y) = 2^{x+y} = 2^x 2^y = \phi(x)\phi(y)$
So ϕ preserves operation.
Therefore ϕ is an isomorphism.

2. Let $\phi : R \to R$ defined by $\phi(x) = x^3$
One-one: $\phi(x) = \phi(y) \Rightarrow x^3 = y^3 \Rightarrow x = y$.
So ϕ is one-one.
Onto: For $y \in R$ we need to find $x \in R$ such that $\phi(x) = y$
$x^3 = y \Rightarrow x = y^{1/3}$.So ϕ is onto.
Operation Preserving: $\phi(x + y) = (x + y)^3 \neq x^3 + y^3 \Rightarrow \phi(x + y) \neq \phi(x) + \phi(y)$
Therefore ϕ is not an isomorphism.

Calyley's Theorem:
Statement: Every group is isomorphic to a group of permutation.
Proof: Let G be a group. we need to construct a permutation group from G.
For any $g \in G$ define a function $T_g : G \to G$ by $T_g(x) = gx$ for all $x \in G$
To prove: T_g is a permutation on the set of elements of G
One-one: Suppose that $T_g(x) = T_g(y) \Rightarrow gx = gy \Rightarrow x = y$
T_g is one-one.
Onto: For $y \in G$ we need to find out $x \in G$ such that $T_g(x) = y$
Consider $T_g(x) = y \Rightarrow gx = y$, multiply by g^{-1} on both side we get
$g^{-1}gx = g^{-1}y \Rightarrow x = g^{-1}y$ so there exists $x = g^{-1}y \in G$ such that $T_g(x) = y$.
T_g is a bijective function and so T_g is a permutation on the set of elements of G.

Let $\bar{G} = \{T_g | g \in G\}$
Since $\bar{G}$ is non-empty set as $e \in G$ so $T_e \in \bar{G}$.
Let $T_g, T_h \in \bar{G}$ so $g, h \in G$
Consider $T_g T_h(x) = T_g(T_h(x)) = T_g(hx) = g(hx) = (gh)(x) = T_{gh}(x)$ for all $x \in G$
$T_g T_h = T_{gh}$
Since set of bijective functions from G to G is associative w.r.t. Composition.
As $e \in G$ so $T_e \in \bar{G}$ such that $T_g T_e(x) = T_g(T_e(x)) = T_g(ex) = g(ex) = (ge)(x) = gx = T_g(x)$
so $T_g T_e = T_g$.
Let $T_g \in \bar{G}$ consider $T_g T_{g^{-1}}(x) = T_g(g^{-1}x) = g(g^{-1}(x)) = (gg^{-1})x = ex = T_e x$
So $T_g T_{g^{-1}} = T_e$
Therefore $\bar{G}$ is a group w.r.t. composition.
Now to prove $G \approx \bar{G}$
Define a function $\phi : G \to \bar{G}$ such $\phi(g) = T_g$
Supoose $\phi(g) = \phi(h) \Rightarrow T_g = T_h \Rightarrow T_g(e) = T_h(e) \Rightarrow ge = he \Rightarrow g = h$
ϕ is one-one.
Since for every $T_g \in \bar{G}$ we defined this for every $g \in G$ so ϕ is onto.
Now consider $\phi(ab) = T_{ab}$
$\phi(a)\phi(b) = T_a T_b$
$T_{ab}(x) = ab(x)$ and $T_a T_b(x) = T_a(bx) = a(bx) = ab(x)$
Therefore $T_{ab} = T_a T_b \Rightarrow \phi(ab) = \phi(a)\phi(b)$.
Therefore ϕ is isomorphism.
Hence G is isomorphic to $\bar{G}$.
So every group is isomorphic to its group of permutation.

Example:
Let $U(10) = \{1, 3, 7, 9\}$ and define the elements

$$T_1 = \begin{bmatrix} 1 & 3 & 7 & 9 \\ 1 & 3 & 7 & 9 \end{bmatrix}$$
$$T_3 = \begin{bmatrix} 1 & 3 & 7 & 9 \\ 3 & 9 & 1 & 7 \end{bmatrix}$$
$$T_7 = \begin{bmatrix} 1 & 3 & 7 & 9 \\ 7 & 1 & 9 & 3 \end{bmatrix}$$
$$T_9 = \begin{bmatrix} 1 & 3 & 7 & 9 \\ 9 & 7 & 3 & 1 \end{bmatrix}$$

There is one to one correspondence between $U(10)$ and $\{T_1, T_3, T_7, T_9\}$

Properties of Isomorphisms:
Suppose ϕ is an isomorphism from a group G to $\bar{G}$.Then

1. ϕ carries the identity of G to the identity of $\bar{G}$.
Proof: Let $\phi : G \to \bar{G}$ be an isomorphism.
Let e be an identity of G and $\bar{e}$ be an identity of $\bar{G}$.
As $e = ee$ apply ϕ on both side we get
$\phi(e) = \phi(ee) \Rightarrow \phi(e) = \phi(e)\phi(e) \Rightarrow \phi(e) = \bar{e}$

2. For every integer n and for any element a in G, $\phi(a^n) = [\phi(a)]^n$.
Proof: Consider $\phi(a^n) = \phi(a.a...a)$, $n-$ times
$\phi(a^n) = \phi(a)\phi(a)...\phi(a) \Rightarrow \phi(a^n) = [\phi(a)]^n$

3. For any element a and b in G, a and b commute if and only if $\phi(a)$ and $\phi(b)$ commute.
Proof: Let $a, b \in G$ such that $ab = ba$ apply ϕ on both side we get
$\phi(ab) = \phi(ba) \Rightarrow \phi(a)\phi(b) = \phi(b)\phi(a)$.

4. $G =< a >$ if and only if $\bar{G} =< \phi(a) >$.
Proof: Suppose $G =< a >$ so $a^k \in G \Rightarrow \phi(a^k) \in \bar{G} \Rightarrow [\phi(a)]^k \in \bar{G}$
but $[\phi(a)]^k \in < \phi(a) >$ so $< \phi(a) > \subset \bar{G}$
Now let $b \in \bar{G}$ since ϕ is onto so there exists an element say a^m in G
such that $\phi(a^m) = b \Rightarrow [\phi(a)]^m = b$ so $b \in < \phi(a) >$ therefore $\bar{G} \subset < \phi(a) >$.
Hence $\bar{G} =< \phi(a) >$.
Conversely, suppose $\bar{G} =< \phi(a) >$ as $\phi(a) \in \bar{G}$ so $a \in G$ because ϕ is onto.
But $a \in < a >$ so $< a > \subset G$
Now let $b \in G$ so we have $\phi(b) \in \bar{G} =< \phi(a) >$
so for some integer k we have $\phi(b) = [\phi(a)]^k \Rightarrow \phi(b) = \phi(a^k)$
As ϕ is one-one so $b = a^k$ so $b \in < a >$ therefore $G \subset < a >$
Hence $G =< a >$.

5. $|a| = |\phi(a)|$ for all $a \in G$
Proof: Let $|a| = n$ so $a^n = e$ apply ϕ on both side we get
$\phi(a^n) = \phi(e) \Rightarrow [\phi(a)]^n = \bar{e}$ So n divides the $|\phi(a)|$
Let $|\phi(a)| = k \Rightarrow [\phi(a)]^k = \bar{e} \Rightarrow \phi(a^k) = \phi(e)$ as ϕ is one-one $a^k = e$
$\Rightarrow k$ divides n that is $|\phi(a)|$ divides n.
Therefore $n = k$ that is $|\phi(a)| = |a|$.

6. For a fixed integer k and a fixed group element $b \in G$, the equation $x^k = b$
has the same number of solutions in G as does the equation $y^k = \phi(b)$ in $\bar{G}$.
Proof: Consider the equation $x^k = b$,
suppose this equation have n solutions say $a_1, a_2, ...a_n$
so we have $(a_i)^k = b$ for all $a_i, i = 1, 2, ...n$
so $\phi(a_i^k) = \phi(b) \Rightarrow [\phi(a_i)]^k = \phi(b)$ for all $a_i, i = 1, 2, ...n$
so we have n number of solutions for $y^k = \phi(b)$
If suppose c is another solution of $y^k = \phi(b)$ that is $c^k = \phi(b)$
since $c = \phi(a)$ so $[\phi(a)]^k = \phi(b) \Rightarrow \phi(a^k) = \phi(b) \Rightarrow a^k = b$
so a is also solution of $x^k = b$ but this equation have n solutions only
so the equation $x^k = b$ has the same number of solutions in G as does
the equation $y^k = \phi(b)$ in $\bar{G}$.

7. If G is finite, then G and $\bar{G}$ have exactly same number of elements of every order.
Proof: Since $|a| = |\phi(a)|$ for all $a \in G$ so
G and $\bar{G}$ have exactly same number of elements of every order.

Properties of Isomorphism acting on subgroups:
Suppose that ϕ is an isomorphism from a group G onto a group $\bar{G}$. Then
1. ϕ^{-1} is an isomorphism from $\bar{G}$ onto G.
Proof: Let $\phi : G \to \bar{G}$ be an isomorphism.
Consider $\phi^{-1} : \bar{G} \to G$
Since ϕ is one-one so $\phi(a) = \phi(b) \Rightarrow a = b$
So consider $\phi^{-1}(a) = \phi^{-1}(b) \Rightarrow \phi(\phi^{-1}(a)) = \phi(\phi^{-1}(b))$
$\Rightarrow (\phi \circ \phi^{-1})(a) = (\phi \circ \phi^{-1})(b) \Rightarrow a = b$.
ϕ^{-1} is one-one.
Since ϕ is onto so for every element $y \in \bar{G}$ there exists and element $x \in G$
such that $\phi(x) = y \Rightarrow x = \phi^{-1}(y)$ so for every $x \in G$
there exist $y \in G$ such that $x = \phi^{-1}(y)$
Since $\phi(ab) = \phi(a)\phi(b)$,
Consider $\phi^{-1}(\phi(a)\phi(b)) = \phi^{-1}(\phi(ab)) = ab = \phi^{-1}(\phi(a))\phi^{-1}(\phi(b))$.
ϕ^{-1} preserves operation.
Therefore ϕ^{-1} is an isomorphism.

2. G is abelian if and only if $\bar{G}$ is abelian.
Proof: Suppose G is abelian so $ab = ba$ for all $a, b \in G$
then $\phi(ab) = \phi(ba) \Rightarrow \phi(a)\phi(b) = \phi(b)\phi(a) \Rightarrow \bar{G}$ is abelian.
Similarly Suppose $\bar{G}$ is abelian so $\phi(a)\phi(b) = \phi(b)\phi(a)$, for all $\phi(a), \phi(b) \in \bar{G}$.
So $\phi(ab) = \phi(ba) \Rightarrow ab = ba \Rightarrow \bar{G}$ is abelian.

3. G is cyclic if and only if $\bar{G}$ is cyclic.
Since $G =< a >$ if and only if $\bar{G} =< \phi(a) >$ so G is cyclic if and only if $\bar{G}$ is cyclic.

4. If K is a subgroup of G, then $\phi(K) = \{\phi(k) | k \in K\}$ is a subgroup of $\bar{G}$.
Proof: Let K be a subgroup of G and consider $\phi(K) = \{\phi(k) | k \in K\}$.
Let $\phi(k)$ and $\phi(h) \in \phi(K)$, $\phi(k)\phi(h) = \phi(kh) \in \phi(K)$ as $k.h \in K$
and $(\phi k)^{-1} = \phi(k^{-1}) \in \phi(K)$ as $k^{-1} \in K$.
Therefore $\phi(K)$ is a subgroup of $\bar{G}$.

Automorphism: An isomorphism from a group G to itself is called an automorphism of G.

Example: Let $\phi : \mathbf{C} \to \mathbf{C}$ defined by $\phi(a + bi) = a - bi$
One-one: Suppose $\phi(a + bi) = \phi(c + di) \Rightarrow a - bi = c - di \Rightarrow a = c, b = d$
So $a + bi = c + di \Rightarrow \phi$ is one-one.
Onto: For $a + bi \in C$ there exists $a - bi \in C$ such that $\phi(a - bi) = a + bi$
Operation Preserving:
Suppose $\phi[(a+bi)+(c+di)] = \phi[(a+c)+(b+d)i] = (a+c)-(b+d)i = (a-bi)+(c+di) = \phi(a+bi)+\phi(c+di)$
Similarly $\phi[(a + bi)(c + di)] = \phi(a + bi)\phi(c + di)$.
Therefore ϕ is an isomorphism from C to C so ϕ is an automorphism.

Inner Automorphism induced by a
Let G be a group, and let $a \in G$. The function ϕ_a defined by $\phi_a(x) = axa^{-1}$ for all $x \in G$ is called the inner automorphism of G induced by a.

Theorem: The set of automorphisms of a group and the set of inner automorphisms of a group are both groups under the operation.
Proof: Let G be a group and $A = \{\phi \mid \phi : G \to G\}$ where ϕ is an isomorphism.
So A is set of automorphisms of group G.
Let $\phi, \psi \in A$ So $\phi \circ \psi : G \to G$ and composition of two isomorphism is an isomorphism so $\phi \circ \psi \in A$
Associativity holds in A.
Since $I : G \to G$ be an identity map which is isomorphism and $\phi \circ I = \phi = I \circ \phi$.
So identity element exist in A.
For $\phi \in A, \phi^{-1} \in A$ such that $\phi \circ \phi^{-1} = I$ so inverse exists for all elements in A.
Therefore A is a group with respect to composition.
Similarly Set of inner automorphisms are group with respect to composition.

Theorem: For every positive integer n, $Aut(Z_n)$ is isomorphic to $U(n)$.
Proof: Define a map $T : Aut(Z_n) \to U(n)$ by $T(\alpha) = \alpha(1)$
To show that: $Aut(Z_n) \approx U(n)$.
One-one: Suppose $T(\alpha) = T(\beta) \Rightarrow \alpha(1) = \beta(1)$
multiply by k on both side we get $k\alpha(1) = k\beta(1) \Rightarrow \alpha(k) = \beta(k) \ \ \forall \ \ k \in Z_n \Rightarrow \alpha = \beta$.
Therefore T is one-one.
Onto: Let $r \in U(n)$ and consider the mapping $\alpha : Z_n \to Z_n$
defined by $\alpha(s) = rs(modn)$ for all $s \in Z_n$.
To prove α is automorphism.
Suppose $\alpha(s) = \alpha(t) \Rightarrow sr(modn) = tr(modn) \Rightarrow s \equiv t(modn) \Rightarrow s = t$ in Z_n,
therefore α is one-one.
Let $y \in Z_n$ we need to find $x \in Z_n$ such that $\alpha(x) = y \Rightarrow rx(modn) = y \Rightarrow x = r^{-1}y(modn)$,
therefore α is onto.
Operation Preserving: Now consider $\alpha(s + t) = (s + t)r(modn) \Rightarrow$
$\alpha(s + t) = sr(modn) + tr(modn) \Rightarrow \alpha(s + t) = \alpha(s) + \alpha(t)$.
Therefore α is an isomorphism from Z_n to Z_n so α is an automorphism.
Since $T(\alpha) = \alpha(1) = r$, So T is onto.
Let $\alpha, \beta \in Aut(Z_n)$, consider $T(\alpha\beta) = (\alpha\beta)(1) = \alpha(\beta(1)) = \alpha(1 + 1 + ... + 1)$, $\beta(1)$ times
$T(\alpha\beta) = \alpha(1) + \alpha(1) + ... + \alpha(1) = \alpha(1)\beta(1) = T(\alpha)T(\beta)$.

Coset of H in G:
Let G be a group and H be a subset of G, for any $a \in G$ the set
$aH = \{ah | h \in H\}$ is called the left coset of H in G containing a
and $Ha = \{ha | h \in H\}$ is called right coset of H in G containing a.
The element a is called coset representative of aH or Ha
$|aH|$ denote the number of elements in the set aH.
$|Ha|$ denote the number of elements in the set Ha.

Example:

1. Let $H = \{0, 1, 2\}$ in Z_6
Cosets of H in Z_6 are
$0 + H = \{0, 1, 2\}$, $1 + H = \{1, 2, 3\}$, $2 + H = \{2, 3, 4\}$,
$3 + H = \{3, 4, 0\}$, $4 + H = \{4, 5, 0\}$, $5 + H = \{5, 0, 1\}$

2. Let $U(12) = \{1, 5, 7, 11\}$ and $H = \{1, 11\}$
Cosets of H in $U(10)$ are
$1H = \{1, 11\}$, $5H = \{5, 7\}$, $7H = \{7, 5\}$, $11H = \{11, 1\}$.

Properties of Cosets:

Let H be a subgroup of G and let $a, b \in G$. Then
1. $a \in aH$
Proof: Let H be a subgroup of G, and $a \in H$
So $aH = \{ah | h \in H\}$
Since $e \in H$ so $a = ae \in aH$.
2. $aH = H$ if and only if $a \in H$.
Proof: Suppose $aH = H$, Since $a \in aH \Rightarrow a \in H$
Conversely, suppose $a \in H$
To prove: $aH = H$ that is $aH \subset H$ and $H \subset aH$
Since $a \in aH \Rightarrow aH \subset H$.
Let $h \in H$ and since $a \in H \Rightarrow a^{-1} \in H$ as H is a subgroup so $a^{-1}h \in H$,
so $h = eh = (aa^{-1})h = a(a^{-1}h) \in H$.

3. $aH = bH$ if and only if $a \in bH$.
Proof: Suppose $aH = bH$, To show: $a \in bH$
Since $a = ae \in aH$ and $aH = bH$ so $a \in bH$.
Conversely suppose $a \in bH$, To prove $aH = bH$,
As $a \in bH \Rightarrow a = bh$ for $h \in H$ but $a \in aH$ so $aH \subset bH$
Now $a = bh \Rightarrow b = ah^{-1} \in aH$ but $b \in bH$ so $bH \subset aH$.
Therefore $aH = bH$.

4. $aH = bH$ or $aH \cap bH = \phi$.
Proof: If $aH \cap bH \neq \phi \Rightarrow c \in aH \cap bH$ for some $c \in G$,
then $c \in aH \Rightarrow cH = aH$ and $c \in bH \Rightarrow cH = bH$
so we have $aH = bH$.

5. $aH = bH$ if and only if $a^{-1}b \in H$.
Proof: Suppose $aH = bH$, To prove $a^{-1}b \in H$
Since $b \in bH \Rightarrow b \in aH \Rightarrow b = ah$ for some $h \in H$,
so $h = a^{-1}b$ as $h \in H$ so $a^{-1}b \in H$.
Suppose $a^{-1}b \in H \Rightarrow a^{-1}b = h \Rightarrow b = ah \Rightarrow b \in aH$ So $bH = aH$.

6. $|aH| = |bH|$
Proof: To prove: $|aH| = |bH|$,
It is sufficient to prove that there is one to one correspondence between aH and bH.
Let $\phi : aH \to bH$ by $\phi(ah) = bh$
Suppose $\phi(ah) = \phi(ah') \Rightarrow bh = bh' \Rightarrow h = h' \Rightarrow ah = ah'$
So ϕ is one-one. Therefore $|aH| = |bH|$.

7. $aH = Ha$ if and only if $H = aHa^{-1}$
Proof: Suppose $aH = Ha$, to prove: $H = aHa^{-1}$
Suppose $aH = Ha \Rightarrow aH \subset Ha$ and $Ha \subset aH$
we have $ah = h'a \Rightarrow h' = aha^{-1}$ but $h' \in H$ so $H \subset aHa^{-1}$.
Also $aha^{-1} \in aHa^{-1}$ so $aHa^{-1} \subset H$.
Conversely suppose $H = aHa^{-1}$ so $H \subset aHa^{-1}$ and $aHa^{-1} \subset H$
we have $h = ah'a^{-1} \Rightarrow ha = ah' \Rightarrow Ha = aH$.

8. aH is a subgroup of G if and only if $a \in H$.
Proof: Suppose aH is a subgroup of G, so $e \in aH$
therefore $aH \cap eH \neq \phi \Rightarrow aH = eH = H$ as $a \in aH \Rightarrow a \in H$.
Conversely suppose $a \in H \Rightarrow aH = H$
therefore aH is a subgroup as H is a subgroup of G.

Lagranges Theorem: If G is a finite group and H is a subgroup of G, then $|H|$ divides $|G|$. Moreover the number of left cosets of H in G is $|G|/|H|$.
Proof: Let G be a finite group and H be a subgroup of G
Suppose $a_1H, a_2H, ..., a_rH$ be distinct cosets of H in G.
Then for each $a \in G$, $aH = a_iH$ for some i.
Since $a \in aH$ so every element of G is an elements of one of the cosets a_iH,
then we can write
$G = a_1H \cup a_2H \cup ...a_rH$
Since all are distinct cosets so $a_iH \cap a_jH = \phi$ for all i, j
Then $|G| = |a_1H| + |a_2H| + ... + |a_rH|$, Since $|a_iH| = |H|$ for all i
so $|G| = |H| + |H| + ... + |H|$, r times
$|G| = r|H| \Rightarrow |H|$ divides $|G|$.
And $r = |G|/|H|$ and there are r number of left cosets
Therefore the number of left cosets of H in G is $|G|/|H|$.

Index of a subgroup: The index of a subgroup H in G is the number of left cosets of H in G.
Notation: $|G : H|$

Corollary: If G is a finite group and H is a subgroup of G, then $|G : H| = |G|/|H|$.
Proof: Let G be a group and H be a subgroup. As $|G : H|$ is number of left cosets of H in G and by Lagranges theorem number of left cosets is equal to $|G|/|H|$.
Therefore $|G : H| = |G|/|H|$.

Corollary: In a finite group, the order of each element of the group divides the order of group.
Proof: Since order of an element is the order of subgroup generated by that element and by Lagranges theorem order of subgroup divides order of group, therefore order of element divides order of group.

Corollary: A group of prime order is cyclic.
Proof: Let G be a group such that $|G| = p$, where p is prime
Let $a \in G$ and $a \neq e$ then $| < a > |$ divides $|G|$ here $| < a > | \neq 1$,
so $| < a > | = p$ that is $| < a > | = |G|$ so G is generated by an element of G.
Therefore G is cyclic.

Corollary: Let G be a finite group, and let $a \in G$. Then $a^{|G|} = e$.
Proof: Let G be a finite group and $a \in G$. Since $|a|$ divides $|G|$,
so we have $|G| = |a|k$, therefore $a^{|G|} = a^{|a|k} = a^{|a|}k = e^k = e$.

Fermat's Theorem: For every integer a and every prime p, $a^p(mod)p = a(mod)p$.
Proof: Let a be an integer and p be a prime, by division algorithm there exists q, r such that $a = pq + r$, where $0 \leq r < p$.
Here if we take modulo p, we have $a(mod)p = r$
so it is sufficient to prove that $r^p(mod)p = r$.
If $r = 0$ then result is trivial, as $r^p = 0^p = 0$.
Suppose $r \neq 0$, so $r \in U(p)$ since $|U(p)| = p - 1$
so we have $r^{|U(p)|} = e \Rightarrow r^{p-1} = 1 \Rightarrow r^p = r$
we can write this as $r^p(mod)p = r$.
Therefore $a^p(mod)p = a(mod)p$.

An application of cosets to permutation groups

Stabilizer of a Point: Let G be a group of permuations of a set S. For each i in S, the stabilizer of i in G is the set $stab_G(i) = \{\phi \in G | \phi(i) = i\}$

Note: Stabilizer of i in G is a subgroup of G.
Proof: Consider $stab_G(i) = \{\phi \in G | \phi(i) = i\}$
Let $\phi, \psi \in stab_G(i)$ so that $\phi(i) = i$ and $\psi(i) = i$, now $\phi(\psi(i)) = \phi(i) = i$ therefore $\phi\psi \in stab_G(i)$ so $stab_G(i)$ is closed w.r.t. composition. Associativity holds. Since identity function is in $stab_G(i)$ as $I(i) = i$ so identity element exists. Also for $\phi \in stab_G(i)$ there exists $\phi^{-1} \in stab_G(i)$ such that $\phi(i) = i \Rightarrow \phi^{-1}(i) = i$.

Orbit of a Point: Let G be a group of permutation of a set S. For each $s \in S$, the orbit of s in G is $orb_G(s) = \{\phi(s) | \phi \in G\}$.

For example: Let $G = \{(1), (132)(465)(78), (132)(465), (123)(456), (123)(456)(78), (78)\}$
$orb_G(1) = \{1, 3, 2\}$, $orb_G(2) = \{2, 1, 3\}$,
$orb_G(4) = \{4, 6, 5\}$, $orb_G(7) = \{7, 8\}\}$,

$stab_G(1) = \{(1), (78)\}$, $stab_G(2) = \{(1), (78)\}$,
$stab_G(4) = \{(1), (78)\}$, $stab_G(7) = \{(1), (132)(465), (123)(456)\}$

Orbit-Stabilizer Theorem:
Let G be a finite group of permutation of a set. Then for any i from S,
$|G| = |orb_G(i)||stab_G(i)|$.
Proof: Let G be a group and $stab_G(i)$ is a subgroup of G
so by Lagrange's theorem $|G|/|stab_G(i)|$ is the number of left cosets of $stab_G(i)$ in G.
To prove $|G| = |orb_G(i)||stab_G(i)|$ that is $|G|/|stab_G(i)| = |orb_G(i)|$
so it is sufficient to prove that there is one to one correspondence between
left cosets of $stab_G(i)$ and $orb_G(i)$.
Let A =Left cosets of $stab_G(i) = \{\phi stab_G(i) | \phi \in G\}$
Define a map $T : A \to orb_G(i)$ by $T(\phi stab_G(i)) = \phi(i)$
To show T is one-one: Suppose $T(\phi stab_G(i)) = T(\psi stab_G(i))$
$\Rightarrow \phi(i) = \psi(i) \Rightarrow \psi^{-1}\phi(i) = i \Rightarrow \psi^{-1}\phi \in stab_G(i) \Rightarrow \psi stab_G(i) = \phi stab_G(i)$.
Therefore T is one-one.
To show T is onto: Let $j \in orb_G(i) \Rightarrow \phi(i) = j$ for some $\phi \in G$
Then $T(\phi stab_G(i)) = \phi(i) = j$. Therefore T is onto.
Hence there is one-to-one correspondence between left cosets of $stab_G(i)$ and $orb_G(i)$
so $|G|/|stab_G(i)| = |orb_G(i)|$ that is $|G| = |orb_G(i)||stab_G(i)|$.