Group

A nonempty set G with binary operation $*$ is called group if the binary operation $*$ is associative and

1) for all $a \in G$, $\exists\ e \in G$ s.t. $a * e = e * a = a$

2) For each $a \in G$, $\exists\ a^{-1} \in G$ s.t. $a * a^{-1} = a^{-1} * a = e$.

AKHTAR ABBAS
Lecturer (Mathematics)
Govt. Degree College
Shah Jewna (Jhang)

Examples

1). $(\mathbb{Z}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, $(\mathbb{Q}, +)$
$(\mathbb{R}^*, \cdot)$, $(\mathbb{C}^*, \cdot)$, $(\mathbb{Q}^*, \cdot)$.

2). $(\mathbb{Q}^+, \cdot)$, $(\{1, -1, i, -i\}, \cdot)$, $(\{1, \omega, \omega^2\}, \cdot)$.

3). Set $M(2, \mathbb{R}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a, b, c, d \in \mathbb{R} \right\}$.
Then $(M(2, \mathbb{R}), +)$ is group.

4). Set $GL(2, \mathbb{R}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a, b, c, d \in \mathbb{R} \wedge ad - bc \neq 0 \right\}$.
Then $(GL(2, \mathbb{R}), \cdot)$ is group.

5). Set $SL(2, \mathbb{R}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a, b, c, d \in \mathbb{R} \wedge ad - bc = 1 \right\}$
Then $(SL(2, \mathbb{R}), \cdot)$ is a group.

6) $\mathbb{Z}_n = \{0, 1, 2, \cdots, n-1\}$ is a group under addition modulo n.

7) $U(n) = \{ j \in \mathbb{Z}_n : (j, n) = 1 \}$ is a group under multiplication modulo n.

i.e., $U(10) = \{1, 3, 7, 9\}$ is group under multiplication modulo 10.

$\odot_{10}$	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

8). The set of complex nth roots of unity

$$\left\{ \cos\left(\frac{2k\pi}{n}\right) + i\sin\left(\frac{2k\pi}{n}\right) : k = 0, 1, 2, \dots, n-1 \right\}$$

is a group under multiplication.

9). The set $\mathbb{R}^n = \{(a_1, a_2, \dots, a_n) \mid a_i \in \mathbb{R}\}$

is a group under componentwise addition.

Properties of Groups:-

1). In a group G, there is only one identity element.

2). In a group G, the inverse of an element is unique.

3). For group elements a, b, $(ab)^{-1} = b^{-1}a^{-1}$.

Order of a Group:-

The number of elements in a group G is called order of G, denoted by $|G|$.

Order of an element:-

The order of an element $g \in G$ is the smallest positive integer n such that $g^n = e$.

Example: Consider $U(15) = \{1, 2, 4, 7, 8, 11, 13, 14\}$ under multiplication modulo 15. The order of group is 8. Order of each element can be found as

$|1| = 1$

$2^1 = 2, \quad 2^2 = 4, \quad 2^3 = 8, \quad 2^4 = 16 = 1$

$\Rightarrow \quad |2| = 4$

$4^1 = 4, \quad 4^2 = 16 = 1$

$\Rightarrow \quad |4| = 2$

$7^1 = 7, \quad 7^2 = 49 = 4, \quad 7^3 = 7 \cdot 7^2 = 7 \cdot 4 = 28 = 13$

$7^4 = 7 \cdot 7^3 = 7 \cdot 13 = 91 = 1$

$\Rightarrow \quad |7| = 4$

Similarly $|8| = 4, \ |11| = 2, \ |13| = 4, \ |14| = 2.$

Example: Every nonzero element of $\mathbb{Z}$ has infinite order.

Subgroup: A subset H of a group G is subgroup if for any $a, b \in H$, $ab^{-1} \in H$. (In case of addition $a - b \in H$). We denote as $H \leq G$.

Example: Let G be an Abelian group. Then

$$H = \{x \in G : x^2 = e\} \leq G.$$

Example: Let G be an Abelian group and $H, K \leq G$. Then $HK = \{hk : h \in H, k \in K\} \leq G$.

Theorem: Let $H, K \leq G$. Then $HK \leq G$ if and only if $HK = KH$.

Cyclic subgroup generated by single element.

Let $a \in G$, we define a subgroup of G generated by a as

$$\langle a \rangle = \{ a^n : n \in \mathbb{Z} \}$$

If G is group under addition, then

$$\langle a \rangle = \{ na : n \in \mathbb{Z} \}.$$

Example

1) In $U(10)$, $\langle 3 \rangle = \{3, 9, 7, 1\} = U(10)$.

2) In $\mathbb{Z}_{10}$, $\langle 2 \rangle = \{0, 2, 4, 6, 8\}$.

3) In $\mathbb{Z}$, $\langle 1 \rangle = \langle -1 \rangle = \mathbb{Z}$.

Center of a group:-

The center of a group G is defined as

$$Z(G) = \{ a \in G : ga = ag, \ \forall \ g \in G \}$$

$$\boxed{Z(G) \le G}.$$

If G is Abelian, then $Z(G) = G$.

Group G is called centerless if $Z(G) = \{e\}$.

Example:

The center of the quaternion group

$$Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$$

is $\{1, -1\}$.

AKHTAR ABBAS
Lecturer (Mathematics)
Govt Degree College
Shah Jewna (Jhang)

Centralizer of an element:- (Normalizer of an element).

The centralizer of an element $a \in G$ is

$$C(a) = \{g \in G : ga = ag\}.$$

$$\boxed{C(a) \leq G}$$

Centralizer of a subgroup

The centralizer of a subgroup H of G is

$$C(H) = \{g \in G : gh = hg, \ \forall \ h \in H\}.$$

$$\boxed{C(H) \leq G}$$

Normalizer of a subgroup

The normalizer of a subgroup H of G is

$$N(H) = \{g \in G : gH = Hg\}$$

$$\boxed{N(H) \leq G}.$$

AKHTAR ABBAS
Lecturer (Mathematics)
Govt Degree College
Shah Jewna (Jhang)

Remark

1). $C(H) \leq N(H)$.

2). $H \nsubseteq C(H)$ but $H \subseteq C(C(H))$.

3). For any two subsets (subgroups) H and K of G

$$H \subseteq C(K) \iff K \subseteq C(H).$$

4). If G is Abelian, then $C(G) = Z(G) = G$.

5). G is Abelian iff $C(a) = G \quad \forall \ a \in G$.

6). $Z(G) = \bigcap_{a \in G} C(a)$. (7). $C(a) = C(a^{-1})$.

Question Let $G = GL(2, \mathbb{R})$.

(a) Find $C\left(\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}\right)$

(b) Find $C\left(\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\right)$

(c) Find $Z(G)$.

Cyclic Groups

A group G is called cyclic if $G = \langle a \rangle$ for some $a \in G$.

Examples

1) $\mathbb{Z}$ is cyclic. 1 and -1 are generators.

2). $\mathbb{Z}_n$ is cyclic. 1 is a generator.

3). $\mathbb{Z}_8 = \langle 1 \rangle = \langle 3 \rangle = \langle 5 \rangle = \langle 7 \rangle$.

$\boxed{\text{In general } \mathbb{Z}_n = \langle k \rangle \text{ where } (k, n) = 1.}$

4). $U(10) = \langle 3 \rangle = \langle 7 \rangle$.

5). $U(8)$ is noncyclic.

$\boxed{\text{For what } n,\ U(n) \text{ is cyclic ?}}$ (Not concentrate more than 2 minutes).

Criterion for $a^i = a^j$.

Let G be a group and $a \in G$.
If $|a|$ is infinite, then $a^i = a^j \Leftrightarrow i = j$.
If $|a|$ is finite, say $|a| = n$, then $a^i = a^j \Leftrightarrow n \mid (i-j)$.

<u>Results</u>

1). $|a| = |\langle a \rangle|$

2). $a^k = e \Rightarrow |a| \mid k$.

3). If $|a| = n$, then $\langle a^k \rangle = \langle a^{\gcd(n,k)} \rangle$ and $|a^k| = \dfrac{n}{\gcd(n,k)}$.

4). If $|a| = n$, then $|a^i| = |a^j|$ if and only if $\gcd(n,i) = \gcd(n,j)$.

5). If $|a| = n$, then $\langle a \rangle = \langle a^j \rangle \Leftrightarrow \gcd(n,j) = 1$.

6). Every subgroup of a cyclic group is cyclic.

7). If $|\langle a \rangle| = n$, then for each positive divisor k of n, $\langle a^{n/k} \rangle$ is unique subgroup of order k.

(Discuss $\mathbb{Z}_{30}$ as an example).

8). For each positive divisor k of n, the set $\langle \frac{n}{k} \rangle$ is the unique subgroup of $\mathbb{Z}_n$ of order k.

AKHTAR ABBAS
Lecturer (Mathematics)
Govt. Degree College
Shah Jewna (Jhang)

<u>Euler phi function</u>:-

Let $\phi(1) = 1$ and for any integer > 1, we define $\phi(n)$ as the number of positive integers less than n and relatively prime to n.

i.e. $\phi(n) = \left| \{ j \in \mathbb{Z}_n : \gcd(n,j) = 1 \} \right| = |U(n)|$.

For a prime p, $\phi(p^n) = p^n - p^{n-1}$.

Theorem:- Let G be a group of order n. If $d|n$, then there are $\phi(d)$ elements of order d.

i.e., $\mathbb{Z}_8$, $\mathbb{Z}_{640}$ and $\mathbb{Z}_{80000}$ each have $\phi(8)=4$ elements of order 8.

Theorem:-

In a finite group, the number of elements of order d is a multiple of $\phi(d)$.

Properties of $\phi(n)$.

1)- For a prime p, $\phi(p) = p-1$.

2)- For a prime p, $\phi(p^n) = p^n - p^{n-1}$.

3)- If m and n are relatively prime, then

$$\phi(mn) = \phi(m)\,\phi(n).$$

4)- $\phi(n) = n \prod_{p|n}\left(1-\frac{1}{p}\right)$, where p is prime.

(or)

5)- If $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ where $p_1 < p_2 < \cdots < p_r$ are prime numbers and each $k_i \geq 1$, then

$$\phi(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_r}\right).$$

6)- $$\sum_{d|n} \phi(d) = n$$

where the sum is over all positive divisors d of n.

Permutation Groups

A permutation of a set A is a bijective function from A to A.

A permutation group of A is the collection of all permutations of A that forms a group under function composition.

For example, we define a permutation α of the set $\{1,2,3,4\}$ by

$$\alpha(1)=2, \quad \alpha(2)=3, \quad \alpha(3)=1, \quad \alpha(4)=4.$$

A convenient way is

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$$

AKHTAR ABBAS
Lecturer (Mathematics)
Govt Degree College
S. u Jewna (Jhang)

Consider $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 5 & 1 \end{pmatrix}$

and $\gamma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 2 & 3 \end{pmatrix}$

then
$$\sigma\gamma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 5 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 2 & 3 \end{pmatrix}$$
$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 2 & 4 & 3 \end{pmatrix}$$

and
$$\gamma\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 2 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 5 & 1 \end{pmatrix}$$
$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 1 & 3 & 5 \end{pmatrix}$$

Here $\sigma\gamma \neq \gamma\sigma$.

Symmetric Group S_3 :-

Let S_3 denote the permutations of $\{1,2,3\}$. Then S_3, under function composition, is a group with six elements. The six elements are

$$\varepsilon = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \alpha^2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix},$$

$$\beta = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad \alpha\beta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \quad \alpha^2\beta = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

Here $\alpha\beta \neq \beta\alpha$, so that S_3 is non-Abelian.

Symmetric Group S_n :-

Let $A = \{1, 2, \dots, n\}$. The set of all permutations of A is called the symmetric group of degree n and order $n!$. This group is denoted by S_n.

S_n is non-Abelian when $n \geq 3$.

The group S_4 has 30 and S_5 has 100 subgroups.

Cycle Notation

An expression of the form $(a_1, a_2, \dots, a_m)$ where

$$(a_1, a_2, \dots, a_m) = \begin{pmatrix} a_1 & a_2 & \cdots & a_m \\ a_2 & a_3 & \cdots & a_1 \end{pmatrix}$$

is called a cycle of length m or an m-cycle. This can also be written as

$$(a_1\ a_2\ \dots\ a_m) = (a_2\ a_3 \dots a_m\ a_1)$$
$$= (a_3\ a_4\ \dots\ a_m\ a_1\ a_2)$$

and so on.

A cycle of length 2 is called a transposition.

Consider the permutation $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 4 & 6 & 5 & 3 \end{pmatrix}$.
In cycle notation, we write $\alpha = (1\ 2)(3\ 4\ 6)(5)$
or simply $\alpha = (12)(3\ 4\ 6)$.

Theorem:-

1) Every permutation of a finite set can be written as a cycle or as a product of disjoint cycles.

2). If the pair of cycles $\alpha = (a_1\, a_2 \cdots a_m)$ and $\beta = (b_1\, b_2 \cdots b_n)$ have no entries in common, then $\alpha\beta = \beta\alpha$.
(Disjoint cycles commute).

3). The order of a permutation on a finite set written is disjoint cycle form is the least common multiple of the lengths of the cycles.

4). The order of a k-cycle is k.

For example $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 1 & 7 & 6 & 4 & 5 & 3 \end{pmatrix}$

Then $\alpha = (1\ 2)(3\ 7)(4\ 6\ 5)$

and $|\alpha| = \text{lcm}(2, 2, 3) = 6$

AKHTAR ABBAS
Lecturer (Mathematics)
Govt Degree College
Shah Jewna (Jhang)

5). Every permutation in S_n, $n>1$, is a product of 2-cycles. For example $(1632)(457) = (12)(13)(16)(47)(45)$.

6). If $\varepsilon = \beta_1 \beta_2 \cdots \beta_r$, where the β's are 2-cycles, then r is even.

7). If $\alpha = \beta_1 \beta_2 \cdots \beta_r = \gamma_1 \gamma_2 \cdots \gamma_s$, where the β's and γ's are 2-cycles, then r and s are both even or both odd.

Even and Odd Permutations:-

A permutation that can be expressed as a product of an even (odd) number of 2-cycles is called an even (odd) permutation.

Alternating group of Degree n:-

The set of even permutations in S_n forms a subgroup of S_n, called the alternating group of degree n, denoted as A_n and $|A_n| = \frac{n!}{2}$.

Example:-

$$S_3 = \{1, \alpha, \alpha^2, \beta, \alpha\beta, \alpha^2\beta\}$$

$$= \left\{\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}, \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}, \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}, \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}, \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}, \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}\right\}$$

In cycle notations

$$S_3 = \{\varepsilon, (1\,2\,3), (1\,3\,2), (2\,3), (1\,2), (1\,3)\}$$

AKHTAR ABBAS
Lecturer (Mathematics)
Govt Degree College
Shah Jewna (Jhang)

$$= \{\varepsilon, (1\,3)(1\,2), (1\,2)(1\,3), (2\,3), (1\,2), (1\,3)\}$$

$\Rightarrow$ order of each non-identity element is 2 or 3.

$$A_n = \{\varepsilon, (1\,2\,3), (1\,3\,2)\}$$

Conjugate Permutations:- Let $\alpha, \beta \in S_n$. Then α and β are called conjugate if there exists $\gamma \in S_n$ such that

$$\gamma \circ \alpha \circ \gamma^{-1} = \beta.$$

Theorem:- Let $\pi = (b_1\, b_2 \ldots b_r) \in S_n$. Then for all $\alpha \in S_n$,

$$\alpha \circ \pi \circ \alpha^{-1} = (\alpha(b_1)\ \alpha(b_2) \ldots \alpha(b_r)).$$

Two cycles in S_n are conjugate if and only if they have the same length.

Theorem:- Every element of A_n is a product of 3-cycles, $n \geq 3$.

Questions.

1). Express $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 8 & 5 & 6 & 4 & 7 & 1 \end{pmatrix}$ as a product of disjoint cycles and then as a product of transpositions.

2). Write all elements of S_4. Show that S_4 has no elements of order ≥ 5.

3). Find the order of $(1234)(657)$ in S_7.

4). Let $\alpha = (2\ 5\ 9)(1\ 3\ 6)$ and $\beta = (1 5 7)(2 4 6 9) \in S_9$ Find $\alpha \circ \beta \circ \alpha^{-1}$.

5). Let $(1\ 3\ 5\ 7)$ and $(2\ 3\ 6\ 8) \in S_8$. Find $\alpha \in S_8$ such that $\alpha \circ (1\ 3\ 5\ 7) \circ \alpha^{-1} = (2\ 3\ 6\ 8)$.

6). Prove that $(1\ 2\ \cdots\ n\text{-}1\ \ n)^{-1} = (n\ \ n\text{-}1\ \cdots\ 2\ 1)$.

7). Show that the number of distinct cycles of length r in S_n is $(r-1)!\,{}^nC_r = \frac{1}{r}\frac{n!}{(n-r)!}$.

AKHTAR ABBAS
Lecturer (Mathematics)
Govt. Degree College
Shah Jewna (Jhang)

Cosets:-

Let G be a group and $H \leq G$. For any $a \in G$, We define

$$aH = \{ah : h \in H\} \quad \text{(Left coset of } H \text{ containing } a)$$

and $$Ha = \{ha : h \in H\} \quad \text{(Right coset of } H \text{ containing } a)$$

(In general $aH \neq Ha$).

Example:-

(1) Let $G = S_3 = \{I, (123), (132), (12), (23), (13)\}$.

and $H = \{I, (13)\}$. Then

$$IH = H$$

$$(12)H = \{(12), (12)(13)\} = \{(12), (132)\} = (132)H$$

$$(13)H = \{(13), (13)(13)\} = \{(13), I\} = H$$

$$(23)H = \{(23), (23)(13)\} = \{(23), (123)\} = (123)H.$$

Distinct cosets of H in G are

$$H, \ (12)H, \ (23)H$$

(2) Let $G = \mathbb{Z}_9 = \{0, 1, 2, 3, 4, 5, 6, 7, 8\}$

and $H = \{0, 3, 6\}$

Then cosets of H in G are

$$0 + H = \{0, 3, 6\} = 3 + H = 6 + H.$$

$$1 + H = \{1, 4, 7\} = 4 + H = 7 + H.$$

$$2 + H = \{2, 5, 8\} = 5 + H = 8 + H.$$

AKHTAR ABBAS
Lecturer (Mathematics)
Govt Degree College
Shah Jewna (Jhang)

Properties of Cosets:-

Let $H \leq G$ and $a, b \in G$. Then

1). $a \in aH$.

2). $aH = H$ if and only if $a \in H$.

3). $(ab)H = a(bH)$.

4). $aH = bH$ if and only if $a \in bH$.

5). $aH = bH$ or $aH \cap bH = \phi$

6). $aH = bH$ if and only if $ab^{-1} \in H$. or $a^{-1}b \in H$.

7). $|aH| = |bH| = |Ha| = |Hb| = |H|$.

8). $aH = Ha$ if and only if $H = aHa^{-1}$.

9). $aH \leq G$ if and only if $a \in H$.

Question:-

Find the cosets of $H = \{1, 15\}$ in $G = U(32)$.

Lagrange's Theorem:-

If G is a finite group and $H \leq G$, then $|H|$ divides $|G|$.

Index of a subgroup:-

If $H \leq G$, then the number of distinct left (or right) cosets of H in G is called index of H in G, denoted as $[G:H]$ or $|G:H|$.

Consequences of Lagrange's Theorem:-

1). If G is a finite group and $H \leq G$, then
$$[G:H] = \frac{|G|}{|H|}$$

2). If $a \in G$, then $|a|$ divides $|G|$.

3). A group of prime order is cyclic.

(4) In a finite group G, $a^{|G|} = e$, $\forall\ a \in G$.

5) Let a be an integer and p be a prime, then $$a^p \equiv a \mod p.$$

AKHTAR ABBAS
Lecturer (Mathematics)
Govt. Degree College
Shah Jewna (Jhang)

Converse of Lagrange's Theorem:-

The converse of Lagrange's Theorem is false. For example, A_4 has no subgroup of order 6, where as $|A_4| = 12$.

(A_4 is ~~the~~ of smallest order ~~sub~~group for which converse of Lagrange's Theorem is not true).

Theorem:-

For any two subgroups H and K of a finite group G, $|HK| = \dfrac{|H|\,|K|}{|H \cap K|}$.

Example:- A group of order 75 can have at most one subgroup of order 25. For this, suppose H and K are two subgroups of order 25. Since $|H \cap K| \mid |H|$ so $|H \cap K| = 1$ or 5 results in $|HK| = \dfrac{25 \cdot 25}{|H \cap K|} = 625$ or 125.

Exercises :-

1). Find all right cosets of $6\mathbb{Z}$ in $\mathbb{Z}$.

2). Let $|G| = pq$, where p and q are prime integers. Show that every proper subgroup of G is cyclic.

3). Let $H \leq G$. Define a relation $\sim$ on G by for all $a, b \in G$, $a \sim b$ if and only if $b^{-1}a \in H$.
Show that $\sim$ is an equivalence relation on G and the equivalence classes of $\sim$ are the cosets aH, $a \in G$.

4). Let $|G| = pq$ $(p > q)$, where p and q are distinct primes. Show that G has at most one subgroup of order p.

5). Let G be a finite group and $A, B \leq G$ such that $A \subseteq B$. Prove that

$$[G:A] = [G:B][B:A].$$

6). Let $|G| = 35$ and $A, B \leq G$ such that $|A| = 3$ and $|B| = 7$. Show that $G = AB$.

7). We define double coset of H and K in a group G as

$$HaK = \{hak : h \in H, k \in K\}$$

where $a \in G$ and $H, K \leq G$.
Prove that $$|HaK| = \frac{|H|\ |K|}{|H \cap aKa^{-1}|}, \quad \forall\, a \in G.$$

Normal Subgroup

A subgroup N of G is called normal subgroup if $aN = Na$, for all $a \in G$.

We denote this by $N \trianglelefteq G$.

Normal Subgroup Test:-

A subgroup N of G is normal if and only if $xNx^{-1} \subseteq N$, $\forall\ x \in G$, or $xnx^{-1} \in N$ $\forall x \in G$ and $n \in N$.

Examples

1). Every subgroup of an Abelian group is normal.

2)- $A_n \trianglelefteq S_n$ for all $n \geq 2$.

3). Every subgroup of index 2 is normal.

4). $Z(G) \trianglelefteq G$.

5). Let $H \trianglelefteq G$ and $K \leq G$, then $HK \leq G$.

6)- If H is a unique subgroup of finite order of G, then $H \trianglelefteq G$.

7). $SL(2,\mathbb{R}) \trianglelefteq GL(2,\mathbb{R})$.

8)- If $H, K \trianglelefteq G$, then $H \cap K \trianglelefteq G$.

9)- Let $H \leq G$. Then $\bigcap_{g \in G} gHg^{-1} \trianglelefteq G$.

10)- $H \trianglelefteq G$ if and only if $N(H) = G$.

11)- $H \trianglelefteq N(H)$.

Simple Group:- A group G is simple if $G \neq \{e\}$ and the only normal subgroups of G are $\{e\}$ and G.

Factor Group:-

Let G be a group and $H \trianglelefteq G$. The set $G/H = \{gH : g \in G\}$ is a group under the operation

$$(g_1H)(g_2H) = g_1g_2H.$$

This is called factor (quotient) group.

Examples:-

1). $\mathbb{Z}/4\mathbb{Z} = \{0+4\mathbb{Z},\ 1+4\mathbb{Z},\ 2+4\mathbb{Z},\ 3+4\mathbb{Z}\}$.

2). Let $G = \mathbb{Z}_{18}$ and $H = \langle 6 \rangle = \{0, 6, 12\}$.
Then $G/H = \{0+H,\ 1+H,\ 2+H,\ 3+H,\ 4+H,\ 5+H\}$.

3). Let $G = U(32) = \{1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25, 27, 29, 31\}$ and $H = \{1, 17\}$. Then

$$G/H = \{H, 3H, 5H, 7H, 9H, 11H, 13H, 15H\}.$$

$\boxed{\text{In case of finite group } G,\ \left|\frac{G}{H}\right| = \frac{|G|}{|H|}}$.

$\boxed{A_n \text{ is simple if } n \geq 5}$.

Theorem:- For a group G, if $G/Z(G)$ is cyclic, then G is commutative.

Exercise:- Let G be a commutative group. Show that G is simple if and only if G is of prime order.

Natural Homomorphism:-

Let $H \trianglelefteq G$. Define a map $\phi : G \to G/H$ by

$$\phi(a) = aH \quad \text{for all } a \in G.$$

Then ϕ is a homomorphism from G onto G/H and $\text{Ker}\,\phi = H$. This homomorphism is called the natural homomorphism of G onto G/H.

Example:-

Consider S_3 and the normal subgroup

$$H = \{I, (1\,2\,3), (1\,3\,2)\}.$$

AKHTAR ABBAS
Lecturer (Mathematics)
Govt Degree College
Shah Jewna (Jhang)

Define $\phi : S_3 \to S_3/H$ by

$$\phi(\alpha) = \alpha H \quad \text{for all } \alpha \in S_3.$$

Then ϕ is a homomorphism which is onto and $\ker \phi = H$.

Question: Determine all homomorphisms from $\mathbb{Z}_{12}$ to $\mathbb{Z}_{30}$.

Sol:- Such a homomorphism is completely specified by image of 1. That is, if $1 \mapsto a$, then $x \mapsto xa$.
Lagrange's theorem requires that $|a|$ divides 30 and also $|a| \mid |1| = 12$. So $|a| = 1, 2, 3,$ or 6.

Thus $a = 0, 15, 10, 20, 5$ or 25.

Hence there are six $(= \gcd(12, 30))$ homomorphisms from $\mathbb{Z}_{12}$ to $\mathbb{Z}_{30}$.

Result:- In general, $|\text{Hom}(\mathbb{Z}_m, \mathbb{Z}_n)| = \gcd(m, n)$

In particular, if $(m, n) = 1$, then $|\text{Hom}(\mathbb{Z}_m, \mathbb{Z}_n)| = 1$.

Example:- The mapping $\phi : S_n \to \mathbb{Z}_2$ that takes an even permutation to 0 and an odd permutation to 1, is a homomorphism with $\ker\phi = A_n$.

Examples of Isomorphisms:-

1). $U(10) \cong \mathbb{Z}_4$ and $U(5) \cong \mathbb{Z}_4$.

2). Any infinite cyclic group is isomorphic to $\mathbb{Z}$ and any finite cyclic group is isomorphic to $\mathbb{Z}_n$.

3). $U(10) \not\cong U(12)$

4). Let $G = SL(2,\mathbb{R})$. Define a map $\phi : SL(2,\mathbb{R}) \to SL(2,\mathbb{R})$ by $\phi_M(A) = MAM^{-1}$, for all $A \in SL(2,\mathbb{R})$, where M is any fixed 2×2 real matrix with $|M| = 1$. Then ϕ_M is an isomorphism.

Properties of Isomorphisms acting on elements:-

Suppose that $\phi : G \to G'$ is an isomorphism. Then;

1). $\phi(e) = e'$

2). $\phi(g^n) = [\phi(g)]^n$ for all $n \in \mathbb{Z}$ and $g \in G$.

3). For any $a, b \in G$, $ab = ba$ if and only if $\phi(a)\phi(b) = \phi(b)\phi(a)$.

4). $G = \langle a \rangle$ if and only if $G' = \langle \phi(a) \rangle$.

5). For all $a \in G$, $|a| = |\phi(a)|$.

6). If G is finite, then G and G' have exactly the same number of elements of every order.

Properties of Isomorphisms acting on groups:-

Suppose that $\phi: G \to G'$ is an isomorphism. Then

1). $\phi^{-1}: G' \to G$ is an isomorphism.

2). G is Abelian if and only if G' is Abelian.

3). G is cyclic if and only if G' is cyclic.

4). $\phi(Z(G)) = Z(G')$.

Cayley's Theorem:-

Every group is isomorphic to a group of permutations of its own elements.

$$\left(G \cong F(G) = \{ f_a : a \in G,\ f_a(b) = ab \} \text{ under } \phi(a) = f_a \right).$$

Example:- Let $\gcd(|G|, |H|) = 1$, then trivial homomorphism is the only homomorphism (isomorphism). from G into H.

Example:- $(\mathbb{Q}, +) \not\cong (\mathbb{Q}^*, \cdot)$

since every nonidentity element of $(\mathbb{Q}, +)$ is of infinite order while -1 is a nonidentity element of $(\mathbb{Q}^*, \cdot)$ which is of finite order.

Example:- $(\mathbb{Z}, +) \not\cong (\mathbb{Q}, +)$

since $(\mathbb{Z}, +)$ is cyclic and $(\mathbb{Q}, +)$ is non cyclic.

Prepared by:- Akhtar Abbas.

Properties of Homomorphisms:-

Let $\phi : G \to G'$ be a homomorphism and $g \in G$.

Then :

1) $\phi(e) = e'$

2) $\phi(g^n) = [\phi(g)]^n$ for all $n \in \mathbb{Z}$.

3). If $|g|$ is finite, then $|\phi(g)|$ divides $|g|$.

4). $Ker\,\phi \trianglelefteq G$.

5). $\phi(a) = \phi(b)$ if and only if $a\,Ker\,\phi = b\,Ker\,\phi$.

6). If $\phi(g) = g'$, then $\phi^{-1}(g') = \{x \in G : \phi(x) = g'\} = g\,Ker\,\phi$.

Properties of Subgroups under Homomorphisms:-

Let $\phi : G \to G'$ be a homomorphism and $H \leq G$. Then;

1). $\phi(H) = \{\phi(h) : h \in H\} \trianglelefteq G'$.

2). If H is cyclic, then $\phi(H)$ is cyclic.

3). If H is Abelian, then $\phi(H)$ is Abelian.

4). If $H \trianglelefteq G$, then $\phi(H) \trianglelefteq \phi(G)$.

5). If $|H| = n$, then $|\phi(H)|$ divides n.

6). If $|Ker\,\phi| = n$, then ϕ is an n-to-1 mapping from G onto $\phi(G)$.

7). If $K' \leq G'$, then $\phi^{-1}(K') = \{k \in G : \phi(k) \in K'\} \leq G$.

8) If $K' \trianglelefteq G'$, then $\phi^{-1}(K') \trianglelefteq G$.

9). ϕ is one-one if and only if $Ker\,\phi = \{e\}$.

Prepared by: Akhtar Abbas.

Homomorphism:-

A map $\phi : G \longrightarrow G'$ is called homomorphism if $\phi(ab) = \phi(a)\,\phi(b)$ for all $a, b \in G$.

Kernel of a Homomorphism:-

Let $\phi : G \longrightarrow G'$ be a homomorphism. We define $\operatorname{Ker}\phi = \{ g \in G : \phi(g) = e' \}$.

Examples:-

1). A map $\phi : GL(2,\mathbb{R}) \rightarrow \mathbb{R}^*$, defined by

$$\phi(A) = |A|$$

is a homomorphism with $\ker(\phi) = SL(2,\mathbb{R})$.

2). The map $\phi : \mathbb{R}^* \longrightarrow \mathbb{R}^*$, defined by

$$\phi(x) = |x|$$

is a homomorphism with $\ker\phi = \{-1, 1\}$.

3). The map $\phi : \mathbb{Z} \rightarrow \mathbb{Z}_n$, defined by

$$\phi(x) = x \bmod n$$

is a homomorphism with $\ker\phi = \langle n \rangle$.

Definitions:-

A homomorphism $\phi : G \rightarrow G'$ is called a;

i) monomorphism, if ϕ is onle-one (injective).

ii) epimorphism, if ϕ is onto (surjective).

iii) isomorphism, if ϕ is one-one and onto (bijective).

iv) endomorphism, if $G = G'$.

v) automorphism, if ϕ is an isomorphism and $G = G'$.

First Isomorphism Theorem:-

Let $\phi : G \to G'$ be a homomorphism. Then

$$G/_{\text{Ker}\,\phi} \cong \phi(G).$$

Example:-

$$\mathbb{Z}/_{n\mathbb{Z}} \cong \mathbb{Z}_n .$$

AKHTAR ABBAS
Lecturer (Mathematics)
Govt Degree College
Shah Jewna (Jhang)

Second Isomorphism Theorem:-

Let $H, K \leq G$ with $K \trianglelefteq G$. Then

$$H/_{(H \cap K)} \cong HK/_{K} .$$

Example

Consider the group $(\mathbb{Z}, +)$ and its subgroups $H = \langle 2 \rangle$ and $K = \langle 3 \rangle$. Then

$$H + K = \langle 2 \rangle + \langle 3 \rangle = \mathbb{Z} \quad \text{and} \quad H \cap K = \langle 6 \rangle .$$

Therefore
$$\frac{\langle 2 \rangle}{\langle 6 \rangle} \cong \frac{\mathbb{Z}}{\langle 3 \rangle}$$

Notice that
$$\frac{\langle 2 \rangle}{\langle 6 \rangle} = \{ 0 + \langle 6 \rangle,\ 2 + \langle 6 \rangle,\ 4 + \langle 6 \rangle \}$$

while
$$\frac{\mathbb{Z}}{\langle 3 \rangle} = \{ 0 + \langle 3 \rangle,\ 1 + \langle 3 \rangle,\ 2 + \langle 3 \rangle \}.$$

The mapping $\phi : \dfrac{\langle 2 \rangle}{\langle 6 \rangle} \longrightarrow \dfrac{\mathbb{Z}}{\langle 3 \rangle}$

defined by $\phi(0 + \langle 6 \rangle) = 0 + \langle 3 \rangle$, $\phi(2 + \langle 6 \rangle) = 2 + \langle 3 \rangle$, $\phi(4 + \langle 6 \rangle) = 1 + \langle 3 \rangle$ is the required isomorphism.

Third Isomorphism Theorem:-

Let $H_1, H_2 \trianglelefteq G$ with $H_1 \subseteq H_2$. Then

$$\frac{\left(G/H_1\right)}{\left(H_2/H_1\right)} \cong \frac{G}{H_2}.$$

Example:-

Let $G = (\mathbb{Z}, +)$, $H_1 = \langle 6 \rangle$ and $H_2 = \langle 3 \rangle$

Then $H_1 \subseteq H_2$ and

$$\frac{G}{H_2} = \frac{\mathbb{Z}}{\langle 3 \rangle} = \{0+\langle 3\rangle,\ 1+\langle 3\rangle,\ 2+\langle 3\rangle\}$$

$$\frac{G}{H_1} = \frac{\mathbb{Z}}{\langle 6 \rangle} = \{0+\langle 6\rangle, 1+\langle 6\rangle, 2+\langle 6\rangle, 3+\langle 6\rangle, 4+\langle 6\rangle, 5+\langle 6\rangle\}$$

$$\frac{H_2}{H_1} = \frac{\langle 3\rangle}{\langle 6\rangle} = \{0+\langle 6\rangle,\ 3+\langle 6\rangle\}$$

Now
$$\frac{\left(G/H_1\right)}{\left(H_2/H_1\right)} = \left\{0+\langle 6\rangle + \frac{\langle 3\rangle}{\langle 6\rangle},\ 1+\langle 6\rangle+\frac{\langle 3\rangle}{\langle 6\rangle},\ 2+\langle 6\rangle+\frac{\langle 3\rangle}{\langle 6\rangle}\right\}.$$

It is clear that
$$\frac{\mathbb{Z}}{\langle 3\rangle} \cong \frac{\left(\mathbb{Z}/\langle 6\rangle\right)}{\left(\langle 3\rangle/\langle 6\rangle\right)}.$$

Group of automorphisms:-

Let G be a group, then the collection of all automorphisms of G, $\mathrm{Aut}(G)$ is a group under the composition of functions.

Inner automorphism:-

Let G be a group and $a \in G$. We define inner automorphism $\theta_a : G \to G$ by $\theta_a(g) = aga^{-1}$, $\forall\, g \in G$.

We denote by $Inn(G)$ the set of all inner automorphisms of G.

$$\boxed{Inn(G) \trianglelefteq Aut(G)}$$

Theorem:- Let G be a group and $H \leq G$. Then

$$\frac{N(H)}{C(H)} \cong \text{a subgroup of } Aut(G).$$

and $$\frac{G}{Z(G)} \cong Inn(G).$$

AKHTAR ABBAS
Lecturer (Mathematics)
Govt. Degree College
Shah Jewna (Jhang)

Exercises:-

1). Show that $Aut(\mathbb{Z}_n) \cong U(n)$.

2). Show that $|Aut(\mathbb{Z}_p)| = \phi(p) = p-1$, where p is a prime.

3). Show that $Aut(S_3) = Inn(S_3) \cong S_3$.

4). Determine $Aut(S_4)$.

5). Let G be a cyclic group of order n. Prove that $|Aut(G)| = \phi(n)$.

6). Let G be a group such that $Z(G) = \{e\}$. Prove that $Z(Aut(G)) = \{e\}$.

Characteristic Subgroup:-

Let G be a group and $H \leq G$. H is called a characteristic subgroup of G if $\phi(H) \subseteq H$, $\forall\ \phi \in Aut(G)$.

Properties:-

1). Every characteristic subgroup of G is normal.
2). $Z(G)$ is characteristic subgroup of G.
3). Every subgroup of a cyclic group is characteristic.
4). The product and intersection of two characteristic subgroups is characteristic