PITHAPUR RAJAH'S GOVERNMENT COLLEGE (AUTONOMOUS), KAKINADA
KAKINADA 533 001-ANDHRA PRADESH
An AUTONOMOUS and NAAC Accredited Institution(A Grade- 3.17 CGPA)
(Affiliated to ADI KAVI NANNAYA UNIVERSITY, Rajamahendravarm.)

G.SYAM PRASAD REDDYM.Sc.,M.Phil.,B.Ed.,SET

LECTURER IN MATHEMATICS

P.R.G.C(A), KAKINADA.

GROUP THEORY

Binary Operation :

Let S be a non-empty set. If f: S x S → S is a mapping, then f is called binary operation or binary composition in S or on S.

Thus if a relation in S such that every pair (distinct or equal) of elements of S taken in definite order is associated with a unique element of S then it is called a binary operation in S. Otherwise the relation is not binary operation in S and the relation is simply an operation in S.

Symbolism :

1. For a,b ϵ S ⇒ a + b ϵ S then "+ " is a binary operation in S.
2. For a,b ϵ S ⇒ a • b ϵ S then {"• " is a binary operation in S.
3. For a,b ϵ S ⇒ a○b ϵ S then " ○ "is a binary operation in S.
   This also called **closure law**.

Algebraic Structure :

A non-empty set G equipped with one or more binary operations is called an algebraic structure or an algebraic system .
If ' ○ ' is a binary operation on G , then the algebraic structure is written as (G,○).

Associative Law :

' ○ ' is a binary operation in a set S. If for a,b,c ϵ S , (a○b)○c = a○(b○c) then ' ○ ' is said to be associative in S . This is called Associative law . Otherwise ' ○ ' is said to be not associative in S .

Identity Element :

Let S be a non-empty set and '○' be a binary operation on S.

i) If there exists an element e_1 ϵ S such that e_1○a=a for a ϵ S then e_1 is called a left identity of S w.r.t. the operation '○' .

ii) If there exists an element e_2 ϵ S such that a○e_2=a for a ϵ S then e_2 is called a right identity of S w.r.t. the operation '○' .

iii) If there exists an element $e \in S$ such that e is both left and a right identity of S w.r.t. '$\circ$' , then e is called an identity of S .

Invertible Element :

Let ($S,\circ$) be an algebraic structure with the identity element e in S w.r.t. '$\circ$'.

i) An element $a \in S$ is said to be left invertible or left regular if there exists an element $x \in S$ such that $x\circ a = e$. x is called a left inverse of a, w.r.t. '$\circ$' .

ii) An element $a \in S$ is said to be right invertible or right regular if there exists an element $y \in S$ such that $a\circ y = e$. y is called a right inverse of a, w.r.t. '$\circ$' .

iii) An element x which is both a left inverse and a right inverse of 'a' is called an inverse of 'a' and 'a' is said to be invertible or regular.

Semi Group :

An Algebraic structure ($S,\circ$) is called a semi Group if the binary operation '$\circ$' is associative in S .

Monoid:

A semi Group ($S,\circ$) with the identity element w.r.t. '$\circ$' is known as a monoid. i.e ($S,\circ$) is a monoid if S is a non-empty set and '$\circ$' a binary operation in S such that '$\circ$' is associative and there exists an identity element w.r.t. '$\circ$' .

Group:

If G is a non-empty set and '$\circ$' is a binary operation defined on G such that the following three laws are satisfied then ($G,\circ$) is a group.

i). Associative law

ii). Identity law

iii). Inverse law.

Note :

1. A group is an algebraic structure. It can also be written by $< G,\circ >$.
2. A semi group ($G,\circ$) is a group if identity law and inverse law are satisfied.
3. A monoid ($G,\circ$) is a group if inverse law is satisfied.

Abelian Group or Commutative Group :

For the Group $a,b \in G$, $a\circ b = b\circ a$ is satisfied , then ($G,\circ$) is called an abelian group or a commutative group.

Finite and Infinite Group :

If the set G contains a finite number of elements then the group ($G,\circ$) is called a finite group. Otherwise the group ($G,\circ$) is called an infinite group.

Order of a Group :

The number of elements in a finite group ($G,\circ$) is called the order of the group and is denoted by O(G). If G is infinite , then we say that the order of G is infinite.

Thus : i) If the number of elements in a group G is n, then $O(G) = n$.

ii) If the group G is finite we sometimes write $O(G) < \infty$.

iii) If $O(G) = 2n$, $n\in N$,we say that the group is of even order.

iv) If $O(G) = 2n-1$, $n\in N$ we say that the group is of odd order.

Cancellation Laws :

Let S be non-empty set and $\circ$ be binary operation on S.

For $a,b,c \in S$,

i) $a\circ b = a\circ c \Rightarrow b = c$ (is called left cancelation law)

ii) $b \circ a = c \circ a \Rightarrow b = c$ (is called Right cancelation law)

(i) and (ii) are called cancelation laws.

Note:

- Identity element in a group is unique.
- Inverse of each element of a group is unique.
- If a, b ϵ g, then $(ab)^{-1} = b^{-1} a^{-1}$. This law is called reversal rule.
- Cancelation law holds in a group.
- If a, b ϵ G, then linear equations $a \circ x = b$, $y \circ a = b$ have unique solutions for x, y ϵ G.
- The order of every element of a group is finite.
- The order of every element of a finite group is less than or equal to the order of the group.
- The order of an element of a group is same as that of its inverse.
- The order of any integral power of an element a ϵ G cannot exceed the order of a.
- If a ϵ G a group, o(a) = n and $a^m = e$ then $\frac{n}{m}$.
- If a ϵ G is an element of order n and p is prime to n, then a^p is also of order n.
- If every element of a group except the identity element is of order two, then G is abelian.
- If every element of a group g is its own inverse, then g is abelian.

Sub Groups

A non – empty subset H of a group G is said to be subgroup of G, if under the operation defined on G, h itself forms a group.

Since every set is a subset of itself, group G is a subgroup of itself, called trivial subgroup. If e is the identity of G, then subset of G containing only one element e is also a subgroup of G. i.e {e} is subgroup of g call it trivial subgroup of g. Thus, there are two trivial subgroups of each group.

Note:

- The identity of a subgroup is the same as that of the group.
- The inverse of any element of a subgroup is the same as inverse of the same regarded as an element of the group.
- A subset H of a group G is subgroup of G if and only if (i) a, b ϵ H $\Rightarrow$ ab ϵ H (ii) a ϵ H $\Rightarrow$ a^{-1} ϵ G where a^{-1} is the inverse of a in G.
- A necessary and sufficient condition for a non-empty subset H of group G to be a subgroup is that a, b ϵ H => ab^{-1} ϵ H where b^{-1} is the inverse of b in G.
- The intersection of two subgroups of a group G is a subgroup of G.
- The union of two subgroups is not a necessarily a subgroup.
- The union of two subgroups is a subgroup if and only if one is contained in the other.
- A subgroup of an abelian group is abelian.
- A finite non-empty subset H of G is subgroup of G if and only if HH = H.
- If H and K are two subgroups of G, then HK is a subgroup of G if and only if HK = KH.
- Every abelian group has abelian subgroup.
- A non-abelian group can have an abelian subgroup.

Coset

Let H be subgroup of G, then for all a ϵ G, the set Ha = { ha / h ϵ H } is called right coset of H in G generated by a and aH = { ah / h ϵ H } is called left coset of H in G generated by a. Also Ha, aH are called cosets of H generated by a in G.

Note:

- If a ϵ G is also in H then Ha = aH = H.
- H is any subgroup of a group G and h ϵ G then h ϵ H if and only if hH = H = Hh.
- If a, b are any two elements of a group G and H any subgroup of G, then Ha = Hb iff ab^{-1} ϵ H and aH = bH iff $a^{-1}b$ ϵ H.
- If a, b are any two elements of a group G and H any subgroup of G then a ϵ bH iff ah = bH and a ϵ Hb iff Ha = Hb.
- Any two left(right) cosets of a subgroup are either disjoint or identical.
- Let H be a subgroup of a group G, then there is one-one correspondence between any two right cosets of H in G.
- If H is a subgroup of a group G, then there is one to one correspondence between the set of all distinct left cosets of H in G and the set of all distinct right cosets of H in G.

Index of a subgroup of a finite group:

If H is a subgroup of a finite group G, then the number of distinct left(right) cosets of H in G is called the index of H in G. It is denoted by (G : H) or $i_G(H)$.

Lagrange's Theorem:

The order of a group of a finite group divides the order of the group. i.e O(H)/O(G).

- The converse of Lagrange's theorem is not true.
- The order of every element of a finite group is a divisor of the order of the group. i.e O(a)/O(G)
- Let H and K be finite subgroups of a group G, then $O(HK) = \frac{O(H)O(K)}{O(H\cap K)}$.

Euler Theorem:

If **n** is a positive integer and **a** is any integer relative prime to **n**, then $a^{\phi(n)} \equiv 1 (\text{mod } n)$, where ϕ is the Euler ϕ - function.

Fermat theorem:

If **p** is prime number and **a** is any integer, then $a^p \equiv a (\text{mod } n)$.

Normalizer of an element of a group:

If **a** is an element of a group G, then the normalizer on **a** in G is the set of all those elements of G which commute with **a**. The normalizer of **a** in G is denoted by N(a) where N(a) = { x ϵ G / ax = xa}.

Self-Conjugate element of a group:

If G is a group and a ϵ G such that a = $x^{-1}ax$ ∀ x ϵ G. then a is called self-conjugate of G. A self-conjugate element is sometimes called an invariant element.

Here a = $x^{-1}ax \Rightarrow xa = ax$ ∀ x ϵ G.

The Centre of a group:

The Z of all self-conjugate elements of a group G is called the centre of the group G.

Thus Z = { z ϵ G / zx = xz ∀ x ϵ G}.

Normal Subgroups

A subgroup H of a group G is said to be a normal subgroup of G if $\forall$ x ϵ G and $\forall$ h ϵ H, xhx^{-1} ϵ H.

From the definition we conclude that

- H is a normal subgroup of G iff $xHx^{-1} \subseteq H$, $\forall$ x ϵ G where $xHx^{-1} = \{xhx^{-1} / x \in G, h \in H\}$.
- H is a normal subgroup of G iff $x^{-1}Hx \subseteq H$, $\forall$ x ϵ G.
- The improper subgroup H = {e} is a normal subgroup.
- The improper subgroup H = G is a normal subgroup.

  H = {e} and H = G are called improper or trivial normal subgroups of a group G and all other subgroups of G, if exists are called proper normal subgroups of G.

Notation: If N is a normal subgroup of G we write $N \lhd G$. We read $N \lhd G$ as 'N normal subgroup G'.

Note: Any non-abelian group whose every subgroup is normal, is called a Hamilton group.

- A subgroup H of a group G is normal $xHx^{-1} = H$ $\forall$ x $\in$G.
- A subgroup H of a group G is a normal subgroup of G iff each left cosets of H in G is a right coset of H in G.
- A subgroup H of a group G is a normal subgroup of G iff the product of two right(left) cosets of H in G is again a right(left) coset of H in G.
- Every subgroup of an abelian group is normal.
- If G is a group and H is a subgroup of index 2 in G, then H is a normal subgroup of G.
- The intersection of any two normal subgroups of a group is a normal subgroup.
- A normal subgroup of a group G is commutative with every complex of G.
- If N is a normal subgroup of G and H is any subgroup of G then HN is a subgroup of G.
- If H is a subgroup of G and N is a normal subgroup of G, then (i) $H \cap N$ is a normal subgroup of H and (ii) N is a normal subgroup of HN.
- If N, M are normal subgroups of G, then NM is also a normal subgroup of G.
- If M, N are two normal subgroups of G such that $M \cap N$ = {e]. Then every element of M commutes with every element of N.

Homomorphisms, Isomorphisms of Groups

Homomorphism Into:

Let G, G' be two groups and f a mapping from G into G'. If for a, b $\in$ G, f(a.b) = f(a) . f(b) then f is said to be homomorphism from G into G'.

Image of Homomorphism:

Let f: G $\rightarrow$ G' is a homomorphism. Then {f(a) / a$\in$G} is called homomorphic image of f or range of f. It is denoted by f(G) or $I_m(f)$.

Homomorphism onto:

Let G, G' be two groups and f a mapping from G onto G'. If for a, b $\in$ G, f(a.b) = f(a) . f(b) then f is said to be homomorphism from G onto G'.

Monomorphism:

If the homomorphism into is one-one, then it is called monomorphism.

Endomorphism:

A homomorphism of a group G into itself is called an endomorphism.

Isomorphism:

Let G, G' be any two groups and f be a one-one mapping of G onto G'. If for a, b $\in$ G, f(a.b) = f(a) . f(b) then f is said to be an isomorphism from G to G'. In this case we say that G is isomorphic to G' and we write $G \cong G'$.

Automorphism:

An isomorphism from a group G onto itself is called an automorphism of G.

Properties of Homomorphism:

- Let G, G' be two groups. Let f be a homomorphism from G into G'. Then (i) f(e) = e' where e is the identity in G and e' is the identity in G'. (ii) $f(a^{-1}) = \{f(a)\}^{-1}$.
- The homomorphic image of a group is a group.
- Every homomorphic image of an abelian group is abelian.

Kernel of a Homomorphism:

If f is a homomorphism of a group G into a group G', then the set K of all those elements of G which are mapped by f onto the identity e' of G' is called the Kernel of the homomorphism f.

i.e Kernel f = $\{ x \in G / f(x) = e' \}$ = K. Sometimes kernel f is written as ker f.

- If f is a homomorphism of a group G into a group G', then the kernel of f is a normal subgroup of G.
- The necessary and sufficient condition for a homomorphism f of a group G onto a group G' with kernel K to be an isomorphism of G into G' is that K = [e}.
- Let f be a homomorphism from a group G into a group G' then f is monomorphism iff ker f = {e} where e $\in$ G is identity.
- Let G be a group and N be a normal subgroup of G. Let f be a mapping from G to G/N defined by f(x) = Nx for x $\in$ G. Then f is a homomorphism of G onto G/N and ker f = N.

Natural or Canonical Homomorphism:

The mapping f: $G \to G/N$ such that f(x) = Nx for x $\in$ G is called Natural or Canonical Homomorphism.

Fundamental theorem of Homomorphism of Groups:

Every homomorphic image of a group G is isomorphic to some quotient group of G.

If ϕ is a homomorphism from a group G onto a group G', then G / kerϕ is isomorphic with G'.

Automorphism of a Group:

If f: $G \to G$ is an isomorphism from a group G to itself, then f is called an automorphism of G.

The set of all automorphisms of a group G forms a group w.r.t. composition of mappings.

Inner Automorphism, Outer Automorphism:

Let G be a group. If the mapping $f_a : G \to G$, defined by $f_a(x) = a^{-1}xa$ for every x $\in$ G and a, a fixed element of G, is an automorphism of G, then f_a is known as inner automorphism.

An automorphism which is not inner called an outer automorphism.

Permutation Groups

Permutation:

A permutation is a one-one mapping of a non-empty set onto itself.

Thus, a permutation is a bijective mapping of a non-empty set into itself.

If S = { a_1, a_2, … a_n} then a one-one mapping from s onto itself is called a permutation of degree n. The number n of elements in S is called the degree of permutation.

Symbol for a permutation when S = { a_1, a_2, … a_n }:

Let f : S → S be a permutation such that $f(a_1) = b_1$, $f(a_2) = b_2$, … $f(a_n) = b_n$ where b_1, b_2, … b_n are nothing but the elements a_1, a_2, … a_n of S in some order. So we write $\begin{pmatrix} a_1 & a_2 & \dots & a_n \\ b_1 & b_2 & \dots & b_n \end{pmatrix}$, where each element in the second row is the f image of the corresponding element in the first row. Then we have n! elements of the type in S_n where S_n is the set of all permutations defined on S.

Equal permutation:

Two permutations f and g defined over a non-empty set S are said to be equal if f(a) = f(b) for $a \in S$.

Permutation multiplication or product of permutations:

If f, g are two permutations defined over S, then the product of permutations f, g is defined as gof or gf where (gf)(a) = g{f(a)} for $a \in S$.

Permutation Group:

The set A(S) of all permutations defined over a non-empty set S form a group under the operation permutation multiplication.

The permutation group is also is also known as the symmetric group of order n on n symbols.

The permutation group on n symbols is generally denoted by S_n or P_n. The elements of S can be denoted also by 1, 2, 3, … n or by any other symbols.

Identity permutation:

If f is a permutation of S such that $f(a) = a \ \forall \ a \in S$, then f is identity of S and we denoted f as I.

Order of a permutation:

If $f \in S_n$ such that $f^m = I$, the identity permutation in S_n, where m is the least positive integer, then the order of the permutation f in S_n is m. Order of S_n is n!

Orbits and Cycles of permutation:

Consider a set S = { a_1, a_2, … a_n} and a permutation f on S. If for $s \in S$ there exists a smallest positive integer l depending on s such that $f^l(s) = s$, then the set $\{s, f^1(s), f^2(s), \dots f^{l-1}(s)\}$ is called the orbit of s under the permutation f. The ordered set $\{s, f^1(s), f^2(s), \dots f^{l-1}(s)\}$ is called a cycle of f.

Cyclic Permutation:

Consider a set S = { a_1, a_2, … a_n} and a permutation $f = \begin{pmatrix} a_1 & a_2 & \dots a_k & a_{k+1} & \dots & a_n \\ a_2 & a_3 & \dots a_1 & a_{k+1} & \dots & a_n \end{pmatrix}$ on S.

i.e $f(a_1) = a_2$, $f(a_2) = a_3$, … $f(a_k) = a_1$, $f(a_{k+1}) = a_{k+1}$, … $f(a_n) = a_n$

This type of permutation f is called a cyclic permutation of length k and degree n. it is represented by $(a_1\ a_2\ \dots a_k)$ which is a cycle of length k or k – cycle.

Thus, the number of elements permuted by a cycle is called its length.

Transposition:

A cycle of length 2 is called a transposition.

Disjoint Cycles:

Let S = { a_1, a_2, … a_n}. If f, g be two cycles on S such that they have no common elements, then they are called disjoint cycles.

Note:

- The multiplication of disjoint cycles is commutative.
- Every permutation can be expressed as a product of disjoint cycles, which is unique.
- Every cycle can be expressed as a product of transpositions.
- Every permutation can be expressed as a product of transpositions in many ways.

Even and Odd permutations:

A permutation is said to be even (odd) permutation if it can be expressed as a product of an even (odd) number of transpositions.

Note:

- If f is expressed as a product of n transpositions, then either n is even or n is odd but cannot be both and n is not unique.
- Every transposition is an odd permutation.
- Identity permutation I is always an even permutation.
- A cycle of length n can be expressed as a product of (n – 1) transpositions. If n is odd, then the cycle can be expressed as a product of even number of transpositions. If n is even, then the cycle can be expressed as a product of odd number of transpositions.
- The product of two odd permutations is an even permutation.
- The product of two even permutations is an even permutation.
- The product of an odd permutation and an even permutation is an odd permutation.
- The inverse of an odd permutation is an odd permutation.
- The inverse of an even permutation is an even permutation.
- Let S_n be the permutation group on n symbols. Then of the n! permutations in (n! / 2) are even permutations and (n! / 2) are odd permutations.
- The set A_n of all even permutations of degree n forms a group of order (n! / 2) w.r.t. permutation multiplication.
- The set A_n of all even permutations on n symbols is a normal subgroup of the permutation group S_n on the n symbols.
- **Cayley's theorem:** Every finite group G is isomorphic to a permutation group.

Cyclic Groups

If G is a group and there is an element a $\in$ G such that G = { a^n / n $\in$ Z }. Then G is called a cyclic group and 'a' is called a generator of G. we denote G by < a > or (a) or {a}.

Note:

- Every cyclic group is an abelian group.
- If 'a' is a generator of a cyclic group G, then a^{-1} is also a generator of G.
- Every subgroup of cyclic group is cyclic.
- If G is a group of order pq where p, q are prime numbers, then every proper subgroup of G is cyclic.

- If a cyclic group G is generated by an element 'a' of order n, then a^m is a generator of G iff the greatest common divisor of m and n is 1. i.e m, n are relatively prime.
- The order of a cyclic group is equal to the order of its generator.
- Every isomorphic image of a group is again cyclic
- A cyclic group of order n has $\phi(n)$ generators.
- If G is an infinite cyclic group, then G has exactly two generators which are inverse of each other.
- Every group of prime order is cyclic
- The order of cyclic group is same as the order of its generator.
- Every group of order 3 is cyclic.
- An abelian group of order six is cyclic.

****