ips academy

Regenerating Mathematics

An ISO 9001 : 2008 Certified Institute

India's Pioneer Institute of

MATHEMATICS

NET/JRF | GATE | IIT-JAM | UPSC | M.Sc. Ent. (DU)

A High Quality Study Material
for
Higher Level Exam for U.G. & P.G. Students

Group Theory

Ph. : 011-26537527, 9999183434, 9899161734, 8588844789

MODERN ALGEBRA

GROUP THEORY

Put Your Own Notes

empty set is well define.

CHAPTER 1

SET AND RELATIONS

1.1. Set

A collection of well-defined objects or things is called set. By well-defined we mean there is no ambiguity / confusion regarding the inclusion or exclusion of any object.

Note:

(a) "This is widely accepted definition for the set but not absolute"

(b) Generally, sets are denoted by Capital letters whereas the objects collected in the set are called elements and denoted by small letters.

(c) When a set is formed by collecting objects, a new object is created different from the objects in that collection

(d) No set can be a member of itself i.e. if A is any set then $A \notin A$ but $A \subseteq A$.

Cardinality of Set: The number of elements in a set is called cardinality of the set. The cardinality of any set A is denoted by $|A|$ or card (A)

Subset: A set A is called a subset of the set B, if each element of A is also an element of B.

OR

Any sub-collection of elements from a set is called subset of that set. Symbolically, we write it as $A \subset B$ or $A \subseteq B$.

Note: If $A \subseteq B$ it includes the possibility $A = B$ whereas $A \subset B$ means there is at least one element in B which does not belong to A.

Power Set: Let S be any set .The collection of all the subsets of S is called power set of S, and denoted by $P(S)$. If $|S| = n$ then $|P(S)| = 2^{|S|} = 2^n$.

Example: Let $A = \{1,2,3\}$. Then Power set of A,

$P(A) = \{\phi, \{1\}, \{2\}, \{3\}, \{1,2\}, \{2,3\}, \{1,3\}, \{1,2,3\}\}$, Contains $2^3 = 8$ elements

Empty Set: The set without any element is called null / void / empty set and denoted by ϕ . It is subset of all the sets.

Note:

(a) $P(S)$, the power set too includes ϕ and S itself. Hence $P(S)$ is never empty for any S (even if S is empty).

(b) The cardinality of power set is always some power of 2. i.e. of the form 2^n, $n \in \mathbb{Z}^+ \cup \{0\}$. Hence, the name power set.

Propositions on Sets:

1. There is no set containing all the sets.
2. The empty set ϕ is subset of every set.
3. The power set of any set is never empty.

Laws and Theorems For Union & Intersection:

Let A, B, C be arbitrary sets. Then

1. **Idempotent**: $A \cup A = A$ & $A \cap A = A$
2. **Commutative:** $A \cup B = B \cup A$ & $A \cap B = B \cap A$
3. **Associative**: $A \cup (B \cup C) = (A \cup B) \cup C$ & $A \cap (B \cap C) = (A \cap B) \cap C$
4. **Identity laws**: ϕ is null set & U is superset of A
   (a) $A \cup \phi = A$
   (b) $A \cup U = U$
   (c) $A \cap \phi = \phi$
   (d) $A \cap U = A$
5. **Distributive Law**:
   (a) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
   (b) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
6. **Demorgan's Laws**: Let U be universal set and $A, B \subseteq U$
   (a) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
   (b) $(A \cap B)' = A' \cup B'$
   (c) $A - (B \cup C) = (A - B) \cap (A - C)$
   (d) $A - (B \cap C) = (A - B) \cup (A - C)$
7. **Important Theorem:** If $P(A)$ & $P(B)$ are power sets of A and B. Then
   (a) $P(A) \cap P(B) = P(A \cap B)$
   (b) $P(A) \cup P(B) \subseteq P(A \cup B)$
8. **More Results**:
   (a) $(A \cup B) \cap (A \cup B)' = \phi$
   (b) $(A - B) \cup (B - A) \cup (A \cap B) = A \cup B$
   (c) $A - (A - B) = A \cap B$
   (d) $A - B = B - A \Leftrightarrow A = B$
   (e) $A \cup B = A \cap B \Leftrightarrow A = B$
   (f) $A \subseteq B \Leftrightarrow B' \subseteq A'$
   (g) $A - B = B' - A'$

   Hint: $A \cap B^c$

   $B^c \cap (A^c)^c = A \cap B^c$

Put Your Own Notes

1.2. Relations and Counting of Relations

Put Your Own Notes

Cartesian Product: Let X and Y be two sets. Then set $X \times Y = \{(a,b) : a \in X, b \in Y\}$, is called Cartesian product of X and Y. If $|X| = n, |Y| = m$ then $|X \times Y| = m.n$

Properties on Cartesian Product:

1. $X \times Y \neq Y \times X \Leftrightarrow X \neq Y$, where $X \neq \phi, \quad Y \neq \phi$
2. If $X \cap Y = \phi \Rightarrow (X \times Y) \cap (Y \times X) = \phi$
3. If $|X \cap Y| = r \Rightarrow |(X \times Y) \cap (Y \times X)| = r^2$
4. If either $X = \phi, Y = \phi$. Then $X \times Y = \phi$ and $Y \times Y = \phi$.

Relation: A subset of $X \times Y$ is called a relation from X to Y or a binary relation from X to Y.

Number of Relations: Total number of relation from X to Y is equal to the number of subsets of $X \times Y$ i.e., $|P(X \times Y)|$ or number of element in the power set of $X \times Y$ i.e., $2^{|X \times Y|} = 2^{n.m}$

Binary Relation: A subset S of $A \times A$ is called a binary relation on A or simply a relation on A if for $a, b \in A, (a,b) \in S$ and then we write aSb and say a is related to b.

Number of binary relations on a set: Let A be a set such that $|A| = n$. Then $A \times A$ have n^2 elements. So, every subset of $A \times A$ is a relation implies total number of relations on A is $= |P(A \times A)| = 2^{n^2}$

Types of Relations:

Empty relation: As ϕ is subset of every set hence $\phi \subset A \times A$ is also a relation on A called **Empty relation.** i.e., no any pair of element satisfies the given condition.

Identity Relation: A subset I of $A \times A$ is called Identity relation on A if $a \in A$ then $(a,a) \in I$ and $(a,b) \notin I$ if $a \neq b$.

Let $A = \{a_1, a_2, ..., a_n\}$ be a set of n elements. Then a subset $I = \{(a_1,a_1), (a_2,a_2), ..., (a_n,a_n)\}$ of $A \times A$ is called identity relation.

Note:

(a) On a set a relation is said to be identity if every element of A is related to itself only.

(b) Identity relation is unique for each set A.

Reflexive relation: A relation S on a set A is called **Reflexive relation** if Every element of A must related to itself i.e. a subset S of $A \times A$ is called reflexive relation on A, if $\forall a \in A \ (a,a) \in S$

→ $I \subseteq S$
↓
identity

Properties:

(i) Total number of reflexive relation on $A = 2^{n^2-n}$, where $|A| = n$

Example: Number of reflexive relations on a set $A = \{1,2,3\}$ is 64

(ii) Empty relation on non-empty set is never Reflexive relation.

(iii) Empty relation on empty set is always Reflexive relation.

(iv) The least cardinality of a Reflexive relation on a set with n elements is n.

Irreflexive Relation: A subset S of $A \times A$ is irreflexive if $\forall a \in A \Rightarrow (a,a) \notin S$, i.e. S is Irreflexive relation on A if no element of A is related to itself.

Properties:

(i) Total number of irreflexive relations on $A = 2^{n^2-n}$

Example: Number of irreflexive relations on a set $A = \{1,2,3\}$ is 64

(ii) Irreflexive relation is not an exact negation of reflexive relation i.e., there exist some relations on set A which are reflexive as well as Irreflexive.

(iii) Empty relation on an empty set is Reflexive relation as well as Irreflexive relation

(iv) There Does not exist any non-empty relation which is reflexive as well as Irreflexive relation

(v) There are relations, which are neither reflexive nor Irreflexive.

Example: If $A = \{a,b\}$, then relation $S = \{(a,a),(a,b)\}$ is neither reflexive nor Irreflexive

Symmetric Relation: A relation S on a set A is called symmetric if $(b,a) \in S$ whenever $(a,b) \in S$ for $a,b \in A$ i.e. a relation is symmetric if and only if a is related to b implies that b is related to a

Properties:

(i) Number of Symmetric relations $= 2^{\sum n}$

Example: Number of Symmetric relations on a set $A = \{1,2,3\}$ is 64

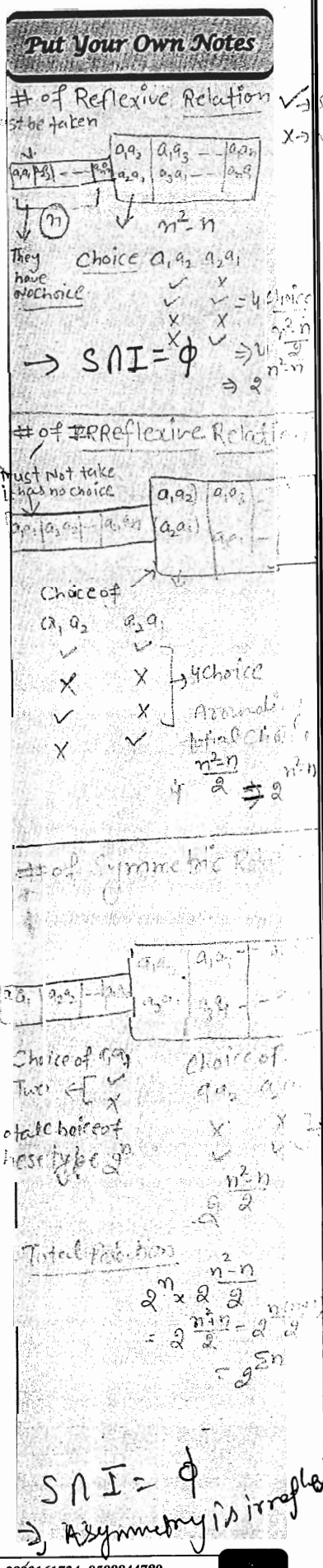
(ii) Empty relation is always symmetric relation on any set A as $\nexists$ any $(a,b) \in S$ such that $(b,a) \notin S$.

(iii) Identity relation is symmetric relation but $\exists$ some relations which are symmetric but not identity.

Example: Let $R = \{1,2,3\}$ and $R = \{(1,2),(2,1)\}$ be a relation on A. Then R is symmetric relation on A but not identity relation.

Asymmetric Relation: A relation S defined on A is called asymmetric whenever $(a,b) \in S \Rightarrow (b,a) \notin S$

Put Your Own Notes



Properties:

(i) Total number of Asymmetric relation $= 3^{\sum(n-1)}$

Example: Number of Asymmetric relations on a set $A = \{1,2,3\}$ is 27.

(ii) Asymmetric relation is not an absolute negation of Symmetric relation.

(iii) Empty relation is both Asymmetric as well as Symmetric.

(iv) A non-empty relation cannot be both Asymmetric as well as Symmetric.

(v) A relation can be neither symmetric nor a Asymmetric

Example: If $x \in A$, then relation $S = \{(a,a),(a,b)\}$ is neither symmetric nor a Asymmetric.

(vi) A non-empty reflexive relation cannot be Asymmetric.

Anti-symmetric Relation: A relation S on a set A is called Anti-symmetric Relation if $(a,b) \in S$ and $(b,a) \in S \Rightarrow a = b$ for $a,b \in A$

Properties:

(i) Number of Anti-symmetric relations on $A = 2^n 3^{\sum(n-1)}$

Example: Number of Anti-symmetric relations on a set $A = \{1,2,3\}$ is 6^3

(ii) Empty set is always anti-symmetric.

(iii) A relation is anti-symmetric if and only if there are no pairs of distinct elements a and b with a related to b and b related to a.

(iv) The terms symmetric & anti-symmetric are not opposite.

(v) A relation can be both symmetric & anti-symmetric.

Example: If $x \in A$, then relation $S = \{(a,a),(b,b)\}$ is both symmetric & anti-symmetric

(vi) A relation cannot be both symmetric and anti-symmetric if it contains some pair of the form (a,b) where $a \neq b$.

(vii) Every asymmetric relation is anti-asymmetric as well but not converse.

Example: Let $A = \{1,2,3\}$ and $R = \{(1,1),(2,2)\}$ be a relation on A. Then R is Anti-symmetric but not Asymmetric.

Transitive Relation: A relation S on a set A is called transitive if $(a,b) \in S$ and $(b,c) \in S$, then $(a,c) \in S$ for $a,b,c \in A$

Properties:

(i) Empty set is always Transitive Relation

(ii) If $S \subseteq A \times A$, be a relation failing to be transitive it must have at least one pair of ordered pair like $(a,b) \& (b,c) \in S$ and $(a,c) \notin S$.

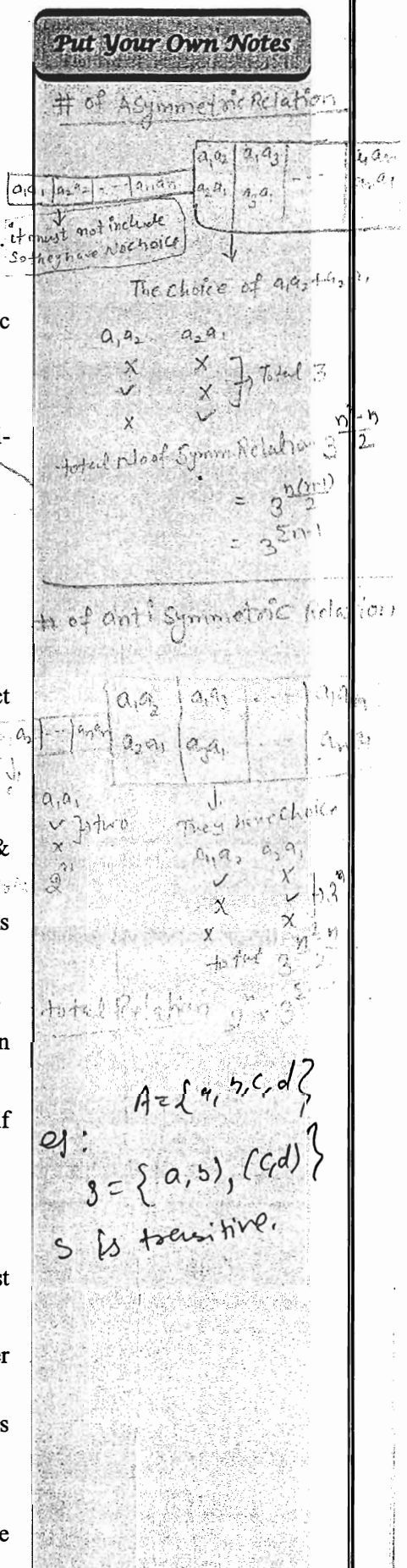
Example: Blood Relation is not transitive. As mother related to daughter and daughter related to father. But mother does not related to father.

Equivalence Relation: Any relation on a set A i.e., a subset of $A \times A$ is called an equivalence relation if it is reflexive, symmetric & transitive.

Example: Relation of parallel lines on a set of lines in a plane

Example: Relation of brother-hood over set of male's an equivalence relation

Put Your Own Notes



Equivalence Class: Let S be an Equivalence Relation on a set A and $a \in A$. Then the set defined and denoted as $cl(a) = \{x \in A \mid (x,a) \in S\}$ is called an equivalence class of $a \in A$ by the relation S.

Note: The Equivalence classes are either disjoint or identical.

Quotient Set: Let A be any non-empty set and $\sim$ be Equivalence relation on A. Then the set of all Equivalence Classes corresponding to the relation $\sim$ is called Quotient Set. This Quotient Set is denoted by $|A|_{\sim}$ i.e.,

$|A|_{\sim}$ = {Equivalence Classes corresponding to relation $\sim$ on set A}

Example: Let A = Set of Integers = $(\mathbb{Z})$ Let us define a relation $\sim$ on $\mathbb{Z}$ as $a \sim b$ iff $a-b$ is an even integer. Clearly, $\sim$ is an Equivalence relation on $\mathbb{Z}$

Now Equivalence Classes corresponding to $\sim$ are following:

$cl[0] = \{b \in \mathbb{Z} : b \sim 0\} = \{b \in \mathbb{Z} : b - 0 \text{ is even integer}\} = \{\text{even integers}\}$

$cl[1] = \{b \in \mathbb{Z} : b \sim 1\} = \{b \in \mathbb{Z} : b - 1 \text{ is even integer}\} = \{\text{odd integers}\}$

Thus, Quotient Set is {even integers, odd integers = Q[0], Q[1]}

Partial Ordered Relation: Any relation on a set A i.e., a subset of $A \times A$ is called a Partial Ordered Relation if it is reflexive, anti-symmetric and transitive. The set A with partial ordered relation R is called POSET and denoted by (A,R).

Example: Divisibility is Partial Ordered Relation over set of Natural numbers.

Example Divisibility is Partial Ordered Relation over set of Natural numbers.**:**

Partition of A Set: Let A be a set and $A_1, A_2, ..., A_n$ are subsets of A then the collection of these subsets defines a partition of A if

(i) They are disjoint i.e. $A_i \cap A_j = \phi, \forall i \neq j$

(ii) $A = \bigcup_{i}^{n} A_i$

Example: $A = \mathbb{N}$ then $\{A_1, A_2\}$ is a partition of A, where A_1 = set of even numbers $\subseteq N$ and A_2 = set of odd numbers $\subseteq N$

Example: A_1 = set of prime numbers, A_2 = set of composite numbers, $A_3 = \{1\}$ then A_1, A_2, A_3 form a partition of $\mathbb{N}$.

Example: $A = \{1,2,3,4\}$ let A_1, A_2 be subsets of A as $A_1 = \{1,2\}$ $A_2 = \{3,4\}$ .Then A_1, A_2 forms a partition of A.

Fundamental Theorem on Equivalence Relation (FTR): "Every equivalence relation on a set partitions the set into disjoint subsets. These subsets are called equivalence classes and conversely". If R is an equivalence relation on A and if $a \in A$, then by equivalence class of a written as $cl(a)$ or $[a]$ or $\bar{a}$ we mean $cl(a) = \{x \in A \mid xRa\}$

Put Your Own Notes

eg: $A = \{a,b,c,d\}$

$S = \{(a,a), (b,b), (c,c)\}$

$x_a = \{x \in A \mid xRa\}$

$= \{a, b\}$

$x_b = \{\}$

$x_c = \{a\}$

$x_d = \{\}$

$A|_R = \{cl(a) \; ; a \in A\}$

= set of all distinct eq. class

= The quotients set of A by R

Any equivalence relation R on A

$A|_R \subseteq P(A)$

if $A = \{a\}$ then

$R|_A = \{a\}$

if $A \neq \phi$

then $R|_A \neq P(A)$

$R|_A \subseteq P(A)$

Propositions on Equivalences Classes: If R is an equivalence relation on A and $a,b \in A$ then

(i) Either $cl(a) = cl(b)$ or $cl(a) \cap cl(b) = \phi$

(ii) $cl(a) = cl(b) \Leftrightarrow aRb$

(iii) Total number of equivalence relations on A = Total number of partitions of A

(iv) If $P(r)$ denotes the number of equivalence relations on a set with r elements. Then $P(0)=1, P(1)=1, P(2)=2, P(3)=5, P(4)=15$

(v) In general, $P(n+1) = \sum_{r=0}^{n} {}^{n}C_{r} P(r)$

Tabular Form for Number of Partitions of a Set

$P(1) =$ [1]

$P(2) = 1 \rightarrow$ [2]

$P(3) = 2 \rightarrow 3 \rightarrow$ [5]

$P(4) = 5 \rightarrow 7 \rightarrow 10 \rightarrow$ [15]

$P(5) = 15 \rightarrow 20 \rightarrow 27 \rightarrow 37 \rightarrow$ [52]

$P(6) = 52 \rightarrow 67 \rightarrow 87 \rightarrow 114 \rightarrow 151 \rightarrow$ [203]

$P(7) = 203 \rightarrow 255 \rightarrow 322 \rightarrow 409 \rightarrow 523 \rightarrow 674 \rightarrow$ [877]

Congruence Relation of $\mathbb{Z}$ (The set of integers): Let $a,b \in \mathbb{Z}$ and m be a positive integer. Then we say a is congruent to b modulo m iff $m|(a-b)$, symbolically $a \equiv b(\text{mod}\, m)$ and read as a is congruent to b modulo m

Properties:

(i) Congruence relation is an equivalence relation

(ii) If $a \equiv b(\text{mod}\, m)$ then a & b both leave the same remainder when divided by m.

(iii) If $ca \equiv cb(\text{mod}\, m) \Rightarrow a \equiv b(\text{mod}\, m/d)$, where $d = g.c.d(c,m)$

(iv) If $a \equiv b(\text{mod}\, m)$ and $c \equiv d(\text{mod}\, m)$ then $a+c \equiv b+d(\text{mod}\, m)$ & $ac \equiv bd(\text{mod}\, m)$

(v) If $a \equiv b(\text{mod}\, m) \Rightarrow a^k \equiv b^k(\text{mod}\, m)$ for any positive integer k. Converse need not be true.

Note: $a^2 \equiv b^2(\text{mod}\, m)$ need not imply that $a \equiv b(\text{mod}\, m)$. For example : $3^2 \equiv 2^2 \text{ mod } 5$ but $3 \not\equiv 2 \text{ mod } 5$

(vi) If $c.a \equiv c.b(\text{mod}\, p) \,\&\, p \nmid c$ then $a \equiv b(\text{mod}\, p)$ where p is prime number.

(vii) $a \equiv b(\text{mod}\, m) \Rightarrow g.c.d(a,m) = g.c.d(b,m)$

Put Your Own Notes

Put Your Own Notes

Some Important Theorems:

Fermat's Theorem: If p is prime, then $a^p \equiv a(\text{mod } p)\ \ \forall a \in \mathbb{Z}$

Fermat's Little Theorem: If p is prime, then $a^{p-1} \equiv 1(\text{mod } p)$ and point $a\ \ \forall a \in \mathbb{Z}$. Converse of Fermat's theorem need not be true.

Wilson's Theorem: If p is a prime number , then $(p-1)! \equiv -1(mod\ p)$ or $(p-1)!+1 \equiv 0(mod\ p)$

Converse of Wilson's Theorem: If $(m-1)!+1$ is divisible by m, then m is a prime number.

Pseudo Prime: A composite integer n is called pseudo prime if it satisfies the congruence equation $2^n \equiv 2(mod\ n)$.

Note: Upto 340, integers which satisfies above equation are prime only and 341 is the first composite which satisfies the above equation and is the smallest pseudo prime. Few next pseudo primes are 641, 645.

Congruence Equation: Let $a,b \in \mathbb{Z}$ and n is a positive integer. Then $ax = b(\text{mod}\, n)$ is congruence Equation.

Rule: The linear congruence $ax = b(\text{mod}\, n)$ has a solution iff $g.c.d(a,n) = d \mid b$; and it has exactly d mutually incongruent solutions modulo n.

Some important Properties:

(i) Let $P(x) = \sum_{i=0}^{m} a_i x^i, a_i \in \mathbb{Z}$ be a polynomial and $a \equiv b(\text{mod}\, n)$. Then $P(a) \equiv P(b)(\text{mod}\, n)$

(ii) If p is prime number and $d \mid (p-1)$. Then the congruence equation $x^d \equiv 1(\text{mod}\, p)$ or $x^d - 1 \equiv 0(\text{mod}\, p)$ has exactly d solutions.

(iii) Let a be an odd integer. Then

(a) $x^2 \equiv a(\text{mod}\, 2)$ always has a solution

(b) $x^2 \equiv a(\text{mod}\, 4)$ has a solution iff $a \equiv 1(\text{mod}\, 4)$

(c) $x^2 \equiv a(\text{mod}\, 2^n)$; *for* $n \geq 3$ has a solution iff $a \equiv 1(\text{mod}\, 8)$

Diophantine Equation: Let $a,b,c \in \mathbb{Z}$ such that $a \neq 0, b \neq 0$. An equation of the form $ax + by + c = 0$ is called Diophantine equation. The integers x_0, y_0 is said to be solution of equation $ax + by + c = 0$ if $ax_0 + by_0 + c = 0$.

Note: $ax + by + c = 0$ has solution $(a \neq 0, b \neq 0)$ if and only if $d \mid c$ where $d = g.c.d(a,b)$. If x_0, y_0 is any particular solution of $ax + by + c = 0$ then all other solution of this equation are given by $x = x_0 + \frac{b}{d}t$ and $y = y_0 - \frac{a}{d}t$ varying over integers t

Put Your Own Notes

Example: Find the remainder when 2^{50} divided by 7.

$2^1 \equiv 2(\text{mod } 7) \Rightarrow 2^2 = 4(\text{mod } 7) \Rightarrow 2^3 \equiv 8(\text{mod } 7) \Rightarrow 2^3 \equiv 1(\text{mod } 7)$

$\Rightarrow (2^3)^{16} \equiv 1(\text{mod } 7)$

$\Rightarrow 2^{48} \equiv 1(\text{mod } 7) \quad \Rightarrow 2^{48} \cdot 2^2 \equiv 4(\text{mod } 7) \quad \Rightarrow 2^{50} \equiv 4(\text{mod } 7)$ Thus, 4 is remainder when 2^{50} is divided by 7.

Example: Find the remainder if 3^{40} is divided by 23.

Solution:

$3^1 \equiv 3(\text{mod } 23) \quad \Rightarrow 3^3 \equiv 9(\text{mod } 23) \quad \Rightarrow 3^3 \equiv 4(\text{mod } 23) \quad \Rightarrow (3^3)^3 \equiv -5(\text{mod } 23)$
$\Rightarrow 3^9 \equiv -5(\text{mod } 23)$

$\Rightarrow 3^{18} \equiv 2(\text{mod } 23) \Rightarrow 3^{36} \equiv 4(\text{mod } 23) \Rightarrow 3^{36} \equiv 4(\text{mod } 23)$
$\Rightarrow 3^{36} \cdot 3^3 \equiv 16(\text{mod } 23) \Rightarrow 3^{39} \equiv 16(\text{mod } 23)$

$\Rightarrow 3^{39} \cdot 3 \equiv 3.16(\text{mod } 23) \Rightarrow 3^{40} \equiv 2(\text{mod } 23)$ Thus, 2 is remainder.

Example: Find the remainder obtained by dividing $1!+2!+3!+4!+.....+100!$ by 12.

Solution: Since $4! \equiv 24 \equiv 0(\text{mod } 12)$ Thus for $k \geq 4$ $k! = 4! 5 \cdot 6..... k \equiv 0 \cdot 5 \cdot 6....k \equiv 0(\text{mod } 12)$ In this way, we get, $1!+2!+3!+4!+.....+100! \equiv 1!+2!+3!+0+....+ \equiv 9(\text{mod } 12)$, 9 is the required remainder.

Linear Congruence: A polynomial congruence of degree 1 is a linear congruence. Any linear congruence can be written in the form $ax \equiv b(\text{mod } m)$ where a is not congruent to 0 mod m i.e., a is not divisible by m.

Solution of Linear Congruence: An integer x_1 is said to be a solution of the linear congruence $ax \equiv b(\text{mod } m)$ if $ax_1 \equiv b(\text{mod } m)$ i.e. if $m \mid (ax_1 - b)$

Properties:

(i) A linear congruence may or may not have a solution.

(ii) The linear congruence $ax \equiv b(\text{mod } m)$ has a solution if and only if g.c.d (a, m) divides b.

(iii) If g.c.d $(a, m) = 1$, the congruence $ax \equiv b(\text{mod } m)$ has a unique solution.

Example: Find the number of solutions of $3x \equiv 5(\text{mod } 7)$.

Solution: The given congruence is $3x \equiv 5(\text{mod } 7)$. On comparing with $ax \equiv b(\text{mod } m)$ we have $a = 3, b = 5$ and $m = 7$ Since $d = g.c.d(a, m) = g.c.d(3, 7) = 1$, which divides $b = 5$ Hence the congruence $3x \equiv 5(\text{mod } 7)$ has one and only one incongruent solution (moulo 7)

Chinese Remainder Theorem: If $(m, n) = 1$ then we can find integers u and v such that $mu + nv = 1$ and then $x = bmu + anv(\text{mod } mn)$ is solution of this system.

Important Result

Let p be a prime number. The least value of m such the p^m divide $n!$ but p^{m+1} does not divide $n!$, where n is natural number greater than 1, is

$$m = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + ...$$

Put Your Own Notes

1.3. Functions and Their Properties

Definition: Let A and B be non-empty sets. Then a function f from A to B is a rule which assigns each element of A to a unique element of B.

We write $f(a)=b$, if b is the unique element of B assigned by the function f to the element a of A. b is called image of a under f and a is called a pre-image of b.

Note: A is called domain of f; B is called co-domain of f and the collection of all images is called range of f. Clearly $range\ f \subseteq B$

Types of Function:

Let $f: A \to B$ be a function. Then f is said to be

One-one (injective): If $f(x_1)=f(x_2) \Rightarrow x_1 = x_2$ i.e. no two elements of A have same images.

Many–one: If at least two elements of A have same image.

Onto (Surjective): If $range\ f = B$ i.e. every element of B has pre image.

Into: If $range\ f \subset B$ i.e., range f is proper subset of co-domain **OR** there exists at least one element of B which has no pre-image in A.

Bijection: A map (function) which is one–one & onto both is called bijection.

Inverse: If $f: A \to B$ and f is a bijection. Then $f^{-1}: B \to A$ such that if $f(a)=b \Rightarrow f^{-1}(b)=a$ is called Inverse map of f.

Note: A function $f: A \to B$ is invertible $\Leftrightarrow$ f is bijective.

1.4. Number Theoretic Functions

Euler's ϕ – Function: It is a function from $\mathbb{Z}^+$ to $\mathbb{Z}^+$, denoted by $\phi: \mathbb{Z}^+ \to \mathbb{Z}^+$ and defined as $\phi(n)$ = number of natural number which are less than or equal to n and co-prime to n.

Properties on Euler's ϕ – function:

(i) If $n = p^a q^b r^c ...$, where $p,q,r....$ are primes and $a,b,c \in \mathbb{Z}^+$ then

$$\phi(n) = n\left(1-\frac{1}{p}\right)\left(1-\frac{1}{q}\right)\left(1-\frac{1}{r}\right)$$

(ii) For positive integer n, $\phi(n)=(n-1) \Leftrightarrow n$ is prime number.

(iii) If p is prime and $k>0$, then $\phi(p^k) = p^k\left(1-\frac{1}{p}\right) = p^k - p^{k-1}$

(iv) $\phi(2n)=\phi(n)$, if n is odd positive integer

Put Your Own Notes

(v) The sum of positive integers which are less than n and co-prime to n is $\frac{n\phi(n)}{2}$, for $n>1$

(vi) $\phi(n)$ tends to infinity as n tends to infinity

(vii) If n and d are two positive integers such that d divides n, $(d \mid n)$ then $\phi(d)$ divides $\phi(n)$ i.e. $\phi(d) \mid \phi(n)$

(viii) $\phi(m.n) = \phi(m)\phi(n)$, if $\gcd(m,n)=1$ i.e. if m and n are co-prime

(ix) $\phi(n_1 n_2 ... n_k) = \phi(n_1)\phi(n_2)...\phi(n_k)$ if $n_1, n_2, ..., n_k$ are pair wise co-prime number i.e. $g.c.d.(n_i, n_j) = 1 \ \forall \ i \neq j$

(x) $\phi(n)$ is an even number $\forall\ n \geq 3$.

(xi) $\phi(n)$ function is neither one-one nor onto.

Euler's Theorem: Let a be any integer and n be any positive integer such that a and n are co-prime then $a^{\phi(n)} \equiv 1 (\text{mod } n)$

Gauss Theorem: For each $n \in \mathbb{Z}^+$, $n = \phi(d_1) + \phi(d_2) + ... + \phi(d_k)$ where $d_1, d_2 ... d_k$ are positive divisors of n

Tau- function $\tau(n)$: It is a function from $\mathbb{Z}^+$ to $\mathbb{Z}^+$ denoted by $\tau : \mathbb{Z}^+ \to \mathbb{Z}^+$ and defined as $\tau(n)$ = number of positive divisors of n.

Properties on Tau- function $\tau(n)$:

(i) If $n = p^a q^b r^c ...$, are prime numbers and $a, b, c, ...$ are natural numbers. Then $\tau(n) = (a+1)(b+1)(c+1)...$ = number of positive divisors of n

(ii) If $(m,n)=1$ i.e., m and n are co-prime. Then $\tau(m.n) = \tau(m).\tau(n)$

(iii) If $n \in \mathbb{Z}^+$ then $\tau(n) = 2 \Leftrightarrow n$ is prime

(iv) For $n \in \mathbb{Z}^+$ and $n > 1$. Then $\tau(n)$ is odd $\Leftrightarrow$ n is perfect square i.e. $n = m^2$ for some $m \in \mathbb{Z}^+$

(v) If $n > 1$ be an integer, then product of all positive divisors of n is $\frac{n\tau(n)}{2}$

(vi) $\tau(n) \geq 2 \ \forall n > 1, \ n \in \mathbb{Z}^+$

(vii) $\tau(n) \to \infty$ as $n \to \infty$.

Put Your Own Notes

Sigma-function $\sigma(n)$: It is a function from $\mathbb{Z}^+$ to $\mathbb{Z}^+$ denoted by $\sigma:\mathbb{Z}^+\to\mathbb{Z}^+$ and defined as $\sigma(n)$ = sum of positive divisors of n.

Properties on Sigma-function $\sigma(n)$

(i) If $n=p^aq^br^c...$ where $p,q,r,...$ are primes and $a,b,c,...\in\mathbb{Z}^+$. Then

$$\sigma(n)=\frac{\left(p^{a+1}-1\right)}{(p-1)}.\frac{\left(q^{b+1}-1\right)}{(q-1)}...$$

(ii) If $(m,n)=1$ i.e., m and n are co-prime. Then $\sigma(mn)=\sigma(m).\sigma(n)$

(iii) For integer $n>1$, $\sigma(n)$ =odd number $\Leftrightarrow n$ is a perfect square or twice of a perfect square

(iv) $\sigma(n)\to\infty$ as $n\to\infty$

1.5. Some of the Tests of Divisibility:

1. For every N be any positive integer N is of the form $a_ka_{k-1}a_{k-2}...a_2a_1a_0$ where $a_i\in\{0,1,2,...,9\}\ \forall i=0,1,.....k$

   Example: $N=20691$ then $a_4=2,a_3=0,a_2=6,a_1=9,a_0=1$

2. N is divisible by $2\Leftrightarrow a_0$ is divisible by $2\Leftrightarrow$ last terms is divisible by 2.
3. N is divisible by $3\Leftrightarrow$ sum of $a_0,a_1,...,a_k$ is divisible by 3 i.e. $a_0+a_1+...+a_k$ is divisible by 3.
4. N is divisible by $4\Leftrightarrow a_1a_0$ is divisible by 4 i.e. last two terms are divisible by 4.
5. N is divisible by $5\Leftrightarrow$ either $a_0=0$ or $a_0=5$
6. N is divisible by $6\Leftrightarrow N$ is divisible by 2 and 3 both
7. N is divisible by $7\Leftrightarrow(a_2a_1a_0)-(a_5a_4a_3)+(a_8a_7a_6)...$ is divisible by 7.

   Example: If $N=2\underline{587}\underline{322}\underline{568}\underline{103}$ As $103-568+322-587+2=-728$, which is divisible by 7. So N is divisible by 7.

8. N is divisible by $8\Leftrightarrow a_2a_1a_0$ is divisible by 8 i.e. last three digits must be divisible by 8.
9. N is divisible by $9\Leftrightarrow$ sum of $a_0,a_1,a_2,...,a_k$ is divisible by 9 i.e. $a_0+a_1+...+a_k$ is divisible by 9.
10. N is divisible by $10\Leftrightarrow a_0=0$

Put Your Own Notes

11. N is divisible by 11 $\Leftrightarrow$ 11 divide $(a_0 - a_1 + a_2 ... + (-1)^k a_k)$

Example: If $N = 1571427$ As $1-5+7-1+4-2+7=11$, which is divisible by 11 so N is divisible by 11

12. N is divisible by 12 $\Leftrightarrow$ N is divisible by 4 and 3 both

13. N is divisible by 13 $\Leftrightarrow (a_2a_1a_0)-(a_5a_4a_3)+(a_8a_7a_6)...$ is divisible by 13.

14. N is divisible by 14 $\Leftrightarrow$ N is divisible by 2 and 7 both

15. N is divisible by 15 $\Leftrightarrow$ N is divisible by 3 and 5 both

16. N is divisible by 37 if $(a_2a_1a_0)+(a_5a_4a_3)+...$ is divisible by 37

Example: If $N = 22125744515$ As $515+744+125+22=1406$, which is divisible by 37, then N is divisible by 37.

Put Your Own Notes

CHAPTER 2

BASIC ALGEBRAIC STRUCTURE

2.1. Self Contained System

Binary Operation and Algebraic Structure:

Binary Operation: Let G be a non-empty set. Any mapping or function from $G\times G$ to G itself is called binary operation on a set G i.e., a function $f: G\times G \to G$ is a binary operation on set G

Number of binary operations: Number of binary operation on a non-empty finite set G with cardinality n is n^{n^2}

Algebraic Structure: A non-empty set equipped with one or more binary operations is called algebraic structure. The algebraic structure consisting of a set G and binary operations $*$, $\circ$ on G is denoted by $(G, *, \circ)$

Notations:

$+$ = Ordinary addition of complex numbers

$\bullet$ = Ordinary multiplication of complex numbers

$-$ = Ordinary subtraction of complex numbers

Examples of Binary operation and algebraic structures:

1. Let us consider $G = \mathbb{N}$(set of natural numbers). If $\forall a,b \in \mathbb{N}$, we define '$*$' on $\mathbb{N}$ as

   (i) $a*b = a+b$, then $(\mathbb{N},+)$ is algebraic structure since sum of two natural numbers is again natural number.

   (ii) $a*b = \min\{a,b\}$. then $(\mathbb{N},*)$ is algebraic structure.

   (iii) $a*b = \max\{a,b\}$ then $(\mathbb{N},*)$ is algebraic structure.

   (iv) $a*b = LCM\{a,b\}$ then $(\mathbb{N},*)$ is algebraic structure.

   (v) $a*b = HCF\{a,b\}$ then $(\mathbb{N},*)$ is algebraic structure.

   (vi) $a*b = a-b$. Then '$*$' is not binary operation on N as for $2 \& 1 \in \mathbb{N}$ but $1-2 = -1 \notin \mathbb{N}$

   (vii) $a*b =$ at most 5 more than $a+b$. Then '$*$' is not **binary operation** on $\mathbb{N}$ as for $1,2 \in \mathbb{N}$ $1*2 = 3$ or 4 or 5 or 6, which not unique.

2. For $G = \mathbb{R}$ =(set of real numbers). If $\forall\ a,b \in \mathbb{R}$, we define '$*$' on $\mathbb{R}$ as

   (i) $a*b = a+b$ then $(\mathbb{R},+)$ is algebraic structure.

   (ii) $a*b = \min\{a,b\}$ $(\mathbb{R},*)$ is algebraic structure.

   (iii) $a*b = a^b$ then '$*$' is not binary operation on G as for $a = -1 \& b = \frac{1}{2}$, then $a*b = (-1)^{1/2} = i \notin \mathbb{R}$

   (iv) $a*b = a-b$ then $(\mathbb{R},-)$ is algebraic structure.

Put Your Own Notes

3. $G = P(\mathbb{N})$ (power set of natural numbers). If $\forall\ A, B \in P(\mathbb{N})$, define '$*$' as

(i) $A * B = A \cup B$, as union of two subset of $\mathbb{N}$ is again subset of $\mathbb{N}$ $\Rightarrow A * B \in P(\mathbb{N}) \Rightarrow (P(\mathbb{N}), \cup)$ is algebraic structure

(ii) $A * B = A \cap B$, then $A \cap B$, is again subset of $\mathbb{N}$ $\Rightarrow (P(\mathbb{N}), \cap)$ is algebraic structure

(iii) $A * B = (A - B) \cup (B - A)$ then $(P(\mathbb{N}), \Delta)$ algebraic structure and this binary operation is called symmetric difference of two sets and denoted as $A \Delta B = (A \cup B) - (A \cap B)$

4. $G = M_{n \times n}(\mathbb{R})$ (= set of all $n \times n$ matrices over set of real numbers). For $A = [a_{ij}], B = [b_{ij}]$, define '$*$' as

(i) $A * B = [a_{ij} * b_{ij}] = [c_{ij}]$ (= component wise multiplication). Clearly, $[c_{ij}]$ is $n \times n$ matrix over $\mathbb{R}$ $\Rightarrow$ $(G, *)$ is an algebraic structure

(ii) $A * B = [a_{ij} + b_{ij}]$ (component wise addition). Then $(G, *)$ is an algebraic structure

(iii) $A * B = [c_{ij}]$ matrix obtained by ordinary matrix multiplication then $(G, *)$ in an algebraic structure.

5. For $G = \mathbb{Z}$ (Set of integers). For every $a, b \in \mathbb{Z}$. Define '$*$' as

(i) $a * b = a + b$ then $(\mathbb{Z}, +)$ is an algebraic structure

(ii) $a * b = a - b$ then $(\mathbb{Z}, -)$ is an algebraic structure

(iii) $a * b = a.b =$ ordinary multiplication of integer. Then $(\mathbb{Z}, .)$ is an algebraic structure

Associative binary Operation: Let * be a binary operation * on a set G. Then if two or more elements operated together, we get a string. A binary operation is said to be associative if anywhere in the string brackets are inserted then the result is unchanged. It is property of binary operation alone not of the set. That is a binary operation * is called is associative if $\forall\ a, b, c \in G$, $a * (b * c) = (a * b) * c$.

Note: The associativity of a binary operation does not depend on the set. It is property of operation only i.e., once this holds, then will remain satisfy with every subset.

Commutative Binary Operation: Let * be a binary operation on G. Then * is said be commutative if and only if $a * b = b * a\ \forall a, b \in G$ i.e., each element of G commutes with each other.

Number of Commutative Binary Opertations: Under a commutative binary operation on a set G, ordered pairs (a, b) and (b, a) are mapped to the same element. So the total number of commutative binary operations on G of cardinality n is equal to $n^{\frac{n(n-1)}{2}+n} = n^{\frac{n(n+1)}{2}}$ and number of non-commutative binary operation $= n^{n^2} - n^{\frac{n(n+1)}{2}}$

Put Your Own Notes

Quasi Group / Groupoid: A non-empty set equipped with unique binary operations is called quasi group or groupoid.

Example: $(\mathbb{N}, +), (\mathbb{Z}, +), (\mathbb{Q}, \cdot), (\mathbb{Z}, -)$ are all Groupoid.

Semi-Group: A Quasi group in which binary operation is associative is called semi group.

Examples:

(i) $(\mathbb{N}, +), (\mathbb{N}, \cdot), (\mathbb{Z}, +), (\mathbb{Z}, \cdot), (\mathbb{Q}, +), (\mathbb{R}, \cdot) (\mathbb{R}^*, \cdot), (\mathbb{R}^+, \cdot)$ all are semi group

(ii) $(P(\mathbb{N}), \cup), (P(\mathbb{N}), \cap), (P(\mathbb{N}), \Delta)$ all are semi group.

(iii) $(Q^*, \div), (\mathbb{Z}, -)$ are not semi groups.

2.2. Status Quo and Inverse Element

Identity Element: Let G be a non-empty set and $*$ be a binary operation on G. Then the element $e \in G$ such that $x * e = e * x = x, \ \forall x \in G$. Then e is called identity element (neutral element) with respect to $*$.

Monoid: A semi group $(G, *)$ is said to be monoid if it has an identity element.

Examples:

1. $(\mathbb{N}, \cdot)$ is a monoid with identity element 1.
2. $(\mathbb{Z}, +)$ is a monoid with identity element 0.
3. $(P(\mathbb{N}), \cup)$ is a monoid with identity element, the null set ϕ.
4. $(P(\mathbb{N}), \cap)$ is a monoid with identity element, the set $\mathbb{N}$.
5. $(P(\mathbb{N}), \Delta)$ is a monoid with identity element, the null set ϕ.
6. $(\mathbb{R}, \cdot)$ is a monoid with identity element 1.

S. no.	Examples	Binary operation	Quasi group	Semi group	Monoid
1.	$(\mathbb{N}, *), a*b = L.C.M\{a,b\}$	Yes	Yes	Yes	$Y(e=1)$
2.	$(\mathbb{N}, *), a*b = H.C.F\{a,b\}$	Y	Y	Y	No
3.	$(\mathbb{N}, *), a*b$=1 less then $\min\{a,b\}$	No	No	No	No
4.	$(\mathbb{N}, *), a*b = a^b$	Y	Y	N	N
5.	$(\mathbb{N}, *), a*b$=at most $a+b$	N	N	N	N
6.	$(\mathbb{N}, *), a*b$=at least	N	N	N	N

	5 less than $a+b$				
7.	$(P(\mathbb{N}),*)$, $X*Y=X\cup Y$	Y	Y	Y	$Y(e=\phi)$
8.	$(P(\mathbb{N}),*)$, $X*Y=X\cap Y$	Y	Y	Y	$Y(e=\mathbb{N})$
9.	$(P(\mathbb{N}),*)$, $X*Y=X\Delta Y$	Y	Y	Y	$Y(e=\phi)$
10.	$(\mathbb{N},*)$, $a*b=(a+b+ab)$	Y	Y	Y	N
11.	$A=\mathbb{N}\cup\{1/n:n\in\mathbb{N}\}$ $a*b=ab$ (ordinary multiplication of $\mathbb{N}$)	N	N	N	N

Inverse Element: Let * be a binary operation on a set G and let e be the identity element in G for binary operation *. The element $a'\in S$ is said to be an inverse of $a\in S$ if $a*a'=a'*a=e$

1. In $(\mathbb{N},\cdot)$, the identity element is only element which has inverse .
2. In $(\mathbb{Z},+)$, every element has an inverse and for each $n\in\mathbb{Z}$ its inverse is $(-n)$.
3. In $(\mathbb{Z},\cdot)$ only 1 and -1 have inverse elements .
4. In $(P(\mathbb{N}),\cap)$, the identity element is $\mathbb{N}$, and only one element $\mathbb{N}$ has inverse.
5. In $(\mathbb{R},+)$, every element has an inverse.
6. In $(\mathbb{R},\cdot)$, every non zero element has an inverse.

Group: A Monoid in which each element has inverse, that is A non-empty set G with a binary operation $*$ is called a group if for every $a,b,c\in G$, the following properties hold:

$P_1:(a*b)*c=a*(b*c)$ called (Associative law)

P_2 : There exists $e\in G$ such that $a*e=e*a=a$

(Existence of identity element)

P_3 : For each $a\in G$ there exists $a^{-1}\in G$ such that $a*a^{-1}=a^{-1}*a=e$

(Existence of inverses)

Order of Group: Let $(G,*)$ be a group. The cardinality of G (finite or infinite) is defined as the order of group and it is denoted by $O(G)=|G|$

Put Your Own Notes

Abelian Group: A group in which binary operation is commutative. That is a non-empty set G with a binary operation $*$ is called a abelian group if for every $a,b,c \in G$, the following properties hold.

$P_1 : (a*b)*c = a*(b*c)$ (Associative law)

P_2 : There exists $e \in G$ such that $a*e = e*a = a$

(Existence of identity element)

P_3 : For each $a \in G$ there exists $a^{-1} \in G$ such that $a*a^{-1} = a^{-1}*a = e$

(Existence of inverses)

P_4 : For each $a,b \in G$ such that $a*b = b*a$

(Commutative binary operation)

Examples:

1. $(\mathbb{C},+)$ set of complex numbers under additions
2. $(\mathbb{R},+)$ set of real numbers under additions
3. $(\mathbb{Q},+)$ set of rational numbers under additions
4. $(\mathbb{Z},+)$ set of integers numbers under additions
5. $(\mathbb{C}^*,\bullet)$ set of non zero complex numbers under multiplication
6. $(\mathbb{R}^*,\bullet)$ set of non zero real numbers under multiplication
7. $(\mathbb{Q}^*,\bullet)$ set of non zero rational numbers under multiplication
8. $(P(\mathbb{N}),\Delta)$ power set of natural numbers under symmetric difference
9. $GL(n,F)$ the group of $n \times n$ matrices with non-zero determinant with entries from the **field** F under matrix multiplication is group named as General linear group is a non abelian
10. $SL(n,F)$ the group of $n \times n$ matrices with determinant 1 entries from the field F under matrix multiplication is group named as special linear group is non abelian group
11. The set $A = \left\{\omega_1 = \frac{-1+\sqrt{3}i}{2},\ \omega_2 = -\frac{1+\sqrt{3}i}{2},\ \omega_3 = 1\right\}$ of the cube roots of 1 forms abelian group with respect to multiplication of complex numbers $\mathbb{C}$ since

*	ω_1	ω_2	ω_3
ω_1	ω_2	ω_3	ω_1
ω_2	ω_3	ω_1	ω_2
ω_3	ω_1	ω_2	ω_3

Put Your Own Notes

Put Your Own Notes

2.3. Basic Properties of Group G

1. **Cancellation Law:**
   (i) Left cancellation law: If $a,b,c \in G$, then $ab = ac$ implies $b = c$
   (ii) Right cancellation law: If $a,b,c \in G$, then $ba = ca$ implies $b = c$
2. A finite semi-group in which both the cancellation law hold is a group
3. A finite semi-group G is a group if and only if G satisfies both the cancellation laws.
4. The identity element of a group is unique.
5. The inverse of each element in a group is unique.
6. $\forall a,b \in G$, each of the equations $ax = b$ and $ya = b$ has a unique solution.
7. For every $a \in G$, the inverse of the inverse of a is a, i.e., $\left(a^{-1}\right)^{-1} = a$.
8. (Reversal law) For every $a,b \in G$, $(ab)^{-1} = b^{-1}a^{-1}$ **(Also called socks-shoes property)**
9. For every $a_1, a_2, \ldots, a_n \in G$, $(a_1 \bullet a_2 \bullet \ldots \bullet a_n)^{-1} = a_n^{-1} \bullet a_{n-1}^{-1} \bullet \ldots \bullet a_1^{-1}$
10. For any $a \in G$, and $m \in \mathbb{Z}^+$, we define $a^m = aaa\ldots a$ (m times),
11. $a^{-m} = \left(a^{-1}\right)^m = a^{-1}a^{-1}a^{-1}\ldots a^{-1}$ (m times).

    Note: The notation has been borrowed from the notation of usual multiplication operation. Whenever the operation is addition, a^n when $n > 0$ is to be interpreted as $na = a + a + a + \ldots + a$ (n times), and a^{-n} as $n(-a) = (-a) + (-a) + (-a) + \ldots (-a)$ (n times). Note that na is also shorthand and is not to be considered as the product of $n \in \mathbb{Z}$ and $a \in G$

    For any $a \in G$,
12. For any $a \in G$,
13. $a^m\, a^n = a^{m+n}$, where $m,n \in \mathbb{Z}$.
14. $\left(a^m\right)^n = a^{mn}$, where $m,n \in \mathbb{Z}$.
15. If $a^m = e = a^n, m \neq 0, n \neq 0 \Rightarrow a^d = e$ where $d = \text{g.c.d.}(m,n)$.
16. The integral power of an element commutes with each other i.e., $a^m a^n = a^n a^m = a^{m+n}$

    Note: $(a * b)^{-2} \neq b^{-2} * a^{-2}$

Put Your Own Notes

CHAPTER 3

GROUPS WITHIN GROUPS

3.1. Subgroup

Let $(G, *)$ be a group and H be a non-empty subset of G, then H is called a subgroup of G if H itself is a group with respect to same binary operation defined on G. It is denoted by $H < G$.

Example:

(a) Set of even integers is subgroup of $(\mathbb{Z},+)$ i.e., $(2\mathbb{Z},+) < (\mathbb{Z},+)$

(b) $(\mathbb{Z},+)$ **Subgroup of** $(\mathbb{Q},+)$ **Subgroup of** $(\mathbb{R},+)$ **Subgroup of** $(\mathbb{C},+)$

(c) $(\mathbb{Q}^*,\cdot)$ **Subgroup of** $(\mathbb{R}^*,\cdot)$ **Subgroup of** $(\mathbb{C}^*,\cdot)$

(d) For each $\phi \neq X$ be a non empty subset of $\mathbb{N}$, $(P(X),\Delta)$ is a subgroup of $(P(\mathbb{N}),\Delta)$

One-step test for Subgroup: Let G be group and H a non-empty subset of G, then H is a subgroup of G iff $ab^{-1} \in H$ whenever a and b are in H. (In additive notation, H is a subgroup iff $a-b$ is in H whenever a and b are in H).

Example: Let $G = GL(2,\mathbb{R})$ and $H = \left\{\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} : a \neq 0 \text{ and } a,b \in \mathbb{R}\right\}$, then H is subgroup of G

Two-step test for Subgroup: Let G be a group and H a non-empty subset of G. Then H is a subgroup of G if $ab \in H \ \forall\, a,b \in H$ (closed under multiplication), and $a^{-1} \in H$ whenever $a \in H$ (closed under taking inverse).

Example: $H = \{(1,b) : b \in \mathbb{R}\}$ is a subgroup of the group $G = \{(a,b) : a \neq 0,\ b \in \mathbb{R}\}$ under the binary operation * given by $(a,b)*(c,d) = (ac, bc+d)$

Finite subgroup test: Let H be a non-empty finite subset of a group G. Then H is a subgroup of G if H is closed under the operation of G

Proper and improper subgroup: For any group G, $\{e\}$ and G itself is always subgroup of G and called trivial subgroup (improper subgroup) and all other subgroups are called non-trivial (proper) subgroups.

3.2. Subgroup Generated by an Element

Let $(G, *)$ be a group let $a \in G$ be any element define $H = \{a^r \mid r \in \mathbb{Z}\}$ where a^r denotes $\overset{r-time}{a * a * \ldots * a}$ then H is subgroup of G with identity element a^0 and for each $a^k \in H$ inverse element is a^{-k}, called subgroup generated by a and denoted by $< a > = \{a^r \mid r \in \mathbb{Z}\}$

Algorithm to check subgp
1. Show $H \neq \phi$
2. Take $a, b \in H$ then membership of H
3. Evaluate, using steps to $ab \in H$

Result
For any $H \neq \phi$, $H \subseteq G$ always subgp of G called improper or rest proper.

Arbitrary intersection of subgp is subgp

Every element of gp generates a subgp, $H = \langle a \rangle \subseteq G$ of the same order as of the order of element i.e. o(H) = o(a)

If G is non-abelian then G has proper cyclic/abelian subgp.

Every subgp of cyclic/abelian gp is cyclic/abelian

Non-abelian Gp may have abelian gp moreover it have a gp which is abelian but not cyclic eg: S_3

Order of Element: Let $a \in G$ then $< a >= \{a^r \mid r \in \mathbb{Z}\}$ is subgroup of G and the order of this subgroup is called order of a and denoted by $o(a)$. That is $o(a) = o(< a >)$.

Or

If $\exists m \in \mathbb{N}$ (smallest +ve integer) such that $a^m = e \,\&\, a^r \neq e$ for any $r < m$. Then m is called $o(a)$. In other words, the number of distinct elements in $< a >= \{a^r : r \in \mathbb{Z}\}$ is defined as order of $a \in G$ If no such m exist then we say $o(a)$ is infinite i.e., $H =< a >$ is of infinite cardinality that is $|H| = \aleph_0$ (aleph naught).

Self-inverse element: Let $(G, *)$ be a group then $a \in G$ is called self-inverse element if it is inverse of itself.

Properties on Order of element:

(i) The identity element is always self-inverse.

(ii) Each group has a self-inverse element namely identity.

(iii) Let G be a group. Then Identity element is always of order one and it is the only element of order one

(iv) Let G be a group, $a \in G$. Then $o(a) = o(a^{-1})$ i.e., order of an element and its inverse is always same

(v) Let G be a finite group of even order then number of elements of order 2 in G are always odd

(vi) Let G be a finite group then number of elements of fixed order $k \in \mathbb{N}, k \geq 3$ are always even number

(vii) Let G be a finite group of even order then number of self-inverse elements in G are always even number.

(viii) Let a, b, x are elements of a group G then

(a) $o(a) = o(x^{-1}ax)$

(b) $(x^{-1}ax)^k = x^{-1}a^k x$

(c) $o(ab) = o(ba)$

Propositions 3.1: Let G be a finite group and let $a \in G$ be an element of order n. Then $a^m = e$ iff n is a divisor of m i.e. m is multiple of n.

Propositions 3.2: Let G be a group and let $a \in G$ be an element of order O.

Then $O(a^k) = \dfrac{m}{\gcd(m,k)}$, where $k \in \mathbb{N}$

Propositions 3.3: If a, b be any element of a group G such that $a.b = b.a$ and $O(a) = m, O(b) = n$. Then $O(ab) = O(a)O(b)$ if $g.c.d(m,n) = 1$

Remark: $a, b \in G$ be elements of finite order of a group G, then O(ab) may not be finite and if it is finite even then it need not be equal to O(a) O(b).

Example: Let $G = \{f : \mathbb{R} \to \mathbb{R}$ be one-one and onto function$\}$ be a group under operation of composition of functions. Let $f_1, f_2 \in G$ be two elements such that $f_1(x) = -x$ and $f_2(x) = 1 - x$. Then $O(f_1) = 2 = O(f_2)$, but $O(f_1 f_2)$ is ∞.

Put Your Own Notes

No gp can be expressed as union of two proper subgp.

3.3. Cosets and its Properties

Let G be a group and H be a subgroup of G, and a be an arbitrary element of G. We define the right coset denoted by Ha of H in G, generated by a, the subset of G as $Ha=\{ha:h\in H\}$ and as the left coset denoted by aH of H in G, generated by a, the subset of G as $aH=\{ah:h\in H\}$.

Equivalence Relation on Group: Let G be a group and H be a subgroup of G define a relation on G, for any $a,b\in G$ (a related to b) $a\sim b$ iff $ab^{-1}\in H$ then $\sim$ is an equivalence relation on G.

The equivalence classes of this relation corresponds to right cosets that is $cl(a)=Ha$ for all $a\in G$

Index of a Subgroup: The **index** of a subgroup H of a group G is defined as the number of distinct right (or left) cosets of H in G. It is denoted by $i_G(H)$ or $[G:H]$.

Properties on Cosets: Let H be a subgroup of G and $a,b\in G$. Then

(i) $a\in aH$ that is cosets of every subgroup always non-empty.

(ii) $aH=H$ iff $a\in H$

(iii) $aH\neq bH$ or $aH\cap bH=\phi$ (null set) cosets are either identical or disjoint

(iv) $aH=bH$ iff $a^{-1}b\in H$ OR $Ha=Hb$ iff $ab^{-1}\in H$

(v) $|aH|=|bH|$

(vi) $aH=Ha$ iff $H=aHa^{-1}$

(vii) aH is a subgroup of G iff $a\in H$

(viii) H is subgroup G, then H itself is right as well left coset of G by e (identity element) as $He=eH=H$

(ix) If G is Abelian group then there is no difference between left and right coset of any subgroup H.

3.4. First Milestone of Modern Algebra

Lagrange's Theorem: For any finite group G, the order (number of elements) of every subgroup H of G divides the order of G.

Note: Converse of Lagrange's theorem is not true.

Propositions 3.4: If G is a finite group and $a\in G$, then order of a divides $o(G)$.

Propositions 3.5: The index of a subgroup H of a finite group G divides the order of the group and $i_G(H)=\frac{o(G)}{o(H)}$.

Product of Subgroups: Let H and K be two subgroups of a group G. Then their product, denoted by HK, is defined as $HK=\{hk:h\in H,k\in K\}$.

Propositions 3.6: If H and K are two subgroups of a group G, then HK is a subgroup of G if and only if $HK=KH$. And $o(HK)=\frac{o(H)o(K)}{o(H\cap K)}$, provided H and K are of finite order.

Put Your Own Notes

(2)
$Z(a)=\{x\in G \mid xy=yx, \forall y\in G\}$ is called Centre of Gp.
$Z(G)\subseteq G$
$Z(G)\subseteq N(a)$

Gn infinite gp
index is no. of Right/Left Cosets.
Note infinite subgp may have finite index.
Eg: $5\mathbb{Z}\subseteq\mathbb{Z}$ have index 5.

Put Your Own Notes

Propositions 3.7: If H and K are subgroups of an abelian group G, then HK is a subgroup of G.

Propositions 3.8: if G is a finite group of order pq, where p and q are prime numbers $(p>q)$. Then G has one subgroup of order p.

Example: If $O(G)=6$ and $H \neq K$ are subgroups of G each of order 2, then HK cannot be a subgroup of G.

Propositions 3.9: A group G of order $2p$, where p is prime and $p>2$, has exactly one subgroup of order p.

Propositions 3.10: No element can have order more than that of the order of the group itself.

Propositions 3.11: Order of group is finite $\Rightarrow$ order of each element is finite but order of each element finite $\not\Rightarrow$ order of group is finite.

Example: $(P(\mathbb{N}),\Delta)$ group in which every element is of finite order but order of group is infinite.

Propositions 3.12: Let G be any finite group let $S=\{x \in G \mid x^k = e, x \neq e\}$ then

1. k is odd prime then $|S|$ is multiple of $(k-1)$ that is $|S| = t.(k-1)$ that is $t=0,1,2,...$
2. k is even number then $|S| = \begin{cases} even & ,o(G)=odd \\ odd & ,o(G)=even \end{cases}$
3. k is odd composite then $|S| = even$

Put Your Own Notes

CHAPTER 4

SOME IMPORTANT GROUPS OF FINITE ORDER

Generation of Element: Let G be a group and $a \in G$ be any arbitrary element. Define $H = \{a^n : n \in \mathbb{Z}\}$ .Then $H = \{a^n : n \in \mathbb{Z}\}$ is a Subgroup of G , as $e = a^0 \in H \Rightarrow H \neq \phi$.

Let $x, y \in H$ be arbitrary $\Rightarrow x = a^n$ and $y = a^m$ for some $m, n \in \mathbb{Z}$ Consider, $xy^{-1} = (a^n)(a^m)^{-1} = a^n a^{-m} = a^{n-m} \in H$, so by one step test H is subgroup of G. called subgroup generated by a and denoted by $H = < a >$ Thus, for any group G and any element $a \in G$, $\langle a \rangle$ are always subgroups of G.

4.1. Cyclic Group and its Properties

A group $(G, *)$ is called a cyclic group if $\exists a \in G$ s.t. $G = \langle a \rangle$ i.e., every element of G is an integral power of a, such a is called generator of G.

Examples of cyclic group

(a) $(\mathbb{Z}, +)$ is an Infinite cyclic group

(b) $(\mathbb{Z}_n, +_n)$ is a cyclic group of order n , called group of integers under the operation integer modulo n .

(c) $G = \{\alpha, \alpha^2, ... \alpha^n = e\}$, where $\alpha = e^{\frac{2\pi i}{n}}$ is a finite cyclic group of order n

(d) $G = \left\{ \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix}, a \in \mathbb{Z}_n \right\}$ is a finite cyclic group of order n

(e) $G = \left\{ \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix}, a \in \mathbb{Z} \right\}$ is an Infinite cyclic group

Proposition 4.1: A finite group G is cyclic iff it has an element, which has the same order as that of the group itself i.e., if $o(G) = n$ and $\exists a \in G$ s. t. $o(a) = n$. Then G is cyclic and conversely

Example:

(a) $(\mathbb{Z}_n, +_n)$ is a finite cyclic group of order n , $1 \in \mathbb{Z}_n$ is of order n

(b) $G = \{1, -1, i, -i\}$ is a cyclic group under ordinary multiplication and order of $i, -i$ is four

Proposition 4.2: For each $n \in \mathbb{N}$, there exists a finite cyclic group G of order n , namely $(\mathbb{Z}_n, +_n)$

Proposition 4.3: Let G finite group and $a \in G$. Then $o(a) | o(G)$ i.e., $o(a)$ divides $o(G)$.

Put Your Own Notes

Proposition 4.4: Every prime order group is cyclic i.e., If $o(G)=p$ (p is prime) then G is cyclic and hence abelian.

Proof: Let $o(G)=p, p$ being a prime. Let $e\neq a\in G$. Define $H=<a>$, then H is cyclic subgroup of G. By lagrange's theorem, $o(H)$ divides $o(G)=p$. consequently, $o(H)=1$ or $o(H)=p$ but $a\neq e$ implies $o(H)=p\Rightarrow <a>=H=G$. hence G is cyclic generated by a.

Example: Every group of order $2,3,5,7,11,13,...$ is cyclic group

Proposition 4.5: A group $G\neq\{e\}$ has no proper subgroups iff G is a finite cyclic groups of prime order.

Proposition 4.6: Every Subgroup of cyclic group is cyclic

Proposition 4.7: Let $G=\langle a\rangle$ be a cyclic group of order n then $G=\langle a^k\rangle$ *iff* $g.c.d.(k,n)=1$

Proposition 4.8: Let $G=\langle a\rangle$ be a cyclic group of order n then a^k is a generator of G *iff* $g.c.d.(k,n)=1$

Proposition 4.9: The number of generator of a cyclic group $G=\langle a\rangle$ of order n is $\phi(n)$ where ϕ is Euler ϕ-function

Example: Consider $(\mathbb{Z}_{20},+_{20})$ then number of generators of $\mathbb{Z}_{20}$ are 8 and they are 1,3,7,9,11,13,17,19.

Proposition 4.10: Number of generators in every cyclic group G of order >2 are always even (as $\phi(n)$ is even $\forall\ n\geq 3$).

Proposition 4.11: If $G=\langle a\rangle$ be a cyclic group of order n then the order of any subgroup of G is a divisor of n.

Proposition 4.12 (Fundamental Theorem of Cyclic Groups): If $G=<a>$ be a cyclic group of order n then for each positive divisor k of n, G has unique subgroup of order k - namely, $\langle a^{n/k}\rangle$.

Proposition 4.13: The number of subgroups of a cyclic group of order n are $\tau(n)$ i.e., number of positive division of n.

Proposition 4.14: If $G=\langle a\rangle$ be a cyclic group of order n, If d is a positive divisor of n, the number of elements of order d in G is $\phi(d)$, when ϕ is Euler's ϕ-function.

Example: Consider $(\mathbb{Z}_{200},+_{200})$ then

(a) Number of subgroups of $\mathbb{Z}_{200}=\tau(200)=12$

(b) Number of elements of order 100 $=\phi(100)=40$

(c) Number of generators $=\phi(200)=80$

Put Your Own Notes

Proposition 4.15: Every cyclic group is abelian but converse need not to be true

Example: Group of rational numbers $(\mathbb{Q},+)$ with respect to addition is abelian but not cyclic.

Proposition 4.16: If G is infinite cyclic group. Then G has exactly two generators.

Example: The group of integers $(\mathbb{Z},+)$ has two generators namely, $1,-1$

Proposition 4.17: Let $(G, *)$ be a group and $a \in G$ be any element.

(i) Every non-identity, self-inverse element is of order two

(ii) Every infinite group has infinite number of subgroups

(iii) Every group has cyclic subgroup.

(iv) Every proper subgroup of a group G is cyclic $\not\Rightarrow$ G is cyclic.

Example: In quaternion group Q_8 every proper subgroup is cyclic but group itself is non abelian, non cyclic.

(v) Every Composite order group has a proper subgroup.

(vi) Every group of Composite order has a proper cyclic subgroup.

(vii) Every group of Composite order has a proper abelian subgroup.

(viii) If G be a cyclic group such that G does not have proper subgroup. Then

(a) $O(G) =$ finite

(b) $O(G)$ is Either 1 or prime.

(ix) Let G be finite cyclic group generated by a and $H =< a^m >$, for fixed $m \in \mathbb{Z}$ and index of $H = \gcd(m, o(a))$.

Example: Let $G = \{1,-1,i,-i\}$ be a group under ordinary multiplication of complex number. $o(i) = 4$ as $i^2 = -1 \Rightarrow i^4 = 1$ Also $o(G) = 4 \Rightarrow G$ must be cyclic and $G = \langle i \rangle = \{i, i^2, i^3, i^4\} = \{i.-i,-1,1\}$

(x) There exist a finite group whose each proper subgroup is cyclic but group it self is abelian but not cyclic. $G = K_4 = \{e, a, b, ab : a^2 = e = b^2, ab = ba\}$. This group is known as Klein's-4 group.

(xi) There exist finite groups whose each proper subgroup is cyclic but group itself non- abelian. $G = Q_8 =$ Quaternion group

(xii) If $G = (\mathbb{Z}_6, +_6)$. then number of generator is two and list of generator is $1,5$

(xiii) If $G = (\mathbb{Z}_{15}, +_{15})$. then number of generator is 8 and list of generator is $1,2,4,7,8,11,13,14$

Put Your Own Notes

4.2. Klein's Four-Group

A group of order four in which every element is self inverse is called **Klein four-group** and denoted by K_4 or a group generated by two element $K_4 = \left\{a,b \mid a^2 = b^2 = (ab)^2 = e\right\}$. We will defined this groups $K_4 = \{e,a,b,c\}$ of four elements with $a.b = c = b.a, a.c = b = c.a, b.c = a = c.b$ and $a^2 = e, b^2 = e, c^2 = e$ and e is the identity element. The cayley's table is given by

Element/element	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Properties of Klein's four-group

(i) All non-identity elements of the Klein group have order 2

(ii) Any two non-identity elements can serve as generators.

(iii) The Klein four-group is the smallest non-cyclic group. It is however an abelian group

(iv) The Klein four-group has five subgroups, the list of subgroups and number of elements are given below:

Possible order	Number of elements	Number of subgroup
1	1	1
2	3	3
4	zero	1

(v) The list of all subgroup of Klein four-group are: $H_1 = \{e\}$, $H_2 = \{e,a\}$, $H_3 = \{e,b\}$, $H_4 = \{e,c\}$, $H_5 = K_4$

(vi) The Klein four-group is an example of a non cyclic group whose every proper subgroup is cyclic

Quaternion Group:

One of the most famous finite groups is the quaternion group denoted by Q_8 is group of 8 elements defined as $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ with binary operations defined as follow $i^2 = j^2 = k^2 = -1$, $i.j = -j.i = 1$, $j.k = -k.j = i$, $k.i = -i.k = 1$. The Cayley table (multiplication table) is given by

	1	-1	i	$-i$	j	$-j$	k	$-k$
1	1	-1	i	$-i$	j	$-j$	k	$-k$
-1	-1	1	$-i$	i	$-j$	j	$-k$	k
i	i	$-i$	-1	1	k	$-k$	$-j$	j
$-i$	$-i$	i	1	-1	$-k$	k	j	$-j$
j	j	$-j$	$-k$	k	-1	1	i	$-i$
$-j$	$-j$	j	k	$-k$	1	-1	$-i$	i
k	k	$-k$	j	$-j$	$-i$	i	-1	1
$-k$	$-k$	k	$-j$	j	i	$-i$	1	-1

Note: Here $\pm 1, \pm i, \pm j, \pm k$ denoting symbols

Put Your Own Notes

Example: we can take $1=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}, i=\begin{pmatrix}i & 0\\ 0 & -i\end{pmatrix}, j=\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}, k=\begin{pmatrix}0 & i\\ i & 0\end{pmatrix}$ then $Q_8=\{\pm 1, \pm i, \pm j, \pm k\}$ is group order eight under the operation of matrix multiplication.

Properties of Quaternion Group:

(i) **The Relational Definition of Quaternion Group:** The Quaternion Group can also be defined as $Q_8=\left\{a,b \mid o(a)=4, a^2=b^2, b^{-1}ab=a^{-1}\right\}$ (take, for instance, $i=a, j=b, k=ab$)

(ii) Any two elements a and b are of order four, which satisfied above relation, can serve as generators.

(iii) The quaternion group is non abelian group of order eight

(iv) The **quaternion group** has 6 subgroups, the list of subgroups and number of elements is given below

Possible order	Number of elements	Number of subgroup
1	1	1
2	1	1
4	6	3
8	Zero	1

(v) Every proper subgroup of the **quaternion group is cyclic**

(vi) The **quaternion group** is a example of a non-abelian group whose every proper subgroup is cyclic

The list of all 6 subgroup of the **quaternion group** are as follow: $H_1=\{1\}$, $H_2=\{1,-1\}$, $H_3=\{\pm 1, \pm i\}$, $H_4=\{\pm 1, \pm j\}$., $H_5=\{\pm 1, \pm k\}$, $H_6=Q_8$ Here, H_1, H_2, H_3, H_4, H_5 are cyclic subgroups

Put Your Own Notes

CHAPTER 5

SYMMETRIC GROUP OR PERMUTATION GROUP

5.1. Symmetric Group

In mathematics, the symmetric group on a set is the group consisting of all bijections of the set (all one-to-one and onto functions) from the set to itself with function composition as the group operation. The symmetric group has high importance in group theory. For Instance, as Cayley's theorem states that every group G is isomorphic to a subgroup of the symmetric group. Formally, The symmetric group on a non empty set S is the group whose underlying set is the collection of all bijections from S onto S and whose group operation is that of function composition and denoted by S_X.

Proposition 5.1: Symmetric group is non-abelian: The symmetric group defines on a set S with at least three elements is always non-abelian group.

Let $a,b,c \in S$ are three elements and define $f(a)=b, f(b)=a, f(x)=x, \forall x \in S-\{a,b\}$ and $g(a)=c, g(c)=a, g(x)=x, \forall x \in S-\{a,c\}$. Then $f,g \in S_X$ and $f \circ g \neq g \circ f$. Hence S_X is non-abelian.

5.2. Definitions and Properties of Permutation Group

Permutation: Let $S=\{a_1,a_2,...,a_n\}$ is finite set of n symbols/elements. Then a permutation on a set S is a bijection $f: S \to S$. It is also called permutation on n-symbols.

Example: A permutation α of the set $\{1,2,3,4\}$ by specifying $\alpha(1)=2, \alpha(2)=3, \alpha(3)=1, \alpha(4)=4$

Representation of Permutations: A more convenient way to express this correspondence is to write α in array form as $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$

Therefore, a permutation on a set with n symbols is a two row – n-column array in which first row is element of the set in a random order and $\alpha(i)$ is placed directly below to i, for each i to form second row. That is, if $f: S \to S$ is a permutation then $f = \begin{pmatrix} a_1 & a_2 & ... & a_n \\ f(a_1) & f(a_2) & ... & f(a_n) \end{pmatrix}$ in which first row represent the symbols and second row represent the image of each symbol under the permutation f.

Permutation Group: Let S be a finite set of n symbols. The set of all permutations on S under composition of permutations is a group, called group of permutations or symmetric group of n symbols and denoted by S_n

Note: The composition of two bijections is itself a bijection, hence S_n is closed under composition. It is also associative, and has identity and inverse, since function, composition is associative and has identity and inverse (and the identity function is of course a bijection and the inverse of a bijection is a bijection). So, S_n satisfies all the axioms of a group.

Put Your Own Notes

Note: The n-symbols of a set S can be represent by first n integers that we can consider set of n symbols $X=\{1,2,...,n\}$ and S_n is symmetric group on S

Order of Permutation Group: Clearly, there are exactly $n!$ permutations can be define on as set of n symbols. So, the order of permutation group S_n is $n!$.

Equivalence relation on S_n : Let S be a non-empty set and σ a permutation on S. For $a,b\in S$ define a relation $\sim$ on S by $a\sim b \Leftrightarrow \sigma^n(a)=b$ for some integer n. This relation $\sim$ is an equivalence relation. Which partitions the group S into equivalence classes and these classes are called **Orbits.**

Note: $\sigma^n=\sigma\circ\sigma\circ\sigma\circ.....\sigma$ (n times) i.e., composition of σ with itself , n times .

Cycles /Cyclic Permutation: Let S be a finite set. Let $a\in S$ and σ be a permutation on S then $\exists\, a$ positive integer m s.t. a $\sigma(a),\sigma^2(a)\ldots\sigma^{m-1}(a)$ are distinct and $\sigma^m(a)=a$

Example: Consider the permutation $\sigma=\begin{pmatrix}1&2&3&4&5&6&7&8\\8&7&5&4&6&2&1&3\end{pmatrix}$. Then

$\sigma(1)=8,\sigma^2(1)=\sigma(8)=3,$

$\sigma^3(1)=\sigma(3)=5,\ \sigma^4(1)=6,\sigma^5(1)=2,\sigma^6(1)=7,\sigma^7(1)=1.$ Thus a cycle of σ is $(1\,8\,3\,5\,6\,2\,7)$

Cycle of length r : An element $\sigma\in S_n$ is called cycle of length r or r-cycle if there exist r symbols $i_1,i_2\ldots i_r$ such that $\sigma(i_1)=i_2,\sigma(i_2)=i_3,\sigma(i_3)=i_4\ldots\sigma(i_{r-1})=i_r,\sigma(i_r)=i_1$ and $\sigma(j)=j$ for all $j\neq i_1,i_2\ldots i_r$. We use the notation $(i_1,i_2,i_3\ldots i_r)$ to denote such an r-cycle

Example: Consider the permutation $\sigma=\begin{pmatrix}1&2&4&5\\2&4&5&1\end{pmatrix}$ then $\sigma\in S_6$ is 4-cycle

Transposition: An element $\sigma\in S_n$ is called a transposition if there exists two symbols i and j such that $\sigma(i)=j,\sigma(j)=i,\sigma(k)=k\ \forall\, k\neq i,j$ and the notations for transposition is $(i\ j)$. i.e., every cycle of length 2 is a transposition and vice-versa

Example: The group of permutations on 3 symbols $S_3=\{I,(12),(13),(23),(123),(132)\}$ Contains three transpositions and two 3-cycles and one identity element.

Disjoint cycles: Let $c_1=(a_1,a_2,a_3\ldots a_r)$ and $c_2=(b_1,b_2,b_3\ldots b_s)$ be two cycles , c_1,c_2 are called disjoint if there is no common symbol in these two cycles i.e., $\{a_1,a_2,a_3\ldots a_r\}\cap\{b_1,b_2,b_3,\ldots,b_s\}=\phi$

Put Your Own Notes

Proposition 5.1: Every permutation $\sigma \in S_n$ can be expressed as a product of disjoin cycles.

Example: $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 4 & 2 & 1 & 6 & 5 & 8 & 9 & 7 \end{pmatrix} = (1\,3\,2\,4)(5\,6)(7\,8\,9)$

Proposition 5.2: Every r-cycle can be expressed as a product of $(r-1)$ transpositions

Example:

(a) $(1234) = (14)(13)(12)$

(b) $(235) = (25)(23)$

Proposition 5.3: Every permutation σ of S_n can be expressed as a product of transpositions.

Example: Let $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 4 & 2 & 1 & 6 & 5 & 8 & 9 & 7 \end{pmatrix}$

$= (1\,3\,2\,4)(5\,6)(7\,8\,9) = (1\,4)(1\,2)(1\,3)(5\,6)(7\,9)(7\,8)$

Proposition 5.4: The symmetric group S_n can be generated by transposition namely, $(12),(13),\ldots(1n)$ (Hint : every permutation can be express as product of transpositions)

Proposition 5.5: The symmetric group S_n can be generated by two cycles namely, and $\tau = (12)$

Inversion of a Permutation: Let $\sigma \in S_n$ be permutation and let $\sigma = \begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \ldots & \sigma(n) \end{pmatrix}$. Then inversion of a symbol say is denoted by $Inv(i)$ and is defined as $Inv(i) =$ number of symbols less than $f(i)$ and right to $f(i)$ And inversion of permutation σ define as $\mathrm{Inv}(\sigma) = \sum_{i=1}^{n-1} \mathrm{Inv}(i)$

Example: Let $\sigma \in S_6$. defined as $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 6 & 1 & 4 & 3 & 5 \end{pmatrix}$ then,

$\mathrm{Inv}(1) = 1, \mathrm{Inv}(2) = 4, \mathrm{Inv}(3) = 0,$
$\mathrm{Inv}(4) = 1, \mathrm{Inv}(5) = 0, \mathrm{Inv}(6) = 0$ and

$\mathrm{Inv}(\sigma) = \mathrm{Inv}(1) + \mathrm{Inv}(2) + \mathrm{Inv}(3) + \mathrm{Inv}(4) + \mathrm{Inv}(5) = 6$

Signature of Permutation: If $\sigma \in S_n$, then the signature of σ is defined as the product $\prod_{1 \le i < j \le n} \frac{\sigma(i) - \sigma(j)}{i - j}$ and it is denoted by $sig(\sigma)$

Relation between Signature and Inversion: Let $\sigma \in S_n$ be any permutation. Then $Sig(\sigma) = (-1)^{Inv\,\sigma}$

Put Your Own Notes

Example:

Proposition 5.6: Let $\sigma, \tau \in S_n$ then

1. $sig(I) = 1$, where I is identity permutation
2. $sig(T) = -1$, where T is Transposition
3. $sig(\sigma \circ \tau) = sig(\sigma).sig(\tau)$
4. $sig(\sigma^{-1}) = sig(\sigma)$

Example: The group of permutation on 3 symbols $S_3 = \{I, (12), (13), (23), (123), (132)\}$ Contain three transpositions namely $(12), (13), (23)$, hence $sig((12)) = -1$, $sig((13)) = -1$, $sig((23)) = -1$, and two 3-cycles $(123), (132)$ and one identity element. Also, $sig((123)) = 1$, $sig((132)) = 1$

Example: The group of permutation on 3 symbols $S_3 = \{I, (12), (13), (23), (123), (132)\}$. Contain three Odd permutations namely $(12), (13), (23)$ and three even permutations namely $I, (123), (132)$

Proposition 5.7: The number of transpositions in the decomposition of any permutation σ is either always odd or always even according to σ is odd or even permutation.

Proof: Let $\sigma = t_1 . t_2 \ldots t_k$ be a product of transposition Then $sig\ \sigma = sig\ t_1 . sig\ t_2 \ldots sig\ t_k$. Now for each transposition t_1, we have sig $t_i = -1$. Hence $sig\ \sigma = (-1)^k$ But sig σ has a fixed value $+1$ *or* -1. Thus k is always even (when $sig\ \sigma = +1$) or always odd (when $sig\ \sigma = -1$)

Proposition 5.8: If $\sigma \in S_n$ be a r-cycle, then σ is even permutation if r is odd and odd permutation if r is even can be express as product of $r-1$ transpositions.

Example: $\sigma = (1\ 3\ 2\ 4\ 5) \in S_5$ is an even permutation and $\sigma = (1\ 3\ 2\ 4\ 6\ 5) \in S_6$ is an Odd permutation

Proposition 5.9: Every subgroup H of S_n either contains all even permutations or exactly half-even and exactly half-odd permutations

Proposition 5.10: Every odd order subgroup H of S_n contains only even permutations

5.3. Alternating Group (A_n)

The Set of all even permutation of S_n forms group w.r.t. composition of mappings and is subgroup of S_n denoted by A_n and called alternating subgroup of S_n or group of even permutations

Proposition 5.11: The number of elements in A_n are $\frac{n!}{2}$

Proof: Let $e_1, e_2, \ldots, e_k$ be all even permutations of S_n and $o_1, o_2, \ldots, o_l$ be all odd permutations of S_n. Then $k + l = n!$ let $\tau \in S_n$ is a transposition then $\tau e_1, \tau e_2, \ldots, \tau e_k$ are odd permutations and all are distinct $\therefore \quad k \le l$ ...(1)
Similarly $\tau o_1, \tau o_2, \ldots, \tau o_l$ are even permutations and all are distinct $\therefore \quad l \le k$ ...(2)

$\therefore \quad k = l$ by (1) & (2) $\therefore$ $\frac{n!}{2}$ permutations in S_n are even and the remaining $\frac{n!}{2}$ permutations are odd.

Put Your Own Notes

Proposition 5.12: the permutation group S_n exactly half are even and half are odd

Proposition 5.13: every subgroup of A_n contains only even permutations

Example: A_5 is group of all even permutations on 5 symbols of order 60

Proposition 5.14: If H is subgroup A_n contains all 3-cycles. Then $H = A_n$

Proposition 5.15: The alternating group $A_n (n \geq 3)$ can be generated by $n-2$, 3-cycles namely, $(123),(124),\ldots(12n)$

Proposition 5.16: If H is subgroup of S_n contains 3-cycles and a odd permutation. Then $H = S_n$

Proposition 5.17: Every odd order subgroup H of S_n is also subgroup of A_n i.e., Every odd order subgroup H of S_n contained in A_n

Order of r -Cycle: Let $c \in S_n$ be $r-$ cycle. Then r is the least positive integer such that $c^r = I$ i.e., the order of any cycle is same as its length.

Order of Permutation: Let $\sigma \in S_n$ be arbitrary. As every permutation can be expressed as a product of disjoint cycles. Let $\sigma = c_1.c_2.c_3 \ldots c_k$, where $c_1, c_2, \ldots, c_k$ are disjoint cycles. Then order of $o(\sigma) = l.c.m\{l(c_1), l(c_1), ..., l(c_k)\}$ where $l(c)$ denotes the length of cycle c

Note: Order of any transposition is 2 i.e. $\tau \in S_n$ is a transposition then $\tau^2 = e$. Every transposition is self-inverse element S_n

Proposition 5.18: The number of r-cycles in a symmetric group on n-symbols (S_n) is given by $\frac{{}^nP_r}{r} = \frac{n!}{r(n-r)!}$

Example: number of 3-cycles in $S_4 = \frac{{}^4P_3}{3} = 8$

Partition of a Natural Number: Let n be a positive integer. A Sequence of positive integers $n_1, n_2, n_3, \ldots n_q$ is called partition of n if

1. $n_1 \leq n_2 \leq n_3 .... \leq n_q$
2. $n_1 + n_2 + n_3 + \ldots n_q = n$ and it is denote by $\{n_1, n_2 \ldots n_q\}$

Example: if $n = 5$, then it has following partitions. $\{1,1,1,1,1\},\{1,1,1,2\},\{1,1,3\},\{1,4\},\{5\},\{1,2,2\},\{2,3\}$. Let $p(n)$ denotes the number of partition of n. Then one can easily compute that $p(1)=1, p(2)=2,\ p(3)=3, p(4)=5, p(5)=7, p(6)=11, p(7)=15, p(8)=22 \ldots$

Note: Look here $p(i)$, i^{th} prime for $i \leq 6$.

Put Your Own Notes

Cycle-Decomposition: Let $\sigma \in S_n$ be expressed as a product of disjoint cycles of lengths $n_1, n_2, ..., n_q$ with $n_1 \le n_2 \le n_3 .... \le n_q$ and $n_1 + n_2 + ... n_q = n$ .Then we say that σ has the cycle decomposition $\{n_1, n_2 ... n_q\}$.

Example: Let $\sigma = (145) \in S_6$ be a 3-cycle. Then the cycle decomposition of σ is $\{1,1,1,3\}$ because $\sigma = (145) = (2)(3)(6)(145) \in S_6$, $\tau = (12)(34) \in S_4$ has the cycle decomposition $\{2,2\}$

Relation of Similarity: Let us define a relation $\sim$ on S_n as $\sigma \sim \tau \Leftrightarrow \sigma$ and τ have same cycle decompositions. Clearly '$\sim$' is an equivalence relation on S_n and hence '$\sim$' partitions the S_n into equivalence classes and the permutations belong to same class are called permutation

Similar Permutations: Two permutation σ and $\tau \in S_n$ are said to be similar permutations if σ and τ have the same cycle decompositions.

Example: $\sigma = (145)(23) \in S_6$ and $\sigma = (135)(26) \in S_6$ are similar permutations as they have same cycle decomposition viz. $\{1,2,3\}$

Example: Let us consider S_4, symmetric group on four symbols. Let us define a relation of similarity $\sim$ on S_4. Then Equivalence classes are

Equivalence class of $(1) = \{(1)\}$, which is identity permutation

Equivalence class of $(12) = \{(12),(13),(14),(23),(24),(34)\}$ then all the permutation are of order 2

Equivalence class of $(123) = \{(123),(124),(132),(134),(142),(143),(234),(243)\}$ then all the permutation are of order 3

Equivalence class of $(1234) = \{(1234),(1243),(1324),(1342),(1423),(1432)\}$ then all the permutation are of order 4

Equivalence class of $(12)(34) = \{(12)(34),(14)(23),(13)(24)\}$ then all the permutation are of order 2

Proposition 5.19: The number of distinct cycle decomposition of permutations in S_n are same as number of partitions of n

Example: Number of distinct cycle decomposition in S_5 are number of partition of S_5 , $p(5) = 7$. The cycle decomposition in S_5 are $\{1,1,1,1,1\},\{1,1,1,2\},\{1,1,3\},\{1,4\},\{5\},\{1,2,2\},\{2,3\}$

Proposition 5.20: If $\sigma \in S_n$ has the cycle decompositions $\{n_1, n_2, ..., n_q\}$. Then order of σ is l.c.m. of $n_1, n_2, ...n_q$ i.e., $o(\sigma) = l.c.m\{n_1, n_2 ... n_q\}$

Example: The different possible order of permutation's in S_5 are $1,2,3,4,5,6$. Thus maximum possible order of any element in S_5 is 6 , where as order of S_5 is 120

Put Your Own Notes

An Important Formula: Let $\sigma \in S_n$ has the cycle decomposition $\{n_1, n_2, \ldots, n_k\}$ then and let α_i denotes the number of cycles of length i in $\{n_1, n_2, \ldots, n_k\}$ such that $\sum_{i=1}^{n} \alpha_i = n$.

Then number of elements similar to $\sigma = \dfrac{n!}{1^{\alpha_1}, 2^{\alpha_2} \ldots n^{\alpha_k} . \alpha_1 ! \alpha_2 ! \ldots \alpha_k !}$

Some Particular Example of Permutation Group:

1. The permutation group on 3-symbols denoted by S_3
$S_3 = \{I, (12), (13), (23), (123), (132)\}$

Possible order of elements	Number of elements	Number of subgroup
1	1	1
2	3	3
3	2	1
6	Zero	1

2. The permutation group on 4-symbols (S_4). Order of S_4 is 24.
$S_4 = \{I, (12), (13), (14), (23), (24), (34), (13)(24), (14)(23), (123), (132), (234), (243), (341), (412), (421), (1234), (1432), (1342), (1243), (1423), (1324)\}$

Possible order of elments	Number of elements	Number of subgroup
1	1	1
2	9	9 (all are cyclic)
3	8	8 (all are cyclic)
4	6	7 (3 is isomorphic to $\mathbb{Z}_4$, 4 is isomorphic to K_4)
6	Zero	4 (all are isomorphic to S_3)
8	Zero	3 (all are isomorphic to dihedral group)
12	Zero	1-(Alternative group A_4)
24	Zero	1-(S_4 itself)

3. The Alternative group on 3-symbols (A_3), $o(A_3) = 3$: The Alternative group on 3-symbols is cyclic group of order 3 i.e., $A_3 = \{I, (123), (132)\}$

Put Your Own Notes

4. The structure of Alternative group on 4-symbols (A_4), $o(A_4)=12$: The alternative group on 4-symbols is non-cyclic group of order 12 and the structure is given below $A_4 = \{I,(12)(34),(13)(24),(14)(23),(123),(132),$ $(234),(243),(341),(314),(412),(421)\}$.

Table related to A_4 .

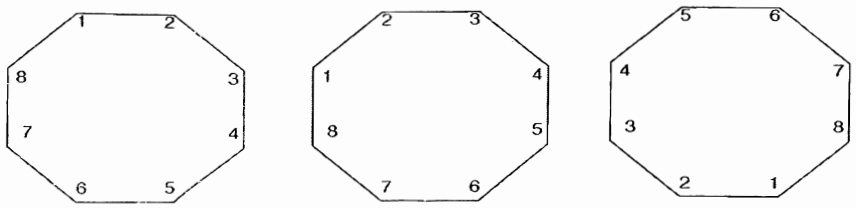
Possible Order	Number of Elements of Order	Number of Subgroup of Order
1	1	1
2	3	3 (all are cyclic)
3	8	4 (all are cyclic)
4	Zero	1 (Isomorphic to K_4)
6	Zero	Does Not exists
12	Zero	A_4

5.4. Dihedral Group

Sometimes, groups appear to be just sets with some binary operation but in fact most groups are in some sense much more than that. One basic class of groups in which this "much more" is readily seen is in groups of symmetry of certain objects (symmetries of tessellations, of polyhedra, etc). In section we'll study one such symmetry group: the dihedral group denoted by D_n .

How to Learn

Let we draw a regular $n-$gon (meaning a convex polygon with n sides of equal length and n angles of the same size) on the floor, and cut out a polygon of exactly the same size and shape from paper. You also label each vertex of your paper polygon (on both sides of the paper) with a number. So the vertices are now labeled $1,2,...,n$. You line up the paper with the picture on the floor so that it looks like the first picture below (which illustrates what happens with an octagon or 8-gon). Now you are allowed to pick up the paper and put it back down on the floor however, you want: the only rule is that it has to line up with the picture on the floor. The question is, what different motions can you do here?

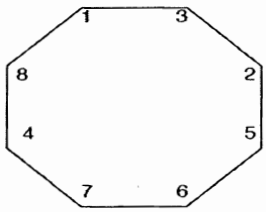


(i) (ii) (iii)

One thing you can do is rotate (counter clockwise or clockwise, though note that rotating clockwise by α is the same thing as rotating counterclockwise by $2\pi-\alpha$). In the second picture above (ii), we have rotated the octagon

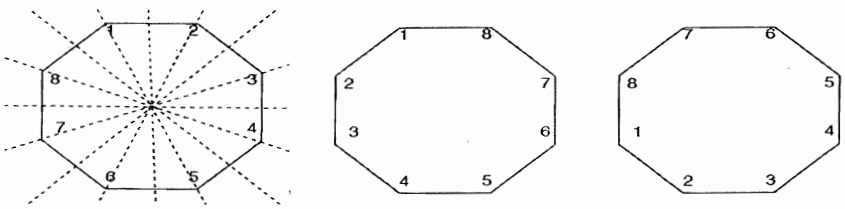
Put Your Own Notes

counterclockwise by $\frac{\pi}{4}$, and in the third picture (iii), we have rotated the octagon counterclockwise by π. If we denote the angle $\frac{2\pi}{8}$ by θ, these two rotations are then rotations by θ and 4θ, respectively. It's not hard to see that the only different rotations we can perform for this picture are counterclockwise rotations by $0, \theta, 2\theta, 3\theta, ..., 7\theta$.



However, there are other things we can do to the octagon. But whatever we do, note that the order of the numbers we have written will remain the same: 1 is followed by 2, 2 is followed by 3, and so on. We won't suddenly get an octagon whose vertices are labeled 1;3;2;5;6;7;4;8 as in the picture below, because no matter what we do the numbers we've written on the vertices will stay exactly where they are.

However, we can reverse whether the numbers are increasing in the clockwise direction, or in the Counter-clockwise direction as above by flipping the octagon in one of its lines of symmetry, which are drawn in the first picture below. In the second picture below, we have flipped the octagon in the line going through 1 and 5, and in the third picture we have flipped it in the line going through 4 and 8.



Note that there are precisely 8 flips we can make like this: one for every line of symmetry.

Furthermore, this exhausts all of the possible motions we can perform: keeping in mind that the only labeling of the vertices we can end up with is 1;2;3;4;5;6;7;8 increasing either clockwise or counterclockwise, it's not hard to see that there are precisely 16 different labelings like this: 8 coming from rotating the original picture, and 8 coming from flipping the original picture.

In the more general situation of an n-gon, we let $\theta = \frac{2\pi}{n}$, and note that the only motions we can perform are rotations p_i counterclockwise by $.\theta$ for $0 \le i < n-1$, and flips (reflections) in n lines of symmetry. Let's denote the set of all $2.n$ of these motions by D_n. It turns out that Dn under composition of the motions (composing motion 1 and motion 2 means "do motion 2 then do motion 1") is a group, and we call it a dihedral group.

Put Your Own Notes

Relation Definition of Dihedral Group: There is a much less spectacular way to think about D_n. Namely, let x denotes rotation by $\frac{2\pi}{n}$, and let y be any one of the reflections in D_n. We know $x^n = e$ (the identity element), and that $y^2 = e$ as well. Furthermore, we can deduce from our discussion of composition of rotations and reflections above that $yx = x^{n-1}y$. We say x and y are generators of D_n, and the equations $x^n = e = y^2, yx = x^{n-1}y$ are relations for these generators. With this in mind, the dihedral group can be thought of just as an abstract group.

$D_{2n} = \{x^i y^j \mid i = 0,1, j = 1,2,..,n-1, x^n = e, y^2 = e, yx = x^{n-1}y\}$

Properties on Dihedral Group:

(i) D_n is Non abelian group of order $2n$ $\forall n \geq 3$

(ii) Number of element of order two in D_n are
$\begin{cases} n, & n \text{ odd } (n \text{ reflections}) \\ n+1, & n \text{ even } (n \text{ reflections \& 1 rotation}) \end{cases}$

(iii) Number of element of order $k \neq 2$ in D_n are $\phi(k)$, provided $k \mid n$ (Where $\phi(k)$ is Euler function)

(iv) Largest possible order of any element in D_n is n

(v) For each $k \mid n$, D_n has a cyclic group of order k

(vi) Number of Cyclic subgroups in $D_n = \tau(n) + n$, where $\tau(n)$ denotes number of positive divisors of n

(vii) Total number of subgroup in $D_n = \tau(n) + \sigma(n)$, where $\tau(n)$, denotes number of positive divisors of n and $\sigma(n)$ denotes the sum of positive divisors of n

5.5. Group under Multiplication Modulo $n, (\times_n)$

Let $U(n) = \{x \in \mathbb{Z} \mid 1 \leq x < n, \gcd(x,n) = 1\}$ under the operation of multiplication modulo $n, (\times_n)$.

Properties of $U(n)$

(i) $U(n)$ Finite abelian group for each $n \in N$ of order $\phi(n)$ {Euler's ϕ function }

(ii) $U(n), \forall n \geq 3$ is even order group {as $\phi(n)$ is even for $n \geq 3$ }

(iii) $U(n), \forall n \geq 3$ has even number of self-inverse elements

(iv) $U(n), \forall n \geq 3$ always has odd number of elements of order 2 , hence it always has odd number of subgroup of order 2

(v) It is cyclic group if $n = p^k (p \text{ is odd prime})$

$U(2) \approx \{0\}$

$U(4) \approx \mathbb{Z}_2$

$U(2^n) \approx \mathbb{Z}_2 \oplus \mathbb{Z}_{2^{n-2}}$

$U(p^n) \approx \mathbb{Z}_{p^n - p^{n-1}}$ for p an odd prime.

Put Your Own Notes

CHAPTER 6

SOME IMPORTANT GROUPS OF INFINITE ORDER

6.1. Infinite Cyclic Group of Integers under Addition

Let $\mathbb{Z}$ be set of integers. Then $\mathbb{Z}$ is group under addition of integers and it is denoted by $(\mathbb{Z},+)$

Properties of $(\mathbb{Z},+)$:

(i) The set of integers $\mathbb{Z}$ is a cyclic group of infinite order

(ii) $(\mathbb{Z},+)$ has excatly two generaters namely $1,-1$ that is $\mathbb{Z}=<1>=<-1>$

(iii) The identity elements is only elements of finite order in $(\mathbb{Z},+)$

(iv) $(\mathbb{Z},+)$ has exactly one subgroup of finite order

(v) Every non trivial subgroup of $(\mathbb{Z},+)$ is infinite ordered cyclic subgroup

(vi) Every subgroup of $(\mathbb{Z},+)$ is of the form $m\mathbb{Z}$, $\forall m \in \mathbb{Z}$

(vii) Every finitely generated subgroup of $(\mathbb{Z},+)$ is cyclic

(viii) Every subgroup of $(\mathbb{Z},+)$ is finitly generated.

(ix) If $S=\{n_1,n_2,...,n_k\}$ is subset of $\mathbb{Z}$ and $H=<S>$ subgroup generated by S then $H=<\gcd(n_1,n_2,...n_k)>$

(x) If $H_1=<n_1>$ and $H_2=<n_2>$, $n_1,n_2 \in \mathbb{Z}$ are subgroup generated by $n_1 \& n_2$ respectivaly then $H=H_1 \cap H_2$ is subgroup of $\mathbb{Z}$ generated by $lcm(n_1,n_2)$

6.2. Power Set of Natural Numbers

Let $P(\mathbb{N})$ be the power set of natural numbers and let Δ be symmetric difference of two sets A,B defined $A\Delta B=(A\cup B)-(A\cap B)$ then $(P(\mathbb{N}),\Delta)$ is a abelian group of infinite order

Properties on $\left(P(\mathbb{N}),\Delta\right)$:

(i) Every element is self-inverse

(ii) Is group of infinite order in which every non-identity element is of order two

(iii) Has Infinite number of subgroups of finite order

(iv) If $H \subseteq P(\mathbb{N})$ is a finite order subgroup then $o(H)=2^k$, $k=0,1,...$

(v) $X \subseteq \mathbb{N}$ is a subset with n elements then $(P(X),\Delta)$ is finite order subgroup of $(P(\mathbb{N}),\Delta)$ of order 2^n

(vi) $(P(\mathbb{N}),\Delta)$ has countable number of Subgroups of finite order

(vii) $(P(\mathbb{N}),\Delta)$ has uncountable number of Subgroups of infinite order

(viii) In $(P(\mathbb{N}),\Delta)$, there does not any subgroup of $(P(\mathbb{N}),\Delta)$ whose order is divisible by distinct primes , or by any odd prime

Put Your Own Notes

6.6. Group of Matrices under Matrix Multiplication

Let $(F,+,\bullet)$ be a field and $GL(n,F)$ be the set of $n\times n$ matrices of non-zero determinant with entries form field F then $GL(n,F)$ is group under usual matrix multiplication called general linear group

Properties of $GL(n,F)$:

(i) $GL(n,F)$ is a non abelian group $\forall n>1 \& F$ is non-trivial field

(ii) $GL(n,F)$ is of infinite order if F is of infinite cardinality

(iii) $O\left[GL\left(n,\mathbb{Z}_p\right)\right]=\left(p^n-p^{n-1}\right)\left(p^n-p^{n-2}\right)\left(p^n-p^{n-3}\right)....\left(p^n-1\right)$, where $\mathbb{Z}_p$ is field of cardinality p

(iv) $SL(n,F)$ be the set of $n\times n$ matrices of determinant 1 with entries in the field F, is subgroup of $GL(n,F)$ called special linear group

(v) $O\left[SL\left(n,\mathbb{Z}_p\right)\right]=\dfrac{\left(p^n-p^{n-1}\right)\left(p^n-p^{n-2}\right)\left(p^n-p^{n-3}\right)....\left(p^n-1\right)}{(p-1)}$, where p is a prime number.

External Direct Product: Let $(G,*)\&(G',\circ)$ are two groups then their External direct product is dentoted by $G\times G'$ and defined $G\times G'=\{(a,b)\mid a\in G \& b\in G'\}$ and it is group under bineary $(a_1,b_1)\bullet(a_2,b_2)=(a_1*a_2,b_1\circ b_2)$

Order of Element: Let $(G,*)\&(G',\circ)$ are two groups and $G\times G'$ be the external direct product then

$\forall(a,b)\in G\times G'$ order of $o(a,b)=l.c.m\{o(a),o(b)\}$

Theorem: Let G and G' be cyclic groups of order *m, n* respectively. Then $G\times G'$ is cyclic group of order *mn* iff $g.c.d\,(m,n)=1$

Put Your Own Notes

CHAPTER 7

CONJUGATE CLASSES AND CLASS EQUATION

7.1. Definition

A reflection across one line in the plane is, geometrically, just like a reflection across any other line. That is, any two reflections in the plane have the same type of effect on the plane. Similarly, two permutations of a set that are both transpositions (swapping two elements while fixing everything else) look the same except for the choice of the pairs getting moved. So all transpositions have the same type of effect on the elements of the set. The concept that makes this notion of same except for the point of view precise is called conjugacy.

Centre of a Group: The Centre, denoted by $Z(G)$ of a group G is the subset of element of G that commute with every element of G i.e, $Z(G)=\{a\in G|\ ax=xa\ \forall\ x\in G\}$

Note: centre is a subgroup of G

Centralizer or Normalizer of a in G : Let a be a fixed element of a group G . The centralizer (normalizer) of a in G denoted by $C(a)\ or\ N(a)$, is the set of all elements in G that commute with a i.e, $N(a)\ or\ C(a)=\{g\in G|\ ag=ga\}$

Note: is a subgroup $N(a)\ or\ C(a)$ of G

Conjugate Element in a Group: Let G be a group, $a\in G$ and $b\in G$. Then b is said to be conjugate to a ,if $b=xax^{-1}$ for some $x\in G$

Conjugate Relation: Let G be a group, and $\sim$ be the relation on G given by $b\sim a$ iff b is conjugate to a. Then $\sim$ is an equivalence relation in G .i.e., the set defined as $cl(a)=\{xax^{-1}:\ x\in G\}$ is called conjugate class of a in G.

Conjugate Classes: The equivalence classes under the **Conjugate Relation** are called conjugate classes.

Example: Consider the group of permutations on 3-symbols (S_3) and $a=(12)\in S_3$. Then for conjugate of $a=(12)\in S_3$, we need to find $\sigma(12)\sigma^{-1}$ where $T\in S_3$

σ	(1)	(12)	(13)	(23)	(123)	(132)
$\sigma(12)\sigma^{-1}$	(12)	(12)	(23)	(13)	(23)	(13)

Self-Conjugate Element: Let G be a group. An element $a\in G$ is called self-conjugate element of G if a is conjugate to itself only

Put Your Own Notes

7.2. Some Important Results

Let G be a group.

Proposition 7.1: Identity element in every group is conjugate to itself. The conjugate class of identity $e \in G$ contains only e is $cl(e) = \{e\}$. Hence identity element is always self-conjugate element of every group.

Proposition 7.2: every non-trivial group has at least two conjugate classes

Proposition 7.3: $a \in G$ is self-conjugate iff $a \in Z(G)$ hence we have alternate definition of

Centre of Group: The collection of self-conjugate elements of any group form subgroup of that group and is called the centre of that group.

Proposition 7.4: Every element of an abelian group is self-conjugate element.

Proposition 7.5: G is abelian iff $G = Z(G)$

Proposition 7.6: $Z(G) = \bigcap_{a \in G} N(a)$, where $N(x)$ denotes the normalizer of a and $Z(G)$ is centre of group G.

Proposition 7.7: If G be a group and $a, b \in G$. If a is conjugate to b. Then $o(a) = o(b)$.

Proposition 7.8: Let G be a group and $a \in G$. $cl(a)$ denotes conjugate class of a, then all element of $cl(a)$ are of same order

Note: All the elements of a group of same order may not be in same conjugacy class.

***Example*:** let $G = S_4 =$ Symmetric group on 4-symbols. $cl(12) = \{(12),(13),(23),(14),(24),(34)\}$ and

$cl((12)(34)) = \{(12)(34),(13)(24),(14)(23)\}$

Proposition 7.9: If $a \in G$ is only element of order of 2. Then a is self conjugate element. Hence $a \in Z(G) \Rightarrow Z(G)$ has at least two element $\Rightarrow$ order of $Z(G)$ even (provided finite)

Proposition 7.10: If $a \in G$ is only element of order of 2. Then G has at least two conjugate classes each of cardinality one

Proposition 7.11: If G has exactly $\phi(k)$ element of order $k \Rightarrow$ there exists a conjugate class with cardinality $\phi(k)$, ϕ is Euler's ϕ – function.

Proposition 7.12: Conjugate classes are equivalence classes. So, conjugate classes are either disjoint or identical i.e. if G be a group then $G = \bigcup_{a \in T} cl(a)$, where T is set of representative of each conjugacy class.

Proposition 7.13: Let G be a finite group. Then $O(G) = \sum_{a \in T} |cl(a)|$, where T is set of representative of each class

Proposition 7.14: Let G be a finite group. Then $\forall a \in G$ there is one-to-one correspondence between cosets of $N(a)$ and $cl(a)$ i.e, $\frac{O(G)}{O(N(a))} = |cl(a)|$.

Hence the cardinality of conjugate class divides order of group G.

Put Your Own Notes

Proposition 7.15: Let G be a finite group of order n. Then largest possible cardinality of any conjugate class is $\left[\frac{n}{2}\right]$, where $[n]$ denotes the greatest integer function.

Proposition 7.16: Let G be a finite group. Then

1. $a \in Z(G)$ iff $N(a) = G$
2. $a \notin Z(G)$ iff $|cl(a)| \geq 2$
3. $O(G) = Z(G) + \sum_{\substack{a \in T \\ a \notin Z(G)}} \frac{O(G)}{O(N(a))}$, where, where T is set of representative of each class.

Class Equation: Let G be a finite group of order say, n. *i.e.*, $o(G) = n$, and $c_1, c_2, ...c_k$ be k-distinct conjugate classes of cardinality $n_1, n_2, ..., n_k$ respectively. Then the expression $n_1 + n_2 + ... + n_k$, is defined as class equation of G. Clearly, $n_1 + n_2 + ... + n_k = n = o(G)$.

Proposition 7.17: Let G be a finite group such that $O(G) = p^n \Rightarrow O(Z(G)) \geq p$, where p is prime number.

Proposition 7.18: Every group G of order $O(G) = p^2$ is abelian, where p is prime number.

7.3. Class Equation for some important Groups

Non Abelian group G of order p^3 (where p is prime number),

1. $O(Z(G)) = p$
2. For all $a \notin Z(G)$, $o(N(a)) = p^2$
3. For all $a \notin Z(G)$, $|c(a)| = p$
4. Number of conjugate classes of cardinality one are p
5. Number of conjugate classes of cardinality p are $p^2 - 1$
6. Total number of conjugate classes G are $p^2 + p - 1$
7. Class equation of a non abelian group G

$$p^3 = o(G) = \overbrace{1 + 1 + ... + 1}^{p-times} + \overbrace{p + p + ... + p}^{(p^2-1)-times}$$

Class Equation of Q_8 (order of group is 2^3)

$$2^3 = o(Q_8) = \overbrace{1 + 1}^{2-times} + \overbrace{2 + 2 + 2}^{(p^2-1)=3-times}$$

Non abelian group G of order $2.p$ (where p is odd prime number)

1. $O(Z(G)) = 1$ (centre is always trivial)
2. For all $a \notin Z(G)$, $o(N(a)) = p$ or 2
3. Converse of Lagrange's theorem is true for a group G
4. There are $\left(\frac{p-1}{2}\right)$ conjugate classes of cardinality 2
5. There are exactly one conjugate classes of cardinality p
6. Total number of conjugate classes are $\frac{p+3}{2}$
7. Class equation of a non abelian group G is given by

$$o(G) = 2.p = 1 + p + \overbrace{2 + 2 + ... + 2}^{\frac{p-1}{2}-\text{times}}$$

Put Your Own Notes

Example:

Class Equation of group of permutation S_3 : order of group is $6 = 2.3$

$o(S_3) = 2.3 = 1 + 3 + 2$

Class Equation of Dihedral group D_5 : order of group is $10 = 2.5$

$o(D_5) = 2.5 = 1 + 5 + 2 + 2$

Class Equation of non Abelian group of order 22 :

$o(G) = 2.11 = 1 + 11 + 2 + 2 + 2 + 2 + 2$

Note: Two non-isomorphic group can have same class Equation

Example: K_4 & $\mathbb{Z}_4$ are non isomorphic but having same class Equation

Proposition 7.19: Let G be a finite group and $a, b \in G$. Then the probability that a and b be will

commute $= \dfrac{No.of\ Conjugate Classes}{o(G)}$

Example: Let $G = Q_8 \Rightarrow o(G) = 8$ Now, No. of conjugate class = 5 $\Rightarrow$ Probability that $a \& b$

commutes $= \dfrac{5}{8}$.

Proposition 7.20: Every non Abelian group has at least two conjugate classes

Proposition 7.21: If G is a group with trivial center, then the group Aut(G) also has trivial center.

Conjugacy classes in S_n and A_n

Proposition 7.22: For any cycle $(a_1 a_2 a_3 ... a_r) \in S_n$ and $\sigma \in S_n$. Then $\sigma(a_1 a_2 ... a_r)\sigma^{-1} = (\sigma(a_1)\sigma(a_2)...\sigma(a_r))$

Example: In S_5, let $\sigma = (13)(254)$. Then

$$\sigma(1432)\sigma^{-1} = (\sigma(1)\sigma(4)\sigma(3)\sigma(2)) = (3215)$$

since $\sigma(1) = 3,\ \sigma(4) = 2,\ \sigma(3) = 1$, and $\sigma(2) = 5$.

Example: In S_7, let $\sigma = (13)(265)$.

Then $\sigma(73521)\sigma^{-1} = (71263)$

since $\sigma(7) = 7,\ \sigma(3) = 1,\ \sigma(5) = 2,\ \sigma(2) = 6$, and $\sigma(1) = 3$.

Proposition 7.23: All cycles of the same length in S_n are conjugate.

Proposition 7.24: If π_1 and π_2 are disjoint permutations in S_n , then $\sigma\pi_1\sigma^{-1}$ & $\sigma\pi_2\sigma^{-1}$ are disjoint

permutations for any $\sigma \in S_n$

Proposition 7.25: Any two permutations in S_n are similar if they have same cycle decomposition

Put Your Own Notes

Proposition 7.26: Any two permutations in S_n are conjugate iff have same cycle decomposition

Proposition 7.27: Number of Conjugate classes in S_n are equal to number of distinct cycle decompositions

Proposition 7.28: Number of Conjugate classes in $S_n \doteq P(n)$, Where $P(n)$ is number of partitions of natural number n

Proposition 7.29: Let $\sigma \in S_n$ has the cycle decomposition $\{n_1, n_2, \ldots, n_k\}$ and let α_i be number of cycles of length i in $\{n_1, n_2, \ldots, n_k\}$ such that $\sum_{i=1}^{n} \alpha_i = n$. Then number of elements conjugate to σ i.e.,

$$|cl(\sigma)| = \frac{n!}{1^{\alpha_1}, 2^{\alpha_2} \ldots n^{\alpha_k} . \alpha_1 ! \alpha_2 ! \ldots \alpha_k !}$$

Example:

Number of Conjugate classes in S_3 are $P(3) = 3$ and S_4 are $P(4) = 5$

Conjugacy classes in A_n : If π is an even permutation, then $\sigma\pi\sigma^{-1}$ is also even, so a conjugacy class in S_n that contains one even permutation contains only even permutations. However, two permutations π_1 and π_2 in A_n can have the same cycle decomposition type (and thus be conjugate in the larger group S_n) while being non-conjugate in A_n. The point is that we might be able to get $\pi_2 = \sigma\pi_1\sigma^{-1}$ for some $\sigma \in S_n$ without being able to do this for any $\sigma \in A_n$.

Example: The 3-cycles (123) and (132) in A_3 are conjugate in $S_3 : (23)(123)(23)^{-1} = (132)$. However, (123) and (132) are not conjugate in A_3 because A_3 is abelian: an element of A_3 is conjugate in A_3 only to itself.

Example: The 3-cycle (234) and its inverse (243) are conjugate in S_4 but they are not conjugate in A_4. To see this, let's determine all possible $\sigma \in S_4$ that conjugate (234) to (243). For $\sigma \in S_4$, the condition $\sigma(234)\sigma^{-1} = (243)$ is the same as $(\sigma(2)\sigma(3)\sigma(4)) = (243)$. There are three possibilities:

Proposition 7.30: Let $\pi \in A_n$. Then its conjugacy class in S_n remains as a single conjugacy class in A_n or it breaks into two conjugacy classes in A_n of equal size.

Proposition 7.31: Let $\pi \in A_n$ be arbitrary. Then its conjugacy class in S_n breaks up into two conjugacy classes in A_n of equal size if and only if the cycle decomposition of π contains distinct odd numbers.

Example:

Let us Consider the group of permutation on 4-symbols

$S_4 = \{I, (12), (13), (14), (23), (24), (34), (12)(34), (13)(24), (14)(23), (123), (132),$

$(234), (243), (341), (314), (412), (421), (1234), (1432), (1342), (1243), (1423), (1324)$

$cl(I) = \{I\}$, Corresponding cyclic decomposition is $\{1,1,1,1\}$

Put Your Own Notes

$cl((12)) = \{(12),(13),(14),(23),(24),(34)\}$, Corresponding cyclic decomposition is $\{1,1,2\}$

$cl((12)(34)) = \{(12)(34),(13)(24),(14)(23)\}$ Corresponding cyclic decomposition is $\{2,2\}$

$cl((123)) =, \{(123),(132),(234),(243),(341),(314),(412),(421)\}$ Corresponding cyclic decomposition is $\{1,3\}$

$cl((1234)) = \{(1234),(1432),(1342),(1243),(1423),(1324)\}$ Corresponding cyclic decomposition is $\{4\}$

Thus Class Equation of S_4 is $o(S_4) = 24 = 1+6+3+8+6$

Now the Group of even permutations on 4-symbols

$A_4 = \{I,(12)(34),(13)(24),(14)(23),(123),(132),(234),(243),(341),(314),(412),(421)\}$ and the different cyclic decomposition are $\{1,1,1,1\}, \{2,2\}, \{1,3\}$

By Proposition 7.30, the different conjugate class of A_4 are

$cl(I) = \{I\}$,

$cl((12)(34)) = \{(12)(34),(13)(24),(14)(23)\}$ Corresponding cyclic decomposition is $\{2,2\}$ does not contains distinct odd numbers so the conjugacy class in S_n remains as a single conjugacy class in A_n

$cl((123)) =, \{(123),(132),(234),(243),(341),(314),(412),(421)\}$ Corresponding cyclic decomposition is $\{1,3\}$ contains distinct odd numbers. So, the conjugacy class in S_n breaks up into two conjugacy classes in A_n of equal size. Thus there are two conjugate classes.

$cl((123)) = \{(123),(234),(341),(412)\}$ and $cl((132)) = \{(132),(243),(314),(421)\}$

Conjugacy classes in S_n and A_n : The following tables list a representative from each conjugacy class in symmetric and alternating groups on 3 through 6 symbols , along with the size of the conjugacy classes.

1. Conjugacy classes and their size in S_3

	S_3		
Rep.	(1)	(123)	(12)
Size	1	2	3

Hence Class Equation is

$o(S_3) = 6 = 1+3+2$

2. Conjugacy classes and their size in A_3

A_3		
(1)	(123)	(132)
1	1	1

Hence Class Equation is

$o(A_3) = 3 = 1+1+1$

Put Your Own Notes

3. Conjugacy classes and their size in S_4

	S_4				
Rep.	(1)	(12)(34)	(12)	(1234)	(123)
Size	1	3	6	6	8

Hence Class Equation is

$o(S_4) = 24 = 1+6+3+8+6$

4. Conjugacy classes and their size in A_4

	A_4		
(1)	(12)(34)	(123)	(132)
1	3	4	4

Hence Class Equation is

$o(A_4) = 12 = 1+3+4+4$

5. Conjugacy classes and their size in S_5

	S_5						
Rep.	(1)	(12)	(12)(34)	(123)	(12)(345)	(12345)	(1234)
Size	1	10	15	20	20	24	30

Hence Class Equation is

$o(S_5) = 120 = 1+10+15+20+20+24+30$

6. Conjugacy classes and their size in A_5

	A_5				
Rep.	(1)	(12345)	(21345)	(12)(34)	(123)
Size	1	12	12	15	20

Hence Class Equation is

$o(A_5) = 60 = 1+12+12+15+20$

7. Conjugacy classes and their size in S_6

	S_6					
Rep.	(1)	(12)	(12)(34)(56)	(123)	(123)(456)	(12)(34)
Size	1	15	15	40	40	45
Rep.	(1234)	(12)(3456)	(123456)	(12)(345)	(12345)	
Size	90	90	120	120	144	

Hence Class Equation is

$o(S_6) = 720 = 1+15+15+40+40+45+90+90+120+120+144$

Put Your Own Notes

8. Conjugacy classes and their size in A_6

	A_6						
Rep.	(1)	(123)	(123)(456)	(12)(34)	(12345)	(23456)	(1234)(56)
Size	**1**	40	40	45	72	72	90

Hence Class Equation is

$o(A_6) = 360 = 1+40+40+45+72+72+90$

Conjugacy classes in dihedral Group D_n

Let's D_n is a dihedral Group of order $2n$, and $D_n = < a,b >$ where $a^2 = e$ is the reflection and b is the rotation such that $b^n = e$.

Case 1: Let n is an odd number. i.e., $n = 2m+1$ where $m \in \mathbb{N}$. Then the conjugacy classes, are the $\{b^i, b^{-i}\}$ for $1 \le i \le m$ and $\{ab^k \mid 0 \le k < n\}$. Thus

1. Class Equation of D_n is $o(D_n) = 2.n = 1+n+\underbrace{2+2+\ldots+2}_{\frac{n-1}{2}\text{ times}}$
2. Number of Conjugate Classes are $\frac{n+3}{2}$
3. $Z(D_n) = \{e\}$

Case 2: Let n is an even number. That is $n = 2m$ where $m \in \mathbb{N}$. Then the conjugacy classes, are the $\{b^i, b^{-i}\}$ for $1 \le i \le m$, $\left\{ab^{2k} \mid 0 \le k < \frac{n}{2}\right\}$ and $\left\{ab^{2k+1} \mid 0 \le k < \frac{n}{2}\right\}$. thus we have D_n where n is an odd number is

1. Class Equation of D_n is

$$o(D_n) = 2.n = 1+1+\frac{n}{2}+\frac{n}{2}+\underbrace{2+2+\ldots+2}_{\frac{n-2}{2}\text{ times}}$$

2. Number of Conjugate Classes are $\frac{n+6}{2}$

$Z(D_n) = \left\{e, b^{n/2}\right\}$

Put Your Own Notes

CHAPTER 8

INVARIANT / NORMAL SUBGROUP

8.1. Conjugacy of Subgroups

Let G be a group, H be subgroup of G and any $a \in G$ the set $aHa^{-1} = \{aha^{-1} : h \in H\}$ is a subgroup of G Conjugate of H. That two subgroup H and K are called conjugate if there exist $g \in G$ such that $K = gHg^{-1}$

Example: Let $G = S_3$ and $H = \{I, (12)\}$ be a subgroup of S_3. Then conjugate subgroups of H are $K_1 = \{I, (23)\}$ and $K_2 = \{I, (13)\}$

Proposition 8.1: The relation of conjugacy of subgroup is an equivalence relation

Proposition 8.2: Conjugate subgroup of group G are Isomorphic but converse need not to be

Example: $H_1 = \{e, a\}, H_2 = \{e, b\}$ are isomorphic subgroup of K_4 but they are not conjugate

8.2. Invariant/Normal Subgroups

A subgroup H of a group G is called an invariant subgroup (normal subgroup or normal divisor) of G if $g^{-1}h\,g \in G$ for all $g \in G$ and all $h \in H$

Note: H is an invariant subgroup of G and we writing $H \triangleright G$

Improper and Proper Normal Subgroups: In any group G has $\{e\}$ and G itself are invariant subgroups. They are called improper while other invariant subgroups, if any of G are called proper.

Proposition 8.3: Let G be a group and H is a invariant subgroup (normal subgroup) of G then

1. $gH = Hg$, $\forall g \in G$ since $g^{-1} \in G$ whenever $g \in G$
2. $g^{-1}Hg = H$ for every $g \in G$

Proposition 8.4: A subgroup H of a group G is normal subgroup of G iff H is only conjugate of subgroups of H.

8.3. Simple Group

A group G having no proper invariant subgroups is called simple.

Proposition 8.5: Every subgroup H of an abelian group G is an invariant subgroup of G since $g\,h = h\,g$, for any $g \in G$ and every $h \in H$.

Note: A Non-Abelian Group can have each of its subgroups a normal Subgroup

Example: Q_8 is a non abelian group & its every subgroup is normal

Put Your Own Notes

Proposition 8.6: Every non-trivial group G has at least two invariant subgroups $\{e\}$, and G itself.

Proposition 8.7: If H is a subgroup of index 2 of G the cosets generated by H consist of H and $G-H$ hence, H is an invariant subgroup of G

Proposition 8.8: If H is only subgroup G of order k then H is normal in G

Proposition 8.9: Intersection of normal subgroups is also normal

Proposition 8.10: If H and K are normal subgroup of G such that $H \cap K = \{e\} \Rightarrow HK$ subgroup of G

Examples of Normal Subgroups:

1. For $G = \{a, a^2.a^3, \ldots a^{12} = e\}$ its every subgroup is invariant.
2. The subgroup $H = \{I, (12)\}$ is not an invariant subgroup of S_4 since for $\alpha = (1234) \in S_4$ and $(12) \in S_4$, we have $(12)^{-1}\alpha(12) = (1342) \notin H$
3. $SL(n, R)$ is a Normal subgroup of $GL(n, R)$
4. $Z(G)$ is a Normal subgroup of G
5. A_n is Normal in S_n , $\forall n \in N$
6. H be a subgroup of G such that $x^2 \in H$, $\forall x \in G \Rightarrow H$ normal in G

8.4. Quotient Group

Let H normal subgroup of G and then $\frac{G}{H} = \{$set of all right/left cosets of H in G $\}$ $\frac{G}{H}$ is a Group under binary operation $Ha \cdot Hb = Hab$ and $O\left(\frac{G}{H}\right) = \frac{O(G)}{O(H)}$.

Examples of Quotient Group:

1. Let $(\mathbb{Z}, +)$ be group of integers and $m\mathbb{Z}$ be subgroup of $\mathbb{Z}$ then $\frac{\mathbb{Z}}{m\mathbb{Z}} = \{\mathbb{Z}, 1+\mathbb{Z}, 2+\mathbb{Z}, \ldots, (m-1)+\mathbb{Z}\}$ is fin ite Cyclic Group
2. $(\mathbb{Q}, +)$ is a group and $(\mathbb{Z}, +)$ is a subgroup then $\frac{\mathbb{Q}}{\mathbb{Z}} = \{\frac{m}{n} + \mathbb{Z} \mid \frac{m}{n} \in \mathbb{Q}\}$ is infinite order group

Properties of Quotient Group of $(\mathbb{Q}, +)$ by $(\mathbb{Z}, +)$:

1. $\frac{\mathbb{Q}}{\mathbb{Z}} = \left\{\frac{m}{n} + \mathbb{Z} \mid \frac{m}{n} \in \mathbb{Q}\right\}$ is an infinite order abelian group
2. $\frac{\mathbb{Q}}{\mathbb{Z}}$ is generated by $S = \left\{\frac{1}{p^n} + \mathbb{Z} \mid p \text{ is prime}, n \in \mathbb{N}\right\}$ hence infinitely generated group
3. Every element of $\frac{\mathbb{Q}}{\mathbb{Z}}$ is of finite order.

Put Your Own Notes

4. $\forall n \in \mathbb{N}$, $\frac{\mathbb{Q}}{\mathbb{Z}}$ has an element of order n namely $\frac{1}{n}+\mathbb{Z}$

5. $\forall n \in \mathbb{N}$, $\frac{\mathbb{Q}}{\mathbb{Z}}$ has exactly $\phi(n)$ elements order n namely $m<n$, where $\gcd(m,n)=1$ and $m<n$

6. $\forall n \in \mathbb{N}$, $\frac{\mathbb{Q}}{\mathbb{Z}}$ has cyclic subgroup of order n

   (a) $\forall n \in \mathbb{N}$, $\frac{\mathbb{Q}}{\mathbb{Z}}$ has exactly one subgroup of order n

7. $\frac{\mathbb{Q}}{\mathbb{Z}}$ has countable number of subgroup of finite order.

8. Every Finite order subgroup of $\frac{\mathbb{Q}}{\mathbb{Z}}$ is cyclic and finitely generated.

9. Every infinite order subgroup of $\frac{\mathbb{Q}}{\mathbb{Z}}$ is not cyclic.

10. Every infinite order subgroup of $\frac{\mathbb{Q}}{\mathbb{Z}}$ is not finitely generated.

11. Every proper subgroup of $\frac{\mathbb{Q}}{\mathbb{Z}}$ is of infinite index.

Important Subgroup Quotient group of $(\mathbb{Q},+)$ by $(\mathbb{Z},+)$

Consider the subset $H=\left\{\frac{m}{2^n}+\mathbb{Z} \mid m \in \mathbb{Z}, n=0,1,2...\right\}$ of $\frac{\mathbb{Q}}{\mathbb{Z}}$

1. H is proper Normal Subgroup of $\frac{\mathbb{Q}}{\mathbb{Z}}$ and it is of infinite order

2. H is infinitely generated Subgroup of $\frac{\mathbb{Q}}{\mathbb{Z}}$

3. H is non cyclic subgroup of $\frac{\mathbb{Q}}{\mathbb{Z}}$

4. Every elements of H is finite order and $\forall a \in H$ the order of a is 2^k form

5. Every finite order subgroup of H is cyclic

6. Every proper subgroup of H is of finite order where as H is of infinite order

7. Every proper subgroup of H is Cyclic where as H is non cyclic

8. Every proper subgroup of $\frac{\mathbb{Q}}{\mathbb{Z}}$ is of infinite index.

Proposition 8.11: Quotient group of finite group is finite

Proposition 8.12: Let $(\mathbb{Z},+)$ be group of $\frac{\mathbb{Z}}{m\mathbb{Z}} \cong \mathbb{Z}_m$ thus in general quotient group of infinite group is may or may not finite

Proposition 8.13: Quotient group of infinite group may or may not be finite.

Example: $H=2\mathbb{Z}, G=\mathbb{Z}$ then $\frac{G}{H}=\frac{\mathbb{Z}}{2\mathbb{Z}} \cong \mathbb{Z}_2$

Put Your Own Notes

Proposition 8.14: Quotient group of Abelian group is abelian, i.e. if G is abelian $\Rightarrow \frac{G}{H}$ is abelian

Proposition 8.15: Quotient group of cyclic group is cyclic, i.e. if G is cyclic $\Rightarrow \frac{G}{H}$ is cyclic

Proposition 8.16: Quotient group $\frac{G}{H}$ abelian $\not\Rightarrow$ G abelian e.g. A_n normal in S_n , $\forall n \in N$ $\frac{S_n}{A_n}, \forall n \geq 3$ abelian but S_n , $\forall n \geq 3$ non-abelian

Proposition 8.17: Quotient group $\frac{G}{H}$ cyclic $\not\Rightarrow$ G cyclic e.g. A_n normal in S_n , $\forall n \in N$, $\frac{S_n}{A_n}, \forall n \geq 3$ is cyclic but S_n , $\forall n \geq 3$ is non-cyclic.

Proposition 8.18: H is normal subgroup of G and index of $H = m$ $\Rightarrow \forall\ x \in G,\ x^m \in H$

Proposition 8.19: Let $Z(G)$ is the centre of G then $\frac{G}{Z(G)}$ cyclic $\Rightarrow G$ abelian

Proposition 8.20: Every normal subgroup of any group is union of it's complete conjugacy classes.

Proposition 8.21: If H and K are subgroups of a group G, then HK is subgroup if if either H or K is normal in G

Propositions 8.22: If H and K are normal subgroups of a group G, then HK is normal subgroup

8.5. Maximal Subgroups

A normal subgroup H of a group G called maximal provided there does not exist any proper normal subgroup K of G having H as a proper subgroup.

Example:

(a) A_4 is a maximal invariant subgroup of S_4 since it is a subgroup of index 2 in S_4

(b) $\{I,(12)(34),(13)(24),(14)(23)\}$ is a maximal invariant subgroup of A_4

(c) They cyclic group $G = \{e, a, a^2, \ldots, a^{11}\}$ has $H = \{e, a^2, a^4, \ldots, a^{10}\}$ and $K = \{e, a^3, a^6, \ldots, a^9\}$ as maximal invariant subgroups. Also $J = \{e, a^4, a^8\}$ is a maximal invariant subgroup of H while $L = \{e, a^6\}$ is a maximal invariant subgroup of both H and K

Note: A_5 is simple as no combination of terms in its classes equation divides 60

Put Your Own Notes

Some Important Theorems:

Theorem 8.1: Let H and K be invariant subgroups of G with H an invariant subgroup of K, and let $P = K/H$ and $S = G/H$. Then quotient groups S/P and G/K are isomorphic. (Freshman's Theorem)

Theorem 8.2: If H is a maximal invariant subgroup of group G then G/H is simple, and conversely.

Theorem 8.3: Let H and K be distinct maximal invariant subgroups of a group G. Then $D = H \cap K$ is an invariant subgroup of G, and H/D is isomorphic to G/K and K/D is isomorphic to G/H.

Normal Subgroups of S_n

1. Number of normal subgroup of $S_n = \begin{cases} 4 & n = 4 \\ 3 & n \neq 4 \end{cases}$
2. List of Normal Subgroup of $S_n = \begin{cases} \{I\}, \cong K_4, A_4, S_4 & , n = 4 \\ \{I\}, A_n, S_n & , n \neq 4 \end{cases}$
3. A_n is proper normal subgroup of S_n
4. S_n is not simple for all $n \geq 3$

Normal Subgroups of $A_n, n > 3$

1. Number of normal subgroup of $A_n = \begin{cases} 3 & n = 4 \\ 2 & n \neq 4 \end{cases}$
2. List of Normal Subgroup of $A_n = \begin{cases} \{I\}, \cong K_4, A_4 & , n = 4 \\ \{I\}, A_n & , n \neq 4 \end{cases}$
3. A_n is simple for all $n \geq 5$

Put Your Own Notes

CHAPTER 9

HOMOMORPHISM AND THEIR COUNTING

9.1. Definitions

Homomorphism: Let $(G,*)\&(G',\circ)$ are two groups then a homomorphism ϕ from G to G' is a mapping from G into G' that preserves the group operation; that is $\phi(a*b)=\phi(a)\circ\phi(b)\ \forall a,b\ in\ G$.

OR

Let G, G' be two groups. By a homomorphism of G into G' meant a mapping. $\phi: G\to G':\ g\to g'$ such that every $g\in G$ has a unique image $g'\in G'$ such that $\phi(g_1.g_2)=\phi(g_1)*\phi(g_2)$.

Note: If we have a homomorphism of G onto G' and we then call G' a homomorphic image of G.

Kernel of Homomorphism: The kernel of a homomorphism ϕ from G to a group G' with identity e' is the set of all elements of G which are mapped to identity $e'\in G'$. The kernel of ϕ is denoted by $\ker\phi$. i.e., $\ker\phi=\{x\in G:\phi(x)=e'\}$

Note: $\phi: G\to G'$ be a homomorphism then $\ker\phi$ is normal subgroup of G.

Range set of homomorphism: Let $f: G\to G'$ be a homomorphism the range set of f is set of all elements of G' whose pre-image exists, i.e., $R(f)=\{f(x)\in G'|x\in G\}$

Epimorphism: Onto homomorphism from $f: G\to G'$ is called Epimorphism

Isomorphism: One-one homomorphism from $f: G\to G'$ is called Isomorphism

Isomorphic: Two Groups $(G,*)$ and (G',o) are called isomorphic if there exists Isomorphism from $(G,*)$ onto (G',o)

Endomorphism: A homomorphism from $f: G\to G$ is called Endomorphism

Automorphism: - An **Isomorphism** from $(G,*)$ **onto** $(G,*)$ itself is called automorphism

Inner- Automorphism: - Let $(G,*)$ be a group then a $f: G\to G$ such that $f_a(x)=axa^{-1}, \forall x\in G$ is an automorphism is called inner automorphism

Put Your Own Notes

9.2. Notations

Let $e \in G$ be the identity elements of group G ,and $e' \in G'$ be the identity elements of group G'

$Hom(G,G')$ denotes set of all homomorphisms from $(G,*)$ into $(G',\circ)$

$Hom(G,*)$ denotes set of all homomorphisms from $(G,*)$ into $(G,*)$ itself

$Iso(G,G')$ denotes set of all Isomorphisms from $(G,*)$ into $(G',\circ)$

$Iso(G,*)$ denotes set of all Isomorphisms from $(G,*)$ into $(G,*)$ itself

$Aut(G,*)$ denotes set of all Automorphisms from $(G,*)$ onto $(G,*)$ itself

$Inn(G,*)$ denotes set of all Inner-automorphisms from $(G,*)$ onto $(G,*)$ itself

Some Examples

1. Consider the mapping $n \to i^n$ from the additive group $\mathbb{Z}$ onto the multiplicative group of the fourth roots of unity 1 . This is a homomorphism since, $m+n \to i^{m+n} = i^m\ i^n$ and the group operation is preserved.
2. Consider the cyclic group $G = \{a, a^2, a^3, \ldots, a^{12} = e\}$ and its subgroup $G' = \{a^2, a^4, a^6 \ldots, a^{12} = e\}$. It follows readily that the mapping. $a^n \to a^{2n}$ is a homomorphism of G onto G' while the mapping $a^n \to a^n$ is a homomorphism of G' into G .

9.3. Elementary Properties of Homomorphism

Let $(G,*)$ and (G',o) are two group and $f: G \to G'$ be a homomorphism. Then

(a) The identity element of group G maps to the identity elements of group G',i.e $f(e) = e'$

(b) The Image of inverse of an element is inverse of image of that element,i.e. $f(a^{-1}) = (f(a))^{-1}$

(c) If $f(a) = x \Rightarrow f(a^r) = x^r \quad \forall\ r \in \mathbb{Z}$

(d) The $Kerf = \{x \in G \mid f(x) = e'\}$ is Normal subgroup of G

(e) $R(f)$ is subgroup of G' but need not to be normal subgroup G' (but normal if f is onto).

(f) Order of image of an element divide the order of that element, i.e. $O(f(a)) / O(a) \quad \forall a \in G$, provided $O(a)$ is finite

(g) If $O(a)$ finite $\Rightarrow$ $O(f(a))$ finite but $O(f(a))$ finite $\not\Rightarrow$ $O(a)$ finite

(h) If $f(a) = \alpha$ then $\forall\ x \in a \cdot Kerf$ (coset of $Kerf$) $f(x) = \alpha$,i.e. the image of all element of a coset $a \cdot Kerf$ is same as the image of a i.e., There is one-to-one correspondence between coset of $Kerf$ and elements of $f(G)$

Put Your Own Notes

(i) Let G be a finite group Index of $Kerf = O(f(G))$ i.e., If order of G finite then $\frac{o(G)}{0(Kerf)} = o(f(G))$

(j) $O(Kerf) = m \Leftrightarrow f$ is m to 1 homomorphism. Hence $Kerf = \{e\}$ iff f 1-1 homomorphism

(k) The relation of isomorphism is an equivalence relation.

(l) Let H is subgroup of G, then $f(H)$ is subgroup of G'

(m) If image of subgroup H under homomorphism is normal then H is normal,i.e. Let H is subgroup of G. Then if $f(H) \triangleleft G' \Rightarrow H \triangleleft G$, but converse need not be true.

(n) Image of abelian group under homomorphism is abelian, i.e. If G is abelian $\Rightarrow f(G)$ is abelian

(o) Image of cyclic group under homomorphism is cyclic ,i.e. If G is cyclic $\Rightarrow f(G)$ is cyclic

(p) There never exist any onto homomorphism from an abelian group onto a non-abelian group

(q) There never exist any onto homomorphism from a cyclic group onto non-cyclic group

9.4. Some Important Theorems

Theorem 9.1: Every infinite cyclic group $G =< a >$ is isomorphic to $(\mathbb{Z}, +)$

Define $f : \mathbb{Z} \to G$ such that $f(n) = a^n$. Then f is one-one homomorphism from $\mathbb{Z}$ onto G

Theorem 9.2: Every finite cyclic group $G =< a >$ of order n is isomorphic to $(\mathbb{Z}_n, +_n)$

Define $f : \mathbb{Z}_n \to G$ such that $k \to a^k$ then f is one-one homomorphism from $\mathbb{Z}_n$ onto G

Theorem 9.3: Let $\mathbb{Z}$ be group of integers and $< n >$ is subgroup of $\mathbb{Z}$. Then quotient group $\frac{\mathbb{Z}}{< n >} \cong \mathbb{Z}_n$ where $n \in \mathbb{N}$.

Theorem 9.4: Let G and G' are two cyclic group of same order then they are isomorphic and isomorphism is which map generator of G onto generator of G'

Theorem 9.5: A group G abelian iff $f(x) = x^{-1}$ is an automorphism

Theorem 9.6: Every odd order abelian group has non-trival automorphism, namely $f(x) = x^{-1} \ \forall x \in G$

Theorem 9.7: G Is finite cyclic group of order n then $f : G \to G$ defined as $f(x) = x^m$, $f; g : G \to G$ defined as $f(a) = a$ and $g(a) = a$, $\gcd(m, n) = 1$, $1 \le m < n$ is an automorphism and $Aut(G) \cong U(n)$.

Put Your Own Notes

Theorem 9.8: If $G =< a >$ be an infinite cyclic group. Then are the only automorphisms and $Aut(G) \cong Z_2$

Theorem 9.9 (Cayley's Theorem): Every finite group of order n is isomorphic to a subgroup of a permutation group on n Symbols

Theorem 9.10: If H is an invariant subgroup of G of order m and order of G is n, then the quotient group G/H is of order n/m

Theorem 9.11: If H is an invariant subgroup of a group G, the mapping $\phi : G \to G/H$ defined as $\phi(g) = Hg$ Is a homomorphism of G onto G/H

Theorem 9.12: If H is an invariant subgroup of a group G and if H is also a subgroup of a subgroup K of G, then H is an invariant subgroup of K.

9.5. Fundamental theorem of homomorphism

First Theorem on Isomorphism:

"Every homomorphic image of a group is isomorphic to the quotient group induced by kernel of homomorphism i.e., If $\phi : G \to G'$ is homomorphism, then $\frac{G}{\ker \phi} \cong f(G) \Rightarrow \frac{o(G)}{o(Ker\varphi)} = o\left[\phi(G)\right]$

Note: Every normal subgroup of a group G is the kernel of a homomorphism of G. In particular, normal subgroup N is the kernel of the mapping $f : G \to \frac{G}{N}$ defined by $f(g) = Ng$ or gN

Second Isomorphism Theorem (Correspondence Theorem): If H is normal subgroup of G and K is another subgroup of G. Then $\frac{K}{(H \cap K)} \cong \frac{HK}{H}$

Third Isomorphism Theorem (Freshman's Theorem): Let H and K be normal subgroups of a group G, with $K \leq H$. Then $\frac{G}{H} \cong \frac{(G/K)}{(H/K)}$

9.6. Important Propositions of Homomorphism/Isomorphism

Propositions 9.13: Let G be a group and $Aut(G)$ be set of all automorphism is subgroup of S_G (group of permutation on G) under composition of functions

Propositions 9.14: Inn (G) (set of all Inner automorphism) is normal subgroup of $Aut(G)$

Propositions 9.15: Let $a \in (Z(G))$ be arbitrary. Then corresponding to 'a', there is only one inner Automorphism which is identity map

Propositions 9.16: Index of center $Z(G) = O(Inn(G))$

Propositions 9.17: Let G be a finite Group and $Z(G)$ be centre of G. Then $\frac{G}{Z(G)} \cong Inn(G)$

Put Your Own Notes

Propositions 9.18: If G is an abelian then Identity function is only the inner automorphism G onto itself

Propositions 9.19: G is abelian iff the function $f:G\to G$ such that $f(x)=x^2\ \forall x\in G$ is a homomorphism

Propositions 9.20: G abelian group $f(x)=x^n, \forall x\in G$ Homomorphism for each $n\in N$

9.7. Counting of Homomorphism

1. Counting of from finite cyclic group G of order m to finite cyclic G' of order n

   (i) Number of homomorphism from G to $G' = \gcd(m,n)$

   (ii) Number of onto homomorphism from $G\to G' = \begin{cases} 0 & if\ n\nmid m \\ \phi(m) & if\ n\mid m \end{cases}$

   (iii) Number of one-one homomorphism from $G\to G' = k$ (number of elements of order m in G')

   Examples:

   (a) Number of homomorphism from $\mathbb{Z}_6\to\mathbb{Z}_8 = \gcd(6,8)=2$

   (b) Number of onto homomorphism from $\mathbb{Z}_6\to\mathbb{Z}_8$ zero

   (c) Number of onto homomorphism from $\mathbb{Z}_{16}\to\mathbb{Z}_8 = \phi(8)=4$

   (d) Number of one-one homomorphism from $\mathbb{Z}_{16}\to\mathbb{Z}_8$ zero

   (e) Number of one-one homomorphism from $\mathbb{Z}_5\to\mathbb{Z}_{10} = \phi(5)=4$

2. Counting of from infinite cyclic group G to infinite cyclic G'

   (i) Number of homomorphism from G to G' infinite

   (ii) Number of onto homomorphism from $G\to G'$ exactly two

   (iii) Number of one-one homomorphism from $G\to G'$ infinite

3. Counting of from infinite cyclic group G to any finite group G' of order m

   (i) Number of homomorphism m

   (ii) Number of onto homomorphism $= \begin{cases} 0 & G'\ non\ cyclic \\ \phi(m) & G'\ cyclic \end{cases}$

   (iii) One-one homomorphism does not exist.

Put Your Own Notes

Example

From	Hom.	Onto Hom	Ono-One Hom
$Z \to Z_n$	n	$\phi(n)$	0
$Z \to S_n, n \geq 3$	$n!$	0	0
$Z \to A_n, n \geq 4$	$\frac{n!}{2}$	0	0
$Z \to K_4$	4	0	0
$Z \to Q_8$	8	0	0
$Z \to Z_n \times Z_m$ $g.c.d(m,n) \neq 1$	$n \cdot m$	0	0
$Z \to D_{2n}$	$2n$	0	0
$Z \to GL(n, Z_p)$	$(P^n - 1)(P^n - P)\ldots(P^n - P^{n-1})$	0	0
$Z \to SL(n, Z_p)$	$\frac{(P^n - 1)(P^n - P)\ldots(P^n - P^{n-1})}{P-1}$	0	0

4. Counting of homomorphism from any finite group G' of order m to infinite cyclic group G to

(i) There is only trivial homomorphism from $G' \to G$

(ii) Number of onto homomorphism from G' onto G

$$= \begin{cases} 0 & , \ m > 1 \\ 1 & , \ m = 1 \end{cases}$$

(iii) There does not exist any one-one homomorphism from G' into G

5. Counting of homomorphism from finite G cyclic group of order n to any finite group G' of order m

(i) Number of homomorphism $= \sum_{k/o(G)} \alpha_k$, Where α_k number of elements of order k in G'

(ii) Number of onto homomorphism $= \begin{cases} \phi(m) : G' cyclic \ \& \ m \mid n \\ 0 \qquad otherwise. \end{cases}$

(iii) Number of one-one homomorphism $= \alpha_n$, Where α_n number of elements of order n in G'

Example

Put Your Own Notes

Group's	Hom.	Onto Hom.	One-one Hom.

6. Counting of from $S_n \to Z_m, (n \geq 3,)$

(i) Number of homomorphism $= \begin{cases} 1 & \text{if m odd} \\ 2 & \text{if m even} \end{cases}$

(ii) Number of onto homomorphism $= \begin{cases} 1 & ,m = 1,2 \\ 0 & ,other\ wise \end{cases}$

(iii) Number of one-one homomorphism does not exist

7. Counting of from $A_4 \to Z_m$

(i) Number of homomorphism $= \begin{cases} 3 & ,if\ 3|\text{m} \\ 1 & ,if\ 3\nmid \text{m} \end{cases}$

(ii) Number of onto homomorphism $= \begin{cases} 1 & ,if\ \text{m=1} \\ 2 & ,if\ m = 3 \\ 0 & ,Otherwise \end{cases}$

(iii) Number of one-one homomorphism does not exist

8. Counting of from $A_n \to Z_m, (n \geq 5)$

(i) Number of homomorphism only trivial

(ii) Number of onto homomorphism $= \begin{cases} 1 & ,if\ \text{m=1} \\ 0 & ,Otherwise \end{cases}$

(iii) Number of one-one homomorphism does not exist

9. Counting of from $K_4 \to Z_n$

(i) Number of homomorphism $= \begin{cases} 4 & m \text{ even.} \\ 1 & m \text{ odd.} \end{cases}$

(ii) Number of onto homomorphism $= \begin{cases} 1 & m = 1. \\ 3 & m = 2. \\ 0 & otherwise. \end{cases}$

(iii) Number of one-one homomorphism does not exists

Put Your Own Notes

10. Counting of from $Q_8 \to Z_m$

(i) Number of homomorphism $= \begin{cases} 4 & m \text{ even.} \\ 1 & m \text{ odd.} \end{cases}$

(ii) Number of onto homomorphism $= \begin{cases} 1 & m = 1. \\ 3 & m = 2. \\ 0 & otherwise. \end{cases}$

(iii) Number of one-one homomorphism does not exists

11. Counting of from $K_4 \to Q_8$

(i) Number of homomorphism $= 4$

(ii) Number of onto homomorphism does not exist

(iii) Number of one-one homomorphism does not exist

12. Counting of from $Q_8 \to K_4$

(i) Number of homomorphism $= 16$

(ii) Number of onto homomorphism $= 6$

(iii) Number of one-one homomorphism does not exist

13. Counting of from $S_n \to K_4, (n \geq 3)$

(i) Number of homomorphism $= 4$

(ii) Number of onto homomorphism does not exist

(iii) Number of one-one homomorphism does not exist

14. Counting of from $K_4 \to S_4$

(i) Number of homomorphism $= 52$

(ii) Number of onto homomorphism does not exist

(iii) Number of one-one homomorphism $= 24$

15. Counting of from $K_4 \to S_n, n \neq 4$ & $n \geq 3$.

(i) Number of homomorphism =3(Number of elements of order 2)+6(Number of Non-cyclic subgroup of order 4)+1

(ii) Number of onto homomorphism does not exist

(iii) Number of one-one homomorphism =6 (number of non-cyclic subgroup of order 4)

16. Counting of from $S_n \to Q_8, n \geq 3$

(i) Number of homomorphism $= 2$

(ii) Number of onto homomorphism does not exist

(iii) Number of one-one homomorphism does not exist

17. Counting of from $A_n \to K_4, n \geq 4$

(i) Number of homomorphism only trivial

(ii) Number of onto homomorphism does not exist

(iii) Number of one-one homomorphism does not exist

18. Counting of from $A_n \to Q_8, n \geq 4$

(i) Number of homomorphism only trivial

(ii) Number of onto homomorphism does not exist

(iii) Number of one-one homomorphism does not exist

Put Your Own Notes

9.8. Internal Direct Product

Let $H_1, H_2, ..., H_n$ be subgroups of a group G. Then G is the Internal direct product of $H_1, H_2, ..., H_n$ iff

1. Every element of H_i commute with every element of $H_j, i \neq j$ and

2. Every element of G is uniquely expressible as $g = h_1 h_2 ... h_n$, where $h_i \in H_i,\ 1 \leq i \leq n$.

Example:

(a) The multiplication group $\mathbb{R}^*$ of all non-zero real numbers is the internal direct product of $\mathbb{R}^+$ and T, where $\mathbb{R}^+$ is the set of all positive real numbers and $T = \{1, -1\}$.

(b) Let $\mathbb{C}^*$ be the multiplication group of non-zero complex numbers. If $\mathbb{R}^+$ is the set of positive real numbers and $T = \{z \in \mathbb{C}^* : |z| = 1\}$ Then, $\mathbb{C}^*$ is the internal direct product of $\mathbb{R}^+$ and T.

Internal Direct Product: Let G be a group. We say G is internal direct product of it's subgroups H_1 and H_2 if and only if

(i) $H_1 \trianglelefteq G,\ H_2 \trianglelefteq G,\ H_1 \cap H_2 = \{e\}$

(ii) $G = H_1 H_2$

***Theorem* 9.1:** If a group G is the internal direct product of its subgroups $H_1, H_2 ... H_n$, then G is isomorphic to the external direct product of $H_1, H_2 ... H_n$

***Theorem* 9.2:** If p, q be distinct primes. then Z_{pq} can be expressed as a direct product of a cyclic group of order p and a cyclic group of order q and

Propositions 9.21: The external direct product of additive group of integers $\mathbb{Z}$ with itself is not a cyclic group i.e. $\mathbb{Z} \times \mathbb{Z}$ is not a cyclic group

Propositions 9.22: The external direct product of additive group of integers $\mathbb{Z}$ with $\mathbb{Z}_m, m \neq 1$ is not a cyclic group i.e. $\mathbb{Z} \times \mathbb{Z}_m, m \neq 1$ is not a cyclic group

Propositions 9.23: If $G_1, G_2, ...G_n$ are n groups then $Z(G_1 \times G_2 \times ..... \times G_n) = Z(G_1) \times Z(G_2) \times ..... \times Z(G_n)$

Propositions 9.24: If G is a group and H, K are subgroups of G such that $G = H \times K$, then $H \cong G/K$ and $K \cong G/H$.

Propositions 9.25: Let G be a finite group having at least three elements in which $a^2 = e, \forall a \in G$. Show that G is internal direct product of a finite number of subgroups each order 2; and $o(G) = 2^n$, for some $n \geq 2$

Propositions 9.26: The external direct product of two group is abelian iff both are abelian

Propositions 9.27: The external direct product of two cyclic group need not be cyclic

Put Your Own Notes

CHAPTER 10

SYLOW THEOREMS

In this section, we consider p, q, r etc stand for prime numbers

10.1. Definitions

p - Groups: let G be a group then G is called p - group if order of every element is some power of p

Example:

(a) $(P(\mathbb{N}), \Delta)$ is 2-group of infinite order

(b) Q_8 is 2-Group of finite order

(c) $K_4 = \{e, a, b, c\}$ is 2-Group of finite order

(d) $H_{p^n} = < \alpha >$, where α is $p^n - th$ root of unity in $\mathbb{C}^*$ and p is prime number then $H = \bigcup_{n \in \mathbb{N} \cup \{0\}} H_{p^n}$ is a subgroup of $(\mathbb{C}^*, \bullet)$ is p-group

(e) For each prime p there exists p-group

(f) $H = \left\{ \frac{m}{p^n} + \mathbb{Z} \mid m \in \mathbb{Z}, n = 0, 1, 2... \right\}$ is subgroup of $\frac{\mathbb{Q}}{\mathbb{Z}}$ for each prime is p-Group

Propositions 10.1: A finite group G is a ^{p}-group if and only if $o(G) = p^n$

Propositions 10.2: Every subgroup of a p-group is p-subgroup

Propositions 10.3: A non- p-group can have p-subgroup

Example: $\frac{\mathbb{Q}}{\mathbb{Z}}$ is not a p-group but $H = \left\{ \frac{m}{p^n} + \mathbb{Z} \mid m \in \mathbb{Z}, n = 0, 1, 2... \right\}$ is p-subgroup

Propositions 10.4: Every group of Composite order group have p-subgroup for distinct prime p Such that $p \mid O(G)$

Maximal p-subgroup or p-sylow subgroup $(p\text{-}SSG)$: The largest p-subgroup of any group G is defined as maximal p-subgroup or sylow p-subgroup

Example:

1. $H = \left\{ \frac{m}{p^n} + \mathbb{Z} \mid m \in \mathbb{Z}, n = 0, 1, 2... \right\}$ is maximal p-subgroup $\frac{\mathbb{Q}}{\mathbb{Z}}$
2. $\{\pm 1, \pm i\}, \{\pm 1, \pm j\}, \{\pm 1, \pm k\}$ are maximal subgroup of Q_8
3. $\{e, a\}, \{e, b\}, \{e, c\}$ are maximal subgroup of K_4

Put Your Own Notes

Propositions 10.5: Let G be finite order group if $H < G$ and $O(H) = p^m$ *s.t.* $p^{m+1} \nmid O(G)$ then H is a $p-SSG$.

Cauchy's Theorem for Finite Groups: Let G be a finite group and p divides the order of G, then G contains an element of order p.

Example: Every group of order 15 has an element of order 5 and an element of order 3 as 5 & 3 are primes and $5 \mid 15$, $3 \mid 15$.

Generalized Cayley's Theorem: Let G be a group and has a subgroup H of index n then there exist a homomorphism from G into S_n. Whose kernel is contained in H and kernel of their homomorphism contains every that normal subgroup of G which is contained in H.

Index Theorem: Let G be a group and H is proper subgroup of G such that index of H is n. If $O(G)$ does not divide $n!$ then G is not simple i.e., G must contain a proper normal subgroup.

Example: Let $o(G) = 24$ and H be subgroup of G such that $o(H) = 8$. then $i_G(H) = 3$. Since, $o(G) = 24 \nmid 3! \Rightarrow G$ must has a proper normal subgroup $\Rightarrow G$ is not simple group

Note: Index theorem is only a sufficient condition to check whether group is simple or not.

Embedded Group: Let G and G' be two groups then G is said to be **embedded in** G' if there exist a subgroup H of G' such that G is isomorphic to H.

Example:

(a) K_4 Embedded in D_4

(b) K_4 Embedded in S_4

(c) K_4 Embedded in A_4

(d) Q_8 Embedded in S_8

(e) D_4 Embedded in S_4

(f) S_3 Embedded in D_3

(g) S_3 Embedded in S_4

Embedding Theorem: Let G be a finite simple group having a proper subgroup of index n then G is isomorphic to a subgroup of A_n i.e., G is embedded in A_n

Note: Embedding theorem is generally used to find the groups which not simple.

Propositions 10.6: G has a proper subgroup of index n such that $o(G) \nmid \left(\frac{n!}{2}\right)$ then G cannot be simple.

Propositions 10.7: If a finite group G has a proper subgroup H of index less than 5. Then G cannot be simple. i.e., the smallest index of any proper subgroup in a simple group is 5.

Put Your Own Notes

10.2. Sylow Theorems

(Sylow's First Theorem): Every finite group G of order n has at least one p-SSG corresponding to each prime factor of n.

(Generalized Sylow's First Theorem): If $p^\alpha / o(G)$ then G has a subgroup of order p^α

Propositions 10.8: Converse of Lagrange's theorem holds for every p-groups.

Note: Converse of Lagrange's theorem is not true in general; A_5 has no subgroup of order 30 though $30 / o(A_5) = 60$

(Sylow's Second Theorem): Any two sylow p-subgroup of a finite group G are conjugate to one another.

(Sylow's Third Theorem): Let k be the number of p-SSG of a finite group G. Then

1. k divides $o(G)$
2. k is of the form $1 + pt$, where $t = 0, 1, 2, 3...$

10.3. Structure of Some Important Groups

Group of order $p.q$: Let G be a group of order pq, where $p < q$ are distinct primes

1. If $p \nmid q-1$ then G must be cyclic that is $G \cong \mathbb{Z}_{p.q}$ that is there is unque group of order $p.q$ upto isomorphic

   Example:

   (a) The groups of the order 15, 33, 51 are cyclic

   (b) The groups of the order 35 & 65 c are cyclic

2. If $p \mid q-1$ then there exist two group of order $p.q$ upto isomorphic one is non cyclic another is non cyclic

   (a) There are two group of each order $2.q$ for each prime q upto isomorphism

   (b) There are two group of each order 21 upto isomorphism

   (c) There are two group of each order 22 upto isomorphism

   (d) There are two group of each order 55 upto isomorphism

3. Every abelian group of order $p.q$ where $p < q$ distinct primes is cyclic
4. There does not exists any group of order $p.q$ where $p < q$ distinct primes which non cyclic abelian

Propositions 10.8: Let G be a finite p-group, Then every proper subgroup is a proper subgroup of its normaliser in G (i.e, if $o(G) = p^n, H \le G, H \ne G$, then $\exists\ g \in G,\ g \in H$, s.t. $gHg^{-1} = H$)

Put Your Own Notes

Propositions 10.9: Let $o(G) = p^n$ (p=prime). If $H \leq G$ s.t. $o(H) = p^{n-1}$, show that H is normal in G.

Propositions 10.10: Let G be an abelian group of order n. Then for every divisior m of n, G has a subgroup of order m

Propositions 10.11: Converse of Lagrange's theorem holds in finite abelian groups

Propositions 10.12: Let p be a prime and m be a positive integer such that p^m divides $o(G)$. Then $\exists$ a subgroup H of G s.t. $o(H) = p^m$

Propositions 10.13: If G a finite group of order $n = p^k q (k \geq 1)$, where p is a prime and q be a positive integer (p, q relatively prime) then for each i, $1 \leq i \leq k$. G has a subgroup of order p^i

Propositions 10.14: let H be a Sylow p-subgroups of G then the number of Sylow p-subgroups of G is equal to $\frac{o(G)}{o(N(H))}$

Propositions 10.15: Let H be a Sylow p-subgroup of G. Let $x \in N(P)$ s.t. $o(x) = p^i$. Then $x \in H$

Propositions 10.16: Every p-subgroup of a finite group G is contained in some Sylow p-subgroup of G

Propositions 10.17: Let G be a finite group and H be a p-subgroup of G then H is Sylow p-subgroup of G if and only if no p-subgroup of G properly contains H

Propositions 10.18: If G is a finite non-abelian simple group and $H \leq G$. Then $[G:H] \geq 5$

Example: There is no simple group of order 144

Propositions 10.19: Suppose that G is a finite group and p is the smallest prime divisor of $o(G)$, then a subgroup H of index p in G is normal in G

Propositions 10.20: Let G be a group of order pqr, $p < q < r$ being primes then

1. G is not simple
2. Sylow r-subgroup is normal in G.
3. G has a normal subgroup of order qr.
4. If $q \nmid r-1$ then Sylow q-subgroup is normal in G

Propositions 10.21: Let G be a finite abelian group and m be a positive integer such that $m \mid o(G)$ Then G has a subgroup of order m.

Propositions 10.22: Every finite Abelian group can be expressed as the direct product of its Sylow's p-subgroups.

Group of order $2.p$:

Let G be a group of order $2.p$, where p is odd prime number then

Put Your Own Notes

1. There are two group upto isomorphism one is cyclic isomorphic to $\mathbb{Z}_{2p}$ another is non-abelian isomorphic to dihedral group D_p
2. Every abelian group of order $2.p$ is cyclic
3. If G is non cyclic then it has exactly $p+3$ subgroups
4. If G is non cyclic then it has exactly three normal subgroup one is $p-SSG$ another two are improper

Group of order 21:

Let G be a group of order 21

1. There are two group upto isomorphism one is cyclic isomorphic to $\mathbb{Z}_{2p}$ another is non-abelian isomorphic to dihedral group D_p
2. Every abelian group of order 21 is cyclic
3. $7-SSG$ is always normal , If G be a non- cyclic group of order 21
4. $3-SSG$ is never normal (if G is not cyclic)

Non-cyclic Group G of order 21		
Possible order	**Number of elements**	**Number of subgroup**
1	1	1
3	14	7
7	6	1
21	Zero	1

Group of order 30 :

Let G be a group of order 30 then

1. There are 4 groups of order 30 upto isomorphism
2. Any group of order 30 is isomorphic to one of the group $\mathbb{Z}_{30}, D_{15}, D_5 \times \mathbb{Z}_3, S_3 \times \mathbb{Z}_6$
3. $5-SSG \,\&\, 3-SSG$ are always unique hence normal
4. Any G not simple
5. If $|G|=30$ & G has only element of order 2 then it is $\mathbb{Z}$ isomorphic to $\mathbb{Z}_{30}$.

Group of order 45 :

1. $5-SSG$ is always unique hence normal
2. $3-SSG$ is always unique hence normal
3. Every group of order 45 is isomorphic to one of the group $\mathbb{Z}_{45}, \mathbb{Z}_5 \times \mathbb{Z}_3 \times \mathbb{Z}_3$
4. Every group of order 45 is abelian