V.P. & R.P.T.P. SCIENCE COLLEGE
V.V.NAGAR

T.Y. B.Sc. (Sem-V)
MATHEMATICS
US05CMTH04
M-304
(ABSTRACT ALGEBRA)

UNIT : 1 TO 4

Name :....Nilesh Y. Patel.....

Address : .....

.....

Contact No.: 9428151689.....

UNIVERSITY

ALGEBRA

BY. N.S. Gopalkrishnan

UNIT-1 (Pg. 1 to 50)
UNIT-2 (Pg: 51 to 85)
UNIT-3 (Pg: 86 to 127)
UNIT-4 (Pg. 128 to 160)

SARDAR PATEL UNIVERSITY , VALLABH VIDYANAGAR
SYLLABUS FOR B.Sc.(MATHEMATICS) SEMESTER - V
USO5CMTH04 (Abstract Algebra - 1)
THREE HOURS PER WEEK (3 CREDIT)
Effective from June 2012
Marks:-100(30 internal+70 external)

UNIT-1 Binary operations , Definition of Group and examples , Laws of exponents , Subgroups : Definition and examples , Centre of group .

UNIT-2 Cyclic group : Definiton and examples , Cosets of subgroup , Lagrange's theorem ,Index of subgroup , Euler's theorem ,Fermat's theorem .

UNIT-3 Isomorphism : Definition and examples, Isomorphic groups, Automorphism , Inner automorphism , Homomorphism :Definition and examples , Kernel of homomorphism , Normal subgroup , Simple group , Commutator subgroup , Quotient groups , First ,second and third isomorphism theorem .

UNIT-4 Direct products : Definition and examples , External direct products , Permutation groups , Transposition , Cycle , Signature of permutation , even and odd permutation , Cayley's theorem for group .

Recommended texts :

N.S.Gopalakrishnan, University Algebra, second Edition, Wiley Eastern Ltd., New Delhi 1994. Chapter 1(Except 1.12, 1.13 and 1.14), chapter 2.

Reference Books :

(1) I.N.Herstein, Topics in algebra.
(2) Asha Rani Singal, Algebraic structures,
(3) J.Whitesitt, Principles of modern algebra.

SARDAR PATEL UNIVERSITY
B.Sc.(MATHEMATICS) SEMESTER - V
QUESTION BANK OF US05CMTH04
(Abstract Algebra)
Effective from June 2012
Marks:-100(30 internal + 70 external)

Unit-1

(1) Define Group , Semigroup , Subgroup , Order of group .
(2) Check whether the following sets forms a group or not.Verify it. Is it commutative ? . 5
(i) $(Z, *)$, where $*$ is defined as $a * b = a + b - ab \ \ \forall\, a, b \in Z$.
(ii) $(Q - \{1\}, *)$, where $*$ is defined as $a * b = a + b - ab \ \forall\, a, b \in Q - \{1\}$.

(iii) $(G, *)$,where G is a set of all subsets of $\mathbb{R}$ and $*$ defined as $A * B = (A - B) \cup (B - A) \; \forall \; A, B \in G$.
i.e $A * B = (A \cup B) - (A \cap B)$ *for all* $A, B \in G$
i.e $A * B = A \triangle B \; \forall \; A, B \in G$
(iv) $(Z_6, +)$
(v) $(Z_7^*, \cdot)$
(vi) $(G, .)$ where $G = \{\pm 1, \pm i\}$.i.e G = fourth root of unity.
(vii)$(G, \cdot)$,where $G = \{e, a, b, c\}$ and the operation defined by
$a^2 = b^2 = c^2 = e^2 = e$, $ab = ba = c$, $ac = ca = b$, $bc = cb = a$,
$ae = ea = a$, $be = eb = b$, $ce = ec = c$.
(viii) $(M_2(\mathbb{R}), +)$
(ix) $(G, \cdot)$, where G is set of all 2×2 non singular matrices .

(3) Prove that every group has unique unit element. 2

(4) In group G ,prove that every element of G has unique inverse. 2

(5) State and prove cancelation laws for group. 4

(6) Let G be a set with binary operation which is associative.Assume that G has a right unit element, and every element of G has a right inverse.Then prove that G is a group. 5
OR : Let G be a semigroup.Assume that G has a right unit element, and every element of G has a right inverse.Then prove that G is a group.

(7) Let G be a semigroup.Assume that,for all a,b$\in G$,the equations $ax = b$ and $ya = b$ have unique solutions in G.Then prove that G is a group. 5

(8) Prove that Z_4 is a subgroup of $(Z, +)$. 2

(9) Prove that a non-empty subset H of a group G is subgroup iff $ab^{-1} \in H \;\; \forall \;\; a, b \in H$. 4

(10) If H and K are subgroups of group G then prove that $H \cap K$ is a subgroup of G. 2
OR : Prove that intersection of two subgroups of a group G is also a subgroup of G.

(11) Prove that intersection of any number of subgroups of a group G is also a subgroup of G. 4

(12) Prove or disprove:Union of two subgroups of group is also a subgroup. 2

(13) Let H be a finite subset of group G such that $ab \in H$ whenever $a, b \in H$.Then prove that H is a subgroup of G. 4

(14) For any group G,prove that the set $H = \{x / x \in G, \; xa = ax, \; \forall \; a \in G\}$ is a subgroup of G. 2
OR : Prove that Z(G),the centre of group G is a subgroup of G.

(15) Prove that group G is abelian iff $G = Z(G)$. 2

(16) Let H and K be subgroups of group G.Then prove that HK is subgroup of G iff $HK = KH$. 5
OR : Prove that the product of two subgroup of group is a subgroup iff they commute with each other.
OR : Let H and K be subgroups of group G.Then write the necessary and sufficient condition for HK is subgroup of G.Also prove it.

(17) Let H and K be finite subgroups of group G such that HK is a subgroup of G.Then prove that $O(HK) = \frac{O(H)O(K)}{O(H \cap K)}$. 5

(18) For group G prove that 2
(i) $(a^{-1})^{-1} = a$ (ii) $(ab)^{-1} = b^{-1}a^{-1}$

USO5CMTH04
Unit-2

(1) Define Cyclic group .

(2) Check whether following groups are cyclic or not .
OR : Find generators of following group,if possible 2
(i) Z (ii) $\{\pm 1, \pm i\}$(iii) Z_n (iv) $\{...\frac{1}{8}, \frac{1}{4}, \frac{1}{2}, 1, 2, 4, 8, ...\}$

(3) Give an example of finite cyclic group.Verify it. 4

(4) If G is a cyclic group then prove that G is abelian. 4
OR : Prove that every cyclic group is abelian.
OR : IF G is non-abelian then group then prove that G is not cyclic.

(5) Let G be a cyclic group and H,a subgroup of G.Then prove that H is cyclic. 6
OR Prove that every subgroup of cyclic group is also cyclic.

(6) Prove that any subgroup of an infinite cyclic group is also an infinite cyclic group. 5

(7) Prove that every subgroup of Z is of the form nZ,for some $n \in Z$. 3

(8) Let G be a finite cyclic group of order n.Then prove that G has unique subgroup of order d for every divisor d of n. 4

(9) Prove that an infinite cyclic group has exactly two generators. 3

(10) If G is cyclic group of order n and $a^m = e$ for some $m \in \mathbb{Z}$ then prove that n/m . 3

(11) Let G be a finite cyclic group of order n ,then prove that G has $\phi(n)$ generators. 5

(12) Define order of element in group G . 2
Find (i) O(i) in C^* (ii) O(2) in Z (iii) $O(\bar{3})$ *in* Z_6
(iv)O(i),O(-i),O(-1) in $\{\pm 1, \pm i\}$.

(13) Let G be a group and $a, b \in G$ such that $ab = ba$.If $O(a) = n$, $O(b) = m$ with m,n relatively prime,then prove that $O(ab) = mn$. 4

(14) Define right and left Cosets of subgroup , Index of subgroup .

(15) Let H be a subgroup of group G.Then prove that G is the union of all left cosets of H in G and any two distinct left cosets of H in G are disjoint. 4

(16) Prove that any two left(right) cosets of H in G have the same (finite or infinite) number of elements. 4

(17) Let H be a subgroup of G.Then prove that the number of left cosets of H in G is same as the number of right cosets of H in G. 4

(18) State and prove Lagrange's theorem. 4
OR : Prove that the number of distinct left cosets of H in finite group G is equal to $\frac{O(G)}{O(H)}$. 2

OR : If G is a finite group and H a subgroup of G,then prove that $O(G) = O(H)(G : H)$.

(19) Let H be any subgroup of group G.Then prove that 2
(i) $aH = H \Leftrightarrow a \in H$
(ii) $aH = bH \Leftrightarrow b^{-1}a \in H$
(iii) $Ha = Hb \Leftrightarrow ab^{-1} \in H$

(20) State and prove Euler's theorem. 2

(21) State and prove Fermat's theorem. 2

USO5CMTH04
Unit-3

(1) Define Isomorphic groups . Group homomorphism ,Group isomorphism , Group automorphism , Inner automorphism ,Kernal of homomorphism .

(2) Let $G' = \{1, \rho, \rho^2, ..., \rho^{n-1}\}$ be the multiplicative group of n-th root of unity,
where $\rho = e^{2\pi i/n}$.Then prove that $Z_n \simeq G'$. 5

(3) Let G and G' be two isomorphic groups,G is abelian then prove that G' is also abelian. 2
OR:Prove that isomorphic image of abelian group is also abelian.
OR:Prove that homeomorphic image of abelian group is also abelian.

(4) Let $\theta : G \to G'$ be an isomorphism of G onto G'.Let e and e' be the unit elements of G and G' respectively.Then prove that 2
(i) $\theta(e) = e'$
(ii) $\theta(a^{-1}) = \theta(a)^{-1}$, for all $a \in G$.marginpar4
OR:Let $\theta : G \to G'$ be an homomorphism of G onto G'.Let e and e' be the unit elements of G and G' respectively.Then prove that
(i) $\theta(e) = e'$
(ii) $\theta(a^{-1}) = \theta(a)^{-1}$, $\forall\ a \in G$.

(5) Prove that any infinite cyclic group is isomorphic to Z. 2

(6) Prove that any finite cyclic group of order n is isomorphic to Z_n. 2

(7) Let G be an infinite cyclic group.Then prove that G has only one non-trivial automorphism. 5
OR:Prove that every infinite cyclic group has only one non-trivial automorphism. 4

(8) Prove that any group of order 4 is abelian. 2

(9) Prove that $\theta : Z \to Z$ defined by $\theta(n) = -n$ is an automorphism of Z. 2

(10) For any abelian group G,prove that $\theta : G \to G$ defined by $\theta(a) = a^{-1}$, $\forall\ a \in G$ is an automorphism of G. 2

(11) Let G be a group and $x \in G$ be a fixed element.Then prove that the mapping $i_x : G \to G$ defined by $i_x(a) = xax^{-1}$ is an automorphism of G. 2

(12) Let $G = (a)$ be a finite cyclic group of order n.Then prove that the mapping
$\theta : G \to G$ defined by $\theta(a) = a^m$ is an automorphism of G iff m is relatively prime to n. 6

(13) Prove that the following mapping is a group homomorphism. Is it one one?Is it onto? 5
(i) $\theta : (R, +) \to (R^+, \cdot)$ defined by $\theta(a) = 2^a$
(ii) $\theta : Z \to Z_n$ defined by $\theta(a) = \bar{a}$

(14) Prove that homeomorphic image of cyclic group is also cyclic. 2

(15) Prove that a homomorphism $\theta : G \to G'$ of G to G' is an one-one iff $Ker\theta = \{e\}$. 3
OR : Prove that a homomorphism $\theta : G \to G'$ of G onto G' is an isomorphism iff $Ker\theta = \{e\}$. 3

(16) Define Normal subgroup ,Simple group , Quotient group .

(17) Let $\theta : G \to G'$ be a homomorphism.Then prove that
(i) $Ker\theta$ is a subgroup of G. 2
(ii) $Ker\theta$ is a normal subgroup of G. 2
(iii) θ is one one iff $Ker\theta = \{e\}$. 3

(18) Prove that every subgroup of abelian group G is normal in G. 2

(19) Prove that a cyclic group of prime order is a simple group. 3

(20) Prove that a subgroup H is normal in group G iff $xH = Hx \; \forall \; x \in G$. 4

(21) State and prove First isomorphism theorem. 5

(22) Let $G = Z$, $G' = \{z/z \in C \; , \; |z| = 1\}$,then prove that $G/Z \simeq G'$. 4

(23) Let $\theta : G \to G'$ be a homomorphism of groups.
(i) If H is a subgroup of G then prove that $H' = \theta(H)$ is a subgroup of G'.If H is normal in G and θ is onto then prove that H' is normal in G' . 3
(ii) If H' is a subgroup of G' then prove that $H = \theta^{-1}(H')$ is a subgroup of G.If H' is normal in G' then prove that H is normal in G. 3
(iii) If further θ is onto then prove that $G/H \simeq G'/H'$. 5

(24) State and prove Second isomorphism theorem. 3

(25) State and prove Third isomorphism theorem. 6

USO5CMTH04
Unit-4

(1) Define Direct product of normal subgroups , Direct sum of subgroups , External direct product of groups , External direct sum of groups.

(2) Let $G = (a)$ be a cyclic group of order 6 $H = \{e, a^2, a^4\}$, $K = \{e, a^3\}$.Show that $G = H \times K$. 2

(3) Let$G = \{e, a, b, c\}$ be the Klein 4-group,$H = \{e, a\}$, $K = \{e, b\}$.Show that
$G = H \times K$. 2

(4) Prove that external direct product of two groups forms a group. 4

(5) Prove that G is direct product of subgroups H and K iff (i) every $x \in G$ can be uniquely expressed as $x = hk$, $h \in H$, $k \in K$ (ii) $hk = kh$, $h \in H$, $k \in K$. 7

(6) Let $G = \mathbb{R} \oplus \mathbb{R}$ with operation defined by $(a, b) + (c, d) = (a+c, b+d)$.Show that $G = \mathbb{R} \oplus \mathbb{R}$ is the additive group. 4

(7) Show that $G = Z_2 \times Z_2$ is the Klein 4-group. 3
OR: Prove that the external direct product of two cyclic groups each of order 2 is the Klein 4-group. 4

(8) If G is a direct product (internal) of subgroups H and K ,then prove that G is isomorphic to the external direct product of H and K. 4
Conversely, if $G = H \times K$ is the external direct product of H and K then prove that H and K are isomorphic to subgroups H' and K'of G respectively and G is direct product (internal) of the subgroups H' and K'. 6

(9) Let $G = H \times K$ be a direct product of H and K ,then prove that the mapping $p_H : G \to H$ and $p_K : G \to K$defined by $p_H(h,k) = h$ and $p_K(h,k) = k$ are group homomorphism whose kernels are respectively
$K' = \{(e_H, k)/k \in K\}$ and $H' = \{(h, e_K)/h \in H\}$.
In particular $G/H' \simeq K$ and $G/K' \simeq H$. 5

(10) Define permutation on n-symbol ,Transposition , Cycle , Signature of permutation . 1

(11) Prove that product of two permutation need not be commutative. 2

(12) Prove that the set S_n of all permutation on n symbols forms a non-commutative group. 4

(13) Prove that S_n is a finite group of order n! . 2

(14) Prove that every $\sigma \in S_n$ can be expressed as a product of disjoint cycles. 2
OR: Prove that every permutation can be written as a product of disjoint cycles.

(15) Prove that every $\sigma \in S_n$ can be expressed as a product of transpositions. 2
OR: Prove that every permutation can be written as a product of transpositions.

(16) Prove that the mapping $\epsilon : S_n \to \{-1, 1\}$ given by $\sigma \to \epsilon\sigma$ is a homomorphism of S_n onto the multiplicative group $-1, 1$. 3

(17) $\sigma \in S_n$ be expressed as a product of transpositions.Then prove that the number of transpositions in the decomposition of σ is either always odd or always even. 2

(18) Prove that the set A_n of all even permutations forms a subgroup of S_n and is a normal subgroup of S_n. 2

(19) Prove that $O(A_n) = \frac{n!}{2}$ and S_n/A_n is a cyclic group of order 2. 2

(20) Which of the following permutations are odd. 2
(i) (1 2 3)(4 5 6) (ii) (1 2)(25 36)(13 24)

(21) Express the inverse of cycle (1 2 4 5 3) as a product of transpositions. 2

(22) Express the following permutation as a product of disjoint cycles 2
(i) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 4 & 5 & 7 & 6 & 8 & 1 \end{pmatrix}$ (ii) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 6 & 5 & 1 \end{pmatrix}$.

(23) State and prove Cayley's theorem. 5

SARDAR PATEL UNIVERSITY
B.Sc.(MATHEMATICS) SEMESTER - V
Multiple Choice Question Of US05CMTH04
(Abstract Algebra - 1)
Effective from June 2012

Unit-1

Que. Fill in the following blanks.

(1) Additive inverse of 2 in Z_6 is .....

(a) 1 (b) 3 (c) 2 (d) **4**

(2) Multiplicative inverse of 5 in $Z_7{}^*$ is .....

(a) **3** (b) 6 (c) 2 (d) 1

(3) Multiplicative inverse of 6 in $Z_7{}^*$ is .....

(a) 3 (b) **6** (c) 2 (d) 1

(4) Multiplicative inverse of 2 in $Z_7{}^*$ is .....

(a) 3 (b) 2 (c) **4** (d) 1

(5) In Klein 4-group $G = \{e, a, b, c\}$, ab = ...

(a) e (b) b (c) **c** (d) a

(6) In Klein 4-group $G = \{e, a, b, c\}$, b^2 = ...

(a) **e** (b) b (c) c (d) a

(7) In Klein 4-group $G = \{e, a, b, c\}$, abc = ...

(a) c (b) **e** (c) b (d) a

(8) In group G , $(ab)^{-1}$ = ...

(a) ab **(b)** $b^{-1}a^{-1}$ (c) $a^{-1}b^{-1}$ (d) $a^{-1} + b^{-1}$

(9) In group G , $(aba^{-1})^{-1}$ = ...

(a) aba^{-1} (b) $a^{-1}b^{-1}a$ **(c)** $ab^{-1}a^{-1}$ (d) $a^{-1}ba$

(10) Every group has atleast ..... subgroups.

(a) 3 (b) 4 (c) **2** (d) 1

(11) $Z_n{}^*$ forms a group if n is .....

(a) 6 (b) **prime** (c) 4 (d) 1

(12) Z_n^* forms a group if n is .....

(a) 6 (b) **7** (c) 4 (d) 1

(13) Centre of $\mathbb{Z}$ is .....

(a) $\mathbb{Z}$ (b) 2 (c) N (d) 1

(14) ..... is called trivial subgroup of group G .
(a) G **(b)** $\{e\}$ (c) $\{e, G\}$ (d) $\{0\}$

(15) ..... is subgroup of $(\mathbb{Q}, +)$.
(a) $\mathbb{C}$ (b) $\mathbb{R}$ **(c)** $\mathbb{Z}$ (d) $\mathbb{N}$

(16) ..... is subgroup of group $\{z \in \mathbb{C} \ / \ |z| = 1\}$.
(a) $\{\pm 1, \pm 2i\}$ (b) $\{\pm 2, \pm i\}$ (c) $\{-1, -i\}$ **(d)** $\{\pm 1, \pm i\}$

(17) A nonempty subset H of group $(G, +)$ is a subgroup of G if .....
(a) $a - b \in H$ (b) $a + b \in H$ (c) $ab^{-1} \in H$ (d) $a - b \in G$

UNIT-2

(18) Cyclic group of order 5 has only ..... generator .
(a) 6 **(b)** 4 (c) 5 (d) 1
(19) Cyclic group of order 6 has only ..... generator .
(a) 6 (b) 5 **(c)** 2 (d) 1
(20) ..... is generator of group $\mathbb{Z}$.

(a) -2 (b) 3 (c) **-1** (d) 2

(21) ..... is generator of group $\{\pm 1 \ , \ \pm i\}$.

(a) 2 (b) -1 (c) 1 (d) **-i**

(22) ..... is generator of group $\{...\frac{1}{8}, \frac{1}{4}, \frac{1}{2}, 1, 2, 4, 8, ...\}$.

(a) $\frac{1}{2}$ (b) 1 (c) 2 (d) $\frac{1}{4}$

(23) ..... is generator of group $\{...\frac{1}{8}, \frac{1}{4}, \frac{1}{2}, 1, 2, 4, 8, ...\}$.

(a) $\frac{1}{6}$ (b) 1 (c) **2** (d) $\frac{1}{4}$

(24) ..... is generator of group Z_n .

(a) $\bar{0}$ (b) $\bar{3}$ **(c)** $\bar{1}$ (d) $\bar{2}$

(25) ..... is generator of group Z_5^*.

(a) $\bar{3}$ (b) $\bar{1}$ (c) $\bar{4}$ (d) $\bar{5}$

(26) ..... is generator of group Z_5^*.

(a) $\bar{0}$ (b) $\bar{1}$ (c) $\bar{4}$ **(d)** $\bar{2}$

(27) O(i) in C^* is .....

(a) 1 (b) **2** (c) 3 (d) 4

(28) O(2) in Z is .....

(a) 0 (b) 3 (c) **infinite** (d) 2

(29) $O(\bar{3})$ in Z_6 is .....

(a) 1 (b) 3 (c) 4 (d) **2**

(30) $O(\bar{5})$ in Z_6 is .....
(a) **6** (b) 3 (c) 4 (d) 2

(31) O(i)in $\{\pm 1, \pm i\}$ is .....
(a) **4** (b) 1 (c) i (d) 3

(32) O(-i) in $\{\pm 1, \pm i\}$ is .....
(a) 3 (b) **4** (c) 1 (d) 2

(33) Every infinity cyclic group has exactly ..... generators .
(a) 3 (b) 1 (c) **2** (d) 4

UNIT-3

(34) Every group of order .....is abelian group .

(a) 2 (b) 5 (c) **4** (d) 6

(35) Every noncyclic group of order 4 is isomorphic to .....

(a) **Klein 4-group** (b) Z (c) N (d) Z_4

(36) Every cyclic group of order 4 is isomorphic to .....

(a) Klein 4-group (b) Z (c) N **(d)** Z_4

(37) Every infinite cyclic group has exactly ..... nontrivial automorphism.
(a) 2 (b) 3 (c) 4 (d) **1**

(38) Homomorphic image of abelian group is .....

(a) simple (b) cyclic (c) **abelian** (d) 2

(39) Every group has atleast ..... normal subgroups.
(a) 3 (b) **2** (c) 4 (d) 1

(40) If H is any normal subgroup of G then .....

(a) Hx=Hy (b) **Hx = xH** (c) Hx = H (d) xH = yH

(41) A homomorphism f is ..... iff $Kerf = \{e\}$.

(a) **one-one** (b) onto (c) isomorphism (d) automorphism

(42) Every subgroup of ..... group is normal subgroup .

(a) cyclic (b) nonabelian (c)**abelian** (d) noncyclic

(43) Every cyclic group of ..... order is simple group .

(a) 4 (b) **prime** (c) 6 (d) 1

(44) Every cyclic group of ..... order is simple group .

(a) 4 (b) **7** (c) 6 (d) 1

UNIT-4

(45) External direct sum of Z_2 is .....

(a) **Klein 4- group** (b) Q (c) Z (d) Z_2

(46) S_n is ..... group.

(a) Klein 4- group (b) cyclic (c) commutative (d) **noncommutative**

(47) Order of S_4 is .....

(a) 3 (b) 12 (c)**24** (d) 4

(48) Signature of every transposition is .....

(a) 1 (b) **-1** (c) 2 (d) -2

(49) Order of A_n is .....

(a) n (b) 1 (c) $n!$ **(d)** $n!/2$

(50) Order of S_n/A_n is .....

(a) n (b) **2** (c) $n!$ (d) 0

(51) S_n/A_n is .....group.

(a) commutative (b) noncommutative (c) noncyclic (d) **cyclic**

(52) A permutation σ is said to be even permutation if signature of σ is .....

(a) 2 (b) -1 (c)**1** (d) -2

(53) A permutation σ is said to be odd permutation if signature of σ is .....

(a) 2 (b) **-1** (c) 1 (d) -2

Unit-1 : Group-1

* Group :-
A non empty set G with binary operation * is said to be a group if following conditions are satisfied :-

(1) Associative property :-
$(a*b)*c = a*(b*c)$, $\forall\ a, b, c \in G$.

(2) Identity property :-
For any $a \in G$, $\exists\ e \in G \ni a*e = a = e*a$.
where 'e' is called identity element of G.

(3) Inverse property :-
For any $a \in G$, $\exists\ b \in G \ni a*b = e = b*a$
where 'b' is called inverse of 'a' i.e. $a^{-1} = b$.

* Commutative group :-
Group G with binary operation * i.e. (G,*) is said to be a commutative group if
$a*b = b*a$.

* Binary operation :-
Let G be any non empty set. A mapping $f : G \times G \to G$ is called a binary operation or binary mapping on G.
We use the symbol $a*b$ i.e. operation * is said to be a binary operation if
$a*b \in G$, $\forall\ a, b \in G$.

* Semi group :-
A non empty set G with binary operation *

Date: / /

is said to be a semi group if $(a*b)*c = a*(b*c)$

* Check whether the following sets form a group or not, if not check it is semi group or not, if not check it is semi group with identity or not. Is it commutative?

(1) $(N, +)$:-

Identity property is not satisfied because

$a+0 = a = 0+a$, $\forall a \in N$ but $0 \notin N$

$\therefore$ $(N, +)$ is not a group.

- Also it is not semi group with identity.
- associative property :-

Clearly $(a+b)+c = a+(b+c)$, $\forall a, b, c \in N$.

$\therefore$ $(N, +)$ is a semi group.

- Also it is commutative because $a+b = b+a$, $\forall a, b \in N$.

(2) $(N, -)$:-

Clearly $(-)$ is not a binary operation on N because $1-2 = -1 \notin N$. Thus closure property is not satisfied.

$\therefore$ $(N, -)$ does not form a group.

It is not a semi group with identity.

It is not a semi group.

also it is not commutative.

(3) $(N, \cdot)$:-

It does not satisfy inverse property because.

$2 \cdot \frac{1}{2} = 1 = \frac{1}{2} \cdot 2$ but $\frac{1}{2} \notin N$.

∴ $(N, \cdot)$ does not form a group.

Now we check for semi group with identity.

(1) Closure prop.:-

$a \cdot b \in N, \forall\ a, b \in N$.

(2) Associative prop.:-

$(a \cdot b) \cdot c = a \cdot (b \cdot c)$

(3) Identity prop.:-

For any $a \in N$, $\exists\ 1 \in N$ $\ni$ $a \cdot 1 = a = 1 \cdot a$.

where 1 is identity element.

∴ $(N, \cdot)$ is a semi group with identity.

Clearly it is commutative because $a \cdot b = b \cdot a, \forall a, b \in$

*	sets	group	s.I.	semi	comm.
(1)	$(N, \div)$	×	×	×	×
(2)	$(Z, +)$	✓	-	-	✓
(3)	$(Z, -)$	×	×	×	×
(4)	$(Z, \cdot)$	×	✓	-	✓
(5)	$(Q, +)$	✓	-	-	✓
(6)	$(Q, -)$	×	×	×	×
(7)	$(Q, \cdot)$	×	✓	-	✓
(8)	$(Q - \{0\}, \cdot)$	✓	-	-	✓
(9)	$(R^+, +)$	×	×	✓	✓

Date : / /

* Check whether the following sets forms a group or not. Is it commutative?

(1) $(Z, *)$, where $*$ is defined as

$$a*b = a+b-ab, \forall\ a,b \in Z.$$

Sol:- Clearly $a*b = a+b-ab \in Z$, $\forall\ a,b \in Z$.

$\therefore$ '$*$' is binary operation.

(1) Associative prop. $((a*b)*c = a*(b*c))$:-

$$L.H.S. = (a*b)*c$$
$$= (a+b-ab)*c$$
$$= a+b-ab+c-(a+b-ab)c$$
$$= a+b+c-ab-bc-ca+abc.$$

$$R.H.S. = a*(b*c)$$
$$= a*(b+c-bc)$$
$$= a+b+c-bc-a(b+c-bc)$$
$$= a+b+c-ab-bc-ca+abc.$$

Thus $L.H.S. = R.H.S.$

(2) Identity prop.:-

For any $a \in Z$, $a*e = a$

$$\Rightarrow a+e-ae = a$$
$$\Rightarrow e(1-a) = a-a$$
$$\Rightarrow e(1-a) = 0$$
$$\Rightarrow e = 0 \in Z.$$

Thus $a*0 = a = 0*a$, $\forall\ a \in Z$.

Thus 0 is identity element of $(Z, *)$.

(3) Inverse prop.:-

For any $a \in Z$, $a*b = 0$

$$\Rightarrow a+b-ab = 0$$

$\Rightarrow a + b(1-a) = 0$

$\Rightarrow b(1-a) = -a$

$\Rightarrow b = \frac{a}{a-1} \notin Z, \quad \forall a = 3,4,5,6,\cdots$

$\therefore$ Inverse prop. is ~~##~~ not satisfied.

Thus $(Z, *)$ does not form a group.

Clearly it is commutative because

$a * b = a + b - ab = b + a - ba = b * a, \quad \forall a, b \in Z.$

(2) $(Q, *)$, where $*$ is defined as above.

Hint:- → Inverse prop:-

$$a * b = 0 \Rightarrow b = \frac{a}{a-1}$$

For $a = 1$, b does not exist.

$\therefore$ inverse of 1 does not exist.

$\therefore$ It does not form a group.

(3) $(Q - \{1\}, *)$.

Hint: clearly $a * b = 0 \Rightarrow b = \frac{a}{a-1} \in Q - \{1\}, \forall a \in Q - \{1\}$

$\therefore$ It forms a group.

or

Inverse

~~Identity~~ property :-

For any $a \in Q - \{1\}$, $\exists\ b \in Q - \{1\}$ $\ni$

$$a * b = 0 = b * a$$

Now $a * b = 0$

$\Rightarrow a + b - ab = 0$

$\Rightarrow b(1-a) = -a$

$\Rightarrow b = \frac{a}{a-1} \in Q - \{1\} \quad (\because a \neq 1)$

Thus $a^{-1} = \frac{a}{a-1} \in Q - \{1\}$

Hence $(Q - \{1\}, *)$ forms a group.

also $a*b = a+b-ab = b+a-ba = b*a$.

$\therefore$ It is commutative group.

(4) $(\mathbb{Q}, *)$, where '$*$' is defined by $a*b = a+b+ab$.

Sol:- Clearly $a*b = a+b+ab \in \mathbb{Q}$, $\forall\ a, b \in \mathbb{Q}$

$\therefore$ '$*$' is binary operation in $\mathbb{Q}$

(1) Associative property:-

$$(a*b)*c = (a+b+ab)*c$$
$$= a+b+ab+c+(a+b+ab)c$$
$$= a+b+c+ab+bc+ac+abc.$$

$$a*(b*c) = a*(b+c+bc)$$
$$= a+b+c+bc+a(b+c+bc)$$
$$= a+b+c+ab+bc+ac+abc$$

Thus, $(a*b)*c = a*(b*c)$.

(2) Identity property :-

For any $a \in \mathbb{Q}$ $\exists\ e \in \mathbb{Q} \ni a*e = a = e*a$.

$$a*e = a$$
$$\Rightarrow a+e+ae = a.$$
$$\Rightarrow a+e(1+a) = a$$
$$\Rightarrow e(1+a) = 0$$
$$\Rightarrow e = 0 \in \mathbb{Q}$$

Thus $e=0$ is identity element of $(\mathbb{Q}, *)$

(3) Inverse property :-

For any $a \in \mathbb{Q}$ $\exists\ b \in \mathbb{Q} \ni a*b = a = b*a$

$$a*b = 0 = b*a.$$

Now $a*b = 0$

$$\Rightarrow a+b+ab = 0$$
$$\Rightarrow a+b(1+a) = 0$$

Date: / /

$\Rightarrow b = \frac{-a}{1+a} \notin \mathbb{Q}$ for $a = -1$.

Thus inverse property is not satisfied for $a = -1$

$\therefore$ It does not form a group.

also $a * b = a + b + ab = b + a + ba = b * a \in \mathbb{Q}$.

Thus it is commutative semigroup with identity.

(5) $\{\mathbb{Q} - \{-1\}, *\}$.

Sol^n:- Inverse property :- from above ex.

$$b = \frac{-a}{1+a} \in \mathbb{Q} \quad (\because a \neq -1)$$

(6) Let G be the set of all subsets of R & * defined by $A * B = A \cup B$, $\forall A, B \in G$

Sol^n:-

Clearly $A * B = A \cup B \in G$, $\forall A, B \in G$.

$\therefore$ '*' is binary operation in G.

(1) Associative property :-

For $A, B, C \in G$

$$\text{L.H.S. } (A * B) * C = (A \cup B) \cup C$$
$$= A \cup (B \cup C)$$
$$= A * (B * C) = \text{R.H.S.}$$

(2) Identity property :-

For any $A \in G$ $\exists$ $E \in G$ $\ni$ $A * E = A = E * A$.

$A * E = A$, $\forall A \in G$.

$\Rightarrow A \cup E = A$, $\forall A \in G$.

$\Rightarrow E = \phi \in G$.

Thus ϕ is identity for $(G, *)$.

Date : / /

(3) Inverse property :-

For any $A \in G$ $\exists$ $B \in G$ $\ni$ $A * B = \phi = B * A$.

Here for any non empty set $A \in G$ we can not find $B \in G \ni A \cup B = \phi$ i.e $A * B = \phi$.

i.e. $A * B \neq \phi$, $\forall B \in G, A \in G$. (non empty)

Thus inverse property is not satisfied.

$\therefore$ It does not form a group.

also $A * B = A \cup B = B \cup A = B * A$, $\forall A, B \in G$.

$\therefore$ It is commutative semi group with identity.

(7) $A * B = A \cap B$, $\forall A, B \in G$.

Sol :- Hint :-

Identity prop. :-

For any $A \in G$ $\exists$ $E \in G$ $\ni$ $A * E = A$.

$A * E = A$

$\Rightarrow A \cap E = A$

$\Rightarrow E = R \in G$.

Thus R is identity for $(G, *)$.

Inverse :-

For any $A \in G$ $\exists$ $B \in G$ $\ni$ $A * B = R = B * A$.

Hence for any proper set $A \in G$, we cannot find $B \in G \ni A \cap B = R$ i.e $A * B = R$.

$\therefore$ $A * B \neq R.$, $\forall B \in G, A \in G$.

(proper subset of R)

(8) $\therefore$ It does not form a group also it is commutative.

Ex Let X be any Non empty set - G be set of all subsets of X. * is defined by

$A * B = A \Delta B$ $\forall A, B \in G$ (Symmetric difference)

(8) Let R^* be the set of all non zero real numbers and operation '$*$' is defined as $a * b = \frac{1}{2}ab, \forall\ a, b \in R^*$.

Sol.:-

Clearly $a*b = \frac{1}{2}ab \in R^*, \forall\ a, b \in R^*$.

$\therefore$ '$*$' is binary operator.

(1) Associative property:-

$$(a*b)*c = \left(\frac{1}{2}ab\right)*c = \frac{1}{2}\left(\frac{1}{2}abc\right)$$

$$= \frac{1}{4}abc$$

$$a*(b*c) = a*\left(\frac{1}{2}bc\right)$$

$$= \frac{1}{2}\left(a \cdot \frac{1}{2}bc\right)$$

$$= \frac{1}{4}abc.$$

Thus, $(a*b)*c = a*(b*c)$.

(2) Identity:-

For any $a \in R^*$ $\exists\ e \in R^*$ $\ni$ $a*e = a$

$$\Rightarrow \frac{1}{2}ae = a$$

$$\Rightarrow e = 2$$

(3) Inverse prop.:-

For any $a \in R^*$ $\exists\ b \in R^*$ $\ni$ $a*b = 2$.

$$a*b = 2$$

$$\Rightarrow \frac{1}{2}ab = 2$$

$$\Rightarrow ab = 4$$

$$\Rightarrow b = \frac{4}{a} \in R^* \quad (\because a \neq 0)$$

$$\Rightarrow a^{-1} = \frac{4}{a}$$

Thus it forms a group.

also it is commutative because
$a*b = \frac{1}{2}ab = \frac{1}{2}ba = b*a, \forall a,b \in R^*$.

(9) $G = \{\pm 1, \pm i\}$ with '+' or.
(Let G be the 4th root of unity)

Sol: Here for $1, -1 \in G$ but $1 + (-1) = 0 \notin G$.
Thus '+' is not binary operation in G.
∴ It does not form a group.

(10) $G = \{\pm 1, \pm i\}$ with '$\cdot$'.

$\cdot$	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

From above table we can easily say that '$\cdot$' is binary operation in G, also from the table we can easily say that $a \cdot (b \cdot c) = (a \cdot b) \cdot c$, $\forall a, b, c \in G$. From the table 1 is the identity element for G.

Also from the above table, we say that $1^{-1} = 1$, $(-1)^{-1} = -1$, $(i)^{-1} = -i$, $(-i)^{-1} = i$.

Thus it forms a group.

Also it is commutative.

(11) Let G be the set of all +ve integers i.e $G = N$. and '$*$' is defined by $a*b = \max\{a, b\}$, $\forall a, b \in$

Date: 11

soln:- Here $a*b = \max\{a,b\} = a \text{ or } b \in G$

$\therefore$ '*' is binary operation in G.

(1) Associative prop:-

$$(a*b)*c = \max\{a,b\} * c$$
$$= \max\{\max\{a,b\}, c\}$$
$$= \max\{a,b,c\}.$$
$$a*(b*c) = a * \max\{b,c\}$$
$$= \max\{a, \max\{b,c\}\}$$
$$= \max\{a,b,c\}$$

Thus $(a*b)*c = a*(b*c)$.

(2) Identity prop:-

For any $a \in G$ $\exists$ $e \in G$ $\ni$ $a*e = a$

$\Rightarrow \max\{a,e\} = a$

$\Rightarrow e = 1 \in G$.

$\Rightarrow$ For $a = 2$ $\nexists$ $b \in G \Rightarrow \max\{2,b\} = 1$ i.e $2*b \neq 1$ $\therefore$ 2 is not possible

(3) Inverse prop:-

For any $a \in G$ [$\exists$ $b \in G$ $\ni$] $\times$ $a*b \neq 1$, $\forall$ $a \neq 1 \in G$, $\forall$ $b \in G$

i.e $\max\{a,b\} \neq 1$, $\forall$ $a \in G$

$\therefore$ Inverse property does not satisfied

$\therefore$ It does not form a group.

Also it is commutative because

$$a*b = \max\{a,b\} = \max\{b,a\}, \forall a,b \in G.$$
$$= b*a$$

(12) $a*b = \min\{a,b\}$.

Hint:- identity property:-

For any $a \in G$, $\exists$ $e \in G$ $\ni$ $a*e = a$

$a*e = a$

i.e $\Rightarrow \min\{a,e\} = a$, $\forall e \in G$

i.e we cannot find any finite value of e

∴ Identity property is not satisfied

(3) Inverse prop. :-

Since identity element does not exist, inverse prop. is not satisfied.

Thus it cannot form group.

It is cummutative with semigroup.

(13) Let $G = \{e, a, b, c\}$ be the set with four elements, defined a binary operation '.' in G by following table:

.	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Check for $(G, \cdot)$.

Soln:- From the above table, we say that given operation is binary operation.

also from the table, we say that

$(xy)z = x(yz)$, $\forall\ x, y, z \in G$.

from the table, we say that 'e' is the identity element

from the table we say that,

$e^{-1} = e$, $a^{-1} = a$, $b^{-1} = b$, $c^{-1} = c$.

also from the table, we say that

$xy = yx$, $\forall\ x, y \in G$.

Thus, $(G, \cdot)$ is commutative group.

* Remark:- Above group is known as "Klein 4-group".

Date: / /

(14) $G = \{a, b, c, d\}$, define operation in G by following table:

$\cdot$	a	b	c	d
a	a	b	c	d
b	b	c	c	d
c	c	d	d	a
d	d	b	d	c

Soln:-

From the table we say that given operation is binary operation

from the table, we say that

$(bc)d = cd = a$

but $b(cd) = b(a) = b$

Thus $(bc)d \neq b(cd)$.

∴ It does not form a group.

from the table, we say that 'a' is the identity element for G.

from the table, $a^{-1} = a$ and b^{-1}, c^{-1}, d^{-1} not possible.

It is not commutative as $cd = a$ but $dc = d$

(15) G is the set of all 2×2 real matrices with operation '+'. $(M_2(R), +)$.

Soln:- we know that,

$$M_2(R) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} / a, b, c, d \in R \right\}$$

for

$$A = \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}, B = \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix},$$

$$C = \begin{bmatrix} a_3 & b_3 \\ c_3 & d_3 \end{bmatrix} \in M_2(R).$$

Date : / /

Clearly,

$$A+B = \begin{bmatrix} a_1+a_2 & b_1+b_2 \\ c_1+c_2 & d_1+d_2 \end{bmatrix} \in M_2(R)$$

$\therefore$ '+' is binary operation for $M_2(R)$

* Associative property :-

$$(A+B)+C = \begin{bmatrix} a_1+a_2 & b_1+b_2 \\ c_1+c_2 & d_1+d_2 \end{bmatrix} + \begin{bmatrix} a_3 & b_3 \\ c_3 & d_3 \end{bmatrix}$$

$$= \begin{bmatrix} (a_1+a_2)+a_3 & (b_1+b_2)+b_3 \\ (c_1+c_2)+c_3 & (d_1+d_2)+d_3 \end{bmatrix}$$

$$= \begin{bmatrix} a_1+(a_2+a_3) & b_1+(b_2+b_3) \\ c_1+(c_2+c_3) & d_1+(d_2+d_3) \end{bmatrix}$$

$$= A+(B+C).$$

* Identity property :-

$$O = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \in M_2(R)$$

also $A+O = O+A = A, \forall\ A \in M_2(R)$

$\therefore$ O matrix is additive identity

* Inverse property :-

clearly $A+(-A) = (-A)+A = O$

Date :

* commutative property :-

$$A+B=\begin{bmatrix} a_1+a_2 & b_1+b_2 \\ c_1+c_2 & d_1+d_2 \end{bmatrix}$$

$$=\begin{bmatrix} a_2+a_1 & b_2+b_1 \\ c_2+c_1 & d_2+d_1 \end{bmatrix}$$

$$= B+A \quad , \forall A, B \in M_2(R).$$

Thus $(M_2(R), +)$ is a commutative group.

(16) $(M_2(R), \cdot)$.

Hint :- Inverse prop. is not satisfied because

$$A=\begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}$$

then $A^{-1}=\frac{1}{|A|}|adjA|$

but $|A|=0$

$\therefore A^{-1}$ not possible.

(17) Let G be the set of all 2x2 non singular matrices then prove that $(G, \cdot)$ is a group. Is it commutative ?.

Sol :-

$$\text{Here } G=\left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} / \begin{matrix} a,b,c,d \in R \\ ad-bc \neq 0 \end{matrix} \right\}.$$

Let $A=\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}$, $B=\begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix}$,

$$C=\begin{bmatrix} a_3 & b_3 \\ c_3 & d_3 \end{bmatrix} \in G.$$

then $|A| \neq 0$, $|B| \neq 0$, $|C| \neq 0$.

Clearly,

$$AB = \begin{bmatrix} a_1a_2 + b_1c_2 & a_1b_2 + b_1d_2 \\ ca_2 + d_1c_2 & cb_2 + d_1d_2 \end{bmatrix} \in G.$$

$(\because |AB| = |A||B| \neq 0$

Thus '.' is a binary operation in G.

* Associative property :-

We know that matrix multiplication is always associative

i.e. $(AB)C = A(BC)$, $\forall A, B, C \in G$.

* Identity property :-

Let $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in G$

also $AI = A = IA$.

Thus,

$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in G$ is identity matrix for G.

* Inverse property :-

for any

$A = \begin{bmatrix} a_1 & b_1 \\ c & d_1 \end{bmatrix} \in G$ then $|A| \neq 0$.

$$A^{-1} = \frac{1}{|A|}[\text{adj } A]$$

$$= \frac{1}{a_1 d_1 - b_1 c_1} \begin{bmatrix} d_1 & -b_1 \\ -c_1 & a_1 \end{bmatrix}$$

also, $|A^{-1}| = \frac{1}{a_1 d_1 - b_1 c_1} (a_1 d_1 - b_1 c_1) = 1 \neq 0.$

$\therefore A^{-1} \in G.$

and

$$AA^{-1} = I = A^{-1}A$$

$\therefore (G, \cdot)$ is a group.

also it is not commutative because for $A = \begin{bmatrix} 1 & 2 \\ -1 & 3 \end{bmatrix}$, $B = \begin{bmatrix} 3 & 0 \\ 0 & 2 \end{bmatrix} \in G$

$$AB = \begin{bmatrix} 3 & 4 \\ -3 & 6 \end{bmatrix} \text{ and } BA = \begin{bmatrix} 3 & 6 \\ -2 & 6 \end{bmatrix}$$

Thus $AB \neq BA$.

(18) Let G be the set of all 2×2 real matrices with determinant 1 then prove that $(G, \cdot)$ forms a group. Is it commutative?

Here $G = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} / a, b, c, d \in R \text{ and } ad - bc = 1 \right\}$.

Let $A = \begin{bmatrix} 1 & 2 \\ 1 & 3 \end{bmatrix}$, $B = \begin{bmatrix} 2 & -5 \\ -1 & 3 \end{bmatrix}$.

$$C = \begin{bmatrix} 4 & 11 \\ 1 & 3 \end{bmatrix} \in G.$$

$|A| = 1$, $|B| = 1$, $|C| = 1$.

Date: / /

Clearly, $AB = \begin{bmatrix} 2-2 & -5+6 \\ 2-3 & -5+9 \end{bmatrix}$

$= \begin{bmatrix} 0 & 1 \\ -1 & 4 \end{bmatrix} \in G$

Thus, '.' is binary operation in G.

(*) Associative property :-
Matrix multiplication is always associative.
i.e. $(AB)C = A(BC)$, $\forall A, B, C \in G$.

(*) Identity property :-

Let $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in G$.

also $AI = A = IA$

Thus, $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in G$ is identity matrix for G.

(*) Inverse property :-

for any $A = \begin{bmatrix} 1 & 2 \\ 1 & 3 \end{bmatrix} \in G$

then $|A| = 1$

$A^{-1} = \frac{1}{|A|} |adj A|$

$= \begin{bmatrix} 3 & -2 \\ -1 & 1 \end{bmatrix} \Rightarrow |A^{-1}| = 3-2 = 1 \in G$.

& $AA^{-1} = I = A^{-1}A$

For every $A \in G$,

then $|A| = 1$

$A^{-1} = \frac{1}{|A|}[adj A]$

$|A^{-1}| = |adj A| = 1$

$\Rightarrow A^{-1} \in G$

$\therefore (G, \cdot)$ is a group.

$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$

then $A^{-1} = \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$

also it is not commutative

because for $A=\begin{bmatrix}1 & 2\\ 1 & 3\end{bmatrix}$, $B=\begin{bmatrix}2 & -5\\ -1 & 3\end{bmatrix}$

then $AB=\begin{bmatrix}0 & 1\\ -1 & 4\end{bmatrix}$

and $BA=\begin{bmatrix}-3 & -11\\ 2 & 7\end{bmatrix}$

Thus $AB \neq BA$.

(19) Let G be the set of all non negative integers $(N \cup \{0\})$ and operation '*' is defined by $a*b = a^2+b^2, \forall a,b \in R$ check for $(G,*)$.

Sol:- Clearly $a*b = a^2+b^2 \in R, \forall a,b \in R$

* associative prop.:-

$(a*b)*c = (a^2+b^2)*c$

$= (a^2+b^2)^2+c^2$

$a*(b*c) = a*(b^2+c^2)$

$= a^2+(b^2+c^2)^2$

Thus, $(a*b)*c \neq a*(b*c)$.

∴ associative prop. is not satisfied

* Identity prop.:-

for any $a \in R$ there does not exist $e \ni a*e = a^2+e^2 = a$.

∴ Identity prop. is not satisfied

Hence inverse " " " "

∴ It is not group.

also it is commutative as,

$m*n = m^2+n^2 = n^2+m^2 = n*m, \forall m,n \in G$.

Date : / /

6

20) Let Z_m be the set of residue classes modulo m (integer modulo m) define '+' in Z_m by $\bar{a}+\bar{b}=\bar{c}$.

where $\bar{a}+\bar{b}$ = remainder obtained when $a+b$ divided by m.

where $a+b \equiv c \pmod m$

Sol^n :-

Here Z_m be the set of residue classes modulo m

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	...	$\overline{m-2}$	$\overline{m-1}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	...	$\overline{m-2}$	$\overline{m-1}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	...	$\overline{m-1}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	...	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	...	$\bar{1}$	$\bar{2}$
⋮	⋮						
$\overline{m-2}$	$\overline{m-2}$	$\overline{m-1}$	$\bar{0}$	$\bar{1}$	...	$\overline{m-4}$	$\overline{m-3}$
$\overline{m-1}$	$\overline{m-1}$	0	$\bar{1}$	$\bar{2}$	...	$\overline{m-3}$	$\overline{m-2}$

from the above table, we say that '+' is binary operation in Z_m.

also from the table we say that associative prop. is satisfied

i.e $(\bar{a}+\bar{b})+\bar{c} = \bar{a}+(\bar{b}+\bar{c}),\ \forall\ \bar{a},\bar{b},\bar{c} \in Z_m$

Clearly $\bar{0} \in Z_m$ is identity element

from the table we say that,

$\bar{0}+\bar{0} = \bar{0}$

$\bar{1}+(\overline{m-1}) = \bar{0}$

$\bar{2}+(\overline{m-2}) = \bar{0}$

⋮

$(\overline{m-1})+\bar{1} = \bar{0}$

Thus additive inverse of

$\bar{0} = \bar{0}$

$\bar{1} = \overline{m-1}$

$\bar{2} = \overline{m-2}$

$\overline{m-1} = \bar{1}$.

also from the table we say that

$\bar{a}+\bar{b} = \bar{b}+\bar{a}, \forall\ \bar{a}, \bar{b} \in Z_m$.

(21) $(Z_6, +)$.

Sol :- $Z_6 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$.

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{2}$	$\bar{4}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{3}$	$\bar{0}$	$\bar{7}$
$\bar{4}$	$\bar{4}$	$\bar{5}$	$\bar{2}$	$\bar{0}$	$\bar{4}$	$\bar{2}$
$\bar{5}$	$\bar{5}$	$\bar{0}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

queiHy wrong table

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{5}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$

as above ex- it forms a group.

Date : / /

(22) $(Z_6, \cdot)$.

$\cdot$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{0}$	$\bar{2}$	$\bar{4}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{2}$	$\bar{0}$	$\bar{4}$	$\bar{2}$
$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Clearly from the table we say that, '$\cdot$' is inary operation & $(\bar{a}\bar{b})\bar{c} = \bar{a}(\bar{b}\bar{c})$, $\forall \bar{a}, \bar{b}, \bar{c} \in Z$

from the table we say that $\bar{1} \in Z_6$ is identity.

from the table, we say that $(\bar{0})^{-1}$ is not possible. $(\bar{1})^{-1} = \bar{1}$.

also $\bar{2}^{-1}$, $\bar{3}^{-1}$ & $\bar{4}^{-1}$ not possible

$(\bar{5})^{-1} = \bar{5}$.

Thus $(Z_6, \cdot)$ is not a group.

* also it is commutative.

✓ $(Z_5, \cdot)$

(23) $(Z_7^*, \cdot)$. , $Z_7^* = Z_7 - \{\bar{0}\}$.

Sol:- $Z_7^* = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}\}$.

$\cdot$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
$\bar{2}$	$\bar{2}$	$\bar{4}$	$\bar{6}$	$\bar{1}$	$\bar{3}$	$\bar{5}$
$\bar{3}$	$\bar{3}$	$\bar{6}$	$\bar{2}$	$\bar{5}$	$\bar{1}$	$\bar{4}$
$\bar{4}$	$\bar{4}$	$\bar{1}$	$\bar{5}$	$\bar{2}$	$\bar{6}$	$\bar{3}$
$\bar{5}$	$\bar{5}$	$\bar{3}$	$\bar{1}$	$\bar{6}$	$\bar{4}$	$\bar{2}$

Date: / /

Sol^n:- From the table we say that '.' is binary operation in Z_7^*.

from the table,

$(\bar{a}\cdot\bar{b})\cdot\bar{c} = \bar{a}\cdot(\bar{b}\cdot\bar{c})$

and $\bar{1}$ is identity element.

also,

$(\bar{1})^{-1} = \bar{1}$, $(\bar{2})^{-1} = \bar{4}$, $(\bar{3})^{-1} = \bar{5}$,

$(\bar{4})^{-1} = \bar{2}$, $(\bar{5})^{-1} = \bar{3}$, $(\bar{6})^{-1} = \bar{6}$.

$\therefore (Z_7^*, \cdot)$ forms a comm. group.

(2q) $(Z_8^*, \cdot)$.

Hint:- $\bar{2} \in Z_8^*$, $\bar{4} \in Z_8^*$

but $\bar{2}\cdot\bar{4} = \bar{0} \notin Z_8^*$

Thus '.' is not binary operation.

$\therefore$ It is not group.

* Remark:- If p is prime then $(Z_p^*, \cdot)$ forms a group otherwise not possible.

* Theorem-1:

Prove that, identity is unique in group G.

proof:- Let e & e' be two identity in group G then $ae = a = ea, \forall a \in G$ -(1) &

$ae' = a = e'a, \forall a \in G$ -(2)

Since $e \& e' \in G$.

put $a = e'$ in (1)

$e'e = e' = ee'$ -(3)

put $a = e$ in (2)

$ee' = e = e'e$ -(4)

Date: / /

Hence identity is unique in G.

* Theorem-2:

Prove that every element of group G has unique inverse (~~of~~ ~~of~~) in G.

proof:- For $a \in G$, let a' and a'' be two inverses of a in G.

$$aa' = e = a'a \quad -(1)$$

$$aa'' = e = a''a \quad -(2)$$

we have to prove that $a' = a''$

L.H.S. $a' = a'e = a'(aa'')$

$= (a'a)a''$

$= ea''$ (by (1))

$= a''$

$=$ RHS.

Hence result is proved.

* Theorem-3:

State and prove cancellation laws in G.

* Statement:-

Let G be any group

for any $a, b, c \in G$

(I) $ab = ac \Rightarrow b = c$ (left cancellation law)

(II) $ba = ca \Rightarrow b = c$ (right " ")

proof:- (I) For any $a, b, c \in G$ then $a^{-1} \in G$

Now $ab = ac$

$\Rightarrow a^{-1}(ab) = a^{-1}(ac)$

$\Rightarrow (a^{-1}a)b = (a^{-1}a)c$

Date: 03

$\Rightarrow eb = ec \Rightarrow b = c$, where e is identity element

Thus, left cancellation law is proved

(II) $ba = ca \Rightarrow (ba)a^{-1} = (ca)a^{-1}$

$\Rightarrow b(aa^{-1}) = c(aa^{-1})$

$\Rightarrow be = ce$, where e is identity elemen

$\Rightarrow b = c$

Thus right cancellation law is proved

* Theorem-4:

State and prove cancellation laws in group $(G, *)$.

Statement:- Let $(G, *)$ be any group for any $a, b, c \in G$.

$a * b = a * c \Rightarrow b = c$

proof:- for $a, b, c \in G$ then $-a \in G$.

$a * b = a * c$

$\Rightarrow -a * (a * b) = -a * (a * c)$

$\Rightarrow (-a * a) * b = (-a * a) * c$

$\Rightarrow e * b = e * c$

$\Rightarrow b = c$

Thus $(G, *)$ satisfies L.C.L

Similarly " " R.C.L

* Theorem-5:

Let G be a group and $a, b \in G$ then prove that, equation $ax = b$ and $ya = b$ have unique soln in G.

Date : / /

proof:- Here $a, b \in G$.

Now, $ax = b$

$\Rightarrow a^{-1}(ax) = a^{-1}b$

$\Rightarrow (a^{-1}a)x = a^{-1}b$

$\Rightarrow ex = a^{-1}b$

$\Rightarrow x = a^{-1}b \in G \quad (\because a^{-1}, b \in G$

Thus $ax = b$ has soln. $x = a^{-1}b$ in G.

Now, we prove that above soln is unique (!)

If x_1 & x_2 are two solns of eqn. $ax = b$

then $ax_1 = b$ & $ax_2 = b$

$\Rightarrow ax_1 = ax_2$

$\Rightarrow x_1 = x_2$ (by L.C.L)

Hence, $ax = b$ has unique soln.

Now, $ya = b$

$\Rightarrow (ya)a^{-1} = ba^{-1}$

$\Rightarrow y(aa^{-1}) = ba^{-1}$

$\Rightarrow ye = ba^{-1}$

$\Rightarrow y = ba^{-1} \in G$.

If y_1 & y_2 are two solns of eqn. $ya = b$ then

$y_1a = b$ & $y_2a = b \Rightarrow y_1a = y_2a$

$\Rightarrow y_1 = y_2 \in$ (by R.C.L)

* Remark:-

(i) If $ae = a$, $\forall a \in G$.

then G has right identity (right unit) element e.

(ii) If $aa^{-1} = e$, $\forall a \in G$ then a has right inverse in G.

Similarly, we can define for left.

* Theorem-6:

Let G be a semigroup. If G has a right unit element and every element of G has right inverse then prove that G is a

Date: 1/7/17

proof:- Let $e \in G$ be the right unit element then $ae = a, \forall a \in G$

also every element of G has a right inverse

$\therefore$ for $a \in G$, $\exists\ a^{-1} \in G \ni aa^{-1} = e$

we have to prove that G satisfies right cancellation law.

i.e $ac = bc \Rightarrow a = b, \forall\ a, b, c \in G$

Here $ac = bc$

$\Rightarrow (ac)c^{-1} = (bc)c^{-1}$

$\Rightarrow a(cc^{-1}) = b(cc^{-1})$

$\Rightarrow ae = be$

$\Rightarrow a = b$.

Now we prove that G is a group

$\therefore$ It is sufficient to prove that

(i) $ea = a, \forall\ a \in G$

(ii) $a^{-1}a = e, \forall\ a \in G$

We can write

$(ea)a^{-1} = e(aa^{-1})$

$= ee = e = aa^{-1}$.

Thus $(ea)a^{-1} = aa^{-1}$

$\Rightarrow ea = a$ (by RCL), $\forall\ a \in G$

Now we prove that

$a^{-1}a = e, \forall\ a \in G$

We know that

$ea^{-1} = a^{-1}$ ($\because$ e is left unit element)

$\Rightarrow ea^{-1} = a^{-1}e$

$\Rightarrow ea^{-1} = a^{-1}(aa^{-1})$

$\Rightarrow ea^{-1} = (a^{-1}a)a^{-1}$

$\Rightarrow ea^{-1} = (a^{-1}a)a^{-1}$

Date : / /

* Theorem-1 :-

Let G be a semigroup. If G has left unit element and every element of G has left inverse then prove that G is a group.

Proof :- Let $e \in G$ be the left unit element then

$ea = a, \forall a \in G$

also every element of G has left inverse

i.e for any $a \in G$ $\exists$ $a^{-1} \in G$ $\ni$ $a^{-1}a = e$

We have to prove that G satisfies left cancellation law.

i.e $ca = cb \Rightarrow a = b, \forall a, b, c \in G$.

Here $ca = cb$

$\Rightarrow c^{-1}(ca) = c^{-1}(cb)$

$\Rightarrow (c^{-1}c)a = (c^{-1}c)b$

$\Rightarrow ea = eb \Rightarrow a = b$.

Now we p.t. G is a group

$\therefore$ It is sufficient to p.t

(i) $ae = a, \forall a \in G$

(ii) $aa^{-1} = e, \forall a \in G$

we can write,

$a^{-1}(ae) = (a^{-1}a)e$

$= ee = e = a^{-1}a$

Thus $a^{-1}(ae) = a^{-1}a$

$\Rightarrow ae = a$ (by L.C.L), $\forall a \in G$

also we know that

$a^{-1}e = a^{-1}$ ($\because e$ is right unit elemen.)

$\Rightarrow a^{-1}e = ea^{-1}$

$\Rightarrow a^{-1}e = (aa^{-1})(a^{-1}a)a^{-1}$

Date: 15/10

* Theorem-8:

Let G be a semi group, $\forall a, b \in G$. If the eq^{ns} $ax=b$ and $ya=b$ have unique soln^{n} then prove that G is a group.

proof:- We have given that G is a semi group and we have to prove that G is a group.

$\therefore$ By above theorem it is sufficient to prove that,

(1) G has a right identity element

(2) Every element of G has right inverse.

~~Consider the eq^{n} $ax=a$; for some~~ Since $ax=b$ has soln^{n} ~~(for $b=a$)~~ $\forall a \in G$

$\therefore ax=a$ has soln; ~~$ax=a \Rightarrow x=e$~~ $x=e$.

Thus $ae=a$ for some $a \in G$

We have to prove that $be=b, \forall b \in G$.

if y_1 is soln^{n} of $ya=b$ then $y_1 a=b$.

Now,

$$be=(y_1 a)e=y_1(ae)=y_1 a=b$$

Thus $be=b, \forall b \in G$.

Thus G has right identity element e.

Now we prove result (2)

We know that

$ax=b$ has unique soln^{n} in G, $\forall a, b \in G$

$\therefore ax=e$ has unique soln^{n} in G ($\because e \in G$.

Let $x=a'$ be the soln^{n} then

$aa'=e$

$\Rightarrow a'$ is right inverse of a

$\Rightarrow$ every element of G has right inverse.

Hence, G is a group.

Date : / /

* Finite group :-

A group G is said to be finite group if it contains finite number of element. The number of elements in a finite group G is called the order of group G. It is denoted by O(G).

→ Let G be a group and $n \in Z$, $a \in G$, then "powers of a" are defined by

(i) $a^n = a \cdot a \cdot a \cdots$ (n times), if $n > 0$.

(ii) $a^0 = e$

(iii) $a^n = (a^{-1})^m$ if $n = -m$, $m > 0$.

State & prove laws of exponents in a group G.

* Theorem : 9 :-

Let G be a group then prove the following results :-

① $a^n \cdot a^m = a^{n+m}$, $\forall a \in G$, n, m are integers.

② $(a^n)^m = a^{nm}$, " " " " "

③ $(ab)^n = a^n b^n$, " " " " "

provided $ab = ba$.

Proof :- (1)

* case-(I) :- $m > 0$, $n > 0$.

$$a^n \cdot a^m = (a \cdot a \cdot a \cdots (n \text{ times})) \cdot (a \cdot a \cdot a \cdots (m \text{ times}))$$

$$= a \cdot a \cdot a \cdots a \ ((n+m) \text{ times})$$

$$= a^{n+m}$$

* case-(II) :- $m < 0$, $n < 0$, then we can write $n = -n_1$, $m = -m_1$, for some $n_1 > 0, m_1 > 0$

$$L.H.S. = a^n \cdot a^m = (a^{-1})^{n_1} (a^{-1})^{m_1}$$

$$= a^{-1} \cdot a^{-1} \cdots (n_1 \text{ times}) \cdot a^{-1} \cdot a^{-1} \cdots (m_1 \text{ times})$$

Date: 31

$= a^{-1} \cdot a^{-1} \cdot a^{-1} \cdots (n+m)$ times

$= (a^{-1})^{n+m}$

$= a^{n+m}$ = RHS.

*case (III) :-

If either $n=0$ or $m=0$.

If $n=0$ then

L.H.S. $= a^0 a^m$

$= e a^m$

$= a^m$

$= a^{0+m} = a^{n+m}$ = RHS.

If $m=0$ then

L.H.S. $= a^n a^0$

$= a^n e$

$= a^n = a^{n+0} = a^{n+m}$ = RHS

*case (IV) :-

If $n>0$ and $m<0$ then

$m = -m_1$, for some $m_1 > 0$.

Now, we prove the result by using mathematical induction method

for $n=1$

LHS $= a^1 a^m = a^1 (a^{-1})^{m_1}$

$= a(a^{-1} \cdot a^{-1} \cdots m_1$ times)

$= a^{-1} \cdot a^{-1} \cdots (m_1 - 1)$ times

$= (a^{-1})^{m_1 - 1}$

$= a^{-m_1 + 1}$

$= a^{m+1} = a^{1+m}$ = RHS

Thus, result is true for $n=1$

Suppose, result is true for $n-1$ i.e.

$a^{n-1} \cdot a^m = a^{n-1+m}$.

then we have to prove that result is true for n

$$L.H.S. = a^n a^m = a^1 \cdot a^{n-1} \cdot a^m$$
$$= a^1 \cdot a^{n-1+m}$$
$$= a^{1+n-1+m} \quad (\because \text{result is true for } n=1)$$
$$= a^{n+m}$$
$$= R.H.S.$$

Thus, result is true for n.
Hence, by mathematical induction, we say that,

$$a^n \cdot a^m = a^{n+m}, \forall\ n>0,\ m<0.$$

* case-(V) :-

If $n<0$ and $m>0$ then we can prove the result.

Hence from case (I), (II), (III), (IV) & (V) we say that,

$$a^n \cdot a^m = a^{n+m}, \forall\ a \in G \text{ \& } m, n \text{ are integers}$$

(2) we have to prove that

$$(a^n)^m = a^{nm}, \forall\ a, b \in G \text{ \& } m, n \text{ are integers.}$$

* case (I) :- $m>0,\ n>0$

$$L.H.S = (a^n)^m$$
$$= (a \cdot a \cdot a \cdots n \text{ times})^m$$
$$= (a \cdot a \cdot a \cdots (n \text{ times})) \cdot (a \cdot a \cdot a \cdots (n \text{ times})) \cdots (m \text{ times})$$
$$= a \cdot a \cdot a \cdots mn \text{ times}$$
$$= a^{mn} = R.H.S.$$

* case (II) :-

If $n<0, m<0$ then $n=-n_1, m=-m_1$, for some $n_1>0,\ m_1>0$.

L.H.S. $= (a^n)^m$, let $a^n = x$

$= (x^{-1})^{m_1}$ $\Rightarrow x = (a^{-1})^{n_1}$

$= (a^{n_1})^{m_1}$ $\Rightarrow x^{-1} = [(a^{-1})^{n_1}]^{-1}$

$= a^{m_1 n_1}$ $= a^{n_1}$

$= a^{(-n)(-m)}$

$= a^{mn}$ = R.H.S.

* case-(iii) :-

If either $n=0$ or $m=0$.

If $n=0$ then $(a^0)^m = e^m = e = a^0$

$= a^{0m} = a^{nm}$ = RHS

Similarly, we can prove for $m=0$.

* case-(IV) :-

If $n>0$ & $m<0$, then $m = -m_1$ for some $m_1 > 0$.

$(a^n)^m$ let $a^n = x$ then

$= (x^{-1})^{m_1}$ $x^{-1} = (a^n)^{-1}$

$= ((a^{-1})^n)^{m_1}$ $= (a^{-1})^n$

$= a^{nm}$

= RHS.

* case-(v) :-

Similarly, we can prove the result when $m>0$ & $n<0$.

(3) $(ab)^n = a^n b^n$

* case-(I) $n>0$

$(ab)^n = ab \cdot ab \cdot ab \cdots$ (n times)

$= (a \cdot a \cdot a \cdots$ n times$)$

$(b \cdot b \cdot b \cdots$ n times$)$ $(\because ab = ba)$

$= a^n \cdot b^n$.

(ii) $(ab)^n = b^n a^n$ $\forall a, b \in G$ Date: / /

* case-(II) $n < 0$ then $n = -n_1$, $n_1 > 0$.

$\therefore (ab)^n = [(ab)^{-1}]^{n_1}$

$= (b^{-1}a^{-1})^{n_1}$

$= (a^{-1}b^{-1})^{n_1}$ ($\because ab = ba$

$= a^n b^n$.

* case-(III) $n = 0$ then

$(ab)^0 = e = e \cdot e = a^0 b^0$

Hence, $(ab)^n = a^n b^n$, $\forall a, b \in G$,
n is integer

* Subgroup of a group:- (nonempty)
Let G be any group. A subset H of G is said to be a subgroup of G if following conditions are satisfied:

(1) $ab \in H$, $\forall a, b \in H$.
(2) $e \in H$, where e is identity of G.
(3) For any $a \in H$ $\exists$ $a^{-1} \in H$.

* Theorem-10:
Prove that, a nonempty subset H of group G is a subgroup of G if and only if
$ab^{-1} \in H$, $\forall a, b \in H$.

proof:-

If H is a subgroup of G then we have to prove that, $ab^{-1} \in H$, $\forall a, b \in H$.

For any $a, b \in H$ then $b^{-1} \in H$ ($\because$ H is subgroup

Thus $a \in H$, $b^{-1} \in H$

$\Rightarrow ab^{-1} \in H$ (by 1st condition of subgroup

→ converse part :-

If $ab^{-1} \in H, \forall a,b \in H$ (*), then we have to prove that H is subgroup of G.

For any $a \in H$, then for $b=a$ by (*)

$$aa^{-1} \in H$$

$$\Rightarrow \boxed{e \in H}$$

Now, $e \in H$, for any $a \in H$ then by (*)

$$ea^{-1} \in H$$

$$\Rightarrow \boxed{a^{-1} \in H}$$

Now, for any $a,b \in H$ then $b^{-1} \in H$

Thus $a \in H, b^{-1} \in H$ then by (*)

$$a(b^{-1})^{-1} \in H$$

$$\Rightarrow \boxed{ab \in H, \forall a,b \in H}$$

Hence, H is subgroup of G.

* Theorem-11:

Prove that a non empty subset H of group $(G,+)$ is a subgroup of $(G,+)$ if and only if $a-b \in H, \forall a,b \in H$

proof :-

→ If H is a subgroup of $(G,+)$ then we have to prove that $a-b \in H$.

For any $a,b \in H$ then $-b \in H$ ($\because$ H subgroup

Thus $a \in H, -b \in H$

$$\Rightarrow a-b \in H$$

→ converse part :-

If $a-b \in H, \forall a,b \in H$ — (*)

then we have to prove that H is subgroup of G.

For any $a \in H$, then for $b=a$, by *

Date : / /

Now $0 \in H$, for any $a \in H$ then by (*)

$0 - a \in H \Rightarrow -a \in H$

Now, for any $a, b \in H$, $-b \in H$

Thus $a \in H$, $-b \in H$, then by (*)

$a-(-b) \in H$

$\Rightarrow a+b \in H$

Hence, H is subgroup of G

* Remark:-

(1) Every group G has atleast two subgroups e & G itself.

(2) A subgroup $\{e\}$ of G is called trivial subgroup and all subgroups of G otherthan e are called non-trivial subgroup of G.

(3) All subgroups otherthan G itself are called proper subgroup of G

* Theorem-12:

Prove that Z is subgroup of Q.

proof:- We know that $(Q, +)$ is a group and $Z \subset Q$ & $Z \neq \phi$.

Clearly $a, b \in Z \Rightarrow a-b \in Z$

Hence, Z is subgroup of $(Q, +)$.

* P.T. Q is subgroup of $\mathbb{C}$.

" R " " " "

" Z " " " "

" Q " " " R.

proof:- We know that $(\mathbb{C}, +)$ is group and $Q \subset \mathbb{C}$ & $Q \neq \phi$

Clearly $a, b \in Q \Rightarrow a-b \in Q$

$-4 \in Z_4$ $a-b \in Z_4$ $\forall a, b \in Z_4$ Date: 10/11

Similarly, $R \subset \mathbb{C}$, $Z \subset \mathbb{C}$ & $Q \subset R$

$\therefore$ R is s.g. of $\mathbb{C}$, Z is s.g. of $\mathbb{C}$ & Q is s.g. of R

* Prove that the set $\{\pm 1, \pm i\}$ is a sub-group of the group of all complex numbers with absolute value 1 under multiplication.

Sol^n Let $H = \{\pm 1, \pm i\}$.

Here $G = \{z \in \mathbb{C} / |z| = 1\}$ group.

Clearly $H \subset G$.

$\cdot$	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

E_2, Z_4 is subset of Z

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$

from the table, we say that,

$ab^{-1} \in H$, $\forall a, b \in H$.

Hence H is subgroup of G.

* Theorem-13 :-

Prove that intersection of two sub-groups of a group is also a subgroup of G.

proof :- Let H_1 and H_2 be any two subgroups of group G then we have to p.t. $H_1 \cap H_2$ is subgroup of G.

i.e. p.t. $ab^{-1} \in H_1 \cap H_2$, $\forall a, b \in H_1 \cap H_2$

Since $H_1 \subset G$, $H_2 \subset G$

$\therefore H_1 \cap H_2 \subset G$ & $H_1 \neq \phi$, $H_2 \neq \phi$.

for any $a, b \in H_1 \cap H_2$ then

$a, b \in H_1$ & $a, b \in H_2$

$\Rightarrow ab^{-1} \in H_1$ & $ab^{-1} \in H_2$

$\Rightarrow ab^{-1} \in H_1 \cap H_2$ ($\because H_1$ & H_2 are subgroups of G)

$\forall a, b \in H_1 \cap H_2$

* Theorem-14:

Prove that, finite no. intersection of subgroup of group G is also a subgroup of G. OR

P.T. Intersection of finite no. of subgroup of group G is also a subgroup of G.

proof:-

Let $H_1, H_2, \ldots, H_n$ be any subgroups of group G then we have to prove that $H_1 \cap H_2 \cap \ldots H_n$ i.e. $\bigcap_{i=1}^{n} H_i$ is a subgroup of G

since $H_i \subset G$, $\forall i = 1, 2, \ldots, n$ & $e \in H_i, \forall i = 1, 2, \ldots, n$

$\therefore \bigcap_{i=1}^{n} H_i \subset G$ & $e \in \bigcap_{i=1}^{n} H_i$

$\therefore \bigcap_{i=1}^{n} H_i \neq \emptyset$.

We have to prove that

$ab^{-1} \in \bigcap_{i=1}^{n} H_i$, $\forall a, b \in \bigcap_{i=1}^{n} H_i$

For any $a, b \in \bigcap_{i=1}^{n} H_i$

$\Rightarrow a, b \in H_i, \forall i = 1, 2, \ldots, n$

$\Rightarrow ab^{-1} \in H_i, \forall i = 1, 2, \ldots, n$

($\because$ each H_i is subgroup of G)

Date: / /

$\Rightarrow ab^{-1} \in \bigcap_{i=1}^{n} H_i$

Hence, $\bigcap_{i=1}^{n} H_i$ is subgroup of G.

* Theorem-15:

Prove that intersection of any no. of subgroups of group G is also a subgroup of G.

proof:- Let $\wedge$ be index set.

Let $H_i, \forall i \in \wedge$ be subgroups of group G then we have to prove that

$\bigcap_{i \in \wedge} H_i$ is a subgroup of G.

Since $H_i \subset G, \forall i \in \wedge, e \in H_i, \forall i \in \wedge$

$\therefore \bigcap_{i \in \wedge} H_i \subset G$ & $e \in \bigcap_{i \in \wedge} H_i$

we have to prove that,

$ab^{-1} \in \bigcap_{i \in \wedge} H_i, \forall a, b \in \bigcap_{i \in \wedge} H_i$

For any $a, b \in \bigcap_{i \in \wedge} H_i$

$\Rightarrow a, b \in H_i, \forall i \in \wedge$

$\Rightarrow ab^{-1} \in H_i, \forall i \in \wedge$ ($\because$ each H_i is

$\Rightarrow ab^{-1} \in \bigcap_{i \in \wedge} H_i$ subgroup of G)

Hence, $\bigcap_{i \in \wedge} H_i$ is subgroup of G.

(*) Theorem-16:

Prove that mZ is subgroup of Z ($\forall$ some $m \in Z$)

proof:- Let $H = mZ = \{0, \pm m, \pm 2m, \pm 3m, \ldots\}$

Here $G = (Z, +)$

Date : / /

Clearly $H \subseteq G$ and $H \neq \phi$.

We have to prove that $a-b \in H, \forall a,b \in H$.

for any $a,b \in H = mZ$ then

$a = ma_1, b = mb_1$ for some $a_1, b_1 \in$

$\therefore a-b = ma_1 - mb_1$

$\Rightarrow a-b = m(a_1-b_1) \in mZ = H \quad (\because a_1-b_1 \in Z)$

$\Rightarrow a-b \in H, \forall a,b \in H$

$\Rightarrow H = mZ$ is a subgroup of Z.

* Prove or disprove.

Union of two subgroups of a group is ~~not~~ a subgroup.

soln :- Union of two subgroups of a group need not be a subgroup.

Let $G = (Z, +)$

Let $H_1 = 2Z, H_2 = 3Z$ be subgroups of Z.

Since $3 \in H_2, 2 \in H_1$

$\Rightarrow 3 \in H_1 \cup H_2, 2 \in H_1 \cup H_2$

but $3-2 = 1 \notin H_1 \cup H_2$

Thus $H_1 \cup H_2$ is not a subgroup.

* Prove that union of 3 subgroups of group need not be a subgroup.

proof :- Let $G = (Z, +)$

Let $H_1 = 2Z, H_2 = 3Z, H_3 = 5Z$. be subgroups of Z

since $2 \in H_1, 3 \in H_2, 5 \in H_3$

$\Rightarrow 2 \in H_1 \cup H_2 \cup H_3, 3 \in H_1 \cup H_2 \cup H_3$ &

$5 \in H_1 \cup H_2 \cup H_3$

but $3-2 = 1 \notin H_1 \cup H_2 \cup H_3$

Thus $H_1 \cup H_2 \cup H_3$ is not a subgroup.

Date :

* Theorem-16 :

Let H be any finite subset of group G such that $a, b \in H \Rightarrow a \cdot b \in H$ then p.t. H is subgroup G.

proof :-

Here H is finite subset of G. and

$a \cdot b \in H, \forall a, b \in H$

We have to p.t. H is subgroup of G

∴ By def^n. of subgroup it is sufficient to p.t. $e \in H$ & $a^{-1} \in H$ for $a \in H$.

for any $a \in H$ then $a^2 \in H, a^3 \in H, \ldots a^n \in H, \ldots$

i.e $a, a^2, a^3, a^4, \ldots, a^n, \ldots \in H$ — (*)

Since H is finite, atleast two elements of (*) are same

Let $a^m = a^n$ for $m \neq n$ & $m > n$.

* Then $a^m = a^n$

$\Rightarrow a^m \cdot a^{-n} = a^n \cdot a^{-n}$

$\Rightarrow a^{m-n} = e \quad (m-n > 0)$

Now, $a^{m-n} = a^m \cdot a^{-n}$

$= a^m (a^n)^{-1}$

$= a^n \cdot (a^n)^{-1} = e$

$\Rightarrow a^{m-n} = e$ & $m > n$ ∴ $m-n > 0$

thus $e \in H$ (∵ $a^{m-n} \in H$)

We know that,

$a^{m-n} = e$

∴ $a^{-1} \cdot a^{m-n} = a^{-1} \cdot e = a^{-1}$

∴ $a^{m-n-1} = a^{-1}$

∴ $a^{-1} = a^{m-n-1} \in H \quad (\because m > n)$.

$a \cdot a^{m-n-1} = e = a^{m-n-1} a$

∴ Inverse prop. is satisfied

Date: / /

* Theorem-17 :-

Let H be any finite subset of group $(G,+)$ such that $a+b \in H$ whenever $a,b \in H$ then H is subgroup of G.

proof :- Here H is finite subset of G and $a+b \in H, \forall a,b \in H$.

we have to p.t. H is subgroup of G

∴ By def^n. of subgroup it is sufficient to p.t. $0 \in H$ & $-a \in H$ for $a \in H$

for any $a \in H$ then $2a \in H, 3a \in H, \ldots$ $na \in H, \ldots$

i.e $a, 2a, 3a, \ldots, na, \ldots \in H$ — (*)

Since H is finite

∴ atleast two [of them] elements of (*) are same

Let $ma = na$ for $m \neq n$ & $m > n$

Now,

$$ma - na = ma + (-na)$$
$$= ma - ma = 0$$
$$\Rightarrow ma - na = 0 \quad \& \; m > n$$

thus $0 \in H$

We know that,

$$ma - na = 0$$
$$\Rightarrow ma - na - a = 0 - a = -a$$
$$\Rightarrow a(m-n-1) = -a$$
$$\Rightarrow -a = a(m-n-1) \in H \; (\because m > n$$

Thus, $a + a(m-n-1) = 0 = a(m-n+1) +$

∴ Inverse property is satisfied

Hence,

H is a subgroup of G.

Date : / /

* Centre of group:-
Centre of group G is denoted by $Z(G)$ and defined as

$$Z(G) = \{x \in G / xa = ax, \forall a \in G\}$$

* Theorem-18:
Prove that $Z(G)$ is a subgroup of group G

proof:-
Clearly, $Z(G) \subset G$ and $e \in Z(G)$.
$\therefore Z(G) \neq \phi$.
Now we prove that,
$xy^{-1} \in Z(G), \forall x, y \in Z(G)$

for any $x, y \in Z(G)$ then
$xa = ax, \forall a \in G$ &
$ya = ay, \forall a \in G$
Now,

$$\begin{aligned}(xy^{-1})a &= x(y^{-1}a) \\ &= x(ay^{-1}) \\ &= (xa)y^{-1} \\ &= (ax)y^{-1} \\ &= a(xy^{-1})\end{aligned}$$

$ya = ay$
$\Rightarrow y^{-1}(ya)y^{-1} = y^{-1}(ay)y^{-1}$
$\Rightarrow ay^{-1} = y^{-1}a$

Thus $(xy^{-1})a = a(xy^{-1}), \forall a \in G$
Hence, $Z(G)$ is subgroup of G.

* Theorem-19:
If group G is abelian group then p.t.
$G = Z(G)$ also prove the converse.

Date: / /

proof:- If G is abelian group then

$$xy = yx, \forall\ x, y \in G \cdots (*)$$

we have to p.t.

$$G = Z(G)$$

Clearly $Z(G)$ is a subset of G.

Now,

we p.t. G is subset (set) of $Z(G)$.

for any $x \in G$ then

$$xa = ax, \forall\ a \in G. \quad (\because G \text{ is abelian})$$

$$\Rightarrow x \in Z(G).$$

$\therefore G$ is subset of $Z(G)$.

Hence,

$$G = Z(G)$$

→ converse part:-

If $G = Z(G)$ then we have to p.t.

G is abelian group.

for any $x, y \in G$ then $xy \in Z(G)$.

$\therefore xa = ax, \forall a \in G$

$\Rightarrow xy = yx \quad (\because y \in G)$

$\Rightarrow G$ is abelian group.

* Find centre of $(Z, +)$.

soln:- we know that $(Z, +)$ is abelian group.

$\therefore$ By above thm we say that

$$Z(Z) = Z$$

i.e. centre of Z is Z itself.

★ Let H_1 and H_2 be two subsets of group G then

$$H_1 + H_2 = \{ h_1 + h_2 / h_1 \in H_1, h_2 \in H_2 \}$$

$$H_1 H_2 = \{ h_1 h_2 / h_1 \in H_1, h_2 \in H_2 \}$$

$$H_1^{-1} = \{ h_1^{-1} / h_1 \in H_1 \}$$

for $a \in G$

$$H_1 a = \{ h_1 a / h_1 \in H_1 \}$$

$$a H_1 = \{ a h_1 / h_1 \in H_1 \}$$

$$H_1 + a = \{ h_1 + a / h_1 \in H_1 \}$$

Defⁿ

★ Let G be any group and 'a' be fixed element of G then the centrelizer of 'a' is denoted by N(a) and defined as

$$N(a) = \{ x \in G / xa = ax \}$$

Let $A \subset G$ then the normalizer of A is denoted by N(A) and defined as

$$\{ x \in G / xA = Ax \}$$

→ If $A = \{a\}$ then $N(A) = N(a)$.

Theorem-20: Prove that, N(A) is subgroup of group G, $\forall A \subset G$.

Solⁿ:- We know that,

$$N(A) = \{ x \in G / xA = Ax \}.$$

Clearly $N(A) \subset G$. & $eA = Ae$

$\therefore e \in N(A)$

$\therefore N(A) \neq \phi$.

Date: / /

we have to prove that

$xy^{-1} \in N(A), \forall x, y \in N(A)$.

i.e to p.t.

$(xy^{-1})A = A(xy^{-1})$

$L.H.S. = (xy^{-1})A = x(y^{-1}A)$

$= x(Ay^{-1})$

$= (xA)y^{-1}$

$= (Ax)y^{-1}$

$= A(xy^{-1})$

$= R.H.S.$

$yA = Ay$

$\Rightarrow y^{-1}(yA)y^{-1} = y^{-1}(Ay)y^{-1}$

$\Rightarrow Ay^{-1} = y^{-1}A$

Hence, $N(A)$ is subgroup of G.

Theorem-21 ▶ For $a \in G$ prove that, $N(a)$ is subgroup of G also prove that, $Z(G) \subset N(a)$.

proof:- $N(a) = \{x \in G / xa = ax\}$

Clearly $N(a) \subset G$ & $ea = ae$

$\therefore e \in N(a)$

$\therefore N(a) \neq \phi$.

we have to prove that,

$xy^{-1} \in N(a), \forall x, y \in N(a)$

i.e to prove that

$(xy^{-1})a = a(xy^{-1})$

$L.H.S. = (xy^{-1})a = x(y^{-1}a)$

$= x(ay^{-1})$

$= (xa)y^{-1}$

$= (ax)y^{-1}$

$= a(xy^{-1}) = R.H.S.$

$x \in N(a)$ ($\because N(a) = \{x / xa = ax\}$)

$\Rightarrow Z(a) \subset N(a)$

Hence $N(a)$ is subgroup of G

(**) for any $x \in Z(G)$ then by def^n of $Z(G)$

Theorem-22 ▶ Let H and K be any subgroups of G then prove that,

HK is a subgroup of G iff HK=KH

proof:-

If HK is a subgroup of G then we have to prove that HK=KH

first we prove that,

$HK \subset KH$

for any $x \in HK$,

Since HK is subgroup, $x^{-1} \in HK$.

$\therefore x^{-1} = hk$ for some $h \in H, k \in K$.

Now,

$x = (x^{-1})^{-1} = (hk)^{-1} = k^{-1}h^{-1} \in KH$

(∵ H and K are subgroups $\therefore h^{-1} \in H, k^{-1} \in K$)

Thus, $HK \subset KH$ —— (*)

Now, we prove that,

$KH \subset HK$.

for any $x \in KH$, then $x = kh$, for some $k \in K$ and $h \in H$

$x = kh \Rightarrow x^{-1} = (kh)^{-1}$

$= h^{-1}k^{-1} \in HK$

$x^{-1} \in HK$ & HK is subgroup

$\Rightarrow (x^{-1})^{-1} \in HK$

$\Rightarrow x \in HK$

Thus, $KH \subset HK$ —— (**)

By (*) & (**),

$\boxed{KH = HK}$

Date: / /

→ Converse part :-

If $HK = KH$ then we have to prove that

$$xy^{-1} \in HK, \forall x, y \in HK$$

for any $x, y \in HK$

$x = h_1k_1$, $y = h_2k_2$ for some $h_1, h_2 \in H$ & $k_1, k_2 \in K$.

$$y^{-1} = k_2^{-1}h_2^{-1}.$$

Now, $xy^{-1} = h_1k_1k_2^{-1}h_2^{-1}$

$= h_1k_3h_2^{-1}$, where $k_3 = k_1k_2^{-1} \in HK$

$= h_1h_4k_4$, where $k_3h_2^{-1} \in KH = HK$

$\therefore k_3h_2^{-1} = h_4k$

$= h_5k_4$ & $h_5 = h_1h_4$

$\in HK$

* Remark :-

Product of two subgroups of group need not be a subgroup.

Theorem-23 ▶ Let H and K be any finite subgroup of group such that HK is also a subgroup then p.t.

$$O(HK) = \frac{O(H)\,O(K)}{O(H \cap K)}.$$

proof:- Let $H = \{h_1, h_2, \ldots, h_m\}$

$K = \{k_1, k_2, \ldots, k_n\}$ then

$O(H) = m$, $O(K) = n$

also, $HK = \{h_i k_j / 1 \le i \le m, 1 \le j \le n, h_i \in H, k_j \in K\}$.

It contains mn elements

Clearly all elements of HK need not be distinct

Now, we shall find out how many times a particular element repeat

Suppose, we consider the element $h_4 k_4$

Let $h_4 k_4 = h_i k_j$, for some i, j then

$h_4 k_4 = h_i k_j \Rightarrow h_i^{-1}(h_4 k_4) k_4^{-1} = h_i^{-1}(h_i k_j) k_4^{-1}$

$\Rightarrow h_i^{-1} h_4 = k_j k_4^{-1} = t$ (say)

Since,

$h_i^{-1} h_4 \in H$, $k_j k_4^{-1} \in K$

$\therefore t \in H$ & $t \in K$

i.e $t \in H \cap K$

also,

$h_i^{-1} h_4 = t \Rightarrow h_i h_i^{-1} h_4 = h_i t$

$\Rightarrow h_4 t^{-1} = h_i t t^{-1}$

$\Rightarrow h_i = h_4 t^{-1}$

& $k_j k_4^{-1} = t \Rightarrow k_j = t k_4$

Thus, $h_i = h_4 t^{-1}$, $k_j = t k_4$, where $t \in H \cap K$

Thus, $h_4 k_4$ repeats $O(H \cap K)$ times.

(**) For any $a \in Z(G)$ then

$xa = ax$

$\therefore a \in N(a)$ $\left(\because N(a) = \{x \in G \mid xa = ax\}\right)$

Similarly we can say that each element of HK repeats $O(H \cap K)$ times.

Hence,

$$mn = O(H \cap K)\, O(HK)$$

$$\Rightarrow O(HK) = \frac{mn}{O(H \cap K)}$$

$$\Rightarrow O(HK) = \frac{O(H)\, O(K)}{O(H \cap K)}$$

Hence, theorem is proved.

corrolary :- If H and K are finite subgroup of group G such that $G = HK$ and $H \cap K = \{e\}$ then $O(G) = O(H)\, O(K)$.

proof :-

By above theorem we get

$$O(HK) = O(G) = \frac{O(H)\, O(K)}{O(H \cap K)}$$

$$\Rightarrow O(G) = \frac{O(H)\, O(K)}{1} \quad \left(\because G = HK,\ O(H \cap K) = 1\right)$$

$$\Rightarrow O(G) = O(H)\, O(K).$$

Theorem 24 ➤

Let G be a group and $a \in G$ then prove that, $\{a^n / n \in Z\}$ is the smallest subgroup of G containing 'a'.

proof:- $H = \{a^n / n \in Z\}$

first we prove that H is subgroup of G.

since, $a \in G \therefore a^n \in G \therefore H \subset G$.

also $e = a^0 \in H \therefore H \neq \emptyset$.

Now we prove that

$xy^{-1} \in H, \forall x, y \in H$

for any $xy \in H$ then

$x = a^{n_1}, y = a^{n_2}$ for some $n_1, n_2 \in Z$

$xy^{-1} = a^{n_1}(a^{n_2})^{-1}$

$= a^{n_1} a^{-n_2} = a^{n_1 - n_2} \in H \ (\because n_1 - n_2 \in Z)$

Thus, H is subgroup of G.

also,

clearly $a = a^1 \in H$

If K is any subgroup of G containing a then it is sufficient to p.t. $H \subset K$.

for any $a^{n_1} \in H$ then since $a \in K$ and K is subgroup of G

$\therefore a^{n_1} \in K$

Thus, $H \subset K$

Hence, H is the smallest subgroup of G containing a.

U-2 **UNIT-2**

* ~~Remarks~~:- Definition: Cyclic Group:

(1) Group G is said to be a cyclic group if it is generated by some of its element $= \{a^n / n \in Z\}$

i.e. $G = \langle a \rangle$ for some $a \in G$

Unit 2

(2) A group $(G,*)$ is said to be a cyclic group if.

$G = \langle a \rangle$, for some $a \in G$

i.e $G = \{na / n \in \mathbb{Z}\}$.

* Find all generators of $\mathbb{Z}$, if possible. Is $\mathbb{Z}$ cyclic group?

Sol:-

We know that,

$\mathbb{Z} = \{0, \pm 1, \pm 2, \cdots\}$

$(\mathbb{Z}, +)$ is group.

We know that,

if $\langle a \rangle = \mathbb{Z}$ then a is generator of $\mathbb{Z}$.

Clearly,

$\langle 1 \rangle = \{n1 / n \in \mathbb{Z}\} = \{n / n \in \mathbb{Z}\}$

$= \{0, \pm 1, \pm 2, \cdots\} = \mathbb{Z}$

similarly,

$\langle -1 \rangle = \{n(-1) / n \in \mathbb{Z}\}$

$= \{0, \pm 1, \pm 2, \cdots\} = \mathbb{Z}$

Thus ± 1 are generators of $\mathbb{Z}$.

i.e. $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$.

also $\mathbb{Z}$ is cyclic group.

* Is $\{\pm 1, \pm i\}$ cyclic group?

Sol:- Is fourth root of Unity cyclic group?

Let $G = \{\pm 1, \pm i\}$ then

$(G, \cdot)$ is a group.

$\langle 1 \rangle = \{1^n / n \in Z\} = \{1\} \neq G$

$\langle -1 \rangle = \{(-1)^n / n \in Z\} = \{-1, 1\} \neq G$

$\langle i \rangle = \{i^n / n \in Z\} = \{1, i, -1, -i\} = G$

$\langle -i \rangle = \{(-i)^n / n \in Z\} = \{1, -i, -1, i\} = G$

Thus, $G = \langle i \rangle = \langle -i \rangle$.

Hence, G is cyclic group generated by $\pm i$.

* (I) Is $\{\ldots, \frac{1}{16}, \frac{1}{8}, \frac{1}{4}, \frac{1}{2}, 1, 2, 4, 8, 16, \ldots\}$ cyclic group?

(II) Is $(Z_n, +)$ cyclic group?

Soln :- (I) Let $G_1 = \{\ldots, 1/16, 1/8, 1/4, 1/2, 1, 2, 4, \ldots\}$

Then $\{G_1, \cdot\}$ is group.

$\langle 1 \rangle = \{1^n / n \in Z\} = \{1\} \neq G_1$

$\langle 2 \rangle = \{2^n / n \in Z\} = \{\ldots, 1/16, 1/8, 1/4, 1/2, 1, 2, \ldots\}$

$= G$

Similarly,

$\langle 1/2 \rangle = \{(1/2)^n / n \in Z\} = \{\ldots, 1/8, 1/4, 1/2, 1, 2, \ldots\}$

$= G$

Hence, $G_1 = \langle 2 \rangle = \langle 1/2 \rangle$

$\therefore$ G_1 is cyclic group.

(II) $G_2 = (Z_n, +)$

$Z_n = \{\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{n-1}\}$

$\langle \bar{0} \rangle = \{\bar{0}\} \neq Z_n$

$\langle \bar{1} \rangle = \{\bar{0}, \bar{1}, \bar{2}, \ldots \overline{n-1}\} = Z_n$

(25) Every cyclic group is abelian.

proof:-

Let G be any cyclic group generate by a

i.e. $G = \langle a \rangle = \{a^n / n \in Z\}$.

We have to p.t. G is abelian

i.e. p.t. $xy = yx$, $\forall x, y \in G$.

for any $x, y \in G$ then

$x = a^{n_1}$, $y = a^{n_2}$, for $n_1, n_2 \in Z$.

$$\therefore xy = a^{n_1} \cdot a^{n_2}$$
$$= a^{n_1+n_2}$$
$$= a^{n_2+n_1}$$
$$= a^{n_2} \cdot a^{n_1}$$
$$= yx$$

Hence, G is abelian.

(26) Every subgroup of a cyclic group is also cyclic.

proof:-

Let G be any cyclic group generate by a.

i.e $G = \langle a \rangle = \{a^n / n \in Z\}$.

Let H be any subgroup of G

* case-1 : If $H = \{e\}$ then

clearly $H = \langle e \rangle$.

$\therefore$ H is cyclic.

* case-2 : If $H \neq \{e\}$

then $\exists\ x \in H \ni x \neq e$.

Now, $x \in H \subset G = \langle a \rangle$.

$\therefore x = a^n$, for some $n \in Z$.

also H is subgroup and $x \in H$.

$\therefore x^{-1} \in H$

$\Rightarrow (a^n)^{-1} \in H$

$\Rightarrow a^{-n} \in H$.

Thus $a^n \in H$ & $a^{-n} \in H$ for $n \in Z$.

Thus, we say that $a^p \in H$, for some $p > 0$.

Let m be the least +ve integer $\ni a^m \in H$.

then $(a^m)^n \in H$ ($\because$ H is subgroup)

Hence, $\langle a^m \rangle \subset H$ ($\because \langle a^m \rangle = \{(a^m)^n / n \in Z\}$

Now, we prove that, $H \subset \langle a^m \rangle$.

for any $y \in H$ then

$y \in H \subset G = \langle a \rangle$.

$\therefore y = a^l$, for some $l \in Z$.

Now, by division algorithm property for $l, m \in Z$, we say that, $\exists\ q, r \in Z \ni$

$l = qm + r$, $0 \leq r \leq m-1$ .... (*)

suppose $r > 0$ then

$a^r = a^{l-qm}$

$= a^l \cdot (a^m)^{-q} \in H$ ($\because a^l \in H, a^m \in H$ & H is subgroup

Thus, if $0 < r \leq m-1$ then $a^r \in H$.

Thus we get contradiction because m is the least +ve power such that $a^m \in H$.

$\therefore r > 0$ is not possible

$\therefore r = 0$.

$\therefore$ By (*) $l = qm$

$\therefore y = a^l = a^{qm} = (a^m)^q \in \langle a^m \rangle$.

Thus $H \subset \langle a^m \rangle$

Date: / /

* Corollary:-

P.T. any subgroup of Z is of the form nZ, for some n∈Z.

proof:- We know that, Z is cyclic group generated by ±1.

i.e. $Z = \langle 1 \rangle = \langle -1 \rangle$.

Let H be any subgroup of (Z,+) then by above theorem, we say that H is also cyclic group.

and H is $\langle m \cdot 1 \rangle = \langle m(-1) \rangle$

i.e. $H = \langle m \rangle = \langle -m \rangle$.

$\therefore H = \{nm / n \in Z\} = \{0, \pm m, \pm 2m, \ldots\}$

$\therefore H = mZ$, for some $m \in Z$.

Hence, every subgroup of Z is of the form nZ, for $n \in Z$

(21) Every subgroup of an infinite cyclic group is also an infinite cyclicgroup.

proof:-

Let G be any infinite cyclic group generated by a.

$\therefore G = \langle a \rangle$.

first we p.t. all elements of G are distinct.

Suppose, $a^i = a^j$ for some $i \neq j$, $i > j$ then,

$$a^{i-j} = a^i \cdot a^{-j} = a^i \cdot (a^j)^{-1}$$

$$= a^j \cdot (a^j)^{-1} = e$$

Thus, $a^{i-j} = e$, where $i - j > 0$.

Date: 5/10

Let m be the least positive integer
$\ni$ $a^m = e$.

Let any $x \in G$ then $x = a^n$, for some $n \in Z$

then by divison-algorithm property for m, n we say that $\exists\ q, r \in Z\ \ni$

$n = qm + r$, where $0 \leq r < m$.

Now,

$$a^r = a^{n-qm}$$
$$= a^n (a^m)^{-q}$$
$$= a^n \cdot e = a^n = x$$

Thus, $x = a^r$, where $0 \leq r < m$

$\therefore G = \{a^0 = e, a^1, a^2, a^3, \ldots, a^{m-1}\}$

which is finite set $\because$

because G is an infinite set.

Hence all elements of G are distinct

Let H be any subgroup G then H is cyclic group and $H = \langle a^m \rangle$, for some m

also all elements of H are distinct

$\therefore H = \langle a^m \rangle = \{(a^m)^n / n \in Z\}$ is an infinite cyclic group.

Hence thm is proved.

* Remark:-

We say that 'a divides b' if $b = am$, for some $m \in Z$

'a divides b' is denoted by a/b.

(28) Let G be a finite cyclic group of order n, then prove that G has unique subgroup of order 'd' for every divisor d of n.

proof:-

Let $G = \langle a \rangle$ be any cyclic group of order n.

first we p.t n is the smallest +ve integer $\ni a^n = e$.

Suppose m is the smallest +ve integer $\ni a^m = e$ then by division algorithm property on m, k, we say that $\exists\ q, r \in \mathbb{Z}$ $\ni k = qm + r$, where $0 \le r \le m-1$.

Now, $a^r = a^{k-qm}$

$= a^k \cdot a^{-qm}$

$= a^k \cdot (a^m)^{-q}$

$= a^k e = a^k = x$, $0 \le k < m$,

Thus for any $x = a^n \in G$, we get

$G = \{e = a^0, a^1, a^2, \ldots, a^{m-1}\}$

Thus $o(G) = m$ but $o(G) = n$

$\therefore m = n$

Hence n is the smallest +ve integer $\ni a^n = e$.

Let d be any divisor of n

i.e. $d/n \Rightarrow n = dd'$ for some $d' \in \mathbb{Z}$.

Since G is cyclic group generated by a $\therefore$ its subgroup $H = \langle a^{d'} \rangle$ is also cyclic subgroup of G.

Now, we show that, $O(H) = d$.

Here, $(a^{d'})^d = a^{dd'} = a^n = e$.

Thus, d is the least +ve integer $\ni$ $(a^{d'})^{d^*} = e$.

Hence, H contains d elements i.e $O(H) = d$

$O(H) = d$. Now we prove that this subgroup of order d is unique.

Suppose H' is any subgroup of order d then H' is also cyclic

Let $H' = \langle a^l \rangle$, for some $l \in Z$.

then $(a^l)^d = a^{ld} = e$

Now, by divison algorithm property for l and d' we say that $\exists$ q, r such that

$$l = qd' + r \text{, where } 0 \le r \le d'-1 \quad \text{---(*)}$$

$$\therefore e = (a^l)^d = a^{ld}$$
$$= a^{qd'd + rd}$$
$$= a^{qn + rd} \quad (\because dd' = n$$
$$= a^{qn} \cdot a^{rd}$$
$$= (a^n)^q \cdot a^{rd}$$
$$= e \cdot a^{rd}$$
$$= a^{rd}$$

Thus, $a^{rd} = e$, where $0 \le r \le d'-1$

i.e. $0 \le r < d'$

i.e $0 \le rd < dd'$

i.e $0 \le rd < n$

Thus, $a^{rd} = e$, where $0 \le rd < n$ $\ast$

because n is the least +ve integer $\ni$ $a^n = e$

$\therefore r = 0 \quad \therefore l = qd'$

$\therefore a^l = a^{qd'} = (a^{d'})^q \Rightarrow H' \subset H$

Date: / /

also $O(H) = O(H') = d$

$\therefore H = H'$

Hence, H is the unique subgroup of order d.

(Eg) Prove that, every infinite cyclic group has exactly two generators.

proof:-

Let $G = \langle a \rangle$ be any infinite cyclic group.

Let b be any generator of G then $G = \langle b \rangle$.

since $b \in G$ & $G = \langle a \rangle$.

$\therefore b \in \langle a \rangle$ $\therefore b = a^m$, for some $m \in Z$. —(*)

similarly, $a \in G$ & $G = \langle b \rangle$

$\therefore a \in \langle b \rangle$

$\therefore a = b^n$ for some $n \in Z$.

Now,

$a = b^n = (a^m)^n = a^{mn}$.

$\Rightarrow a a^{-1} = a^{mn} \cdot a^{-1}$

$\Rightarrow e = a^{mn-1}$.

$\Rightarrow a^{mn-1} = e = a^0$

$\Rightarrow mn - 1 = 0$ (∵ G is infinite cyclic group)

$\Rightarrow mn = 1$

$\Rightarrow m = \pm 1$

$\Rightarrow b = a^{\pm 1}$ (by (*))

$\Rightarrow b = a, b = a^{-1}$ are generators of G

Thus every infinite cyclic group has exactly two generators.

* Prime no.:-
p is said to be a prime if either 1/p or p/p

* Relatively prime no.:-
Two numbers a and b are said to be relatively prime nos. if G.C.D. of a & b is 1
i.e. $(a,b)=1$.

* Euler's function:-
Euler's function of $n (n \geq 2)$ is denoted by $\phi(n)$ and defined as
$\phi(n)$ = Total nos of elements which are less than n & relatively prime to n

n	2	3	4	5	6	7	8	9	10	11	12
$\phi(n)$	1	2	2	4	2	6	4	6	4	10	4

→ If n is prime no., then $\phi(n)=n-1$.
→ $(m,n)=1$ iff $\exists\ x,y \in \mathbb{Z}$ s.t. $mx+ny=1$

(30) If $G=\langle a \rangle$ is cyclic group of order n then prove that n is the smallest +ve integer s.t. $a^n=e$.

proof:- Let $G=\langle a \rangle$ be any cyclic group of order n.
We have to p.t. n is the smallest +ve integer s.t. $a^n=e$.
suppose m is smallest +ve integer s.t. $a^m=e$. Then by division algorithm property on m & n we say that $\exists\ q,r \in \mathbb{Z}$

Date: / /

Now $a^r = a^{k-qm}$

$= a^k \cdot a^{-qm}$

$= a^k \cdot (a^m)^{-q}$

$= a^k \cdot e$

$= a^k$, $0 \le r < m$

Thus for any $x = a^k \in G$, we get

$G = \{a^0 = e, a^1, a^2, a^3, \cdots, a^{m-1}\}$

Thus $o(G) = m$ & $o(G) = n$

$\therefore m = n$

Hence n is the smallest +ve integer $\ni$ $a^n = e$

(31) If $G \overset{\langle a \rangle}{=}$ is cyclic group of order n and $a^m = e$ for some $m \in Z$ then prove that n/m.

proof :-

Here we have given that $G \overset{\langle a \rangle}{=}$ is cyclic group of order n.

$\therefore n$ is the least +ve integer $\ni$ $a^n = e$

also given that $a^m = e$.

$\therefore$ By division-algorithm property on m, n, we say that $\exists\ q, r \in Z \ni$

$m = qn + r$, $0 \le r < n$

if $0 < r < n$ then

$a^r = a^{m-qn}$

$= a^m \cdot a^{-qn}$

$= a^m \cdot (a^n)^{-q} = e \cdot e = e$

Thus $0 < r < n$, $a^r = e$ ✗

$\therefore r = 0$

$\therefore m = qn \Rightarrow n/m$

Date: 6/3/20

(32) If G is a finite cyclic group of order n then prove that G has $\phi(n)$ generators.

proof:-

Let $G = \langle a \rangle$ be any finite cyclic group of order n.

Let any $b \in G$ then $b = a^m$, for some $m \in Z$.

Now it is sufficient to p.t. b is generator of G iff $(m,n) = 1$.

If b is generator of G then $G = \langle b \rangle$

since, $a \in G$ & $G = \langle b \rangle$.

$\therefore a \in \langle b \rangle$.

$\therefore a = b^k$, for some $k \in Z$

$\therefore a = (a^m)^k$

$\Rightarrow a = a^{mk}$.

$\Rightarrow a a^{-1} = a^{mk} \cdot a^{-1}$

$\Rightarrow a^{mk-1} = e$

$\Rightarrow n / mk-1$ ($\because O(G) = n$).

$\Rightarrow mk-1 = qn$, for some $q \in Z$

$\Rightarrow km - qn = 1$, for some $q \in Z$

$\Rightarrow km + (-q)n = 1$ " " $q \in Z$

$\Rightarrow (m,n) = 1$ " " $q \in Z$.

→ converse part:-

If $(m,n) = 1$ then $\exists\ x, y \in Z \ni$

$mx + ny = 1$.

Now, $a = a^1 = a^{mx+ny}$

$= (a^m)^x (a^n)^y$

$= (a^m)^x e$

$= (a^m)^x$

Date: / /

Thus for any $a \in G$, we have

$a = (a^m)^x \in \langle a^m \rangle = \langle b \rangle$ ($\because b = a^m$)

Thus $G \subset \langle b \rangle$

also clearly $\langle b \rangle \subset G$ ($\because b = a^m$)

Thus $G = \langle b \rangle$.

i.e b is generator of G.

Hence G has total $\phi(n)$ generators.

* Remarks:-

(1) If G is cyclic group of prime order p then by above thm G has $\phi(p) = p-1$ generators and all non trivial elements of G are generators of G.

(2) If $G = \langle a \rangle$ is an infinite cyclic group then $a^n \neq e$ for any $n \neq 0$.

* Order of element:-

Let G be any group and $a \in G$, then 'order of a' is said to be n' if n is the least integer such that $a^n = e$.

If no such n exists then order of a is said to be infinite.

order of a is denoted by $o(a)$.

* $G = \langle a \rangle$ is cyclic group of order n iff $o(a) = n$.

Sol:- If $G = \langle a \rangle$ is cyclic group of order n then n is the least +ve integer $\ni a^n = e$

Hence $o(a) = n$ (if Ex asked in

$\therefore a^r = a^{qn} \cdot a^s = a^s, \quad 0 \le s < n$

$\therefore a^r = a^s, \quad 0 \le s < n$

→ converse part:- $\therefore G = \{e, a, a^2, \ldots, a^{n-1}\}$

$o(a) = n$ then by def^n n is the least positive integer $\ni a^n = e$

then $G = \{a^0 = e, a^1, a^2, \ldots, a^{n-1}\}$.

Thus $o(G) = n$.

* If G is an infinite cyclic group generated by a then $o(a)$ is infinite

proof:-

Suppose $o(a)$ is finite (say n) then by above thm G is cyclic group of order n ✗

because G is infinite cyclic group

Thus $o(a)$ is infinite.

* Let C^* be the set of all non zero complex numbers then find $o(i)$ & $o(-i)$.

soln:-

$i^1 = i$	$(-i)^1 = -i$
$i^2 = -1$	$(-i)^2 = -1$
$i^3 = -i$	$(-i)^3 = i$
$i^4 = 1$	$(-i)^4 = 1$

Thus $o(i) = o(-i) = 4$

* Find $o(2)$ in Z.

soln:- We know that $(Z, +)$ is group.

$1 \cdot 2 = 2$

$2 \cdot 2 = 2+2 = 4$

$3 \cdot 2 = 2+2+2 = 6$

$4 \cdot 2 = 2+2+2+2 = 8$

⋮

Thus we cannot find any two integers n

* Find order of each element of $(Z_6, +)$

Sol^n :-

$(Z_6, +)$ is a group.

$Z_6 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$.

$O(\bar{0}) = 1 \cdot \bar{0} = \bar{0}$ $\therefore O(\bar{0}) = 1$

$O(\bar{1}) = 6 \cdot \bar{1} = \bar{0}$ $\therefore O(\bar{1}) = 6$

$O(\bar{2}) = 3 \cdot \bar{2} = \bar{0}$ $\therefore O(\bar{2}) = 3$

$O(\bar{3}) = 2 \cdot \bar{3} = \bar{0}$ $\therefore O(\bar{3}) = 2$

$O(\bar{4}) = 3 \cdot \bar{4} = \bar{0}$ $\therefore O(\bar{4}) = 3$

$O(\bar{5}) = 6 \cdot \bar{5} = \bar{0}$ $\therefore O(\bar{5}) = 6$.

* Find order of each element of group $\{\pm 1, \pm i\}$.

Sol^n :- Here $(G, \cdot)$ is group.

$O(1)$:- $1^1 = 1$ $\therefore O(1) = 1$

$O(-1)$:- $(-1)^2 = 1$ $\therefore O(-1) = 2$.

$O(i)$:- $(i)^4 = 1$ $\therefore O(i) = 4$

$O(-i)$:- $(-i)^4 = 1$ $\therefore O(-i) = 4$.

* Remarks :- (i) $O(a) = 1$ iff $a = e$.

(ii) If G is an infinite cyclic group then $O(a)$ is infinite, $\forall\, a \in G$ $(a \neq e)$.

(3) If G is commutative group then $(ab)^n = a^n b^n$ $\forall n \in N$.

(4) If $(n, m) = 1$, $n/lcm \Rightarrow n/k$

(5) If $(n, m) = 1$, n/k, $m/k \Rightarrow nm/k$

(33) Let G be a group and $a, b \in G$ ∋ $ab = ba$ if $o(a) = n$, $o(b) = m$ and m, n are relative prime then prove that $o(ab) = mn$

OR

Let G be any abelian group then p.t $o(ab) = o(a) \cdot o(b)$ if $(o(a), o(b)) = 1$, where $a, b \in G$.

proof:-

If $o(ab) = k$ then k is the least +ve integer ∋ $(ab)^k = e$ — (*)

Let $o(a) = n$ and $o(b) = m$

Now, $(ab)^{mn} = a^{mn} b^{mn}$ ($\because ab = ba$

$= (a^n)^m (b^m)^n$

$= e^m \cdot e^n$ ($\because o(a) = n, o(b) =$

$= e$

Thus $o(ab) = k$ and $(ab)^{mn} = e$

$\Rightarrow \boxed{k \leq mn}$ — (A)

also $(ab)^k = e$

$\Rightarrow a^k b^k = e$

$\Rightarrow a^k b^k b^{-k} = e b^{-k}$

$\Rightarrow a^k = b^{-k}$

$\Rightarrow (a^k)^m = (b^{-k})^m$

$\Rightarrow a^{km} = (b^m)^{-k}$

$\Rightarrow a^{km} = e$ ($\because b^m = e$

Now $o(a) = n$ & $a^{km} = e$

$\Rightarrow n / km$

$\Rightarrow n / k$ ($\because (n, m) = 1$

— (**)

Similarly

Thus n/k, m/k & $(m,n)=1$

$\Rightarrow mn/k$

$\Rightarrow \boxed{mn \leq k}$ — (B)

from eq^{n} (A) & (B)

$\boxed{k = mn}$

Hence $o(ab) = mn = o(a)\,o(b)$

* Right coset and left coset of subgroup.

Let H be any subgroup of group G.
For any $a \in G$, the set,

(i) $Ha = \{ha / h \in H\}$ is called right coset of H in G.

(ii) $aH = \{ah / h \in H\}$ is called left coset of H in G.

* Remark:-

(i) If G is commutative then $Ha = aH$

proof:- $x \in Ha \Rightarrow x = ha = ah \in aH \Rightarrow Ha \subset aH$

$y \in aH \Rightarrow y = ah = ha \in Ha \Rightarrow aH \subset Ha$

Thus, $Ha = aH$.

(ii) If H is subgroup of group $(G,+)$ then

(1) $H+a = \{h+a / h \in H\}$ (right coset)

(2) $a+H = \{a+h / h \in H\}$ (left coset)

* Find all cosets of $4\mathbb{Z}$ in $\mathbb{Z}$.

Sol^n:- Let $H = 4\mathbb{Z}$, $G = \mathbb{Z}$

Thus $(G, +)$ is group, also it is commutative.

first we find all right cosets.

Here, $H = 4\mathbb{Z} = \{4n / n \in \mathbb{Z}\}$

$H+0 = \{4n+0 / n \in \mathbb{Z}\} = \{4n / n \in \mathbb{Z}\} = H$

$H+1 = \{4n+1 / n \in \mathbb{Z}\}$

$H+2 = \{4n+2 / n \in \mathbb{Z}\}$

$H+3 = \{4n+3 / n \in \mathbb{Z}\}$

$H+4 = \{4n+4 / n \in \mathbb{Z}\} = \{4(n+1) / n \in \mathbb{Z}\}$

$= 4\mathbb{Z} = H$

$H+5 = H+4+1 = H+1$

⋮

also,

$H-1 = \{4n-1 / n \in \mathbb{Z}\}$

$= \{4(n-1)+3 / n \in \mathbb{Z}\} = H+3$

$H-2 = H+2$

$H-3 = H+1$

⋮

Thus $H = 4\mathbb{Z}$ has four distinct right cosets say $H, H+1, H+2, H+3$.

Here G is commutative group.

$\therefore 0+H = H+0 = H$

$1+H = H+1$

$2+H = H+2$

$3+H = H+3$

Date: / /

* Find all cosets of $-3\mathbb{Z}$ in $\mathbb{Z}$.

Sol :-

Let $H = -3\mathbb{Z}$, $G = \mathbb{Z}$

Thus $(G,+)$ is group, also it is commutative

first we find all right cosets.

Here $H = -3\mathbb{Z} = \{-3n / n \in \mathbb{Z}\}$

$H+0 = \{-3n / n \in \mathbb{Z}\} = H$

$H+1 = \{-3n+1 / n \in \mathbb{Z}\} = H+1$

$H+2 = \{-3n+2 / n \in \mathbb{Z}\} = H+2$

$H+3 = \{-3n+3 / n \in \mathbb{Z}\}$

$= \{-3(n-1) / n \in \mathbb{Z}\} = H$

$H+4 = \{-3n+4 / n \in \mathbb{Z}\}$

$= H+3+1 = H+1$

⋮

also,

$H-1 = \{-3n-1 / n \in \mathbb{Z}\}$

$= \{-3n-3+2 / n \in \mathbb{Z}\}$

$= \{-3(n+1)+2 / n \in \mathbb{Z}\}$

$= H+2$

$H-2 = H+1$

⋮

Thus $H = 4\mathbb{Z}$ has three distinct right cosets say $H, H+1, H+2$.

$H = \{0, \pm 1\}$, $G = \{\pm 1, \pm i\}$ Date: 17

Here G is commutative group.

$\therefore 0 + H = H + 0 = H$

$1 + H = H + 1$

$2 + H = H + 2$

$3 + H = H + 3$

(34) Let H be a subgroup of group G then prove that G is union of all left cosets of H in G. also prove that two distinct left cosets of H in G are disjoint.

proof:-

We know that every left coset of H in G is subset of G.

i.e $aH \subset G$, $\forall a \in G$ then

$$\bigcup_{a \in G} (aH) \subset G$$

Now we p.t $G \subset \bigcup_{a \in G} (aH)$

for any $x \in G$, we can write

$x = xe \in xH \subset \bigcup_{a \in G} (aH)$.

Thus $G \subset \bigcup_{a \in G} (aH)$

Hence $G = \bigcup_{a \in G} (aH)$.

Let aH & bH be any two distinct left cosets of H in G. then we have to p.t $aH \cap bH = \phi$

suppose $aH \cap bH \neq \phi$ then

$\exists\ x \in aH \cap bH$

$\therefore x \in aH$ & $x \in bH$

$\Rightarrow x = ah_1$, $x = bh_2$, for some $h_1, h_2 \in H$.

$\Rightarrow a = xh_1^{-1}$

for any $y \in aH$ then $y = ah_3$ for some $h_3 \in H$

$\therefore y = xh_1^{-1}h_3$

$\Rightarrow y = (bh_2)h_1^{-1}h_3 \in bH$

$\Rightarrow y \in bH$.

Thus $aH \subset bH$

Similarly we can p.t $bH \subset aH$

Thus we get $aH = bH$ ※

because aH & bH are distinct

Hence $aH \cap bH = \emptyset$.

(35) Let H be any subgroup of group G then p.t. G is union of all right cosets of H in G also p.t. two distinct ~~left~~ right cosets of H in G are disjoint.

proof:-

x [we know that every subgroup of group of is subset of group] x

we know that every right coset is subset of H in G is subset of G

i.e $Ha \subset G$, $\forall a \in G$ then

$\bigcup_{a \in G} (Ha) \subset G$

Now we p.t. $G \subset \bigcup_{a \in G} (Ha)$

for any $x \in G$, we can write,

$x = ex \in Hax \subset \bigcup_{a \in G} Ha$

Thus $G \subset \bigcup_{a \in G} Ha$

Hence $G = \bigcup_{a \in G} Ha$

Let Ha & Hb be any two distinct right cosets of H in G. Then we have to p.t. $Ha \cap Hb = \emptyset$

Suppose $Ha \cap Hb \neq \emptyset$ then

$\exists\ x \in Ha \cap Hb$

$\Rightarrow x \in Ha$ & $x \in Hb$

$\Rightarrow x = h_1 a$, $x = h_2 b$, for some $h_1, h_2 \in H$

$\Rightarrow a = h_1^{-1} x$.

for any $y \in Ha$ then $y = h_3 a$, for some $h_3 \in H$.

$\therefore y = h_3 h_1^{-1} x$

$= h_3 h_1^{-1} (h_2 b)$

$\in Hb$

$\Rightarrow y \in Hb$

Thus $Ha \subset Hb$

Similarly we can p.t $Hb \subset Ha$

Thus we get $Ha = Hb$ ✱

because Ha & Hb are distinct

(36) P.T. any two left (right) cosets of H in G have same number of elements

proof:-

Let aH and bH be any two left cosets of H in G. Then we have to p.t $O(aH) = O(bH)$

It is sufficient to p.t aH & bH are in one-one correspondance

i.e we have to p.t

$\exists\ f: aH \to bH \ni f$ is one-one & onto.

Let $f: aH \to bH$ be defined by

$f(ah) = bh \quad \forall\ ah \in aH$

first we p.t f is one-one

for any $ah_1, ah_2 \in aH$

$f(ah_1) = f(ah_2)$

$\Rightarrow bh_1 = bh_2$

$\Rightarrow h_1 = h_2$ (by L.C.L)

$\Rightarrow ah_1 = ah_2$

Thus f is one-one

Now we p.t f is onto.

for any $y \in bH$ then $y = bh$ for some $h \in H$

~~Then~~ let $x = ah \in aH$ then

$f(x) = f(ah) = bh = y$

Hence, aH & bH have same no. of elements.

(31) State and prove Lagrange's theorem ▷ Let G be a finite group and H be a subgroup of G then p.t. $O(H)/O(G)$

OR

P.T. the no. of distinct left coset of H in G is $\frac{O(G)}{O(H)}$, where G is finite group.

proof:- Here we have given that G is finite group.

∴ No. of left coset of H in G is also finite.

Let $a_1H = H, a_2H, a_3H, \ldots a_kH$ be the left cosets of H in G. —(*)

Then by Thm, $G = \bigcup_{i=1}^{k} a_iH$, where a_iH are distinct left cosets. —(*)

also we know that all left cosets have same no. of elements.

$\therefore O(H) = O(a_1H) = O(a_2H) = \ldots = O(a_kH)$

Then by (*)

$O(G) = k \times O(H)$ (∵ all a_iH are mutually disjoint)

$\Rightarrow O(H)/O(G)$ —(**)

also, $\frac{O(G)}{O(H)} = k$ = Total no of distinct left coset of H in G.

Date: / /

(*) Index of subgroup:-
Let H be a subgroup of group G then index of H in G is denoted by (G:H) and defined as

$$(G:H) = \text{no. of distinct left coset of } H \text{ in } G.$$

(38) Let H be any subgroup of group G then prove the following:

(I) $aH = H \Leftrightarrow a \in H$

(II) $aH = bH \Leftrightarrow b^{-1}a \in H$

(III) $Ha = Hb \Leftrightarrow ab^{-1} \in H$

proof:-

(I) first we p.t $aH = H$ then $a \in H$

Now,

$a = ae \in aH = H$ Thus $a \in H$

Conversely. if $a \in H$

for any $x \in aH$ then $x = ah$ for some $h \in H$

$\Rightarrow x \in H$

Thus $aH \subset H$

for any $x \in H$ then

$x = aa^{-1}x$

$= a(a^{-1}x) \in aH$

Thus $H \subset aH$

Thus $aH = H$

Hence

$aH = H \Leftrightarrow a \in H$

(II) If $aH = bH$ then

$b^{-1}aH = b^{-1}bH$

$\Rightarrow b^{-1}aH = eH$

$\Rightarrow b^{-1}aH = H$

$\Rightarrow b^{-1}a \in H$ (by (I))

*converse;-

$b^{-1}a \in H$

$\Rightarrow b^{-1}aH = H$ (by (I))

$\Rightarrow bb^{-1}aH = bH$

$\Rightarrow aH = bH$

Hence,

$aH = bH \Leftrightarrow b^{-1}a \in H$.

(39) Let H be a subgroup of group G then prove that, the number of left coset of H in G is same as the number of right coset of H in G.

proof:-

Let L be the set of all left cosets and R be the set of all right cosets of H in G then

$L = \{aH / a \in G\}$

$R = \{Hb / b \in G\}$

It is sufficient to p.t. L & R are in one-one correspondance.

Define a (1-1) function $f: L \to R$ by

$f(aH) = Ha^{-1}$.

first we p.t. f is well defined

ie we have to p.t.

$a_1H = a_2H$

$\Rightarrow a_2^{-1}a_1H = H$

$\Rightarrow a_2^{-1}a_1 \in H$

$\Rightarrow Ha_2^{-1}a_1 = H.$

$\Rightarrow Ha_2^{-1}a_1a_1^{-1} = Ha_1^{-1}$

$\Rightarrow Ha_2^{-1} = Ha_1^{-1}$

$\Rightarrow f(a_1H) = f(a_2H)$

Thus f is well defined

Now, we p.t. f is one-one

$f(a_1H) = f(a_2H)$

$\Rightarrow Ha_1^{-1} = Ha_2^{-1}$

$\Rightarrow Ha_1^{-1}a_1 = Ha_2^{-1}a_1$

$\Rightarrow Ha_2^{-1}a_1 = H$

$\Rightarrow a_2^{-1}a_1 \in H$

$\Rightarrow a_1H = a_2H$

Thus f is one-one

Now we p.t. f is onto

for any $y \in R$ then $y = Hb$ for some $b \in G$

$\therefore x = b^{-1}H \in L \ni$

$f(x) = f(b^{-1}H) = H(b^{-1})^{-1} = Hb = y$

Hence L & R have same no. of elements. □

* corollary :-

Let G be a finite group of order n and $a \in G$ then p.t. $O(a) / n$ (i.e. $O(a) / O(G)$) also prove $a^n = e$. OR

If G be a finite group then p.t. order of each element 'a' divides order

o(a)/p ⇒ o(a) = p ⇒ G = ⟨a⟩ = is cyclic

proof:- Here G is finite group of order n and a∈G then H is cyclic group generated by a and also H is subgroup of G

$\therefore O(H) = O(a)$ ($\because H = \langle a \rangle$ $H = \{a^0 = e, a^1, a^2, \ldots\}$)

also by Lagrange's thm

$O(H) / O(G)$

$\Rightarrow O(a) / n$

also we know that,

$a^{O(G)} = e$

$\Rightarrow a^n = e.$

Th(6) :-

⇒(■) Let $G = \{\bar{m} \in Z_n / (m,n) = 1\}$ then G is group under multiplication with identity I.

Remark:- This group is called the group of prime residue classes modulo n.

Clearly $O(G) = \phi(n)$

(*) Let G be a group and a, b ∈ G then prove the following.

(i) $(a^{-1})^{-1} = a$

(ii) $(ab)^{-1} = b^{-1}a^{-1}$

proof (i) since G be a group, for any a∈G ∃ $a^{-1} \in G$ ∋

$aa^{-1} = a^{-1}a = e$

$\therefore ax = xa = e$

This inverse of $a = x$

and inverse of $x = a$

$x^{-1} = a$

Date: / /

(ii) We have to p.t
$(ab)^{-1} = b^{-1}a^{-1}$

i.e we have p.t
$(ab)(b^{-1}a^{-1}) = e$.

L.H.S.
$= (ab)(b^{-1}a^{-1})$
$= abb^{-1}a^{-1}$
$= aea^{-1}$
$= aa^{-1}$
$= e$ = R.H.S.

(Q10) Prove that group G is abelian iff $(ab)^2 = a^2b^2$, $\forall a, b \in G$.

proof :-

Necessary →

If G is abelian then
$ab = ba$, $\forall a, b \in G$
we have to prove that,
$(ab)^2 = a^2b^2$.

L.H.S. $= (ab)^2$
$= (ab)(ab)$
$= abba$ | $= aabb$
$= ab^2a$ | $= a^2b^2$
$= aab^2$ | R.H.S (i)
$= a^2b^2$

Sufficient →

If $(ab)^2 = a^2b^2$ then we have to p.t $ab = ba$, $\forall a, b \in G$

Date: 5/10

$(ab)^2 = a^2b^2$

$\Rightarrow ab \cdot ab = a \cdot a \cdot b \cdot b$

$\Rightarrow ba = ab$ (by using L.C.L & R.C.L)

* If G is commutative group then p.t. $(ab)^3 = a^3b^3$. Does the converse hold? verify it.

Soln:- since G is comm.

$ab = ba, \forall a, b.$

Now,

$(ab)^3 = (ab)(ab)(ab) = a(ba)(ba)b$
$= a(ab)(ab)b$
$= abbaab$
$= (aa)(bb)(ab)$
$= aabbab$
$= a^3b^3$

converse need not be true

because,

$(ab)^3 = a^3b^3$

$\Rightarrow ababab = aaabbb$

$\Rightarrow baba = aabb$ (by LCL & RCL)

$\Rightarrow (ba)^2 = a^2b^2$

(Q1) Define generator of a group. If G is cyclic group of prime order n then p.t. every non trivial element of G is a generator of G.

Sol

A group which is generated by some of its element is called cyclic group and these elements are called generators of a group.

We know that, If G is finite group of order n then it has $\phi(n)$ generator.

Here n is prime

$\therefore$ G has $\phi(n) = n-1$ generators.

Since $O(G) = n$

Let $\# G = \{e, a_1, a_2, \ldots, a_{n-1}\}$

clearly $\langle e \rangle \neq G$.

i.e. e is not generator of G.

$\therefore$ All elements other than e are generators of G

Hence, every non trivial element of G is a generator of G

* Define group. Giving all details, give examples of each of abelian group and non abelian group.

Sol :-

* Abelian group :-

(i) $(Z, +)$

for any $a, b \in Z$, then $a+b \in Z$

$\therefore$ Z is a binary operation under addition

also, $a+b = b+a$, $\forall a, b \in Z$

$\therefore$ $(Z, +)$ is abelian

* Non-abelian group:-

$G = \{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} / a,b,c,d \in R, ad-cb \neq 0 \}$

see-ex-(17)

* Define cydic group. Giving all details give ex of each of finite & infinite cydic group.

Sol :-

* Let $G = \{\pm 1, \pm i\}$. then $(G, \cdot)$ is a cydic group generated by $\pm i$.

Thus G is finite cydic group.

~~(ex-10)~~

(proof after Thm-24)

* $(\mathbb{Z}, +)$ is infinite cydic group. generated by ± 1. (prove it)

* Let $(G, \cdot)$ be a group and H be a subset of G show that H is sub-group of G iff H is closed under multiplication.

Sol :-

Here we have to prove that H is subgroup of G iff. $ab \in H, \forall a,b \in H$ where H is finite

see thm-16

** converse :-

H is closed under multiplication

i.e $ab \in H, \forall a,b \in H$

Thus by def. of subgroup.

Date: / /

(42) State and prove Euler's theorem

* Statement:-

If a is relatively prime to n then $a^{\phi(n)} \equiv 1 \pmod{n}$.

proof:-

Here $(a,n)=1$

we know that,

$G = \{\bar{m} \in Z_n / (m,n)=1\}$ is a group with identity $\bar{1}$ and $o(G) = \phi(n)$.

Clearly, $\bar{a} \in G$

We know that,

$\bar{a}^{o(G)} = e$

i.e $\bar{a}^{\phi(n)} = \bar{1}$

$\Rightarrow \bar{a}^{\phi(n)} - \bar{1} = \bar{0}$ in Z_n

$\Rightarrow \bar{a}^{\phi(n)} - \bar{1} = \bar{0}$

$\Rightarrow a^{\phi(n)} - 1 = qn$, for some $q \in Z$

$\Rightarrow n / a^{\phi(n)} - 1$

$\Rightarrow a^{\phi(n)} \equiv 1 \pmod{n}$.

→ Remark:-

$a \equiv r \pmod{n}$

$\Leftrightarrow n / a-r$

$\Leftrightarrow a-r = qn$, for some $q \in Z$

$\Leftrightarrow a = qn+r$, $0 \le r < n$

(Q3) State and prove Fermat's thm ▶

* Statement:-

If p is prime no. and a is any integer then $a^p \equiv a \pmod{p}$ or ~~$a^{p-1} \equiv 1 \pmod{p}$~~

proof:-

case-I :- If p/a then

$$p/a(a^{p-1}-1)$$

$$\Rightarrow p/a^p - a$$

$$\Rightarrow a^p \equiv a \pmod{p}$$

case-II :-

If $p \nmid a$ then

$$(p,a) = 1$$

then by Euler's thm

$$a^{\phi(p)} \equiv 1 \pmod{p}$$

$$\Rightarrow a^{p-1} \equiv 1 \pmod{p}$$

$$\Rightarrow a^p \equiv a \pmod{p}.$$

— x —

** If H is subgroup of G then by def^n

$$a,b \in H,\ a, b \in H$$

i.e. H is closed under multi-

Unit-3 : Group-2

Date : 7/07/07

* **Isomorphic group :-**

Let $(G,*)$ and (G',o) be any two groups. G' is said to be isomorphic to G if $\exists\ f:(G,*)\to(G',o)$ such that f is one-to-one, onto and $f(a_1 * a_2) = f(a_1) \circ f(a_2)\ \forall\ a_1, a_2 \in G$.
(i.e f preserve composition)

It is denoted by $G' \simeq G$.

* **Remarks →**

(i) Mapping $f:(G,*)\to(G',o)$ is said to be isomorphism if f is one-one and it preserve composition.

(ii) If $f:(G,*)\to(G',o)$ is onto isomorphism then $f^{-1}:(G',o)\to(G,*)$ exists and also f^{-1} is onto isomorphism.

Thus, $G' \simeq G \Leftrightarrow G \simeq G'$

(1) Let $G = Z_n$, $G' = \{1, \varepsilon, \varepsilon^2, \varepsilon^3, \cdots, \varepsilon^{n-1}\}$ be the multiplicative group of n^{th} root of unity, where $\varepsilon = e^{2\pi i/n}$. then prove that $G \simeq G'$.

proof :-

Define $f:(G,+)\to(G',\cdot)$ by

$$f(\bar{k}) = \varepsilon^k \quad (= e^{2\pi ki/n})$$

first we prove that f preserves composition i.e.

$$f(\bar{k_1} + \bar{k_2}) = f(\bar{k_1}) \cdot f(\bar{k_2}),\ \forall\ \bar{k_1}, \bar{k_2} \in G \quad \text{---} f$$

$$L.H.S. = f(\overline{k_1 + k_2}) = \varepsilon^{k_1+k_2} = \varepsilon^{k_1} e^{k_2}$$

$$= L(\bar{k_1}) \cdot L(\bar{k_2})$$

Now, we p.t. f is one-one.

$$f(\bar{l}_1) = f(\bar{l}_2)$$
$$\Rightarrow e^{il_1} = e^{il_2}$$
$$\Rightarrow e^{2\pi k_1 i/n} = e^{2\pi l_2 i/n}$$
$$\Rightarrow \frac{2\pi l_1}{n} - \frac{2\pi l_2}{n} = 2\pi k, \text{ for some } k \in \mathbb{Z}.$$

$\left(e^{z_1 i} = e^{z_2 i} \Rightarrow z_1 - z_2 = 2k\pi \text{ for } k \in \mathbb{Z} \right)$

$$\Rightarrow l_1 - l_2 = nk$$
$$\Rightarrow \overline{l_1 - l_2} = \overline{nk} = \bar{n} \cdot \bar{k} = \bar{0}$$
$$\Rightarrow \bar{l}_1 = \bar{l}_2$$

$\#$ Thus f is one-one.

For any $y \in G'$ then $y = s^k$, for some $0 \le k \le n-1$.

also, $\bar{k} \in \mathbb{Z}_n = G$

Let $x = \bar{k} \in G$ then

$$f(x) = f(\bar{k}) = s^k = y$$

Thus f is onto.

Hence, $G \cong G'$.

(2) If G and G' are isomorphic group and G is abelian then p.t. G' is also abelian.

OR

P.T. isomorphic image of commutative group is also commutative.

proof:-

Since $G \cong G'$, $\exists\ f: G \to G'$ ∋ f is one-one and onto. & $f(ab) = f(a)f(b)$, $\forall a, b \in G$.

We have to p.t. G' is abelian
i.e. $x'y' = y'x'$, $\forall\ x', y' \in G'$.

For any $x', y' \in G'$ since f is onto
$\exists\ x \in G, y \in G$ s.t. $f(x) = x'$
$f(y) = y'$.

Now, LHS $= x'y'$
$= f(x) f(y)$
$= f(xy)$ — (by $*$)
$= f(yx)$ ($\because$ G is abelian)
$= f(y) f(x)$
$= y'x' =$ RHS.

Thus G' is commutative
Hence, isomorphic image of commutative group is commutative

(3) Let a mapping $\theta : G \to G'$ be an isomorphism of G onto G'. Let e and e' be the unit elements of G and G' respectively then prove the following:
(I) $\theta(e) = e'$
(II) $\theta(a^{-1}) = \theta(a)^{-1}$, $\forall\ a \in G$.

proof:

(I) clearly, $ee = e$
$\Rightarrow \theta(ee) = \theta(e)$
$\Rightarrow \theta(e) \cdot \theta(e) = \theta(e) = \theta(e) \cdot e'$
($\because$ θ preserve composition)
$\Rightarrow \theta(e) = e'$ (by LCL)

(II) For any $a \in G$ then

$$aa^{-1} = e$$

$$\Rightarrow \theta(aa^{-1}) = \theta(e)$$

$$\Rightarrow \theta(a)\,\theta(a^{-1}) = e'$$

Similarly, $\Rightarrow \theta(a^{-1})\,\theta(a) = e'$

Thus $\theta(a)\,\theta(a^{-1}) = e' = \theta(a^{-1})\,\theta(a)$

$\therefore$ Inverse of $\theta(a)$ is $\theta(a^{-1})$

i.e. $\theta(a)^{-1} = \theta(a^{-1})$.

(4) Prove that, any infinite cyclic group is isomorphic to Z.

proof:-

Let G be any infinite cyclic group (i.e. $G = \langle a \rangle$) generated by a then we have to p.t G is isomorphic to Z i.e. $G \simeq Z$

i.e. $Z \simeq G$.

Define a mapping $f: Z \to G$ by

$$f(n) = a^n, \quad \forall n \in Z$$

First we prove that.

$$f(n_1 + n_2) = f(n_1)\,f(n_2)$$

$$\text{LHS} = f(n_1 + n_2)$$

$$= a^{n_1 + n_2}$$

$$= a^{n_1} \cdot a^{n_2}$$

$$= f(n_1)\,f(n_2) = \text{RHS}.$$

Now we p.t f is one-one

$$f(n_1) = f(n_2) \Rightarrow a^{n_1} = a^{n_2}$$

$$\Rightarrow a^{n_1 - n_2} = e = a^0$$

Thus f is one one

Now we p.t f is onto

For any $y \in G = \langle a \rangle$ then $y = a^n$, for some $n \in \mathbb{Z}$

Let $x = n \in \mathbb{Z}$, then

$$f(x) = f(n) = a^n = y$$

Thus f is onto.

Hence $\boxed{\mathbb{Z} \cong G \text{ i.e } G \cong \mathbb{Z}}$

(5) Prove that, any finite cyclic group of order n is isomorphic to $\mathbb{Z}_n$.

proof:-

Let $G = \langle a \rangle$ be any finite cyclic group of order n. then we have to p.t $G \cong \mathbb{Z}_n$ i.e $\mathbb{Z}_n \cong G$

Define a mapping $f: \mathbb{Z}_n \to G$ by

$$f(\bar{k}) = a^k, \forall \bar{k} \in \mathbb{Z}_n$$

first we p.t

$$f(\bar{k_1} + \bar{k_2}) = f(\bar{k_1}) f(\bar{k_2})$$

$$f(\overline{k_1 + k_2}) = a^{k_1 + k_2}$$
$$= a^{k_1} \cdot a^{k_2}$$
$$= f(\bar{k_1}) f(\bar{k_2})$$

Now, we p.t f is one-one

i.e $f(\bar{k_1}) = f(\bar{k_2})$

$\Rightarrow a^{k_1} = a^{k_2}$

$\Rightarrow a^{k_1 - k_2} = e$ $\Rightarrow n \mid k_1 - k_2$

$\Rightarrow k_1 - k_2 = 0$ $\Rightarrow k_1 - k_2 = nq$

$n \mid k_1 - k_2$

$\Rightarrow k_1 - k_2 = kn$

$\Rightarrow \overline{k_1 - k_2} = \bar{0}$

Thus f is one-one

Now we p.t f is onto

for any $g \in G = \langle a \rangle$ then $g = a^k$ $0 \le k \le n-1$

then $\bar{k} \in Z_n$

let $x = \bar{k} \in Z_n \Rightarrow f(x) = f(\bar{k}) = a^k = g$.

Thus f is onto.

$\therefore Z_n \cong G$ i.e $G \cong Z_n$

(6) corrolary :- Prove that any two cyclic group of same order are isomorphic

proof :-

Let $G = \langle a \rangle$ and $G' = \langle b \rangle$ be any two cyclic group of order n. Then by abo Thm. $G \cong Z_n$ & $G' \cong Z_n$

$\Rightarrow G \cong G'$.

(7) Prove that any noncyclic group of order 4 is isomorphic to Klein 4-group.

proof :-

Let $G = \{e, a, b, c\}$ be any noncyclic group of order 4.

we know that, $o(a) / o(G)$, $o(b) / o(G)$, $o(c) / o(G)$. i.e $o(a)/4$, $o(b)/4$, $o(c)/4$

Now, $o(a)/4$

$\Rightarrow o(a) = 1$ or 2 or 4

If $o(a) = 1$ then $a = e$ ✗

If $o(a) = 4$ then $a^4 = e$ (4 is the least +ve int)

$\therefore G$ is cyclic group ✗

Date: / /

Similarly we can prove that,
$b^2=e$ & $c^2=e$

also G is a group
$\therefore$ • $ab=a$ or b or c

if $ab=a$ then $ab=ae$
$\Rightarrow b=e$ ✱
(by LCL.)

if $ab=b$ then
$ab=eb$
$\Rightarrow a=e$ ✱ (by RCL)

$\therefore ab=c$
By $ba=c$
and $bc=a=cb$
$ae=b=ca$

Hence, G is Klein's 4 group
Hence, any noncyclic group of order 4 is isomorphic to Klein-4 group.

(8) corollary: Any group of order 4 is abelian group.

proof :- * case-I :-
If G is cyclic.
Here $O(G)=4$
$\therefore G \simeq Z_4$ (by thm-5)
we know that Z_4 is commutative
$\therefore$ G is also commutative.
(by thm 2)

* case-2 :

If G is noncyclic then by above thm.
$G \cong$ Klein-4-group.
we know that Klein 4-group is abelian
$\therefore$ G is also abelian.

* Automorphism :-

If $f: G \to G$ is onto isomorphism then f is called an automorphism of G.

(9) Prove that, mapping $f: Z \to Z$ defined by $f(n) = -n, \forall n \in Z$ is an automorphism of Z.

proof :-

First we prove that,

$f(n_1 + n_2) = f(n_1) + f(n_2), \forall n_1, n_2 \in Z.$

$L.H.S. = f(n_1 + n_2)$
$= -(n_1 + n_2)$
$= (-n_1) + (-n_2)$
$= f(n_1) + f(n_2) = R.H.S.$

Now we p.t. f is one-one.

$f(n_1) = f(n_2) \Rightarrow -n_1 = -n_2$
$\Rightarrow n_1 = n_2$

Thus f is one-one.

Now we p.t. f is onto.

for any $y \in Z$ then $x = -y \in Z$.

also $f(x) = f(-y) = -(-y) = y$

Thus, f is onto.

Hence,

f is an automorphism of Z.

Date : / /

(10) Let G be any group

* Identity map :-
Let G be any group then the mapping $I_G : G \to G$ defined by $I_G(x) = x, \forall x \in G$ is called identity map on G.
Clearly I_G is an automorphism on G
It is known as trivial automorphism

(10) Let G be any abelian group then p.t. the mapping $f : G \to G$ defined by $f(a) = a^{-1}, \forall a \in G$ is an automorphism of G.

proof:

First we prove that,

$$f(a_1 a_2) = f(a_1) \cdot f(a_2), \forall a_1, a_2 \in G$$

$$\begin{aligned} \text{L.H.S.} &= f(a_1 a_2) \\ &= (a_1 a_2)^{-1} \\ &= a_2^{-1} a_1^{-1} \quad (\because G \text{ is abelian}) \\ &= a_1^{-1} a_2^{-1} \\ &= f(a_1) \cdot f(a_2) = \text{R.H.S.} \end{aligned}$$

Now we prove that f is one-one

$$\begin{aligned} f(a_1) = f(a_2) &\Rightarrow a_1^{-1} = a_2^{-1} \\ &\Rightarrow (a_1^{-1})^{-1} = (a_2^{-1})^{-1} \\ &\Rightarrow a_1 = a_2 \end{aligned}$$

Thus f is one-one.

Now, we p.t. f is onto.
for any $y \in G$ then $x = y^{-1} \in G$.

also, $f(x) = f(y^{-1}) = (y^{-1})^{-1} = y$

Thus,
f is onto.

Hence given map is an automorphism of G.

(11) Let G be any group and mapping, $f: G \to G$ defined by $f(a) = a^{-1}$, $\forall a \in G$.
Is f automorphism? verify it.

sol^n:- f is not automorphism.
because,

$$f(a_1 a_2) = (a_1 a_2)^{-1}$$
$$= a_2^{-1} a_1^{-1}$$
$$= f(a_2) f(a_1)$$
$$\neq f(a_1) f(a_2).$$

Thus f does not preserve composition

(12) Let G be any group and x any fixed element of G then prove that the mapping $i_x : G \to G$ defined by $i_x(a) = xax^{-1}$ $\forall a \in G$ is an automorphism of G.

proof :-

First we p.t.
$i_x(a_1 a_2) = i_x(a_1)\, i_x(a_2)$, $\forall a_1, a_2 \in G$.

LHS $= i_x(a_1 a_2)$
$= x a_1 a_2 x^{-1}$
$= x a_1 1 x^{-1}$

Date : / /

Now we p.t i_x is one-one

$i_x(a_1) = i_x(a_2)$

$\Rightarrow x a_1 x^{-1} = x a_2 x^{-1}$

$\Rightarrow a_1 = a_2$ (by L.C.L. & R.C.L)

Now we p.t i_x is onto.

for any $y \in G$ then $x_1 = x^{-1}yx \in G$

$f(x_1) = f(x^{-1}yx) = xx^{-1}yxx^{-1} = eye$

$= y$

$\therefore f$ is onto.

Hence, i_x is an automorphism of G

* Inner automorphism :-

Let G be any group and x be any fixed element of G, then mapping $i_x : G \to G$, $i_x(a) = xax^{-1}$, $\forall a \in G$ is called inner automorphism defined by x.

(13) Prove that, group G is abelian iff $i_x = I_G$, $\forall x \in G$.

proof:-

G is abelian $\Leftrightarrow xa = ax$, $\forall x, a \in G$

$\Leftrightarrow xax^{-1} = axx^{-1}$

$\Leftrightarrow xax^{-1} = ae$

$\Leftrightarrow xax^{-1} = a$

$\Leftrightarrow i_x(a) = I_G(a)$, $\forall a \in G$

$\Leftrightarrow i_x = I_G$ Hence proved

Remark: If $f : G \to G'$ is isomorphism & $G = \langle a \rangle$ then $G' = \langle f(a) \rangle$

(14) Prove that, every infinite cyclic group has only one non trivial automorphism

proof:-

Let G be any infinite cyclic group then

$G \cong Z$ (Z has ↑)

∴ It is sufficient to p.t. only one non trivial automorphism.

Let $f: Z \to Z$ be any automorphism of Z

we know that,

$Z = \langle 1 \rangle$ & f is auto morphism

$\therefore Z = \langle f(1) \rangle$ i.e. f(1) is generator of Z.

but we know that,

generators of Z are ±1 only.

$\therefore f(1) = \pm 1$

If $f(1) = 1$ then we p.t. $f(n) = n$, $\forall n \in Z$.

for $n \in N$,

$f(n) = f(1+1+1 \dots (n \text{ times}))$

$= f(1) + f(1) + f(1) + \dots (n\text{-times})$

(∵ f is automor.

$= n f(1)$

$= n \cdot 1$

$= n$

Thus $f(n) = n$, $\forall n \in N$.

for -ve integer n, let $n = -m$ for some $m \in N$.

then, $f(n) = f(-m)$

$= -f(m)$ (∵ f is automor

$= -m$ (∵ $m \in N$

$= n$

also, clearly $f(0)=0$ ($\because f$ is auto.)

Thus,

$f(n)=n$, $\forall n\in Z$, if $f(1)=1$

$\Rightarrow f$ is identity mapping of Z.

i.e $f=I_Z$

i.e f is trivial automorphism of Z, if $f(1)=1$

If $f(1)=-1$ then we can easily p.t. $f(n)=-n$, $\forall n\in Z$ which is non identity map.

Thus $f(n)=-n$ is non trivial automorphism of Z.

Hence Z has only one non trivial automorphism.

i.e G has only one non-trivial automorphism

(15) Let $G=\langle a\rangle$ be any finite cyclic group of order n then p.t. the mapping $f: G\to G$ defined by $f(a)=a^m$, $\forall a\in G$ is an automorphism of G iff $(m,n)=1$

proof:-

Here $G=\langle a\rangle$ is cyclic group and $o(G)=n$

If $f: G\to G$ defined by $f(a)=a^m$, $\forall a\in G$ is an automorphic of a then $G=\langle f(a)\rangle$.

($\because G=\langle a\rangle$ & f is auto.)

we know that every finite cyclic group of order n has $\phi(n)$ generators.

∴ Given group G has $\phi(n)$ generators.

∴ Any automorphism f of G is of the form $f(a) = a^m$, where $(m,n) = 1$.

→ converse part :-

If $(m,n) = 1$ then we have to p.t. $f: G \to G$ defined by $f(a) = a^m, \forall a \in G$ is an automorphism of G.

first we p.t. $f(xy) = f(x)f(y), \forall x, y \in G$

for any $x, y \in G$ then $x = a^i$, $y = a^j$. for some $i, j \in \mathbb{Z}$

$$\begin{aligned} \text{LHS} = f(xy) &= f(a^i a^j) \\ &= (a^i a^j)^m \\ &= a^{im} \cdot a^{jm} \\ &= f(a^i) f(a^j) \\ &= f(x) f(y). \end{aligned}$$

Now we p.t. f is one-one

$$\begin{aligned} & f(x) = f(y) \\ \Rightarrow\ & f(a^i) = f(a^j) \\ \Rightarrow\ & (a^i)^m = (a^j)^m \\ \Rightarrow\ & a^{im} = a^{jm} \\ \Rightarrow\ & a^{(i-j)m} = e \\ \Rightarrow\ & n \mid (i-j)m \quad (\because o(G) = n \\ \Rightarrow\ & n \mid i-j \quad (\because (m,n) = 1 \\ \Rightarrow\ & i - j = kn, \text{ for some } k \in \mathbb{Z} \\ \Rightarrow\ & a^{i-j} = a^{kn} = (a^n)^k \quad \text{K} \end{aligned}$$

$\Rightarrow a^{i-j} = e$

$\Rightarrow a^i = a^j$

$\Rightarrow x = y$

Thus f is one-one

Now we p.t. f is onto.

for any $y \in G$ then $y = a^i$ for some $i \in \mathbb{Z}$.

since $(m,n) = 1$,

$\exists \ \lambda, \mu \in \mathbb{Z} \ni \lambda m + \mu n = 1$

Now,

$$y = a^i = a^{i1}$$
$$= a^{i(\lambda m + \mu n)}$$
$$= a^{i\lambda m} \cdot a^{i\mu n}$$
$$= (a^{i\lambda})^m \cdot (a^n)^{i\mu}$$
$$= (a^{i\lambda})^m \cdot e \quad (\because a^n = e$$
$$= (a^{i\lambda})^m$$
$$= f(a^{i\lambda})$$
$$= f(x), \text{ where } x = a^{i\lambda} \in G$$

Thus f is onto

Hence f is an automorphism

* **Homomorphism :-**

Let G and G' be any groups. A mapping $f: G \to G'$ is said to be a homomorphism (group homomorphism) if

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

* **Remarks :-**

(1) Every isomorphism is homomorphism

(2) " automorphism of G is also

(16) Let $G = Z$, $G' = \{\pm 1\}$ be any groups then prove that, the mapping $f: G \to G'$ defined by

$$f(n) = \begin{cases} 1 & , \text{if } n \text{ is even} \\ -1 & , \text{" " " odd} \end{cases}$$

is a homomorphism.

Is it one-one? Is it onto?

Soln:-

First we prove that,

$$f(m+n) = f(m) \cdot f(n)$$

for any $m, n \in G$

if m & n both are even then $m+n$ is also even.

$$\therefore f(m+n) = 1 = 1 \cdot 1 = f(m) \cdot f(n)$$

if m & n both are odd then $m+n$ is also even

$$\therefore f(m+n) = 1 = (-1)(-1) = f(m) f(n).$$

if m is odd and n is even then $m+n$ is odd

$$\therefore f(m+n) = -1 = (-1)(1) = f(m) f(n).$$

if m is even and n is odd then $m+n$ is odd

$$\therefore f(m+n) = -1 = (1)(-1) = f(m) f(n)$$

Thus,

$$f(m+n) = f(m) f(n), \quad \forall\ m, n \in G$$

Hence, f is homomorphism.

It is not one-one because

$$f(2) = 1 = f(4) \quad \text{but } 2 \neq 4.$$

Date : / /

Clearly, f is onto because for any $y \in G'$, $\exists\, x \in G \ni f(x) = y$

(17) Give an example of function which is group homomorphism but non-isomorphism.

ex-16

(18) Define a mapping $f: R \to R^+$ by $f(a) = 2^a$, $\forall\, a \in R$

Is f homomorphism, one-one, onto, automorphism, isomorphism?

Sol:

Here $(R, +)$ & $(R^+, \cdot)$ are groups.

first we check that,

$f(a+b) = f(a) f(b)$, $\forall\, a, b \in R$

$f(a+b) = 2^{a+b}$

$= 2^a \cdot 2^b$

$= f(a) f(b)$

$\therefore f$ is homomorphism

for one-one →

$f(a) = f(b)$

$\Rightarrow 2^a = 2^b$

$\Rightarrow a = b$

f is one-one

for onto →

Sol:

For any $y \in R^+$

then $x = \log_2 y \in R$

Also $f(x) = 2^x$

$= 2^{\log_2 y}$

$= y$

for $y \in R^+$ we know that $2^x \neq y$, $\forall\, x \in R$.

Thus $\nexists\, x \in R \ni f(x) = y$

∴ It is onto.
It is isomorphism
It is not automorphism
because $R \neq R'$.

(19) Define $f: Z \to Z_n$ by $f(a) = \bar{a}$, $\forall a \in Z$.
Is f homomorphism, one-one, onto, isomorphism, automorphism?

Soln:-

first we check $f(a+b) = f(a) + f(b)$

$$f(a+b) = \overline{a+b}$$
$$= \bar{a} + \bar{b}$$
$$= f(a) + f(b)$$

for one-one →
Here $f(n) = \bar{n} = \bar{0}$.
$f(2n) = \overline{2n} = \bar{0}$.
$f(n) = f(2n)$
but $n \neq 2n$
∴ f is not one-one

for onto →
any $\bar{y} \in Z_n$ then $0 \leq y \leq n-1$

for $y \in Z$, also $f(y) = \bar{y}$.

Thus f is onto.
f is not isomorphism & automorphism.

Date : / /

(20) P.T. a mapping $f: G \to G'$ defined by $f(a) = e', \forall a \in G$ is a group homo. (trivial homo.).

proof:- we have to P.T,

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

$$L.H.S. = f(ab) = e'$$
$$= e'.e'$$
$$= f(a)f(b)$$

Thus f is homo.

(21) P.T. mapping $f: G \to G$ defined by $f(a) = a, \forall a \in G$ is a homomorphism (identity homo.) and denoted by I_G

Sol:-

$$f(ab) = ab$$
$$= f(a)f(b)$$

Thus f is homo.

(22) P.T. homomorphic image of abelian group is also abelian

proof:-

Let $f: G \to G'$ be any homomorphism of G onto G'

If G is abelian then we have to p.t G' is abelian

i.e we have to p.t $x'y' = y'x', \forall x', y' \in G'$

for any

$x', y' \in G'$,

since $f: G \to G'$ is onto. $\exists\ x, y \in G \to$

$f(x) = x'$ & $f(y) = y'$

Now,
LHS = $x'y' = f(x)f(y)$
$= f(xy)$ ($\because$ G is homo.)
$= f(yx)$ ($\because$ G is abelian
$= f(y)f(x)$
$= y' \cdot x' =$ RHS.

(23) Let $f: G \to G'$ be any homomorphism then prove the following:
(I) $f(e) = e'$
(II) $f(a^{-1}) = f(a)^{-1}$, $\forall\ a \in G$.

proof (I) :- we have,
$ee = e$
$\Rightarrow f(ee) = f(e)$
$\Rightarrow f(e)f(e) = f(e) \cdot e'$ ($\because$ f preserve composition
$\Rightarrow f(e) = e'$ (by L.C.L)

(II) for any $a \in G$ then
$aa^{-1} = e$
$\Rightarrow f(aa^{-1}) = f(e)$
$\Rightarrow f(a)f(a^{-1}) = e'$
Ily $\Rightarrow f(a^{-1})f(a) = e'$

Thus $f(a)f(a^{-1}) = e' = f(a^{-1})f(a)$
Thus inverse of $f(a) = f(a^{-1})$
i.e $f(a^{-1}) = f(a)^{-1}$.

(24) Homomorphic image of cyclic group is also cyclic OR
Let $f: G \to G'$ be group homo. of G onto

Date : / /

proof:- Let $G = \langle a \rangle$ be any cyclic group. $f: G \to G'$ be onto homo. Then we have to p.t G' is also cyclic

i.e

first we p.t $G' = \langle f(a) \rangle$

clearly

$\langle f(a) \rangle \subset G'$ $(\because f(a) \in G')$

Now we p.t $G' \subset \langle f(a) \rangle$

for any $b' \in G'$,

Since $f: G \to G'$ is onto $\exists$ $b \in G$ s

$f(b) = b'$.

$b \in G$ & $G = \langle a \rangle$

$\therefore b \in \langle a \rangle$

$\therefore b = a^i$, for some $i \in Z$

Now, $f(b) = b'$

$\Rightarrow b' = f(a^i)$

$= f(a)^i$ $(\because f$ is homo

$\in \langle f(a) \rangle$

$\Rightarrow b' \in \langle f(a) \rangle$

Thus,

$G' \subset \langle \langle f(a) \rangle$

Hence

$G' = \langle f(a) \rangle$

ie G' is cyclic.

* **Kernal of homomorphism:-**

Let $f: G \to G'$ be any group homomorphism then the kernal of f is denoted by $\ker f$ and defined as

$$\ker f = \{a \in G / f(a) = e'\}$$

(25) Prove that, $\ker f$ is a subgroup of group.

proof:- Let $f: G \to G'$ be any homomorphism and $\ker f = \{a \in G / f(a) = e'\}$.

clearly, $\ker f \subset G$ & $f(e) = e'$

$\therefore e \in \ker f$

$\therefore \ker f \neq \emptyset$.

Now we have to p.t.,

$ab^{-1} \in \ker f$, $\forall a, b \in \ker f$.

i.e. $f(ab^{-1}) = e'$, $\forall a, b \in \ker f$.

L.H.S. $= f(ab^{-1})$

$= f(a) f(b^{-1})$ ($\because f$ is homo.

$= f(a) f(b)^{-1}$ ("

$= e' \cdot (e')^{-1}$ ($\because a, b \in \ker f$, $f(a) = e' = f(b)$

$= e'$

$=$ R.H.S.

(26) P.T. a homomorphism f is one-one iff $\ker f = \{e\}$.

proof:-

Let $f: G \to G'$ be any homomorphism

If f is one-one then we have

Date : / /

for any $a \in \ker f$ then $f(a) = e'$

$\Rightarrow f(a) = f(e)$

$(\because f$ is homo.

$\Rightarrow a = e$ $(\because f$ is one-one

Thus, $\ker f = \{e\}$.

* converse part:-

If $\ker f = \{e\}$ then p.t. f is one-one.

Now $f(a) = f(b)$

$\Rightarrow f(a) f(b)^{-1} = e'$ $(\because f$ is homo)

$\Rightarrow f(ab^{-1}) = e'$ $(\because$ "

$\Rightarrow ab^{-1} \in \ker f = \{e\}$

$\Rightarrow ab^{-1} = e$

$\Rightarrow a = b$.

* Normal subgroup :-

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

i.e. $xHx^{-1} \subset H$, $\forall x \in G$.

(21) Prove that kernal of group homomorphism is a normal subgroup of group.

proof :- Let $f : G \to G'$ be any homomorphism and $\ker f = \{a \in G \mid f(a) = e'\}$.

first we p.t $\ker f$ is subgroup of G (Thm - 25).

Now we prove that

$xax^{-1} \in \ker f$, $\forall x \in G$, $a \in \ker f$.

i.e $f(xax^{-1}) = e'$, $\forall x \in G$, $a \in \ker f$

$(\because f(a) = e')$

$LHS = f(xax^{-1})$

$= f(x) f(a) f(x^{-1})$

$= f(x)\, e'\, f(x)^{-1}$ $(\because f$ is homo.)

$= f(x) f(x)^{-1}$

$= e' = RHS$.

Thus $\ker f$ is normal subgroup of G

(28) If G is abelian group then prove that every subgroup of [abelian] G is normal subgroup.

OR

P.T. every subgroup of abelian group is normal subgroup.

proof:-

Let H be any subgroup of Group G and G be abelian

We have to prove that H is normal

i.e. $xax^{-1} \in H$, $\forall x \in G$, $a \in H$.

for any $x \in G$, $a \in H$ then

$xax^{-1} = xx^{-1}a$ $(\because G$ is abelian

$= ea$

$= a \in H$

H is normal.

Date : / /

* Remarks:-

(1) Every group G has atleast two normal groups say ($\{e\}$, G itself)

proof:-

Let G be any group.

clearly $e \in G \Rightarrow \{e\}$ s.g. of G

for any $x \in G$

Now, $xex^{-1} = xx^{-1}$

$= e \in \{e\}$

$\therefore \{e\}$ is normal group.

clearly G is s.g. of G

also $xax^{-1} \in G$ for any $x, a \in G$

$\therefore$ G is normal s.g. of G

(2) Normal subgroup $\{e\}$ is called trivial normal s.g. of G

(3) Normal s.g. G of G is called improper normal s.g. of G and others are called proper normal s.g. of G

* Simple group:-

Group G is said to be simple group if its normal s.g. are $\{e\}$ & G itself

(29) Prove that every cyclic group of order p, where p is prime is a simple group.

proof :-

Let $G = \langle a \rangle$ be any cyclic group of order p, where p is prime

Let H be any subgroup of G then by Lagrange's thm, we say that

$$o(H) / o(G)$$

$$\Rightarrow o(H) / p$$

$$\Rightarrow o(H) = 1 \quad \text{or} \quad o(H) = p$$

($\because$ p is prime)

$$\Rightarrow H = \{e\} \text{ or } H = G.$$

clearly $\{e\}$ & G both are normal subgroup of G

$\therefore$ G is simple group.

(30) prove that, a subgroup H of group G is normal in G iff $xH = Hx$, $\forall x \in G$

proof :-

Let H be any normal s.g. of group G.

then by def^n. $xax^{-1} \in H$, $\forall x \in G$, $a \in H$.

$$\Rightarrow xHx^{-1} \subset H, \quad \forall x \in G$$

$$\Rightarrow xH \subset Hx, \quad \forall x \in G \quad -(*)$$

Date : / /

Replacing x by x^{-1} in (*) we get

$$x^{-1}Hx \subset H$$
$$\Rightarrow x(x^{-1}Hx)x \subset x(Hx^{-1})x$$
$$\Rightarrow Hx \subset xH \quad -(**)$$
$$\forall x \in G$$

By (*) & (**), we say that

$$xH = Hx, \forall x \in G$$

→ Converse part :-

If $xH = Hx, \forall x \in G$ then
$xHx^{-1} = H, \forall x \in G$.

for any $x \in G$, $a \in H$,

$$xax^{-1} \in xHx^{-1} = H$$
$$\Rightarrow xax^{-1} \in H$$

Thus H is normal subgroup of G.

(31) Prove that, a subgroup H of group G is normal in G iff every left coset of H in G is a right coset of H in G

proof :-

Let H is normal subgroup of G then by above thm,

$$xH = Hx$$

Thus every left coset of H in G is a right coset of H in G

→ converse part:-

If every left coset of H in G is a right coset of H in G.

Let xH be any left coset of H in G then

$$xH = Hy \text{ , for some } y \in G.$$

We know that $x = xe \in xH = Hy$

$\therefore x \in Hy$

$\Rightarrow Hx = Hy$ ($\because a \in Hb \Leftrightarrow Ha = Hb$, prove it)

$\Rightarrow Hx = xH$ ($\because Hy = xH$)

$\Rightarrow xHx^{-1} = H$, $\forall x \in G$

$\Rightarrow$ H is normal

~~for any~~

$\Rightarrow HxCHHy$

$\Rightarrow HxCHy$

$x \in Hy$ then y

$\Rightarrow x = ex \in Hx$

$\Rightarrow HyCHx$

(32) Let H be any subgroup of group G then p.t. following are equivalent:

(i) H is normal in G.

(ii) $Hx = xH$, $\forall x \in G$.

(iii) every left coset of H in G is a right coset of H in G.

proof:-

(*) (i) $\Leftrightarrow$ (ii) $\Leftrightarrow$ (iii)

or (i) $\Rightarrow$ (ii) $\Rightarrow$ (iii) $\Rightarrow$ (i)

(*) Thm-30 & Thm-31 (converse).
(not converse)

Date: / /

(33) Let G be any group consider the set

$S = \{aba^{-1}b^{-1} / a, b \in G\}$,

$K = \{s_1 \cdot s_2 \cdots s_m / s_i \in S, \forall i = 1, 2, \ldots, m\}$

then prove that K is normal subgroup of G

proof :-

First we prove that, K is subgroup of G

Clearly $K \subset G$ and $e \in K$

Now we p.t $xy^{-1} \in K$, $\forall x, y \in K$.

for any $x, y \in K$ then

$x = s_1 \cdot s_2 \cdots s_n$

$y = s_1' \cdot s_2' \cdots s_p'$.

for some, $s_1, s_2, \ldots, s_n$,

$s_1', s_2', \ldots s_p' \in S$.

$\therefore y^{-1} = s_p'^{-1} \cdot s_{p-1}'^{-1} \cdots s_2'^{-1} \cdot s_1'^{-1}$.

$(\forall s_i'^{-1} \in S$

also,

$xy^{-1} = s_1 \cdot s_2 \cdots s_p'^{-1} \cdot s_{p-1}'^{-1} \cdots s_1^{-1}$

$\therefore xy^{-1} \in K$ (∵ It is finite product of elements of S.

Now we p.t K is normal subgroup of G

i.e p.t $xax^{-1} \in K$, for $a \in K$, $x \in G$

we can write

$xax^{-1} = xax^{-1}a^{-1}a \in K$

(∵ $xax^{-1}a^{-1} \in S$ & $a \in K$)

$\therefore a = s_1 \cdot s_2 \cdots s_n$

Hence K is normal in G

* Commutator subgroup of G:-
Let G be a group then the subgroup of G whose elements are finite product of the elements of the form $aba^{-1}b^{-1}$, $a,b \in G$ is called commutator subgroup of G

* Remark:-
Let G be a group and $S = \{aba^{-1}b^{-1} / a,b \in G\}$ then the set $G' = \{s_1 \cdot s_2 \cdots s_m / s_i \in S\}$ is called commutator subgroup of G.

(34) Prove that commutator subgroup of group G is a normal subgroup of G
Theorem (33)

(34) Prove that group G is abelian iff the commutator subgroup of G is trivial OR
Under which condition commutator subgroup of group is trivial? verify your answer.

proof:-
If group G is abelian
Let G' be the commutator subgroup of G then we have to prove that $G' = \{e\}$
for any $x \in G'$ then $x = s_1 \cdot s_2 \cdots s_n$,
for some $s_i = a_i b_i a_i^{-1} \cdot b_i^{-1}$,
$a_i, b_i \in G$, $i = 1, 2, \ldots$
Since, G is abelian,
all $s_i = a_i a_i^{-1} b_i b_i^{-1} = e$
$x = e \cdot e \cdots e = e$

Date : / /

Hence G' is trivial subgroup.

* Converse part :-

If G' is trivial subgroup then

$G' = \{e\}$.

Clearly $aba^{-1}b^{-1} \in G'$, $\forall a, b \in G$

$\Rightarrow aba^{-1}b^{-1} \in \{e\}$

$\Rightarrow aba^{-1}b^{-1} = e$

$\Rightarrow aba^{-1}b^{-1}b = eb$

$\Rightarrow aba^{-1} = b$

$\Rightarrow ab = ba$, $\forall a, b \in G$

Hence G is abelian

(35) Let H be a normal subgroup of group G then the set of all left cosets of H in G forms a group under the operation $aHbH = abH$, $\forall a, b \in G$

proof :-

$L = \{aH / a \in G\}$ be the set of all left cosets of H in G then we have to p.t L is a group.

Clearly, $aH \cdot bH = abH \in L$, $\forall a, b \in G$

$\therefore$ Given operation is binary operation

* Associative prop. :-

$(aHbH)cH = aH(bHcH)$

LHS $= (aHbH)cH$

$= abHcH$

$= abcH)$

$= aHbcH$

Date : / /

(36) State and prove 1st isomorphism theorem.

statement :-

Let $f: G \to G'$ be any group homomorphism of G onto G' and $K = \ker f$ then K is normal subgroup of G and $G/K \cong G'$.

proof :-

Clearly $K = \ker f$ is subgroup of G

Now, we p.t K is normal in G

i.e p.t $xax^{-1} \in K, \forall x \in G, a \in K$

i.e $f(xax^{-1}) = e'$

LHS $= f(xax^{-1})$

$= f(x) f(a) f(x^{-1})$ ($\because f$ is homo.

$= f(x) e' f(x)^{-1}$ ($\because$

$= f(x) f(x)^{-1}$

$= e'$

$=$ RHS

Thus f is normal

Now,

we p.t $G/K \cong G'$

Define a function $\phi: G/K \to G'$ by

$\phi(ak) = f(a), \forall ak \in G/K$.

First we prove that

ϕ is well defined

for any $ak = bk$

$\Leftrightarrow a^{-1}b \in K = \ker f$

$\Leftrightarrow f(a^{-1}b) = e'$

$\Leftrightarrow f(a^{-1}) f(b) = e'$ ($\because$ f is homo.

Date: 7/17/25

* Identity prop.:-
for any $aH \in L$ then $H = eH \in L$

also $aH \cdot H = aH \cdot eH$
$= aeH = aH$

Similarly $H \cdot aH = aH$
Thus H is identity.

* Inverse prop.:-
for $aH \in L$ then $a \in G \therefore a^{-1} \in G$
and $a^{-1}H \in L$
also, $aHa^{-1}H$
$= aa^{-1}H = eH = H$
Similarly, $a^{-1}HaH = a^{-1}aH = eH = H$
Thus inverse of aH is $a^{-1}H$
Hence, L is a group.

* Quotient group:-
Let H be any normal subgroup of group G then the set of all left cosets (or right cosets) of H in G is called the quotient group of G by H. It is denoted by G/H. (G/H G quotient H)

By def^n we say that $G/H = L$
$= \{aH / a \in G\}$
and operation in G/H is defined by $aHbH = abH, \forall a, b \in G$

$\Leftrightarrow f(a)^{-1} f(b) = e'$

$\Leftrightarrow f(b) = f(a)$

$\Leftrightarrow f(a) = f(b)$

$\Leftrightarrow \phi(ak) = \phi(bk)$

Thus, ϕ is well defined and one-one

Now we p.t ϕ is onto.

for any $y \in G'$, since $f: G \to G'$ is onto,

$\exists\ x \in G \ni f(x) = y$.

Now, $xK \in G/K$ &

$\phi(xK) = f(x) = y$

Now, we p.t.

$\phi(aK \cdot bK) = \phi(aK) \cdot \phi(bK)$,

$\forall\ aK, bK \in G/K$

LHS $= \phi(aK \cdot bK)$

$= \phi(abK)$

$= f(ab)$

$= f(a) f(b)$ ($\because f$ is homo.

$= \phi(aK)\, \phi(bK)$.

Thus ϕ preserve composition

Hence, $G/K \cong G'$.

(31) Let $G = R$, $G' = \{z \in \mathbb{C} / |z| = 1\}$ [G' multi. group]

then prove that $G/K \cong G'$

proof:- Define $f: G \to G'$ by $f(a) = e^{2\pi a i}$

first we p.t $f(a+b) = f(a) f(b)$,

$\forall\ a, b \in G$

$f(a+b) = e^{2\pi(a+b)i}$

$= e^{2\pi a i} \cdot e^{2\pi b i}$

Thus f is homomorphism

Now, we p.t. f is onto.

for any $y \in G'$ then $y \in \mathbb{C}$, $|y| = 1$.

$\therefore y = e^{2\pi x i}$ for some $x \in R = G$

Thus $f(x) = e^{2\pi x i} = y$

Thus f is onto.

Now we p.t. $\ker f = Z$.

$$\ker f = \{a \in G / f(a) = e'\}$$
$$= \{a \in G / f(a) = 1\} \quad (\because \text{identity of } G' \text{ is } 1)$$
$$= \{a \in G / e^{2\pi a i} = 1\}$$
$$= \{a \in G / \cos(2\pi a) + i\sin(2\pi a) = 1\}$$
$$= \{a = 0, \pm 1, \pm 2, \pm 3, \ldots\} = Z$$

Thus $f : G \to G'$ is onto homomorphism & $\ker f = Z$

$\therefore$ By 1st isomorphism theorem, we say that $G/Z \simeq G'$.

(38) Let G be a group and G' be the commutator subgroup of G then prove the following:

(I) G/G' is abelian

(II) If H is normal subgroup of G such that G/H is abelian, then $G' \subset H$.

proof:-

we know that,

$$G' = \{s_1 \cdot s_2 \cdot s_3 \cdots s_n / \forall s_i = a_i b_i a_i^{-1} b_i^{-1}, \forall a_i, b_i \in G\}$$

(i) we have to prove that G/G' is abelian

i.e. to p.t $aG' \cdot bG' = bG' \cdot aG'$,

$\forall\, aG', bG' \in G/G'$.

i.e p.t $abG' = baG'$, $\forall\, aG', bG' \in G/G'$

i.e p.t $(ba)^{-1}(ab) \in G'$, $\forall\, a, b \in G$.

$\because aH = bH \Rightarrow b^{-1}a \in H$

Now, $(ba)^{-1}ab = a^{-1}b^{-1}ab \in G'$

$\therefore G/G'$ is abelian

(II) If H is normal subgroup of G such that G/H is abelian

$\therefore aHbH = bHaH$, $\forall\, a, b \in G$

$\Rightarrow abH = baH$, $\forall\, a, b \in G$

$\Rightarrow (ba)^{-1}ab \in H$, $\forall\, a, b \in G$

$\Rightarrow a^{-1}b^{-1}ab \in H$, $\forall\, a, b \in G$

$\Rightarrow aba^{-1}b^{-1} \in H$, $\forall\, a, b \in G$

We have to p.t $G' \subset H$.

for any $x \in G'$ then $x = s_1 \cdot s_2 \cdot s_3 \cdots s_m$

where $s_i = a_i b_i \cdot a_i^{-1} b_i^{-1}$,

$a_i, b_i \in G$.

Clearly each $s_i = a_i b_i a_i^{-1} b_i^{-1} \in H$.

$\therefore s_1 \cdot s_2 \cdot s_3 \cdots s_m \in H$. $\because$ H is subgroup

Thus $G' \subset H$

(39) Let $\theta : G \to G'$ be a homomorphism,

(i) If H is subgroup of G then p.t $H' = \theta(H)$ is a subgroup of G' and θ is onto then p.t H' is normal in G'.

If H is normal in G

H is normal

(ii) If H' is subgroup of G' then p.t. $H = \theta^{-1}(H')$ is subgroup of G if H' is normal in G' then p.t. H is normal

$\Rightarrow H \trianglelefteq G \mid H'$ Date: / /

Proof: (i) we have to p.t $H' = \theta(H)$ is subgroup of G'

i.e p.t $ab^{-1} \in H'$, $\forall a', b' \in H'$.

for any $a', b' \in H'$ then $a' = \theta(a)$, $b' = \theta(b)$ for some $a, b \in H$.

Now $a'b'^{-1} = \theta(a)\theta(b)^{-1}$

$= \theta(a)\theta(b^{-1})$ * (θ homo)

$= \theta(ab^{-1}) \in \theta(H) = H'$.

($\because$ H is subgroup $\Rightarrow ab^{-1} \in H$)

Thus H' is subgroup of G'.

we p.t

Now, H' is normal in G'.

i.e p.t $x'a'x'^{-1} \in H'$ $\forall x' \in G'$, $a' \in H'$.

for any $x' \in G'$, $a' \in H'$ then $a' = \theta(a)$ for $a \in H$

also $\theta: G \to G'$ is onto

$\therefore \exists\ x \in G \ni \theta(x) = x'$

Now, $x'a'x'^{-1} = \theta(x)\theta(a)\theta(x^{-1})$

$= \theta(xax^{-1})$ ($\because$ θ homo

$\in \theta(H)$ ($\because$ H is normal

$= H'$.

Thus H' is normal in G'.

(ii) we have to p.t $H = \theta^{-1}(H')$ is a subgroup of G.

$H = \theta^{-1}(H') = \{a \in G \mid \theta(a) \in H'\}$

we have to p.t $ab^{-1} \in H$, $\forall a, b \in H$

for any $a, b \in H$ then $\theta(a), \theta(b) \in H'$

also $\theta(ab^{-1}) = \theta(a)\,\theta(b^{-1})$

$= \theta(a)\,\theta(b)^{-1}$

$\in H'$ ($\because H'$ is subgroup

$\therefore ab^{-1} \in H, \forall a, b \in H$.

Thus H is subgroup of G

Now we p.t H is normal in G

i.e p.t $xax^{-1} \in H, \forall x \in G, a \in H$

For any $x \in G, a \in H$ then

$\theta(a) \in H'$ & $\theta(x) \in G'$

Now,

$\theta(xax^{-1}) = \theta(x)\,\theta(a)\,\theta(x^{-1})$

$= \theta(x)\,\theta(a)\,\theta(x)^{-1}$ # $\theta(xax^{-1})$,

$\in H'$ ($\because H'$ is normal in G'

$\therefore xax^{-1} \in H, \forall x \in G, a \in H$

Hence H is normal in G

(iii) we have to p.t $G/H \cong G'/H'$.

Define a mapping $f: G/H \to G'/H'$ by

$f(aH) = \theta(a)H'$.

first we p.t f is well defined

$aH = bH \Leftrightarrow a^{-1}b \in H$

$\Leftrightarrow \theta(a^{-1}b) \in H'$ ($\because H' = \theta(H)$)

$\Leftrightarrow \theta(a^{-1})\,\theta(b) \in H'$ ($\because \theta$ homo

$\Leftrightarrow \theta(a)^{-1}\theta(b) \in H'$

$\Leftrightarrow \theta(a)H' = \theta(b)H'$

Thus f is well defined

Now we p.t f is onto

for any $y \in G'/H'$ then $y = a'H'$ for some $a' \in G'$

Since $\theta : G \to G'$ is onto,

$\exists\ a \in G \ni \theta(a) = a'$

$\Rightarrow aH \in G/H$ $(\because a \in G)$

Let $x = aH$ then $x \in G/H$

also $f(x) = f(aH) = \theta(a)H'$

$= a'H' = y$

Now we p.t $f(aH \cdot bH) = f(aH) \cdot f(bH)$, $\forall aH, bH \in G/H$.

$L.H.S = f(aH \cdot bH)$

$= f(abH)$

$= \theta(ab)H'$

$= \theta(a)\theta(b)H'$

$= \theta(a)H' \cdot \theta(b)H'$

$= f(aH)\, f(bH)$

$= R.H.S$

Thus f preserves composition

Hence $G/H \cong G'/H'$.

(Q0) State & prove 2nd isomorphism theorem.

Ans:- Statement :-

Let G be a group and H, K normal subgroups of G $\ni$ $K \subset H$ then H/K is normal in G/K and also the quotient group $(G/K)/(H/K) \cong G/H$

proof:- consider the mapping $p: G \to G/K$ defined by, $p(a) = aK$, $\forall a \in G$

Clearly, $p(ab) = abK$
$= aKbK$
$= p(a)p(b)$, $\forall a, b \in G$

Thus, p is homomorphism.

Now, we prove that p is onto

for any $y \in G/K$ then $y = xK$, for some $x \in G$.

also $p(x) = xK = y$.

Thus p is onto.

Also we have given that H is normal

$\therefore p(H) = H/K$ is normal in G/K (by above thm (ii))

also,

$p^{-1}(H/K) = H$

$\therefore$ by above thm (iii) we say that

$$\boxed{G/H \cong G/K \,/\, H/K}$$

(41) State & prove third isomorphism theorem

Ans:-

* Statement:-

Let G be a group, H & K are subgroups of G such that K is normal in G then $H \cap K$ is normal in H and

$$H/(H \cap K) \cong (HK)/K.$$

proof:- we have given that K is normal in G

$\therefore aK = Ka$, $\forall a \in G$

Date: / /

$\Rightarrow aK = Ka \quad \forall a \in H$

$\Rightarrow HK = KH$

$\Rightarrow HK$ is subgroup of G

also $K \subset HK$ & K is normal in G

$\therefore K$ is normal in HK

Now, we prove that $H \cap K$ is normal in H.

i.e we have to prove that,

$xax^{-1} \in H \cap K, \forall x \in H, a \in H \cap K,$

low for any $x \in H, a \in H \cap K$ then $a \in H$ & $a \in K$

since K is normal in G,

$xax^{-1} \in K, \forall x \in G, a \in K$

$\Rightarrow xax^{-1} \in K, \forall x \in H, a \in K$ — (1)

also, $x \in H, a \in H$ & H is subgroup

$\therefore x^{-1} \in H$ & $xax^{-1} \in H, \forall x \in H, a \in H$ — (2)

By (1) & (2), we say that,

$xax^{-1} \in H \cap K, \forall x \in H, a \in H \cap K$

Hence, $H \cap K$ is normal in H.

Now we p.t $H/(H \cap K) \cong (HK)/K$.

define a mapping $f : H \to (HK)/K$ by $f(a) = aK$

clearly $f(ab) = abK$

$= aKbK$

$= f(a) f(b)$

Thus f is homomorphism

Now, we p.t f is onto

for any $y \in (HK)/K$, $y = (h_1k_1)K$, for some $h_1 \in H$, $k_1 \in K$

$= h_1k_1K$

$= h_1K$, for some $h_1 \in H$

also $f(h_1) = h_1K = y$

Thus f is onto.

Now we p.t. $\ker f = H \cap K$

$LHS = \ker f = \{a \in H / f(a) = e'\}$

$= \{a \in H / f(a) = K\}$ ($\because$ K is identity of $(HK)/K$)

$= \{a \in H / aK = K\}$

$= \{a \in H / a \in K\}$

$= \{a / a \in H \cap K\}$

$= H \cap K$.

Thus $f : H \to (HK)/K$ is onto homomorphism and $\ker f = H \cap K$

$\therefore$ By 1st isomorphism thm we say that

$$H/H \cap K \cong (HK)/K.$$

(Q2) Corollary :-

Let H & K be finite subgroups of group G such that K is normal in G then p.t

$$O(HK) = \frac{O(H)\,O(K)}{O(H \cap K)}$$

proof:- By 3rd isomorphism thm, we say that

$$\therefore O(H/H\cap K) = O((HK)/K)$$

$$\Rightarrow \frac{O(H)}{O(H\cap K)} = \frac{O(HK)}{O(K)} \Rightarrow O(HK) = \frac{O(H)O(K)}{O(H\cap K)}$$

UNIT-4

* **Direct product:-**

Let H, K be normal subgroups of G such that $G = HK$ and $H\cap K = \{e\}$ then G is called direct product (or internal direct product) of H & K

It is denoted by,

$$G = H \times K$$

(Q3) Let $G = \langle a \rangle$ be cyclic group of order 6. Let $H = \{e, a^4, a^2\}$, $K = \{e, a^3\}$ be subgroups of G then prove that G is direct product of H and K (i.e. $G = H \times K$).

$\{e, a^2, a^4\}$

proof:-

Here $G = \{e, a, a^2, a^3, a^4, a^5\}$ is cyclic group of order 6.

$\therefore$ G is commutative

$\therefore$ H & K are normal in G

also,

$$HK = \{hk / h\in H, k\in K\}$$
$$= \{e\cdot e, e\cdot a^3, a^4\cdot e, a^4 a^3, a^2\cdot e, a^2\cdot a^3\}$$
$$= \{e, a^3, a, a^4, a^2, a^5\}$$
$$= \{e, a, a^2, a^3, a^4, a^5\} = G$$

also,

$$H\cap K = \{e\}$$

Hence G is direct product of H & K

(44) Let $G = \{e, a, b, c\}$ be the Klein's 4-group $H = \{e, a\}$ & $K = \{e, b\}$ then p.t. $G = H \times K$.

proof :-

Clearly H and K are subgroups of G and G is abelian group

$\therefore$ H and K are normal subgroups of G

also,

$HK = \{e \cdot e, e \cdot b, a \cdot e, a \cdot b\}$

$= \{e, b, a, c\} = G$

& $H \cap K = \{e\}$.

Hence G is direct product of H & K.

i.e. $G = H \times K$.

(45) p.T. G is direct product of subgroups H & K iff following conditions are satisfied.

(i) Every $x \in G$ can be expressed uniquely as $x = hk$, $h \in H$, $k \in K$.

(ii) $hk = kh$, $\forall\ h \in H$, $k \in K$.

proof :-

If $G = H \times K$ then by def^n. we say that H & K are normal subgroups of G $G = HK$ and $H \cap K = \{e\}$

(i) for any $x \in G$, $x \in HK$ ($\because G = HK$)

$\therefore x = hk$ for some $h \in H, k \in K$

Now we p.t above representation of x is unique.

Suppose $x = h'k'$ for some $h' \in H$, $k' \in K$. be another representation of x then

$hk = h'k'$

$\Rightarrow h'^{-1}(hk)k^{-1} = h'^{-1}(h'k')k^{-1}$

$\rightarrow$ $k^{-1}k = h'^{-1}h'k^{-1}$

Date: / /

Since $h'^{-1}h \in H$, $k'k^{-1} \in K$

$\therefore h'^{-1}h = k'k^{-1} \in H \cap K = \{e\}$

$\Rightarrow h'^{-1}h = e = k'k^{-1}$

$\Rightarrow h = h'$ & $k = k'$

Thus condition (i) is satisfied

(ii) Now we p.t $hk = kh$

for any $h \in H$, $k \in K$ we know that

$hkh^{-1}k^{-1} = h(kh^{-1}k^{-1}) \in H$

(∵ H is normal s.g.)

also, $hkh^{-1}k^{-1} = (hkh^{-1})k^{-1} \in K$

(∵ K is normal s.g.)

Thus $hkh^{-1}k^{-1} \in H \cap K = \{e\}$

$\therefore hkh^{-1}k^{-1} = e$

$\Rightarrow hkh^{-1} = k$

$\Rightarrow \boxed{hk = kh}$, $\forall h \in H, k \in K$

(*) Converse part :-

If conditions (i) & (ii) are satisfied then we have to p.t $G = HK$

i.e p.t H & K are normal s.g. of G

$G = HK$ & $H \cap K = \{e\}$

from condition (i) we say that

$G = HK$

If $t \in H \cap K$ then $t \in H$ & $t \in K$

$t = t.e$ for some $t \in H$, $e \in K$

$t = e.t$ " " $e \in H$, $t \in K$

Hence by uniqueness we say that

$t = e$

Thus $H \cap K = \{e\}$.

Now we p.t H is normal in G
i.e p.t $xhx^{-1} \in H$, $\forall x \in G, h \in H$
for any $x \in G$, $h \in H$. Then
$x = h_1 k_1$ for some $h_1 \in H$ & $k_1 \in K$

Now, $xhx^{-1} = (h_1 k_1) h (h_1 k_1)^{-1}$
$= h_1 k_1 h k_1^{-1} h_1^{-1}$
$= h_1 k_1 k_1^{-1} h h_1^{-1}$ ($\because hk = kh$, $\forall h \in H, k \in K$)
$= h_1 h h_1^{-1}$
$\in H$

Thus H is normal in G
Similarly we can p.t K is normal in G.

Hence $G = H \times K$.

* Direct sum of subgroups:-
Let $(G, +)$ be any commutative group. and H, K are subgroups of G then the direct product of H & K is known as the direct sum of H & K.
i.e G is direct sum of H & K if.
(i) $G = H + K$.
(ii) $H \cap K = \{0\}$.

(Q6) Let G be an abelian group. H & K are subgroups of G then p.t: G is direct sum of H & K iff every $x \in G$ can be expressed uniquely as $x = h + k$, for some $h \in H, k \in K$.

Proof: If G is direct sum of H & K then by def^n. we say that,

$$G = H + K \text{ & } H \cap K = \{0\}$$

Now for any $x \in G$ then $x = h + k$ for some $h \in H, k \in K$

If possible suppose $x = h' + k'$ for some $h' \in H, k' \in K$ be the another representation of x then

$$h + k = h' + k'$$

$$\Rightarrow (-h') + (h + k) + (-k) = (-h') + (h' + k') + (-k)$$

$$\Rightarrow -h' + h = k' - k$$

since $-h' + h \in H$, $k' - k \in K$

$$\therefore -h' + h = k' - k \in H \cap K = \{0\}$$

$$\Rightarrow -h' + h = 0 = k' - k$$

$$\Rightarrow h = h', \; k = k'$$

Thus uniqueness is proved

* Converse part:-

If every $x \in G$ can be expressed uniquely as $x = h + k$, $h \in H, k \in K$ then we have p.t. $G = H + K$ & i.e. $H \cap K = \{0\}$

As $x = h + k$, $h \in H, k \in K$, we say that

$$G = H + K$$

If $t \in H \cap K$ then $t \in H$ & $t \in K$

$t = t + 0$ for some $t \in H, 0 \in K$

$t = 0 + t$ " " $0 \in H, t \in K$

Hence by uniqueness we say that

$$t = 0$$

Thus $H \cap K = \{0\}$.

Thus G is direct sum of H & K

denoted by $H \oplus K$.

* **Remark :-**
If G is abelian and $H_1, H_2, \ldots, H_n$ are subgroups of G then G is direct sum of $H_1, H_2, \ldots, H_n$ iff every $x \in G$ can be expressed uniquely as $x = h_1 + h_2 + \cdots + h_n$ for $h_i \in H_i$, $i = 1, 2, \ldots n$

* **External direct product of group :-**
Let H & K be any groups then the cartesian product $H \times K$ is called the external direct product of H & K

Clearly $H \times K = \{(h, k) / h \in H, k \in K\}$.

Binary operation in $H \times K$ is defined by
$(h_1, k_1) \cdot (h_2, k_2) = (h_1 h_2, k_1 k_2)$,
$\forall (h_1, k_1), (h_2, k_2) \in H \times K$.

(Q) P.T. external direct product of two groups also forms a group.

proof :-

Let H and K be any two groups then we have to p.t. the cartesian product,
$H \times K = \{(h, k) / h \in H, k \in K\}$
forms a group.

* Clearly $(h_1, k_1) \cdot (h_2, k_2)$
$= (h_1 h_2, k_1 k_2) \in H \times K$, $\forall (h_1, k_1), (h_2, k_2) \in H \times K$
Thus operation is binary.

* **Associative property :-**
we have to p.t.
$[(h_1, k_1) \cdot (h_2, k_2)] \cdot [(h_3, k_3)]$
$= [(h_1, k_1)] [(h_2, k_2) \cdot (h_3, k_3)]$,

Date: / /

LHS $= (h_1, h_2, k_1 k_2)(h_3, k_3)$

$= (h_1, h_2 h_3, k_1 k_2 k_3)$

$= [h_1 (h_2 h_3), k_1 (k_2 k_3)]$ ($\because$ H & K are groups

$= [(h_1, k_1)(h_2 h_3, k_2 k_3)]$

$= (h_1, k_1)[(h_2, k_2)(h_3, k_3)]$

$=$ RHS.

⊛ Identity prop.:-

* Let e_H and e_K be identity of H & K respectively then $(e_H, e_K) \in H \times K$.

also,

$(h, k)(e_H, e_K)$

$= (h e_H, k e_K) = (h, k)$

Similarly $(e_H, e_K)(h, k) = (h, k)$,

$\forall (h, k) \in H \times K$.

Thus $(e_H, e_K) \in H \times K$ is the identity element of $H \times K$

* Inverse prop.:-

for any $(h, k) \in H \times K$ then $(h^{-1}, k^{-1}) \in H \times K$.

($\because$ H & K are groups)

Also $(h, k)(h^{-1}, k^{-1})$

$= (h h^{-1}, k k^{-1})$

$= (e_H, e_K)$

similarly $(h^{-1}, k^{-1})(h, k)$

$= (h^{-1} h, k^{-1} k)$

$= (e_H, e_K)$

Thus, $(h, k)^{-1} = (h^{-1}, k^{-1})$, $\forall (h, k) \in H \times K$

Thus $H \times K$ is a group.

i.e external direct product of H & K is group.

* Commutative prop :-

$(h_1, k_1)(h_2, k_2) = (h_1 h_2, k_1 k_2)$ &

$(h_2, k_2)(h_1, k_1) = (h_2 h_1, k_2, k_1)$

Thus $(h_1, k_1)(h_2 k_2) \neq (h_2, k_2)(h_1, k_1)$

$\therefore H \times K$ is not commutative.

We can say that $H \times K$ is commutative only if H & K both are commutative groups.

(48) P.T. external direct sum of two groups form a group.

proof :-

Let H & K be two groups with operation '+' then the external direct sum of H & K is denoted by $H \oplus K$ and defined as $H \oplus K = \{(h, k) / h \in H, k \in K\}$.

We have to p.t. $H \oplus K$ is a group.

* closure property :-

Clearly $(h_1, k_1) + (h_2, k_2)$

$= (h_1 + h_2, k_1 + k_2) \in H \oplus K,$

$\forall (h_1, k_1), (h_2, k_2) \in H \oplus K$

Thus operation is binary.

$\therefore$ closure prop. is satisfied.

* Associative prop :-

$[(h_1, k_1) + (h_2, k_2)] + (h_3, k_3) =$

$(h_1, k_1) + [(h_2, k_2) + (h_3, k_3)]$

Date: / /

L.H.S. $= [(h_1, k_1) + (h_2, k_2)] + (h_3, k_3)$

$= [(h_1 + h_2), (k_1 + k_2)] + (h_3, k_3)$

$= (h_1 + h_2 + h_3, k_1 + k_2 + k_3)$

$= (h_1 + (h_2 + h_3), k_1 + (k_2 + k_3))$

($\because$ H & K are groups)

$= (h_1, k_1) + [(h_2 + h_3), (k_2 + k_3)]$

$= (h_1, k_1) + [(h_2, k_2) + (h_3, k_3)]$.

$=$ R.H.S

* Identity prop:-

Here 0 be the identity of H & K

clearly $(0, 0) \in H \oplus K$.

also, $(h, k) + (0, 0)$

$= (h + 0, k + 0)$

$= (h, k)$

i.e., $(0, 0) + (h, k) = (h, k)$,

$\forall (h, k) \in H \oplus K$

Thus $(0, 0) \in H \oplus K$ is the identity element of $H \oplus K$.

* Inverse prop:-

for any $(h, k) \in H \oplus K$ then $(-h, -k) \in H \oplus K$

Also, $(h, k) + (-h, -k)$

$= (h - h, k - k)$

$= (0, 0) = (-h, -k) + (h, k)$

Thus $(h, k)^{-1} = (-h, -k)$, $\forall (h, k) \in H \oplus K$

Thus $H \oplus K$ is group.

Thus external direct sum of H & K is

(49) P.T. external direct sum of R forms a group.

proof :- We have to p.t. $R \oplus R = \{(h,k) / h \in R, k \in R\}$ forms a group.

* Clearly $(h_1, k_1) + (h_2, k_2)$
$= (h_1 + h_2, k_1 + k_2) \in R \oplus R$,
$\forall (h_1, k_1), (h_2, k_2) \in R \oplus R$

Thus operation is binary.

* Associative :-
$[(h_1, k_1) + (h_2, k_2)] + (h_3, k_3)$
$= (h_1, k_1) + [(h_2, k_2) + (h_3, k_3)]$

L.H.S. $= (h_1 + h_2, k_1 + k_2) + (h_3, k_3)$
$= (h_1 + h_2 + h_3, k_1 + k_2 + k_3)$
$= (h_1 + (h_2 + h_3), k_1 + (k_2 + k_3))$ ($\because$ R is group
$= (h_1, k_1) + (h_2 + h_3, k_2 + k_3)$
$= (h_1, k_1) [(h_2, k_2) + (h_3, k_3)]$
$=$ R.H.S.

* Identity :-

Here 0 be the identity of R
Clearly $(0,0) \in R \oplus R$
also,
$(h,k) + (0,0)$
$= (h+0, k+0) = (h,k) = (0,0) + (h,k)$,
$\forall (h,k) \in R \oplus R$

Thus $(0,0) \in R \oplus R$ is identity element
of $R \oplus R$

Date: / /

* Inverse :-

for any $(h,k) \in R \oplus R$ then
$(-h,-k) \in R \oplus R$ ($\because R$ group

also, $(h,k) + (-h,-k)$
$= (h-h, k-k)$
$= (0,0) = (-h,-k) + (h,k)$

Thus $(h,k)^{-1} = (-h,-k)$,
$\forall (h,k) \in R \oplus R$

Thus $R \oplus R$ is a group.
i.e. external direct sum of R forms a group.

(50) P.T. external direct sum of Z_2 is a Klein's 4-group.

proof :-

We know that, $Z_2 = \{\bar{0}, \bar{1}\}$
& $Z_2 \oplus Z_2 = \{(h,k) / h,k \in Z_2\}$
$= \{(\bar{0},\bar{0}), (\bar{0},\bar{1}), (\bar{1},\bar{0}), (\bar{1},\bar{1})\}$
$= \{e, a, b, c\}$

where,
$e = (\bar{0},\bar{0})$, $a = (\bar{0},\bar{1})$, $b = (\bar{1},\bar{0})$,
$c = (\bar{1},\bar{1})$

also, $2a = a+a$
$= (\bar{0},\bar{1}) + (\bar{0},\bar{1}) = (\bar{0}+\bar{0}, \bar{1}+\bar{1})$
$= (\bar{0},\bar{2})$
$= (\bar{0},\bar{0}) = e = 2b = 2c$

also,
$a+b = (\bar{0},\bar{1}) + (\bar{1},\bar{0})$
$= (\bar{0}+\bar{1}, \bar{1}+\bar{0})$

Similarly, $(b+c) = a = c+b$

$(a+c) = b = c+a$

Hence, $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ is a klein's 4-group.

(51) If G is a ~~external~~ direct product of subgroups H and K then p.t. G is isomorphic to the external direct product of H & K. (~~then~~) conversly if G is external direct product of H & K then p.t. H & K are isomorphic to the subgroups H' & K' of G respect. also p.t. G is direct product of s.g. H' & K'.

* Note :- If $f: A \to B$ is homomorphism & one-one (but not onto) then $A \cong f(A)$.

proof :-

If G is direct product of H & K then every $x \in G$ can be expressed uniquely as $x = hk$, for some $h \in H, k \in K$

We have to p.t. $G \cong H \times K$ (ext. dir. prod)

Define a mapping $f: G \to H \times K$ by

$f(x) = (h, k)$, $\forall x \in G$

where $x = hk$.

first we p.t. $f(xy) = f(x) f(y)$,

where $x = hk$

for any $x, y \in G$ then $x = h_1k_1$, $y = h_2k_2$

for some $h_1, h_2 \in H$,

$k_1, k_2 \in K$.

L.H.S. $f(xy) = f(h_1k_1h_2k_2)$

$= f(h_1h_2k_1k_2)$ ($\because$ G is dir. prod. of H & K

$= (h_1h_2, k_1k_2)$

Date: / /

Now we p.t f is one-one

$f(x) = f(y)$

$\Rightarrow (h_1, k_1) = (h_2, k_2)$

$\Rightarrow h_1 = h_2, k_1 = k_2$

$\Rightarrow h_1 k_1 = h_2 k_2$

$\Rightarrow x = y$

Now we p.t. f is onto.

for any $y \in H \times K$ then $y = (h, k)$ for some $h \in H, k \in K$

Let $x = hk \in G$ then

$f(x) = f(hk) = (h, k) = y$.

Thus f is onto.

Hence, $G \cong H \times K$

* converse part :-

If $G = H \times K$ is the external direct product of H & K

Define a mapping $i_H : H \to G$ by $i_H(h) = (h, e_K)$ for $\forall h \in H$.

first we p.t $i_H(h_1 \cdot h_2) = i_H(h_1) \cdot i_H(h_2)$, $\forall h_1, h_2 \in H$

$i_H(h_1 \cdot h_2) = (h_1 h_2, e_K)$

$= (h_1, e_K)(h_2, e_K)$

$= i_H(h_1)\, i_H(h_2)$

Now we p.t i_H is one-one

$i_H(h_1) = i_H(h_2)$

$\Rightarrow (h_1, e_K) = (h_2, e_K)$

$\Rightarrow h_1 = h_2$

Thus i_H is one-one

Now we check that i_H is onto or not

for any $g \in G$ then $g = (h, k)$, for some $h \in H, k \in K$

but $i_H(h) = (h, e_K) \neq (h, k)$

i.e $i_H(h) \neq g$.

$\therefore i_H$ is not onto.

Thus $i_H : H \to G$ is homomorphism, one-one but not onto.

$\therefore H \cong i_H(H)$

Let $H' = i_H(H)$ then H' is subgroup of G

($\because xy^{-1} \in H', \forall x, y \in H'$

* Let $x = i_H(h_1)$, $y = i_H(h_2)$ then

$y^{-1} = i_H(h_2)^{-1}$

$= i_H(h_2^{-1})$

$\therefore xy^{-1} = i_H(h_1) \cdot i_H(h_2^{-1})$

$= i_H(h_1 h_2^{-1})$ ($\because i_H$ is homo

$\in i_H(H) = H'$)

Thus $H \cong H'$ where H' is s.g. of G

Similarly we can p.t. $K \cong K'$, where K' is s.g. of G.

Now we p.t G is dir. prod of H' & K'.

i.e we have to p.t H' & K' are normal in G, $G = H'K'$, $H' \cap K' = \{e'\}$.

Date: / /

clearly $H'K' = K'H'$

$(\because (h, e_K)(e_H, k)$
$= (h, k) = (e_H, k)(h, e_K)$

$\therefore$ H' & K' are normal in G

Now we p.t $G = H'K'$

clearly $H'K' \subset G$

for any $x \in G$, $G = H \times K$

$x = (h, k)$

$= (h, e_K)(e_H, k)$

$\in H'K'$

$\therefore G \subset H'K'$.

Hence $G = H'K'$

Now we p.t $H' \cap K' = \{e'\}$

for any $t \in H' \cap K'$ then $t \in H'$ & $t \in K'$

$\therefore t = (h, e_K)$, $h \in H$

$t = (e_H, k)$, $k \in K$

$\therefore (h, e_K) = (e_H, k)$

$\Rightarrow h = e_H$ & $k = e_K$

$\therefore t = (e_H, e_K) = e'$

Hence $H' \cap K' = \{e'\}$

Hence, G is direct product of H' & K'.

external

(52) Let $G = H \times K$ be the direct product of H & K then p.t. the mapping $\rho_H : G \to H$ & $\rho_K : G \to K$ defined by $\rho_H(h,k) = h$ & $\rho_K(h,k) = k$.

are group homomorphism whose kernals are $K' = \{(e_H, k) / k \in K\}$, $H' = \{(h, e_K) / h \in H\}$ respectively. In perticular p.t. $G/H' \cong K$ & $G/K' \cong H$ or

p.T. $G/H' \cong K$ and $G/K' \cong H$.

external

where $G = H \times K$ is the direct product of H & K. $H' = \{(h, e_K) / h \in H\}$

$K' = \{(e_H, k) / k \in K\}$.

proof:

Here $\rho_H : G \to H$ is defined by

$\rho_H(h,k) = h$

first we p.t $\rho_H(xy) = \rho_H(x)\rho_H(y)$, $\forall x, y \in G$

[LHS = $\rho_H(xy)$]

for any $x, y \in G$ then $x = (h_1, k_1)$, $y = (h_2, k_2)$

for some $h_1, h_2 \in H$, $k_1, k_2 \in K$

$$\begin{aligned} LHS &= \rho_H(xy) \\ &= \rho_H((h_1, k_1)(h_2, k_2)) \\ &= \rho_H(h_1 h_2, k_1 k_2) \\ &= h_1 h_2 \\ &= \rho_H(x)\rho_H(y) = R.H.S. \end{aligned}$$

Thus ρ_H is homomorphism

clearly ρ_H is onto because

for any $h \in H$ we have $(h, k) \in G$, $\forall k \in K$

Date: / /

Now we prove that,

$\ker \rho_H = K'$

$LHS = \ker \rho_H$

$= \{ x \in G / \rho_H(x) = e_H \}$

$= \{ x = (h, k) \in G / h = e_H \}$

$= \{ (e_H, k) / k \in K \}$

$= K'$

Thus, $\rho_H : G \to H$ is onto homomorphism & $\ker \rho_H = K'$.

$\therefore$ By 1st isomorphism thm, we say that

$$\boxed{G/K' \cong H}$$

Similarly we can p.t $\rho_K : G \to K$ is onto homomorphism & $\ker \rho_K = H'$ (prove it)

$$\therefore \boxed{G/H' \cong K}$$

* Permutation :-

A permutation on 'n' symbols is a one-one mapping of the set, $I_n = \{1, 2, 3, \ldots, n\}$ onto itself.

If σ is a permutation on n symbol then σ is completely determined by its value $\sigma(1), \sigma(2), \ldots, \sigma(n)$.

We use the following notations to denote permutations :-

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \cdots & \sigma(n) \end{pmatrix}$$

e.g. $\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$ is permutation on 4-symbols and

$\sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$ is another representation on 4-symbols.

also, $\sigma_1\sigma_2(1) = (\sigma_1 \circ \sigma_2)(1) = \sigma_1(\sigma_2(1))$
$= \sigma_1(4) = 4$

$\sigma_1\sigma_2(2) = \sigma_1(\sigma_2(2)) = \sigma_1(3) = 1$

$\sigma_1\sigma_2(3) = \sigma_1(\sigma_2(3)) = \sigma_1(2) = 2$

$\sigma_1\sigma_2(4) = \sigma_1(\sigma_2(4)) = \sigma_1(1) = 3.$

$\therefore \sigma_1\sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$

$\sigma_2\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$ ←

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

Thus $\sigma_1\sigma_2 \neq \sigma_2\sigma_1$.

(53) P.T. product of permutation on 4-symbol need not be commutative

above ex.

(59) Let S_n be the set of all permutations on n symbols then p.t. S_n forms a group.

<u>or</u>

P.T. S_n is a non commutative group.

pf:- W.K.T $S_n = \{\theta / \theta : \{1,\dots,n\} \to \{1,\dots,n\}$ is one-one & onto map$\}$

We know that, composition of two one-one and onto map is also one-one and onto.

∴ product of two permutations on n-symbols is also permutation on n-symbols.

i.e $\sigma_i \cdot \sigma_j \in S_n \ \forall \ \sigma_i, \sigma_j \in S_n$

Thus operation is binary.

* → Associative :-

We know that composition of functions are always associative.

$(\sigma_i \cdot \sigma_j) \cdot \sigma_k = \sigma_i \cdot (\sigma_j \cdot \sigma_k)$

$\forall \ \sigma_i, \sigma_j, \sigma_k \in S_n$.

* → Identity :-

For any $\sigma \in S_n$ then

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & \dots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \sigma(4) & \dots & \sigma(n) \end{pmatrix}$$

Let

$$I = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ 1 & 2 & 3 & \dots & n \end{pmatrix} \in S_n$$

also $\sigma I = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix} = \sigma = I\sigma$

$\therefore I = \begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{pmatrix}$ is identity permutation of S_n.

* → Inverse :-

For any $\sigma \in S_n$, σ is one-one & onto map $\therefore \sigma^{-1}$ exists and also σ^{-1} is one-one and onto. also $\sigma\sigma^{-1} = I = \sigma^{-1}\sigma$.

Thus S_n forms a group also it is not commutative.

because,

ib $\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & n \\ 2 & 3 & 1 & 4 & \cdots & n \end{pmatrix} \in S_n$

$\sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & n \\ 3 & 2 & 1 & 4 & \cdots & n \end{pmatrix} \in S_n$

$\sigma_1\sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & n \\ 1 & 3 & 2 & 4 & \cdots & n \end{pmatrix}$ &

$\sigma_2\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & n \\ 2 & 1 & 3 & 4 & \cdots & n \end{pmatrix}$

Thus $\sigma_1\sigma_2 \neq \sigma_2\sigma_1$.

Hence S_n is non commutative group.

* Remark :-

Above group S_n is called symmetric

(55) P.T. S_n is a finite group of order $n!$ also p.t. S_n is non abelian group for $n>2$.

Proof:-

Clearly S_n is group. (prove it)

If $\sigma \in S_n$ then σ is one-one and onto map.

$\therefore \sigma(1)$ can be defined by n different ways.

$\sigma(2)$ can be defined by $n-1$ different ways. and so on.

Thus any permutation $\sigma \in S_n$ can be defined by $n(n-1)(n-2)\cdots 3\cdot 2\cdot 1$ ways. i.e $n!$ different ways.

Hence order of S_n is $n!$

Now. for $n>2$.

Let $\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & n \\ 2 & 3 & 1 & 4 & \cdots & n \end{pmatrix}$

$\sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & n \\ 3 & 2 & 1 & 4 & \cdots & \end{pmatrix}$

$\sigma_2\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & n \\ 2 & 1 & 3 & 4 & \cdots & n \end{pmatrix}$ &

$\sigma_1\sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & n \\ 1 & 3 & 2 & 4 & \cdots & n \end{pmatrix}$

Thus $\sigma_1\sigma_2 \neq \sigma_2\sigma_1$

Hence S_n is non abelian group.

* Transposition :-

A permutation $\sigma \in S_n$ is said to be a transposition if $\exists$ two symbols i, j $\ni \sigma(i) = j$ & $\sigma(j) = i$ & $\sigma(k) = k, \forall k \neq i, j$.

We use the notation (i, j) to denote such transposition.

e.g. (1) $\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}$

$= (2, 4)$ in S_4.

(2) $\sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 2 & 3 & 4 & 1 & 6 \end{pmatrix}$

$= (1, 5)$ in S_6.

* Cycle :-

A permutation $\sigma \in S_n$ is said to be a cycle of order 'r' if $\exists$ r symbols $i_1, i_2, \dots, i_r \ni \sigma(i_1) = i_2, \sigma(i_2) = i_3, \sigma(i_3) = i_4 \dots = \sigma(i_r) = i_1$ & $\sigma(j) = j \cdot \forall j \neq i_1, i_2, \dots, i_r$

we use the notation $(i_1, i_2, \dots, i_r)$ to denote such cycle of order 'r' in S_n. It is also called r-cycle

e.g. (1) $\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}$

$= (2, 4)$ i.e 2-cycle in S_4.

(2) $\sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 1 & 5 \end{pmatrix}$

$$\sigma_3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 3 & 5 & 4 & 2 & 6 \end{pmatrix}$$

$= (2, 3, 5)$ is 3-cycle in S_6.

$$\sigma_4 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix}$$

$= (1, 2, 3, 4, 5)$ is 5-cycle in S_5

Remark :-

$(i_1, i_2, \cdots, i_r) = (i_1, \sigma(i_1), \sigma^2(i_1), \cdots \sigma^{r-1}(i_1))$

(56) P.T. every $\sigma \in S_n$ can be expressed as a product of disjoint cycle

Proof :-

Let $\sigma \in S_n$ and consider the cycle $(1, \sigma(1), \sigma^2(1), \cdots)$

Since order of cycle is finite

$\therefore \sigma^k = 1$ for some k

select least +ve integer $k \ni \sigma^k(1) = 1$

then we have cycle

$(1, \sigma(1), \sigma^2(1), \cdots, \sigma^{k-1}(1))$

If σ fixes all the remaining symbols then $\sigma = (1, \sigma(1), \sigma^2(1), \cdots \sigma^{k-1}(1))$ is k-cycle.

which is product of disjoint cycle.

otherwise we can select a symbol $i \ni \sigma(i) \neq i$ then $\exists$ least +ve

number r s.t. $\sigma^r(j) = j$
we get $(j, \sigma(j), \sigma^2(j), \ldots \sigma^{r-1}(j))$

If σ fixes all the remaining symbols then $\sigma = (1, \sigma(1), \sigma^2(1) \ldots)(j, \sigma(j), \sigma^2(j) \ldots)$
which is product of disjoint cycle, otherwise
If there is another symbol p s.t. $\sigma(p) \neq p$
then continue the same process and after a finite no. of steps process will stop.

$\therefore \sigma = (1, \sigma(1), \ldots \sigma^{k-1}(1))(j, \sigma(j), \ldots \sigma^{r-1}(j)) \ldots$
is product of disjoint cycle.

(51) Express $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 3 & 4 & 6 & 5 & 7 & 1 & 8 & 10 & 12 & 11 & 2 & 9 \end{pmatrix}$
as product of disjoint cycle.

Sol :- $\sigma = (1,3,6)(2,4,5,7,8,10,11)(9,12)$
is the required product of disjoint cycle

(58) P.T. every permutation can be expressed as a product of transposition.

proof :- We know that,
every permutation $\sigma \in S_n$ can be expressed as a ...

Date: / /

∴ It is sufficient to p.t, every cycle can be expressed as a product of transposition

Let $(i_1, i_2, \dots, i_r)$ be any r-cycle then we can write,

$$(i_1, i_2, \dots, i_r) = (i_1, i_r)(i_1, i_{r-1}) \cdots (i_1, i_2)$$

which is product of transposition Hence every permutation σ can be expresed as a product of transposition

(59) Prove or disprove:
Every permutation (cycle) can be expressed as a product of disjoint transposition.

Sol^n:-

Every permutation cannot be expressed as a product of disjoint transposition

because,

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 5 & 4 & 6 & 1 \end{pmatrix}$$

$$= (1, 3, 5, 6)$$

$$= (1, 6)(1, 5)(1, 3)$$

which is product of transpositions.

but transpositions are not disjoint.

* Signature of permutation :-

Let $\sigma \in S_n$ be any permutation then the signature of σ is denoted by $\epsilon\sigma$ and defined as

$$\epsilon\sigma = \prod_{1 \le i < j \le n} \left[\frac{\sigma(i) - \sigma(j)}{i - j} \right]$$

The value of $\epsilon\sigma$ is either 1 or -1

* Signature of transposition is always -1

(60) Find $\epsilon\sigma$ for $\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}$

and $\sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 3 & 1 & 5 \end{pmatrix}$.

Sol :-

$$\epsilon\sigma_1 = \left(\frac{\sigma(1)-\sigma(2)}{1-2}\right)\left(\frac{\sigma(1)-\sigma(3)}{1-3}\right)\left(\frac{\sigma(1)-\sigma(4)}{1-4}\right)$$
$$\left(\frac{\sigma(2)-\sigma(3)}{2-3}\right)\left(\frac{\sigma(3)-\sigma(4)}{3-4}\right)\left(\frac{\sigma(2)-\sigma(4)}{2-4}\right)$$

$$= \left(\frac{2}{-1}\right)\left(\frac{1}{-2}\right)\left(\frac{-1}{-3}\right)\left(\frac{-1}{-1}\right)\left(\frac{-2}{-1}\right)\left(\frac{-3}{-2}\right)$$

$$= 1$$

$$\epsilon\sigma_2 = \left(\frac{2}{-1}\right)\left(\frac{1}{-2}\right)\left(\frac{3}{-3}\right)\left(\frac{-1}{4}\right)\left(\frac{-1}{-1}\right)\left(\frac{1}{-2}\right)\left(\frac{-3}{3}\right)$$
$$\left(\frac{2}{-1}\right)\left(\frac{-2}{-2}\right)\left(\frac{-4}{-1}\right)$$

$$= -1$$

(61) Prove that, the mapping $\epsilon: S_n \to \{1,-1\}$ given by $\sigma \to \epsilon\sigma$ is a homomorphism of S_n onto $\{1,-1\}$.

Pf:-

First we have to p.t

$$\epsilon\sigma_1\sigma_2 = \epsilon\sigma_1 \epsilon\sigma_2$$

$$LHS = \epsilon\sigma_1\sigma_2$$

$$= \prod_{1\le i<j\le n} \left[\frac{\sigma_1\sigma_2(i) - \sigma_1\sigma_2(j)}{i-j} \right]$$

$$= \prod_{1\le i<j\le n} \left[\frac{\sigma_1(\sigma_2(i)) - \sigma_1(\sigma_2(j))}{\sigma_2(i) - \sigma_2(j)} \times \frac{\sigma_2(i)-\sigma_2(j)}{i-j} \right]$$

$$= \prod_{1\le i<j\le n} \left[\frac{\sigma_1(\sigma_2(i)) - \sigma_1(\sigma_2(j))}{\sigma_2(i) - \sigma_2(j)} \right] \times$$

$$\prod_{1\le i<j\le n} \left[\frac{\sigma_2(i) - \sigma_2(j)}{i-j} \right]$$

$$= \epsilon\sigma_1 \cdot \epsilon\sigma_2 = RHS.$$

Clearly ϵ is onto because $\epsilon\sigma$ is either 1 or -1.

(62) Prove or disprove:

The mapping $\epsilon: S_n \to \{1,-1\}$ is one-one or Is $S_n \simeq \{1,-1\}$?

Soln:- Let $\sigma_1 = (1,3)$ in S_3

$\sigma_2 = (1,2)$ in S_3 then

$$\epsilon\sigma_1 = \left(\frac{3-2}{1-2}\right)\left(\frac{3-1}{1-3}\right)\left(\frac{2-1}{2-3}\right) = -1$$

&

$$\epsilon\sigma_2 = \left(\frac{2-1}{1-2}\right)\left(\frac{2-3}{1-3}\right)\left(\frac{1-3}{2-3}\right)$$

$$= -1$$

Thus $\epsilon\sigma_1 = \epsilon\sigma_2$ but $\sigma_1 \neq \sigma_2$

Thus ϵ is not one-one

Hence $S_n \not\cong \{-1, 1\}$.

(63) Let $\sigma \in S_n$ be expressed as a product of transposition then no. of transposition in the decomposition of σ is either always odd or always even

proof:-

Let $\sigma = T_1 * T_2 * \cdots * T_n$ be a product of transposition then

$$\epsilon\sigma = \epsilon(T_1 T_2 \cdots T_n)$$

$$\Rightarrow \epsilon\sigma = \epsilon(T_1)\cdot\epsilon(T_2)\cdots\epsilon(T_n) \quad \text{(prove it)}$$

$$\Rightarrow \epsilon\sigma = (-1)^n \quad (\because \epsilon T_i = -1, \forall i)$$

We know that $\epsilon\sigma$ has a fix value either 1 or -1.

$\therefore$ n is always even or always odd i.e no. of transposition is either always even or always odd

* Even permutation :-

A permutation σ is said to be even per-

Date: / /

* Odd permutation:-
A permutation σ is said to be odd permutation if $\in\sigma = -1$.

→ Remark:-

(1) Every even permutation can be expressed as a product of even no. of transposition

Proof:-
Let σ be any even permutation then
$\in\sigma = 1$
We know that every permutation σ can be expressed as a product of transposition
Let $\sigma = T_1 T_2 \cdots T_n$
where each T_i is transposition
we have to p.t n is even
suppose n is odd
then $\in\sigma = \in T_1 T_2 \cdots T_n$
$= \in(T_1) \in(T_2) \cdots \in(T_n)$
$= (-1)(-1) \cdots (-1)$ (n times)
$= -1$ ($\because n$ is odd) ✗
($\because \in\sigma = 1$)
$\therefore n$ is even
$\therefore$ No of transposition is even

(2) Every odd permutation can be expressed as a product of odd no. of transposition

(64) P.T. the set A_n of all even permutation forms a subgroup of S_n also p.t. it is normal subgroup of S_n

proof:

Define $\epsilon : S_n \to \{1, -1\}$ by $\sigma \to \epsilon\sigma$

Clearly ϵ is homomorphism (prove it)

also kernal $\epsilon = \{\sigma \in S_n / \epsilon\sigma = 1\}$

$= \{\sigma \in S_n / \sigma$ is even per$^n\}$

$= A_n$

Thus $\ker\epsilon = A_n$

we know that ker of group-homomorphism is a normal subgroup.

$\therefore A_n$ is a normal subgroup of S_n

(65) corollary :-

P.T. $O(A_n) = \frac{n!}{2}$, Also p.t. S_n/A_n is cyclic group of order 2. OR

P.T. $S_n/A_n \cong \{1, -1\}$.

proof :- we know that,

$\epsilon : S_n \to \{1, -1\}$ defined by $\sigma \to \epsilon\sigma$ is onto homomorphism and $\ker\epsilon = A_n$ (prove it) then by 1st isomorphism thm,

$$S_n/\ker\epsilon \cong \{1, -1\}.$$

i.e $S_n/A_n \cong \{1, -1\}$ —(*)

$\therefore O(S_n/A_n) = 2$

Date: / /

$\therefore O(A_n) = \frac{O(S_n)}{2} = \frac{n!}{2}$,

Also, clearly $\{1, -1\}$ is a cyclic group of order 2.

$\therefore$ By (*) S_n/A_n is also cyclic group of order 2.

* Remark:-

Group A_n is called alternating group on n-symbols.

(66) State & Prove cayley's theorem:-

→ Let G be a finite group of order n then G is isomorphic to a sub-group of S_n

Proof:-

Let $G = \{a_1, a_2, \ldots, a_n\}$ be any finite group of order n.

For any $a_i \in G$

we say that,

$a_i a_1, a_i a_2, \ldots, a_i a_n \in G$ and all elements are distinct

(∵ If $a_i a_j = a_i a_k$, $j \neq k$.

then $a_j = a_k$ (by L.C.L) $j \neq k$ ※)

Hence $\{a_i a_1, a_i a_2, \ldots, a_i a_n\} = G$.

Thus every $a_i \in G$ defines a permutation σa_i on n

symbols by $\sigma_{a_i}(l) = k$ if $a_i a_l = a_k$

Let $S = \{\sigma_{a_1}, \sigma_{a_2}, \cdots, \sigma_{a_n}\}$ be any set of permutation then clearly S is subgroup of S_n

Now we p.t $G \cong S$

Define a function $f: G \to S$ by

$f(a_i) = \sigma_{a_i}, \forall a_i \in G$

first we p.t $f(a_i a_j) = f(a_i) f(a_j)$, $\forall a_i, a_j \in G$

i.e p.t $\sigma_{a_i a_j}(p) = \sigma_{a_i} \sigma_{a_j}(p)$, $\forall p \in \{1, 2, \cdots, n\}$

Let $\sigma_{a_j}(p) = l$ if $a_j a_p = a_l$ &

$\sigma_{a_i}(l) = k$ if $a_i a_l = a_k$

Now:

$a_i a_l = a_k$

$\Rightarrow a_i (a_j a_p) = a_k$

$\Rightarrow (a_i a_j) a_p = a_k$

$\Rightarrow \sigma_{a_i a_j}(p) = k = \sigma_{a_i}(l)$

$\Rightarrow \sigma_{a_i a_j}(p) = \sigma_{a_i}(\sigma_{a_j}(p))$

$\Rightarrow \sigma_{a_i a_j}(p) = \sigma_{a_i} \sigma_{a_j}(p)$, $\forall p \in \{1, 2, \cdots n\}$

$\Rightarrow \sigma(a_i a_j) = \sigma_{a_i} \sigma_{a_j}$

$\Rightarrow f(a_i a_j) = f(a_i) f(a_j)$

Now we p.t f is one-one

$f(a_i) = f(a_j) \Rightarrow \sigma_{a_i}(p) = \sigma_{a_j}(p) = k$

$\Rightarrow a_i a_p = a_k = a_j a_p$

Date: / /

Now we p.t. f is onto.
for any $\sigma a_i \in S$ then $a_i \in G$ also
$f(a_i) = \sigma a_i$.
Hence $G \cong S$.
i.e G is isomorphic to s.g. of S_n

— x —

(1) Q. Which of following are odd permutation

$(1\ 2\ 3)(4\ 5\ 6)$ (ii) $(1\ 2)(2\ 5\ 3\ 6)(3\ 2\ 4)$

Sol (i) $(1\ 3)(1\ 2)(4\ 6)(4\ 5)$ | (ii) $\varepsilon 6 = (-1)^3 = -1$ odd
$\varepsilon 6 = (-1)^4 = 1$ even

Express the inverse of cycle

(2) $(1\ 2\ 4\ 5\ 3)$ as a product of transpositions

(3) Express following as a product of disjoint cycles

(i) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 4 & 5 & 7 & 6 & 8 & 1 \end{pmatrix}$

(ii) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 6 & 5 & 1 \end{pmatrix}$

Sol (i) $(1\ 2\ 3\ 4\ 5\ 7\ 8)$
(ii) $(1\ 2\ 3\ 4\ 6)$

(2) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 1 & 5 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 5 & 2 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}$

Unit-1

(1) P.T. symmetry of equilateral triangle forms a group also pt. it is non abelian group. (by using rotation & reflection or by using permutation).

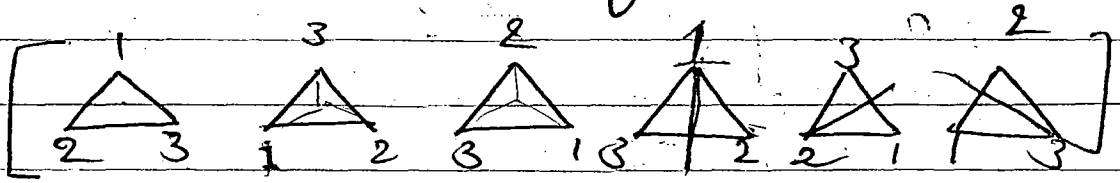
Soln:

We know that following transportation transformation gives a symmetry of equilateral triangle

(i) The 3 rotations about the centre through the angle 0°, 120°, 240°. (anticlockwise).

(ii) The three reflections along the 3 bisectors.

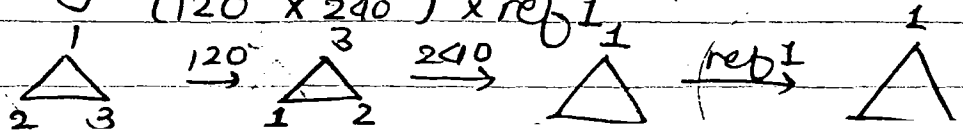
Thus symm. of equilateral triangle contains 6 transformation.



(1) Closure prop:- clearly product of two symmetry is also a symmetry.

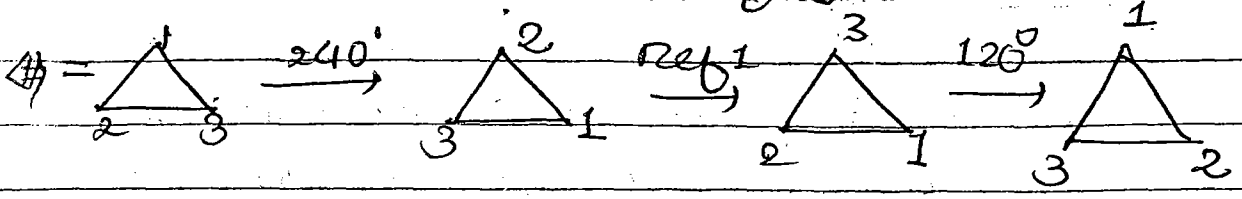
(2) Associative prop:- clearly product of symmetry is always associative

i.e. $(120° \times 240°) \times \text{ref}_1$



Date: / /

also $120^\circ \times [240^\circ \times \text{ref}1]$

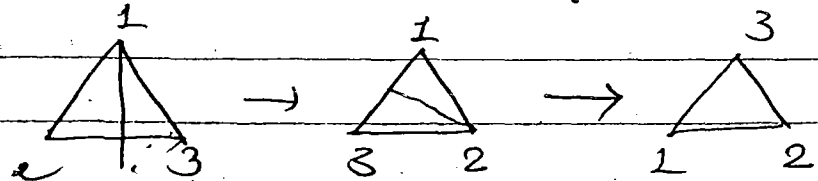


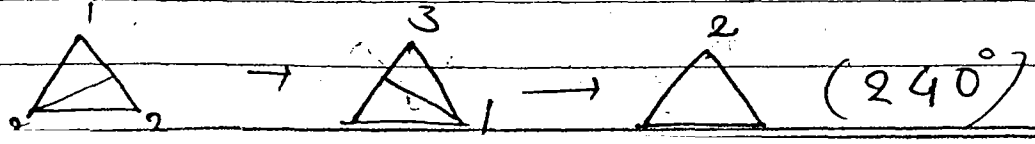
Thus $(120^\circ \times 240^\circ) \times \text{ref}1 = 120^\circ \times (240^\circ \times \text{ref}1)$.

(iii) Identity prop:-
clearly rotation through angle 0° is the identity.

(iv) Inverse prop:-
clearly rotation through angle 120° & 240° are inverse of each other.
also inverse of reflection is itself.

Hence, symmetry of equilateral triangle forms a group
also it is non abelian group because
product of reflection along bisector passing through 1 with bisector passing through 2 is the rotation through 120°.
but reflection along the bisector passing through 2 with the bisector passing through 1 is the rotation about 240°.





(2) Make a multiplication table for the symmetry of equilateral triangle hence it forms a non abelian group.

OR

Show that, S_3 is non abelian group.

OR

P.T. symmetry of equilateral triangle forms a non abelian group by using permutation

Soln:-

The three reflections along a bisector give following permutations:

$$\phi_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad \phi_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix},$$

$$\phi_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

Similarly three rotations about centre give following permutations:

$$\phi_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \phi_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

$$\phi_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

Thus the set of all symmetry of equilateral triangle is,

$$S_3 = \{\phi_0, \phi_1, \phi_2, \phi_3, \phi_4, \phi_5\}$$

The multiplication table for S_3 is given below:

	ϕ_0	ϕ_1	ϕ_2	ϕ_3	ϕ_4	ϕ_5
ϕ_0	ϕ_0	ϕ_1	ϕ_2	ϕ_3	ϕ_4	ϕ_5
ϕ_1	ϕ_1	ϕ_0	ϕ_4	ϕ_5	ϕ_2	ϕ_3
ϕ_2	ϕ_2	ϕ_5	ϕ_0	ϕ_4	ϕ_3	ϕ_1
ϕ_3	ϕ_3	ϕ_4	ϕ_5	ϕ_0	ϕ_1	ϕ_2
ϕ_4	ϕ_4	ϕ_3	ϕ_1	ϕ_2	ϕ_5	ϕ_0
ϕ_5	ϕ_5	ϕ_2	ϕ_3	ϕ_1	ϕ_0	ϕ_4

From the above table we say that,

(i) Closure property & ass. poop. are satisfied

(ii) ϕ_0 is the identity of S_3

(iii) $\phi_0^{-1} = \phi_0$

$\phi_1^{-1} = \phi_1$

$\phi_2^{-1} = \phi_2$

$\phi_3^{-1} = \phi_3$

$\phi_4^{-1} = \phi_5$

$\phi_5^{-1} = \phi_4$

also $\phi_3 \phi_2 = \phi_4$ & $\phi_2 \phi_3 = \phi_5$

$\therefore \phi_3 \phi_2 \neq \phi_2 \phi_3$

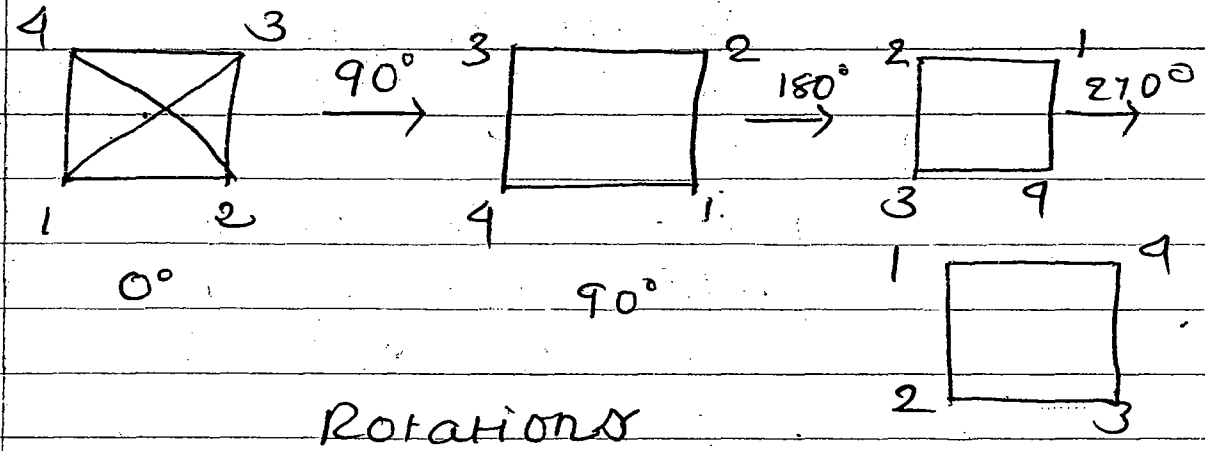
Hence S_3 is non abelian group

(3) P.T. symmetry of a square forms a group. P.T. it is non abelian group.

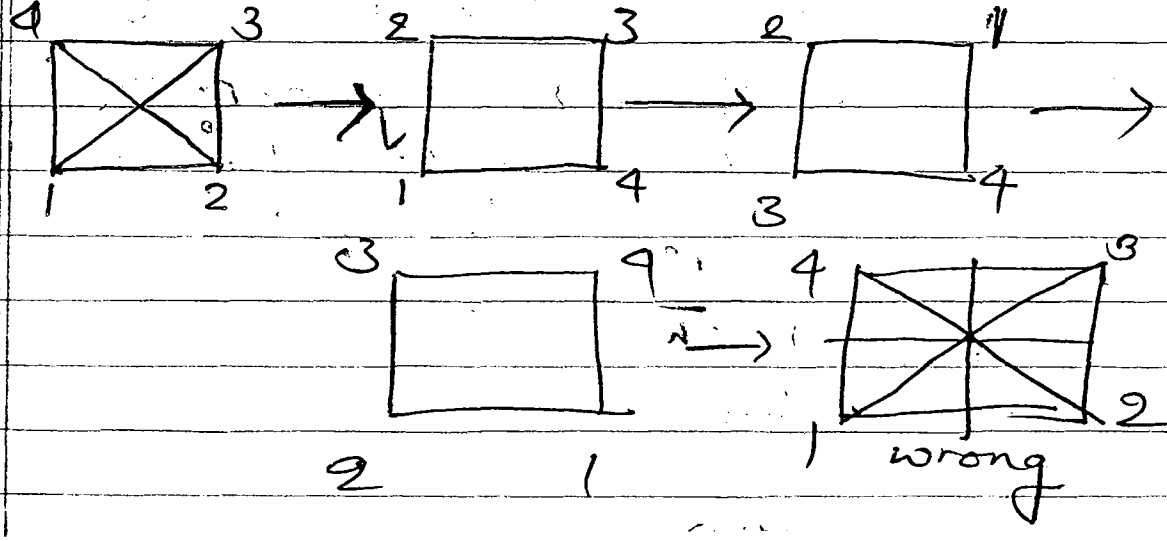
Soln:- Following transformation gives following symmetry on square

The four rotations about the centre through 0°, 90°, 180°, 270° respectively (anticlockwise).

The two reflections along the diagonal and the two refections along the horizontal & vertical bisectors.



Rotations



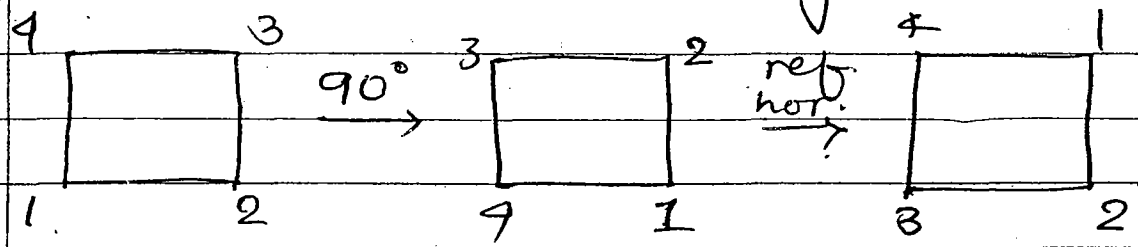
(i) Closure:-
Product of any two symm. is also a symm.

(ii) Ass.:-
product of symm. is always associative

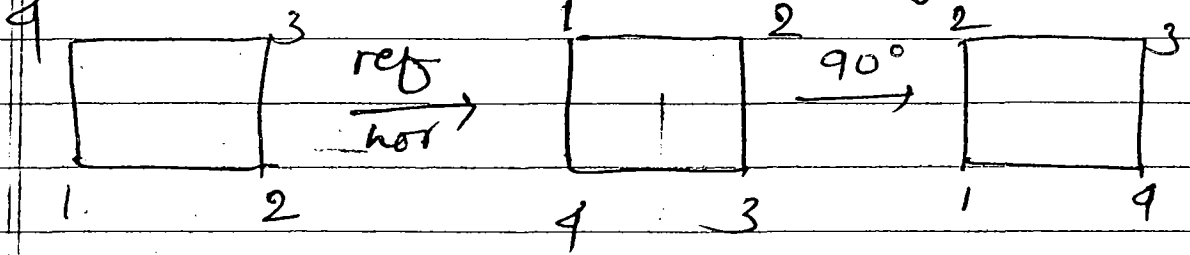
(iii) Identity:-
Rotation through 0° angle is identity.

(iv) Inverse:-
Inverse of 90° rotation is 270°
180° is 180° & 270° is 90°.
also inverse of any reflection is that reflection itself

Also.
rotation through 90° x reflection by horizonal bisector gives



but ref by hor. x rot. thr. 90° gives



Thus S_4 is non abelian group

(4) P.T. symm of square forms a non abelian group (by using per.) make multi. table for symm of square.

Similarly as ques. (2)

— x —.

RING-1

Date: 1/7/20

* **Ring:** A non empty set R with two binary operations '+' & '·' is said to be a ring if it satisfies the following conditions:

(1) $(R,+)$ is commutative group.
(2) $(R,\cdot)$ is semi group.
(3) multiplication is distributive over addition.

i.e. $a(b+c) = ab+ac$
& $(b+c)a = ba+ca$, $\forall\ a,b,c \in R$.

Ring ~~are~~ R with '+' & '·' is denoted by $(R,+,\cdot)$

* **Ring with unit element:**
Ring R is said to be a ring with unit element if $\exists\ e \in R$ ∋
$ae = ea = a$, $\forall\ a \in R$

* **Commutative ring:**
Ring R is said to be a commutative ring if $ab = ba$, $\forall\ a,b \in R$.

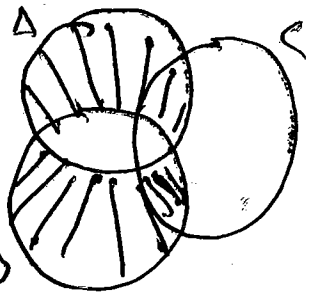
* **zero divisor:**
Let R be a ring and $a,b \in R$, $a \neq 0$, $b \neq 0$, for $ab = 0$.
(i.e $ab = 0 \Rightarrow a \neq 0$ & $b \neq 0$).
then a is said to be left zero divisor

Ex. $A * B = A \Delta B$, $\forall A, B \in G$

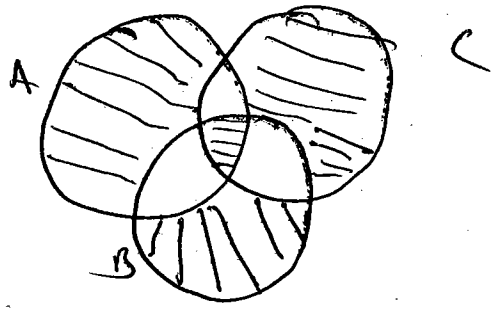
(i) $A * B = A \Delta B = (A - B) \cup (B - A) \in G$

(ii) P.T $(A * B) * C = A * (B * C)$

L-H-S

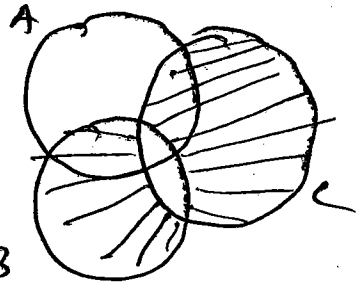


$A \Delta B = (A - B) \cup (B - A)$

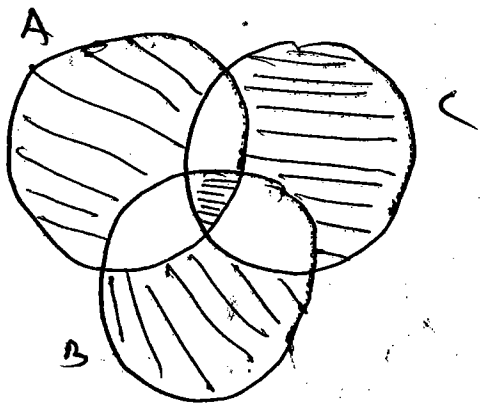


$(A \Delta B) \Delta C$

R.H.S



$(B \Delta C) = (B - C) \cup (C - A)$



$A \Delta (B \Delta C)$

Thus $A \Delta (B \Delta C) = (A \Delta B) \Delta C$

(iii) For any $A \in G$ $\exists E \in G \ni A * E = A$

$A \Delta E = A$

$\Rightarrow (A - E) \cup (E - A) = A$

$\Rightarrow \boxed{E = \phi}$

Thus $A = \phi \in G$ is identity element

(iv) For any $A \in G$, $\exists B \in G \ni A * B = \phi$.

$\because (A - B) \cup (B - A) = \phi \Rightarrow B = A$

Thus

$= (B - A) \cup (A - B)$
$= B * A$

Thus $(G, *)$ is comm. group.

Ex. P.T $[\bar{a}]^{-1} = a$, $\forall a \in G$
w.k.t G is group $\therefore a\bar{a}^{-1} = e = \bar{a}^{-1}a$
$\Rightarrow$ inverse of $\bar{a}$ is a
$\Rightarrow (\bar{a})^{-1} = a$

Ex. P.T $(ab)^{-1} = \bar{b}\bar{a}$, $\forall a, b \in G$
Soln
$(ab)(\bar{b}\bar{a}) = ab\bar{b}\bar{a} = a e \bar{a} = e$
Also $(\bar{b}\bar{a})(ab) = e$
$\Rightarrow (ab)^{-1} = \bar{b}\bar{a}$.

UNIT-2

Ex Find all cosets of $\{\pm 1\}$ in $\{\pm 1, \pm i\}$

Soln
W.K.T $H = \{\pm 1\}$, $G = \{\pm 1, \pm i\}$
$Ha = \{ha \mid h \in H\}$

$H1 = H$,	$1H = H$
$H(-1) = -H$	$(-1)H = -H$
$Hi = \{\pm i\}$	$iH = \{\pm i\}$
$H(-i) = \{\pm i\}$	$(-i)H = \{\pm i\}$

Hence H & $\{\pm i\}$ are only two distinct cosets of H in G.

Ex P.T Z_5^* is cyclic grp with generators $\bar{2}$ & $\bar{3}$

Soln $Z_5^* = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}\}$ & $(Z_5^*, \cdot)$ grp
$\langle \bar{2} \rangle = \{\bar{2}^n \mid n \in Z\} = \{\bar{1}, \bar{2}, \bar{4}, \bar{3}\} = Z_5^*$
$\langle \bar{3} \rangle = \{\bar{3}^n \mid n \in Z\} = \{\bar{1}, \bar{3}, \bar{4}, \bar{2}\} = Z_5^*$