$G \neq \phi$

$A \times B = \{(a,b) : a \in A, b \in B\}$

If $S \neq \phi$

$\rho \subseteq S \times S = \{(a,b) : a,b \in S\}$

↓ Binary relation defined in S

$\rho \subseteq S \times S \times S$

$|S| = n$, $P(S) = 2^n$

$[{}^nC_0 + {}^nC_1 + {}^nC_2 + \dots + {}^nC_n]$

no. of Binary relation $P(S \times S) = 2^{n^2}$

Equivalence relation Partially ordered relation

* $S \neq \phi$

$\rho \rightarrow$ Equivalence relation defined in S

$[a]_\rho = \{b \in S : a \rho b \text{ holds}\}$

↓ Equivalence class.

$Z_n = \{[0], [1], \dots [n-1]\}$

$a \rho b \Leftrightarrow a - b$ is divisible by n

$[a] = \{b \in Z_n : a \rho b \text{ holds}\}$

$= \{b \in Z : b - a \text{ is divisible by } n\}$

$= \{b \in Z : b - a = nt, \; b = a + nt\}$

* $S \neq \phi$

$\rho \rightarrow$ Equivalence relation defined on S.

$A_i \subseteq S$ $S = \cup A_i$ $A_i \cap A_j = \phi$

$\{A_i\}$ $i \in I$ $A_i = A_j$

Partition $\Leftrightarrow$ equivalence relation

2 partitions

3 partition

* Invertible :

$f : A \to B$
$g : B \to A$ | $\Rightarrow$ Bijective

$f \circ g = I$ (Identity

* $* : S \times S \to S$
$* : S \times S \times S \to S$
$\vdots$
$* : S \times S \times S \times \ldots \times S \to S$
(n times)

$|S| = n$

No. of binary relations = 2^{n^2}
$(S \times S)$

No. of Binary operations = n^{n^2}
$(\phi : S \times S \to S)$
$n^2 \quad n$
n^{n^2}

$f : A \to B$
$m \quad n$
n^m

* Quotient set of a set :

$S \neq \phi$, $\rho \to$ equivalence relation defined on P

Quotient set of a set $S/\rho = \{ [a]_\rho , a \in S \}$

* Algebric structure :

$S \neq \phi$ Binary operation [Not only binary relation]

$*$

↓

A special type of binary relation

$* : S \times S \to S$

↓

Binary composition / Binary operation.

$|A| = m$, $|B| = n$ $f : A \to B$

No. of mappings is n^m

No. of bijection is $n!$ $(n = m)$

No. of injective is ${}^nP_m$

[Injective :

$f(a) = f(b)$

$a = b$ $|A| \leq |B|$

Surjective :

if $x \in A$, $y \in B$

there exist $f(x) = y$. $|B| \leq |A|$

Bijective :

$|A| = |B|$]

$(Z, +)$

$+ : Z \times Z \to Z$

$(a, b) \to a + b$

$\cdot : Z \times Z \to Z$

$(a, b) \to a \cdot b$

$\cdot : Z^- \times Z^- \to Z^-$

$(a, b) \to a \cdot b$

} Not a binary operation . is not binary operation for Z^-.

[$* : S \times S \to S$

$a, b \in S$

$a * b \in S$

[$(Z, +)$ this means that if we take two element of Z and do binary operation '+' and the result is also the element of Z then the set is called algebric structure and is represented by $(Z, +)$

$a, b \in G$

closure : $a \circ b \in G$

Associative :

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

commutative :

$a \circ b = b \circ a$]

1. $(S, *) \rightarrow$ groupoid $\quad * : S \times S \rightarrow S$

Any non empty set with binary operation $(S, *)$ is called Groupoid.

(closure, Associative)

2. $(S, *) \rightarrow$ Semigroup if $*$ is associative.

$(a * b) * c = a * (b * c)$ for all $a, b, c \in S$

Associative property

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

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

3. $(S, *) \rightarrow$ Monoid $* : S \times S \rightarrow S$ (closure, Associative, existance of identity)

$e \in S$ is called identity of S if

$a * e = e * a = a$ for $a \in S$

e.g: $(N, \cdot) \Rightarrow 1 \cdot a = a \cdot 1 = a$.

[For every element $a \in G$, if there exists an element $b \in G$ such that $a * b = b * a = e_G$.

$a * a^{-1} = a^{-1} * a = e_G$

b is inverse of b; $b = a^{-1}$]

Let G be a non-empty set and $*$ be a binary operation defined on G then $(G, *)$ is called a group if the following condition holds:

1. $(a * b) * c = a * (b * c)$ for all $a, b, c \in G$ (Associative)
2. If $e_G \in G$ such that $a * e_G = e_G * a = a$ for all $a \in G$ (identity)
3. for every $a \in G$, if $b \in G$ such that $a * b = b * a = e_G$ (Commutative)

Group $\Rightarrow$ Monoid $\Rightarrow$ Semigroup $\Rightarrow$ Groupoid

$\not\Leftarrow$ $\not\Leftarrow$ $\not\Leftarrow$

$(Z, \cdot)$ $(N, +)$ $(Z, -)$

Group: $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$

Infinite commutative group

$(\mathbb{Q} \setminus \{0\}, \cdot)$, $(\mathbb{R} \setminus \{0\}, \cdot)$, $(\mathbb{C} \setminus \{0\}, \cdot)$

$(\mathbb{N}, \cdot)$ $\quad 1 \cdot a = a \cdot 1 = a$

4. $(S, *)$ Monoid if it is a semigroup together with identity.

$\begin{bmatrix} (\mathbb{N}, +) \rightarrow X \text{ not a monoid} \\ (\mathbb{N}, \cdot) \rightarrow \text{is a monoid} \end{bmatrix}$

GROUP

Let G be a non-empty set and $*$ be a binary operation defined on G.

$G \neq \phi$

$(a * b) * c = a * (b * c) \quad \forall \; a, b, c \in G$

if $e_g \in G$, $a * e_G = e_G * a = a$ if $a \in$

For identity of G.

- $\mathbb{Z}_n = \{[0], [1], \ldots [n-1]\}$

  $[a] \, z_n \, [b] = [a+b]$ for all $[a], [b] \in \mathbb{Z}_n$

  $[b] \, z_n \, [a] = [b+a]$ " " "

  $(\mathbb{Z}_n, +_n) \rightarrow$ commutative finite group.

  $[a] \cdot_n [b] = [ab]$ for all $[a], [b] \in \mathbb{Z}_n$

  $(\mathbb{Z}_n, \cdot_n)$ X Not a group.

  $[2][2] = [4] = [0]$

$U_n = \{ [a] \in \mathbb{Z}_n \setminus \{0\} , \gcd(a, n) = 1 \}$

Matrices

$M_{m \times n}(\mathbb{K})$

$(M_{m \times n}(\mathbb{K}), +)$ → form Group.

$A + O = O + A$ → Additive Inverse

$(M_{m \times n}(\mathbb{K}), \cdot) \longrightarrow \times$

$(\mathbb{Z}, \cdot)$, $(\mathbb{Q}, \cdot)$ → NO Groups

- Group G is said to be a commutative group if $a * b = b * a$ for all $a, b \in G$
- Finite Group

  $G = \{1, -1, i, -i\}$

  Inverse exist.
- Cyclic Group (Finite commutative)

  $G = \{1, \omega, \omega^2\}$
- $K_n = \{e, a, b, c\}$

  $a^2 = b^2 = c^2 = e$

  $ab = ba = c$

  $ac = ca = b$

  $bc = cb = a$

•	e	a	b	c
e				
a				
b				
c				

Q) $G = \left\{ \begin{pmatrix} a & a \\ a & a \end{pmatrix} : a \in \mathbb{R} \right\}$

$(G, +)$ ✓

Q) $G = \left\{ \begin{pmatrix} a & a \\ a & a \end{pmatrix} : a \in \mathbb{R} \neq 0 \right\}$

$(G, \cdot)$ $\qquad e_G = \begin{pmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{pmatrix}$

$$\begin{pmatrix} a & a \\ a & a \end{pmatrix}\begin{pmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{pmatrix} = \begin{pmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{pmatrix}\begin{pmatrix} a & a \\ a & a \end{pmatrix}$$

$$= \begin{pmatrix} a & a \\ a & a \end{pmatrix} \rightarrow \text{Identity}$$

$$A = \begin{pmatrix} a & a \\ a & a \end{pmatrix} \qquad B = \begin{pmatrix} b & b \\ b & b \end{pmatrix}$$

$$AB = BA = e_G = \begin{pmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{pmatrix}$$

$$\therefore B = \begin{pmatrix} 1/4a & 1/4a \\ 1/4a & 1/4a \end{pmatrix}$$

Finite non commutative group :

$S \neq \phi \qquad f : S \longrightarrow S$ (bijection)

* permutation

$B = \{ f : S \to S \mid f \text{ is bijective map} \}$

$(g \circ f)(x) = g(f(x))$ for all $x \in S$.

$(f \circ g) \circ h = f \circ (g \circ h)$

- $GL_n(\mathbb{R})$ → Non-singular matrix

$GL(n, \mathbb{R}) = \{ A \in M_{n \times n}(\mathbb{R}) : \text{Let } A \neq 0 \}$

↙ Infinite non-commutative groups)

↓ General Group of degree n.

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

- $SL(n, \mathbb{R}) = \{ A \in GL(n, \mathbb{R}) : \text{Let } A = 1 \}$

Infinite non-commutative groups

↓ Special linear group of degree n.

Ramij Rohit Shouvik Arnab Preeti

Permutation Group

- $S \neq \phi$
- $f : S \to S$

$f : A \to B$

$g : B \to B$

$gof = i_A$

$fog = i_B$

$A(S) = \{$collection of all permutations defination$\}$

$A(S) = \{ \sigma : \sigma$ is a permutation on $S \}$

$o : S \times S \to S$

$(\sigma_1 o \sigma_2)(x) = \sigma_1(\sigma_2(x))$ $\quad [\because (fog)x + (\sigma(x)]$

$S =$ finite set

$S = \{1, 2, \cdots, n\}$

$|A(S)| = n!$

$S_n = \{ \sigma : \sigma$ is a permutation on $S \}$

S_n ← Symmetric group of degree

$|S_n| = n!$ ← order of S.

Order of the group = length of the group.

Even permutation = Decomposte in even number of transposition.

Odd permutation : Decompose in odd number of transposition.

composition of odd-odd = even permutation

" " even-even = even permutation.

" " odd-even = Odd permutation.

* Collection of all even permutation form a group.

$A_n = \{\sigma \in S_n : \sigma \text{ is even}\}$

Alternative group of degree n

$\sigma_1, \sigma_2 \in S_n$

$\sigma_1 \circ \sigma_2 \in A_n$

$|A_n| = \frac{n!}{2}$.

* Collection of all odd permutation does not form a group.

* Any group of order less than 6 is always commutative.

S_n $(n \geq 3)$ Non-commutative group.

Order of an element in a group

G is a set

$a, b \in G$ $e_g \rightarrow$ identity element is unique.

a^{-1} is unique.

$ab \in G$

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

$ab = ac$ holds for any $a, b, c \in G$

$\Rightarrow b = c$

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

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

$\Rightarrow e_g b = e_g c$

$\Rightarrow b = c$

$(G, \cdot)$ Let G be a group and $a \in G$.

$o(a) = n$, $n \in N$ if there exists

$a^n = e_g$ = identity [·]

$n a = e_g$ [+]

$\mathbb{Z}_{10} = \{[0], [1], \cdots, [9]\}$

$(\mathbb{Z}_{10}, +) = [a] + [b] = [a+b]$

Every identity element has order 1

$o(e_g) = 1$.

$X \rightarrow$ infinite set

$(P(X), \Delta)$

$A + B = A \Delta B = (A - B) \cup (B - A)$

$A \Delta A = \phi$.

$A + A = \phi$

$2A = \phi$ [$\because nA = eg$.]

$n = 2$.

order = 2.

* $a \in G$ $G \rightarrow$ Group

$o(a) = n$

$o(a^t) = \dfrac{o(a)}{\gcd(o(a), t)}$

$a^n = e_G$ $m > n$ } m/n

$a^m = e_G$

$ab = ba$ and $\gcd(o(a), o(b)) = 1$

$o(ab) = o(a)\, o(b)$

Conjugate element

$b = xax^{-1} \quad \exists\, x \in G$

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

Subgroup

$(G, *) \rightarrow$ Group

$* : G \times G \rightarrow G$

$H \neq \phi \in G$

$(H, *) \rightarrow$ group.

$* : H \times H \rightarrow H$

Let G be a group and H be a non-empty set of G. Then H is a subgroup of G if and only if $ab^{-1} \in H \;\forall\; a, b \in H$

$ab \in H$

$b^{-1} \in H$

$G = (Z, +)$

$H = (N, +)$

$H \neq G$ $\quad H \rightarrow$ proper subgroup.

In a group G if every non identity element is of order 2 then G is a commutative group.

$a, b \in G$ $\quad ab \in G$

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

$= ba$

* Subgroup ∪ subgroup may not be subgroup

Subgroup ∩ subgroup = subgroup.

Let G be a group and H_1, H_2 be two subgroups of G. Then $H_1 \cap H_2$ is also a subgroups

$G = (\mathbb{Z}, +)$

$2 \in H_1 = 2\mathbb{Z}, 3 \in H_2 = 3\mathbb{Z}$

$H_1 \cup H_2$

$2 \in H_1 \subseteq H_1 \cup H_2$

$3 \in H_2 \subseteq H_1 \cup H_2$

Let G be a finite group. G is a cyclic group if and only if there exists an element $a \in G$, such that $o(a) = |G|$

Z_{10}, [1], [3] $Z_{10} = \langle [1] \rangle$

If a generator then a^{-1} as well generator.

Infite set = 2 generators [Always a and a^{-1}]

Subgroup of a cyclic group is a cyclic group.

Let G be a cyclic group. suppose $G = \langle a \rangle$

Let H be a subgroup of G.

$H = \{e_G\} = \langle e_G \rangle$

$H = G = \langle a \rangle$

$H \neq \{e_G\}$ $H \neq G$

$x \in H \subseteq G$ $x \in G$

$x = a^n$ $x \in H$

$a^n \in H$

$an^n \in H$

n is least +ve integer.

$a^n \in H$

$H = \langle a^n \rangle$

$\langle a^n \rangle \subseteq H$

$H \subseteq \langle a^n \rangle$

Let $b \in H = G$

$b \in G = \langle a \rangle$

$b = a^m, \quad m \in Z$

By Division algorithm,

$m = nq + r, \quad r = 0$

$r = m - nq$

$a^r = a^{m-nq} \in H$

$m = nq$

$b = a^m = a^{nq} = (a^n)^q \in \langle a^n \rangle$

Normal subgroup

Let G be a group and H be a subgroup of G

Left coset of H on G,

$$aH = \{ah : h \in H\}$$

Let $a, b \in G$

$$a \mathcal{L}_H b \iff a^{-1}b \in H$$

$$[a]_{\mathcal{L}_H} = \{b \in G : b \mathcal{L}_H a\} = aH$$

$$= \{b \in G : b^{-1}a \in H$$

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

$$a^{-1}b = h$$

$$b = ah$$

$aH \neq Ha \quad \forall a \in G$ Not always

Right coset H in G

$$aH = \{ah : h \in H\}$$

$$Ha = \{h'a : h' \in H'\}$$

$aH = Ha \quad \forall a \in G \longrightarrow$ Normal subgroup.

centre of G

$$Z(G) = \{a \in G : ab = ba \ \forall \ b \in G\}$$

$Z(G)$ is a sub group of G

$$a, b \in Z(G)$$

$$ab^{-1} \in Z(G)$$

$$gHg^{-1} \subseteq H$$

If commutative $G = Z(G)$

If G is commutative group then every subgroup

$ghg^{-1} = (gg^{-1})h = eh = h \in H$

Q $G = GL(n, \mathbb{R})$

$H = SL(n, \mathbb{R})$

$A, B \in SL(n, \mathbb{R})$

$AB^{-1} \in SL(n, \mathbb{R})$

$\det(AB^{-1}) = \det A \det(B^{-1})$

$= \det A \det(B^{-1})$

Lagrange's Theorem

Let G be a finite group and H be a subgroup of G. Then $|H|$ divides $|G|$ → order of G

↓ order of H

Left Poset or Right Poset

Let H be a subgroup of G.

Then for any $x \in G$

$aH = \{ah : h \in H\}$

$Ha = \{h'a : h' \in H\}$

$a \alpha_H b \Leftrightarrow a^{-1}b \in H$

$[x]_{\alpha H} = xH = \{xh : h \in H\}$

$y \in [x]_{\alpha H} \Rightarrow y \alpha_H x : y^{-1}x \in H$

$x^{-1}y \in H$

$y = xh$

Right Coset

$aR_H b \Leftrightarrow ab^{-1} \in H$

$[x]_{RH} = Hx = \{h'x : h' \in H\}$

$\boxed{xH \neq Hx}$

$\boxed{xH = Hx}$ → only for Normal subgroup

It is an equivalence relation

⇒ R_H has partioned G.

$$G = \bigcup_{x \in G} xH$$

$$x_i H \cap x_j H = \phi$$

$$G = \bigcup_{x \in G} Hx \qquad x_i H = x_j H \cdot i \neq j$$

* $|xH| = |Hx| = |H|$

Proof: $f : xH \longrightarrow H$

$f(xh) = h$

$|A| = |B|$

$f : A \to B$

$t : H \to Hx$

$t(h) = hx$

$t(h) = hx$

Index of a subgroup H of G

No. of Left Coset = No. of Right coset

= No. of distinct left Posets of H in G

= No. of " Right " " " "

To prove Lagrange's theorem,

~~$|G| = [G : H]\,[H]$~~

$$|G| = [G : H]\,|H|$$

Proof:

Since G is finite

$G \to \{x_1, \ldots\ldots x_n\}$

$xH = \{x_i H, \ldots\ldots\}$

⇒ Since G is finite index of $[G : H]$ is also finite = r (say)

Then $x_1 H, x_2 H, \ldots\ldots x_n H$ are the distinct left cosets of H in G.

Since the left coset form a partition of G.

So, $G = \bigcup_{i=1}^{x} x_i H$

$x_i H \cap x_j H = \phi$ if $i \neq j$

$|G| = |\bigcup_{i=1}^{x} H_i H| = |x_1 H| + |x_2 H| + \ldots + |x_n H|$

$[|xH| = |H|]$

$\Rightarrow |G| = |H| + |H| + \ldots + |H|$

$= x|H|$

Order of any subgroup must divide order of the group.

Converse of Lagrange's theorem always doesn't hold.

On a finite group G, for every divider of the order of G, there exists a subgroup H.

Holds only when a is a cyclic group.

→ Not only ~~when G is a cyclic group~~ existance of subgroup but also unique subgroup.

ex: $G = A_4$

$G = |A_4| = 12.$

$= 1, 2, 3, 4, 6, 12.$

If H & K are two finite subgroups ~~and~~ of a groups.

then $|HK| = \frac{|H||K|}{|H \cap K|}$

$[\because H \cap K = 1]$

$|HK| = |H||K|$

S_n

No. of distinct cycles of length r

$$= \frac{n!}{r(n-r)!}$$

S_4 = No. of 3-cycles in $S_4 = \frac{1}{3}\frac{3!}{(4-3)!} = 8$

$= (123)(132)(124)(142)$
$(234)(243)(134)(143)$

All 3-cycles are in even permutation

$(123) = (12)(13)$.

Suppose H is a subgroup of order 3.

No. of 3 cycles $= 8$

$\Rightarrow$ All three cycles cannot be in H since

$|H| = 6$.

$\Rightarrow$ There exists a 3 cycle α

i.e $\alpha \notin H$

$\because$ 3 cycle $\alpha^3 = e$

$\alpha^2 = \alpha^{-1} \in H$

K [constructing α such] $= \{e, \alpha, \alpha^2\}$

↓

forms a subgroup

$|K| = 3$.

~~$|H|$~~ & $|H|$ and ~~K~~ have only e in common

$$|HK| = \frac{|H||K|}{|H \cap K|} = 6 \cdot 3 = 18 > |A_4|$$

which is a contradiction.

$\Rightarrow$ A_4 doesnot have a subgroup of order 6

→ Any group of prime order is cyclic group.

Proof :

Let G be a group of prime order

then G is cyclic

$|G| = p$ = prime.

$p > 1$

G has an element $a \neq e$

Let $H = \langle a \rangle$

By Lagrange's theorem $|H|$ divides $|G|$

$|\langle a \rangle| = |H| \; |G| = p.$

$|\langle a \rangle| = 1$ and $|\langle a \rangle| = p$

since $\langle a \rangle$ is a non identity elements

$|\langle a \rangle| \neq 1.$

$\Rightarrow |\langle a \rangle| = p$

$H = \langle a \rangle \subseteq G$

$\Rightarrow G = H$

→ Order of an element of a finite group G must divides $|G|$.

→ Any Group of order 4 is commutative.

Proof :

$|G| = 4$

Suppose G is not cyclic.

$\Rightarrow$ G has no element of order 4.

Element order = {1, 2}

only e has order 1

$\Rightarrow$ Every element has order 2.

→ Any group of order < 6 is always commutative

$|G| = 1, \quad G = \{e\}$

$|G| = 2, 3, 5.$

Every cyclic group is commutative

$G = K_4 = \{e, a, b, c\}$

$a^2 = b^2 = c^2 = e$

$ab = ba = c$

$bc = cb = a$

$ac = ca = b.$

Every cyclic group is commutative.

Let G be a cyclic group.

Then $G = \langle a \rangle \quad a \in G.$

Let $x, y \in G = \langle a \rangle$

$x = a^m$

$y = a^n \quad m, n \in x$

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

$= a^{n+m}$

$= a^n a^m$

$= yx$

→ Any Group of order 2 where p is prime is always commutative.

$|G| = p^2$ is commutative.

p - is prime.

Let G be a group and $Z(G)$ be the centre of G.

$$Z(G) = \{a \in G : ab = ba \text{ if } b \in G\}$$

Quotient Group

Let G be a group and H be a normal subgroup of G.

consider $G/H = \{aH : a \in G\}$

$G/H = *$ $\quad * : G/H \times G/H \to G/H$

$(aH, bH) \to (aH) * (bH)$

$(aH) * (bH) = (ab)H \quad \forall\ aH, bH \in G/H$

$a \equiv b \pmod n$

$a + c \equiv b + c \pmod n$

$G = S_3 \quad H = A_3$

$[G : H] = 2$ then H's must are a most mad sub group converse doesnot hold.

$|G| = [G : H]\,|H|$

$\Rightarrow |G/H| = [G : H] = |G|/|H|$

Let G be a subgroup $Z(G)$ be the centre $O: G$ $G/Z(G)$ is cyclic

Then G is commutative

$$G(Z/G) = \langle gH \rangle$$

[$x, y \in G$ to show $xy = yx$]

$x, y \in G \quad xH, yH \in G/H$] Left coset

$$= \langle GH \rangle$$

$$xH = (GH)^m = g^m H$$

$$yH = (GH)^n = g^n H \quad m, n \in Z$$

$$x : xe \in xH = g^m H$$

$$x = g^m c \quad c \in H = Z(G)$$

$$y = ye \in yH = g^n H$$

$$y = g^n \alpha \quad \alpha \in H = Z/a$$

$$xy = (g^m c)(g^n \alpha)$$

$$= (g^m c)(\alpha g^n)$$

$$= c g^m \alpha g^n$$

$$= c\alpha\, g^m g^n$$

$$= c\alpha\, g^{m+n}$$

$$= (g^n \alpha)(g^m c)$$

$$= yx.$$

Let G be a non commutative ~~then~~ then

$$|Z(G)| \leq \frac{1}{4}|G|$$

$$\frac{|G|}{|Z(G)|} \geq 4 \quad \text{if } |G/Z(G)| = \frac{|G|}{|Z(G)|} \leq 3$$

$$|G/Z(G)| = 2 \text{ or } 3 \quad |G/Z(G)| \leq 3$$

Homo morphism and Iso morphism of Group

Let $(G, *)$ and $(G', \circ)$ be two groups. A mapping $f : G \to G'$ is called a homo morphism if $f(a * b) = f(a) \circ f(b)$ $\forall$ $a, b \in G$.

1) $f : R \to R^+$

$f(x) = e^x$ for all $x \in R$

$f(x+y) = e^{x+y} = e^x \cdot e^y$

$= f(x) \cdot f(y)$ $\forall$ $x, y \in R$

2) $G = (Z, +)$ $G' = (Z_n, +_n)$

$f : Z \to Z_n$ by $f(a) = [a]$ $\forall$ $a \in Z$

$f(a+b) = [a+b]$

$= [a] +_n [b] = f(a) +_n f(b)$

$\forall$ $a, b \in Z$

3) $G = (GL(n, R), \cdot)$

$G' = (R^*, \cdot) = (R - [0], \cdot)$

$f : GL(n, R) \to R^*$

$f(A) = \det A$

$f(AB) = \det(AB)$

$= \det A \det B$

$= f(A) f(B)$ $\forall$ $A, B \in GL(n, R)$

4. $G = (S_n, \circ)$ $G' = (Z_n, +)$

$f : G \to G'$ by

$$f(\sigma) = \begin{cases} [0] & \text{if } \sigma \text{ is even} \\ [1] & \text{if } \sigma \text{ is odd} \end{cases}$$

$f(\sigma_1 \circ \sigma_2) = f(\sigma_1) + f(\sigma_2) \quad \forall \sigma_1, \sigma_2 \in S_n$

i) $\sigma_1, \sigma_2 \to$ even

$f(\sigma_1, \sigma_2) = [0] = [0] + [0]$

$= f(\sigma_1) + f(\sigma_2)$

ii) σ_1 is odd, σ_2 is even

$f(\sigma_1 \circ \sigma_2) = [1] = [1] + [0]$

$= f(\sigma_1) + f(\sigma_2)$

iii) σ_1 is even, σ_2 is odd

$f(\sigma_1 \circ \sigma_2) = [1] = [0] + [1]$

$= f(\sigma_1) + f(\sigma_2)$

iv) $\sigma_1, \sigma_2 \to$ odd

$f(\sigma_1, \sigma_2) = [0] = [1] + [1]$

$= f[\sigma_1) + f(\sigma_2)$

$\therefore f$ is a homomorphism.

5. $G \to e_G \qquad G' \to e_{G'}$

If $f : G \to G'$ is homomorphism then it shows following properties:

i) $f(e_G) = e_{G'}$

ii) $f(a^n) = [f(a)]^n$

iii) $f(a^{-1}) = [f(a)]^{-1}$ $\forall$ any $a \in G$ and $n \in Z$

Let G and G' be two groups and $f: G \to G'$ be a homomorphism.

Then image of f, denoted by Imf and is defined by

$Imf = \{ f(x) = x \in G \} \to$ subgroup of G'

Kernel of f, denoted by $Kerf$ and is defined by

$Kerf = \{ x \in G : f(x) = e_{G'} \} \to$ subgroup of G
$\to$ Normal subgroup of G

Let $x, y \in Kerf$. Then $f(x) = e_{G'}$

$f(y) = e_{G'}$

$xy^{-1} \in Knf$

$f(xy^{-1}) = e_{G'}$

$f(xy^{-1}) = f(x) f(y^{-1})$

$= f(x) (f(y))^{-1}$ $[\because f(a^{-1}) = (f[a])^{-1}]$

$= e_{G'}$

Let $g \in G$ $h \in Kerf \Rightarrow f(h) = e_{G'}$

$f(ghg^{-1}) = e_{g'}$

$ghg^{-1} \in Kerf$

$f(ghg^{-1})$

$= f(g) f(h) f(g^{-1})$

$= f(g) e_{G'} (f(g))^{-1}$

$= f(g) [f(g)]^{-1} = e_{G'}$

Let G and G' be two groups and $f: G \to G'$ be a homomorphism.

Then f is called a monomorphism if f is injective f is called an isomorphism if f is surjective.

f is called an isomorphism if f is bijective

$f: G \to G'$ isomorphism

$G \cong G'$

$f: G \to G$ → Isomorphism.

Automorphism

$Ant(G) = \{ f: G \to G \mid f$ is an automorphism $\}$.

$f, g \in Ant(G)$

$(f \circ g) \circ h = f \circ (g \circ h)$

$(Ant(G), \circ)$ → Automorphism group.

Inner Automorphism

Let G be a group and $g \in G$.

Define a mapping $f_g: G \to G$ by

$f_g(x) = gxg^{-1} \quad \forall \; x \in G$

$f_g(xy) = g(xy)g^{-1}$

$= gx(g^{-1}g)yg^{-1}$

$= (gxg^{-1})(gyg^{-1})$

$= f_g(x) f_g(y)$

$Inn(G) = \{ f_g: G \to G \}$

$f: G \to G$

$f(H) \subseteq H$

H is called a characteristic subgroup of G if $f(H) \subseteq H$ for any automorphism.

$f_g : G \to G$ $\quad H \to$ subgroup of a group

$f_g(H) \subseteq H$ i.e $gHg^{-1} = c$.

First Isomorphism Theorem

Let G and G' be two groups and $f: G \to G'$ be an epimorphism.

Then $G'_{\ker} \cong G'$.

Proof: Define a mapping $\phi : G/\ker \to G'$

$\phi(a\ker) = f(a) \quad \forall\ a\ker \in G/\ker$.

$\phi(a\ker) = \phi(b\ker)$

$\Rightarrow f(a) = f(b)$

$\Rightarrow f(a)[f(b)]^{-1} = e_{G'}$

$\Rightarrow f(a) f(b^{-1}) = e_{G'}$

$\Rightarrow f(ab^{-1}) = e_{G'}$

$\Rightarrow ab^{-1} \in \ker f$ $\quad [\because aH = bH \Rightarrow ab^{-1} \in H]$

$\Rightarrow a\ker = b\ker$

Also,

$a\ker = b\ker$

$ab^{-1} \in \ker f$

$f(ab^{-1}) = e_{G'}$

$f(a) f(b^{-1}) = e_G$

~~$f(ab) = e'$~~

$f(a)\,[f(b)]^{-1} = e_{G'}$

$\Rightarrow f(a) = f(b)$

$\therefore \phi$ is injective.

$f : G \to G'$

$\exists\ x \in G$

$f(a) \in G'$

$f(x) = y$

Let $y \in G'$ Since f is surjective.

$\exists\ x \in G$ s.t. $f(x) = y$

$y = f(x) = \phi\ (x\,\text{ker}f)$

$\exists\ x\,\text{ker}f \in G/\text{ker}f$ s.t $\phi\,(x\,\text{ker}f) = y$.

$\therefore \phi$ is surjective.

$\phi\,[(a\,\text{ker}f)(b\,\text{ker}f)]$

$= \phi\,[(ab)\,\text{ker}f]$

$= f(ab)$

$= f(a)\,f(b) = \phi\,[a_{\text{ker}f}]\,[b_{\text{ker}f}]$

for all $a\,\text{ker}f,\ b\,\text{ker}f \in G/\text{ker}f$.

$\therefore \phi$ is homomorphism.

$\because \phi$ is injective, surjective, and homomorphism.

$\therefore \phi$ is isomorphism.

2. $\mathbb{Z}/n\mathbb{Z} \cong Z_n$

Define a mapping $\phi : \mathbb{Z} \to Z_n$ by

$\phi(a) = [a] \quad \forall \ a \in \mathbb{Z}$

Now,

$\ker \phi = \{a \in \mathbb{Z} : \phi(a) = [0]\}$

$= \{a \in \mathbb{Z} : [a] = [0]\}$

$= \{a \in \mathbb{Z} : a = nt \text{ for some } t \in \mathbb{Z}\}$

$= n\mathbb{Z}$

3. Define a mapping

$\phi : GL(n, \mathbb{R}) \to \mathbb{R}^*$ by

$\phi(A) = \det A$ for all $A \in GL(n, \mathbb{R})$

$\exists X = \begin{pmatrix} x & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$ $\quad \phi(X) = x$

$GL(n, \mathbb{R}) / SL(n, \mathbb{R})$

$\phi(A) = \det A$ for all $A \in GL(n, \mathbb{R})$

$\ker \phi = \{A \in GL(n, \mathbb{R}) : \phi(A) = 1\}$

$= \{A \in GL(n, \mathbb{R}) : \det A = 1\}$

$= SL(n, \mathbb{R})$

$F \to$ finite field $\quad |F| = q$

$[GL(n, \mathbb{R}) : SL(n, F)] = ??$

$GL(n,F)/SL(n,F) \cong F^* = F - \{0\}$

$G \cong G'$ [$\because$ two groups are isomorphism]

$|G| = |G'|$

$|GL(n,F)/SL(n,F)| = |F - \{0\}|$

$= q - 1$

$[G : H] = |G/H| = \frac{|G|}{|H|}$

$|G| = [G : H]\,|H|$

$S_n/A_n \cong Z_2$

Define a mapping $\phi : S_n \to Z_n$ by

$$\phi(\sigma) = \begin{cases} [0] & \text{if } \sigma \text{ is even} \\ [1] & \text{if } \sigma \text{ is odd.} \end{cases}$$

$S_n/\ker\phi \cong Z_2$

$\ker\phi = \{\sigma \in S_n : \phi(\sigma) = [0]\}$

$= \{\sigma \in S_n : \sigma \text{ is even}\}$

$= A_n.$

$|S_n/A_n| = |Z_2| = 2$

$\Rightarrow \frac{|S_n|}{|A_n|} = 2$

$\Rightarrow \frac{n!}{|A_n|} = 2 \Rightarrow |A_n| = \frac{n!}{2}.$

5. Show that any epimorphism from $(Z, +)$ onto itself is a isomorphism.

$f : Z \to Z$

$Z/\ker \cong Z \qquad nZ,\ n = 0,\ n \in N$

$\ker = \{0\}$

To prove: $\ker \neq nZ, n \in N$

If possible, be $\ker = nZ, n \in \mathbb{N}$

$Z/nZ \cong Z$

$Z_n \cong Z$ [Not true], which is a contradiction

becoz Z_n is finite Z is finite

$\therefore f$ is injective

Let G and G' be two groups and $f : G \to G'$ be a homomorphism then f is a monomorphism if and if $\ker f = \{e_G\}$

Let f be an injective map.

Let $x \in \ker f$ then $f(x) = e_{G'} = f(e_G)$

$\Rightarrow f(x) = f(e_G)$

$\Rightarrow x = e_G$

converse:

Let $\ker = \{e_G\}$

Let $x, y \in G$ s.t $f(x) = f(y)$

$\Rightarrow f(x) f(y^{-1}) = e_{G'}$

$\Rightarrow f(xy^{-1}) = e_{G'}$

$\Rightarrow xy^{-1} \in \text{ker} = \{e_4\}$

$\Rightarrow xy^{-1} = e_4$

$\Rightarrow x = y$

1. Does there exists an empimorphism from $(Z_6, +)$ onto $(Z_4, +)$?

2. Any finite cycle group of order n is isomorphic to Z_n any infinite cyclic group is isomorphic to Z.

Ans = 1) $f : Z_6 \to Z_4$

By first isomorphism theorem,

$$Z_6 / \text{ker} \cong Z_4$$

$$\left|\frac{Z_6}{\text{ker}}\right| = |Z_4|$$

$$\Rightarrow |\text{ker}| = \frac{|Z_6|}{|Z_4|} = \frac{6}{4} = \frac{3}{2} \notin \mathbb{N}$$

which is a contradiction.

Ans = 2) No. of homomorphism from $Z_m \to Z_n$ is $d = \gcd(m, n)$

$f : G \to G_1$

$f(a) = e_g'$ of $a \in G$.

$|G| = 1, \quad G \cong \{e_4\}$

$|G| = 2, \quad G \cong Z_2$

$|G| = 3, \quad G \cong Z_3$

$|G| = 4, \quad G \cong Z_4, \quad G \cong K_4 \cong Z_2 \times Z_2$

$|G| = 5, \quad G \cong Z_5$

$G \cong S_3$