NELCO

Sweet Chocolate

my FAVOURITE

soorajcs1989@gmail.com · +91-9400685988

INDEX

Appendix : 2-D
Group Theory

Name: SOORAJ S. Sub:

Std: Div: Roll No:

S. No	Topic	Page No	Date	Grade/ Marks	Signature
	QUANTUM COMPUTATION & QUANTUM INFORMATION				
	- Nielsen & Chuang.				

Cyclic Group

* A group G is called a cyclic group if $G = \langle \{a\} \rangle$ for some $a \in G$. We usually write $\langle \{a\} \rangle$ as $\langle a \rangle$. i.e.,

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

i.e.,

In group theory, a branch of abstract algebra a cyclic group is a group that is generated by a single element. That is, it contains an element 'a' such that every other element of the group may be obtained by repeatedly applying the group operation to 'a' or its inverse. This element 'a' is called a generator of the group.

Inverse of generator of cyclic group is generator, i.e., $\langle a \rangle = \langle a^{-1} \rangle$ for any $a \in G$.

Theorem 7: Every cyclic group is abelian (Not every abelian group is cyclic)

A subgroup H of a group G is called a cyclic subgroup if it is a cyclic group.

- If $K \leq G$ and $a \in K$, then $\langle a \rangle \leq K$

since $\langle a \rangle$ is the smallest subgroup of G containing a.

- All the elements of $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$ may or may not be distinct.

Ex:- Take $a = (1\ 2) \in S_3$

Then,
$\langle (1\ 2) \rangle = \{I, (1\ 2)\}$ since $(1\ 2)^2 = I$, $(1\ 2)^3 = (1\ 2)$
and so on.

$$(1\ 2) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

(OR)

Let G be a group with operation $\times$

For $a \in G$,

'what's the smallest subgroup of G that contains 'a' ?

$\langle a \rangle = \{ \ldots, a^{-3}, a^{-2}, a^{-1}, 1, a, a^2, a^3, \ldots \}$

= group generated by 'a'

= smallest subgroup of G containing 'a'

If $G = \langle a \rangle$ for some a, then we call G a cyclic group.

Let H be a group with operation $+$

For $b \in H$,

$$\langle b \rangle = \{\dots, -3b, -2b, -b, 0, b, 2b, 3b, \dots\}$$

= group generated by b

= smallest subgroup of H containing b

If $H = \langle b \rangle$ for some b, then we call H a cyclic group.

Ex:-

Group : Integers $\mathbb{Z}$ under +

Claim : $\mathbb{Z} = \langle 1 \rangle$

$\langle 1 \rangle = \{ \ldots, -4, -3, -2, -1, 0, 1, 2, 3, 4, \ldots \}$

$\Rightarrow$ $\mathbb{Z}$ is a cyclic group

(infinite cyclic group)

Ex:- Group: G_1 = Integers mod n under addition

$= \mathbb{Z}/n\mathbb{Z}$

$= \{0, 1, 2, \ldots, n-1\}$

G_1 is cyclic : $G = \langle 1 \rangle$

$-2, -1, 0, 1, 2, \ldots, n-1, n, n+1, n+2, \ldots, 2n-1, 2n, 2n+1, \ldots$

$n-2, n-1, 0, 1, 2, \ldots, n-1, 0, 1, 2, \ldots, n-1, 0, 1, \ldots$

$\Rightarrow$ $\mathbb{Z}/n\mathbb{Z}$ is a finite cyclic group under addition

Cyclic groups

Infinite : $(\mathbb{Z}, +)$

Finite : $(\mathbb{Z}/n\mathbb{Z}, +)$

$\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z}$, ...

..., Trivial group : $\{e\}$.

(E.11) Show that if $G \neq \{e\}$ then $G \neq \langle e \rangle$

Ans: $G \neq \{e\} \longrightarrow a \neq e$ in G

$a \neq e \rightarrow a \neq e^r$ for any $r \in \mathbb{Z}$

$\therefore a \notin \langle e \rangle$

$\therefore G \neq \langle e \rangle$.

(E.12) Inverse of generator of cyclic group is generator, i.e., $\langle a \rangle = \langle a^{-1} \rangle$ for any $a \in G$

Proof

Any element of $\langle a \rangle$ is a^n, for $n \in \mathbb{Z}$

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

$\therefore a^n \in \langle a^{-1} \rangle \longrightarrow \langle a \rangle \subseteq \langle a^{-1} \rangle$

Similarly, $\langle a^{-1} \rangle \subseteq \langle a \rangle$

$\therefore \langle a \rangle = \langle a^{-1} \rangle$

* **Theorem 7:** Every cyclic group is abelian.

Proof

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

For any x, y in G there exists $m, n \in \mathbb{Z}$ such that $x = a^m$, $y = a^n$

Then,

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

$\Rightarrow xy = yx$ for all $x, y \in G$.

$\therefore$ G is abelian

Note: every abelian group is not cyclic.

Ex-7

Ex-7 Consider the set $K_4 = \{e, a, b, ab\}$ and the binary operation on K_4 given by the table,

$\cdot$	e	a	b	ab
e	e	a	b	ab
a	a	e	ab	b
b	b	ab	e	a
ab	ab	b	a	e.

$\Longrightarrow$ $(K_4, \cdot)$ is a group, and this group is called the Klein 4-group.

$\Longrightarrow$ K_4 is abelian but not cyclic

Q.C Check groupoidness for similar proof Gr. 4

H2

D.L.G.T ①

Define the set $S = \{t \in N \mid x^t \in H\}$

$= \{t \mid t > 0, x^t \in H\}$

Since $H \neq \{e\}$, there is a non-zero integer n such that $x^n \in H$.

i.e., $\exists\ n \in \mathbb{Z}$ such that $x^n \in H$, $n \neq 0$

If $n > 0$ then $n \in S$, and

If $n < 0$ then ~~$n \in S$~~ $-n \in S$;

since $x^{-n} \in H$ and $-n > 0$.

[Since H is a subgroup, $(x^n)^{-1} = x^{-n} \in H$]

$\therefore$ There exists a positive integer m (n or $-n$) such that $x^m \in H$

Hence. $S \neq \emptyset$

$\Rightarrow$

Well-ordering Principle:

- Every non-empty set of +ve integers contain a least element

$\rightarrow$ S has a least element, say k

i.e., k is the least +ve integer that x^k belongs to H.

$$(x^k)^2 \in \langle x^k \rangle$$

② Consider any element $x^{qk} \in \langle x^k \rangle$

If $q=0$ then $x^{qk} = x^0 = e \in H$

If $q>0$, then $x^{qk} = \underbrace{x^k \cdots x^k}_{q \text{ times}} \in H$ [$a, b \in H \Rightarrow ab \in H$]

If $q<0$, then $x^{qk} = \underbrace{x^{-k} \cdots x^{-k}}_{-q \text{ times}} \in H$

$\therefore x^{qk} = (x^k)^q \in H \quad \forall\ q \in \mathbb{Z}$

$\therefore \langle x^k \rangle \subseteq H$ $\longleftarrow$

⑥ Let $x^n \in H$.

$$k \overline{)\, n \;\; m \;\; r}$$

Division algorithm : $n = mk + r$

where $m, r \in \mathbb{Z}$,

$0 \leq r < k$

$$x^r = x^{n-mk} = x^n \cdot x^{-mk} = x^n (x^k)^{-m} \in H$$

since $x^n, x^k \in H$

k is the least +ve integer such that $x^k \in H$

$\therefore x^r \in H$ iff $r = 0$.

Then, $n = mk$ and $x^n = x^{mk} = (x^k)^m \in \langle x^k \rangle$

$\therefore H \subseteq \langle x^k \rangle$

$\longrightarrow H = \langle x^k \rangle$

$\therefore H$ is cyclic

* Corol

* **Corollary:** Let $H \neq \{e\}$ be a subgroup of $\langle a \rangle$. Then $H = \langle a^n \rangle$

where, n is the least +ve integer such that $a^n \in H$.

(E-15) Obtain all the subgroups of Z_4 $(Z_4 = \langle \bar{1} \rangle)$

Ans: Since Z_4 is cyclic, all its subgroups are cyclic.

∴ Its subgroups are:

$Z_4, \langle \bar{2} \rangle, \langle \bar{3} \rangle, \{\bar{0}\}$.

Cosets

Q.C.G.T

* Let G be a group and H, K be non-empty subsets of G. The product of H and K is the set,

$$HK = \{hk \mid h \in H, k \in K\}$$

* Let H and K be subgroups of a group G. Then HK is a subgroup of G iff $HK = KH$.

i.e., If H & K are subgroups of an abelian group G, then HK is a subgroup of G

$$\left.\begin{matrix} H \leq G \\ K \leq G \end{matrix}\right\} \; HK \leq G \text{ iff } HK = KH$$

We'll look at the case when one of the subsets consists of a single element only.

$H\{x\} = \{hx \mid h \in H\}$, where H is a subgroup of a group G and $x \in G$.

We will denote $H\{x\}$ by Hx.

* Let H be a subgroup of a group G, and let $x \in G$. The set $Hx = \{hx \mid h \in H\}$ is called a right coset of H in G.

The element x is a representative of Hx.

Similarly,

the left coset of H in G is defined as, $xH = \{xh \mid h \in H\}$.

Note: If the group operation is $+$, then the right and left cosets of H in $(G,+)$ represented by $x \in G$ are

$$H+x = \{h+x \mid h \in H\} \quad \text{and} \quad x+H = \{x+h \mid h \in H\}.$$

Ex: 1 Show that H is a right as well as a left coset of a subgroup H in a group G.

Ans:

Consider the right coset of H in G represented by e the identity of G.

Then,

$He = \{he \mid h \in H\} = \{h \mid h \in H\} = H$

Similarly, $eH = H$

$\therefore$ H is a right as well as left coset of H in G.

Ex: 2 What are the right cosets of $4\mathbb{Z}$ in $\mathbb{Z}$?

Ans $H = 4\mathbb{Z} = \{\cdots, -8, -4, 0, 4, 8, \cdots\}$

The right cosets of H are,

$H+0 = H$

$H+1 = \{\cdots, -7, -3, 1, 5, 9, \cdots\}$

$H+2 = \{\cdots, -6, -2, 2, 6, 10, \cdots\}$

$H+3 = \{\cdots, -5, -1, 3, 7, 11, \cdots\}$

$H+4 = \{\cdots, -4, 0, 4, 8, 12, \cdots\} = H$

Similarly, $H+5 = H+1$, $H+6 = H+2$, $\cdots$ so on.

∴ the distinct right cosets are $H, H+1, H+2, H+3$.

- The distinct right cosets of $H(=n\mathbb{Z})$ in $\mathbb{Z}$ are $H, H+1, \ldots, H+(n-1)$.

Similarly,
the distinct left cosets of $H(=n\mathbb{Z})$ are $H, 1+H, 2+H, \ldots, (n-1)+H$.

* Theorem

and

(a) $x \in$

(b) Hx

(c) Hx

Proof

(a) e

(b) Assu

x

Conver

Any e
$he H$.

$he H$

* **Theorem 4.1**: Let H be a subgroup of a group G and let $x, y \in G$. Then,

(a) $x \in Hx$

(b) $Hx = H \iff x \in H$

(c) $Hx = Hy \iff xy^{-1} \in H$

Proof

(a) $e \in H$ and $x = ex$

$\Rightarrow x \in Hx$

(b) Assume that $Hx = H$,

$x \in Hx \longrightarrow x \in H$

Conversely,

Assume that $x \in H$,

Any element of Hx is of the form hx, where $h \in H$. i.e., $hx \in Hx$

$h \in H$ & $x \in H \Longrightarrow hx \in H$

$\therefore Hx \subseteq H$

Let $h \in H$, then $h = (hx^{-1})x$

$x \in H \Longrightarrow x^{-1} \in H \Longrightarrow hx^{-1} \in H$ as $h \in H$

$\therefore \; h = (hx^{-1})x \in Hx$

$\therefore H \subseteq Hx$

$\Longrightarrow$ $H = Hx$ whenever $x \in H$

(c)

$Hx = Hy$,

$\Longrightarrow Hxy^{-1} = Hyy^{-1} = He = H$

$\Longrightarrow xy^{-1} \in H$

[since $Hx = H \Longleftrightarrow x \in H$ Theorem 4.1(b)]

Conversely,

$xy^{-1} \in H \Longrightarrow Hxy^{-1} = H$ [since $x \in H \Longleftrightarrow Hx = H$]

$\Rightarrow Hxy^{-1}y = Hy$

$\Rightarrow Hx = Hy$

Similarly,

If H is a subgroup of G and $x, y \in G$, then

(a) $x \in xH$

(b) $xH = H \iff x \in H$

(c) $xH = yH \iff x^{-1}y \in H$

Ex: 3 Let $G = S_3 = \{I, (1\,2), (1\,3), (2\,3), (1\,2\,3), (1\,3\,2)\}$ and H be the cyclic subgroup of G generated by $(1\,2\,3)$. Obtain the left cosets of H in G.

Sol: $(1\,2\,3) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$

$$(1\,2\,3)\cdot(1\,2\,3) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}\cdot\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (1\,3\,2)$$

$$(1\,2\,3)\cdot(1\,2\,3)\cdot(1\,2\,3) = (1\,2\,3)\cdot(1\,3\,2)$$

$$= \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}\cdot\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = I$$

$$\therefore H = \langle (1\,2\,3) \rangle = \{I, (1\,2\,3), (1\,3\,2)\}$$

The left cosets of H in G are:

- $IH = H = \{I, (1\,2\,3), (1\,3\,2)\}$
- $(1\,2)H = \{(1\,2), (1\,2)\cdot(1\,2\,3), (1\,2)\cdot(1\,3\,2)\}$
  $= \{(1\,2), (2\,3), (1\,3)\}$

$$(1\,2)^{-1}\cdot(1\,3) = (1\,2)\cdot(1\,3) \quad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}\cdot\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (1\,3\,2) \in H$$

$$(1\,2)^{-1}\cdot(2\,3) = (1\,2)\cdot(2\,3) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}\cdot\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1\,2\,3) \in H$$

$xH = yH \Leftrightarrow xy^{-1} \in H$ $\Big\}$ $(1\,2)H = (2\,3)H = (1\,3)H$

$x \in H \iff xH = H$

$(1\ 2\ 3)H = H = (1\ 3\ 2)H$

$\therefore$ The distinct left cosets of H are:

H and $(1\ 2)H$.

(E.1) Obtain the left & right cosets of $H = \langle (1\ 2) \rangle$ in S_3. Show that $Hx \neq xH$ for some $x \in S_3$

$S_3 = \{I, (12), (13), (23), (1\ 2\ 3), (1\ 3\ 2)\}$

Ans: $(1\ 2) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$

$(1\ 2) \cdot (1\ 2) = (1\ 2)$

$\Rightarrow H = \langle (1\ 2) \rangle = \{I, (1\ 2)\}$

Left cosets are: $H, (1\ 2)H, (1\ 3)H, (2\ 3)H, (1\ 2\ 3)H, (1\ 3\ 2)H$

$x \in H \iff xH = H$ $\}$ $(1\ 2)H = H$

$(1\,2\,3)H = (1\,3)H$; $(1\,3\,2)H = (2\,3)H$

$\therefore$ The distinct left cosets of H in S_3 are:

$$H, (1\,3)H, (2\,3)H$$

Similarly,

the distinct right cosets of H in S_3 are,

$$H, H(1\,3), H(2\,3)$$

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

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

$\rightarrow (1\,3)H \neq H(1\,3)$

$(2\,3)H \neq H(2\,3)$

Quaternion group

Ex: 4 Consider the following set of eight 2×2 matrices over $\mathbb{C}$.

$Q = \{\pm I, \pm A, \pm B, \pm C\}$ where

$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, $A = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$, $B = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}$, $C = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}$

such that $I^2 = I$ & $A^2 = B^2 = C^2 = -I$,

$AB = C = -BA$, $BC = A = -CB$, $CA = B = -AC$

$\therefore Q_8$ is a non-abelian group under matrix multiplication.

Show that the subgroup $H = \langle A \rangle$ has only two distinct right cosets in Q_8.

Ans: $H = \langle A \rangle = \{I, A, A^2, A^3\} = \{I, A, -I, -A\}$

$HB = \{B, C, -B, -C\}$

$Hx = x \iff x \in H$

$H = HI = HA = H(-I) = H(-A)$

$Hx = Hy \iff xy^{-1} \in H$

$BC^{-1} = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix} \begin{bmatrix} -i & 0 \\ 0 & i \end{bmatrix} = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} = -A \in H$

$\therefore \quad HB = HC = H(-B) = H(-C)$

$\longrightarrow$ $\therefore$ H has only 2 distinct cosets in G_8 : H, HB.

(E·2) Show that $K = \{I, -I\}$ is a subgroup of Q_8. Obtain all its right cosets, in Q_8.

Ans: Since $ab^{-1} \in K \;\forall\; a, b \in K \Longrightarrow K \leq Q_8$

$K = KI = K(-I)$.

$(-A)A^{-1} + (B)B^{-1} + (C)C^{-1} = -I \in K$.

$\Longrightarrow KA = K(-A) = \{A, -A\}$

$KB = K(-B) = \{B, -B\}$

$KC = K(-C) = \{C, -C\}$.

Define: Let H be a subgroup of a group G. We define a relation '$\sim$' on G by $x \sim y$ iff $xy^{-1} \in H$ where $x, y \in G$.

i.e., $x \sim y$ iff $Hx = Hy$

Theorem 2: Let H be a subgroup of a group G. Then the relation '$\sim$' defined by $x \sim y$ iff $xy^{-1} \in H$ (i.e., $x \sim y$ iff $Hx = Hy$) is an equivalence relation.

The equivalence classes are the right cosets of H in G, i.e., $[x] = Hx$

Remark: If Hx and Hy are 2 right cosets of a subgroup H in G, then $Hx = Hy$ or $Hx \cap Hy = \phi$.

$\Rightarrow$ Any subgroup H of a group G partitions G into disjoint right cosets.

Proof.

For any $x \in G$, $xx^{-1} = e \in H$

$\therefore x \sim x$, i.e., '$\sim$' is reflexive

If $x \sim y$ for any $x, y \in G$, then $xy^{-1} \in H$

$\therefore (xy^{-1})^{-1} = yx^{-1} \in H$

$\therefore y \sim x$, i.e., $\sim$ is symmetric.

If $x, y, z \in G$ such that $x \sim y$ and $y \sim z$, then, $xy^{-1} \in H$ and $yz^{-1} \in H$

$$(xy^{-1})(yz^{-1}) = x(y^{-1}y)z^{-1} = xz^{-1} \in H$$

$\therefore x \sim z$, i.e., '$\sim$' is transitive

Thus, '$\sim$' is an equivalence relation.

The equivalence class determined by $x \in G$ is,

$$[x] = \{y \in G \mid y \sim x\} = \{y \in G \mid xy^{-1} \in H\}$$

Let $y = [x]$,

$$xy^{-1} \in H \longrightarrow Hx = Hy$$

$$y \in Hy \longrightarrow y \in Hx$$

$$\therefore \quad [x] \subseteq Hx$$

For any $hx \in Hx$,

$$x(hx)^{-1} = xx^{-1}h^{-1} = h^{-1} \in H$$

$\therefore hx \sim x$, i.e., $hx \in [x]$. for all $hx \in Hx$

$$\therefore \quad Hx \subseteq [x]$$

$$\longrightarrow \underline{[x] = Hx} \; .$$

Theorem 1.1: Let R be an equivalence relation on a set S. For $a \in S$, let $[a]$ denote the equivalence class of a. Then,

(a) $a \in [a]$

(b) $b \in [a] \iff [a] = [b]$

(c) $S = \bigcup_{a \in S} [a]$

(d) if $a, b \in S$ then $[a] \cap [b] = \phi$

(or) $[a] = [b]$

Proof

- An equivalence relation R on a set S divides S into a number of mutually disjoint subsets, i.e., it partitions S called equivalence classes.

Let $a \in S$. Then the set $\{b \in S \mid aRb\}$ is called the equivalence class of a in S, i.e., $[a]$. It is just the set of elements in S which are related to a.

$$[a] = \{b \in S \mid aRb\}$$

(a) R is an equivalence relation.

$\therefore$ R is reflexive

$aRa \;\forall\; a \in S \implies a \in [S]$

(b) Assume that $b \in [a]$, i.e., aRb

Let $x \in [a]$ then xRa and we also know that aRb.

Transitivity of $R \implies xRb$, i.e., $x \in [b]$

$\therefore [a] \subseteq [b]$

Similarly, $[b] \subseteq [a]$.

$\longrightarrow [a] = [b]$

Conversely, assume that $[a] = [b]$,

then $b \in [b] = [a] \implies b \in [a]$

(c) $[a] \subseteq S \quad \forall \; a \in S$

$x \in [a]$ for any $[a]$,

$x \in S$.

i.e., for $x \in \bigcup_{a \in S} [a]$, $x \in S$

$\Longrightarrow \bigcup_{a \in S} [a] \subseteq S$

Conversely,

Let $x \in S$ then $x \in [x]$ by (a)

$[x]$ is one of the sets in the collection whose union is $\bigcup_{a \in S} [a]$.

Hence, $x \in \bigcup_{a \in S} [a] \longrightarrow S \subseteq \bigcup_{a \in S} [a]$.

$\therefore S = \bigcup_{a \in S} [a]$

(d) Suppose $[a] \cap [b] \neq \emptyset$.

Let $x \in [a] \cap [b]$

then $x \in [a]$ and $x \in [b]$

$\rightarrow [x] = [a]$ and $[x] = [b]$ (b)

$\rightarrow \underline{[a] = [b]}$

- Any two left cosets of H in G are identical or disjoint

i.e.,

If xH and yH are two left cosets of a subgroup H in G, then $xH = yH$ or $xH \cap yH = \phi$

- G is the disjoint union of the distinct left cosets of H in G.

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

Ex:- $G = S_3 = \{I, (1\,2), (1\,3), (2\,3), (1\,2\,3), (1\,3\,2)\}$.

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

check Ex 3

The distinct left cosets of H are: H & $(1\,2)H$

$\therefore S_3 = \langle (1\,2\,3) \rangle \cup (1\,2)\langle (1\,2\,3) \rangle$

E.3

- Let H be a subgroup of a group G. There is a one-one correspondence b/w the elements of H and those of any right or left coset of H.

i.e.

the mapping $f: H \to Hx \mid f(h) = hx$ is a bijection

$\Rightarrow$ The # of elements in every coset of H is the same as the # of elements in H

$$|Hx| = |H| = |xH| \quad \forall\, x \in G$$

$$|Hx_1| = |Hx_2| = \cdots = |Hx_r| = |H|$$

$$|x_1H| = |x_2H| = \cdots = |x_rH| = |H|$$

Proof

Let Ha be a coset of H in G.

Consider the function $f: H \to Ha \mid f(h) = ha$

For $h, h' \in H$,

$f(h) = f(h') \implies ha = h'a$

$\to h = h'$

$\therefore f$ is one-one

$y = f(h) = ha \implies h = \frac{y}{a}$

For all $y = f(h) \in Ha$,

there is a $h = \frac{y}{a} \in H$

$\therefore f$ is onto

$\implies f$ is a bijection

Hence, there is a one-to-one correspondence b/w the elements of H and Ha.

Similarly, the map $f: H \to aH \mid f(h) = ah$ is a bijection.

(E·4) Write $\mathbb{Z}$ as a union of disjoint cosets of $5\mathbb{Z}$

Ans $H = 5\mathbb{Z} = \{\ldots, -10, -5, 0, 5, 10, \ldots\}$

The right cosets of $5\mathbb{Z}$ in $\mathbb{Z}$ are:

$5\mathbb{Z}, 5\mathbb{Z}+1, 5\mathbb{Z}+2, 5\mathbb{Z}+3, 5\mathbb{Z}+4$

$\therefore \mathbb{Z} = 5\mathbb{Z} \cup 5\mathbb{Z}+1 \cup 5\mathbb{Z}+2 \cup 5\mathbb{Z}+3 \cup 5\mathbb{Z}+4$

LAGRANGE'S THEOREM

- The order of a finite group G is the # of elements in G. It is denoted by $|G|$ (or) $o(G)$

Ex:- $o(S_3) = |S_3| = 6$

$o(A_3) = |A_3| = 3$ where, $A_3 = \langle (1\,2\,3) \rangle = \{I, (1\,2\,3), (1\,3\,2)\}$

$o(Z_n) = |Z_n| = n$

$o(S_n) = |S_n| = n!$

* Let H be a subgroup of a finite group G.

There is a one-to-one correspondence b/w the right cosets and the left cosets of H in G.

i.e.,

the mapping $f: \{Hx \mid x \in G\} \to \{yH \mid y \in G\}$

such that $f(Hx) = x^{-1}H$ is a bijection.

$\Rightarrow$ The # of distinct right cosets of H in G always equals the # of distinct left cosets of H in G.

$|G:H|$ = the # of distinct cosets of H in G

= the index of H in G

Proof $f: \{Hx \mid x \in G\} \to \{yH \mid y \in G\}$

such that $f(Hx) = x^{-1}H$.

$Hx = Hy \Rightarrow xy^{-1} \in H$ [Theorem 4.1 (c)

$\Rightarrow (xy^{-1})^{-1} \in H$

$\Rightarrow (y^{-1})^{-1} x^{-1} \in H$ [$x \mathcal{H}-y H \iff x^{-1}y \in H$

$\Rightarrow x^{-1}H = y^{-1}H$

$\Rightarrow f(Hx) = f(Hy)$

$\therefore$ f is well defined

$f(Hx) = f(Hy) \Rightarrow x^{-1}H = y^{-1}H$

$\Rightarrow (x^{-1})^{-1}y^{-1} = xy^{-1} \in H$

$\Rightarrow Hx = Hy$

$\therefore$ f is one-one.

Any left coset of H in G is $yH = f(y^{-1})$

$\therefore$ f is on-to

$\longrightarrow$ f is a Bijection.

Ex - $|S_3 : A_3| = 2$

If $H = \{e\}$, then $|G : \{e\}| = |G| = o(G)$

since $\{e\}g = \{g\}$ $\forall$ $g \in G$

and $\{e\}g \neq \{e\}g'$ if $g \neq g'$

$S_3 = \{I, (12), (13), (23), (123), (132)\}$

Proper subgroups of S_3 are:

$A = \langle I \rangle$, $B = \langle (12) \rangle$, $C = \langle (13) \rangle$, $D = \langle (23) \rangle = \{I, (23)\}$

$E = \langle (123) \rangle = \{I, (123), (132)\}$.

The orders of the subgroups of S_3 are:

1, 2, 3, 6

All these divide $o(S_3) = |S_3| = 6$.

⟶ Appeared in a paper in 1770, written by Lagrange.

Theorem (4.3), (4.2.1): Lagrange's theorem

Let H be a subgroup of a finite group G.

Then,

$$|G| = |G:H| \cdot |H|$$

i.e.,

$|H|$ divides $|G|$, and $|G:H|$ divides $|G|$

- The index $|G:H|$ measures the 'relative sizes' of G and H;
  which is the # of distinct cosets of H in G.

Proof

We can write G as a union of disjoint right cosets of H in G.

If $Hx_1, Hx_2, \ldots, Hx_r$ are all the distinct right cosets of H in G such that $|G:H| = r$, which gives the # of distinct cosets of H in G.

Then,

$$G = Hx_1 \cup Hx_2 \cup \cdots \cup Hx_r \quad \text{— (1)}$$

and $Hx_i \cap Hx_j = \phi$ for $i \neq j$

From (E.2),

$$|Hx_1| - |Hx_2| = \cdots = |Hx_r| = |H|$$

$$\therefore |Hx_1 \cup Hx_2 \cup \cdots \cup Hx_r| = r|H|$$

$$= |G:H| \cdot |H|$$

$$\Rightarrow |G| = |G:H| \cdot |H|$$

Application Ex:-

Find all the subgroups of a group G of order 35.

$|\bar{G}| = |G \cdot H| : |H|$ } The only subgroups are those of order 1, 5, 7 and 35

Let G be a group and $g \in G$. Then, the order of the element g is the order of the cyclic subgroup $\langle g \rangle$, if $\langle g \rangle$ is finite, which we denote as $o(g) = |g|$

If $\langle g \rangle$ is an infinite subgroup of G, then we say that g is of infinite order.

$$|g| = |\langle g \rangle|$$ where $g \in G$

Note $\langle g \rangle$ is the smallest subgroup of G containing g.

Definition

Let $g \in G$ have finite order. Then,
the set $\{e, g, g^2, \dots\}$ is finite, since G is finite.

$\therefore$ all powers of g can't be distinct.

$\therefore$ $g^r = g^s$ for some $r > s$.

$g^{r-s} = e$ and $r - s \in \mathbb{N}$.

$\therefore$ the set $\{t \in \mathbb{N} \mid g^t = e\}$ is non-empty.

Well ordering principle $\Rightarrow$ the set has a least element.

Let n be the least +ve integer such that $g^n = e$. Then,

$$\langle g \rangle = \{e, g, g^2, \ldots, g^{n-1}\}$$

$$\therefore |g| = |\langle g \rangle| = n$$

$\Longrightarrow$ $|g|$ is the least +ve integer n such that $g^n = e$.

[If $g \in (G, +)$, then $|g|$ is the least +ve integer n such that $ng = e$]

- If $g \in G$ is of infinite order. Then, for $m \neq n$, $g^m \neq g^n$

(Because, if $g^m = g^n$, then $g^{m-n} = e$, which shows that $\langle g \rangle$ is a finite group)

E.6 What are the order of

(a) $(1\ 2) \in S_3$

Ans: $(1\ 2) \neq I$, $(1\ 2)^2 = (1\ 2)\circ(1\ 2) = I$

$|(1\ 2)| = 2$

(b) $I \in S_4$

Ans: $I^1 = I \implies |I| = 1$

(c) $\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \in Q_8$

Ans: 2.

(d) $\bar{3} \in Z_4$

Ans: $\bar{3} \neq 0$, $\bar{3} + \bar{3} = \bar{6} = \bar{2}$, $3\cdot\bar{3} = \bar{9} = \bar{1}$, $4\cdot\bar{3} = \bar{12} = \bar{0}$

$\therefore |\bar{3}| = 4$

(e) $1 \in \mathbb{R}$

Ans: $\langle 1 \rangle = \mathbb{R}$ is infinite.

$\therefore$ 1 is of infinite order

Theorem 4.4: Let G be a group and $g \in G$ be of order n. Then $g^m = e$ for some $m \in \mathbb{N}$ iff $n \mid m$.

Proof

$|g| = n$ (or) $g^n = e$ $\Big\}$ $g^m = e$ iff $n \mid m$

Division algorithm $\Big\}$ $m = nt + r$

$$\begin{array}{r|l} & t \\ n & m \\ \hline & r \end{array}$$

where $0 \le r < n$

$$e = g^m = g^{nt+r} = g^{nt} \cdot g^r = (g^n)^t g^r = e^t g^r$$

$$= e g^r = g^r$$

$\Rightarrow g^r = e$, But n is the smallest +ve integer such that $g^n = e$ and $r < n$.

$\therefore r = 0 \longrightarrow m = nt$

$g^m = e$

$\therefore n \mid m$ (or) $|g| = n$ divides m

Theorem 4.5: Let $G = \langle g \rangle$ be a cyclic group

(a) If g is of infinite order then g^m is also of infinite order for every $m \in \mathbb{Z}$

(b) If $|g| = n$ then,

$$|g^m| = \frac{n}{\gcd(n,m)} \quad \forall\ m = 1, 2, \ldots, n-1$$

Proof

(a) An element is of infinite order iff all its powers are distinct.

g is of infinite order $\Rightarrow$ all the powers of g are distinct

If possible, let $(g^m)^t = (g^m)^w \Rightarrow g^{mt} = g^{mw}$

But then $mt = mw$

$\therefore t = w$.

$\Rightarrow$ Powers of g^m are all distinct & hence g^m is of infinite order.

(2)

$|g| = n$ & $G = \langle g \rangle = \{e, g, g^2, \ldots, g^{n-1}\}$

Let $H \neq \{e\}$ be a subgroup of $\langle g \rangle = G$ then $H = \langle g^m \rangle$ where m is the least +ve integer such that $g^m \in H$

$\Rightarrow$ $H = \langle g^m \rangle$ must be of finite order

$|g^m|$ is finite

Let $t = |g^m|$ then $(g^m)^t = g^{mt} = e$

& $|g| = n \Rightarrow g^n = e$

Theorem 4.4 $\Rightarrow$ $n \mid tm$

$t = \frac{n}{\gcd(n,m)} = \frac{n}{d} \Rightarrow n = dt$

we need a group,

Let $d = \gcd(n, m)$ then $n = n_1 d$ &
$m = m_1 d$

$$d = \gcd(n, m) = \gcd(n_1 d, m_1 d) = d \gcd(n_1, m_1)$$

$$\Longrightarrow \gcd(n_1, m_1) = 1$$

$$n_1 = \frac{n}{d} = \frac{n}{\gcd(n, m)}$$

Now,

$$n \mid tm \longrightarrow n \mid tm_1 d \longrightarrow n_1 d \mid tm_1 d$$

$$\Longrightarrow n_1 \mid tm_1$$

$$\Longrightarrow n_1 \mid t \text{ (or) } n_1 \mid m_1$$

$$\gcd(n_1, m_1) = 1 \longrightarrow n_1 \nmid m_1$$

$$\therefore n_1 \mid t \qquad \text{——— (1)}$$

$|g| = n \Longrightarrow g^n = e$

Ex:-

$|g^m| = t \Longrightarrow (g^m)^t = g^{mt} = e$

as we defined

$$(g^m)^{n_1} = g^{mn_1} = g^{m_1 d n_1} = g^{m_1 n} = (g^n)^{m_1}$$

$$= e^{m_1} = e$$

Theorem 4.4 $\Longrightarrow t \mid n_1$ — (2)

(1) & (2) $\Longrightarrow t = n_1$

$$t = n_1 = \frac{n}{d} = \frac{n}{\gcd(n,m)}$$

$$|g^m| = \frac{n}{\gcd(n,m)}$$

Ex:-

$|\overline{4}|$ in $\mathbb{Z}_{12}$ is $\frac{12}{\gcd(12,4)} = \frac{12}{4} = 3$ //

* Let G be a finite group, and $g \in G$. Then, $|g|$ divides $|G|$, and in particular $g^{|G|} = e$

$$|g| \mid |G| \rightarrow g^{|G|} = e$$

Proof

$|g| = |\langle g \rangle|$ & $|\langle g \rangle| \mid |G|$ from Lagrange's theorem

$\Rightarrow |g| \mid |G|$

Theorem 4.4 $\rightarrow g^{|g|} = e$

* **Every group of prime order is cyclic.**

Proof.

Let G be a group of prime order p.

i.e., $|G| = p$

Since $p \neq 1$ $\exists$ $g \in G$ such that $a \neq e$.

$|g| \mid |G| \longrightarrow |g| \mid p$

$\therefore |g| = 1$ (or) $|g| = p$

Since $g \neq e$, $|g| \geq 2$.

$\therefore |g| = p$., i.e., $|g| = |\langle g \rangle| = p$

$\langle g \rangle$ is the smallest subgroup of G containing 'g'

$\therefore \langle g \rangle \leq G$ such that $|\langle g \rangle| = |G| = p$

$\Rightarrow \langle g \rangle = G$ $\therefore$ G is cyclic.

*

(a) Let G be an abelian group and $a, b \in G$.

Then,

$$|ab| \mid \text{lcm}(|a|, |b|)$$

If $|a|, |b|$ are coprime, i.e., $\gcd(|a|, |b|) = 1$ then

$$|ab| \mid |a||b|$$

(b) Let a, b be elements of an abelian group G.

If $\langle a \rangle \cap \langle b \rangle = \{e\}$, then $|ab| = \text{lcm}(|a|, |b|)$

(c) Let a, b be elements of an abelian group G.

If $|a|$ and $|b|$ are coprime, i.e., $\gcd(|a|, |b|) = 1$ then,

$$|ab| = |a||b|$$

Proof

(a) Let $|a| = m$, $|b| = n$ and let $c = \text{lcm}(m, n)$.

then,

$c = rm$ for some $r \in \mathbb{Z}$

$= sn$ for some $s \in \mathbb{Z}$

$\therefore (ab)^c = a^c b^c$ $\quad [ab = ba$

$= a^{rm} b^{sn}$

$= (a^m)^r (b^n)^s$

$= e^r e^s = e$

$\Rightarrow |ab| \mid c$ $\quad [\text{Theorem } 4.4]$

$\Rightarrow |ab| \mid \text{lcm}(|a|, |b|)$

⑤ Let $|ab| = r$ and $c = \text{lcm}(|a|, |b|)$
$= \text{lcm}(m, n)$

$|ab| \mid \text{lcm}(m,n) \Rightarrow r \mid c$

$\therefore \boxed{r \leq c}$

$e = (ab)^r = a^r b^r \Rightarrow a^r = b^{-r} \in \langle b \rangle$

$\therefore a^r \in \langle a \rangle \cap \langle b \rangle = \{e\}$; as is taken.

$|H||K| = |G|$

$\Rightarrow a^r = e$

$\therefore |a| = m \mid r$

Similarly, $b^r = (b^{-1})^{-r} = (a^n)^{-r} = e^{-r} = e$

$\therefore |b| = n \mid r$

$m \mid r$ & $n \mid r \Rightarrow r$ is a +ve common multiple of m and n

$\therefore c = \text{lcm}(m,n) \leq r \Rightarrow c \leq r$

$\therefore c = r \Rightarrow \underline{|ab| = \text{lcm}(|a|, |b|)}$

(c) Given the elements a, b of an abelian group G. and $\gcd(|a|,|b|)=1$

Consider the two cyclic subgroups of G.

$\langle a\rangle$ and $\langle b\rangle$, and consider $H=\langle a\rangle\cap\langle b\rangle$

where $H \leq G$.

Lagrange's theorem $\Longrightarrow |H|\,||\langle a\rangle|$ & $|H|\,||\langle b\rangle|$

$|G| = |G:H||H|$

$\Rightarrow |H|\,|m$ & $|H|\,|n$

$\Rightarrow |H|\,|\gcd(m,n)$ [Q.C.N.T : 1

Given $\gcd(|a|,|b|) = \gcd(m,n) = 1$

$\therefore |H|\,|1 \Longrightarrow |H| = 1$

$\therefore H = \{e\} = \langle a\rangle\cap\langle b\rangle$

Using (b), $|ab| = \text{lcm}(|a|,|b|) = |a||b|$

$H = \langle a \rangle \cap \langle b \rangle \Longrightarrow H \leq \langle a \rangle$ and $H \leq \langle b \rangle$

Proof.

* Let H be a non-empty subset of a group G.
Then H is a subgroup of G iff
$a, b \in H \longrightarrow ab^{-1} \in H$

* $e \in \langle a \rangle$ & $e \in \langle b \rangle$ then $e \in \langle a \rangle \cap \langle b \rangle$
$\rightarrow H = \langle a \rangle \cap \langle b \rangle \neq \emptyset$.

$H \subseteq \langle a \rangle$ and $H \subseteq \langle b \rangle$

Let $p, q \in H = \langle a \rangle \cap \langle b \rangle$

$p, q \in \langle a \rangle$ and $p, q \in \langle b \rangle$

$pq^{-1} \in \langle a \rangle$ and $pq^{-1} \langle b \rangle$

$\longrightarrow pq^{-1} \in \langle a \rangle \cap \langle b \rangle$

$\therefore H = \langle a \rangle \cap \langle b \rangle$ is a subgroup of $\langle a \rangle$ and $\langle b \rangle$.

- Let G be a finite abelian group

If n is the maximal order among the element in G, then the order of every element divides n

$\lvert g\rvert \mid \lvert g\rvert_{max}$	if G is abelian & $g \in G$

Proof

Let g have the maximal order n, i.e., $|g|=n$

Pick $h \in G$ and let $|h|=m$.

We want to prove $m|n$

Assume m does not divide n

$\Rightarrow \therefore m > 1$

and $m \leq n$ as is defined.

$\Rightarrow$ $lcm > n$

Special Case: If $\gcd(m,n) = 1$

G is abelian $\longrightarrow |gh| = |g||h| = nm$

i.e., $|gh| > |g| = n$

which is a contradiction as g has the largest order n.

General Case:

If $m \nmid n$, then there is some prime p whose multiplicity (exponent) as a factor of m exceeds that of n.

Let p^k be the highest power of p in m and p^t be the highest power of p in n and so $k > t$

$$m \nmid n : \quad \frac{n}{m} = \frac{p_1^{a_1} p_2^{a_2} \cdots p^t}{p_1^{b_1} p_2^{b_2} \cdots p^k} = p_1^{(a_1 - b_1)} p_2^{(a_2 - b_2)} \cdots p^{(t-k)}$$

where $t - k < 0 \Rightarrow k > t$

Consider g^{p^t} and h^{m/p^k} such that

$g^{p^t}, h^{m/p^k} \in G$ since $p^t, m/p^k \in \mathbb{Z}_+$

Note that $|g| = n$, $|h| = m$

$$|g^{p^t}| = \frac{n}{p^t} \not\mid p \qquad \left[|g^n| = \frac{n}{\gcd(n,i)} \right]_{n=|g|}$$

$$|h^{m/p^k}| = \frac{m}{m/p^k} = p^k$$

$$\Longrightarrow \gcd\left(|g^{p^t}|, |h^{m/p^k}|\right) = 1$$

i.e., The orders of the elements g^{p^t} & h^{m/p^k} are coprime.

Since G_1 is an abelian group, and

$g^{p^t}, h_1^{m/p^k} \in G_1$ we have

$$|g^{p^t} h^{m/p^k}| = |g^{p^t}| \, |h^{m/p^k}|$$

$$= \frac{n}{p^t} \cdot p^k = n p^{k-t} > n$$

since $k > t \Rightarrow k - t > 0$

This contradicts the maximality of n as an order in G_1.