Subgroup

Let $(G,\cdot)$ be a group and H be a non empty subset of G, then H is called a subgroup of G if H is itself a group w.r.t the binary operation defined in G.

Examples.

As $\mathbb{Z} \subset \mathbb{R}$

$\because (\mathbb{Z},+), (\mathbb{R},+)$ are groups

$\therefore (\mathbb{Z},+)$ is a subgroup of $(\mathbb{R},+)$

As $\mathbb{Z} \subset \mathbb{Q}$

$\because (\mathbb{Z},+), (\mathbb{Q},+)$ are groups

$\therefore (\mathbb{Z},+)$ is a subgroup of $(\mathbb{Q},+)$

As $\mathbb{Q} \subset \mathbb{R}$

$\because (\mathbb{Q},+), (\mathbb{R},+)$ are groups

$\therefore (\mathbb{Q},+)$ is a subgroup of $(\mathbb{R},+)$

As $\mathbb{R} \subset \mathbb{C}$

$\because (\mathbb{R},+), (\mathbb{C},+)$ are groups

$\therefore (\mathbb{R},+)$ is a subgroup of $(\mathbb{C},+)$

$(\mathbb{R}', \cdot)$ $(\mathbb{C}', \cdot)$ are groups

$\therefore (\mathbb{R}', \cdot)$ is a sbgp of $(\mathbb{C}', \cdot)$

$(1, \omega, \omega^2)$ is a sbgp of $(\mathbb{C}', \cdot)$

$\{1, -1, i, -i\}$ is a sbgp of $(\mathbb{C}', \cdot)$

$\mathbb{Z}$ = set of integers
$\mathbb{R}$ = Set of Real Nos
$\mathbb{C}$ = Set of Complex Nos
$\mathbb{Q}$ = Set of Rational Nos
$\mathbb{R}' = \mathbb{R} - \{0\}$
$\mathbb{C}' = \mathbb{C} - \{0\}$

Now Every group G has at least two sbgps namely G itself & $\{e\}$ identity. These are called **Trivial Sbgps**

Any sbgp of G other than trivial sbgps is called Non trivial Sbgp of G.

Imp

Theorem :- Let $(G,\cdot)$ be a group. Then a non empty subset H of G is a sbgp if & only if $a,b \in H \Rightarrow ab^{-1} \in H$.

Proof.

Let H is a sbgp of G & to prove that $\forall a,b \in H \Rightarrow a.b^{-1} \in H$.

$\because$ H is sbgp So H is group also.

$\therefore$ If $b \in H$ then $b^{-1} \in H$.

So $a, b^{-1} \in H \Rightarrow ab^{-1} \in H$. by closure law.

proved

Conversely To Prove H is a sbgp of G

Let $\forall a,b \in H \Rightarrow a.b^{-1} \in H$. —①

Put $b=a$.

$a,a \in H \Rightarrow a\bar{a}^{-1} \in H$

$\Rightarrow e \in H$. (Identity exist in H)

$\because$ H is a subset of G. $\therefore$ each element of H is also element of G.

$e,b \in H \Rightarrow eb^{-1} \in H$. using ①

$\Rightarrow b^{-1} \in H$. (Inverse exist in H)

$\because$ G is a group so Associative Law holds in G. & Since H is a subset of G, So Associative Law holds in H also.

Now for $a,b \in H \Rightarrow a(b^{-1})^{-1} \in H$. using ①

$\Rightarrow ab \in H$.

(closure law $a,b \in S \Rightarrow ab \in S$) $\because a \in H \& b \in H$.

$\therefore$ H is closed under binary operation.

So H is a group and being subset of G it is Sbgp of G.

SGB

Theorem The intersection of any collection of sbgps of a group is a sbgp of G.

$H_1 \cap H_2 \cap H_3 \cdots H_n = \bigcap_{i=1}^{n} H_i$

Cond for Sbgp S of G: $a, b \in S \Rightarrow ab^{-1} \in S$

Proof Let $\{H_i, i \in I\}$ be a family of sbgps of G

Let $H = \bigcap_{i \in I} H_i$

Let $a, b \in H \Rightarrow a, b \in H_i, i \in I$

Since each H_i is a sbgp of G, $\therefore ab^{-1} \in H_i, i \in I$

$\therefore ab^{-1} \in \bigcap_{i \in I} H_i = H$

Hence H is a sbgp of G.

Theorem Let G be a group and H a subgp of G. Then the set $aHa^{-1} = \{aha^{-1} : h \in H\}$ is a sbgp of G.

Proof

(To Prove aHa^{-1} is Sbgp)

[Cond for sbgp S of G: $a, b \in S \Rightarrow ab^{-1} \in S$

Let $x, y \in aHa^{-1}$

where $x = ah_1a^{-1}$, $h_1 \in H$

$y = ah_2a^{-1}$, $h_2 \in H$

(we see whether $xy^{-1} \in aHa^{-1}$)

$xy^{-1} = (ah_1a^{-1})(ah_2a^{-1})^{-1}$

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

$= (ah_1a^{-1})((a^{-1})^{-1}h_2^{-1}a^{-1})$

$= ah_1a^{-1}ah_2^{-1}a^{-1}$

$= a h_1 e h_2^{-1} a^{-1}$

$= a h_1 h_2^{-1} a^{-1}$ $\because h_1, h_2 \in H$ & H is sbgp of G
So $h_1 h_2^{-1} \in H$.

$xy^{-1} = a(h_1 h_2^{-1}) a^{-1} \in aHa^{-1}$

So aHa^{-1} is a sbgp of G.

Theorem. The union HUK of two sbgps H & K of a group G is a sbgp of G if & only if $H \subseteq K$ or $K \subseteq H$

Proof Let H, K be sbgps of G.

Suppose $H \subseteq K$ or $K \subseteq H$ (To Prove HUK is sbgp of G)

So $HUK = K$ or $HUK = H$

$\forall a, b \in HUK \Rightarrow ab^{-1} \in HUK$ $\because H$ & K are sbgps of G

So HUK is a sbgp of G.

Conversely Suppose HUK is a sbgp of G. (To Prove $H \subseteq K$, $K \subseteq H$)

Then if $a \in H \setminus K$, $b \in K \setminus H$
and both $a, b \in H \cup K$

$\because HUK$ is sbgp so $\forall a, b \in HUK \Rightarrow ab \in HUK$
Now $\because ab \in HUK$ $\therefore ab \in H$ or $ab \in K$

If $ab \in H$ then $b = (a^{-1}a)b$
$= a^{-1}(ab) \in H$ $\because a^{-1} \in H$ $\because H$ is sbgp
$b \in H$ (Contradiction) $\therefore K \subseteq H$

If $ab \in K$ then $a = abb^{-1}$
$a = (ab)b^{-1} \in K$ (Contradiction)
$\therefore H \subseteq K$

Hence either $H \setminus K = \phi \Rightarrow K \subseteq H$

or $K \setminus H = \phi \Rightarrow H \subseteq K$

proved

Example 16 Find the subgroups of group $G = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$ with the following table

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

Sol Here binary operation is addition modulo 4.

Consider all non-empty subsets of group $G = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$ w.r.t addition modulo 4.

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

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

We know that $\{\bar{0}\} \neq \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$ are trivial subgps

We found that non-trivial subgps is $\{\bar{0}, \bar{2}\}$

$\because$ In $\{\bar{0}, \bar{2}\}$ (i) $\bar{0}$ is identity $\bar{0} + \bar{2} = 2$ $(a*e = a)$ def.

(ii) $\bar{0}, \bar{2}$ are inverse of themselves $(a*b = e)$ def

$\bar{0} + \bar{0} = 0 \qquad \bar{2} + \bar{2} = 0$

(iii) $0 + (2+2) = (0+2) + 2$ Associativ

$0 + 0 = 2 + 2$

$0 = 0$

So $\{\bar{0},\bar{2}\}$ is a group.

but because $\{\bar{0},\bar{2}\}$ is a subset of group $\{\bar{0},\bar{1},\bar{2},\bar{3}\}$

So it is subgp

Hence all the sbgps of group $G_1=\{\bar{0},\bar{1},\bar{2},\bar{3}\}$ are $\{\bar{0}\}, \{\bar{0},\bar{2}\}, \{\bar{0},\bar{1},\bar{2},\bar{3}\}$

× ——— ×

IInd Method Def of Inverse $a*b=e$

Easy Method

Inverse of $\bar{0}=\bar{0}$ $\because \bar{0}+\bar{0}=\bar{0}$

" " $\bar{1}=\bar{3}$ $\because \bar{1}+\bar{3}=\bar{0}$

" " $\bar{2}=\bar{2}$ $\because \bar{2}+\bar{2}=\bar{0}$

" " $\bar{3}=\bar{1}$ $\because \bar{3}+\bar{1}=\bar{0}$

Cond for subgp $\forall a,b\in H \Rightarrow ab^{-1}\in H$.

We found only $\{0,2\}$ is non trivial sbgp among rest of subsets $\{\bar{0}\}, \{\bar{0},\bar{1},\bar{2},\bar{3}\}$ are trivial sbgps.

$\because$ Let $H=\{\bar{0},\bar{2}\}$ $\bar{0},\bar{2}\in H \Rightarrow \bar{0}+(\text{Inverse of }\bar{2})$

$=\bar{0}+\bar{2}$

$=\bar{2}\in H$

Hence $\{\bar{0},\bar{2}\}$ is a sbgp of G.

Let $H=\{\bar{0},\bar{1},\bar{3}\}$

$\bar{0},\bar{1},\bar{3}\in H$

$\bar{0}+(\bar{1})^{-1}=\bar{0}+\bar{3}=\bar{3}\in H$

$\bar{1}+(\bar{3})^{-1}=\bar{1}+\bar{1}=\bar{2}\notin H$ Hence $\{\bar{0},\bar{1},\bar{3}\}$ is not a sbgp of G.

Rest of all subsets of G are not sbgps $\because$ Inverse element doesn't not exist in those subset:

Hence sbgps of G_1 are $\{\bar{0}\}, \{\bar{0},\bar{2}\}, \{\bar{0},\bar{1},\bar{2},\bar{3}\}$

2·2-7

Grp

Example 17 Find the subgroups of the Klein's Four Group $G = \{e, a, b, c\}$ defined by

·	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Consider all non-empty subsets of $G = \{e, a, b, c\}$

$\{e\}, \{e, a\}, \{e, b\}, \{e, c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a\}, \{b\}, \{c\}$

$\{e, a, b\}, \{e, a, c\}, \{e, b, c\}, \{a, b, c\}, \{e, a, b, c\}$

$\{e\}$ & $\{e, a, b, c\}$ are trivial subgps.

From Table

$e^{-1} = e \quad \because e \cdot e = e$

$a^{-1} = a \quad \because a \cdot a = e$

$b^{-1} = b \quad \because b \cdot b = e$

$c^{-1} = c \quad \because c \cdot c = e$

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

Cond for subgp: $a, b \in H \Rightarrow ab^{-1} \in H$

So we found only $\{e, a\}, \{e, b\}$ & $\{e, c\}$ are non trivial subgps.

$\because e, a \in \{e, a\} \Rightarrow e a^{-1} = e \cdot a = a \in \{e, a\}$

$e, b \in \{e, b\} \Rightarrow e \cdot b^{-1} = e \cdot b = b \in \{e, b\}$

$e, c \in \{e, c\} \Rightarrow e \cdot c^{-1} = e \cdot e = c \in \{e, c\}$

(39) EX # 2.2

(9) $H = \{a+b\sqrt{2} \mid a, b \in \mathbb{Z}$ & both a, b are not simultaneously zero$\}$

Let $x, y \in H$ s.t.

$x = a+b\sqrt{2}$ where $a, b, c, d \in \mathbb{Q}$ and all a, b, c, d are not simultaneously zero.
$y = c+d\sqrt{2}$

To Prove H sbgp
$x, y \in H \Rightarrow xy^{-1} \in H$

Now $xy^{-1} = (a+b\sqrt{2})(c+d\sqrt{2})^{-1}$

$= (a+b\sqrt{2}) \frac{1}{(c+d\sqrt{2})}$

$= (a+b\sqrt{2}) \frac{1}{(c+d\sqrt{2})} \times \frac{(c-d\sqrt{2})}{(c-d\sqrt{2})}$

$= \frac{(a+b\sqrt{2}) \times (c-d\sqrt{2})}{c^2-d^2(2)}$

$= \frac{ac - \sqrt{2}ad + \sqrt{2}bc - 2bd}{c^2-2d^2}$

$xy^{-1} = \frac{(ac-2bd) + (bc-ad)\sqrt{2}}{c^2-2d^2}$

$= \left(\frac{ac-2bd}{c^2-2d^2}\right) + \left(\frac{bc-ad}{c^2-2d^2}\right)\sqrt{2}$

$xy^{-1} = E + F\sqrt{2} \in H$ ($\because$ of the form of $a+b\sqrt{2}$)

where $E = \frac{ac-2bd}{c^2-2d^2}$ & $F = \frac{bc-ad}{c^2-2d^2}$ where $c^2-2d^2 \neq 0$,

So H is a sbgp of the group of non-zero Real nos under multiplication.

Now $xy^{-1} = (a+b\sqrt{-5})(c+d\sqrt{-5})^{-1}$

$$= (a+b\sqrt{-5})\frac{1}{(c+d\sqrt{-5})}$$

$$= (a+b\sqrt{-5})\frac{1}{(c+d\sqrt{-5})} \times \frac{(c-d\sqrt{-5})}{(c-d\sqrt{-5})}$$

$$= \frac{(a+b\sqrt{-5}) \times (c-d\sqrt{-5})}{c^2+5d^2}$$

$$= \frac{ac - ad\sqrt{-5} + bc\sqrt{-5} + 5bd}{c^2+5d^2}$$

$$= \frac{ac+5bd + (bc-ad)\sqrt{-5}}{c^2+5d^2}$$

$$= \frac{(ac+5bd)}{(c^2+5d^2)} + \frac{(bc-ad)\sqrt{-5}}{(c^2+5d^2)}$$

$xy^{-1} = E+F\sqrt{-5} \in H$ (∵ of the form of $a+b\sqrt{-5}$)

where $E = \frac{ac+5bd}{c^2+5d^2}$ $\quad F = \frac{bc-ad}{c^2+5d^2}$

Since for $x, y \in H \Rightarrow xy^{-1} \in H$

Hence H is a subgp of group of non zero complex no's under multiplication.

2.2-10

(14) Let H is a subgp of G

To Prove $H \cdot H = H$

Let $H \cdot H = \{h_1 h_2 : h_1, h_2 \in H\}$.

Let $h_1, h_2 \in H \cdot H$

Since H is a subgp of gp G so H is closed under '$\cdot$' i.e $\forall\ h_1, h_2 \in H \Rightarrow h_1 h_2 \in H$

$\Rightarrow H \cdot H \subseteq H$ ——— (I)

Also for each $h \in H$

$h = h \cdot e \in H \cdot H$ ($\because h \in H$, $e \in H$)

$\Rightarrow H \subseteq H \cdot H$ ——— (II)

From (I) & (II) $H \cdot H = H$

×

(13) Let $(Z, +)$ be the group of integers

Let H_1 & H_2 be two subsets of Z

$Z = 0, \pm 1, \pm 2 \cdots$

$H_1 = \{-1, -2, -3, \cdots\}$ $\quad (-1)+(-2) = -3 \in H_1$

$H_2 = \{1, 2, 3, \cdots\}$ $\quad 2+3 = 5 \in H_2$

H_1 & H_2 are closed under $+$.

Now because inverse element does not exist in H_1 & H_2 so H_1 & H_2 are not subgps

Def of Inverse
$a * b = e$

2·2 - 11

Q11 (i) $H = \left\{ \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} : a, b, d \in R \text{ & } ad \neq 0 \right\}$

To Prove H is a subgroup of $G = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a, b, c, d \in R \text{ and } ad - bc \neq 0 \right\}$

Sol Let $A = \begin{bmatrix} a_1 & b_1 \\ 0 & d_1 \end{bmatrix} \in H$, $B = \begin{bmatrix} a_2 & b_2 \\ 0 & d_2 \end{bmatrix} \in H$ where $a_1 d_1 \neq 0$ & $a_2 d_2 \neq 0$

$$B^{-1} = \begin{bmatrix} a_2 & b_2 \\ 0 & d_2 \end{bmatrix}^{-1} = \begin{bmatrix} \frac{d_2}{a_2 d_2} & \frac{-b_2}{a_2 d_2} \\ 0 & \frac{a_2}{a_2 d_2} \end{bmatrix} = \begin{bmatrix} \frac{1}{a_2} & \frac{-b_2}{a_2 d_2} \\ 0 & \frac{1}{d_2} \end{bmatrix}$$

$$AB^{-1} = \begin{bmatrix} a_1 & b_1 \\ 0 & d_1 \end{bmatrix} \begin{bmatrix} \frac{1}{a_2} & \frac{-b_2}{a_2 d_2} \\ 0 & \frac{1}{d_2} \end{bmatrix}$$

$$= \begin{bmatrix} \frac{a_1}{a_2} + b_1 \times 0 & \frac{-a_1 b_2}{a_2 d_2} + \frac{b_1}{d_2} \\ 0 \times \frac{1}{a_2} + d_1 \times 0 & 0 \times \frac{-b_2}{a_2 d_2} + \frac{d_1}{d_2} \end{bmatrix} = \begin{bmatrix} \frac{a_1}{a_2} & \frac{-a_1 b_2}{a_2 d_2} + \frac{b_1}{d_2} \\ 0 & \frac{d_1}{d_2} \end{bmatrix} \in H$$

Thus $A, B \in H \Rightarrow AB^{-1} \in H$ Hence H is subgroup of G.

(ii) $K = \left\{ \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix} : b \in R \right\}$ To Prove K is a subgp of G

$A = \begin{bmatrix} 1 & b_1 \\ 0 & 1 \end{bmatrix} \in K$ $B = \begin{bmatrix} 1 & b_2 \\ 0 & 1 \end{bmatrix} \in K$

$$AB^{-1} = \begin{bmatrix} 1 & b_1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & b_2 \\ 0 & 1 \end{bmatrix}^{-1} =$$

$$= \begin{bmatrix} 1 & b_1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & -b_2 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} (1 \times 1) + (b_1 \times 0) & 1 \times (-b_2) + (b_1 \times 1) \\ (0 \times 1) + (1 \times 0) & 0 \times (-b_2) + (1 \times 1) \end{bmatrix}$$

$$= \begin{bmatrix} 1 & -b_2 + b_1 \\ 0 & 1 \end{bmatrix} \in K$$

Thus $A, B \in K \Rightarrow AB^{-1} \in K$. Hence K is subgp of G.

(15) 2002 (79) 2-2-12

Let H, K be subgroups of an abelian group G.

Let $H \cdot K = \{hk : h \in H, k \in K\}$

To Prove HK is subgroup of G | $\forall x, y \in HK$, $xy^{-1} \in HK$, HK is sbgp

Let $x, y \in HK$ s.t

$x = h_1 k_1 \quad y = h_2 k_2 \quad h_1, h_2 \in H, \; k_1, k_2 \in K$

$xy^{-1} = (h_1 k_1)(h_2 k_2)^{-1}$

$= (h_1 k_1)(k_2^{-1} h_2^{-1}) = (h_1 k_1)(h_2^{-1} k_2^{-1})$ $\because G$ is abelian

$= h_1 (k_1 h_2^{-1}) k_2^{-1}$ Associative Law

$= h_1 (h_2^{-1} k_1) k_2^{-1}$ $\because G$ is abelian

$= (h_1 h_2^{-1})(k_1 k_2^{-1}) \in HK$

$\therefore \; xy^{-1} \in HK$

$h_1 h_2^{-1} \in H :: sbgp$

$k_1 k_2^{-1} \in K :: sbgp$

Since $\forall x, y \in HK \Rightarrow xy^{-1} \in HK$

Hence HK is a sbgp of G.

(16) Let H be a subgp of a group G and $a \in G$. If $(Ha)^{-1} = \{(ha)^{-1} : h \in H\}$ then. Show that $(Ha)^{-1} = a^{-1}H$

Sol Let $x \in (Ha)^{-1}$, then for some $h \in H$

$$x = (ha)^{-1} = a^{-1}h^{-1} \in a^{-1}H \quad \because h^{-1} \in H$$

Hence $(Ha)^{-1} \subset a^{-1}H$ ——— (I)

Now let $y \in a^{-1}H$ then for some $h \in H$

$$y = a^{-1}h = (h^{-1}a)^{-1} \in (Ha)^{-1}$$

Thus $a^{-1}H \subset (Ha)^{-1}$ ——— (II)

From (I) & (II) we have $(Ha)^{-1} = a^{-1}H$

(17) Let H, K be two subgps of a finite group G. Prove that for any $g \in G$ $\quad g(H \cap K) = gH \cap gK$

Sol We know that

$$H \cap K \subset H \text{ and } H \cap K \subset K$$

$\Rightarrow g(H \cap K) \subset gH$ and $g(H \cap K) \subset gK$ $\forall g \in G$.

$\Rightarrow g(H \cap K) \subset gH \cap gK$ ——— (I)

Again Let $y \in gH \cap gK$

$\Rightarrow y \in gH$ and $y \in gK$

$\Rightarrow g(g^{-1}y) \in gH$ and $g(g^{-1}y) \in gK$ $\because gg^{-1} = e$

$\Rightarrow g^{-1}y \in H$ and $g^{-1}y \in K$

$\Rightarrow g^{-1}y \in H \cap K$

pre Multiply by g $\Rightarrow gg^{-1}y \in g(H \cap K) \Rightarrow y \in g(H \cap K)$

Hence $gH \cap gK \subset g(H \cap K)$ ——— (II)

From (I) & (II) $\quad g(H \cap K) = gH \cap gK$

Cyclic Groups:

A group $(G,\cdot)$ is said to be cyclic if every element of G can be written in power of a single element (say) 'a' of G

$$G = \{a^K : K \in Z\}$$

such an element $a \in G$ is called Generator of G.

OR.

A group G is called Cyclic if and only if there exist an element $a \in G$ s.t $G = \{a^K / K \in Z\}$

i,e every element of G is written in the integral power of a. The element a is called generator of G and we write

$$G = [a] = gp(a)$$

Examples (i) $G = \{1, \omega, \omega^2\} = gp(\omega)$

$\omega^0 = 1$
$\omega^1 = \omega$
$\omega^2 = \omega^2$

Thus the group G is generated by ω.

(ii) $G = \{1, -1, i, -i\}$

$(i)^1 = i$, $(i)^2 = -1$, $(i)^3 = i^2 \cdot i = -i$ $(i)^4 = i^2 \cdot i^2 = (-1)(-1) = 1$

Thus G is generated by i

$(-i)^1 = -i$, $(-i)^2 = -1$, $(-i)^3 = i$, $(-i)^4 = (-)^4 (i)^4 = 1$

Thus G is generated by $(-i)$

Thus we see that a cyclic gp can have more than one generator.

If $(G,+)$ is a group then

$G_1 = gp(a) = \{ka / k \in Z\}$ $\quad Z = 0, \pm 1, \pm 2 \cdots$

$(Z,+)$ is a group.

$$Z = \{0, 1, 2, 3 \cdots, -1, -2, -3, \cdots\} = \{0(1), 1(1), 2(1) \cdots, -1(1), -2(1), -3(1) \cdots\}$$

we see that every element of Z is a multiple of 1 i.e Z is generated by 1.

$$Z = [1] = gp(1)$$

Also $Z = \{0(-1), 1(-1), 2(-1) \cdots, -1(-1), -2(-1), -3(-1) \cdots\}$

$$\Rightarrow Z = \{1\} = gp(-1)$$

Group of integers under addition is a cyclic group. $1 \& -1$ are its generators

Note If the order of a is finite i.e if there exist least +ive integer 'n' s.t $a^n = e$ then G is said to be Finite cyclic group of order 'n'.

$$G = \langle a : a^n = e \rangle$$

(order of generator = order of cyclic group)

(G is a cyclic group of order n generated by 'a'.)

If the order of a infinite i.e if there does not exist least +ive integer n, s.t $a^n = e$ then G is said to be Infinite Cyclic group.

Theorem Every Cyclic group is abelian

Let $x, y \in gp(a)$

then $x = a^m$ & $y = a^n$ where $m, n \in Z$

$\therefore xy = a^m \cdot a^n = a^{m+n}$

$= a^{n+m} = a^n \cdot a^m = yx$

$xy = yx$

Hence abelian

Theorem Let G be any group. Let $a \in G$ have order n. Then for any integer K $a^K = e$ if and only if $K = qn$ or n divides K or $\frac{K}{n}$, $n < K$ where q is an integer.

$o(a) = 4, a^4 = e$ Also for $a^{12} = e$ iff 4 divides 12
$a^{13} \neq e$ $\because$ 4 does not divide 13

Proof Suppose that n is the order of a i.e $a^n = e$ and for some integer 'K'; $a^K = e$

By division algorithm, there are integers q & r s.t

$$K = nq + r \quad , 0 \leq r < n \quad \text{---} (1)$$

$$3\overline{)16}\ 5,\ 15,\ 1$$

$16 = 3 \times 5 + 1$
$K = nq + r$

So that $e = a^K = a^{nq+r} = a^{nq} a^r$

$= (a^n)^q a^r = (e)^q a^r = e a^r = a^r$

$\therefore e = a^r$

Since order of a is n, so that n is the smallest integer for which $a^n = e$, So $r = 0$ $(\because r < n)$

$\therefore K = nq$ proved from (1)

Conversely suppose $K = nq$

then $a^K = a^{nq} = (a^n)^q = (e)^q = e$

$a^K = e$ proved.

---

v. Imp. Every subgroup of a cyclic group is cyclic.

Pf Let $G = [a]$ be a cyclic group generated by a. (Then every element of G is a power of a.)

Let H be a non trivial subgp of G. Let K be the least positive integer such that $a^K \in H$

(We have to show that every element of H can be written in power of a. $\because a^K$ is smallest member of H)

For this let $a^m \in H$

If we divide m by K then there are integers q & r s.t

$$m = qK + r \qquad 0 \le r < K \qquad (1)$$

$$a^m = a^{qK+r}$$

$$= a^{qK}\, a^r$$

$$a^{-(qK)}\, a^m = a^{-(qK)}\, a^{qK}\, a^r$$

(pre multiply by $a^{-(qK)}$)

$$\left[(a^K)^q\right]^{-1} a^m = e \cdot a^r$$

$$\left[(a^K)^q\right]^{-1} a^m = a^r$$

$\therefore a^r \in H$

$\because a^r = \left[(a^K)^q\right]^{-1} a^m \in H$

$\because H$ is subgp of G so elements of H are in the powers of a.

$5 \overline{)16}\ (3$, 15, 1

$16 = 3 \times 5 + 1$

$m = qK + r$

$r < K$

$1 < 5$

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

$a^m, a^K \in H,\ a^m (a^K)^{-q} \in H$

$\because a^m, (a^K)^q \in H \Rightarrow a^m \left[(a^K)^q\right]^{-1} \in H$

$\because H$ is subgp

2·2-18

But K is the least +ive integer s.t, $a^K \in H$.
& here $a^r \in H$ & $r < K$ so it is a contradiction unless $r = 0$

$\therefore$ from ① $m = qK \Rightarrow a^m = a^{qK} = (a^K)^q$ ....

$a^m = (a^K)^q$ i.e all the elements of H are in the power of a^K

$\therefore a^K$ is generator of H $\because a^m \in H$

Hence H is cyclic

×——————×

Th Let G be a cyclic group of order n generated by a. Then for each positive divisor 'd' of n, there is a unique subgroup (of G) of order d.

Proof Let $G = [a]$ be a cyclic group of order n

$\Rightarrow a^n = e$ ——— ①

Let d be a positive divisor of n. then

$\exists$ an integer q s.t $\frac{n}{d} = q$

$n = dq$ ——— ②

Take $b = a^q$

$b^d = a^{dq} = a^n = e$ → using ② → using ①

$b^d = e$ $\therefore o(b) = d$

$d < n$ ∵ d is divisor of n

$\therefore o(H) < o(G)$

H is subgp. ∵ subgp of cyclic subgp is cyclic

Hence $H = [b]$ be a cyclic subgp of G and order of H is d.

Now we prove the uniqueness of H.

Let K be another subgp of G. Order of K is 'd' then K is cyclic. ∵ subgp of Cylic Group is cyclic

K is generated by $c = a^p$

where p is least +ive integer s.t $a^p \in K$

$\because O(K) = d$

$\therefore (a^p)^d = a^{pd} = c^d = e$

$\because a^{pd} = e \Leftrightarrow a^n = e$ using ①

$\Rightarrow pd = n$ ——③

from ② $qd = n$

from ②&③ $pd = qd$

so $p = q$

So $c = a^p = a^q = b$

Hence $K = [c] = [b] = H$

$K = H$ Hence H is unique.

Example 18 Let G be a cyclic group of order 12 generated by a. Then the elements of G are

$G = gp(a) = \{a, a^2, a^3, a^4, \ldots\ldots a^{12} = e\}$

Order of G is 12 and the divisors of 12 are 1, 2, 3, 4, 6, 12

$\therefore$ Sbgps of G have orders 1, 2, 3, 4, 6, 12 { ∵ by Theorem 2.21 for each divisor d of 12 G has a sbgp of order d.

sbgp of order 1 $= \{a^{12} = e\}$ $\frac{n}{d} = \frac{12}{1} = q$

" " " 2 $= [a^6] = \{a^6, a^{12} = e\}$ $\frac{12}{2} = 6 = q$

" " " 3 $= [a^4] = \{a^4, a^8, a^{12} = e\}$ $\frac{12}{3} = 4 = q$

" " " 4 $= [a^3] = \{a^3, a^6, a^9, a^{12} = e\}$

" " " 6 $= [a^2] = \{a^2, a^4, a^6, a^8, a^{10}, a^{12} = e\}$

sbgp of order 12 $= [G]$

2·2 -20

Cosets

Let H be a subgp of a group G and $a \in G$, then the set $aH = \{ah : h \in H\}$ is called Left Coset of H in G determined by 'a'.

Similarly $Ha = \{ha : h \in H\}$ is called Right Coset of H in G determined by 'a'.

The above def is for a group under multiplication.

If G is a group under addition i.e $(G, +)$

Then $H+a = \{h+a : h \in H\}$ is called Right Coset of H in G determined by 'a'.

$a+H = \{a+h : h \in H\}$ is called Left Coset of H in G determined by a.

Note 1) $a \in G$ and $a \notin H$

but if $a \in H$ then $Ha = H$.

2) H itself is both a left coset and a right coset in G determined by e as

$$eH = H = He$$

3) In an abelian group the left & right cosets of H coincides.

Example Let $G = \{e, a, a^2, a^3\}$ & $H = \{e, a^2\}$

$He = H$

$Ha = \{e, a^2\}a = \{ea, a^3\} = \{a, a^3\}$ $\quad a^4 = e$

$Ha^2 = \{e, a^2\}a^2 = \{ea^2, a^4\} = \{a^2, e\} = H$

$Ha^3 = \{e, a^2\}a^3 = \{ea^3, a^5\} = \{a^3, a\} = Ha$

Hence $\{H, Ha\}$ is the set of Right cosets of H in G determined by a.

2·2-21

Example 19

$G = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$ be group of residue classes under + modulo 6

$H = \{\bar{0}, \bar{2}, \bar{4}\}$ is a subgp of G

$\bar{0}+H = \bar{0}+\{\bar{0},\bar{2},\bar{4}\} = \{\bar{0},\bar{2},\bar{4}\} = H$

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

$\bar{2}+H = \bar{2}+\{\bar{0},\bar{2},\bar{4}\} = \{\bar{2},\bar{4},\bar{0}\}$

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

$\bar{4}+H = \bar{4}+\{\bar{0},\bar{2},\bar{4}\} = \{\bar{4},\bar{0},\bar{2}\}$

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

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

$\bar{0}+H = \bar{2}+H = \bar{4}+H$

& $\bar{1}+H = \bar{3}+H = \bar{5}+H$

∴ The left Cosets of H in G are only two and these are $\bar{0}+H = \{\bar{0},\bar{2},\bar{4}\}$ & $\bar{1}+H = \{\bar{1},\bar{3},\bar{5}\}$.

Example 20

$G = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$ be group of residue classes under '·' modulo 8

$H_1 = \{1, 3\}$ $H_2 = \{1, 5\}$

$H_3 = \{1, 7\}$

are proper subgps of G.

·	$\bar{1}$	$\bar{3}$	$\bar{5}$	$\bar{7}$
$\bar{1}$	$\bar{1}$	$\bar{3}$	$\bar{5}$	$\bar{7}$
$\bar{3}$	$\bar{3}$	$\bar{1}$	$\bar{7}$	$\bar{5}$
$\bar{5}$	$\bar{5}$	$\bar{7}$	$\bar{1}$	$\bar{3}$
$\bar{7}$	$\bar{7}$	$\bar{5}$	$\bar{3}$	$\bar{1}$

The left Coset of H_1 in G.

$\bar{1}\cdot H_1 = \bar{1}\cdot\{\bar{1},\bar{3}\} = \{\bar{1},\bar{3}\} = H_1$

$\bar{3}\cdot H_1 = \bar{3}\cdot\{\bar{1},\bar{3}\} = \{\bar{3},\bar{1}\} = H_1$

$\bar{5}\cdot H_1 = 5\cdot\{\bar{1},\bar{3}\} = \{\bar{5},\bar{7}\}$

$7\cdot H_1 = 7\cdot\{\bar{1},\bar{3}\} = \{\bar{7},\bar{5}\}$

Here the set of left cosets of H_1 in G is $\{\bar{1}\cdot H_1, \bar{5}\cdot H_1\}$

2·2·22

Partition of a set A we mean a collection of subsets $\{A_i : i \in I\}$ of A s.t

$$\bigcup\{A_i : i \in I\} = A \quad \& \quad A_i \cap A_j = \emptyset \quad \text{where } i,j \in I \text{ \& } i \neq j$$

(Extra)

Example $G = \{e, w, w^2, w^3, w^4, w^5\}$ $\quad w^6 = e$

$H = \{e, w^2, w^4\}$ is a subgp of G

Right Cosets

$He = \{e, w^2, w^4\}e = \{e, w^2, w^4\}$

$Hw = \{e, w^2, w^4\}w = \{w, w^3, w^5\}$

$Hw^2 = \{e, w^2, w^4\}w^2 = \{w^2, w^4, w^6\} = \{w^2, w^4, e\}$

$Hw^3 = \{e, w^2, w^4\}w^3 = \{w^3, w^5, w^7\} = \{w^3, w^5, w\}$

$Hw^4 = \{e, w^2, w^4\}w^4 = \{w^4, w^6, w^8\} = \{w^4, e, w^2\}$

$Hw^5 = \{e, w^2, w^4\}w^5 = \{w^5, w^7, w^9\} = \{w^5, w, w^3\}$

Now similarly left Cosets

$eH = \{e, w^2, w^4\}$

$w^2H = \{w^2, w^4, e\}$

$w^4H = \{w^4, e, w^2\}$

$wH = \{w, w^3, w^5\}$

$w^3H = \{w^3, w^5, w\}$

$w^5H = \{w^5, w, w^3\}$

From above we see that

$eH = He$ $\quad wH = Hw$ $\quad w^2H = Hw^2$

$w^3H = Hw^3$ $\quad w^4H = Hw^4$ $\quad w^5H = Hw^5$

The no of Right Coset of H in G is equal to the no of Left Coset of H in G, i.e. 2 ; He & Hw

$He \cap Hw = \emptyset$ ——— (I)

$He \cup Hw = G$ ——— (II)

From (I) & (II) the no of Right (or Left) Coset of H in G is a partition of G.

i.e ∃ at least one element common {we are taking distinct not disjoint

So $x \in Ha \cap Hb$

$\Rightarrow x \in Ha$ & $x \in Hb$

Now $x \in Ha \Rightarrow x = h_1 a$

$x \in Hb \Rightarrow x = h_2 b$ for some $h_1, h_2 \in H$

So $h_1 a = h_2 b$

$\Rightarrow h_1^{-1} h_1 a = h_1^{-1} h_2 b$

$a = h_1^{-1} h_2 b$ ——— (3)

Let $y \in Ha \Rightarrow y = h_3 a$ $h_3 \in H$.

$= h_3 h_1^{-1} h_2 b$ using (3)

$= h' b \in Hb$ $h' = h_3 h_1^{-1} h_2 \in H$ ∵ H is a subgp

$y \in Hb$

So $Ha \subset Hb$ ——— (4) (∵ $y \in Ha$ and now $y \in Hb$ so $Ha \subset Hb$)

Similarly we can prove

$Hb \subset Ha$ ——— (5)

from (4) & (5) $Ha = Hb$ which is a contradiction ∵ Ha ≠ Hb were distinct.

Hence $Ha \cap Hb = \phi$ proved

Thus $\{Ha : a \in G, h \in H\}$ defines a partition of G.

Def The number of distinct left (or right) cosets of a sbgp H of a group G is called the Index of H in G and is denoted by $[G:H]$

Example 21 Find all the distinct left cosets of

$E = \{0, \pm 2, \pm 4, \dots\} = \{2n : n \in \mathbb{Z}\}$

in $\mathbb{Z} = \{0, \pm 1, \pm 2, \dots\}$

The only distinct left cosets of E in $\mathbb{Z}$ are $0+E$ & $1+E$

$2+E = 4+E \dots = E$
$3+E = 5+E \dots = 1+E$

$0+E = \{0+2n : n \in \mathbb{Z}\} = \{0, \pm 2, \pm 4, \dots\}$

$1+E = \{1+2n : n \in \mathbb{Z}\} = \{\pm 1, \pm 3, \pm 5, \dots\}$

$(0+E) \cup (1+E) = \mathbb{Z}$

$(0+E) \cap (1+E) = \phi$

$\therefore$ Index of E in $\mathbb{Z}$ is 2.

$1+2n$ $\quad n \in 0, \pm 1, \pm 2 \dots$
$1+2(0) = 1$
$1+2(1) = 3$
$1+2(-1) = -1$
$1+2(2) = 5$
$1+2(-2) = -3$
and so on

Lagrange Theorem :-

The order and index of a sbgp of a finite group divide the order of the group.

{i.e $\frac{|G|}{|H|}$

Proof Since G is finite so the set of right cosets of H in G is also finite. Let this set is

$\{Ha_1, Ha_2, Ha_3, \dots Ha_n\}$

Since the set of right cosets of H in G is a partition of G

$\therefore$ Th 2.24

So $G = Ha_1 \cup Ha_2 \cup Ha_3 \cdots Ha_n = \bigcup_{i=1}^{n} Ha_i$

& $Ha_i \cap Ha_j = \phi$ for $i \neq j$ $i,j = 1,2 \cdots n$

$\therefore |G| = |Ha_1| + |Ha_2| + |Ha_3| + \cdots + |Ha_n|$ ①

∵ cosets are disjoint

Now we find order of Ha_i i.e $|Ha_i| = ?$

So we define a mapping $\psi : H \longrightarrow Ha_i$

by $\psi(h) = ha_i$ $\forall h \in H$, $a_i \in G$

which is clearly onto ∵ each element of Ha_i is the image of some element of H. So ψ is onto.

Let $\psi(h_1) = \psi(h_2)$ $h_1, h_2 \in H$

implies $h_1 a_i = h_2 a_i$

by cancellation law $h_1 = h_2$ $\Rightarrow \psi$ is one-one

∵ ψ is onto & one-one so it is bijective

$\therefore |H| = |Ha_i|$

& in ① $|G| = |H| + |H| + |H| + \cdots + |H|$

$= n|H|$

$n = \frac{|G|}{|H|}$ i.e order of subgp H divides order of group G.

n is the index of H in G. { no of distinct cosets of H in G is called index of H in G

$|H| = \frac{|G|}{n}$ i.e index of H divides order of G.

2001

2·2-26 56-A

(12) Let H and K be two subgroups of a group G, whose orders are relatively prime. Prove that

$$H \cap K = \{e\}$$

Sol Let $|H| = m$ and $|K| = n$ where $(m, n) = 1$

Now $H \cap K$ is subgp of G. (∵ intersection of subgps is a subgp)

Also $H \cap K \subset H$ and $H \cap K \subset K$

which implies $H \cap K$ is a subgp of H and of K.

By Lagrange Theorem. "order of subgp divides order of a group"

∴ $|H \cap K|$ divides H and $|H \cap K|$ divides $|K|$

or $|H \cap K|$ is a common divisor of m and n.

$\Rightarrow |H \cap K| = 1$ ∵ m & n are relatively prime only common divisor in 'm' & 'n' is 1

Hence $H \cap K = \{e\}$

Corollary(2.27) The order of an element of a finite group divides the order of the group.

Proof Let G be a group of finite order n.

Let $a \in G$ & order of a is m i,e { To prove 'm' divides 'n'

$a^m = e$ m is least +ive integer

Now $a, a^2, a^3, \ldots\ldots a^{m-1}, a^m = e$ are all distinct and form a sbgp of G. The order of this sbgp is m.

Now by Lagrange. Th "The order of sbgp divides the order of the group".

$\therefore$ m divides n i,e $\frac{n}{m}$

× ——— ×

Corollary(2.28) A group G whose order is a prime number is necessarily cyclic.

Proof Suppose that G is a group of prime order 'p'

i,e $|G| = P$, Let $a(\neq e) \in G$

Also Let H be a cyclic sbgp generated by 'a'; order of H is 'K'. So $a^K = e$

By Lagrange Th K divides P i,e $\frac{P}{K}$

$\therefore$ P is prime { $a^K = e$ $K \neq 1$ $\because a \neq e$
so either K=1 or K=P { so $K = P$ $\because$ P is prime

Hence $H = G$

& since H is cyclic so G is cyclic.

2.2 – 28

Q1 We know $G = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$ be the group of residue class under multiplication modulo 8. {Example 10}.

Also commutative law holds in it i,e $a.b = b.a \ \forall a, b \in G$

$3 \cdot 5 = 5 \cdot 3$

$7 = 7$

So G is abelian

$\cdot$	$\bar{1}$	$\bar{3}$	$\bar{5}$	$\bar{7}$
$\bar{1}$	$\bar{1}$	$\bar{3}$	$\bar{5}$	$\bar{7}$
$\bar{3}$	$\bar{3}$	$\bar{1}$	$\bar{7}$	$\bar{5}$
$\bar{5}$	$\bar{5}$	$\bar{7}$	$\bar{1}$	$\bar{3}$
$\bar{7}$	$\bar{7}$	$\bar{5}$	$\bar{3}$	$\bar{1}$

Now G is not cyclic because every element of G can not be written in the power of one and the same element.

e.g $\bar{3}^2 = \bar{1}$, $\bar{5}^2 = \bar{1}$, $\bar{7}^2 = \bar{1}$

Q2 A gp G of order 47 can not have proper sbgps because 47 is a prime no, so the only divisors of 47 are 1 & 47. By Lagrange Theorem the order of a sbgp of a finite group divides the order of a group. So sbgps of group G are only of order 1 & 47 i,e identity & group itself, which are not proper sbgps of G.

So G has no proper sbgps.

2·2 – 29

Q3 Let G be a group of order 89

(i) Since 12 does not divide 89, so G has no subgp of order 12

(ii) Since 16 does not divide 89, so G has no subgp of order 16

(iii) Since 24 does not divide 89, so G has no subgp of order 24.

Q4 Let $G = [a]$ be an infinite cyclic group generated by a. it implies order of a does not exist. (∵ G is infinite cyclic)

G is infinite so $a \neq a^{-1}$

∵ if $a = a^{-1} \Rightarrow a^2 = e \Rightarrow o(a) = 2$ contradiction so $a \neq a^{-1}$.

For each $x \in G$ $x = a^n$ (i.e generated by a) ∵ G is infinite cyclic

Also $x = (a^{-1})^{-n} = a^n$ (i.e generated by a^{-1})

∴ G has two distinct generators $a \neq a^{-1}$.

Now we show that G has exactly two distinct generators.

Let b is a generator of G s.t $b \neq a$ & $b \neq a^{-1}$

∴ $b \in gp[a]$ & $b \in gp[a^{-1}]$

So ∃ two integers m & n s.t

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

Thus $a^m = a^{-n}$

$\Rightarrow a^m \cdot a^n = a^{-n} \cdot a^n = e$ post-× by a^n

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

$O(a) = m+n$ ∵ order of a does not exist being G an infinite cyclic group.

Hence G has exactly two distinct generators

×————————×

25 Is $(Q,+)$ a cyclic group.

The group $(Q,+)$ of rational numbers under '+' is not cyclic. Because

If Q is cyclic group generated by 'a', then $a = \frac{p}{q}$, $q \neq 0$ and each element of Q must be expressed in the form $\{a, 2a, 3a, \ldots\}$ i.e $na, n \in Z$.

Now particularly $\frac{1}{2}a$ is a rational no

So must be written as na

$\Rightarrow na = \frac{1}{2}a$ By R. Cancellation Law

$n = \frac{1}{2} \notin Z$ (n must $\in Z$)

∴ There is no such 'n' for which

$na = \frac{1}{2}a \in Z$,

Hence $(Q,+)$ is not cyclic.

Note $(Q,+)$ is abelian group but not cyclic (as proved)

Another example for Q1.

2.2-31

Let G be a cyclic group of order 24 generated by a.

i.e. $O(a) = 24 \Rightarrow a^{24} = e$ (24 is the least +ive integer for)

i) $O(e) = 1$ $\because e^1 = e$

$a^{24} = a^{48} = a^{72} = a^{96} \cdots = e$

ii) $O(a^9) = ?$

$(a^9)^8 = a^{72} = (a^{24})^3 = (e)^3 = e$

So $O(a^9) = 8$

iii) $O(a^{10}) = ?$

$(a^{10})^{12} = a^{120} = (a^{24})^5 = (e)^5 = e$

So $O(a^{10}) = 12$

Q Find all subgps of the cyclic gp of order 60 generated by a.

Let G be a cyclic group of order 60 generated by a.

Hence $G = \{a, a^2, a^3, \cdots\cdots, a^{60} = e\}$

We know (by Th 2.21) that for each divisor d of 60 G has a subgp of order d.

Set of all the divisors of 60 are

$\{1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60\}$

- Subgp of G order 1 $= \langle a^{60} \rangle = e$

" " " " 2 $= \langle a^{30} \rangle = \{a^{30}, a^{60}\} = \{a^{30}, e\}$

" " " " 3 $= \langle a^{20} \rangle = \{a^{20}, a^{40}, a^{60}\} = \{a^{20}, a^{40}, e\}$

Subgroup of G of order 4 $= \langle a^{15} \rangle = \{a^{15}, a^{30}, a^{45}, a^{60}=e\}$

" " " " 5 $= \langle a^{12} \rangle = \{a^{12}, a^{24}, a^{36}, a^{48}, a^{60}=e\}$

" " " " 6 $= \langle a^{10} \rangle = \{a^{10}, a^{20}, a^{30}, a^{40}, a^{50}, a^{60}\}$

" " " " 10 $= \langle a^{6} \rangle = \{a^{6}, a^{12}, a^{18}, a^{24}, a^{30}, a^{36}, a^{42}, a^{48}, a^{54}, a^{60}\}$

" " " " 12 $= \langle a^{5} \rangle = \{a^{5}, a^{10}, a^{15}, a^{20}, a^{25}, a^{30}, a^{35}, a^{40}, a^{45}, a^{50}, a^{55}, a^{60}\}$

" " " " 15 $= \langle a^{4} \rangle = \{a^{4}, a^{8}, a^{12}, a^{16}, a^{20}, a^{24}, a^{28}, a^{32}, a^{36}, a^{40}, a^{44}, a^{48}, a^{52}, a^{56}, a^{60}=e\}$

" " " " 20 $= \langle a^{3} \rangle = \{a^{3}, a^{6}, a^{9}, a^{12}, \ldots\ldots a^{60}=e\}$

" " " " 30 $= \langle a^{2} \rangle = \{a^{2}, a^{4}, a^{6}, a^{8}, a^{10}, \ldots\ldots a^{60}=e\}$

" " " " 60 $= \langle a \rangle = \{a, a^{2}, a^{3}, a^{4}, \ldots\ldots a^{60}=e\} = G$

(8) Let G be a cyclic group of order 18 generated by a.

Hence $G = \{a, a^2, a^3, a^4 \ldots\ldots a^{18}=e\}$

The divisors of 18 are 1, 2, 3, 6, 9, 18

We know (by Th 2.21) that for each divisor 'd' of 18 G has a sbgp of order d.

∴ Sbgps of G have orders 1, 2, 3, 6, 9, 18

Sbgp of order 1 $= \{a^{18}\} = e$

" " " 2 $= \{a^{9}\} = \{a^{9}, a^{18}=e\}$

" " " 3 $= \{a^{6}\} = \{a^{6}, a^{12}, a^{18}=e\}$

" " " 6 $= \{a^{3}\} = \{a^{3}, a^{6}, a^{9}, a^{12}, a^{15}, a^{18}\}$

" " " 9 $= \{a^{2}\} = \{a^{2}, a^{4}, a^{6}, a^{8}, a^{10}, a^{12}, a^{14}, a^{16}, a^{18}\}$

" " " 18 $= \{a\} = \{a, a^2, a^3 \ldots a^{18}=e\} = G$

2·2-33

Q) The elements of $(\bar{Z}'_{13}, \cdot)$ under multiplication 18 modulo 13 are $\{\bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}, \bar{8}, \bar{9}, \bar{10}, \bar{11}, \bar{12}\}$

$(\bar{2})^1 = \bar{2} \in \bar{Z}'_{13}$ $\quad (\bar{2})^2 = \bar{4} \in \bar{Z}'_{13}$

$(\bar{2})^3 = \bar{8} \in \bar{Z}'_{13}$ $\quad (\bar{2})^4 = \bar{3} \in \bar{Z}'_{13}$

$(\bar{2})^5 = \bar{6} \in \bar{Z}'_{13}$ $\quad (\bar{2})^6 = \bar{12} \in \bar{Z}'_{13}$

$(\bar{2})^7 = \bar{11} \in \bar{Z}'_{13}$ $\quad (\bar{2})^8 = \bar{9} \in \bar{Z}'_{13}$

$(\bar{2})^9 = \bar{5} \in \bar{Z}'_{13}$ $\quad (\bar{2})^{10} = \bar{10} \in \bar{Z}'_{13}$

$(\bar{2})^{11} = \bar{7} \in \bar{Z}'_{13}$ $\quad (\bar{2})^{12} = \bar{1} \in \bar{Z}'_{13}$

$13 \overline{)16}\ (1$, 13, 3 Remainder

$13 \overline{)128}\ (9$, 117, 11

$13 \overline{)256}\ (19$, 247, 9

$\therefore$ Each element of $\bar{Z}'_{13}$ can be written in the power of $\bar{2}$ so $\bar{Z}'_{13}$ is a cyclic gp generated by $\bar{2}$.

(i) $H_1 = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}, \bar{9}, \bar{11}\}$

$\bar{3} \times \bar{7} = \bar{8} \notin H_1 \Rightarrow H_1$ is not sbgp under $\cdot$ modulo 13.

(ii) $H_2 = \{\bar{1}, \bar{2}, \bar{4}, \bar{6}, \bar{8}, \bar{10}, \bar{12}\}$

$\bar{2} \times \bar{8} = \bar{3} \notin H_2 \Rightarrow H_2$ is not sbgp under $\cdot$ modulo 13.

(iii) $H_3 = \{\bar{1}, \bar{6}, \bar{8}, \bar{10}\}$

$\bar{6} \times \bar{8} = \bar{9} \notin H_2 \Rightarrow H_2$ is not a sbgp under $\cdot$ modulo 13

(iv) $H_4 = \{\bar{1}, \bar{3}, \bar{9}\}$ $\quad \forall a, b \in H \Rightarrow ab^{-1} \in H$. (required cond for sbgp)

$\bar{1} \cdot (\bar{3})^{-1} = \bar{1} \cdot \bar{9} = \bar{9} \in H_4$

$\bar{1} \cdot (\bar{9})^{-1} = \bar{1} \cdot \bar{3} = \bar{3} \in H_4$

$\therefore H_4$ is sbgp of $(\bar{Z}'_{13}, \cdot)$

$H_4 = [\bar{1}, \bar{3}, \bar{9}]$

$\bar{1}$ is identity

$\bar{1} \cdot (\bar{3})^{-1} = \bar{1} \cdot \bar{9} = \bar{9} \in H_4$

$\because \bar{3} \cdot \bar{9} = \bar{1}$

$\bar{1} \cdot (\bar{9})^{-1} = \bar{1} \cdot \bar{3} = \bar{3} \in H_4$

$\bar{1} \cdot \bar{1} = \bar{1}$

$\bar{1} \cdot (\bar{1})^{-1} = \bar{1} \cdot \bar{1} = 1 \in H$

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

Hence H_4 is subgroup of $(Z_{13}', \cdot)$