Let $H_1$ and $H_2$ be two subgroups of a group $G$, then $H_1 \subseteq H_2$ or $H_2 \subseteq H_1$ if and only if $H_1 \cup H_2$ is a subgroup.

**Proof:**

If $H_1 \subseteq H_2$, then $H_1 \cup H_2 = H_2$
$H_2$ is subgroup, hence $H_1 \cup H_2$ is subgroup.

$\underset{\sim}{\Leftarrow}$) we must show $H_1 \subseteq H_2$ or $H_2 \subseteq H_1$ suppose $H_1 \nsubseteq H_2$ or $H_2 \nsubseteq H_1$.
$$\left.\begin{matrix} H_1 \& H_2 \Rightarrow \exists a \in H_1 \& a \& H_2 \\ H_2 \& H_1 \Rightarrow \exists\, b \in H_2 \&\, b \notin H_1 \end{matrix}\right\} a, b \in H_1 \cup H_2$$
But $H_1 \cup H_2$ is subgroup, thenab $b^{-1} \in H_1 \cup H_2$.
So either $ab^{-1} \in H_1, ab^{-1} = h_1$ where
$h_1 \in H_1 \Rightarrow h_1^{-1}a = b \in H_1$C ! $h_2 b = a$
or $ab^{-1} \in H_2, ab^{-1} = h_2$ where $h_2 \in' 2 \Rightarrow h_2^{-1}a \leq \in H$

**Definition:**

Let $H$ be a subgroup of a group $G$, then $H$ is called a proper subgroup of $G$ if $H \neq G$.

**Corollary:**

A group $G$ cannot be the union of two of its proper subgroups.

**Proof:**

Let $H_1$ and $H_2$ be two proper subgroups i.e., $H_1 \neq G$ and $H_2 \neq G$ Suppose $H_1 \cup H_2 = G$, then by theorem
[ $H_1 \subseteq H_2$ or $H_2 \subseteq H_1 \Leftrightarrow H_1 \cup H_2$ is subgroup]
If $H_1 \subseteq H_2$, then $H_1 \cup H_2 = H_2 = G\ C!$ [ Since $H_2 \neq G$ ].
If $H_2 \subseteq H_1$, then $H_1 \cup H_2 = H_1 = G\ C!$ ~Since $H_1 \neq G$].

**Exampl:**

Let $G = \{e, b, c, a\}, \forall a \in G, a^2 = e$

| * | e | a | b | c |
|---|---|---|---|---|
| e | e | a | b | c |

| | | | | |
|---|---|---|---|---|
| a | a | e | c | b |
| b | b | c | e | a |
| c | c | b | a | e |

$H_1 = \{e, a\}, H_2 = \{e, b\}, H_3 = \{e, c\}.$

**Definition:**

Let $G$ be a group, then Cent $G = \{a \in G: ax = xa, V'x \in G\}$ the Cent $G$ is called the center of $G$.

**Remark:**

(1) Cent $G \nexists \emptyset [e \in \text{Cent } G]$
(2) Cent $G = G \Leftrightarrow G$ is abelian.

**Example:**

Gent-GS $= \{\sum, T_2\}$

$$\text{Cent } S_3 = \{\alpha_1\}$$

**Theorem:**

Let $G$ be a group, then Cent $G$ is subgroup.

**Proof:**

Cent $G \neq \emptyset$

$$[e \in \text{ cent } u]$$

Let $a, b \in \text{Cent}G$, then $ax = xa \forall x \in G$ and $bx = xb \forall x \in G$
We must show that $ab^{-1} \in \text{Cent } G$ i.e $x(ab^{-1}) = (ab^{-1})x$

$$
\begin{aligned}
x(ab^{-1}) &= (xa)b^{-1} = (ax)b^{-1} \\
&= a(xb^{-1}) = a(bx^{-1})^{-1} \\
&= a(x^{-1}b)^{-1} = ab^{-1}(x^{-1})^{-1} \\
&= (ab^{-1})x
\end{aligned}
$$

**Definition:**

Let $S$ be a non empty subset of $G$, then the intersection of all subgroups of $G$ containing $S$ is denoted by $\langle S\rangle$ which is called the subgroup generated by $S$.
$\langle S\rangle = \cap\,\{H: H$ is subgroup of $G, H \supseteq S\}$
$S \subseteq \langle S\rangle$
$< S\rangle \neq \emptyset$ [ $G$ is subgroup containing $S$ ]
$\langle S\rangle = S$ if and only if $\mathfrak{S}$ is subgroup

**Definition:**

Let $S$ be a non empty subset of $G$ if $S$ is finite, and then $\langle S\rangle$ is called finitely generated. In particular if $S = \{a\}$. Then $\langle S\rangle = \langle a\rangle$ is called cyclic subgroup.

$$\langle a\rangle = \{na: n \in Z\}$$

$S = \{1\}$
$$\langle 1\rangle = \begin{Bmatrix} 0,1,2,3,4,\ldots \\ -1,-2,-3,-4,\ldots \end{Bmatrix}$$

**Definition:**

A group $G$ is said to be cyclic with generator $a$ if $G = \langle a\rangle$ for some $a \in G$.

**Example:**

The group $(Z_6, +_6)$ is cyclic.
Sol:

$$
\begin{aligned}
&< \bar{1} >= \{\bar{1},\bar{2},\bar{3},\bar{4},\bar{5},\bar{0}\} \\
&< \bar{2} >= \{\bar{2},\bar{4},\bar{0}\} =< \bar{4} >= \{\bar{4},\bar{2},\bar{0}\} \\
&< \bar{3} >= \{\bar{3},\bar{0}\} =< \bar{5} >= \{\bar{5},\bar{4},\bar{3},\bar{2},\bar{1},\bar{0}\} \\
&\mathrm{Z}_6 =< \bar{1} >
\end{aligned}
$$

**Example:**

Is $Z = \langle 1 \rangle$ ? To prove $2 \leq < 1\rangle$
First $\langle 1 \rangle \subseteq Z, k1\rangle = \{n.1 : n \in Z\}$, so that 數

$$\text{Hetes } n = \underbrace{1 + 1 + \cdots + 1}_{\text{n tims}} = 1^n$$

Hence $n \in < 1 >$ and $Z \subseteq < 1 >$
Thus $Z = \langle 1 \rangle$.

**Example :**

$G = \{e, b, c, a\}, \forall a \in G, a^2 = e, G$ is called Klein 4-group, is not cyclic.

$$b^2 = e, c^2 = e$$

| * | e | a | b | c |
|---|---|---|---|---|
| e | e | a | b | c |
| a | a | e | c | b |
| b | b | c | c | a |
| c | c | b | a | e |

$$< e\rangle = \{e\} \neq G$$
$$< a >= \{e, a\} \neq G$$
$$< c >= \{e, c\} \neq G$$

**Example:**

Let $G$ be a group, $H = \{a \in G : a^k = e, k \in Z\}$, then $H$ is subgroup .
Solution: $H \not\subset \emptyset$ since at least $e \in H$.
Let $a, b \in H$, i.e $\exists k \in Z$ such that $a^k = e$
$\exists n \in Z$ such that $b^n = e$
We have to prove $a * b^{-1} \in H$
i.e., $(a * b^{-1})^m = e; m \in Z$
$(a * b^{-1})^{kn} = a^{kn} * (b^{-1})^{nk} = a^{kn} * (b^n)^{-k} = e^n * e^{-k} = e$

Hence $a * b^{-1} \in H_{;}(m = kn)$.
Thus $H$ is subgroup.

**Remark:**

Let $G$ be a group and let $a \in G$, then:
$\langle a \rangle = \{a^0, a^1, a^2, \dots, a^{-1}, a^{-2}, \dots\} = \{a^n : n \in Z\}$.

**Theorem:**

Every cyclic group is abelian.
Proof: Let $G$ be a cyclic group, $\Rightarrow G = \langle a \rangle$
let $x, y \in G, x = a^n, y = a^m; m, n \in Z$
$xy = a^n a^m = a^{n+m} = a^{m+n} = yx$
The converse is not true.

**Example:**

(Klein 4-group) is abelian but not cyclic.

**Definition:**

The order of $G$ denoted by $O(G)$ is the number of element of $G$ if $G$ is is infinite then we say that $G$ has infinite order.

**Theorem:**

Let $G = \langle a \rangle$ be a finite group with $O(G) = n$, then:

$$G = \{e, a, a^2, \dots, a^{n-1}\}$$

Proof: Since $\mathrm{a} \in \mathrm{G}$ and G is group, then $\mathrm{a}, \mathrm{a}^2, \mathrm{a}^3, \dots \in \mathrm{G}$
But $G$ is finite, so $\exists k, J \in Z_{+}$such that $a^k = a^J$ and $k > J$
$\Rightarrow \mathrm{a}^{\mathrm{k-J}} = \mathrm{e}$ with $\mathrm{k} - \mathrm{J} > 0$
ie., the set of positive integers $t$ such that $a^t = e$ is not empty
By the well ordering principle let m be the smallest positive integer such that $\mathrm{a}^{\mathrm{m}} = e$
Let $S = \{e, a, a^2, \dots, a^{m-1}\}$ all element of $S$ are distinct [ if $a^{\ell} = a^{\mathrm{k}}$; $0 \le \ell < \mathrm{k} < \mathrm{m} - 1$ ], implies $a^{k-\ell} = \mathrm{eC}$ !, since m is the smallest one let $w \in G$, then $w = a^r; r \in Z$
Now $\mathrm{r}, \mathrm{m}$ by the division algorithm theorem