# Applications of Group Theory

## References:


- Introduction to Modern Abstract Algebra, by David M. Burton.
- Groups and Numbers, by R. M. Luther.
- A First Course in Abstract Algebra, by J. B. Fraleigh.
- Group Theory, by M. Suzuki.
- Abstract Algebra Theory and Applications, by Thomas W. Judson.
- Abstract Algebra, by I. N. Herstein.
- Basic Abstract Algebra, by P. B. Bhattacharya, S. K. Jain and S. R. Nagpaul.

# 1. The Jordan-Holder Theorem and Related Concepts.

**Definition(1-1):**

By a *chain* for a group $(G,*)$ is meant any finite sequence of subsets of

$G = H_0 \supset H_1 \supset \cdots \supset H_{n-1} \supset H_n = \{e\}$ descending from $G$ to $\{e\}$ with the property that all the pairs $(H_i,*)$ are subgroups of $(G,*)$.

**Remark(1-2):**

The integer $n$ is called the length of the chain. When $n = 1$, then the chain in definition (1-1) will called the trivial.

**Example(1-3):**

Find all chains in a group $(Z_4, +_4)$.

**Solution:** The subgroups of a group $(Z_4, +_4)$ are :

- $H_1 = (Z_4, +_4)$
- $H_2 = (\{0\}, +_4)$
- $H_3 = (\langle 2 \rangle, +_4) = (\{0,2\}, +_4)$

The chains of a group $(\mathrm{Z}_4, +_4)$ are

$$\mathrm{Z}_4 \supset \{0\} \text{ is a chain of length one}$$

$$\mathrm{Z}_4 \supset \langle 2 \rangle \supset \{0\} \text{ is a chain of length two.}$$

**Example(1-4):**

In the group $(\mathrm{Z}_{12}, +_{12})$ of integers modulo 12, the following chains are normal chains:

$$\mathrm{Z}_{12} \supset \langle 6 \rangle \supset \{0\},$$

$$\mathrm{Z}_{12} \supset \langle 2 \rangle \supset \langle 4 \rangle \supset \{0\},$$

$$\mathrm{Z}_{12} \supset \langle 3 \rangle \supset \langle 6 \rangle \supset \{0\},$$

$$\mathrm{Z}_{12} \supset \langle 2 \rangle \supset \langle 6 \rangle \supset \{0\}.$$

All subgroups are normal, since $(\mathrm{Z}_{12}, +_{12})$ is a commutative group.

**Definition(1-5):** (***Normal Chain***)

If $(H_i,*)$ is a normal subgroup of a group $(G,*)$ for all $i = 1, \dots, n$, then the chain $G = H_0 \supset H_1 \supset \cdots \supset H_{n-1} \supset H_n = \{e\}$ is called a *normal chain*.

**Example(1-6):**

Find all chains in the following groups and determine their length and type.

- $(Z_6, +_6)$;
- $(Z_8, +_8)$;
- $(Z_{18}, +_{18})$ (**Homework**);
- $(Z_{21}, +_{21})$ (**Homework).**

**Solution:** The subgroups of a group $(Z_6, +_6)$ are :

$H_1 = (Z_6, +_6)$

$H_2 = (\{0\}, +_6)$

$H_3 = (\langle 2 \rangle, +_6) = (\{0,2,4\}, +_6)$

$H_4 = (\langle 3 \rangle, +_6) = (\{0,3\}, +_6)$

Then the chains in $(Z_6, +_6)$ are:

$Z_6 \supset \{0\}$ is a trivial chain of length one

$Z_6 \supset \langle 2 \rangle \supset \{0\}$ is a normal chain of length two

$Z_6 \supset \langle 3 \rangle \supset \{0\}$ is a normal chain of length two.

The subgroups of a group $(Z_8, +_8)$ are :

$H_1 = (Z_8, +_8)$

$H_2 = (\{0\}, +_8)$

$H_3 = (\langle 2\rangle, +_8) = (\{0,2,4,6\}, +_8)$

$H_4 = (\langle 4\rangle, +_6) = (\{0,4\}, +_8)$

Then the chains in $(Z_8, +_8)$ are:

$Z_8 \supset \{0\}$ is a trivial chain of length one

$Z_8 \supset \langle 2\rangle \supset \{0\}$ is a normal chain of length two

$Z_8 \supset \langle 4\rangle \supset \{0\}$ is a normal chain of length two

$Z_8 \supset \langle 2\rangle \supset \langle 4\rangle \supset \{0\}$ is a normal chain of length three.

**Definition(1-7):** (***Composition Chain***)

In the group $(G,*)$, the descending sequence of sets

$$G = H_0 \supset H_1 \supset \cdots \supset H_{n-1} \supset H_n = \{e\}$$

forms a *composition chain* for $(G,*)$ provided

1. $(H_i,*)$ is a subgroup of $(G,*)$,
2. $(H_i,*)$ is a normal subgroup of $(H_{i-1},*)$,

3. The inclusion $H_{i-1} \supseteq K \supseteq H_i$, where $(K,*)$ is a normal subgroup of $(H_{i-1},*)$, implies either $K = H_{i-1}$ or $K = H_i$.

**Remark(1-8):**

Every composition chain is a normal, but the converse is not true in general, the following example shows that.

**Example(1-9):**

In the group $(\mathrm{Z}_{24}, +_{24})$, the normal chain

$$\mathrm{Z}_{24} \supset \langle 2 \rangle \supset \langle 12 \rangle \supset \{0\}$$

is not a composition chain, since it may be further refined by inserting of the set$\langle 4 \rangle$ or $\langle 6 \rangle$. On other hand,

$$\mathrm{Z}_{24} \supset \langle 2 \rangle \supset \langle 4 \rangle \supset \langle 8 \rangle \supset \{0\}$$

and

$$\mathrm{Z}_{24} \supset \langle 3 \rangle \supset \langle 6 \rangle \supset \langle 12 \rangle \supset \{0\}$$

are both composition chains for $(\mathrm{Z}_{24}, +_{24})$.

**Example(1-10):**

Find all chains in the following groups and determine their length and type.

- $(\mathrm{Z}_8, +_8)$;
- $(\mathrm{Z}_{12}, +_{12})$;
- $(\mathrm{Z}_{18}, +_{18})$ (**Homework**).

**Solution:** The subgroups of a group $(\mathrm{Z}_8, +_8)$ are :

$H_1 = (\mathrm{Z}_8, +_8)$

$H_2 = (\{0\}, +_8)$

$H_3 = (\langle 2 \rangle, +_8) = (\{0,2,4,6\}, +_8)$

$H_4 = (\langle 4 \rangle, +_8) = (\{0,4\}, +_8)$

Then the chains in $(\mathrm{Z}_8, +_8)$ are:

$\mathrm{Z}_8 \supset \{0\}$ is a trivial chain of length one.

$\mathrm{Z}_8 \supset \langle 2 \rangle \supset \{0\}$ is a normal chain of length two, but it is not composition chain, since there is a normal subgroup $\langle 4 \rangle$ in $\mathrm{Z}_8$, such that $\langle 2 \rangle \supset \langle 4 \rangle$.

$Z_8 \supset \langle 4 \rangle \supset \{0\}$ is a normal chain of length two, but it is not composition chain, since there is a normal subgroup $\langle 2 \rangle$ in $Z_8$, such that $\langle 2 \rangle \supset \langle 4 \rangle$.

$Z_8 \supset \langle 2 \rangle \supset \langle 4 \rangle \supset \{0\}$ is a composition chain of length three.

The subgroups of a group $(Z_{12}, +_{12})$ are :

$H_1 = (Z_{12}, +_{12})$

$H_2 = (\{0\}, +_{12})$

$H_3 = (\langle 2 \rangle, +_{12}) = (\{0,2,4,6,8,10\}, +_{12})$

$H_4 = (\langle 3 \rangle, +_{12}) = (\{0,3,6,9\}, +_{12})$

$H_5 = (\langle 4 \rangle, +_{12}) = (\{0,4,8\}, +_{12})$

$H_6 = (\langle 6 \rangle, +_{12}) = (\{0,6\}, +_{12})$

Then the chains in $(Z_{12}, +_{12})$ are:

$Z_{12} \supset \{0\}$ is a trivial chain of length one.

$Z_{12} \supset \langle 2 \rangle \supset \{0\}$ is a normal chain of length two.

$Z_{12} \supset \langle 3 \rangle \supset \{0\}$ is a normal chain of length two.

$Z_{12} \supset \langle 4 \rangle \supset \{0\}$ is a normal chain of length two.

$Z_{12} \supset \langle 6 \rangle \supset \{0\}$ is a normal chain of length two.

$Z_{12} \supset \langle 2 \rangle \supset \langle 4 \rangle \supset \{0\}$ is a composition chain of length three.

$Z_{12} \supset \langle 3 \rangle \supset \langle 6 \rangle \supset \{0\}$ is a composition chain of length three.

**Example(1-11):**

Let $(G,*)$ be the group of symmetries of the square.

A normal chain for $(G,*)$ which fails to be a composition chain is

$$G \supset \{R_{180}, R_{360}\} \supset \{R_{360}\}.$$

**Example(1-12): (Homework)**

Determine the following chain whether normal, composition:

$$G \supset \{R_{90}, R_{180}, R_{270}, R_{360}\} \supset \{R_{180}, R_{360}\} \supset \{R_{360}\}.$$

**Example(1-13):**

The group $(\mathrm{Z},+)$ has no a composition chain, since the normal subgroups of $(\mathrm{Z},+)$ are the cyclic subgroups $(\langle \mathrm{n} \rangle),+)$, n a nonnegative integer, Since the inclusion $\langle \mathrm{kn} \rangle \subseteq \langle n \rangle$ holds for all $\mathrm{k} \in \mathrm{Z}_+$, there always exists a proper subgroup of any given group.

**Definition(1-14):**

A normal subgroup $(H,*)$ is called a *maximal normal subgroup* of the group $(G,*)$ if $H \neq G$ and there exists no normal subgroup $(K,*)$ of $(G,*)$ such that $H \subset K \subset G$.

**Example(1-15):**

In the group $(\mathrm{Z}_{24},+_{24})$, the cyclic subgroups $(\langle 2 \rangle,+_{24})$ and $(\langle 3 \rangle,+_{24})$ are both maximal normal with orders 12 and 8, respectively.

**Example(1-16):**

Determine the maximal normal subgroups in the group $(\mathrm{Z}_{12},+_{12})$.

**Solution:** The normal subgroups of $(\mathrm{Z}_{12}, +_{12})$ are:

$H_1 = (\langle 2\rangle, +_{12}) = (\{0,2,4,6,8,10\}, +_{12})$

$H_2 = (\langle 3\rangle, +_{12}) = (\{0,3,6,9\}, +_{12})$

$H_3 = (\langle 4\rangle, +_{12}) = (\{0,4,8\}, +_{12})$

$H_4 = (\langle 6\rangle, +_{12}) = (\{0,6\}, +_{12})$

The maximal normal subgroups of $(\mathrm{Z}_{12}, +_{12})$ are $H_1$ and $H_2$, since there is no normal subgroup in $\mathrm{Z}_{12}$ containing $H_1$ and $H_2$.

**Remark(1-17):**

A chain $G = H_0 \supset H_1 \supset \cdots \supset H_{n-1} \supset H_n = \{e\}$ is a composition of a group $(G,*)$, if each normal subgroup $(H_i,*)$ is a maximal normal subgroup of $(H_{i-1},*)$, for all $i = 1, \dots, n$.

**Example(1-18);**

In the group $(\mathrm{Z}_{12}, +_{12})$ the chains $\mathrm{Z}_{12} \supset \langle 2\rangle \supset \langle 4\rangle \supset \{0\}$ is a composition of $\mathrm{Z}_{12}$ , since

$\langle 2\rangle$ is a maximal normal subgroup of $\mathrm{Z}_{12}$,

$\langle 4\rangle$ is a maximal normal subgroup of $\langle 2\rangle$,

$\{0\}$ is a maximal normal subgroup of $\langle 4\rangle$, and

$Z_{12} \supset \langle 3\rangle \supset \langle 6\rangle \supset \{0\}$ is a composition of $Z_{12}$, since

$\langle 3\rangle$ is a maximal normal subgroup of $Z_{12}$,

$\langle 6\rangle$ is a maximal normal subgroup of $\langle 3\rangle$,

$\{0\}$ is a maximal normal subgroup of $\langle 6\rangle$.

**Theorem(1-19):**

A normal subgroup $(H,*)$ of the group $(G,*)$ is a maximal if and only if the quotient $({}^{G}/_{H},\otimes)$ is a simple.

**Proof:**

$\Rightarrow$) Let $K$ be a normal subgroup of $G$ with $H \subseteq K$ there corresponds between $({}^{G}/_{H},\otimes)$ and $({}^{K}/_{H},\otimes)$ such that this correspondence is one-to-one. Hence, $H$ is a maximal normal in $K$ $\Rightarrow H$ is a maximal normal in $G$ ( by correspondence) $\Rightarrow {}^{G}/_{H}$ is a simple.

$\Leftarrow$) let ${}^{G}/_{H}$ be a simple

$\Rightarrow {}^{G}/_{H}$ has two normal subgroups which are $e * H$ and ${}^{G}/_{H}$, but $e * H = H$

Therefore $H$ is a maximal ■

**Corollary(1-20):**

The group $({}^{G}/_{H}, \otimes)$ is a simple, if $\left|{}^{G}/_{H}\right|$ is a prime number.

**Examples(1-21);**

1. Show that $(\langle 2\rangle, +_{12})$ is a maximal normal subgroup of $(\mathrm{Z}_{12}, +_{12})$.
2. Show that $(\langle 3\rangle, +_{15})$ is a maximal normal subgroup of $(\mathrm{Z}_{15}, +_{15})$. (**Homework**)

**Solution(1):** $(\langle 2\rangle, +_{12}) = (\{0,2,4,6,8,10\}, +_{12})$

$\left|{}^{G}/_{H}\right| = \frac{|G|}{|H|} = \frac{|\mathrm{Z}_{12}|}{|\langle 2\rangle|} = \frac{12}{6} = 2$ is a prime $\Rightarrow \frac{\mathrm{Z}_{12}}{\langle 2\rangle}$ is a simple (by Corollary (1-20)). From Theorem (1-19), we get that $\langle 2\rangle$ is a maximal normal subgroup of $\mathrm{Z}_{12}$.

**Corollary(1-22):**

A normal chain $G = H_0 \supset H_1 \supset \cdots \supset H_{n-1} \supset H_n = \{e\}$ is a composition of a group $(G,*)$, if $\left({}^{H_i}/_{H_{i-1}}, \otimes\right)$ is a simple group for all $i = 1, \ldots, n$.

**Example(1-23);**

Show that $\mathrm{Z}_{60} \supset \langle 3 \rangle \supset \langle 6 \rangle \supset \langle 12 \rangle \supset \{0\}$ is a composition chain of a group $(\mathrm{Z}_{60}, +_{60})$.

**Solution:** $\frac{|\mathrm{Z}_{60}|}{|\langle 3 \rangle|} = \frac{60}{20} = 3$ is a prime $\Rightarrow \frac{\mathrm{Z}_{60}}{\langle 3 \rangle}$ is a simple.

So, we get that $\langle 3 \rangle$ is a maximal normal subgroup of $\mathrm{Z}_{60}$.

$\frac{|\langle 3 \rangle|}{|\langle 6 \rangle|} = \frac{20}{10} = 2$ is a prime $\Rightarrow \frac{\langle 3 \rangle}{\langle 6 \rangle}$ is a simple.

So, we get that $\langle 6 \rangle$ is a maximal normal subgroup of $\langle 3 \rangle$.

$\frac{|\langle 6 \rangle|}{|\langle 12 \rangle|} = \frac{10}{5} = 2$ is a prime $\Rightarrow \frac{\langle 6 \rangle}{\langle 12 \rangle}$ is a simple.

So, we get that $\langle 12 \rangle$ is a maximal normal subgroup of $\langle 6 \rangle$.

$\frac{|\langle 12 \rangle|}{|\{0\}|} = \frac{5}{1} = 5$ is a prime $\Rightarrow \frac{\langle 12 \rangle}{\{0\}}$ is a simple.

So, we get that $\{0\}$ is a maximal normal subgroup of $\langle 12 \rangle$.

By corollaries (1-19) and (1-21), we have that $Z_{60} \supset \langle 3 \rangle \supset \langle 6 \rangle \supset \langle 12 \rangle \supset \{0\}$ is a composition chain of a group $(Z_{60}, +_{60})$.

**Theorem(1-24):**

Every finite group $(G,*)$ with more than one element has a composition chain.

**Theorem(1-25): (Jordan-Holder)**

In a finite group $(G,*)$ with more than one element, any two composition chains are equivalent.

**Example(1-26):**

In a group $(Z_{60}, +_{60})$, show that the two chains

$$Z_{60} \supset \langle 3 \rangle \supset \langle 6 \rangle \supset \langle 12 \rangle \supset \{0\}$$

$$Z_{60} \supset \langle 2 \rangle \supset \langle 6 \rangle \supset \langle 30 \rangle \supset \{0\},$$

are compositions and equivalent.

**Solution:**

$\left({}^{Z_{60}}/_{\langle 3\rangle}, \otimes\right) \cong \left({}^{\langle 2\rangle}/_{\langle 6\rangle}, \otimes\right)$, since $\left|{}^{Z_{60}}/_{\langle 3\rangle}\right| = \frac{60}{20} = 3 = \left|{}^{\langle 2\rangle}/_{\langle 6\rangle}\right| = \frac{30}{10}$,

$\left({}^{\langle 3\rangle}/_{\langle 6\rangle}, \otimes\right) \cong \left({}^{Z_{60}}/_{\langle 2\rangle}, \otimes\right)$, since $\left|{}^{\langle 3\rangle}/_{\langle 6\rangle}\right| = \frac{20}{10} = 2 = \left|{}^{Z_{60}}/_{\langle 2\rangle}\right| = \frac{60}{30}$,

$\left({}^{\langle 6\rangle}/_{\langle 12\rangle}, \otimes\right) \cong \left({}^{\langle 30\rangle}/_{\{0\}}, \otimes\right)$, since $\left|{}^{\langle 6\rangle}/_{\langle 12\rangle}\right| = \frac{10}{5} = 2 = \left|{}^{\langle 30\rangle}/_{\{0\}}\right| = \frac{2}{1}$,

$\left({}^{\langle 12\rangle}/_{\{0\}}, \otimes\right) \cong \left({}^{\langle 6\rangle}/_{\langle 30\rangle}, \otimes\right)$, since $\left|{}^{\langle 12\rangle}/_{\{0\}}\right| = \frac{5}{1} = 5 = \left|{}^{\langle 6\rangle}/_{\langle 30\rangle}\right| = \frac{10}{2}$.

Therefore, by Jordan-Holder theorem the two chains

$$Z_{60} \supset \langle 3\rangle \supset \langle 6\rangle \supset \langle 12\rangle \supset \{0\}$$

$$Z_{60} \supset \langle 2\rangle \supset \langle 6\rangle \supset \langle 30\rangle \supset \{0\},$$

are compositions and equivalent.

**<u>Exercises(1-27):</u>**

- Check that the following chains represent composition chains for the indicated group.

a. For $(\mathrm{Z}_{36}, +_{36})$, the group of integers modulo 36:

$$\mathrm{Z}_{36} \supset \langle 3 \rangle \supset \langle 9 \rangle \supset \langle 18 \rangle \supset \{0\}.$$

b. For $(G_s, *)$, the group of symmetries of the square:

$$G \supset \{R_{180}, R_{360}, D_1, D_2\} \supset \{R_{360}, D_1\} \supset \{R_{360}\}.$$

c. For $(\langle a \rangle, *)$, a cyclic group of order 30:

$$\langle a \rangle \supset \langle a^5 \rangle \supset \langle a^{10} \rangle \supset \{e\}.$$

d. For $(S_3, \circ)$, the symmetric group on 3 symbols:

$$S_3 \supset \{i, (123), (132)\} \supset \{i\}.$$

- Find a composition chain for the symmetric group $(S_4, \circ)$.
- Prove that the cyclic subgroup $(\langle n \rangle, +)$ is a maximal normal subgroup of $(\mathrm{Z}, +)$ if and only if $n$ is a prime number.
- Establish that the following two composition chains for $(\mathrm{Z}_{36}, +_{36})$ are equivalent:

$$Z_{24} \supset \langle 3 \rangle \supset \langle 6 \rangle \supset \langle 12 \rangle \supset \{0\},$$

$$Z_{24} \supset \langle 2 \rangle \supset \langle 4 \rangle \supset \langle 12 \rangle \supset \{0\}.$$

- Find all composition chains for $(Z_{36}, +_{36})$.
- Find all composition chains for $(G_s, *)$.

## 2. P- Groups and Related Concepts.

**Definition(2-1):** (**p- Group**)

A finite group $(G,*)$ is said to be $p$- *group* if and only if the order of each element of $G$ is a power of fixed prime $p$.

**Definition(2-2):** (**p- Group**)

A finite group $(G,*)$ is said to be $p$- *group* if and only if $|G| = p^k, k \in Z$, where $p$ is a prime number.

**Example(2-3):**

Show that $(Z_4, +_4)$ is a p- group.

**Solution:** $Z_4 = \{0,1,2,3\}$ and $|\ Z_4| = 4 = 2^2$

$\Rightarrow$ $Z_4$ is a 2- group, with

$o(0) = 1 = 2^0$,

$o(1) = 4 = 2^2$,

$o(2) = 2 = 2^1$,

$o(3) = 4 = 2^2$.

**Example(2-4):**

Determine whether $(Z_6, +_6)$ is a p- group.

**Solution:** $Z_6 = \{0,1,2,3,4,5\}$ and $|\ Z_6| = 6 \neq P^k$

$\Rightarrow$ $Z_6$ is not p- group.

**Example(2-5): (Homework)**

Determine whether $(G_s,\circ)$ is a p- group.

**Examples(2-6):**

- $(Z_8,+_8)$ is a 2- group, since $|Z_8| = 8 = 2^3$,
- $(Z_9,+_9)$ is a 3- group, since $|Z_9| = 9 = 3^2$,
- $(Z_{25},+_{25})$ is a 5- group, since $|Z_{25}| = 25 = 5^2$.

**Theorem(2-7):**

Let $H\Delta G$, then G is a p- group if and only if H and ${}^{G}/_{H}$ are p- groups.

**Proof:** $(\Longrightarrow)$ Assume that G is a p- group, to prove that H and ${}^{G}/_{H}$ are p- groups.

Since G is a p- group $\Longrightarrow$ $o(a) = p^x$, for some $x \in Z^+, \forall a \in G$.

Since $H \subseteq G \Longrightarrow \forall a \in H$ group $\Longrightarrow$ $o(a) = p^x$, for some $x \in Z^+$.

So, H is a p- group.

To prove ${}^{G}/_{H}$ is a p- group.

Let $a * H \in {}^{G}/_{H}$, to prove $o(a * H)$ is a power of p.

$(a * H)^{p^x} = a^{p^x} * H = e * H = H$, $(a^{p^x} = e$ since G is a p- group$\Longrightarrow$ o(a) = $p^x$ )

($\Longleftarrow$) Suppose that H and ${}^{G}/_{H}$ are p- groups, to prove G is a p- group.

Let $a \in H$, to prove $o(a)$ is a power of p.

$(a * H)^{p^x} = H \ldots (1)$ (${}^{G}/_{H}$ is a p- group)

$(a * H)^{p^x} = a^{p^x} * H \ldots (2)$

From (1) and (2), we have $a^{p^x} * H = H \Longrightarrow a^{p^x} \in H$ and $H$ is a p- group,

$\Longrightarrow o\left(a^{p^x}\right) = p^r, r \in Z^+$

$\Longrightarrow \left(a^{p^x}\right)^{p^r} = e \Longrightarrow a^{p^{x+r}} = e,\ x + r \in Z^+,$

$\Longrightarrow o(a) = p^{x+r}$

Therefore, G is a p- group ■

**<u>Examples(2-8):</u>**

Apply theorem(2-7) on $(Z_{32}, +_{32})$.

**Solution:**

$|Z_{32}| = 32 = 2^5$ is a 2- group.

By theorem (2-7), H and $G/_H$ are 2- groups.

$o(G)/_{o(H)} \Rightarrow o(H) = 2^x, 0 \leq x \leq 5.$

$o(H) = 2^0$ or $2^1$ or $2^2$ or $2^3$ or $2^4$ or $2^5$,

$o(H) = 2^0$ is a 2- group $\Rightarrow o(G/_H) = o(G)/_{o(H)} = \frac{2^5}{2^0} =$ $2^5$ is a 2- group.

$o(H) = 2^1$ is a 2- group $\Rightarrow o(G)/_{o(H)} = 2^4$

$o(H) = 2^2$ is a 2- group $\Rightarrow o(G)/_{o(H)} = 2^3$

$o(H) = 2^3$ is a 2- group $\Rightarrow o(G)/_{o(H)} = 2^2$

$o(H) = 2^4$ is a 2- group $\Rightarrow o(G)/_{o(H)} = 2$

$o(H) = 2^5$ is a 2- group $\Rightarrow o(G)/_{o(H)} = 1.$

**Remark(2-9);**

If G is a non-trivial p- group, then $\mathrm{Cent(G)} \neq e$.

**Theorem(2-10):**

Every group of order $p^2$ is an abelian.

**Proof:** Let G be a group of order $p^2$, to prove G is an abelian.

Let Cent(G) is a subgroup of G.

By Lagrange Theorem $\mathrm{o(G)} / o(\mathrm{Cent(G)})$ ,

$\Longrightarrow p^2 / o(\mathrm{Cent(G)})$

$\Longrightarrow o(\mathrm{Cent(G)}) = p^0$ or $p^1$ or $p^2$

If $o(\mathrm{Cent(G)}) = p^0 \Longrightarrow o(\mathrm{Cent(G)}) = \{e\}$, but this is contradiction with remark(2-9), so $o(\mathrm{Cent(G)}) \neq p^0$.

If $o(\mathrm{Cent(G)}) = p^2 = o(G) \Longrightarrow \mathrm{Cent(G)} = G$

$\Longrightarrow G$ is an abelian.

If $o\left(\mathrm{Cent(G)}\right) = \mathrm{p}^1 \Rightarrow o\left({}^{G}/_{\mathrm{Cent(G)}}\right) = \frac{\mathrm{p}^2}{\mathrm{p}^1} = \mathrm{p}$

${}^{G}/_{\mathrm{Cent(G)}}$ is a cyclic.

Therefore, $G$ is an abelian ■

**Remark(2-11):**

The converse of theorem(2-10) is not true in general, for example $(\mathrm{Z}_8, +_8)$ is an abelian, but $o((\mathrm{Z}_8) = 2^3 \neq p^2$.

**Exercises(2-12):**

- Let $P$ and $Q$ be two normal p-subgroups of a finite group $G$. Show that $PQ$ is a normal p-subgroup of $G$.
- Determine whether $(\mathrm{Z}_{125}, +_{125})$ is a p-group.
- Determine whether $(\mathrm{Z}_{121}, +_{121})$ is a p-group.
- Determine whether $(\mathrm{Z}_{41}, +_{41})$ is a p-group.
- Determine whether $(\mathrm{Z}_{16}, +_{16})$ is a p-group.
- Determine whether $(\mathrm{Z}_{625}, +_{625})$ is a p-group.
- Determine whether $(\mathrm{Z}_{185}, +_{185})$ is a p-group.
- Determine whether $(\mathrm{Z}_{128}, +_{128})$ is a p-group.
- Determine whether $(\mathrm{Z}_{256}, +_{256})$ is a p-group.

- Determine whether $(Z_{100}, +_{100})$ is a p-group.
- Show that $G_{\ell} = \{\pm 1, \pm i, \pm j, \pm k\}, \cdot)$ is a p-group.

## 3. Sylow Theorem

**Definition(3-1):** (***Sylow p- Subgroup***)

Let $(G,*)$ be a finite group and p is a prime number, a subgroup $(H,*)$ of a group $G$ is called *sylow p- subgroup* if

1. $(H,*)$ is a p- group,
2. $(H,*)$ is not contained in any other p- subgroup of $G$ for the same prime number p.

**Example(3-2);**

Find sylow 2- subgroups and sylow 3- subgroup of the group $(Z_{24}, +_{24})$.

**Solution:** The proper subgroups of the group $(Z_{24}, +_{24})$ are

1. $(\langle 2\rangle, +_{24}) \Longrightarrow o(\langle 2\rangle) = 12 \neq P^k \Longrightarrow \langle 2\rangle$ is not p-subgroup.
2. $(\langle 3\rangle, +_{24}) \Longrightarrow o(\langle 3\rangle) = 8 = 2^3 \Longrightarrow \langle 3\rangle$ is a 2-subgroup.
3. $(\langle 4\rangle, +_{24}) \Longrightarrow o(\langle 4\rangle) = 6 \neq P^k \Longrightarrow \langle 4\rangle$ is not p-subgroup.
4. $(\langle 6\rangle, +_{24}) \Longrightarrow o(\langle 6\rangle) = 4 = 2^2 \Longrightarrow \langle 6\rangle$ is a 2-subgroup.
5. $(\langle 8\rangle, +_{24}) \Longrightarrow o(\langle 8\rangle) = 3 = 3^1 \Longrightarrow \langle 8\rangle$ is a 3-subgroup.
6. $(\langle 12\rangle, +_{24}) \Longrightarrow o(\langle 12\rangle) = 2 = 2^1 \Longrightarrow \langle 12\rangle$ is a 2-subgroup.

**Theorem(3-3): (First Sylow Theorem)**

Let $(G,*)$ be a finite group of order $p^k q$, where p is a prime number is not dividing q, then $G$ has sylow p- subgroup of order $p^k$.

**Example(3-4):**

Find sylow 2- subgroup of the group $(Z_{12}, +_{12})$.

**Solution:** $o(\mathrm{Z}_{12}) = 12 = (4)(3) = (2^2)(3)$, and $2 \nmid 3$

$\Longrightarrow$ by first sylow theorem, the group $(\mathrm{Z}_{12}, +_{12})$ has sylow 2- subgroup of order $2^2$.

$\Longrightarrow$ $(\langle 3 \rangle, +_{12})$ is a sylow 2- subgroup.

**Example(3-5):**

Find sylow 7- subgroup of the group $(\mathrm{Z}_{42}, +_{42})$.

**Solution:** $o(\mathrm{Z}_{42}) = 42 = (7)(6)$, and $7 \nmid 6$

$\Longrightarrow$ by first sylow theorem, the group $(\mathrm{Z}_{42}, +_{42})$ has sylow 7- subgroup of order $7^1$.

$\Longrightarrow$ $(\langle 6 \rangle, +_{42})$ is a sylow 7- subgroup.

**Example(3-6):**

Find sylow 3- subgroup of the group $(\mathrm{Z}_{24}, +_{24})$.

**Solution:** $o(\mathrm{Z}_{24}) = 24 = (3)(8) = (3^1)(8)$, and $3 \nmid 8$

$\Longrightarrow$ by first sylow theorem, the group $(\mathrm{Z}_{24}, +_{24})$ has sylow 3- subgroup of order $3^1$.

$\Longrightarrow (\langle 8 \rangle, +_{24})$ is a sylow 3- Subgroup.

**Theorem(3-7):**

Let p a prime number and G be a finite group such that $p^x \backslash o(G), x \geq 1$, then G has a subgroup of order $p^x$ which is called sylow p- subgroup of G.

**Example(3-8):**

Are the following groups $(S_3, \circ)$ and $(G_s, \circ)$ have sylow p- subgroups.

**Solution:**

$(S_3, \circ)$, $O(S_3) = 6 = (2)(3)$,

$2 \backslash 6 \Longrightarrow \exists$ a subgroup $H$ such that $o(H) = 2$ which is called sylow 2- subgroup.

Also, $3 \backslash 6 \Longrightarrow \exists$ a subgroup $K$ such that $o(K) = 3$ which is called sylow 3- subgroup.

$(G_s, \circ)$, $o(G_s) = 2^3$ is 2- subgroup.

Every subgroup of $G_s$ is 2- subgroup, $o(H) = 2^0$ or $2^1$ or $2^2$ or $2^3$ .

**Theorem(3-9): (Second Sylow Theorem)**

The number of distinct sylow p-subgroups is $k = 1 + tp, t = 0,1, \ldots$ which is divide the order of $G$.

**Example(3-10):**

Find the distinct sylow p-subgroups of $(S_3, \circ)$.

**Solution:**

$o(S_3) = 6 = (2)(3)$,

$2 \setminus 6 \Longrightarrow \exists$ a subgroup $H$ such that $o(H) = 2$.

The number of sylow 2-subgroups is $k_1 = 1 + 2t, t = 0,1, \ldots$ and $k_1 \setminus 6$

if $t = 0 \Longrightarrow k_1 = 1$ and $1 \setminus 6$

if $t = 1 \Longrightarrow k_1 = 3$ and $3 \setminus 6$

if $t = 2 \Longrightarrow k_1 = 5$ and $5 \nmid 6$

if $t = 3 \Longrightarrow k_1 = 7$ and $7 \nmid 6$

so, there are two sylow 2-subgroups.

$3 \setminus 6 \Longrightarrow \exists$ a subgroup $K$ such that $o(K) = 3$.

The number of sylow 3-subgroups is $k_2 = 1 + 3t, t = 0,1, \dots$ and $k_2 \setminus 6$

if $t = 0 \Longrightarrow k_2 = 1$ and $1 \setminus 6$

if $t = 1 \Longrightarrow k_2 = 4$ and $4 \nmid 6$

if $t = 2 \Longrightarrow k_2 = 7$ and $7 \nmid 6$

So, there is one sylow 3-subgroup.

**Example(3-11):**

Find the number of sylow p-subgroups of G such that $\mathrm{o}(\mathrm{G}) = 12$.

**Solution:** $\mathrm{o}(\mathrm{G}) = 12 = (3)(2^2)$

$3 \setminus 12 \Longrightarrow \exists$ a subgroup $H$ such that $o(H) = 3$.

The number of sylow 3-subgroups is $k_1 = 1 + 3t, t = 0,1, \dots$ and $k_1 \setminus 12$

if $t = 0 \Longrightarrow k_1 = 1$ and $1 \setminus 12$

if $t = 1 \Longrightarrow k_1 = 4$ and $4 \setminus 12$

if $t = 2 \Longrightarrow k_1 = 7$ and $7 \nmid 12$

if $t = 3 \Longrightarrow k_1 = 10$ and $10 \nmid 12$

So, there are two sylow 3-subgroups of G.

The number of sylow 2-subgroups is $k_2 = 1 + 2t, t = 0,1, \ldots$ and $k_2 \setminus 12$

if $t = 0 \Longrightarrow k_2 = 1$ and $1 \setminus 12$

if $t = 1 \Longrightarrow k_2 = 3$ and $3 \setminus 12$

if $t = 2 \Longrightarrow k_2 = 5$ and $5 \nmid 12$

if $t = 3 \Longrightarrow k_2 = 7$ and $7 \nmid 12$

So, there are two sylow 2-subgroups of G.

**Remark(3-12):**

The group G has exactly one sylow p-subgroup H if and only if $H\Delta G$.

**Example(3-13):**

$(S_3, \circ), H = \{f_1 = i, f_2 = (123), f_3 = (132)\}$

$H\Delta G \Longrightarrow$ H is a sylow 3-subgroup of $S_3$,

So, there is one sylow 3-subgroup of $S_3$.

**Exercises(3-14);**

- Show that there is no simple group of order 200.
- Show that there is no simple group of order 56.
- Show that there is no simple group of order 20.
- Show that whether $(G_{\ell},\cdot)$ is a sylow.

## 4. Solvable Groups and Their Applications

**Definition(4-1):**

A group $(G,*)$ is called a solvable group if and only if, there is a finite collection of subgroups of $(G,*)$, $H_0, H_1, \dots, H_n$ such that

1. $G = H_0 \supset H_1 \supset \cdots \supset H_{n-1} \supset H_n = \{e\}$,
2. $H_{i+1} \Delta H_i \quad \forall i = 0, \dots, n-1$,
3. $H_i/_{H_{i+1}}$ is a commutative group $\forall i = 0, \dots, n-1$.

**Example(4-2):**

Show that, every commutative group is a solvable group.

**Solution:**

Suppose that $(G,*)$ is a commutative, to show that $(G,*)$ is a solvable.

Let $G = H_0$ and $H_1 = \{e\}$

1. $G = H_0 \supset H_1 = \{e\}$
2. $H_1 \Delta H_0$ satisfies, since $\{e\}\Delta G$, or ( every subgroup of commutative group is a normal)
3. $G/_{\{e\}} \cong G$ is a commutative group, or (the quotient of commutative group is a commutative)

So, $(G,*)$ is a solvable group,

**Example(4-3):**

Show that $(S_3,\circ)$ is a solvable group.

**Solution:** let $H_0 = S_3, H_1 = \{f_1 = i, f_2 = (123), f_3 = (132)\}, H_2 = \{f_1\}$

1. $S_3 = H_0 \supset H_1 \supset H_2 = \{e\}$
2. $H_2 \Delta H_1$ satisfies, since $\{f_1\}\Delta\{f_1, f_2, f_3\}$, $H_1 \Delta H_0$ is true, since $[S_3 : H_1] = 2 \Longrightarrow H_1 \Delta S_3$
3. To prove $H_i/_{H_{i+1}}$ is a commutative group $\forall i = 0,1$

$o\left({}^{H_1}/_{H_2}\right) = \frac{o(\mathrm{H}_1)}{o(\mathrm{H}_2)} = \frac{3}{1} = 3 < 6 \Longrightarrow {}^{H_1}/_{H_2}$ is a commutative group

$o\left({}^{H_0}/_{H_1}\right) = \frac{o(\mathrm{H}_0)}{o(\mathrm{H}_1)} = \frac{6}{3} = 2 < 6 \Longrightarrow {}^{H_0}/_{H_1}$ is a commutative group

Therefore, $(\mathrm{S}_3,\circ)$ is a solvable group.

**Example(4-4): (Homework)**

Show that $(\mathrm{G}_s,\circ)$ is a solvable group.

**Theorem(4-5):**

Every subgroup of a solvable group is a solvable.

**Proof:** let $(H,*)$ be a subgroup of $(G,*)$ and $(G,*)$ is a solvable group.

To prove $(H,*)$ is a solvable.

Since $G$ is a solvable $\Longrightarrow$

there is a finite collection of subgroups of $(G,*)$, $G_0, G_1, \dots, G_n$ such that

1. $G = G_0 \supset G_1 \supset \cdots \supset G_{n-1} \supset G_n = \{e\}$,

2. $G_{i+1} \Delta G_i \quad \forall i = 0, \dots, n-1,$

3. ${G_i}/{G_{i+1}}$ is a commutative group $\forall i = 0, \dots, n-1.$

Let $H_i = H \cap G_i, \quad i = 0, \dots, n$

$H_0 = H \cap G_0, H_1 = H \cap G_1, \dots, H_n = H \cap G_n = \{e\}$

Each $H_i$ is a subgroup of $(G,*)$.

1. $G = H_0 \supset H_1 \supset \cdots \supset H_{n-1} \supset H_n = \{e\}$ is hold
2. $H_{i+1} \Delta H_i \quad \forall i = 0, \dots, n-1, \qquad H_i = H \cap G_i, \; H_{i+1} = H \cap G_{i+1}$ , since $G_{i+1} \Delta G_i \Longrightarrow H_{i+1} \Delta H_i$
3. To prove ${H_i}/{H_{i+1}}$ is a commutative group $\forall i = 0, \dots, n-1.$

Let $f_i : H_i \longrightarrow {G_i}/{G_{i+1}}, i = 0, \dots, n-1$ such that $f_i(x) = x * G_{i+1} \forall x \in H_i \subseteq G_i.$

To prove $f_i$ is a homomorphism,

$f_i(x * y) = f_i(x) \otimes f_i(y)$ ?

$f_i(x * y) = x * y * G_{i+1} = (x * G_{i+1}) \otimes (y * G_{i+1}) = f_i(x) \otimes f_i(y)$

So, $f_i$ is a homomorphism

$f_i$ is onto ?

$$R_{f_i} = \{f_i(x): x \in H_i\} = \{x * G_{i+1}: x \in H_i\} = f_i(H_i)$$
$$\neq {}^{G_i}/_{G_{i+1}}$$

$f_i(H_i) \subseteq {}^{G_i}/_{G_{i+1}} \Longrightarrow f_i$ is not onto

${}^{H_i}/_{\ker f_i} \cong f_i(H_i)$ ( by theorem of homomorphism)

$$\ker f_i = \{x \in H_i: f_i(x) = e'\} = \{x \in H_i: x * G_{i+1} = G_{i+1}\}$$
$$= \{x \in H_i: x \in G_{i+1}\} = \{x \in H_i: x \in H \cap G_{i+1}\}$$
$$= H_{i+1}$$

so, $\left({}^{H_i}/_{H_{i+1}}, \otimes\right) \cong (f_i(H_i), \otimes)$

$f_i(H_i) \subseteq {}^{G_i}/_{G_{i+1}}$ and ${}^{G_i}/_{G_{i+1}}$ is a commutative

Hence, $f_i(H_i)$ is a commutative

Therefore, ${}^{H_i}/_{H_{i+1}}$ is a commutative

So, $(H,*)$ is a solvable ■

**Theorem(4-6):**

Let $H \Delta G$ and $G$ is a solvable, then ${}^{G}/_{H}$ is a solvable.

**Theorem(4-7):**

Let $H \Delta G$ and both $H$, ${}^{G}/_{H}$ are solvable, then $(G,*)$ is a solvable.

**Proof:** since $(H,*)$ is a solvable $\Longrightarrow$

there is a finite collection of subgroups of $(G,*)$, $H_0, H_1, \dots, H_n$ such that

1. $G = H_0 \supset H_1 \supset \cdots \supset H_{n-1} \supset H_n = \{e\}$,
2. $H_{i+1} \Delta H_i \quad \forall i = 0, \dots, n-1$,
3. ${}^{H_i}/_{H_{i+1}}$ is a commutative group $\forall i = 0, \dots, n-1$.

Since $({}^{G}/_{H}, \otimes)$ is a solvable $\Longrightarrow$

there is a finite collection of subgroups of $(G,*)$, $\frac{G_0}{H}, \frac{G_1}{H}, \dots, \frac{G_r}{H}$ such that

1. $\frac{G}{H} = \frac{G_0}{H} \supset \frac{G_1}{H} \supset \cdots \supset \frac{G_r}{H} = \{e\} = H,$

2. $\frac{G_{i+1}}{H} \Delta \frac{G_i}{H} \quad \forall i = 0, \dots, r-1,$

3. $\frac{G_i}{H} \Big/ \frac{G_{i+1}}{H}$ is a commutative group $\forall i = 0, \dots, r-1$.

To prove $(G,*)$ is a solvable group.

$$\frac{G}{H} = \frac{G_0}{H} \Longrightarrow G = G_0$$

$$\frac{G_r}{H} = H \Longrightarrow G_r = \{e\} \text{ or } G_r = H$$

$$H \Delta G_r \Longrightarrow H \subseteq G_r \Longrightarrow G_r = H$$

So, there is a finite collection $G_0, G_1, \dots, G_r = H_0, H_1, \dots, H_n$ such that

1. $G = G_0 \supset G_1 \supset \cdots \supset G_r = H = H_0 \supset H_1 \supset \cdots \supset H_n = \{e\}$.

2. To prove $G_{i+1} \Delta G_i \quad \forall i = 0, \dots, r-1$

Let $x \in G_i$ and $a \in G_{i+1}$ to prove $x * a * x^{-1} \in G_{i+1}$

$$x \in G_i \Longrightarrow x * H \in \frac{G_i}{H}$$

$a \in G_{i+1} \Longrightarrow a * H \in \dfrac{G_{i+1}}{H}$

$\dfrac{G_{i+1}}{H} \Delta \dfrac{G_i}{H} \Longrightarrow (x * H) \otimes (a * H) \otimes (x * H)^{-1} \in \dfrac{G_{i+1}}{H}$

$\Longrightarrow (x * a * x^{-1}) * H \in \dfrac{G_{i+1}}{H} \Longrightarrow x * a * x^{-1} \in G_{i+1}$

$\Longrightarrow G_{i+1} \Delta G_i$

3. To prove $\frac{G_i}{G_{i+1}}$ is a commutative group $\forall i = 0, \dots, r - 1$

$\dfrac{\frac{G_i}{H}}{\frac{G_{i+1}}{H}}$ is a commutative group and $\dfrac{\frac{G_i}{H}}{\frac{G_{i+1}}{H}} \cong \dfrac{G_i}{G_{i+1}}$ $\left(\dfrac{\frac{G}{H}}{\frac{K}{H}} \cong \dfrac{G}{K}\right)$

$\Longrightarrow \dfrac{G_i}{G_{i+1}}$ is a commutative group

Therefore, $(G,*)$ is a solvable group ■

**<u>Exercises(4-8);</u>**

- Show that every $p$-group is a solvable group.
- Show that $(S_4,\circ)$ is a solvable group.
- Show that $(Z_4, +_4)$ is a solvable group.
- Show that $(Z_8, +_8)$ is a solvable group.

- Show that $(Z_5, +_5)$ is a solvable group.
- Show that $(Z_6, +_6)$ is a solvable group.
- Show that $(Z_{12}, +_{12})$ is a solvable group.
- Show that $(Z_{24}, +_{24})$ is a solvable group.

# 5 Some Applications of Group Theory

## 5.1 Cayley Theorem

**Theorem(5-1-1): (Cayley Theorem)**

Every group is an isomorphic to a group of permutations.

This means if $(G,*)$ is any group, then $(G,*) \cong (F_G,\circ)$, where $F_G = \{f_a : a \in G\}, f_a : G \longrightarrow G \ni f_a(x) = a * x, \forall x \in G$.

**Proof:** define $g: G \longrightarrow F_G$ by $g(a) = f_a, \forall a \in G$

To prove $g$ is a homomorphism, one to one and onto.

1. $g$ is a homomorphism, let $a, b \in G$

$g(a * b) = f_{a*b} = f_a \circ f_b = g(a) \circ g(b) \Longrightarrow g$ is a homomorphism.

2. $g$ is a one to one, let$g(a) = g(b),\ \forall a, b \in G$

$\Longrightarrow f_a = f_b \Longrightarrow f_a(x) = f_b(x) \Longrightarrow a * x = b * x \Longrightarrow a = b$

$\Longrightarrow g$ is a one to one.

3. $g$ is a onto, $g(G) = \{g(a): a \in G\} = \{f_a: a \in G\} = F_G$

Therefore, $G \cong F_G$ ■

**Corollary(5-1-2):**

Every finite group $(G,*)$ of order $n$ is an isomorphic to $(S_n,\circ)$.

**Example(5-1-3):**

Consider the following Cayley table of a group $(G = \{e, a, b, c\},*)$

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

Show that$(G,*)$ is an isomorphic to a subgroup of $(S_4,\circ)$.

**Solution:**

$f_e = \begin{pmatrix} e & a & b & c \\ e & a & b & c \end{pmatrix}$, $f_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} = (1)(2)(3)(4) = (1)$

$$f_a = \begin{pmatrix} e & a & b & c \\ a & e & c & b \end{pmatrix}, \quad f_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = (12)(34)$$

$$f_b = \begin{pmatrix} e & a & b & c \\ b & c & e & a \end{pmatrix}, \quad f_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} = (13)(24)$$

$$f_c = \begin{pmatrix} e & a & b & c \\ c & b & a & e \end{pmatrix}, \quad f_4 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} = (14)(23)$$

Hence, $(G,*)$ is an isomorphic to the subgroup of $(S_4,\circ)$:

$\{(1),(12)(34),(13)(24),(14)(23)\}$.

**Example(5-1-4): (Homework)**

Let $(G = \{1,-1,i,-i\},\cdot)$ be a group, apply Cayley Theorem on $G$.

**Example(5-1-5): (Homework)**

Show that $(Z_3,+_3)$ is an isomorphic to a subgroup of $(S_3,\circ)$.

**Exercises(5-1-6):**

- Apply Cayley Theorem on $(Z_4,+_4)$.
- Apply Cayley Theorem on $(G = \{\pm 1, \pm i, \pm j, \pm k\},\cdot)$.
- Apply Cayley Theorem on $(G = \{1,-1\},\cdot)$.

- Apply Cayley Theorem on $(\mathrm{G} = \{\mathrm{A} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, B = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, C = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, D =, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \cdot)$.

## 5.2 Direct Product

**Definition(5-2-1):**

Let $(H,*)$ and $(K,*)$ be two normal subgroups of $(G,*)$, then $(G,*)$ is called an internal direct product of $H$ and $K$ ($G$ is a decomposition by $H$ and $K$ ) if and only if $G = H * K$ and $H \cap K = \{e\}$.

**Example(5-2-2):**

Consider the following Cayley table of a group $(G = \{e, a, b, c\},*)$, $a^2 = b^2 = c^2 = e$

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

*Let* $H = \{e, a\}$ and $K = \{e, b\}$, show that $G = H \otimes K$ is a decomposition by $H$ and $K$.

**Solution:** $H, K \Delta G$ since $G$ is a commutative group

$H * K = \{e, a, b, c\}$ and $H \cap K = \{e\}$

Hence, $G = H \otimes K$ is decomposition by $H$ and $K$.

**Example(5-2-3):**

*Let* $(G,*)$ be any group with $H = G$ and $K = \{e\}$, show that

$G = H \otimes K$ is a decomposition by $H$ and $K$.

**Solution:** $H, K \Delta G$

$H * K = G * \{e\} = G$

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

Therefore, $G = H \otimes K$ is a decomposition by $H$ and $K$.

**Example(5-2-4):**

Let $(Z_4, +_4)$ be a group. Is $Z_4$ has a proper decomposition.

**Solution:** the subgroups of $Z_4$ are $Z_4, \{0,2\}, \{0\}$

Let $H = Z_4$ and $K = \{0,2\}$

$H \otimes_4 K = Z_4 \otimes_4 \{0,2\} = Z_4$

$H \cap K = Z_4 \cap \{0,2\} = \{0,2\}$

So, $Z_4 \neq Z_4 \otimes \{0,2\}$

Let $H = \{0\}$ and $K = \{0,2\}$

$H \otimes_4 K = K \neq Z_4$

Therefore, $Z_4$ has no proper decomposition.

**Theorem(5-2-5):**

Let H and K be two subgroups of G and $G = H \otimes K$, then $G/_{H} \cong K$ and $G/_{K} \cong H$.

**Proof:**

Since $G = H \otimes K \Longrightarrow H * K = G$ and $H \cap K = \{e\}$

$G/_{H} = H * K/_{H}$ and $H * K/_{H} \cong K/_{H \cap K}$ (by second theorem of isomorphic)

$G/_{H} \cong K/_{\{e\}} \Longrightarrow G/_{H} \cong K$ and

$G/_{K} = H * K/_{K}$ and $H * K/_{K} \cong H/_{H \cap K}$

$G/_{K} \cong H/_{\{e\}} \Longrightarrow G/_{K} \cong H$ ■

**Definition(5-2-6):**

Let $(G_1,*)$ and $(G_2,\circ)$ be two groups, define $G_1 \times G_2 = \{(a,b): a \in G_1, b \in G_2\}$ such that $(a,b)\odot(c,d) = (a * c, b \circ d) \ni a,c \in G_1, b,d \in G_2$. Then $(G_1 \times G_2, \odot)$ is a group which is called an external direct product of $G_1$ and $G_2$.

**Example(5-2-7): (Homework)**

Show that $(G_1 \times G_2, \odot)$ is a group.

**Example(5-2-8):**

Let $G_1 = (\mathrm{Z}_3, +_3)$ and $G_2 = (\mathrm{Z}_2, +_2)$. Find $G_1 \times G_2$.

**Solution:**

$$G_1 \times G_2 = \mathrm{Z}_3 \times \mathrm{Z}_2$$
$$= \{(0,0),(0,1),(1,0),(1,1),(2,0),(2,1)\}$$

$(1,1)\odot(2,1) = (0,0)$

$\mathrm{o}(\mathrm{Z}_3 \times \mathrm{Z}_2) = o(\mathrm{Z}_3).o(\mathrm{Z}_2) = 6.$

**Theorem(5-2-9):**

Let $(G_1,*)$ and $(G_2,\circ)$ be two groups, then

1. $(G_1 \times G_2, \odot)$ is an abelian if and only if both $G_1$ and $G_2$ are abelian.
2. $G_1 \times \{e_2\} \vartriangle G_1 \times G_2$.
3. $\{e_1\} \times G_2 \vartriangle G_1 \times G_2$.
4. $G_1 \cong G_1 \times \{e_2\}$.
5. $G_2 \cong \{e_2\} \times G_2$.

**Proof:**

1. $(\Longrightarrow)$ suppose that $G_1 \times G_2$ is an abelian, to prove $G_1$and $G_2$ are abelian.

Let $(a, e_2), (b, e_2) \in G_1 \times G_2 \ni a, b \in G_1, e_2 \in G_2$

Since $G_1 \times G_2$ is an abelian, then

$(a, e_2)\odot(b, e_2) = (b, e_2)\odot(a, e_2)$

$(a * b, e_2) = (b * a, e_2) \Longrightarrow a * b = b * a$

Hence, $(G_1,*)$ is an abelian.

Similarly that $(G_2,*)$ is an abelian.

($\Longleftarrow$) suppose that $(G_1,*)$ and $(G_2,\circ)$ are abelian, to prove $G_1 \times G_2$ is an abelian.

Let $(a,b),(c,d) \in G_1 \times G_2$, to prove $(a,b)\odot(c,d) = (c,d)\odot(a,b)$

$(a,b)\odot(c,d) = (a*c, b*d)$

$(c,d)\odot(a,b) = (c*a, d*b)$

$a*c = c*a$ ($G_1$is an abelian)

$b*d = d*b$ ($G_2$is an abelian)

$\Longrightarrow (a,b)\odot(c,d) = (c,d)\odot(a,b)$

Therefore, $G_1 \times G_2$ is an abelian.

2. To prove $G_1 \times \{e_2\} \triangle G_1 \times G_2$

$G_1 \times \{e_2\} = \{(a,e_2): a \in G_1\} \neq \emptyset$

To prove $(G_1 \times \{e_2\},\odot)$ is a subgroup of $G_1 \times G_2$

Let $(a,e_2),(b,e_2) \in G_1 \times \{e_2\}$

$(a,e_2)\odot(b,e_2)^{-1} = (a,e_2)\odot(b^{-1},{e_2}^{-1}) = (a*b^{-1},e_2)$

So, $(G_1 \times \{e_2\},\odot)$ is a subgroup of $G_1 \times G_2$.

To prove $G_1 \times \{e_2\} \vartriangle G_1 \times G_2$

Let $(x, y) \in G_1 \times G_2$ and $(a, e_2) \in G_1 \times \{e_2\}$

To prove $(x, y) \odot (a, e_2) \odot (x, y)^{-1} \in G_1 \times \{e_2\}$

$(x * a * x^{-1}, y * e_2 * y^{-1}) = (x * a * x^{-1}, e_2) \in G_1 \times \{e_2\}$

Hence, $G_1 \times \{e_2\} \vartriangle G_1 \times G_2$.

3. (**Homework).**
4. To prove $G_1 \cong G_1 \times \{e_2\}$.

**Proof:**

Define $f: (G_1, *) \longrightarrow (G_1 \times \{e_2\}, \odot) \ni f(a) = (a, e_2)$

$f$ is a map ? let $a_1, a_2 \in G_1$ and $a_1 = a_2 \Longrightarrow (a_1, e_2) = (a_2, e_2) \Longrightarrow f(a_1) = f(a_2)$, so $f$ is a map

$f$ is an one to one ? let $f(a_1) = f(a_2) \Longrightarrow (a_1, e_2) = (a_2, e_2) \Longrightarrow a_1 = a_2$, so $f$ is a one to one.

$f$ is a homomorphism ? $f(a * b) = (a * b, e_2) = (a, e_2) \odot (b, e_2) = f(a) \odot f(b)$, so $f$ is a homomorphism

$f$ is an onto ? $R_f = \{f(a): a \in G_1\} = \{(a, e_2): a \in G_1\} = G_1 \times \{e_2\}$ so $f$ is an onto.

Therefore, $(G_1,*) \cong (G_1 \times \{e_2\}, \odot)$■

5. (**Homework**)

**Theorem(5-2-10):**

Let $(G_1,*)$ and $(G_2,\circ)$ be two $p$-groups, then $(G_1 \times G_2, \odot)$ is a $p$-group.

**Proof:**

Since $G_1$ is $p$-group $\Longrightarrow o(G_1) = p^{k_1}, k_1 \in Z^+$

Since $G_2$ is $p$-group $\Longrightarrow o(G_2) = p^{k_2}, k_2 \in Z^+$

$$o(G_1 \times G_2) = o(G_2) \times o(G_1) = p^{k_1} \times p^{k_2}$$
$$= p^{k_1+k_2}, k_1 + k_2 \in Z^+$$

Therefore, $G_1 \times G_2$ is a $p$-group ■

**Exercises(5-2-11):**

- Let $H = \{0,2,4\}$ and $K = \{0,3\}$ are subgroups of $(\mathrm{Z}_6, +_6)$, show that $\mathrm{Z}_6 = H \otimes K$ is a decomposition.

- Let $H = \{0\}$, show that $Z_7 = H \otimes Z_7$ is a decomposition.
- Find $Z_3 \times Z_7$.
- Is $S_3 \times Z_2$ an abelian?
- Is $G_s \times Z_2$ an abelian?
- Is $S_3 \times G_S$ an abelian?
- Is $\{\pm 1, \pm i\} \times Z_2$ an abelian?
- Is $Z_4 \times Z_8$ a $p$-group?
- Is $Z_5 \times Z_{25}$ a $p$-group?
- Is $Z_{11} \times Z_{121}$ a $p$-group?
- Is $Z_7 \times Z_{49}$ a $p$-group?
- Is $Z_{27} \times Z_3$ a $p$-group?
- Is $Z_5 \times Z_{125}$ a $p$-group?
- Is $Z_2 \times Z_{64}$ a $p$-group?
- Is $Z_4 \times Z_{128}$ a $p$-group?
- Is $Z_9 \times Z_{81}$ a $p$-group?
- Is $Z_{27} \times Z_{81}$ a $p$-group?
- Is $Z_{128} \times Z_8$ a $p$-group?
- Is $Z_2 \times Z_{256}$ a $p$-group?