Definition: A binary operation \((\ast)\) on an nonempty set \((G)\) is a function from the set product \(G \times G\) into \(G\). We denoted the image of a pair \((x, y)\) under the binary operation \(\ast\) by \((x \ast y)\) or \(x \ast y \in G\).

The above property is called the closure property, and if this is satisfied, we say that \(G\) is closed under the operation \(\ast\).
A mathematical system is an empty set $G$ and a binary operation defined on $G$ and denoted by $(G, 	imes)$ which satisfy the closure property

\[ \text{서트 الإغلاق} \]

1. $(N_0, +)$ is a mathematical system
2. $(N_0, \cdot)$ is an operation
3. $(N_0, \cdot)$ is not mathematical system

Since $(5, 2) \in N$ and $(2 - 5) = -3 \notin N$
Def: The binary operation \((\ast)\) on an
empty set \(G\) is called

(associative) if

\[(a \ast b) \ast c = a \ast (b \ast c)\]

\(\forall a, b, c \in G\)

Ex: \((\mathbb{Z}, +)\) is associative

since \(\forall a, b, c \in \mathbb{Z}\)

\((x + y) + z = x + (y + z)\)

Def: The mathematical system \((G, \ast)\) is called a semi-group if the binary operation on \(G\) is associative

1. \(G\) is closed under \(\ast\)
2. \(\ast\) is associative
Ex: $(\mathbb{Z}, \cdot)$ is a semi group

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

$(\mathbb{Z}, +)$ is semi group

$(\mathbb{Z}, \div)$ is not semi group

$(2, 3) \in \mathbb{Z}, \left(\frac{2}{3} = \frac{1}{3}\right) \notin \mathbb{Z}$

De: An identity for the binary operation $*$ on an non-empty set $G$ is an element $e$ in $G$ such that

$a * e = e * a = a$

Ex: $(\mathbb{Z}, +)$ the identity is $(Zero 0)$
The inverse المكوس

هو عنصر ينتج للمجموعة حيث إذا تفاعل مع عنصر آخر ينتج المكوس

**Def.** If the binary operation on an non-empty set \((G, \cdot)\) has an identity \(e\), then the inverse for an element \(x \in G\) is \(x^{-1} \in G\) such that \(x \cdot x^{-1} = e\) and \(x^{-1} \cdot x = e\).

\[\exists x^{-1} \in G \quad \forall x \in G\]

\(\mathbb{Z}, +) \Rightarrow \exists x^{-1} \in \mathbb{Z} \quad \forall x \in \mathbb{Z}\)

\((\mathbb{Z}, \times) \Rightarrow \forall x^{-1} \in \mathbb{Z} \quad \forall x \in \mathbb{Z}\)

\((\mathbb{Q}, \times) \Rightarrow \forall x^{-1} \in \mathbb{Q} \quad \forall x \in \mathbb{Q}\)

\((\mathbb{N}, \times) \Rightarrow \forall x^{-1} \in \mathbb{N} \quad \forall x \in \mathbb{N}\)

\((\mathbb{R}, +) \Rightarrow \forall x^{-1} \in \mathbb{R} \quad \forall x \in \mathbb{R}\)

\((\mathbb{R}, \times) \Rightarrow \forall x^{-1} \in \mathbb{R} \quad \forall x \in \mathbb{R}\)

\((\mathbb{C}, +) \Rightarrow \forall x^{-1} \in \mathbb{C} \quad \forall x \in \mathbb{C}\)

\((\mathbb{C}, \times) \Rightarrow \forall x^{-1} \in \mathbb{C} \quad \forall x \in \mathbb{C}\)

\((\mathbb{R}^+, +) \Rightarrow \forall x^{-1} \in \mathbb{R}^+ \quad \forall x \in \mathbb{R}^+\)

\((\mathbb{R}^+, \cdot) \Rightarrow \forall x^{-1} \in \mathbb{R}^+ \quad \forall x \in \mathbb{R}^+\)

\((\mathbb{N}^+, \times) \Rightarrow \forall x^{-1} \in \mathbb{N}^+ \quad \forall x \in \mathbb{N}^+\)

\((\mathbb{Q}^+, \times) \Rightarrow \forall x^{-1} \in \mathbb{Q}^+ \quad \forall x \in \mathbb{Q}^+\)

\((\mathbb{R}^+, \cdot) \Rightarrow \forall x^{-1} \in \mathbb{R}^+ \quad \forall x \in \mathbb{R}^+\)

\((\mathbb{C}^+, \cdot) \Rightarrow \forall x^{-1} \in \mathbb{C}^+ \quad \forall x \in \mathbb{C}^+\)

\((\mathbb{R}^+, \cdot) \Rightarrow \forall x^{-1} \in \mathbb{R}^+ \quad \forall x \in \mathbb{R}^+\)

\((\mathbb{C}^+, \cdot) \Rightarrow \forall x^{-1} \in \mathbb{C}^+ \quad \forall x \in \mathbb{C}^+\)
A non-empty set $G$ with a binary operation $(\star)$ is called a group, denoted by $(G, \star)$, if satisfied:

1. **Closure Property**
   
   $\forall a, b \in G \Rightarrow a \star b \in G$

2. **Associative Law**
   
   $\forall a, b, c \in G$
   
   $(a \star b) \star c = a \star (b \star c)$

3. **Existence of identity**

   $\exists e \in G \text{ s.t. } a \star e = e \star a = a$

4. **Existence of inverses**

   $\forall x \in G$, $\exists x^{-1} \in G \text{ s.t. } x \star x^{-1} = x^{-1} \star x = e$
Ex. \((\mathbb{Z}, +)\)

1. \(\forall a, b \in \mathbb{Z} \Rightarrow a + b \in \mathbb{Z}\)
   \(\therefore \mathbb{Z}\) is closed under (+)

2. \(\forall a, b, c \in \mathbb{Z} \Rightarrow (a + b) + c = a + (b + c)\)
   \(\therefore +\) is associative on \(\mathbb{Z}\)

3. \(\exists 0 \in \mathbb{Z}\) such that \(a + 0 = 0 + a = a\)
   \(\forall a \in \mathbb{Z}\)
   \(\therefore 0\) identity

4. \(\forall x \in \mathbb{Z}, \exists x^{-1} \in \mathbb{Z}\)
   such that \(x + x^{-1} = x^{-1} + x = 0\)
   \(\therefore x^{-1} \forall x \in \mathbb{Z}\) \(\therefore (\mathbb{Z}, +)\) is a group.
Exercise: $(M_2 \times 2, +)$

\[ a + b \]

1. \[ \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} + \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} = \begin{bmatrix} a_1 + a_2 & b_1 + b_2 \\ c_1 + c_2 & d_1 + d_2 \end{bmatrix} \]

2. \[(a + b) \times c = a \times (b + c)\]

\[ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \times \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} + \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} \]

\[ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \times \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} + \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} \]

3. \[ \begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} a^1 & b^1 \\ c^1 & d^1 \end{bmatrix} = \begin{bmatrix} a + a^1 & b + b^1 \\ c + c^1 & d + d^1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \]

4. \[ \begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \]
Commutative group

A group \((G, \cdot)\) is said to be a binary or commutative group if the binary operation \(\cdot\) is commutative.

\[ a \cdot b = b \cdot a, \forall a, b \in G \]

**Ex.** \((\mathbb{Z}, \cdot)\) is a commutative group since \(\forall a, b \in \mathbb{Z}, a \cdot b = b \cdot a\)

**Ex.** \((\mathbb{N}, +)\) is a commutative group since \(\forall a, b \in \mathbb{N}, a + b = b + a\)

**Ex.** \((\mathbb{Z}, +)\), \(a, b \in \mathbb{Z}, a + b = 2a + b\) is not a group since the second condition is not satisfied.
\[(2a + 2b) + c = 2a + (b + c)\]

Theorem: Let \( a, b, c \) be elements of a group \( (G, \cdot) \).

We shall call group \( (G, \cdot) \) a finite if the set \( G \) is finite.

Example: \( (\mathbb{Z}, +) \), \( (R - \{0\}, \cdot) \)

\((\emptyset, +)\) is an infinite group.

But \((\mathbb{C}_3, \cdot)\) is finite group.
Theorem 1.1 (Uniqueness of identity)

The identity element in a group is unique.

Proof: Let \((G, \cdot)\) be a group.

Let \(e, \bar{e}\) be two identity elements.

Then \(e \cdot \bar{e} = \bar{e} \cdot e = e\)

Since \((e)\) is identity.

And \(e \cdot \bar{e} = \bar{e} \cdot e = e\)

Since \(e\) is identity.

\[ e = \bar{e} \]

\[ \therefore \] The identity is unique
Theorem (1.2)
(Uniqueness of Inverse)

Each element of a group has a unique inverse.

Proof: Let \((G, \ast)\) be a group and \(a \in G\) and \(b \in G\) as well as \((C)\) be an inverse of \(a \ast C = C \ast a = e\)

\[ a \ast b = b \ast a = e, \quad a \ast b = b \ast e = b \ast (a \ast c) = (b \ast a) \ast c = e \ast c = C \]

\[ \therefore b = C \]

\[ \therefore the \ inverse \ is \ unique \]
Theorem (1.3) If \( (G, \cdot) \) is a group and \( a \) be any element of \( G \) then \((a^{-1})^{-1} = a\)

Proof Let \( e \) be the identity element in \( G \) then

\[
\tilde{a}^{-1} \cdot a = e
\]

\[
(a^{-1})^{-1} \cdot (\tilde{a}^{-1} \cdot a) = (a^{-1})^{-1} \cdot e
\]

\[
((\tilde{a}^{-1})^{-1} \cdot \tilde{a}^{-1}) \cdot a = (\tilde{a}^{-1})^{-1}
\]

\[
e \cdot a = (\tilde{a}^{-1})^{-1}
\]

\[
\therefore a = (\tilde{a}^{-1})^{-1}
\]
Theorem (1.4)

The Cancelation Laws hold in groups

\[ a \times b = a \times c \]

Proof: \( a \times (a \times b) = a \times (a \times c) \)

\[ (a' \times a) \times b = (a' \times a) \times c \]

\[ e \times b = e \times c \]

\[ b = c \]

and if \( b \times a = c \times a \)

\[ (b \times a) \times a' = (c \times a) \times a' \]

\[ b \times (a \times a') = c \times (a \times a') \]

\[ b \times e = c \times e \]

\[ b = c \]
Theorem 1.5

If \((G, \ast)\) is a group then
\[(a \ast b)^{-1} = b^{-1} \ast a^{-1}\]
for all \(a, b \in G\).

Proof:

\[
(a \ast b) \ast (b^{-1} \ast a^{-1}) = a \ast (b \ast b^{-1}) \ast a^{-1} = a \ast e \ast a^{-1} = a \ast a^{-1} = e
\]

\[
(b^{-1} \ast a^{-1}) \ast (a \ast b) = b^{-1} \ast (a^{-1} \ast a) \ast b = b^{-1} \ast e \ast b = b^{-1} \ast b = e
\]

\[
\therefore (b^{-1} \ast a^{-1}) \text{ is the inverse of } \,(a \ast b)
\]

but \((a \ast b^{-1})\) is also the inverse of \((a \ast b)\)

by (Theorem 1.2)

\[
(a \ast b^{-1})^{-1} = b^{-1} \ast a^{-1}
\]
Theorem (1.6)

If \( a, b \) are any two elements of a group \((G, \ast)\) then the equation

\((a \ast x = b)\) and \((y \ast a = b)\)

have unique solution in \( G \).

Proof \( a \ast x = b \to a^{-1} \ast a \ast x = a^{-1} \ast b \)

\[ e \ast x = a^{-1} \ast b \]

\[ x = a^{-1} \ast b \]

Since \( a^{-1} \in G, b \in G \Rightarrow a^{-1} \ast b \in G \)

Let \( x_1, x_2 \) are two solutions of equation \( a \ast x = b \)

\[ \Rightarrow a \ast x_1 = b \text{ and } a \ast x_2 = b \]

\[ \therefore a \ast x_1 = a \ast x_2 \]

\[ a^{-1} \ast a \ast x_1 = a^{-1} \ast a \ast x_2 \]

\[ e \ast x_1 = e \ast x_2 \Rightarrow x_1 = x_2 \]

\[ \therefore \text{ The equation } a \ast x = b \]

have unique solutions in \( G \).

Similarly in equation \( y \ast a = b \).
Theorem (1.7)

Any non-commutative group has at least six elements.

Proof: If \((G, \cdot)\) is an non-commutative group it must have an identity element \((e)\) and a pair of non-commutative elements \(a\) and \(b\) such that \(a \cdot b \neq b \cdot a\)

\[
\text{\therefore} \quad \text{Now the set } G \text{ is } \{a, b, a \cdot b, b \cdot a\}
\]

\(\therefore\) The element \(a \cdot a\) is different from each element of \(G\).

1. if \(a \cdot a = b\) implies \(a = e\) or \(a = b\) (This is not a correct implication)
2. if \(a \cdot a = b\) implies \(a \cdot b = a \cdot (a \cdot a) = (a \cdot a) \cdot b = b \cdot a\) (This is not a correct implication)
3) If $a \times a = a \times b$ implies $a = b$

4) If $a \times a = b \times a$ implies $a = b$,
   either $a \times a \neq e$ then $a \times a \in G$
   or $a \times a = e$

   In this latter we show
   $(a \times b \times a)$ is (distinct) from $G$

   Now $a \times (a \times b \times a) = (a \times a) \times (b \times a)$
   $\quad = e \times (b \times a) = b \times a$

5) $a \times b \times a = e \Rightarrow b \times a = a \times (a \times b \times a)$
   $\quad = a \times e = a$

6) $a \times b \times a = a \Rightarrow a \times b = e$ Ci

7) $a \times b \times a = b \Rightarrow a \times b = a \times (a \times b \times a)$
   $\quad = (a \times a) \times (b \times a)$
   $\quad = a \times (b \times a)$
   $\quad = e \times b \times a = b \times a$ Ci
order group

Def: Let \((G, \cdot)\) be a finite group. the order of \(G\) is the number of its elements and we denoted by \(|G|\).

Ex: A group \((C_3, \cdot)\) where \(C_3 = \{1, w, w^2\}\)

\(|G| = |C_3| = 3\)

- A group \((\mathbb{R}, \cdot)\) where \(\mathbb{R} = \{1, -1, i, -i\}\)

\(|G| = 4\)
Def: Let \((G, \cdot)\) be a group, the order of an element \(a \in G\) is the least positive integer \(m\) such that \(a^m = e\). We denote by \(o(a) = m\).

Ex: A group \((G, \cdot)\), \(G = \{1, -1, i, -i\}\)

- \(o(1) = 1\) since \(1^1 = 1\)
- \(o(-1) = 3\) since \((-1)^3 = 1\) (\((-1) \cdot (-1) \cdot (-1) = 1\))
- \(o(i) = 4\)
- \(o(-i) = 4\)
Theorem (1.8)

The order of an element of a group is the same as its inverse.

Proof: Let \( a \in G \) such that

\[
\text{order } (a) = m \quad \text{and} \quad \text{order } (a^{-1}) = n
\]

\[
\therefore \text{order } (a) = m \implies a^m = e \implies (a^{-1})^{-1} = e^{-1} = e
\]

\[
\implies (a^{-1})^m = e \implies \text{order } (a^{-1}) = m \quad \text{--- 1}
\]

\[
\therefore \text{order } (a^{-1}) = n \implies (a^{-1})^n = (e)^n = (a^n)^{-1} = e
\]

\[
\implies a^n = e^{-1} = e \implies \text{order } (a) = n \quad \text{--- 2}
\]

From 1 and 2 then

\[
m = n \implies \text{order } (a) = \text{order } (a^{-1})
\]
Theorem (1.9)

If $a$ and $b$ are any two elements of a group $G$, then $O(a) = O(b^{-1} * a * b)$

Proof. Let $O(a) = m$

\[ a^m = e \]

Now \((b^{-1} * a * b)^m = b^{-1} * a * b * b^{-1} * a * b \]

\[ = b^{-1} * a * (b * b^{-1}) * a * (b * b^{-1}) * a \]

\[ = (b * b^{-1}) \]

\[ = (b * b^{-1}) = a * b \]

\[ = b^{-1} * a * e * a * e * a \]

\[ = b^{-1} * a^m * b = b^{-1} * e * b = b^{-1} * b = e \]

\[ \therefore O(b^{-1} * a * b) = m \]

\[ \therefore O(a) = O(b^{-1} * a * b) \]
Theorem (1.10): Division Algorithm

If \( a, b \in \mathbb{Z} \) with \( b \neq 0 \)

then there exist unique \( q, r \in \mathbb{Z} \) such that:

\[
a = q \cdot b + r, \quad 0 \leq r < |b|
\]

\[
\frac{5}{5} = q \cdot 2 + 1
\]
Symmetric and integer modulo n groups

**Def.** A one-one mapping of a finite set \( S \) of \( n \) elements onto itself is called a permutation of degree \( n \).

\[
P = (a_1, a_2, \ldots, a_n)
\]

\[
(P(a_1), P(a_2), \ldots, P(a_n))
\]

**Ex.** Let \( S = \{a, b, c\} \) and the permutation define as \( P(a) = b \), \( P(b) = c \), \( P(c) = a \)

then \( P(a b c a) \)

**Remark** The set of all permutation is called the symmetric set denote by \( (S_n) \) and \( |S_n| = n! \)
Ex) \( S = \{1, 2, 3\} \). Find \( S_3 \):

\[
S_3 = \{ \sigma_1, \sigma_2, \sigma_3 \}, \quad \sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad \sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}
\]

\[
\sigma_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \quad \sigma_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \sigma_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}
\]

\( f = (a \ b \ c \ d), \quad g = (a \ b \ c \ d) \)

\[
g \circ f(a) = f(g(a)) = \sigma(c) = d
\]

\[
g \circ f(a) = g(f(a) = g(b) = d
\]

\[
\sigma^{-1} = \begin{pmatrix} \sigma(a_1) & \sigma(a_2) \\ a_1 & a_2 \end{pmatrix}
\]
Theorem 2.1

Let $S$ be a finite set containing $n$ distinct elements, then the symmetric set of all the permutations of degree $n$ on $S$ forms a finite group of order $n!$ and denoted by $(S_n, *)$.

Proof:

1. Closure Property: If $f, g \in S_n$, then $f \circ g \in S_n$.
2. Associative Law: Since the composite on mapping is associative, so it associative on Permutations.
3. Existence of Identity: The identity permutation $P = (a_1, \ldots, a_n)$.
4. Existence of Inverses: $f = (a_1, \ldots, a_n)$, then $f^{-1} = (b_1, \ldots, b_n)$.

$P \circ f^{-1} = (a_1, \ldots, a_n) \circ (b_1, \ldots, b_n) = (b_1, \ldots, b_n) = f$
Def: A permutation $P$ of sets is a cycle of length $n$ (or $n$-cycle) if there exist $a_1, a_2, \ldots$ such that $P(a_1) = a_2$, $P(a_2) = a_3$, $\ldots$, $P(a_n-1) = a_n$, $P(a_n) = a_1$, and $P(x) = x$ for all $x \in S$. 

Theorem 2.2

The product of disjoint cycles is commutative.

Proof: Let $S$ be a finite set and $f, g$ be any two disjoint cycles on $S$. Then $f$ and $g$ have no common element.
Example: \( f = (1, 2, 3) \) \( g = (3, 4, 6) \)

\( f \circ g = (1, 5, 4, 6) \)

\( g \circ f = (3, 6, 4) (1, 2, 5) \)
نظرية 2: إذا كانت الدوالين

The Product of disjoint is Commutative

\[ f = (1 \ 2 \ 5), \ g = (3 \ 4 \ 6) \]

\[ fog = (1 \ 2 \ 5 \ 3 \ 4 \ 6) \Rightarrow f \circ g = g \circ f \]

\[ g \circ f = (3 \ 4 \ 6 \ 1 \ 2 \ 5) \]

في الناتج نفس الناتج

**Theorem (2.3)**

The symmetric group \((S_n, 0)\) is non-commutative for \(n \geq 3\)

\[ S_2 \Rightarrow \begin{cases} (1, 2) \\ (2, 1) \end{cases} \]

\[ S_3 = \{ I, (1, 2), (1, 3), (2, 3), (1, 2, 3), (1, 3, 2) \} \]

**Proof:** ExC
Theorem (2.4) Every Permutation Can be expressed as a composite of disjoint cycles.

Corollary: Every permutation can be expressed as a composite of transpositions.

Example: \( f = (1 \ 2 \ 3 \ 4 \ 5 \ 6) = (1 \ 3 \ 2 \ 5 \ 6 \ 4) \)

Example: \( f = (2 \ 6 \ 4) = (2 \ 4)(2 \ 6) \)

Definition: A Permutation of a finite set is even (odd) if the number of transpositions is (even) odd.

Example: \( f = (1 \ 2)(3 \ 4 \ 6) = (1 \ 2)(3 \ 6)(3 \ 4) \) is odd.

Example: \( f = (2 \ 5 \ 6 \ 4) = (2 \ 4)(2 \ 6)(2 \ 5) \) is odd.
Theorem 5: A cycle of length \( n \) is an even (odd) permutation according as \( n \) is odd (even).

Proof: Let \( \pi = (a_1, a_2, \ldots, a_n) = (a_1, a_n)(a_1, a_{n-1}) \cdots (a_1, a_2) \)

i.e. \( \pi \) is product of \((n-1)\) transpositions.

If \( n \) is odd then \((n-1)\) is even and \( \pi \) is even.

If \( n \) is even then \((n-1)\) is odd and \( \pi \) is odd.

Remarks:

1. Every transposition is an odd permutation.

\( (1, 2) (1, 3) = (1, 2, 3) \) (odd)

2. The identity is an even permutation.
Exercise: Find $x, y$ if $P = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 2 & x & y & 6 \end{pmatrix}$

when (1) $P$ is even  
(2) $P$ is odd

(1) If $P$ is even, $P = \begin{pmatrix} 1 & 3 & 2 \\ 13 & 2 \end{pmatrix} = (12)(13)(45)$

$\therefore x = 4, y = 5$

(2) If $P$ is odd, $P = \begin{pmatrix} 1 & 3 & 2 \\ 13 & 2 & y \end{pmatrix} = (12)(13)(45)$

$\therefore x = 5, y = 4$
Theorem (6)

1. The product of two even permutations is an even permutation.

2. The product of two odd permutations is an even permutation.

3. The product of an even permutation and an odd permutation is an odd permutation.

Proof
The set of all even permutations of degree \( n \) is called Alternating Set denoted by \((A_n)\) and its order \( \frac{n-1}{2} \)

\[
\text{Ex: } S_3 = \{1, (12), (13), (23), (123), (132)\}
\]

even permutations = \{ (123), (132) \} = A_3

odd permutations = \{ (12), (13), (23) \}

**Theorem 7** \((A_n, o)\) is a group

(*Proof*)

1. \( \forall f, g \in A_n, \ f \circ g \in A_n \)
2. \( \forall h, f, g \in A_n : h, f, g \in S_n \)

\( S_n \) is a group and \( A_n \subseteq S_n \)

3. \( I \in A_n \)

\[
\begin{align*}
\text{If } f = (123) \Rightarrow f^1 = (321) \\
\forall f \in A_n \Rightarrow f^1 \in A_n
\end{align*}
\]

\( \therefore (A_n, o) \) is a group
مناخد الbrihan

الموضوع: 

التاريخ: 15/10/03

دحير

Theorem 2.9

\[ [0] = \{ x \in \mathbb{Z} : x \equiv 0 \pmod{3} \} \]

\[ [1] = \{ x \in \mathbb{Z} : x \equiv 1 \pmod{3} \} \]

\[ [2] = \{ x \in \mathbb{Z} : x \equiv 2 \pmod{3} \} \]

\[ = \{ \ldots, -9, -6, -3, 0, 3, 6, 9, \ldots \} \]

\[ = \{ \ldots, -5, -2, 1, 4, 7 \} \]
\[ [2] = \{ \ldots, -4, -1, 2, 4, 8, \ldots \} \]
\[ [3] = \{ \ldots, -6, -3, 0, 3, 6, 9, \ldots \} \]
\[ Z_3 = \{ [0], [1], [2] \} \]
\[ Z_4 = \{ [0], [1], [2], [3] \} \]
\[ Z_n = \{ [0], [1], \ldots, [n-1] \} \]

**Theorem 2.10** Let \( n \) be a positive integer.

1. For every \([a] \in Z_n\), \([a]\neq \emptyset\).
2. If \([a] \in Z_n\) and \(b \in [a]\) then 
   \[ [b] = [a] \]
3. For any \([a],[b] \in Z_n\)
   \[ [a] \neq [b] \text{ then } [a] \cap [b] = \emptyset \]
   \[ [a] \cup [b] \neq \emptyset \]
4. \[ \bigcup \{ [a] : a \in \mathbb{Z} \} = \mathbb{Z} \]

\( \text{هنالك} (\text{هناك}) \text{ إعداد} \)
Def: A binary operation \((\cdot_n)\) defined on \(\mathbb{Z}_n\) by:
if \([a], [b] \in \mathbb{Z}_n\) then
\([a] \cdot_n [b] = [(a+b) \mod n]\).

Example:
\([2] +_5 [4] = [1]\)
\([0] +_5 [1] = [1]\)
\([3] +_5 [2] = [0] \Rightarrow 3 + 2 = 5 - 5 = 0\)

من رقم 5 ونظام الناتج
النتيجة بين 0, 1, 2, 3, 4
Theorem 11

The math. sys. \( \mathbb{Z}_n \) forms a com. group, known as the group of integers modulo \( n \).

Proof: \( \mathbb{Z}_n \neq \emptyset \)

1. by above defi.  

2. \( \forall [a], [b], [c] \in \mathbb{Z}_n \),  

\[ ([a] + n[b]) + n[c] = a + b + c \]

\[ (a + b) + n[c] = (a + b + c) \]

\[ = [a + (b + c)] = [a] + n(b + c) \]

\[ = [a] + n([b] + n[c]) \]

3. the identity is \([0] = [n]\)

4. the inverse of \([a] = [n - a] \)

\[ a + [n - a] = [a + n - a] = [n] = [0] \]
\((\mathbb{Z}_{10}^*, \times 10)\)

\(\forall [a], [b] \in \mathbb{Z}_n\)

\([a] \cdot [b] = (a \cdot b) = ([a] \cdot [b]) \cdot [a] = (\mathbb{Z}_n, \cdot n) \text{ is comm group} \)

\(\exists (\mathbb{Z}_4, \cdot 4) \text{ is comm group} \)

\(\forall [a], [b] \in \mathbb{Z}_4\) \([a] \cdot 4 [b] = ([a] \cdot [b]) \mod 4 \in \mathbb{Z}_4\)

\(\exists [a], [b] \in \mathbb{Z}_4\)

\([a] \in \text{ نفس برهان النظرية}\)

\([x, y, z] \in (\mathbb{Z}_4, \cdot 4)\)

\(3\) \([0] = [4]\)

\(4\) \(\text{invers } [a] = [4 - a]\)

\(y \cdot x \cdot 5 [n] (y \cdot x \cdot 5 [n]) = \text{بمكن} K^2\)
(Ex) Find invers \([a]^{-1}\) of all element of \(\mathbb{Z}_5\)

\[\mathbb{Z}_5 = \{ [0], [1], [2], [3], [4] \}\]

\[
\begin{array}{c|c}
[a] & [a]^{-1} \\
[0] & [0] \\
\end{array}
\]

\[
[0] + _5 [0] = [0] \\
[1] + _5 [4] = [0]
\]
The Sub group

Def: A non-empty subset \( H \) of a group \( (G, \ast) \) is called a sub group if \( (H, \ast) \) is a group.

Ex: Let \( (\mathbb{Z}, +) \) is a group show that \( (\mathbb{Z}e, +) \) is a sub group.

Solution: \( \mathbb{Z}e \neq \emptyset \)

1. For all \((a, b) \in \mathbb{Z}e\) s.t. \(a + b \in \mathbb{Z}e\)
2. Since \(\text{as} \) is hold in \(\mathbb{Z}\) then its hold in \(\mathbb{Z}e\) also
3. Identity \(0 \in \mathbb{Z}e\) s.t. \(0 + a = a + 0 = a \forall a \in \mathbb{Z}e\)
4. \(\forall a \in \mathbb{Z}e\), \(\exists a' = -a \in \mathbb{Z}e\) s.t. \(a + (-a) = (a + a') = 0\)

\(\therefore (\mathbb{Z}e, +) \) is sub group.
Ex) Let \( G = \{1, -1, i, -i\} \), \((G, \cdot)\) is a group
and \( H = \{1, -1\} \), show that \((H, \cdot)\) is
a subgroup of a group \((G, \cdot)\)

\[ \text{so } H \neq \emptyset \]

1. \( \forall a, b \in H \text{ s.t. } (a \cdot b) \in H \]
   
   2. associative

3. identity \( \Rightarrow 1 \in H \text{ s.t. } 1 \cdot a = a \cdot 1 = a, \forall a \in H \)
   
   \( \therefore 1 \) is the identity of \( H \)

4. \( \forall a \in H \exists a' \in H \text{ s.t. } a \cdot a' = a' \cdot a = 1 \)
   
   \( \therefore (H, \cdot) \) is subgroup
Let \((S^4, 0)\) is a group show that
\((A_4, 0)\) is sub-group

\[
\text{So } A_4 \neq \emptyset \quad \text{(Since \(A_4\))}
\]

1. \(f, g \in A_4 \quad \text{s.t} \quad f \circ g \in A_4\)

 ترك الدالة \(f\) مع الدالة الأخرى ينتمي إلى \(A_4\)

2. \(\text{ass} \) is hold in \(S^4\) then its hold in \(A_4\)

3. \(I \in A_4 \quad \text{s.t} \quad I \circ f = f \circ I = f \quad \forall f \in A_4\)

4. \(\forall f \in A_4 \quad \exists f' \in A_4 \quad \text{s.t} \quad f' \circ f = f \circ f' = I\)

\((A_4, 0)\) is a sub-group
Ex) Let \((\mathbb{Z}_{12}, +_{12})\) is a group 
\[ H = \{ [0], [2], [4], [6], [8], [10] \} \]

Show that \((H, +_{12})\) is a subgroup of a group \((\mathbb{Z}_{12}, +_{12})\)

Sol: \(H \neq \emptyset\)

1. \(\forall [a], [b] \in H \implies [a] +_{12} [b] = [(a+b) \mod 12] \in H\)

2. ass is hold in \(\mathbb{Z}_{12}\) then its hold in \(H\)

3. \([0] \in H \implies [0] +_{12} [a] = [a] +_{12} [0] = [a] \forall a \in H\)

4. inverse

\(\forall [a] \in H \exists [a]^{-1} = [n - a] \in H\)

\(s.t. [a] +_{12} [a]^{-1} = [a^{-1}] +_{12} [a] = [0]\)

\((H, +_{12})\) is a subgroup

of a group \((\mathbb{Z}_{12}, +_{12})\)
Remark: Every group \((G, \cdot)\) has two subgroups namely \(G\) and \([e]\), these subgroups are called (trivial subgroup), other than trivial, is called a proper subgroup.
Remarks

1. Every subgroup of an abelian group is abelian.

2. A non-abelian group may have an abelian subgroup.

Example: A group \((S_3, \circ)\) is non-abelian but a subgroup \((A_3, \circ)\) is abelian.

3. A non-abelian group may have a nonabelian subgroup.

Example: A non-abelian group \((S_4, \circ)\) has a non-abelian subgroup \((A_4, \circ)\).
Theorem 3.1: If \((G, \cdot)\) is a group, then \((H, \circ)\) is a subgroup if \(\forall a, b \in H\), \(a \cdot b^{-1} \in H\).

Proof: Suppose that \((H, \circ)\) is a subgroup.

1. \(a \in H, b \in H \Rightarrow a \circ b \in H\)
2. \(a \in H, b \in H \Rightarrow \exists a^{-1} \in H, b^{-1} \in H\)
3. \(a \in H, b \in H \Rightarrow a \circ (b^{-1})^{-1} \in H \Rightarrow a \circ b \in H\)
4. \(a \circ b^{-1} \in H, \forall a, b \in H\)

Thus, \((H, \circ)\) is a group.

\((H, \circ)\) is a subgroup.

\(a \in H, b \in H \Rightarrow a \circ b \in H\)

\((H, \circ)\) is a group.
Th. 3.2 The intersection of any collection of subgroups of a group \((G, \cdot)\) is a subgroup of \(G\).

Proof: Let \(\{H_i : i \in I\}\) be a collection of subgroups of a group \(G\).

\[ \cap \{H_i : i \in I\} \neq \emptyset \text{ since } e \in H \]

\[ : e \in \cap H_i \]

Let \(a, b \in \cap H_i \). Then \(a \cdot b' \in H_i \) for any \(i \in I\).

\[ \Rightarrow a, b \in H_i, \forall i \in I \]

\[ : a \cdot b' \in H_i, \forall i \in I \]

\[ : a \cdot b' \in \cap H_i, \forall i \in I \text{ (by Th. 3.1)} \]

\[ : (\cap H_i, \cdot) \text{ is subgroup} \]
The union of two subgroups of a group \((G, *)\) is a subgroup if and only if one is contained in the other.

Proof:

Let \((H_1, *)\), \((H_2, *)\) be two subgroups of \(G\).

Let \(H_1 \subseteq H_2\) or \(H_2 \subseteq H_1\).

\(\therefore H_1 \cup H_2\) is subgroup.

Since \(H_1 \subseteq H_2\) \(\Rightarrow\) \(H_1 \cup H_2 = H_2\)

Since \(H_2\) is subgroup \(\Rightarrow\) \(H_1 \cup H_2\) is subgroup.

Since \(H_2 \subseteq H_1\) \(\Rightarrow\) \(H_1 \cup H_2 = H_1\).

Since \(H_1\) is subgroup \(\Rightarrow\) \(H_1 \cup H_2\) is subgroup.
Show that \( H_1 \) and \( H_2 \) be a subgroups of \( G \) and \( H_1 \cup H_2 \) is a subgroup.

Suppose that \( H_1 \cap H_2 \) and \( H_2 \not\subseteq H_1 \)

\[ \forall a \in H_1, \ a \not\in H_2 \text{ and } \exists b \in H_2, \ b \in H_1 \]

\[ a \in H_1 \Rightarrow a \in H_1 \cup H_2 \]

\[ b \in H_2 \Rightarrow b \in H_1 \cup H_2 \]

\[ \therefore H_1 \cup H_2 \text{ is a subgroup} \]

\[ a \cdot b \in H_1 \cup H_2 \]

\[ a \cdot b \in H_1 \quad \text{or} \quad a \cdot b \in H_2 \]

\[ \therefore H \text{ is a subgroup} \]

\[ \Rightarrow a \in H_1 \Rightarrow a^{-1} \in H_1 \Rightarrow a \cdot b \in H_1 \]

\[ \Rightarrow a \cdot a \cdot b \in H_1 \Rightarrow b \in H_1 \quad \text{because} \quad b \in H_1 \]

\[ \therefore a \cdot b \in H_2, \text{and } H_2 \text{ is a subgroup} \]

\[ b \in H_2 \Rightarrow b \in H_2, \ a \cdot b \cdot b^{-1} \in H_2 \Rightarrow a \in H_2 \]

\[ \therefore H_1 \cap H_2 \text{ or } H_2 \subseteq H_1 \]
Def: Let $H$ and $K$ be two subgroups of a group $G$. Then the product of $H$ and $K$ denoted by $H \times K$ is defined by $H \times K = \{ h \times k : h \in H, k \in K \}$.

Remark:

1. $H^1 = \{ h^{-1} : h \in H \} = H$
2. $(H \times K) \times L = H \times (K \times L)$
3. $H \times (K \cup L) = H \times K \cup H \times L$
4. $H \times (K \cap L) \subseteq H \times K \cap H \times L$
5. $(H \times K)^{-1} = K^{-1} \times H^{-1}$
6. $H \times H = H \rightarrow \text{identity}$
Theorem 3.4: If \((H, K)\) are subgroups of \(G\) then \(H \times K\) is subgroup if
\[ H \times K = K \times H \]

**Proof:** Suppose that \(H \times K\) is subgroup.

\[ \therefore \quad H \times K = K \times H \]

\(H \times K\) is subgroup
\[ (H \times K)^{-1} = H \times K \]

\[ \therefore \quad K^{-1} \times H^{-1} = H \times K \]

\[ \therefore \quad K \times H = H \times K \]

\[ \iff \quad \text{Suppose that } H \times K = K \times H \]

\[ \therefore \quad H \times K \text{ is subgroup} \]

To show:
\[ (H \times K)^{-1} (H \times K) = H \times K \]

\[ (H \times K)^{-1} (H \times K) = H \times K \times K^{-1} \times H^{-1} = H \times K \times H^{-1} \]

\[ = K \times H \times H^{-1} = K \times H = H \times K \]

\[ \therefore \quad H \times K \text{ is subgroup} \]
Ex. $\mathbb{Z}_{12} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$

is a group, $H_1 = \{0, 8\}$, $H_2 = \{0, 4, 8\}$

so $H_1 \times H_2 = \{0, 6\} +_{12} \{0, 4, 8\}$

$= \{0, 0, 6, 0, 4, 0, 8, 6, 4, 8\}$

$= \{0, 4, 8, 10\}$

The result is

$\{0, 1, 2, 4, 6, 8, 10\}$

An element $a$ in $H_1 \times H_2$ is:

1. Closed under addition:
   $\forall [a], [b] \in S \cdot s + [a] +_{12} [b] = [(a+b) \mod 12] \in S$

2. Associative:
   $[a] \cdot [b] \cdot [c]$

3. Identity: $[0] \in S$

4. Inverse:
   $\forall [a] \in S \cdot [a]^{-1} = [n-a] \in S$

$s + [a] +_{12} [a] = [a] +_{12} [a] = [0]$
Def: The center of group \((G, \ast)\) denoted by \(C(G)\) is the set \(C(G) = \{ a \in G : a \ast b = b \ast a, \forall b \in G \}\).

Ex: In the groups

\((\mathbb{Z}, +) \Rightarrow C(\mathbb{Z})\)
\((\mathbb{Z}, \ast) \Rightarrow C(\mathbb{Z}_{10}) = \mathbb{Z}_{10}\)
\((S_4, \circ) \Rightarrow C(S_4) = \{I\}\)
\((A_4, \circ) \Rightarrow C(A_4) = \{I\}\)
\((S_3, \circ) \Rightarrow C(S_3) = \{I\}\)
\((A_3, \circ) \Rightarrow C(A_3) = A_3\)
Theorem 3.5: If \((G, \star)\) is a group then 
\((C(G), \star)\) is a subgroup.

Proof: \(e \star a = a \star e\), \(\forall a \in G\)

\[ e \in C(G) \Rightarrow C(G) \neq \emptyset \]

Let \(a, b \in C(G)\)

\[ a \star x = x \star a \text{ and } b \star x = x \star b, \forall x \in G \]

Then if \(y \in G, T \circ P (a \star b^{-1}) \in C(G)\)

\[ (a \star b^{-1}) \star y = a \star (b^{-1} \star y) = a \star (y^{-1} \star b) \]

\[ = a \star (b \star y)^{-1} = a \star (y \star b^{-1}) \]

\[ = (a \star y) \star b^{-1} = (y \star a) \star b^{-1} \]

\[ = y \star (a \star b^{-1}) \]

\[ \therefore (a \star b^{-1}) \in C(G) \text{ by Th. (3.1)} \]

\[ \therefore (C(G), \star) \text{ is subgroup.} \]
Def: A group \((G, \cdot)\) is said to be cyclic group, if \(\exists a \in G\) s.t. \(\forall b \in G \Rightarrow b = a^n\) for some \(n \in \mathbb{Z}\), the element \(a\) is called the generator of \(G\), and we write \(G = \langle a \rangle\).

Ex: A group \((\mathbb{Z}, +)\) is cyclic group generated by \(1\) \((\mathbb{Z}, +)\) is cyclic group generated by \(2\).

Ex: A group \((C_3, \cdot)\) where \(C_3\) is the set of all cube roots of unity.

Sol: \(C_3 = \{1, W, W^2\}\)

\(C_3 = \langle W \rangle\) since

\[W^1 = W, \quad (W^2)^1 = W^2, \quad (W^2)^2 = W, \quad (W^2)^3 = 1\]

\(W = W\) since

\[W^3 = 1\]

\(W^2 = W^2\) since

\[W^4 = W\]
Example 1: \((Z_4, +_4)\) is a group. Find all subgroups.

\[ Z_4 = \{ [0], [1], [2], [3] \} \]

\[ [0] = [0], [1] = [1] \]

\[ [1]^' = [1] \]


\[ Z_4 = \{ [1], [2], [3] \} \]


\[ [3]^4 = [0] \]

\[ ([0], +_4) \]

\[ ([1], +_4), ([2], +_4), ([3], +_4) \]

\[ ([1], +_4) \text{ is cyclic group} \]

all the subgroups is \([([0], +_4)), ([([1], +_4)), ([([2], +_4)), ([([3], +_4))\]
Theorem 3.6: Every cyclic group is commutative.

Proof: Let \( G = \langle a \rangle \) be a cyclic group generated by \( a \).

Let \( x, y \in G \Rightarrow x = a^m, \ y = a^n \)

\[ m, n \in \mathbb{Z} \]

\[ x \ast y = a^m \ast a^n = a^{m+n} = a^{n+m} \]

\[ = a^n \ast a^m = y \ast x \]

\( \therefore (G, \ast) \) is commu. group

Remark: A Comm. group is not always a cyclic group.
(Ex) $\mathbb{R}/\mathbb{Z}$ is comm. group but not cyclic

Remark

1. If an element $a$ is generator of cyclic group $G$, then $a^1$ is also generator of $G$

2. The order of cyclic group is the same of the order of its generator.
Theorem 3.7: Every subgroup of a cyclic group is cyclic.

Proof: Let \((G = \langle a \rangle, \cdot)\) be a cyclic group generated by \(a\).

Let \((H, \cdot)\) be a subgroup of \(G\).

If \(H = \{e\}\) or \(H = G\) then \(H\) is cyclic.

If \(H \neq \{e\}\) and \(H \neq G\), if \(a^m \in H\), \(m \in \mathbb{Z}\) then \(a^m = H\).

Hence \(H\) contains positive integer powers of \(a\).

Let \(n\) be the smallest positive integer such that \(a^n \in H\).

To show \(H = \langle a^n \rangle\).

Tip \(H \subseteq \langle a^n \rangle\).

Let \(a^k \in H\), \(k \in \mathbb{Z}\).
by division algorithm then
\[ q, r \in \mathbb{Z} \text{ s.t. } k = qn + r, 0 \leq r < n \]

\[ a^n, a^k \in H \text{ then } \]

\[ a^k = a^{k-qn} = a^k \cdot (a^n)^{-q} \in H \]

If \( r > 0 \) C1 Since \( r < n \) and \( (n) \) is the

Smallest Positive integer \( s.t. a^n \in H \)

\[ r = 0 \text{ and } k = qn \]

\[ a^k \in (a^n) \implies H \subseteq (a^n) \]

Now \( T.P. (a^n) \subseteq H \)

Let \((a^n)^m \in (a^n)\)

\[ a^n \in H \text{ and } H \text{ is Closed under } \ast \]

\((G, \ast)\) is a group and \((H, \ast)\) is a subgroup of \((G, \ast)\)

\[ (a^n)^m \in H \]

\[ (a^n)^m \in H \]

\[ H = (a^n) \implies (H, \ast) \text{ is cyclic subgroup} \]
Example: \((\mathbb{Z}_8, +_8)\) is cyclic group \(\mathbb{Z}_8 = \{0, 1, 2, \ldots, 7\}\)

\[ H = \{[0], [2], [4], [6]\} \]

\((H, +_8)\) is cyclic subgroup

\([0]^1 = [0]\)

\([0]^2 = [0] +_8 [0] = [0]\)

\([2]^1 = [2]\)


\([2]^3 = [6]\)

\([2]^4 = [8] = 0\)
Ex. Find all subgroups and generators of a group \((\mathbb{Z}_{12}, +_{12})\).

Solution:

\[
\mathbb{Z}_{12} = \{ [0], [1], [2], \ldots, [11] \}
\]

\([0]\) = \{ [0] \}

\([1]\) = \{ [1], [2], [3], [4], [5], [6], [7], [8], [9], [10], [11], [0] \}

\([2]\) = \{ [2], [4], [6], [8], [10], [0] \}

\([3]\) = \{ [3], [6], [9], [0] \}

\([4]\) = \{ [4], [8], [0] \}

\([5]\) = \{ [5], [10], [3], [8], [1], [6], [11] \}

\([6]\), \([9]\), \([2]\), \([7]\), \([0]\) = \(\mathbb{Z}_{12}\)

\([6]\) = \{ [6], [0] \}

\([7]\) = \{ [7], [2], [9], [4], [11], [6], [1] \}

\([8]\), \([3]\), \([10]\), [5], [0] \) = \(\mathbb{Z}_{12}\)
The Subgroup of \( \mathbb{Z}_{12} \) is
\[
\{ [0], +_{12}, ( [2], +_{12}, ( [4], +_{12}, ( [6], +_{12}, ( [8], +_{12} ) \}
\]

The trivial subgroups is
\[
\{ [0] \} \tag{2}
\]
and
\[
( [2], +_{12}, ( [4], +_{12}, ( [6], +_{12} ) \)
\]

The proper subgroups is
\[
( [2], +_{12} ) \quad ( [4], +_{12} ) \quad ( [6], +_{12} )
\]

The generators of \( \mathbb{Z}_{12} \) is \{ [1], [5], [7], [11] \}
\( \mathbb{Z}_{10} \) is a group

\( H = \{ [0], [2], [4], [6], [8] \} \)

\( K = \{ [0], [5] \} \) Find \( K +_{10} H \)

\( K +_{10} H = \{ [0] +_{10} [0], [0] +_{10} [2], [0] +_{10} [4], [0] +_{10} [6], [0] +_{10} [8], [5] +_{10} [0], [5] +_{10} [2], [5] +_{10} [4], [5] +_{10} [6], [5] +_{10} [8] \} \)

= \{ [0], [2], [4], [6], [8], [5], [7], [9], [1], [3] \}
Proposition: If \((G, \cdot)\) is a finite cyclic group of prime order then \(G\) has no proper subgroup.

Definition: Let \((H, \cdot)\) be a subgroup of a group \((G, \cdot)\) and \(a \in G\), the set \(a \cdot H = \{a \cdot h : h \in H\}\) is called a left coset of \(H\) in \(G\).

The element \(a\) is a representative of \(a \cdot H\). In a similar way, we can define the right coset \(H \cdot a = \{h \cdot a : h \in H\}\).
Remarks:

0 Since \( e \in H \Rightarrow a \cdot e \in a \cdot H \)

\[ = a \in a \cdot H \]

\[ \therefore a \cdot H \neq \emptyset \]

2 In general \( a \cdot H = H \cdot a \) if \( G \) is a commutative group.

Example: A group \((G, \cdot)\) where \( G = \{i, -1, 1, i\} \)

and \( H = \{-1, 1\} \)

\[ i \cdot H = \{i(-1), i(1)\} = \{-i, i\} \]

\[ i \cdot H = H \]

\[ -1 \cdot H = \{-i(-1), -1(1)\} = \{-1, -1\} = H \]

\[ -i \cdot H = \{-i(-1), -i(1)\} = \{i, -i\} \]
Ex: A group \((\mathbb{Z}, +)\), let \(H = \{3n : n \in \mathbb{Z}\}\).

\[
\begin{align*}
Z + H & = \{-3, 3, 6, 9, 12, \ldots \} \\
0 + H & = \{-6, -3, 0, 3, 6, \ldots \} \\
1 + H & = \{-5, -2, 1, 4, 7, \ldots \} \\
2 + H & = \{-4, -1, 2, 5, 8, \ldots \}
\end{align*}
\]

\[Z = (0 + H) \cup (1 + H) \cup (2 + H)\]

Ex: The symmetric group \((S_3, \circ)\), where \(H = \{I, (123), (132)\}\) is a sub group of \(G = S_3\).

\[\begin{align*}
(12)0H & = \{(12), (23), (13)\} \\
(13)0H & = (23)0H \\
(123)0H & = \{(123), (132)\}
\end{align*}\]
Let \( K = \{ I, (12) \} \)

\((23)O K = \{(23), (13 2)\}\)

\(K(23) = \{(23), (123)\}\)

\[ (23)O K \neq K(23) \]

**Th. 3.8:** If \((H, *)\) is a subgroup of a group \(G\) then \(a \ast H = H\) iff \(a \in H\)

**Proof:**

\(\Rightarrow\) Let \(a \ast H = H\), Then \(a \in H\)

let \(a \ast e \in a \ast H \Rightarrow a \in H\)

\(\Leftarrow\) Let \(a \in H\), Then \(a \ast H = H\)

let \(x \in a \ast H \Rightarrow x = a \ast h, h \in H\)

\(\Rightarrow x \in H \Rightarrow a \ast H \subseteq H\)

and let \(y \in H \Rightarrow (a \ast d') \ast y = a \ast (a' \ast y) \in a \ast H \Rightarrow y \in a \ast H\)

\(\Rightarrow H \subseteq a \ast H\)
Th. 3.9 if \((H, \ast)\) is a subgroup of a group \(G\) and \(a, b \in G\), then \(a \ast H = b \ast H\) iff \(a \ast b \in H\).

Proof => Let \(a \ast H = b \ast H\), i.e. \(a \ast b \in H\),

Let \(x \in a \ast H \Rightarrow x = a \ast h, h \in H\)

\[ \therefore x \in b \ast H \Rightarrow x = b \ast h_1, h_1 \in H \]

\[ \therefore b \ast h_1 = a \ast h \]

\[ a^{-1} \ast b = h \ast h_1 \in H \]

\[ \therefore a^{-1} \ast b \in H\]

<= Let \(a^{-1} \ast b \in H\), i.e. \(a \ast H = b \ast H\),

\[ \therefore a^{-1} \ast b \in H \]

\[ \therefore a^{-1} \ast b = h, h \in H \]

\[ \therefore b = a \ast h \]

\[ \therefore b \ast H = (a \ast h) \ast H = a \ast (h \ast H) = a \ast H \]

by Th. 3.8
If \((H, \ast)\) is a subgroup of a group \(G\), \(a, b \in G\), then either

\(a \ast H \) and \(b \ast H\) are disjoint or else

\[a \ast H = b \ast H\]

**Proof:** Let \(a \ast H \cap b \ast H \neq \emptyset\)

\[\exists x \in a \ast H \cap b \ast H\]

\[\Rightarrow x \in a \ast H \text{ and } x \in b \ast H\]

\[\therefore x = a \ast h_1 \text{ and } x = b \ast h_2, h_1, h_2 \in H\]

\[\therefore a \ast h_1 = b \ast h_2\]

\[a^{-1} \ast b = h_1 \ast h_2^{-1} \in H\]

\(\Rightarrow a \ast b \in H\) by Th. 3.9

\(\Rightarrow a \ast H = b \ast H\)
Th. 3.11 (Lagrange)

The order and index of any subgroup of a finite group divides the order of the group.

**Proof:** Let $H$ be a subgroup of a finite group $G$, then $H$ is finite.

Let $|H| = m$ and $|G| = n$.

Let $H = \{h_1, h_2, \ldots, h_m\}$ where $h_i$ are distinct. Now let $a \in G$.

Then $a \ast H = \{a \ast h_1, \ldots, a \ast h_m\}$, all elements of $a \ast H$ are distinct.

$|a \ast H| = m$.
Now if $G$ contain $k$ distinct cosets of $H$ in $G$

$\therefore |G| = n$ and $\frac{|G|}{|H|} = k$

$\therefore n = mk$

$\therefore$ the order of $H$ and index of $H$ in $G$ divisor the order of $G$

\[ \text{Ex} \] If $H = \{0, 6, 12, 18\}$ is cyclic subgroup of $(\mathbb{Z}_{24}, +_{24})$ find No of all distinct left coset of $H$ in $\mathbb{Z}_{24}$

\[ \text{So} \] $|\mathbb{Z}_{24}| = 24$, $|H| = 4$

$\therefore \frac{|G|}{|H|} = \frac{24}{4} = 6$
Ex) Let \( H = \{ I, (123), (132) \} \) be a subgroup of \( S_3 \) find index \( H \).

\[
\frac{|S_3|}{|H|} = \text{index} \ H
\]

\[
\therefore \text{index} \ H = \frac{6}{3} = 2
\]

Ex) If \( H = \{ [0], [3], [6], [9] \} \) be a subgroup of a group \( G \) and index \( H = 3 \) find \( |G| \).

\[
\frac{|G|}{|H|} = \text{index} \ H
\]

\[
\therefore |G| = |H| \ \text{index} \ H = 4 \cdot 3 = 12
\]
Corollary (7) The order of every element of finite group is divisor of the order of the group.

Proof Let G be a finite group of order n and a ∈ G, o(a) is finite ∀ a ∈ G

Let o(a) = m

Let H = \{a, a^2, a^3, \ldots, a^m = e\} where all a_i's are distinct

∴ |H| = m

by Lagrange th. ⇒ |H| is a divisor of |G|

∴ \exists k ∈ \mathbb{Z}^+ s.t. \frac{n}{m} = k \Rightarrow \frac{|G|}{o(a)} = k

(\text{i.e.} the order of element a, a divisor of order G)
Corollary 2: For an element $a$ of a finite group $G$ then $a^n = e$.

Proof: Let $G$ be a finite group $|G| = n$ and $a \in G \Rightarrow o(a) = m$, $a^m = e$ by Corollary 1 $o(a)$ divisor of $|G|$.

(i.e.) $m$ is divisor of $n$.

Since $n = mk$, $k \in \mathbb{Z}^+$,

$|G| = n = mk$, $k \in \mathbb{Z}^+$.

$a^n = a^{mk} = (a^m)^k = e^k = e$.

$\therefore a = e$.

(Ex) Let a finite group $(\mathbb{Z}_4, +_4)$.

$\mathbb{Z}_4 = \{[0], [1], [2], [3]\}$.

$[0]^4 = [0] +_4 [0] +_4 [0] +_4 [0] = [0]$.


Chapter Four

Def: A subgroup $(H, \cdot)$ of a group $(G, \cdot)$ is said to be an normal subgroup iff $a \cdot H = H \cdot a \; \forall a \in G$

Ex) In the group $(S_3, 0)$ and
$H = \{ I, (123), (132) \}$

So\ since \ $\forall f \in S_3 \Rightarrow f \circ H = H \circ f$

\therefore $H$ is a normal subgroup

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

$(12) \circ H = \{ (12), (132) \}$

$H \circ (12) = \{ (12), (132) \}$

$(12) \circ H \neq H \circ (12)$

\therefore $H$ is not a normal subgroup
Ex) In the group \((\mathbb{Z}_{12}, +_{12})\) and
\[ H = \{ [0], [3], [6], [9] \}\]
\[
\text{Sol.} \quad \text{Since } \forall [a] \in \mathbb{Z}_{12} \Rightarrow [a] +_{12} H = H +_{12} [a]
\]
\[ \therefore H \text{ is normal subgroup} \]

Remark: Every cyclic group is
com. group if follow that

every subgroup of a cyclic group
Theorem 4.1. A subgroup \( H \) of a group \( (G, \ast) \) is normal iff \( \forall a \in G \) \( a \ast H \ast a' \subseteq H \) 

Proof: \( \rightarrow \) Let \( H \) be normal subgroup of a group \( G \) \( \forall a \in H \) \( T.P: a \ast H \ast a' \subseteq H \) 

\[ a \ast H = H \ast a, \forall a \in G \text{ if } h \in H \Rightarrow a \ast H = h \ast a \text{ for some } h \in H \]

\[ a \ast h \ast a' = h \in H \]

\[ a \ast H \ast a' \subseteq H, \forall a \in G \]

\[ \text{Now let } H \text{ be a subgroup of } G \text{ s.t. } a \ast H \ast a' \subseteq H, \forall a \in G \]

\[ \text{T.P: } H \text{ is normal} \]

\[ \Rightarrow a \ast H = H \ast a, \text{ if } a \in G, h \in H \]
\[
\Rightarrow a \ast h \ast a' \in H \\
a \ast h \in a \ast H \\
\therefore a \ast h = a \ast h \ast a' \ast a \\
=(a \ast h \ast a') \ast a \in H \ast a \\
\therefore a \ast H \subseteq H \ast a \quad \text{①}
\]
Let \( h \ast a \in H \ast a \)
\[h \ast a = a \ast a' \ast h \ast a \\
=a \ast (a' \ast h \ast a) \in a \ast H
\]
\[\therefore H \ast a \subseteq a \ast H \quad \text{②}
\]
From ①, ② we get
\[a \ast H = H \ast a
\]
\[\therefore (H, \ast) \text{ is normal subgroup.}\]
**Remarks**

If \((G, \ast)\) is a group then

1. \(C(G)\) is normal subgroup

2. \(C(G)\) and \(G\) are normal subgroups

**Proof:** by Th.3.7 \((C(G), \ast)\) is subgroup

Let \(x \in G\) and \(a \in C(G)\)

\[
x \ast a \ast x^{-1} = (x \ast a) \ast x^{-1}
= (a \ast x) \ast x^{-1}
= a \ast (x \ast x^{-1}) = a \ast e
= a \in C(G)
\]

\[
\therefore x \ast a \ast x^{-1} \in C(G)
\]

\[
\therefore x \ast C(G) \ast x^{-1} \subset C(G)\text{ by Th. 4.1}
\]

\[
\therefore C(G)\text{ is normal subgroup}
\]
<table>
<thead>
<tr>
<th>التاريخ:</th>
<th>المًوضّع:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

(Blank)
Def: An element \( a \) of group \( (G, \cdot) \) is said to be conjugate element to \( b \in G \) if \( \exists x \in G \) s.t. \( a = x^{-1} \cdot b \cdot x \).

Ex) In a symmetric group \( (S_3, \circ) \), let \( a = (132) \), \( b = (123) \) and \( x = (12) \), \( x^{-1} = (13) \) s.t.

\[
\begin{align*}
a &= x^{-1} \circ b \circ x \\
(132) &= (12) \circ (123) \circ (12)
\end{align*}
\]

\[
= (12) \circ (13) = (132)
\]

\( \therefore \) \( a \) Conjugate to \( b \)

\( a = (12) \), \( b = (23) \), \( x = (13) \), \( x^{-1} = (13) \)

\[
(12) = (13) \circ (23) \circ (13)
\]

\[
= (13) \circ (123) = (12)
\]

\( \therefore \) \( a \) Conjugate to \( b \)
Def: Let \((G, \ast)\) be a group and \(a \in G\) then the conjugate class of \(a\) is denoted by \(C(a)\) and defined by:

\[
C(a) = \{ b \in G : b = x \ast a \ast x^{-1} \} = \{ x \ast a \ast x^{-1}, \forall x \in G \}.
\]

Ex: Find all conjugate classes of each element in \((G, \ast)\) where \(G = \{1, -1, i, -i\}\).

Sol: \(C(-i) = \{ x \ast (-i) \ast x^{-1}, \forall x \in G \} = \{ x \ast (-i) \ast (i) \ast (i)^{-1}, -1 \ast (-i) \ast (-i) \ast i^{-1}, i \ast (-i) \ast i^{-1}, -i \ast (-i) \ast (-i)^{-1} \} = \{-i, -i, -i, -i\} = \{-i\} \)

\(C(i) = \{ i^3 \}\)
Ex. In a group \((\mathbb{Z}_3, +_3)\) find \(C([2])\)

\[
\]

H.W. Find all \(C([\alpha])\), \(\forall [\alpha] \in \mathbb{Z}_4\)

\(c([0]) +_4\)
Def: Let $H$ and $K$ be two subgroups of a group $(G, \cdot)$, then $K$ is said to be conjugate subgroup to $H$ if $\exists x \in G$ st $H = xKx^{-1}$

(Ex) In a group $(S_3, \circ)$, let $H = \{I, (12)\}$ and $K = \{I, (13)\}$ are two subgroups of $S_3$. Is $H$ conjugate to $K$?

(Sol) $H = xKx^{-1}$

$\text{id} = (23)$, $H = (23)0\{I, (13)\}0(23)$

$= (23)0\{(23), (132)\}$

$\text{id} x = (12) = \{I, (13)\} = K$
\[
H = (12) \circ \{ I, (13) \} \circ (12) \\
= (12) \circ \{ (12), (123) \} \\
= \{ I, (23) \}
\]

If \( x = (13) \), then \( H = (13) \circ \{ I, (13) \} \circ (13) \)
\[
= (13) \circ \{ (13), I \} \\
= \{ I, (13) \} = K
\]

If \( x = (123) \), then \( H = (123) \circ \{ I, (13) \} \circ (132) \)
\[
= (123) \circ \{ (132) \circ (23) \} \\
= \{ I, (12) \} = H
\]

\[
\vdash \exists (123) \in S_3 \quad S.t. \quad H = (123) \circ K \circ (132)
\]

\[
\therefore H \text{ Conjugate to } K.
\]

\[
\begin{pmatrix}
1 & 2 & 3 \\
3 & 2 & 0
\end{pmatrix}
\begin{pmatrix}
1 & 2 & 3 \\
3 & 1 & 2
\end{pmatrix}
\end{pmatrix}
\frac{}{}
\begin{pmatrix}
1 & 2 & 3 \\
1 & 3 & 2
\end{pmatrix}
= \begin{pmatrix} 2 & 3 \end{pmatrix}
\]
Example: In a group \((\mathbb{Z}_8, +_8)\), let
\[ H = \langle [2] \rangle = \{ [0], [2], [4], [6] \} \]
\[ K = \langle [4] \rangle = \{ [0], [4] \} \] is \( H \) Conjugate to \( K \).

Solution: If \( x = [0] \), \( H = x +_8 \{ [0], [4] \} +_8 x^{-1} \)
\[ = [0] +_8 \{ [0], [4] \} +_8 [0] \]
\[ = [0] +_8 [0] +_8 \{ [0], [4] \} = \{ [0], [4] \} \]

\[ = \{ [0], [4] \} = K \]

\[ \therefore [a] \in \mathbb{Z}_8 \text{ s.t. } H = [a] +_8 K +_8 [a]^{-1} \]
\[ \Rightarrow H \text{ Conjugate to } K. \]
Propositions

1. A subgroup \( H \) of group \((G, \ast)\) is said to be self conjugate iff \( C(H) = H \).

2. A subgroup \((H, \ast)\) of a group \((G, \ast)\) is self conjugate iff \( H \) is a normal subgroup of \( G \).

\[ H \text{ is conjugate with itself} \]
\[ H = x \ast H \ast x^{-1} \]

\[ \iff H \ast x = x \ast H \]

\[ \therefore H \text{ is normal sub.} \]
Def: A group \((G, \cdot)\) s.t. \(G \neq \{e\}\) is said to be a simple group if it has no proper normal subgroup.

Ex: A group \((\mathbb{Z}_7, +)\) is simple group since \(\mathbb{Z}_7\) has no proper normal subgroup

Ex: \((\mathbb{Z}_{10}, +)\) is not a simple group.

Since \([\mathbb{Z}_2, +]\) is a proper normal subgroup

Remark: Every group of prime order is simple.

Ex: A group \((S_3, 0)\) is not simple group since \(A_3 = \{1, (123), (132)\}\) is proper normal subgroup of \(S_3\).
Definition: Let \((H, \cdot)\) be a normal subgroup of a group \((G, \circ)\). We define \(G/H\) by \(G/H = \{aH : a \in G\}\) and \(\circ\) on \(G/H\) by 
\[ aH \circ bH = a \cdot b \cdot H, \forall aH \text{ and } bH \subseteq G/H \]

Theorem 4.2: If \((H, \cdot)\) is a normal subgroup of a group \((G, \circ)\), then \((G/H, \circ)\) is a group called the quotient group or factor group.

Proof: 
\[ G/H = \{aH : a \in G\} \]
\[ \therefore e \in G \Rightarrow eH \in G \Rightarrow G/H \neq \emptyset \]

Now let \(aH = C \cdot H\) and \(bH = d \cdot H\).

Then \(a \cdot b \cdot H = C \cdot d \cdot H\).

\[ \therefore a \cdot H = C \cdot H \Rightarrow a \cdot C^{-1} \in H \]

\[ b \cdot H = d \cdot H \Rightarrow b \cdot d^{-1} \in H \]

Now \((a \cdot b) \circ (C \cdot d)^{-1} = a \cdot b \cdot d^{-1} \cdot C^{-1}\)

\[ \therefore a \cdot C^{-1} \in H, \quad b \cdot d^{-1} \in H \quad \text{and} \quad H \text{ normal} \]

\[ \therefore a \cdot (b \cdot d^{-1}) \cdot a^{-1} \in H \]
\[ a \times (b \times d^{-1}) \times a^{-1} \times (a \times c^{-1}) \in H \]
\[ \Rightarrow (a \times b) \times (c \times d) \in H \]
\[ \Rightarrow a \times b \times H = c \times d \times H \]
\[ \Rightarrow \bigcirc \text{ is well-defined} \]

1. Let \( a \times H \) and \( b \times H \in G/H \)
\[ a \times H \bigcirc b \times H = a \times b \times H \in G/H \]
\[ \Rightarrow a \times H \bigcirc b \times H \in G/H \]

2. Let \( a \times H, b \times H, c \times H \in G/H \)
\[ (a \times H) \bigcirc (b \times H) \bigcirc (c \times H) \]
\[ = (a \times b \times H) \bigcirc (c \times H) \]
\[ = (a \times (b \times c)) \times H = (a \times (b \times c)) \times H \]
\[ = (a \times H) \bigcirc ((b \times c) \times H) \]
\[ = (a \times H) \bigcirc (b \times H) \bigcirc (c \times H) \]
The coset $H = e \times H \in G/H$ is the identity element $\forall (e \times H) \times (a \times H) = e \times a \times H = a \times H$

and $(a \times H) \times (e \times H) = a \times e \times H = a \times H$

If $a \times H \in G/H \implies \exists a' \times H \in G/H$ s.t.

$(a \times H) \times (a' \times H) = a \times a' \times H = e \times H = H$

and $(a' \times H) \times (a \times H) = a' \times a \times H = e \times H = H$

$(G/H ; \times)$ is a group

Example: A group $(S_3, 0)$ and anormal subgroup $P(A_3, 0)$ then $(S_3/A_3, 0)$ is the quotient group

where $S_3/A_3 = \{A_3, (13) \circ A_3\}$

Note: Every quotient group is

Com. group
Def: Let \((G, \ast)\) be a group and \(a, b \in G\) the commutator of \(a\) and \(b\) denoted by \([a, b]\) is defined by

\[
[a, b] = a \ast b \ast a^{-1} \ast b^{-1}
\]

Ex) In the group \((\mathbb{Z}_6, +_6)\), find \([2], [5]\)

\[
\]

\[
\]

\[
= [0]
\]

Ex) In the group \((S_3, \circ)\) Find \([12], (13)\]

\[
[12], (13) = (12) \circ (13) \circ (12)^{-1}
\]

\[
= (12) \circ (13) \circ (12) \circ (13)
\]

\[
= (12) \circ (13) \circ (132)
\]

\[
= (12) \circ (2, 3) = (123)
\]
Remarks:

1. If \((G, \times)\) is a comm. group then \([a, b] = e\)

2. The inverse of the commutator is again a commutator, s.t. \([a, b]^{-1} = [b, a]\)

**Def** Let \((G, \times)\) be a group, then the derived subgroup or commutator subgroup of \((G, \times)\) denoted by \([[G, G], \times]\) where

\[ [[G, G]] = \{ \prod [a_i, b_i] : a_i, b_i \in G \} \]

where \(\prod\) denoted to a product of finitely many commutators of \(G\)

\[ f \circ g(x) = f(g(x)) \]
Theorem 4.3: The group $([G, G], \ast)$ is a normal subgroup of a group $(G, \ast)$

Proof: $e \in G \Rightarrow [e, e] \in [G, G]$

$\therefore [G, G] \neq \emptyset$

Let $x, y \in [G, G]$

$\Rightarrow x = [a_1, b_1] \ast [a_2, b_2] \ast \cdots \ast [a_n, b_n]$

and $y = [c_1, d_1] \ast [c_2, d_2] \ast \cdots \ast [c_n, d_n]$

$x \ast y' = [a_1, b_1] \ast \cdots \ast [a_n, b_n] \ast [c_1, d_1] \ast \cdots \ast [c_n, d_n]$

$= [a_1, b_1] \ast \cdots \ast [a_n, b_n] \ast [d_1, c_1] \ast \cdots \ast [d_n, c_n]$

$\therefore x \ast y' \in [G, G]$

$\therefore ([G, G], \ast)$ is subgroup

$\therefore (P([G, G], \ast)$ is normal)
Let \( x \in [G, G] \)

T.P \( x \in [G, G] \times x' \in [G, G] \)

Let \( a \in x \times [G, G] \times x' \)

\[ a = x \times c \times x' \quad c \in [G, G] \]

\[ = x \times c \times x' \times e \]

\[ = x \times c \times x' \times c \times c \]

\[ = [x, c] \times c \quad c \in [G, G] \]

\[ a \in [G, G] \]

\( ([G, G], x) \) is normal subgroup?
Theorem 4.4: Let \((H, \ast)\) be a normal subgroup of a group \((G, \ast)\) then 
\((G/H, \otimes)\) is commutative iff 
\([G, G] \subseteq H\)

Proof: Let \((a \ast H), (b \ast H) \in G/H\)

which is commutative

\[(a \ast H) \otimes (b \ast H) = (b \ast H) \otimes (a \ast H)\]

\[\iff (a \ast b) \ast H = (b \ast a) \ast H\]

\[\iff (a \ast b) \ast H = (b \ast a) \ast H \subseteq H\]

\[\iff [a \ast b] \subseteq H\]

\[\iff [G, G] \subseteq H\]
Chapter Five

Group Homomorphisms

Definition: Let \((G, \times)\) and \((G', \times')\) be two groups, then a mapping \(\phi: (G, \times) \rightarrow (G', \times')\) is called a homomorphism if
\[\phi(a \times b) = \phi(a) \times' \phi(b), \quad \forall a, b \in G\]

Example: Let \(\phi: (\mathbb{Z}, +) \rightarrow (\mathbb{Z}, +)\) such that \(\phi(n) = 2n\) for all \(n \in \mathbb{Z}\) is \(\phi\) hom. or not

Solution: Let \(n, m \in \mathbb{Z}\).
\[\phi(n + m) = 2(n + m) = 2n + 2m = \phi(n) + \phi(m)\]

\[\therefore \phi\text{ is hom.}\]
Ex) Let \( f : (\mathbb{R}, +) \rightarrow (\mathbb{R}, \cdot) \) S.t
\[ f(a) = e, \quad \forall a \in \mathbb{R} \]
is a hom.

Sol) Let \( a, b \in \mathbb{R} \)
\[ f(a+b) = e^{a+b} = e^a \cdot e^b = f(a) \cdot f(b) \]
\[ \therefore \ f \ \text{is homo.} \]

Ex) Let \( f : (\mathbb{Z}, +) \rightarrow (\mathbb{Z}, \cdot) \) S.t
\[ f(a) = 2a + 5, \quad \forall a \in \mathbb{Z}, \]
is a hom.

Sol) Let \( a, b \in \mathbb{Z} \)
\[ f(a+b) = 2(a+b) + 5 \]
\[ = 2a + 2b + 5 \]
\[ f(a) + f(b) = 2a + 5 + 2b + 5 \]
\[ \therefore \ f(a+b) \neq f(a) + f(b) \]
\[ \therefore \ f \ \text{is not hom.} \]
Example: Let $f: (\mathbb{Z}, +) \rightarrow (\mathbb{Z}/n\mathbb{Z})$

$$f(a) = [a], \forall a \in \mathbb{Z}, \text{is } f \text{ hom.}$$

Solution:

Let $a, b \in \mathbb{Z}$

$$f(a+b) = [a+b] = [a] + n[b] = f(a) + nf(b) \therefore f \text{ is hom.}$$
Exercise: Let \( \phi : (\mathbb{Z}, +) \rightarrow (\mathbb{R} - \{0\}, \cdot) \) defined by
\[
\phi(n) = \begin{cases} 
1 & \text{if } n \in \mathbb{Z}^* \\
-1 & \text{if } n \in \mathbb{Z}^\text{odd}
\end{cases}
\]

Show that \( \phi \) is hom.

Solution:

Let \( n, m \in \mathbb{Z} \) then

1. \( n \) and \( m \) are even.
   \[
   \phi(n + m) = 1 \cdot 1 = 1 = \phi(n) \cdot \phi(m)
   \]
   \( \therefore \) \( \phi \) is hom.

2. \( n \) and \( m \) are odd.
   \[
   \phi(n + m) = 1 + \frac{3}{2}
   \]
   \( \approx \)
   \[
   = (-1) \cdot (-1) = 1 \therefore \phi \text{ is hom.}
   \]
   \[
   = \phi(n) \cdot \phi(m)
   \]

3. One of them is even and the other is odd.
   \[
   (-1) \phi(n + m) = -1 = 1 \cdot (-1) = \phi(n) \cdot \phi(m) \text{ if } \begin{cases} n \text{ even} \\
   m \text{ odd}
\end{cases}
   \]
   \[
   = (-1) \cdot 1 = \phi(n) \cdot \phi(m) \therefore \phi \text{ is hom.}
   \]
   \[
   \text{if } n \text{ odd or } (m) \text{ even}
   \]
Ex) Let \( P : (\mathbb{R}^+, \cdot) \rightarrow (\mathbb{R}^+, +) \), \( P(a) = \ln a \)

is \( P \) hom.

Sol) Let \( a, b \in \mathbb{R}^+ \)

\[
P(a \cdot b) = \ln (a \cdot b) = \ln a + \ln b = P(a) + P(b)
\]

\( \therefore P \) is homo.

Ex) Let \( P : (G, \ast) \rightarrow (G, \ast) \),

\[
P(a) = a \ast a \ast a^{-1} \quad \forall a \in G
\]
is \( P \) hom.

Sol) Let \( a, b \in G \)

\[
P(a \ast b) = a \ast a \ast b \ast x^{-1}
\]

\[
= a \ast a \ast e \ast b \ast x^{-1}
\]

\[
= a \ast x^{-1} \ast x \ast b \ast x^{-1}
\]

\[
= P(a) \ast P(b) \quad \therefore P \) is hom.
Theorem 5.1

If \( f: (G, \cdot) \to (\hat{G}, \hat{\cdot}) \) is homthen
\[ f(e) = \hat{e}, \] where \( e \) and \( \hat{e} \) are identity
of \( G \) and \( \hat{G} \) respectively.

i) \( f(a^1) = f(a)^{-1} \)

Proof

i) \( a \cdot e = a \Rightarrow f(a \cdot e) = f(a) \)
\[ \Rightarrow f(a) \hat{\cdot} f(e) = f(a) \]
\[ f(a)^{-1} \hat{\cdot} f(a) \hat{\cdot} f(e) = f(a)^{-1} \hat{\cdot} f(a) \]
\[ = f(a)^{-1} \hat{\cdot} f(a) \]
\[ \hat{e} \hat{\cdot} f(e) = \hat{e} \]
\[ \Rightarrow f(e) = \hat{e} \]
\[ (i) \quad a \times a' = e \Rightarrow f(a \times a') = f(e) \]
\[ 
\Rightarrow f(a) \times f(a') = e \\
\Rightarrow f(a') \times f(a) = e \\
\Rightarrow f(a') \times f(a) \times f(a') = f(a) \times e \\
\Rightarrow e \times f(a') = f(a) \Rightarrow f(a') = f(a)^{-1} 
\]

**Theorem 5.2** if \( f : (G, \times) \rightarrow (G', \times) \) is hom. then

1. if \((H, \times)\) is a subgroup of \(G\) then \((f(H), \times)\) is asubgroup of \(G\)

**Proof**

2. \( P(H) = \{ f(h) : h \in H \} \)

Let \( f(h_1) \times f(h_2) = f(h_1 \times h_2) \)
\[ h_1, h_2 \in H \implies h_1 \cdot h_2^1 \in H \]

\[ f(h_1 \cdot h_2^1) \in f(H) \]

\[ f(h_1) \cdot f(h_2) \in f(H) \]

\[ (f(H), \cdot) \text{ is a sub group of } G \]

\[ f(H) = \{ h : f(h) \in H \} \]

Let \( h_1, h_2 \in f(H) \),

\[ f(h_1 \cdot h_2) = f(h_1) \cdot f(h_2) \]

\[ = f(h_1) \cdot f(h_2)^1 \]

\[ \implies f(h_1), f(h_2) \in H \]

\[ f(h_1) \cdot f(h_2)^1 \in H \]

\[ f(h_1 \cdot h_2) \in H \]

\[ \implies h_1 \cdot h_2^1 \in f(H) \]

\[ (f(H), \cdot) \text{ is a sub group of } G \]
Def:

1) A one-one hom. is called a monomorphism.
2) An onto hom. is called an epimorphism.
3) A one-one and onto hom. is called (isomorphism)
4) A hom. of a group into itself is called endomorphism
5) An isomorphism of a group onto itself is called automorphism.
(Ex) If \( f : (\mathbb{Z}, +) \rightarrow (\mathbb{Z}_e, +) \) defined by \( f(n) = 2n \) for all \( n \in \mathbb{Z} \) is

1. hom.
2. epimorphism
3. isomorphism
4. automorphism

So let \( n, m \in \mathbb{Z} \)

- \( f(n+m) = 2(n+m) = 2n + 2m \)
- \( = f(n) + f(m) \) \( \therefore f \) is hom.

- By 1 \( f \) is hom.
- \( \therefore f(z) = \{2n : n \in \mathbb{Z}\} = \mathbb{Z}_e \)

\( \therefore \) \( f \) is onto \( \Rightarrow f \) is epimorphism
3. by ①② \( f \) is hom. and onto

Let \( n, m \in \mathbb{Z} \) s.t. \( f(n) = f(m) \)

\[ \Rightarrow 2n = 2m \Rightarrow \therefore n = m \]

\[ \therefore f \text{ is 1-1} \Rightarrow f \text{ is isomorphism} \]

4. by ③ \( f \) is isomorphism but \( \mathbb{Z} \neq \mathbb{Z}_e \)

\[ \therefore f \text{ is not onto morphism} \]
\textbf{Ex:} Let \( f : (G, \ast) \rightarrow (G/H, \circlearrowright) \) s.t
\[ f(a) = a \ast H \]
Show that \( f \) is epimorphism.

\textbf{Sol:} Let \( a, b \in G \)
\[ f(a \ast b) = a \ast b \ast H = a \ast H \circlearrowright b \ast H \]
\[ = f(a) \circlearrowright f(b) \]
\[ \therefore f \text{ is hom.} \]

To show \( f \) is onto.

\[ \forall a \ast H \in G/H \text{, } a \in G \]
\[ \text{s.t } f(a) = a \ast H \]
\[ \therefore G/H \text{ is the set of all images.} \]
\[ \therefore f \text{ is onto} \Rightarrow f \text{ is epimorphism.} \]
**Def:** Let $f : (G, *) \rightarrow (G', \cdot)$ be hom., and let $e'$ be the identity of $G'$.

The kernel of $f$ denoted by $\ker(f)$ is the set

$$\ker(f) = \{ a \in G : f(a) = e' \}$$

**Ex:** Let $f : (\mathbb{Z}, +) \rightarrow (\mathbb{Z}, +)$ s.t.

$$f(n) = 2n, \quad \forall n \in \mathbb{Z}$$

Find $\ker(f)$

**Sol:** $\ker(f) = \{ n \in \mathbb{Z} : f(n) = e' \}$

$$= \{ n \in \mathbb{Z} : 2n = 0 \}$$

$$= \{ n \in \mathbb{Z} : n = 0 \} = \{ 0 \}$$
Ex. Let $\Phi : (\mathbb{R}, +) \to (\mathbb{R}^+, \cdot)$ s.t. $\Phi(a) = e^a$

Let $a \in \mathbb{R}$ find $\ker(\Phi)$.

Sol. $\ker(\Phi) = \{n \in \mathbb{R} : \Phi(a) = 1\}$

$= \{a \in \mathbb{R} : e^a = 1\} = \{0\}$

Ex. Let $\Phi : (\mathbb{Z}, +) \to (\mathbb{Z}_n, +_n)$ s.t. $\Phi(a) = [a]$ find $\ker(\Phi)$.

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

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

$= \{a \in \mathbb{Z} : a \equiv 0 \text{ mod } n\}$

$= \{a \in \mathbb{Z} : a = kn, k \in \mathbb{Z}\}$

$= \{0, \pm n, \pm 2n, \pm 3n, \ldots\}$
Theorem 5.3: If \( \Phi: (G, \ast) \rightarrow (G', \ast') \) is hom., then \( (\ker(\Phi), \ast) \) is normal subgroup.

Proof: \( \ker(\Phi) \neq \emptyset \) since \( \Phi(e) = e \).

Now let \( a, b \in \ker(\Phi) \Rightarrow \Phi(a) = \Phi(b) = e \).

\[
\Phi(a \ast b) = \Phi(a) \ast' \Phi(b) = \Phi(a) \ast' \Phi(b) = e \ast (e')^{-1} = e \ast e = e
\]

\[
\therefore a \ast b^{-1} \in \ker(\Phi) \Rightarrow (\ker(\Phi), \ast) \text{ is subgroup.}
\]

Now, to prove \( \ker(\Phi) \) is normal we must prove that \( a \ast \ker(\Phi) \ast a' \subseteq \ker(\Phi), \forall a \in G \).

Let \( x \in a \ast \ker(\Phi) \ast a' \Rightarrow x = a \ast K \ast a' \)

\[
K \in \ker(\Phi)
\]

\[
\Phi(x) = \Phi(a \ast K \ast a') = \Phi(a) \ast \Phi(K) \ast \Phi(a') = e \ast e = e
\]

\[
\therefore \ker(\Phi) \ast \ker(\Phi) \text{ is normal subgroup.}
\]
Theorem 5.4: If \( f : (G, \ast) \rightarrow (G', \ast') \) is hom. then \( f \) is one-one if \( \text{Ker}(f) = \{e\} \)

Proof: Suppose that \( f \) is 1-1,

T.P. \( \text{Ker}(f) = \{e\} \)

Let \( a \in \text{Ker}(f) \Rightarrow f(a) = e' \)

\[ f(e) = e' \Rightarrow f(a) = f(e) \]

\[ a = e \quad \text{since } f \text{ is 1-1} \]

\[ a \in \{e\} \Rightarrow \text{Ker}(f) \subseteq \{e\} \quad \text{(1)} \]

\[ e \in \{e\} \text{ s.t. } f(e) = e' \Rightarrow e \in \text{Ker}(f) \]

\[ \{e\} \subseteq \text{Ker}(f) \quad \text{(2)} \]

From (1,2) we get \( \text{Ker}(f) = \{e\} \)

\( \Leftarrow \) Suppose that \( \text{Ker}(f) = \{e\} \)

T.P. \( f \) is 1-1

Let \( a, b \in G \) s.t. \( f(a) = f(b) \)
\[
\Rightarrow f(a) \times f(b)^{-1} = e
\]
\[
\Rightarrow f(a) \times f(b) = e
\]
\[
\therefore a \times b' \in \text{ker}(f)
\]

but \( \text{ker}(f) = \{ e \} \)

\[
\therefore a \times b' = e
\]

\[
\therefore a = b
\]

\[
\Rightarrow f \text{ is } 1-1
\]
Theorem 5.5

Every infinite cyclic group is isomorphic to \((\mathbb{Z}, +)\).

Proof: Let \((G, \cdot)\) be a cyclic group generated by \(\alpha\), \(G = \langle \alpha \rangle\).

Let \(f: G \to \mathbb{Z}\) s.t. \(f(\alpha^n) = m\).

1. \(f\) is isomorphism.
   - \(f\) is well-defined
     - \(\alpha^m = \alpha^n \Rightarrow m = n \Rightarrow f(\alpha^m) = f(\alpha^n)\)

2. \(f\) is hom
   - \(f(\alpha^m \cdot \alpha^n) = f(\alpha^{m+n}) = m + n = f(\alpha^m) + f(\alpha^n)\)
3. **TP** \( P \) is 1-1

Let \( a^n, a^m \in G \) s.t. \( P(a^n) = P(a^m) \)

\[ n = m \implies a^n = a^m \]

4. **TP** \( P \) is onto

\[ \forall n \in \mathbb{Z} \implies \exists a \in G \text{ s.t. } a^n \in G \text{ where } P(a^n) = n \]

\[ \therefore P \text{ is isomorphism} \]
**Theorem 5.6** \( (\text{The factor theorem}) \)

Let \( f : (G, \ast) \rightarrow (\hat{G}, \hat{\ast}) \) be hom. of a group \( G \) onto \( \hat{G} \), then

\[ (G/\ker(f), \times) \cong (\hat{G}, \hat{\ast}) \]

**Proof** Let \( g : G/\ker(f) \rightarrow \hat{G} \)

defined by \( g(a \ast \ker(f)) = \hat{f}(a) \)

\[ \forall a \ast \ker(f) \in G/\ker(f) \]

1. **T.P.** \( g \) is well defined

Let \( a \ast \ker(f), b \ast \ker(f) \in G/\ker(f) \)

\[ \text{s.t. } a \ast \ker(f) = b \ast \ker(f) \]

\[ \Rightarrow a \ast b^{-1} \in \ker(f) \Rightarrow \hat{f}(a \ast b^{-1}) = \hat{e} \]

\[ \Rightarrow \hat{f}(a) \ast \hat{f}(b^{-1}) = \hat{e} \Rightarrow \hat{f}(a) = \hat{f}(b) \]

\[ \Rightarrow g(a \ast \ker(f)) = g(b \ast \ker(f)) \]
2. \( G/P \): \( g \) is hom.

Let \( a \star \text{Ker}(P), \ b \star \text{Ker}(P) \in G/\text{Ker}(P) \)

\[ g(a \star \text{Ker}(P)) \star b \star \text{Ker}(P) = g(a \star b \star \text{Ker}(P)) \]

\[ = P(a \star b) = P(a) \star P(b) \]

\[ = g(a \star \text{Ker}(P)) \star g(b \star \text{Ker}(P)) \]

3. \( G/P \): \( g \) is onto

\[ \forall P(a) \in G \Rightarrow \exists a \in G \text{ s.t.} \]

\[ a \star \text{Ker}(P) \in G/\text{Ker}(P) \]

where \( g(a \star \text{Ker}(P)) = P(a) \)

\[ \therefore G/\text{Ker}(P) \cong G \]

\( G/\text{Ker}(P) \) isomorphism
Ex. Show that \( \mathbb{Z}_{20}/\{[5], [10], [15], [16]\} \cong \mathbb{Z}_5^* \)

Sol. Let \( \varphi : \mathbb{Z}_{20} \rightarrow \mathbb{Z}_5^* \) defined by

\[
\begin{align*}
\varphi([0]) &= \varphi([5]) = \varphi([10]) = \varphi([15]) = \varphi([16]) = [0] \\
\varphi(1) &= \varphi(6) = \varphi(11) = \varphi(16) = [1] \\
\varphi(2) &= \varphi(7) = \varphi(12) = \varphi(17) = [2] \\
\varphi(3) &= \varphi(8) = \varphi(13) = \varphi(18) = [3] \\
\varphi(4) &= \varphi(9) = \varphi(14) = \varphi(19) = [4]
\end{align*}
\]

To show \( \varphi \) is hom.

\( \forall [a], [b] \in \mathbb{Z}_{20} \Rightarrow \varphi([a] +_{20} [b]) = \varphi([a] +_5 \varphi([b])) \)

"\( \varphi \) is hom."
\[ P \left( \mathbb{Z}_{20} \right) = \{ [0], [1], [2], [3], [4] \} = \mathbb{Z}_5 \]

\[ \Rightarrow P \text{ is onto} \]

\[ \ker(P) = \{ [0], [5], [10], [15] \} \]

by Th. 3.6 \( (\mathbb{Z}_{20} / [5], +_{20}) \cong (\mathbb{Z}_5, +_5) \)
The Chain

Def: Let \((H_i, *)\) be all subgroups of a group \((G, *)\), the chain of \(G\) is any finite sequence of subgroups of \(G\).

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

The integer \(n\) is called the length of the chain.

Remark: if \(n = 1\) then the chain is called trivial chain.

Def: if \((H_i, *)\) is normal, \(\forall i\) then the chain is called normal chain.
The group \( Z_6 \oplus \mathbb{Z} \)

\[ Z_6 \cong \{ e \} \cong \{ 0 \} \text{ trivial chain} \]

\[ Z_6 \cong \{ 2 \} \cong \{ 0 \} \text{ normal chain of length 2.} \]

**Ex.** Asymmetric group \((S_3, 0)\)

\[ S_3 \cong A_3 \cong \{ 1 \} \text{ is normal chain} \]

**Ex.** In a group \((Z_{10}, +_{10})\)

\[ Z_{10} \cong \{ 2 \} \cong \{ 4 \} \cong \{ 8 \} \cong \{ 0 \} \text{ is a chain of length 4.} \]
A group \((\mathbb{Z}_{12}, +_{12})\) has normal cyclic subgroups is
\[
([2]) = \{[0], [2], [4], [6], [8], [10]\}
\]
and
\[
([3]) = \{[0], [3], [6], [9]\}
\]
are maximal normal subgroups of \(\mathbb{Z}_{12}\).

The chain is
\[
\mathbb{Z}_{12} \supset ([2]) \supset ([4]) \supset ([0])
\]
is composition chain since \([2]\) is maximal of \(\mathbb{Z}_{12}\).

\[
([0]) \supset ([2]) \supset ([4]) \supset ([6]) \supset ([8]) \supset ([10])
\]
Theorem 5.7 (Jordan Holder)

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

**Def**: A group \((G, *)\) is called solvable group if there exists a finite collection of subgroups of \((G, *)\)

\[ H_0 \supset H_1 \supset \cdots \supset H_n \]

1. \(G = H_0 \supset H_1 \supset \cdots \supset H_n = \{e\} \)
2. \(H_{i+1}\) is a normal subgroup of \(H_i\)
3. \(H_i/H_{i+1}\) is comm. group
Ex) Every Comm. group is Solvable

Sol) Let \((G, \cdot)\) be a Comm. group.

T.P \((G, \cdot)\) is Solvable.

Let \(H_0 = G\), \(H_1 = \{e\}\)

1. \(G = H_0 \supset H_1 = \{e\}\)

2. T.P \(H_{i+1}\) normal sub group of \(H_i\)

\(H_i\) is normal sub group of \(H_0\)

Since \(\{e\}\) is normal sub group of \(G\)

3. T.P \(H_i/H_{i+1}\) is Comm. group

\(G/\{e\} = G\) is Comm. group

\(\therefore H_i/H_{i+1}\) is Comm. group

\(\therefore (G, \cdot)\) is Solvable group.
Ex) Show that \((S_3, \circ)\) is solvable

\[ \text{Sol: } H_0 = S_3, \quad H_1 = \{I, (23), (13)\} \]
\[ H_2 = \{I\} \]

1. \(S_3 = H_0 \supset H_1 \supset H_2 = \{I\}\)

2. \(H_1\) is normal subgroup of \(H_2\)
   and \(H_2\) is normal subgroup of \(H_0\)

\[ \therefore H_1\text{ is normal subgroup of } H_i \]

3. \(H_i / H_{i+1}\) is comm. group

\[ |H_i / H_{i+1}| = \frac{|H_i|}{|H_{i+1}|} = 3 \quad \text{and} \quad 3 < 6 \Rightarrow \text{com. group} \]

\[ |H_0 / H_i| = \frac{|H_0|}{|H_i|} = \frac{6}{3} = 2 \quad \text{and} \quad 2 < 6 \Rightarrow \text{Com. group} \]

\[ \therefore (S_3, \circ) \text{ is solvable group.} \]