نـظـريـة الـزمـر

Groups Theory

University of Baghdad – College of Education for Pure Sciences – Ibn Al-Haitham – Department of Mathematic

2^{th} Stage

Year 2025 – 2026

اعـداد و تدريس

أ. د. فـاطـمـة فـيـصـل كـريـم

أ. د. يـوسـف يـعكـوب يـوسـف

م. رنـــا نـــوري مـجـيـد

CONTENTS

المصادر العربية :

[١] مقدمة في الجبر المجرد الحديث. تاليف ديفيد بيرتون وترجمه عبد العالي جاسم.

English References

[1] Introduction to modern abstract algebra. By David M. Burton.

[2] A first course in abstract algebra. By J.B. Fraleigh.

[3] Group theory. By M. Suzuki

Chapter One : Groups Theory
الفصل الاول : نظرية الزمر

Definition 1.1: Binary Operations

Let A be a non empty set. A binary operation on a set A is a function from $A \times A$ into A. (i.e.)

$*: A \times A \to A$ is a binary operation iff

(1) $a * b \in A, \forall a, b \in A$ (Closure)

(2) If $a, b, c, d \in A$ such that $a = c$ and $b = d$, then $a * b = c * d$ (well-define).

Remark 1.2: Some time we used the symbols $*, \circ, \#, \odot, \ldots$ to denote a binary operation.

Example 1. 3:

(1) The operations $\{+, \times\}$arebinary operations on R, Z, Q, C.

(2) The operation " $-$ " is not binary operation on N.

(3) The operations $\{+, -\}$ are not binary operations on O **(**odd number).

(4) The operation $\div$ is abinary operation on $R\backslash\{0\}, Q\backslash\{0\}, C\backslash\{0\}$.

Example 1.4:

Let $a * b = a + b + 2, \forall a, b \in Z^+$**.** Is $*$ a binary operation on Z^+?

Solution:

(1) Closure : Let $a, b \in Z^+$, then $a * b = \overbrace{a + b}^{\in Z^+} + 2 \in Z^+$.

(2) well-define : Let $a, b, c, d \in A$ such that $a = c$ and $b = d$, then $a * b = a + b + 2 = c + d + 2 = c * d$

$\Rightarrow *$ is a binary operation on Z^+.

Example 1.5:

Let $a * b = a^b, a, b \in Z$. Is $*$ is a binary operation on Z.

Solution:

(1) Closure : if $a = 3$ and $b = -1$. Then $a * b = 3^{-1} = \frac{1}{3} \notin \mathrm{Z}$

$\Rightarrow *$ is not a binary operation on Z.

Exercises (1): which of the following are binary operations?

[1] $a * b = a + b, \forall a, b \in R\backslash\{0\}.$

[2] $a \odot b = \frac{a}{b}, \forall a, b \in Z.$

[3] $a \# b = a + b - 3, \forall a, b \in N.$ **(Home Work 1).**

[4] $a \circ b = a + 2b - 5, \forall a, b \in R.$

[5] $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}, \forall \frac{a}{b}, \frac{c}{d} \in Q\backslash\{0\}.$

Definition 1.6: (Commutative)

A binary operation $*$ on a set A is called a commutative if and only if

$$a * b = b * a \quad \forall \quad a, b \in A.$$

Definition 1.7: (Associative)

A binary operation $*$ on a set A is called an associative if

$$(a * b) * c = a * (b * c) \quad \forall \quad a, b, c \in A.$$

Example 1.8: Let R be a set of real numbers and $*$ be a binary operation on R defined as $* b = a + b - ab$. Is $*$ commutative and associative.

Solution:

Let $a, b \in R$, then

$a * b = a + b - ab = b + a - ba = b * a$

Which implies that $*$ is commutative.

Let $a, b, c \in R$, then

$$(a * b) * c = (a + b - ab) * c$$
$$= (a + b - ab) + c - (a + b - ab)c$$
$$= a + b + c - ab - ac - bc + abc \ldots\ldots\ldots\ldots (1)$$
$$a * (b * c) = a * (b + c - bc)$$
$$= a + (b + c - bc) - a(b + c - bc)$$
$$= a + b + c - bc - ab - ac + abc \ldots\ldots\ldots\ldots (2)$$

$\Rightarrow$ (1) = (2) $\Rightarrow$ $*$ is associative.

Exercises (2): Which of the following binary operations is a comm., asso.?

[1] $a * b = a - b, \quad \forall a, b \in Z.$

[2] $a \odot b = 2ab, \quad \forall a, b \in E.$ **(Home Work 2).**

[3] $a \# b = a^3 + b^3, \quad \forall a, b \in R.$

Definition 1.9: (**Mathematical System**)
A Mathematical System or (Mathematical Structure) is a non-empty set of elements with one or more binary operations defined on this set.

Example 1.10:
$(R,+),(R,.),(R,-),(R\backslash\{0\},\div),(R,+,.),(N,+),(E,+,\times)$ are Math. System. But $(N,-),(R,\div),(\mathrm{O},+,-)$are not Math. System.

Definition 1.11: (Semi group)
A semi group is a pair $(S,\ *)$ in which S is an empty set and $*$ is a binary operation on S with associative law.
(i.e.) $(S,*)$ is semi group $\Leftrightarrow$ **(1)** $S \neq \emptyset$,
(2) $*$ is a binary operation,
(3) $\forall\ a,b,c \in S$, (a $*$b) $*$c = a $*$(b $*$c).

Example 1.12:
(1) $(Z,+),(Z,\times),(N,+),(N,\times),(E,+),(E,\times)$ are semi groups.
(2) $(\mathrm{O},+),(Z,-),(\mathrm{E},-),(R\backslash\{0\},\div)$ are not semi groups.

Definition 1.13: (**The identity element**)
Let $(S,*)$ be a Mathematical System and $e \in S$. Then e is called an identity element if $a * e = e * a = a, \forall\ a \in S$.

Definition 1.14: (**The inverse element**)
Let $(S,*)$ be a Mathematical System and $a,b \in S$. Then b is called an inverse of a if $a * b = b * a = e$ and dented by $b = a^{-1}$.

Definition 1.15: (**The Group**)
The pair $(G,*)$ is a group iff $(G,*)$ is a semi group with identity in which each element of G has an inverse.

Definition 1.16: (**The Group**)

A group $(G,*)$ is a non-empty set G and a binary operation $*$, such that the following axioms are satisfied:

(1) The binary operation $*$ is associative.

$$\text{(i.e.) } (a * b) * c = a * (b * c),\ \forall\ a, b, c \in G$$

(2) There is an element e in G such that

$$a * e = e * a = a, \forall a \in G.$$

This element e is an identity element for $*$ on G.

(3) For each a in G, there is an element b in G such that

$$a * b = b * a = e.$$

The element b is an inverse of a and denoted by a^{-1}.

Remark 1.17:

Every group is a semi group but the converse is not true as in the following example shows.

$(N,+)$ is a semigroup but not group because $\nexists a^{-1} \in N, \forall a \in N$.

Definition 1.18: (**Commutative group**)

A group $(G,*)$ is called a Commutative group iff $a * b = b * a, \forall a, b \in G$.

Example 1.19:

(1) $(Z,+),(E,+),(Q,+),(C,+)$ are commutative groups .

(2) $(Z^+,+)$ is not a group because there is no identity element for $+$ in Z^+.

(3) $(Z^+,\ \times)$ is not a group because there is an identity element 1 but no inverse of 5.

(4) $(G = \{1, 0,\ -1, 2\},+)$ is not group since $+$ is not a binary operation on G, 1+2 = 3 $\notin G$.

(5) $(G = \{1,-1\},\times)$ is comm. Group.

(6) $(R\backslash\{0\},\times)$, $(Q\backslash\{0\},\times)$,$(C\backslash\{0\},\times)$ are comm. Groups.

Example 1.20: Let $G = \{a, b, c, d\}$ be a set. Define operation $*$ on G by the following table. (**Klein 4-group)**

$*$	a	b	c	d
a	a	b	c	d
b	b	c	d	a
c	c	d	a	b
d	d	a	b	c

Is $(G,*)$ a commutative group?

Solution:

(1) Closure is true.

(2) Asso. ?

$(a * b) * c = a * (b * c)$?

$b * c = a * d$

$d = d$

$b * (a * c) = b * c = d = (b * a) * c$

$c * (a * b) = c * b = d = (c * a) * b$

$d * (a * c) = d * c = b = (d * a) * c$ ….→

$\Rightarrow *$ is asso.

(3) The identity: To prove $\exists e \in G \ s.t. x * e = e * x = x, \forall x \in G.$

$a * a = a, b * a = b, c * a = c, d * a = d.$

$\Rightarrow e = a$ is an identity element of G.

(4) The inverse: $\forall x \in G$ T.P. $\exists x^{-1} \in G \ s.t. \ x * x^{-1} = x^{-1} * x = e$

$a * a = a \Rightarrow a^{-1} = a$

$b * d = a \Rightarrow b^{-1} = d$

$c * c = a \Rightarrow c^{-1} = c$

$a * a = a \Rightarrow a^{-1} = a$

$d * b = a \Rightarrow d^{-1} = b$

(5) Comm. ? $a * b = b * a$?

$b = b$

$a * c = c * a = c$

$a * d = d * a = d$

$b * c = c * b = d$

$b * d = d * b = a$

$c * d = d * c = b$

$\Rightarrow *$ is a comm.

Therefore $(G,*)$ is a comm. group and called **Klein 4-group**.

Example 1.21: Let $G = \{1, -1, i, -i\}$ be a set and "." be operation on G. Is $(G, .)$ a group ? Comm. ?

Solution:

(1) Closure is true.

(2) Asso. Law is true

(3) 1 is an identity element.

(4) $1^{-1} = 1$, $-1^{-1} = -1, i^{-1} = -i, -i^{-1} = i$

(5) Comm .is true

∴ (G , .) is a comm.group.

.	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

Example 1.22: Let G = { $\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$, a, b ∈ Z }. Show that (G, +) is a group? Is (G, +) is a comm.? **(Home Work).**

Solution:

(1) Closure: Let $A = \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$, $B = \begin{bmatrix} c & 0 \\ 0 & d \end{bmatrix} \in$ G such that *a,b,c,d* ∈ Z, then

$$A + B = \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} + \begin{bmatrix} c & 0 \\ 0 & d \end{bmatrix} = \begin{bmatrix} a+c & 0 \\ 0 & b+d \end{bmatrix} \in G$$

Since $a+c \in$Z and $b+d \in$ Z , Closure is true

(2) Asso. Law: **(Home Work).**

(3) Identity:

Since $\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} = \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$, then $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ is an identity element of G

(4) Inverse: Let $a, b \in Z$, then $-a, -b \in Z$ and since

$$A + C = \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} + \begin{bmatrix} -a & 0 \\ 0 & -b \end{bmatrix} = \begin{bmatrix} a+(-a) & 0 \\ 0 & b+(-b) \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

∴ C = A^{-1} . ∀ A ∈ G ∃ C ∈ G such that C = A^{-1}.

∴ (G , +) is a group.

Example 1.23:

Let **G** = R×R = {(a, b) : a , b ∈ R, $a \neq 0$ } and $*$ be defined by

(a , b) $*$ (c , d) = (ac , bc + d)

Prove that (G , $*$) is a group. Is (G, $*$) Comm.?

Solution:

(1) Closure : Let (a , b) , (c , d) ∈ G $\Rightarrow$ a ≠ 0 , c ≠ 0 $\Rightarrow$ ac ≠ 0

(a , b) $*$ (c , d) = (ac , bc + d) ∈ G ac ≠ 0

(2) Asso. : Let (a , b) , (c , d) , (e , f) ∈ G , we have

(a , b) $*$[(c , d) $*$ (e , f)] = (a , b) $*$ (ce , de + f)

= (ace , bce + de + f) ……(1)

[(a , b) $*$ (c , d)] $*$ (e , f) = (ac , bc + d) $*$ (e , f)

= (ace , (bc + d)e + f))

= (ace , bce + de + f)….. (2)

∴ (1) = (2) , then asso. is true

(3) Idenitity : Let (a , b) , (x , y) ∈ G

$(a, b) * (x, y) = (x, y) * (a, b) = (a, b)$

$(a, b) * (x, y) = (ax, bx + y) = (a, b)$

∴ ax = a $\Rightarrow x = 1$

and $bx + y = b \Rightarrow b + y = b \Rightarrow y = 0$

$\therefore (x, y) = (1,0)$

Also, $(x, y) * (a, b) = (xa, ya + b) = (a, b)$

∴ $xa = a \Rightarrow x = 1$

$ya + b = b \Rightarrow ya = b - b \Rightarrow ya = 0 \Rightarrow y = 0$

$\therefore (x, y) = (1, 0)$

$\therefore (1,0)$ *is an identity element of* G

(4) Inverse: *Let* $(a, b), (c, d) \in G, a \neq 0, c \neq 0$

$(a, b) * (c, d) = (c, d) * (a, b) = (1, 0)$

$(a, b) * (c, d) = (1, 0)$

$(ac, bc + d) = (1,0) \Rightarrow ac = 1 \Rightarrow c = \frac{1}{a}$

$bc + d = 0 \Rightarrow b\frac{1}{a} + d = 0 \Rightarrow d = -\frac{b}{a}$

And $(c, d) * (a, b) = (1, 0)$ (H.W.)

$\therefore (c, d) = \left(\frac{1}{a}, \frac{-b}{a}\right)$ *is an inverse of* G

(5) Comm : G is not comm. , since Take (3,5) , (4,6)

(3, 5) $*$ (4, 6) = (12, 26)
(4, 6) $*$ (3, 5) = (12 , 23) } $\Rightarrow$ G is not comm..

Example 1.24: Let (G , ∗) be any group. The set of the function from G in to G : $F_G = \{f_a : a \in G\}$, $f_a: G \to G$ s.t. $f_a(x) = a * x$, $x \in G$,
With the composition (F_G , o) is forms a group, prove that.

Solution:

(1) Closure: Let $f_a, f_b \in F_G$, $a, b \in G$

$(f_a \text{ o } f_b)(x) = f_a(f_b(x)) = f_a(b * x)$

$= a * (b * x)$

$= (a * b) * x$, since G is a group.

$= f_{a*b}(x) \in F_G$, since $a*b \in G$

(2) Asso : Let $f_a, f_b, f_c \in F_G$, $a, b, c \in G$

$(f_a \text{ o } f_b) \text{ o } f_c = f_{a*b} \text{ o } f_c = f_{(a*b)*c}$

since * is asso. on G

$= f_{a*(b*c)} = f_a \text{ o } f_{b*c} = f_a \text{ o } (f_a \text{ o } f_c)$

(3) Identity : f_e is an identity of F_G, since

$f_a \text{ o } f_e = f_{a*e} = f_{e*a} = f_e \text{ o } f_a = f_a$

(4) Inverse : The inverse of f_a in F_G is $f_{a^{-1}}$, since

$f_a \text{ o } f_{a^{-1}} = f_{a*a^{-1}} = f_{a^{-1}*a} = f_{a^{-1}} \text{ o } f_a = f_e$

Also, if G is comm. group, then (F_G, o) is comm. group .

Exercises (3): Determine the systems (G, ∗). Is (G, ∗) a group? Is (G, ∗) a comm.? **(Home Work 3).**

[1] $(G = \{f_1, f_2, f_3, f_4, f_5, f_6\}, o)$, where

$f_1(x) = x$, $f_2(x) = \frac{1}{x}$, $f_3(x) = 1+x$, $f_4(x) = \frac{x+1}{x}$, $f_5(x) = \frac{x}{x+1}$, $f_6(x) = \frac{1}{1+x}$

[2] $G = \{(a, b) : a, b \in R , a \neq 0 , b \neq 0\}$ s.t.

$(a, b) * (c, d) = (ac, b+d)$

[3] $(G = \{ am : m \in Z \} , +)$

[4] $G = Q^+$, $a * b = \frac{ab}{5}$.

[5] $G = Z$, $a * b = a + b - 2$

[6] Let $G = \{ \begin{bmatrix} 1 & 0 \\ 0 & a \end{bmatrix} , a \in Z \}$. Is (G, +) group?

[7] Let $= \{f_1, f_2, f_3, f_4\}$, where $f_i \ni i = 1, 2, 3, 4$, are mappings on $R\backslash\{0\} \ni f_1(x) = x, f_2(x) = -x , f_3(x) = \frac{1}{x} , f_4(x) = -\frac{1}{x}$.

Show that $(G,)$ is a group. Is (G , ◦) Comm. ?

Some Properties of Groups:

Theorem 1.25: If G is a group with a binary operation $*$, then the left and right cancellation laws hold in G, that is: For all a, b, c ∈ G.

(1) If $a * b = a * c$ implies $b = c$

(2) If $b * a = c * a$ implies $b = c$ (H.W)

Proof: 1) Suppose that $a*b = a*c$, since G is a group. Then $\exists\ a^{-1} \in G$ s. t.

$$a^{-1} * (a * b) = a^{-1} * (a * c)$$
$$(a^{-1} * a) * b = (a^{-1} * a) * c$$
$$e * b = e * c$$
$$\therefore b = c$$

Theorem 1.26: In a group (G, $*$), there is only one element e in G such that

$$e * a = a * e = a, \quad \forall\ a \in G .$$

Proof: Suppose that G has two identity elements e and e' that mean

$\forall a \in G$, we have

$a * e = e * a = a$ and $a * e' = e' * a = a$.

Since each e and e' belong to G , so

$e * e' = e' * e = e$ (e عنصر و e' عنصر محايد)

$e' * e = e * e' = e'$ (e' عنصر و e عنصر محايد)

It follows that $e' = e$.

$\therefore$ ∃ Only one identity element in G.

Theorem 1.27: In a group (G , $*$), the inverse element of each element in G is unique.

Proof: Let $a \in$ G and a has two inverse x and x'. Such that

$$a * x = x * a = e$$
$$a * x' = x' * a = e$$
$$\Longrightarrow x = x * e = x * (a * x')$$
$$= (x * a) * x'$$
$$= e * x'$$
$$= x'$$

$\therefore x = x' \Longrightarrow$ the inverse is an unique element.

Theorem 1.28: If $(G , *)$ is group , then

(1) $e^{-1} = e$

(2) $(a^{-1})^{-1} = a \quad \forall\ a \in G$

(3) $(a * b)^{-1} = b^{-1} * a^{-1} \quad \forall \quad a , b \in G$

Proof:

(1) Let $e^{-1} = x$

e is the identity element of G $\Longrightarrow x * e = e * x = x$ ------- (1)

x is the inverse of e $\Longrightarrow e * x = x * e = e$ ------- (2)

from (1) and(2) $\Longrightarrow x = e \Rightarrow e^{-1} = e$.

(2) $(a^{-1})^{-1} = (a^{-1})^{-1} * e$

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

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

$= e * a = a.$

(3) To prove, $(a * b)^{-1} = b^{-1} * a^{-1}, \quad \forall\ a , b \in G$

Since $(a * b) \in G \Longrightarrow (a * b)^{-1} \in G$

$(a * b) * (a * b)^{-1} = (a * b)^{-1} * (a * b) = e$ (def . of inverse)

$(a * b) * (a * b)^{-1} = e$

$a^{-1} * (a * b) * (a * b)^{-1} = a^{-1} * e$

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

$e * b * (a * b)^{-1} = a^{-1}$

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

$e * (a * b)^{-1} = b^{-1} * a^{-1}$

$\therefore (a * b)^{-1} = b^{-1} * a^{-1}$

Theorem 1.29: Let $(G , *)$ be a group . Then

(1) $(a * b)^{-1} = a^{-1} * b^{-1} \Leftrightarrow$ G is comm. group.

(2) If $a = a^{-1}$, then G is a comm . gp . (Is the converse true?)

Proof: (1) ($\Longrightarrow$) Let $(G , *)$ be a group and $(a * b)^{-1} = a^{-1} * b^{-1}$.

To prove G is comm.

Let $a , b \in G$. To show $a * b = b * a , \forall\ a , b \in G$

$a * b = ((a * b)^{-1})^{-1}$ (by $(a^{-1})^{-1} = a$)

$= (b^{-1} * a^{-1})^{-1}$ (by Theorem 1.28 (3))

$= (b^{-1})^{-1} * (a^{-1})^{-1}$ (by $(a * b)^{-1} = a^{-1} * b^{-1}$)

$= b * a$ (by $(a^{-1})^{-1} = a$)

$\therefore$ G is comm. gp.

($\Leftarrow$) Let $(G, *)$ is a comm . gp.

To prove $(a * b)^{-1} = a^{-1} * b^{-1}$

$(a * b)^{-1} = b^{-1} * a^{-1}$ (by Theorem 1.28 (3))

$= a^{-1} * b^{-1}$ (by comm.)

(2) If $a = a^{-1}$, then G is a comm . gp . (Is the converse true?)

Proof: Let $a = a^{-1}$ To prove, $a * b = b * a$, $\forall a, b \in G$

Let $a, b \in G$ and $a * b \in G \Longrightarrow (a * b) = (a * b)^{-1}$

$= b^{-1} * a^{-1}$ (by Theorem 1.28 (3))

$= b * a$ (by $a = a^{-1}$)

$\therefore$ G is a comm. Group.

The converse of this part is not true.

(i.e.) if $(G, *)$ is comm . $\nRightarrow a = a^{-1}$

For example:

Let $(G = \{1, -1, i, -i\}, .)$ be comm . group,

Let $a = i \Longrightarrow a^{-1} = -i$

$\therefore a \neq a^{-1}$

Give another example **(H. W.).**

Definition 1.30: (**The Integral Powers of *a***)

Let $(G, *)$ be a group . The integral powers of a, $a \in G$ is defined by :

(1) $a^n = \underbrace{a * a \dots * a}_{n-times}$

(2) $a^0 = e$

(3) $a^{-n} = (a^{-1})^n, n \in Z^+$

(4) $a^{n+1} = a^n * a \ , n \in Z^+$.

For example 1.31:

(1) In $(R, +)$,

$3^0 = 0$,

$3^3 = 3 + 3 + 3 = 9$,

$3^{-2} = (3^{-1})^2 = (-3) + (-3)$

$= -6$.

(2) In (R , .) ,

$2^0 = 1$,

$2^3 = 2 \times 2 \times 2 = 8$,

$2^{-4} = (2^{-1})^4 = (\frac{1}{2})^4$

$= \frac{1}{2} \times \frac{1}{2} \times \frac{1}{2} \times \frac{1}{2} = \frac{1}{16}$

(3) In (G = {1, -1, i, -i}, .) ,

$i^o = 1$, $i^2 = i \times i = -1$, $i^{-2} = (i^{-1})^2 = (-i)^2 = - i \times -i = -1$

Theorem 1.32: Let $(G , *)$ be agroup and $a \in G$, $m , n \in Z$, then :

(1) $a^n * a^m = a^{n+m}$ $\forall n , m \in Z$ (H. W.)

(2) $(a^n)^m = a^{n\,m}$ $\forall n , m \in Z^+$

(3) $a^{-n} = (a^n)^{-1}$ $\forall n \in Z^+$

(4) $(a * b)^n = a^n * b^n$ $\forall n \in Z \iff$ G is a comm. group.

Proof:

(2) To prove, $(a^n)^m = a^{n\,m}$, $\forall n , m \in Z^+$

Let p(m) : $((a^n)^m = a^{n\,m} \quad \forall n \in Z^+))$

To prove, P(m) is true $\forall m \in Z^+$

If $m = 1 \Longrightarrow p(1) : (a^n)^1 = a^n = a^{n \times 1} \Longrightarrow$ p(1) is true

Suppose that p(k) is true with $k \in Z^+$ and $k \leq m$

$\therefore (a^n)^k = a^{nk}$

We have to prove that p (k + 1) is true P (k+ 1) : $(a^n)^{k+1} = a^{n(k+1)}$??

$(a^n)^{k+1} = (a^n)^k * (a^n)^1$ (by define of $a^{n+1} = a^n * a^1$)

$= a^{nk} * a^n$

$= a^{nk+n}$ by (1) above

$= a^{n(k+1)}$

$\therefore$ p (k + 1) is true

By the principle of mathematical induction

$\Longrightarrow$ p (m) is true $\forall m \in Z^+$

$\therefore (a^n)^m = a^{nm}$, $\forall n , m \in Z^+$

(3) To prove, $a^{-n} = (a^{-1})^n = (a^n)^{-1}$, $\forall n \in Z^+$

If $n = 1 \Longrightarrow p(1) : (a^{-1})^1 = a^{-1} = (a^1)^{-1}$

Suppose that if $n = k$ is true $\Longrightarrow p(k) = (a^{-1})^k = (a^k)^{-1}$

We must prove p (k+1) is true

$P(k+1) : (a^{-1})^{k+1} = (a^{k+1})^{-1}$?

$(a^{-1})^{k+1} = (a^{-1})^k * (a^{-1})^1 = (a^k)^{-1} * (a^1)^{-1} = (a^1 * a^k)^{-1}$

$=(a^{1+k})^{-1} = (a^{k+1})^{-1}$

$\therefore$ p (k +1) is true

By the principle of math. ind. $\Longrightarrow$ p (n) is true , $\forall n \in Z^+$.

(4) ($\Longrightarrow$) Let $(a * b)^n = a^n * b^n$, $\forall n \in Z$

If $n = 2 \Longrightarrow (a * b)^2 = a^2 * b^2$, To prove, G is a comm. Group.

$(a * b) * (a * b) = a * a * b * b$ (by def . of power int.)

$a * (b * a) * b = a * (a * b) * b$ (by asso .)

$(b * a) * b = (a * b) * b$ (by cancellation law)

$b * a = a * b$ (by cancellation law)

$\therefore$ G is a comm. group.

($\Longleftarrow$) Let G be a comm. group.

To prove, $(a * b)^n = (a^n * b^n)$, $\forall n \in Z$.

Let $p(n) : (a * b)^n = a^n * b^n$

If $n = 1 \Longrightarrow (a * b)^1 = a * b = a^1 * b^1$ is true

Suppose that p (k) is true with $k \in Z^+$ and $k \leq n$

s.t . $(a * b)^k = a^k * b^k$

We must prove P (k +1) is true

$P(k+1) : (a * b)^{k+1} = (a * b)^k * (a * b)^1$

$= a^k * b^k * a^1 * b^1$

$= (a^k * b^k) * (b * a)$ (G is a comm.)

$= a^k * (b^k * b) * a$ (by asso.)

$= a^k * b^{k+1} * a$

$= a^k * a * b^{k+1}$

$= a^{k+1} * b^{k+1}$

$\therefore$ p(k + 1) is true , $\forall n \in Z^+$.

The Group of Integers Modulo *n* زمرة الاعداد الصحيحة مقياس n

Definition 1.33:

Let $a , b \in , Z , n > 0$. Then a is congruent to b modulo n if and only if $a - b = nk , k \in Z$ and denoted by $a \equiv b$ or $a \equiv b \pmod{n}$.

(i.e.) $a \equiv b \pmod{n} \Leftrightarrow a - b = nk , k \in Z.$

Example 1.34:

(1) $17 \equiv 5 \pmod{6}$, sine $17 - 5 = 12 = (6)(2)$

(2) $8 \equiv 4 \pmod{2}$, since $8 - 4 = 4 = (2)(2)$

(3) $-12 \equiv 3 \pmod{3}$, since $-12 - 3 = -15 = (3)(-5)$

(4) $5 \not\equiv 2 \pmod{2}$, since $5 - 2 = 3 \neq (2)(k) , \forall k \in Z$

Theorem 1.35: The congruence module n is an equivalence relation on the set of integers.

Proof: Let $a , b , c \in Z , n > 0$

(1) $a - a = 0 = (n)(0)$

$\therefore a \equiv a \pmod{n}$ **Reflexive is true**

(2) If $a \equiv b \pmod{n}$, To prove, $b \equiv a \pmod{n}$

Since $a \equiv b \pmod{n} \Longrightarrow a - b = nk , k \in Z$

so , $b - a = - nk = (n)(-k) , - k \in Z$

$\therefore b \equiv a \pmod{n} \Longrightarrow$ **Symmetric is true**

(3) If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$. To prove, $a \equiv c \pmod{n}$

Since $a \equiv b \pmod{n}$, then $a-b = nk$

And $b \equiv c \pmod{n}$, then $b - c = nk^{/}$

By adding these two eqs . $\Longrightarrow a - c = n (k + k^{/}) , k + k^{/} \in Z$

$\therefore a \equiv c \pmod{n} \Longrightarrow$ **Transitive is true**

$\therefore$ The congruence modulo n is an equivalence relation.

Definition 1.36: Let $a \in Z , n > 0$. The congruence class of a modulo n, denoted by [a] is the set of all integers that are congruent to a modulo n .

(i.e.) $[a] = \{z \in Z : z \equiv a \pmod{n} \}$

$= \{z \in Z : z = a + k n , k \in Z \}.$

Example 1.37:

If n = 2 , find [0] , [1]

[0] = { z ∈ Z : z ≡ 0 (mod 2) }

= { z ∈ Z : z = 0 + 2k , k∈ Z }

= { 0 , ∓ 2 , ∓ 4 , …….. }

[1] = { z ∈ Z : z ≡ 1 (mod 2) }

= { z ∈ Z : z = 1 + 2k , k ∈ Z }

= {∓ 1 , ∓ 3 , ∓ 5 , …. }.

Example 1.38:

If n = 3 , find [1] , [7]

[1] = { z ∈ Z : z ≡ 1 (mod 3) }={ z ∈ Z : z = 1+3k, k ∈ Z }

= { 1 , 1 ∓ 3, 1 ∓ 6 …. }

= {1 , -2 , 4 , 7 , -5 , ….}.

[7] **(H. W.).**

Definition 1.39:

The set of all congruence classes modulo *n* is denoted by Z_n (which is read Z mod *n*). Thus

Z_n = { [0] , [1] , [2] , …… , [n -1] }, or

$Z_n = \{\bar{0}, \bar{1}, \bar{2}, ..., \overline{n-1}\}$

Z_n has *n* elements.

Example 1.40:

$Z_1 = \{\bar{0}\}$, $Z_2 = \{\bar{0}, \bar{1}\}$, $Z_3 = \{\bar{0}, \bar{1}, \bar{2}\}$.

Now, **we define addition on Z_n** (write $+_n$) by the following :

$$[a] +_n [b] = [a +_n b], \quad \forall [a] , [b] \in Z_n$$

Similarly, **we define multiplication on Z_n** (write "$._n$ " by the following :

$$[a] ._n [b] = [a ._n b] , \quad \forall [a] , [b] \in Z_n$$

It is easy to see that:

1. $(Z_n , +_n)$ is an abelian group with identity [0] and for every [a] $\in Z_n$, $[a]^{-1} = [n – a]$.

   This group is called the Additive Group of Integers Modulo *n* .

2. Also, $(Z_n , ._n)$ is abelian semi group with identity [1].

   It is called the Multiplicative Semi Group of Integers modulo *n*.

Example 1.41: Let $Z_4 = \{ \bar{0}, \bar{1}, \bar{2}, \bar{3} \}$, prove that $(Z_4, +_4)$ is comm.group.

$+_4$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
1	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	3	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$

(1) Closure is true

(2) Asso. is true

(3) $\bar{0}$ is an identity element

(4) Inverse:

$\bar{1}^{-1} = \bar{4} - \bar{1} = \bar{3}$

$\bar{2}^{-1} = \bar{4} - \bar{2} = \bar{2}$

$\bar{3}^{-1} = \bar{4} - \bar{3} = \bar{1}$

(5) Comm :

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

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

$\therefore (Z_4, +_4)$ is a Comm.group.

What about $(Z_4, .4)$,

$\cdot_4$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{0}$	$\bar{2}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

It is clear that we cannot have a group.

(1) Closure is true

(2) Asso. is true

(3) $\bar{1}$ is an identity element

But the numbers $\bar{0}$ and $\bar{2}$ have no inverse.

It follows that $(Z_4, .4)$ is not a group,

But it is semi group.

Definition 1.42: ((**Order of a group**))

The number of elements of a group G is called the order of G and is denoted by $|G|$ or o (G).

G is called a finite group if $|G| < \infty$ and infinite group otherwise .

Definition 1.43: (**The Order of an Element**)

The order of an element a , $a \in G$ is the least positive integer n such that $a^n = e$, where e is the identity element of G. We denoted to order a by $|a|$ or o(a).

(i.e.) $o(a) = n$ if $a^n = e$, $n \in Z^+$

Example 1.44: (Z , +) is an infinite group .

Example 1.45: In a trivial group G = { 0 }
o(*G*)= 1 , G is the only group of order 1.

Example 1.46: find the order of G and the order of each element of (G, .). Such that G = { 1, -1 , i, -i}.

Solution:
o(*G*)= 4 and
o(*a*)= ??
If $a = 1$, and $(1)^1 = 1$, $\Longrightarrow o(a) = o(1)= 1$ (since $e = 1$)
If $a = -1$, and $(-1)^2 = 1$ $\Longrightarrow o(-1)= 2$
If $a = i$, and $i^2 = -1$, $i^4 = 1 \Longrightarrow o(i)= 4$
If $a = -i$, and $-i^2 = -1$, $-i^3 = i$, $-i^4 = 1 \Longrightarrow o(-i)= = 4$

Example 1.47: Find the order of G and the order of each element of (G, *), such that $(G, *) = (Z_6, +_6)$.

Solution:
$Z_6 = \{ \bar{0} , \bar{1} , \bar{2} , \bar{3} , \bar{4} , \bar{5} \}$, $e = \bar{0}$
$o(Z_6) = 6$ since (The number of elements of a group $Z_6 = 6$)
The order of an element a, $a \in Z_6$ is the least positive integer n such that $a^n = \bar{0}$, where $\bar{0}$ is the identity element of Z_6.
$o(\bar{0}) = 1$ since $(\bar{0})^1 = \bar{0} = e$
$o(\bar{1}) = 6$ since $(\bar{1})^6 = \bar{1} + \bar{1} + \bar{1} + \bar{1} + \bar{1} + \bar{1} = \bar{6} = \bar{0} = e$
$o(\bar{2}) = 3$ since $(\bar{2})^3 = \bar{2} + \bar{2} + \bar{2} = \bar{6} = \bar{0} = e$
$o(\bar{3}) = 2$ since $(\bar{3})^2 = \bar{3} + \bar{3} = \bar{6} = \bar{0}$
$o(\bar{4}) = 3$ since $(\bar{4})^3 = \bar{4} + \bar{4} + \bar{4} = \overline{12} = (\bar{6})^2 = \bar{0} = e$
$o(\bar{5}) = 6$ since $(\bar{5})^6 = \bar{5} + \bar{5} + \bar{5} + \bar{5} + \bar{5} + \bar{5} = \overline{30} = (\bar{6})^5 = \bar{0} = e$

Exercises (4): **(Home Work 4).**
1. Find the order of Z_8 and the order of each element of $(Z_8, +_8)$.
2. Find the order of Z_9 and the order of each element of $(Z_9, +_9)$.

The Permutations : (التباديل)

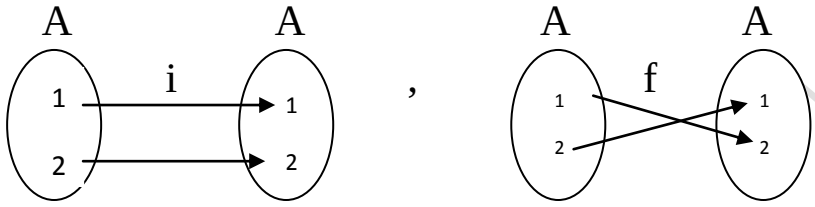
Definition 1.48: A Permutation or a symmetric of a set A is a function from A in to A that is both one to one and on to.

$$f: A \xrightarrow{1-1,onto} A$$

Symm $(A) = \{f \mid f: A \xrightarrow{1-1,onto} A\}$ the set of all permutations on A.
If A is the finite set {1, 2, …, n}, then the set of all permutation of A is denoted by S_n or P_n and $o(S_n) = n!$, where $n! = n(n-1) \dots (3)(2)(1)$

Example 1.49: Let A = {1, 2} . Write all permutation on A.

$o(P_2) = 2! = 2$



Symm(A) = {i, f } = $\{\begin{pmatrix}1 & 2\\ 1 & 2\end{pmatrix}, \begin{pmatrix}1 & 2\\ 2 & 1\end{pmatrix}\}$.

Example 1.50: Let A = {1, 2, 3}. Write all permutation on A.

$o(P_3) = 3! = (3)(2) = 6$

$$f_1 = \begin{pmatrix}1 & 2 & 3\\ 1 & 2 & 3\end{pmatrix}, f_2 = \begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}, f_3 = \begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix}$$

$$f_4 = \begin{pmatrix}1 & 2 & 3\\ 1 & 3 & 2\end{pmatrix}, f_5 = \begin{pmatrix}1 & 2 & 3\\ 3 & 2 & 1\end{pmatrix}, f_6 = \begin{pmatrix}1 & 2 & 3\\ 2 & 1 & 3\end{pmatrix}.$$

$$P_3 = Symm(A) = \{f_1, f_2, f_3, f_4, f_5, f_6\}$$

Theorem 1.51: If $A \neq \varphi$, then the set of all permutations on A Forms a group with composition of Mapps.
(i.e.) If $A \neq \varphi$, then (Symm(A) , o) is a group.

Proof:

Symm $(A) = \{f \mid f: A \xrightarrow{1-1,onto} A \ \ is\ a\ mapp.\}$,

To prove, (Symm(A) ,o) is a group.

since $\exists\ i_A: A \xrightarrow{1-1,onto} A$ a perm. on A

$\therefore i_A \in$ Symm$(A) \implies$ Symm$(A) \neq \varphi$.

(1) Closure : Let f , $g \in$ symm(A) , it follows that

$$f: A \xrightarrow{1-1,onto} A \ , \ g: A \xrightarrow{1-1,onto} A$$

$$\Rightarrow fog: A \xrightarrow{1-1,onto} A \Rightarrow fog \in \text{Symm}(A)$$

(2) Asso. : True since the composition of maps is an asso.

(3) The identity : since $i_A \in$ symm(A) and $i_A of = foi_A = f$ for all f in symm$(A) \Rightarrow i_A$ is an idenetity element

(4) The inverse : $\forall f: A \xrightarrow{1-1,onto} A, \exists f^{-1}: A \xrightarrow{1-1,onto} A$

$\therefore f^{-1} \in$ Symm(A) and $fof^{-1} = f^{-1}of = i_A$

∴ (Symm(A), o) is a group.

Is (Symm(A), o) comm. group ? **(H. W.).**

Example 1.52: Let $A = \{1, 2, 3\}$, then $S_3 = \{f_1, f_2, f_3, f_4, f_5, f_6\}$ and (S_3, o) is a group. This group is called **symmetric group**.

o	f_1	f_2	f_3	f_4	f_5	f_6
f_1	f_1	f_2	f_3	f_4	f_5	f_6
f_2	f_2	f_3	f_1	f_6	f_4	f_5
f_3	f_3	f_1	f_2	f_5	f_6	f_4
f_4	f_4	f_5	f_6	f_1	f_2	f_3
f_5	f_5	f_6	f_4	f_3	f_1	f_2
f_6	f_6	f_4	f_5	f_2	f_3	f_1

But (S_3 , o) is not Comm. Since $f_2 \circ f_4 = f_6 \neq f_4 \circ f_2 = f_5$.

To find the values of the above table, for example:

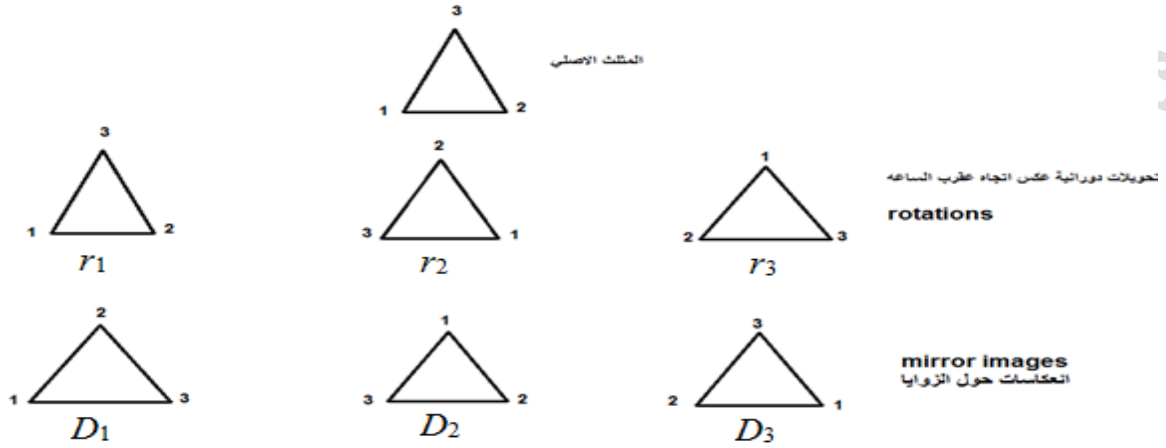
$$f_2 \circ f_4(1) = f_2\big(f_4(1)\big) = f_2(1) = 2$$

$$f_2 \circ f_4(2) = f_2\big(f_4(2)\big) = f_2(3) = 1$$

$$f_2 \circ f_4(3) = f_2\big(f_4(3)\big) = f_2(2) = 3$$

$$f_2 \circ f_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = f_6$$

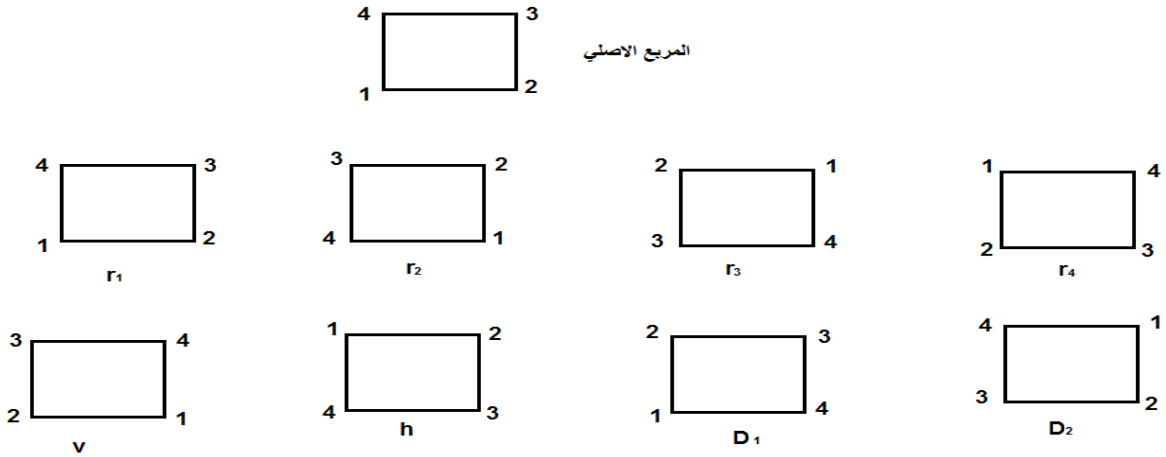
Also (S_3,o) is **called the group of symmetries of on equilateral triangle** .
(زمرة تناظر المثلث متساوي الساقين)



Then $S_3 = \{r_1, r_2, r_3, D_1, D_2, D_3\}$ and $(S_3, \circ)$ is a group of symmetries of on equilateral triangle.

Definition 1.53: (**The Dihedral Group D_n of Order $2n$**)
The n^{th} dihedral group is the group of symmetries of the regular n-gon. $o(D_n) = 2n$
D_3 : is the third dihedral group., o (D_3) = (2) (3) = 6 elements.

Example 1.54: The group of symmetries of square D_4 or Gs, o (D_4) = 8
$G_s = D_4 = \{r_1, r_2, r_3, r_4, h, v, D_1, D_2\}$, where r_i are a clockwise rotation
V, h, D_1, D_2 are mirror images



(1) Write all elements of Gs as a permutation.
(2) Is (Gs , o) comm. group? Use table **(H.W.).**

Definition 1.55: A permutation f of a set A is called a cycle of length n if there exist $a_1, a_2, \ldots\ldots, a_n \in A$ such that
$f(a_1) = a_2$, $f(a_2) = a_3, \ldots., f(a_{n-1}) = a_n$, $f(a_n) = a_1$ and $f(x) = x$,
for $x \in A$ but $x \notin (a_1\ a_2\ \ldots\ldots\ a_n)$. We write $f = (a_1\ a_2\ \ldots\ a_n)$.

Example 1.56: If $A = \{1, 2, 3, 4, 5\}$, then

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 5 & 1 & 4 \end{pmatrix} = (1354)(2) = (1354)$$

Observe that
(1354) = (3541) = (5413) = (4135).

Example 1.57: Let $A = \{1, 2, 3, 4, 5, 6\}$ be a set of a group S_6 . Then

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 3 & 2 & 6 & 5 \end{pmatrix} = (142)o(3)o(56) = (142)o(56)$$

And

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 4 & 3 & 5 & 2 & 1 \end{pmatrix} = (16)o(245)o(3) = (16)o(245)$$

These permutations above are not cycles.

Theorem 1.58: Every permutation f of a finite set A is a product of disjoint cycles.

Definition 1.59: A cycle of length 2 is a transposition.

Example 1.60: The permutation

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} = (24)$$ is a transposition.

Proposition 1.61: Any permutation can be expressed as the product of transpositions.

(i.e.) $(a_1a_2\ \ldots\ a_n) = (a_1a_2)\ (a_1a_3)\quad \ldots..(a_1a_n)$

Therefore any cycle is a product of transpositions.

Example 1.62: We see that (16) (2 5 3) = (16) (2 5) (2 3).

Definition 1.63: A permutation is **even or odd** according as it can be written as the product of an even or odd number of transpositions.

Example 1.64: Let $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix} \in P_4$. Is f even or odd permutation.

Solution: $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix} = (124) = (12)(14)$

f has 2 transpositions $\Rightarrow f$ is an even perm.

Example 1.65: Let $S_3 = \{ f_1, f_2, f_3, f_4, f_5, f_6 \}$, then determine the even and odd permutation of (S_3,o).

Solution: $f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$ is an even

$f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (123) = (12)(13)$ is an even

$f_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (132) = (13)(12)$ is an even

$f_4 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = (23)$ is an odd

, $f_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (13)$ is an odd

, $f_6 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = (12)$ is an odd

Example 1.66: Determine an even and an odd permutation of P_4. **(H.W.).**

Definition 1.67: **(Alternating Group)** زمرة التباديل

The Alternating group on n letters, denoted by A_n is the group consisting of all even permutations in the symmetric group S_n.

$$o(A_n) = \frac{n!}{2} \quad , \quad A_n \subset S_n$$

Example 1.68: Let $S_3 = \{ f_1, f_2, f_3, f_4, f_5, f_6 \}$, then

$A_3 = \{ i , f_2, f_3 \}$ is a sub group of S_3

$o(A_3) = \frac{6}{2} = 3.$

Chapter Two : Subgroups and Cyclic Groups
الفصل الثانـي : الزمر الجزئية والزمر الدائرية

Definition 2.1: Let (G, ∗) be a group and H ⊆ G, H is a non-empty subset of G. Then (H, ∗) is a subgroup of (G,∗) if (H,∗) is itself a group.

Definition 2.2:

Let (G, ∗) be a group and H ⊆ G, Then (H, ∗) is subgroup of G if :

(1) ∀ a, b ∈ H ⇒ a ∗ b ∈ H

(2) The identity element of G is an identity element of H. e ∈ G ⇒ e ∈ H

(3) ∀ a ∈ H ⇒ a^{-1}∈ H

Remark 2.3:

Each group (G, ∗) has at least two subgroup ({e}, ∗) and (G, ∗), these subgroups are known **trivial subgroups** or **improper**, any subgroup different from these subgroups known a **proper subgroup**.

Examples 2.4:

(1) $(Z, +)$ is a proper subgroup of (R, +)

(2) H = {1, – 1} ⊆ {1, –1, i , –i}, then (H, .) is a proper subgroup of ({1,–1, i ,–i}, .)

(3) H = $\{\bar{0}, \bar{2}\} \subseteq Z_4$

(H, $+_4$) is a proper subgroup of (Z_4, $+_4$).

But $\{\bar{0}, \bar{3}\}$ is not subgroup of (Z_4, $+_4$).

(4) (Q\{0}, ×) is a subgroup of (R\{0}, ×).

Theorem 2.5: Let (G, ∗) be a group and ϕ ≠ H ⊆ G. Then (H, ∗) is a subgroup of (G, ∗) iff a ∗ b^{-1} ∈ H, ∀ a, b ∈ H

Proof:

(⇒) Let (H, ∗) be a subgroup of (G, ∗) and a, b ∈ H, then

a, b^{-1}∈ H ⟹ a ∗ b^{-1}∈ H (since ∗ closure)

($\Leftarrow$) Let $a * b^{-1} \in H$ To prove, (H, $*$) is subgroup of (G, $*$).

(1) Since $H \neq \phi \Longrightarrow \exists\ b \in H$ s.t. $b * b^{-1} \in H \Longrightarrow e \in H$.

(2) Let $b \in H$ and $e \in H \Longrightarrow e * b^{-1} \in H \Longrightarrow b^{-1} \in H$

(3) Let $a \in H$ and $b^{-1} \in H$ [by (2)] $\Longrightarrow a * (b^{-1})^{-1} \in H \Longrightarrow a * b \in H$

$\therefore$ By definition (2.2) $\Rightarrow$ (H, $*$) is a subgroup of (G, $*$)

Example 2.6: Let (Z, +) be a group and H ={5a: a ∈ Z}.

Show that (H, +) is a subgroup of (Z, +)

Solution:

By Theorem (2.5) above, let x, y ∈ H, To prove, $x + y^{-1} \in H$

$x \in H \Longrightarrow x = 5a, a \in Z$, $y \in H \Longrightarrow y = 5b, b \in Z$

$x + y^{-1} = 5a + (5b)^{-1} = 5a + 5(-b)$

$= 5\underbrace{(a - b)}_{\in Z} \in H$

$\Longrightarrow$ (H, +) is a subgroup of (Z, +)

Theorem 2.7: If (H_i, $*$) is the collection of subgroups of (G, $*$), then ($\cap H_i$, $*$)) is also subgroup of (G, $*$)

Proof:

(1) Since $\exists\ e \in H_i, \forall i \Longrightarrow e \in \cap H_i \Longrightarrow \cap H_i \neq \phi$ and $H_i \subseteq G, \forall i$
Then $\cap H_i \subseteq G$

(2) Let $x, y \in \cap H_i$ To prove, $x * y^{-1} \in \cap H_i$
Since $x, y \in \cap H_i \Longrightarrow x, y \in H_i\ \forall i$
$\Longrightarrow x * y^{-1} \in H_i, \forall i$ (since H_i subgroups)
$\Longrightarrow x * y^{-1} \in \cap H_i$
$\therefore$ ($\cap H_i$, $*$) is subgroup of (G, $*$)

Theorem 2.8: Let (H_i, $*$) be the collection of subgroups of (G, $*$) and let $H_k, H_j \in \{H_i\}$ such that $\exists H_\ell \in \{H_i\}$, $H_k \subseteq H_\ell$ and $H_j \subseteq H_\ell$, then ($\cup H_i$, $*$) is also subgroup.

Proof: Since $H_i \subseteq G, \forall i$, then $\cup H_i \subseteq G$

(1) Since $\exists\ e \in H_i$ for some $i \Longrightarrow e \in \cup H_i \Longrightarrow \cup H_i \neq \phi$

(2) Let $x, y \in \cup H_i$, then $x, y \in H_k$ or $x, y \in H_j$, so $x, y \in H_\ell$

$\Longrightarrow x * y^{-1} \in H_\ell$, (since H_ℓ subgroup)

$\Longrightarrow x * y^{-1} \in \cup H_i$

$\therefore$ $(\cup H_i, *)$ is subgroup of $(G, *)$

Theorem 2.9: Let $(H_1, *)$ and $(H_2, *)$ be two subgroups of $(G, *)$, then $(H_1 \cup H_2, *)$ is a subgroup of $(G, *)$ iff $H_1 \subseteq H_2$ or $H_2 \subseteq H_1$.

Proof:

$(\Rightarrow)$ Let $(H_1 \cup H_2, *)$ be a subgroup, To prove, $H_1 \subseteq H_2$ or $H_2 \subseteq H_1$

Suppose that $H_1 \not\subset H_2$ and $H_2 \not\subset H_1$

$\therefore \exists\ a \in H_1, a \notin H_2$ and $\exists\ b \in H_2, b \notin H_1$

$\therefore a, b \in H_1 \cup H_2 \Longrightarrow a * b^{-1} \in H_1 \cup H_2$ (since $H_1 \cup H_2$ is a subgp of G)

$\Longrightarrow a * b^{-1} \in H_1$ or $a * b^{-1} \in H_2$

$\Longrightarrow a, b \in H_1$ or $a, b \in H_2$ C!!!! (تناقض)

$\therefore$ $H_1 \subseteq H_2$ or $H_2 \subseteq H_1$

$(\Leftarrow)$ Let $H_1 \subseteq H_2$ or $H_2 \subseteq H_1$ To prove, $(H_1 \cup H_2, *)$ is a subgroup

If $H_1 \subseteq H_2 \Longrightarrow H_1 \cup H_2 = H_2$ is a subgroup.

If $H_2 \subseteq H_1 \Longrightarrow H_1 \cup H_2 = H_1$ is a subgroup

$\therefore$ $H_1 \cup H_2$ is a subgroup in two cases.

Remark 2.10: $(H_1 \cup H_2, *)$ need not be a subgroup of $(G, *)$.

For example:

$H_1 = \{r_1, r_3\}$ is a subgroup of G_s, and $H_2 = \{r_1, v\}$ is a subgroup of G_s.

But $H_1 \cup H_2 = \{r_1, r_3, v\}$ is not a subgroup of G_s, since $r_3 \circ v = h \notin H_1 \cup H_2$

Definition 2.11: Let $(G, *)$ be a group and $(H, *)$, $(K, *)$ be two subgroups of G, then the product of H and K is the set:

$$H*K=\{h*k : h \in H, k \in K\}$$

Example 2.12: let $H=\{\bar{0}, \bar{4}\}$ and $K=\{\bar{0}, \bar{2}, \bar{4}, \bar{6}\}$ are subgroups of $(Z_8, +_8)$.

Find $H +_8 K$.

Sol. $H +_8 K= \{\bar{0}, \bar{2}, \bar{4}, \bar{6}\}$.

Notes 2.13:

(1) $H*H$ is write H^2

(2) If $H = \{a\}$, then $H*K = a*K$. If $K = \{b\}$, then $H*K = H*b$.

(3) $H \cup K \subseteq H*K$.

Theorem 2.14: Let $(G, *)$ be a group and $(H, *)$, $(K, *)$ are two subgroups of $(G, *)$, then

(1) $H*K \neq \phi \wedge H*K \subseteq G$

(2) $H \subseteq H*K$ and $K \subseteq H*K$

(3) $(H*K, *)$ is a subgroup of $(G, *)$ iff $H*K = K*H$

(4) If $(G, *)$ is commutative group, then $(H*K, *)$ is a subgroup of $(G,*)$.

Proof:

(1) $\because e \in H \wedge e \in K \Rightarrow e * e = e \in H*K$

$\therefore H*K \neq \phi$

And let $x \in H*K \Longrightarrow x = a * b \ni a \in H \subseteq G$ and $b \in K \subseteq G$

$\Longrightarrow a \in G \wedge b \in G$

$\Longrightarrow a * b = x \in G \quad \therefore H*K \subseteq G$

(2) Let $x \in H \Longrightarrow x = x * e \in H*K$

$\Longrightarrow x \in H*K \quad \therefore H \subseteq H*k$

Similarly $K \subseteq H*K$

(3) $(\Rightarrow)$ suppose $(H*K, *)$ is a subgroup of $(G, *)$ To prove, $H*K = K*H$

(i.e.) $H*K \subseteq K*H \wedge K*H \subseteq H*K$

Let $x \in H*K \Longrightarrow x = a*b \ni a \in H \wedge b \in K$

Since $H*K$ is subgroup of $G \Longrightarrow x^{-1} \in H*K$

Let $x^{-1} = c * d \ni c \in H \wedge d \in K$

$x = (x^{-1})^{-1} = (c*d)^{-1} = d^{-1}*c^{-1} \ni d^{-1} \in K \wedge c^{-1} \in H$

$\therefore x = d^{-1}*c^{-1} \in K*H$

$\therefore H*K \subseteq K*H.$

$K*H \subseteq H*K$ **(Home Work)**

$(\Leftarrow)$ Let $H*K = K*H$ To prove, $(H*K, *)$ is subgroup of$(G, *)$

$H*K \neq \phi$ and $H*K \subseteq G$ (by 1)

Let x, y ∈ H∗K To prove, $x*y^{-1} \in H*K$

x ∈ H∗K ⟹ x = a∗b ∋ a ∈ H ∧ b ∈ K

y ∈ H∗K ⟹ y = c∗d ∋ c ∈ H ∧ d ∈ K

$x*y^{-1} = (a*b)*(c*d)^{-1}$

$= (a*b)*(d^{-1}*c^{-1})$

$=a*(\underbrace{b*d^{-1}}_{\in K})*\underbrace{c^{-1}}_{\in H}$

$\therefore (b*d^{-1})*c^{-1} \in K*H = H*K$

$\therefore (b*d^{-1})*c^{-1} \in H*K$

$\Rightarrow \exists\ p \in H, \ell \in K \ni (b*d^{-1})*c^{-1} = p*\ell$

$\therefore a*(b*d^{-1})*c^{-1} = \underbrace{a*p}_{\in H}*\underbrace{\ell}_{\in K} \in H*K$

$\therefore\ x*y^{-1} \in H*k$

∴ (H∗K, ∗) is subgroup of (G, ∗)

(4) If (G, ∗) is commutative group, then (H∗K, ∗) is subgroup of (G, ∗).

Proof:

$H*K \neq \phi$ and $H*K \subseteq G$ (by 1)

Let x, y ∈ H∗K To prove, $x*y^{-1} \in H*K$

x ∈ H∗K ⟹ x = a∗b ∋ a ∈ H ∧ b ∈ K

y ∈ H∗K ⟹ y = c∗d ∋ c ∈ H ∧ d ∈ K

$x*y^{-1} = (a*b)*(c*d)^{-1}$

$= (a*b)*(c^{-1}*d^{-1})$ (since G is commutative)

$= a*(b*c^{-1})*d^{-1}$ (∗ is associative)

$= (a*c^{-1})*(b*d^{-1})$ (∗ is commutative and associative)

$\therefore\ x*y^{-1} \in H*K$

∴ (H∗K, ∗) is a subgroup of (G,∗).

Notes 2.15: Let (H, ∗) and (K, ∗) are two subgroup of (G, ∗), then :

(1) $H*K \neq K*H$

(2) (H∗K, ∗) need not be subgroup of (G,∗). Give example **(H. W.)**

Exercises (1): Is (H, ∗) a subgroup of (G, ∗) each of the following:

(1) $(Z_8, +_8)$, $H = \{\bar{0}, \bar{4}\}$. Find H^2.

(2) $(Z_4, +_4)$, $H = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$ and $K=\{\bar{0}, \bar{2}\}$. Find $H +_4 K$. **(Home Work 5)**

Definition 2.16: (The center of a group)

The center of a group (G,∗) denoted by **Cent(G)** or **C(G)** is the set

$$C(G) = \{c \in G: c*x = x*c, \forall x \in G\}$$

مركز الزمرة : العناصر التي تتبادل مع كل عناصر الزمرة

Note 2.17: Cent(G) ≠ ϕ, since ∃ e ∈ G s.t. e∗x = x∗e ∀ x ∈ G ⇒ e ∈ Cent(G).

Examples 2.18:

(1) In a group (R\{0}, .)
Cent(R\{0}) = R\{0},since R\{0} with multiplication is commutative

(2) In a group $(S_3, \circ)$, $Cent(S_3) = \{f_1\}$
Since $Cent(S_3) = \{f \in S_3: f\circ g = g\circ f \ \forall g \in S_3\} = \{f_1\}$

Theorem 2.19: Let (G, ∗) be a group. Then (Cent(G), ∗) is a subgroup of (G, ∗).

Proof:

Cent(G) ≠ ϕ (by note (2.17))

Cent(G) = {a ∈ G: x∗a = a∗x, ∀ x ∈ G} ⊆ G

Let a, b ∈ Cent(G) T. P. $a*b^{-1} \in Cent(G)$

T. P. $(a*b^{-1})*x = x*(a*b^{-1})$ ∀ x ∈ G

a ∈ Cent(G) ⇒ a∗x = x∗a, ∀ x ∈ G

b ∈ Cent(G) ⇒ b∗x = x∗b, ∀ x ∈ G

Now, $(a*b^{-1})*x = a*(b^{-1}*x)$

$$= a*(x^{-1}*b)^{-1}$$

$=a*(b*x^{-1})^{-1}$ (since $b \in Cent(G)$)

$= a*(x*b^{-1})$

$=(a*x)*b^{-1}$

$=(x*a)*b^{-1}$ (since $a \in Cent(G)$)

$= x*(a*b^{-1})$

$\therefore (a*b^{-1}) \in Cent(G)$

$\therefore (Cent(G),*)$ is a subgroup of $(G, *)$.

Theorem 2.20: Let $(G, *)$ be a group. Then

$Cent(G) = G \Leftrightarrow$ G is a commutative group.

Proof: ($\Rightarrow$) Let $Cent(G) = G$ **T.P.** G is a comm. gp.

$\forall a \in G \Rightarrow a \in Cent(G)$

$\therefore a*x = x*a, \forall x \in G$

$\therefore a*x = x*a, \forall x, a \in G$

$\therefore$ G is commutative group

($\Leftarrow$) Suppose that G is comm. group. **T.P.** $Cent(G) = G$

, (i.e) To prove $Cent(G) \subseteq G$ and $G \subseteq Cent(G)$

By definition of Cent(G) we have $Cent(G) \subseteq G$.

To prove, $G \subseteq Cent(G)$

Let $x \in G$, G is commutative group $\Rightarrow x*a = a*x, \forall a \in G$

$\therefore x \in Cent(G) \Rightarrow G \subseteq Cent(G)$

$\therefore$ Cent G = G

Cyclic Groups الزمر الدوارة أو (الزمر الدائرية)

Definition 2.21: Let (G, ∗) be a group and $a \in G$, the **cyclic subgroup of G generated by *a*** is denoted by $\langle a \rangle$ and defined as

$$\langle a \rangle = \{a^k : k \in Z\} = \{\ldots, a^{-1}, a^0, a^1, \ldots\}$$

الزمرة الجزئية الدائرية المتولدة بالعنصر $a \in G$

Definition 2.22: A group (G, ∗) is called **cyclic group generated by *a*** iff $\exists\, a \in G$ such that

$$G = \langle a \rangle = \{a^k : k \in Z\}$$

Examples 2.23: In $(Z_9, +_9)$ find the cyclic subgroup generated by $\bar{1}, \bar{3}, \bar{2}$. Is $(Z_9, +_9)$ cyclic group?

Solution:

$\langle \bar{1} \rangle = \{\ldots, (\bar{1})^{-3}, (\bar{1})^{-2}, (\bar{1})^{-1}, (\bar{1})^0, (\bar{1})^1, (\bar{1})^2, (\bar{1})^3, \ldots\}$

$= \{\ldots, \bar{6}, \bar{7}, \bar{8}, \bar{0}, \bar{1}, \bar{2}, \bar{3}, \ldots\} = \{\bar{0}, \bar{1}, \bar{2}, ,, \ldots, \bar{8}\} = Z_9$

$\therefore$ Z_9 is a cyclic group generated by $\bar{1}$

$\langle \bar{3} \rangle = \{\ldots, (\bar{3})^{-3}, (\bar{3})^{-2}, (\bar{3})^{-1}, (\bar{3})^0, (\bar{3})^1, (\bar{3})^2, (\bar{3})^3, \ldots\}$

$= \{\ldots, \bar{3}, \bar{6}, \bar{0}, \bar{3}, \bar{6}, \bar{0}, \ldots\} = \{\bar{0}, \bar{3}, \bar{6}\}$ is a cyclic subgroup of Z_9.

$\langle \bar{2} \rangle = \{a^k : k \in Z\} = \{\ldots, (\bar{2})^{-3}, (\bar{2})^{-2}, (\bar{2})^{-1}, (\bar{2})^0, (\bar{2})^1, (\bar{2})^2, (\bar{2})^3, \ldots\}$

$= \{\ldots, \bar{3}, \bar{5}, \bar{7}, \bar{0}, \bar{2}, \bar{4}, \bar{6}, \ldots\} = \{\bar{0}, \bar{1}, \bar{2}, ,, \ldots, \bar{8}\} = Z_9$

$\therefore$ Z_9 is cyclic group generated by $\bar{2}$

Examples 2.24: In (Z, +) fined a cyclic subgroup generated by 1, 2, – 1. Is (Z, +) cyclic group?

Solution: $\langle 1 \rangle = \{1^k : k \in Z\} = \{\ldots, 1^{-3}, 1^{-2}, 1^{-1}, 1^0, 1^1, 1^2, 1^3, \ldots\}$

$= \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\} = Z$

$\langle 2 \rangle = \{2^k : k \in Z\} = \{\ldots, 2^{-3}, 2^{-2}, 2^{-1}, 2^0, 2^1, 2^2, 2^3, \ldots\}$

$= \{\ldots, -6, -4, -2, 0, 2, 4, 6, \ldots\} \neq Z$

$\langle -1 \rangle = \{(-1)^k : k \in Z\}$

$= \{\ldots, (-1)^{-3}, (-1)^{-2}, (-1)^{-1}, (-1)^0, (-1)^1, (-1)^2, (-1)^3, \ldots\}$

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

$\therefore$ (Z, +) is cyclic group generated by 1 and – 1.

Examples 2.25: Is $(S_3,\circ)$ a cyclic group ?

Solution: $<f_1> = \{f_1\} \neq S_3$

$<f_2> = \{f_2^k : k \in Z\} = \{\ldots, f_2^{-2}, f_2^{-1}, f_2^0, f_2^1, f_2^2, \ldots..\}$

$= \{\ldots, f_2, f_3, f_1, f_2, f_3, \ldots\} = \{f_1, f_2, f_3\} \neq S_3$

$< f_3> = \{f_1, f_2, f_3\} \neq S_3$

$<f_4> = \{f_1, f_4\} \neq S_3$

$<f_5> = \{f_1, f_5\} \neq S_3$

$<f_6> = \{f_1, f_6\} \neq S_3$

$\therefore$ $(S_3,\circ)$ is not cyclic group.

Examples 2.26: Is $(G,\cdot)$ a cyclic group, such that $G = \{1, -1, i, -i\}$?

Solution:

$<1> = \{1^k : k \in Z\} = \{\ldots, 1^{-3}, 1^{-2}, 1^{-1}, 1^0, 1^1, 1^2, 1^3, \ldots\}$

$=\{\ldots, -1, 1, -1, 1, 1, 1, 1, \ldots\} = \{1, -1\} \neq G$

$<-1> = \{(-1)^k : k \in Z\}$

$= \{\ldots, (-1)^{-3}, (-1)^{-2}, (-1)^{-1}, (-1)^0, (-1)^1, (-1)^2, (-1)^3, \ldots\}$

$= \{\ldots, 1, 1, 1, -1, 1, -1 \ldots\} = \{1, -1\} \neq G$

$<i> = \{i^k : k \in Z\} = \{\ldots, i^{-2}, i^{-1}, i^0, i^1, i^2, i^3, \ldots\}$

$=\{\ldots, -1, i, 1, i, -1, -i, \ldots\} = \{1, -1, i, -i\} = G$

$<-i> = \{(-i)^k : k \in Z\} =$

$\{\ldots, (-i)^{-2}, (-i)^{-1}, (-i)^0, (-i)^1, (-i)^2, (-i)^3, \ldots\}$

$=\{\ldots, -1, i, 1, -i, -1, i, \ldots\} = \{1, -1, i, -i\} = G$

$\therefore$ $(G,\cdot)$ is a cyclic group generated by i and – i.

Examples 2.27: In $(Z_6, +_6)$ find a cyclic subgroup generated by $\bar{1}, \bar{2}, \bar{5}$

Is $(Z_6, +_6)$ a cyclic group? **(Home Work)**

Theorem 2.28: Every cyclic group is a commutative.

Proof: Let (G, $*$) be a cyclic group

$\therefore \exists\, a \in G$ s.t. $G = <a> = \{a^k : k \in Z\}$. T.P. G is a comm. group

Let $x, y \in G$. T.P. $x*y = y*x, \forall\, x, y \in G$

$\because x \in G = <a> \Rightarrow x = a^m \ni m \in Z$ and $y \in G = <a> \Rightarrow y = a^n \ni n \in Z$

$x*y = a^m * a^n = a^{m+n} = a^{n+m} = a^n * a^m = y * x$

$\therefore$ G is commutative group.

The converse of this theorem is not true, for example:

Let (G = {e, a, b, c}, $*$) s.t. $a^2 = b^2 = c^2 = e$

$a^2 = e \Rightarrow a*a = e \Rightarrow a^{-1} = a$

$b^2 = e \Rightarrow b*b = e \Rightarrow b^{-1} = b$

$c^2 = e \Rightarrow c*c = e \Rightarrow c^{-1} = c$

$e^{-1} = e \Rightarrow x^{-1} = x \ \forall x \in G$

$\therefore$ (G, $*$) is commutative group

But (G, $*$) is not cyclic group since:

$< e > = \{e\} \neq G$

$< a > = \{a^k : k \in Z\} = \{e, a\} \neq G$

$< b > = \{b^k : k \in Z\} = \{e, b\} \neq G$

$< c > = \{c^k : k \in Z\} = \{e, c\} \neq G$

$\therefore$ (G,$*$) is not cyclic.

Theorem 2.29: Let (G, $*$) be a group, then $<a> = <a^{-1}> \ \forall a \in G$

Proof:

$$< a > = \{a^k : k \in Z\} = \{(a^{-1})^{-k} : -k \in Z\}$$
$$= \{(a^{-1})^m : m = -k \in Z\}$$
$$= <a^{-1}>$$

Theorem 2.30: If (G, $*$) is a finite group of order n generated by a, then $G = < a > = \{a^k : k \in Z\} = \{a^1, a^2, \dots, a^n = e\}$ such that n is least positive integer $\ni a^n = e$.

(i.e,) $o(a) = n = o(G)$ (رتبة الزمرة = رتبة العنصر الذي يولد الزمرة)

Examples 2.31: Show that $(Z_n, +_n)$ is cyclic group.

Solution:

$Z_n = \{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{n-1}\}$ بما ان الزمرة منتهية فتكتب بالشكل :

$o(Z_n) = n$. To prove, $Z_n = <\bar{1}>$

$$<\bar{1}> = \{(\bar{1})^k : k \in Z\} = \{(\bar{1})^1, (\bar{1})^2, (\bar{1})^3, \dots\dots, (\bar{1})^{n-1}, (\bar{1})^n = \bar{0}\}$$
$$= \{\bar{1}, \bar{2}, \bar{3}, \dots, \bar{n} = \bar{0}\} = Z_n$$

$Z_n = <\bar{1}>$ and $o(Z_n) = o(\bar{1}) = n$.

Definition 2.32: (Division Algorithm for Z) **خوارزمية القسمة**

Let a and b be two integer numbers with b > 0, then there is a unique pair of integer's q and r such that:

$$a = bq + r \quad \text{where } 0 \leq r < b$$

The number q is called the quotient and r is called the remainder when a is divided by b.

Examples 2.33: Find the quotient q and remainder r when 38 is divided by 7 according to the division algorithm.

Solution: $38 = 7(5) + 3 \quad 0 \leq 3 \leq 7$

$\therefore q = 5$ and $r = 3$.

Examples 2.34: If a = 23 , b = 7

$23 = 7(3) + 2 \quad 0 \leq 2 \leq 7 \quad \Rightarrow \quad q = 3 \ , r = 2.$

Examples 2.35: If a = 15 , b = 2

$15 = (2)(7) + 1 \quad 0 \leq 1 \leq 2 \quad \Rightarrow \quad q = 7 \ , \ r = 1$

Theorem 2.36: Any subgroup of acyclic group is cyclic.

Proof: (Without proof)

Corollary 2.37: If (G, $*$) is a finite cyclic group of order *n* generated by *a* , then every subgroup of G is cyclic generated by $a^m \ \ni \ m|n$

Proof: Suppose (G, $*$) is a finite cyclic group and o(G) = *n*

$G = \langle a \rangle = \{a^1, a^2, \ldots\ldots, a^n = e\}$

Let (H, $*$) be a subgroup of (G, $*$). Then (H,$*$) is cyclic (by Theorem 2.36) such that $H = \langle a^m \rangle$

To prove, $m|n$ ($n = mg$, $g \in Z$)

Since $e \in H \Rightarrow a^n \in H$ and $a^m \in H$, by division algorithm of *n* and *m*

$\Rightarrow n = mg + r \quad 0 \leq r < m$

$r = n - mg \ \Rightarrow \ a^r = a^n * (a^m)^{-g}$

$\Rightarrow \ a^r = (a^m)^{-g} \in H$

But $0 \leq r < m \quad \Rightarrow \quad r = 0 \ \Rightarrow \ n = mg$

$\therefore \ m|n$

Examples 2.38: Find all subgroup of $(Z_{15}, +_{15})$

Solution:

$o(Z_{15}) = 15$, $H = <(\bar{1})^m> \ni m|n$

$H = <(\bar{1})^m > \ni m|15$

$m = 1, 3, 5, 15$

If $m = 1 \Rightarrow H_1 = <\bar{1}> = Z_{15}$

If $m = 3 \Rightarrow H_2 = <(\bar{1})^3> = <\bar{3}> = \{\bar{3}, \bar{6}, \bar{9}, \overline{12}, \bar{0}\}$

If $m = 5 \Rightarrow H_3 = <(\bar{1})^5> = \{\bar{5}, \overline{10}, \bar{0}\}$

If $m = 15 \Rightarrow H_4 = <(\bar{1})^{15}> = \{\bar{0}\} = <\bar{0}>$

(H.W.) Find all subgroup of $(Z_8, +_8)$.

Corollary 2.39: If $(G, *)$ is finite cyclic group of prime order, then G has no proper subgroup.

Proof: Let $(G, *)$ be a finite group such that $o(G) = p$ (p prime number)

$G = <a> = \{a^1, a^2, \ldots\ldots, a^p = e\}$

Let $(H, *)$ be cyclic subgroup

$\therefore H = <a^m> \ni m|p \Rightarrow m = 1$ or $m = p$

If $m = 1 \Rightarrow H = <a> = G$ (not proper subgroup)

If $m = p \Rightarrow H = <a^p = e> = \{e\}$ (not proper subgroup)

$\therefore$ G has no proper subgroup.

Examples 2.40: Find all subgroup of $(Z_7, +_7)$

Solution: $o(Z_7) = 7$, let $H = <(\bar{1})^m > \ni m|7$

$\therefore m = 1$, $m = 7$

If $m = 1 \Rightarrow H_1 = <\bar{1}> = Z_7$

If $m = 7 \Rightarrow H_2 = <(\bar{1})^7> = \{\bar{0}\}$.

Definition 2.41: [g.c.d(x,y)] القاسم المشترك الاكبر

A positive integer c is said to be a greatest common divisor of two non-zero number x and y iff

(1) $c \mid x \wedge c \mid y$

(2) If $a \mid x \wedge a \mid y \Rightarrow a \mid c$

(g.c.d(x, y) = c)

Examples 2.42: Find (g.c.d.(12, 18))

Solution:

g.c.d(12, 18) = 6 since

(1) $6|12 \wedge 6|18$

(2) $3|12 \wedge 3|18 \Rightarrow 3|6$

or $2|12 \wedge 2|18 \Rightarrow 2|6$

Remark 2.43: If (G, ∗) is finite cyclic group of order n generated by a , then the generators of G is a^k such that g.c.d $(k, n) = 1$.

Examples 2.44: Find all generators of $(Z_6, +_6)$

Solution:

$o(Z_6) = 6$, $Z_6 = <\bar{1}>$

$Z_6 = <(\bar{1})^k>$ s.t. g.c.d (k, 6) = 1, k =1, 2, 3, 4, 5

$k = 1 \Rightarrow$ g.c.d(1, 6) = 1 $\Rightarrow Z_6 = <\bar{1}>$

$k = 2 \Rightarrow$ g.c.d(2, 6) ≠ 1 $\Rightarrow Z_6 \neq <(\bar{1})^2> = <\bar{2}>$

$k = 3 \Rightarrow$ g.c.d(3, 6) ≠ 1 $\Rightarrow Z_6 \neq <(\bar{1})^3> = <\bar{3}>$

$k = 4 \Rightarrow$ g.c.d(4, 6) ≠ 1 $\Rightarrow Z_6 \neq <(\bar{1})^4> = <\bar{4}>$

$k = 5 \Rightarrow$ g.c.d(5, 6) = 1 $\Rightarrow Z_6 = <(\bar{1})^5> = <\bar{5}>$

The generators of Z_6 are $\{\bar{1}, \bar{5}\}$.

Examples 2.45: Find all generators of $(Z_7, +_7)$ **(H. W.)**

Theorem 2.46: If (G, ∗) is an infinite cyclic group generated by a, then:

(1) a and a^{-1} are only generators of G

(2) Every subgroup of G except {e} is an infinite subgroup.

Proof (1):

Let G = $\langle a \rangle$. To prove, G = $\langle a^{-1} \rangle$

Let $a \in G \ni G = \langle a \rangle = \{\ldots, a^{-2}, a^{-1}, a^0, a^1, a^2, \ldots\}$

Let $b \in G \ni G = \langle b \rangle = \{\ldots, b^{-2}, b^{-1}, b^0, b^1, b^2, \ldots\}$

$a \in G = \langle b \rangle \Rightarrow a = b^r, \ r \in Z$ …(1)

$b \in G = \langle a \rangle \Rightarrow b = a^s, \ s \in Z$ …(2)

Put (1) in (2) $\Rightarrow b = (b^r)^s \Rightarrow b^1 = b^{rs}$

$1 = rs \Rightarrow r = s = 1$ or $r = s = -1$

If $r = s = 1 \Rightarrow a = b \Rightarrow G = \langle a \rangle$

If $r = s = -1 \Rightarrow b = a^{-1} \Rightarrow G = \langle a^{-1} \rangle$

Proof (2):

Let (H, ∗) be a subgroup of (G, ∗) ∋ H ≠ {e}.

To prove, (H, ∗) is an infinite.

Suppose that (H,∗) is finite ∋ o(H) = k, then

(H, ∗) is cyclic subgroup

$H = \langle a^m \rangle = \{(a^m)^1, (a^m)^2, \ldots, (a^m)^k = e\}$

$a^{mk} = e \Rightarrow o(a) = mk$

∴ o(a) = o(G) but G = $\langle a \rangle$, G is finite C!!!!! تناقض

∴ (H, ∗) is infinite.

Definition 2.47: **المجموعات المشاركة للزمرة الجزئية H**

Let (H, ∗) be a subgroup of a group (G,∗) and a ∈ G.

The set **a∗H= {a ∗ h : h ∈ H}** of G is the left coset of H containing a, while the set **H∗ a= { h∗ a : h ∈ H}** is the right coset of H containing a.

Examples 2.48: If $(Z_6, +_6)$, $a = \overline{1}$ and $a = \overline{3}$, $H = \{\overline{0}, \overline{2}, \overline{4}\}$, then

$\overline{1} +_6 H = \{\overline{1}, \overline{3}, \overline{5}\}$, $H +_6 \overline{1} = \{\overline{1}, \overline{3}, \overline{5}\}$

$\overline{3} +_6 H = \{\overline{3}, \overline{5}, \overline{1}\}$, $H +_6 \overline{3} = \{\overline{3}, \overline{5}, \overline{1}\}$.

Notes 2.49:

(1) a∗H is not subgroup in general. Give an example **(H.W.)**

(2) a∗H ≠ H ∗a in general, for example

$(S_3, \circ)$, $H = \{f_1, f_4\}$, $a = f_2$

$f_2 \circ H = \{f_2, f_5\}$, $H \circ f_2 = \{f_2, f_6\}$

$f_2 \circ H \neq H \circ f_2$

Theorem 2.50: Let $(H, *)$ be a subgroup of $(G, *)$ and $a \in G$, then

(1) H is itself left coset of H in G.

Proof :

$e \in G$, $e*H = \{e*h: h \in H\} = H$

(2) If $(G, *)$ is abelian group, then $a*H = H*a$

Proof :

$a*H = \{a*h: h \in H\} = \{h*a: h \in H\} = H*a$

The converse is not true, for example: $(S_3, \circ)$, $H = \{f_1, f_2, f_3\}$, $a = f_4$

$f_4 \circ H = \{f_4, f_5, f_6\}$ and $H \circ f_4 = \{f_4, f_6, f_5\}$

$\therefore f_4 \circ H = H \circ f_4$, but $(S_3, \circ)$ is not abelian group.

(3) $a \in a*H$

Proof :

Since $e \in H \Rightarrow a*e \in a*H \Rightarrow a \in a*H$.

(4) $a*H = H \Leftrightarrow a \in H$

Proof :

($\Rightarrow$) Suppose $a*H = H$, then by (3) we get $a \in H$

($\Leftarrow$) Suppose $a \in H$. To prove, $a*H = H$

We must prove that $a*H \subseteq H \ \wedge \ H \subseteq a*H$

To prove, $a*H \subseteq H$

Let $x \in a*H \Rightarrow x = a*h \in H$ (since $a \in H \ \wedge \ h \in H$)

$\therefore a*H \subseteq H$

To prove, $H \subseteq a*H$

Let $b \in H \Rightarrow b = e*b$

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

$$= a*\underbrace{(a^{-1}*b)}_{\in H} \Rightarrow b \in a*H$$

$\therefore H \subseteq a*H$

Thus, $a*H = H$

(5) $a*H = b*H \Leftrightarrow a^{-1}*b \in H$

Proof :

($\Rightarrow$) Suppose $a*H= b*H$

$a^{-1}*(a*H) = a^{-1}*(b*H)$

$(a^{-1}*a)*H = (a^{-1}*b)*H$

$H = (a^{-1}*b)*H$

By (4) $\Rightarrow a^{-1}*b \in H$

($\Leftarrow$) Suppose $a^{-1}*b \in H$

By (4) $\Rightarrow (a^{-1}*b)*H = H$

$\Rightarrow b*H=a*H$

Remark 2.51: Every coset (left or right) of a subgroup H of a group (G, $*$) has the same number of elements as H.

(6) $a*H = b*H \vee (a*H) \cap (b*H) = \phi$

Proof :

Suppose $(a*H) \cap (b*H) = \phi$. To prove, $a*H = b*H$

$\exists x \ni x \in a*H \wedge x \in b*H$

$x = a* h_1 \wedge x = b*h_2 \ni h_1, h_2 \in H$

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

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

By (5) $\Rightarrow a*H =b*H$

or suppose $a* H \neq b*H$. To prove, $(a*H) \cap (b*H) = \phi$

suppose $(a*H) \cap (b*H) \neq \phi$

$\therefore \exists x \in a* H \wedge x \in b*H$

$x = a*h_1 \wedge x = b*h_2$

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

$\Rightarrow a*H = b*H$ C!!!!! تناقض

$\therefore (a*H) \cap (b*H) = \phi$.

(7) The set of all distinct left coset of H in G form a partition on G.

Proof:

To prove, $G = \cup_{a\in G} a* H$ and $a_i*H \cap a_j*H = \phi$

$\because$ a_i*H , a_j*H are distinct

$\therefore a_i*H \cap a_j*H = \phi$. To prove, $G = \cup_{a\in G} a* H$

$a* H \subseteq G \quad \forall\ a \in G$ (by definition of coset)

$\Rightarrow \cup_{a\in G} a* H \subseteq G$ ……..(1)

$\forall\ a \in G \Rightarrow a \in a*H \Rightarrow a \in \cup_{a\in G} a* H$

$\therefore G \subseteq \cup_{a\in G} a* H$ ……(2)

From (1) and (2) $\Rightarrow G = \cup_{a\in G} a* H$

Example 2.52: The group $(Z_6, +_6)$ is abelian. Find the partition of Z_6 into coset of the subgroup $H = \{\bar{0},\bar{3}\}$

Solution:

$Z_6 = \{\bar{0},\bar{1},\bar{2}, \bar{3},\bar{4},\bar{5}\}$

$\bar{0} +_6 H=\{\bar{0},\bar{3}\} =H, \quad \bar{3} +_6 H=\{\bar{3},\bar{0}\}$

$\bar{1} +_6 H=\{\bar{1},\bar{4}\} \quad \bar{4} +_6 H=\{\bar{4},\bar{1}\}$

$\bar{2} +_6 H=\{\bar{2},\bar{5}\}, \quad \bar{5} +_6 H=\{\bar{5},\bar{2}\}$

$\therefore$All the cosets of H are :$\{\bar{0},\bar{3}\}$, $\{\bar{1},\bar{4}\}$, $\{\bar{2},\bar{5}\}$ and since $(Z_6, +_6)$ is abelian group, then the left coset is equal the right coset.

So, the partition of Z_6 on a subgp H is $\{\bar{0},\bar{3}\}$, $\{\bar{1},\bar{4}\}$, $\{\bar{2},\bar{5}\}$.

Example 2.53: (H.W.)

In $(S_3, \circ)$, let $H = \{f_1,f_4\}$. Find the partitions of S_3 into left cosets of H and the partitions into right cosets of H.

Definition 2.54: Let $(H, *)$ be a subgroup of a group $(G, *)$. The number of left cosets or right cosets of H in G is called the index of H in G and denoted by [G:H].

Remark 2.55: If $(G, *)$ is a finite group. Then, $[G:H] = \frac{o(G)}{o(H)}$.

Example 2.56: $(S_3, \circ)$, $H = \{f_1,f_2, f_3\}$

$\therefore\ [S_3:H] = \frac{o(S_3)}{o(H)} = \frac{6}{3} = 2.$

Example 2.57: $(Z_6, +_6)$, $H = \{\bar{0}, \bar{3}\}$

$\therefore [Z_6:H] = \frac{6}{2} = 3$

Theorem 2.58: (Lagrange Theorem)

Let H be a subgroup of a finite group $(G, *)$. Then the order of H is a divisor of the order of G .

Proof:

Let G be a finite group $\ni o(G) = n$ and H be a subgroup of G $\ni o(H) = m$.

To prove, $o(H) \mid o(G)$ (i.e, To prove, $m|n$, $n = mk$)

Since G is finite $\Rightarrow [G:H] = k$

Let $a_1 * H, a_2 * H, \ldots, a_k * H$ are left cosets of H

$a_1 * H \cup a_2 * H \cup \ldots \cup a_k * H = G$ and

$a_i * H \cap a_j * H = \phi$

$o(a_1 * H) + o(a_2 * H) + \ldots + o(a_k * H) = o(G)$

$$\underbrace{m + m + \cdots + m}_{k-\text{times}} = n$$

$mk = n \Rightarrow m|n \Rightarrow o(H)|o(G)$.

Corollary 2.59: If $(G, *)$ is finite group, then the order of any element of G divides the order of G.

Proof: Suppose that $(G, *)$ is finite $\ni o(G) = n$.

Let $a \in G \Rightarrow$ a is finite order such that $o(a) = m$. To prove, $o(a)|o(G)$.

Since $a \in G \Rightarrow H = \langle a \rangle$ cyclic group.

$H = \{a, a^2, \ldots, a^m = e\}$

$o(H) = o(a) = m \Rightarrow o(H)|o(G)$ (by Lagrange theorem)

$\therefore o(a)|o(G)$

Corollary 2.60: If $(G, *)$ is a finite group, then $a^{O(G)} = e \quad \forall a \in G$.

Proof: Suppose that $o(G) = n$, let $a \in G \ni o(a) = m$

By Corollary (2.59) of Lagrange theorem $\Rightarrow o(a) \mid o(G)$

$\Rightarrow m|n$

$\Rightarrow n = mk$

$a^{O(G)} = a^n = (a^m)^k = e^k = e$

$\therefore\ a^{O(G)} = e \quad \forall\ a \in G.$

Corollary 2.61: Every group of prime order is cyclic.

Proof:

Let $(G, *)$ be finite $\ni o(G) = p$ (p prime number)

By corollary (2.59) of Lagrange theorem $\Rightarrow o(a) \mid p \quad \forall\ a \in G.$

$o(a) = 1$ or p

If $o(a) = 1 \Rightarrow a = e$

If $o(a) = p \Rightarrow o(a) = o(G) \Rightarrow G = \langle a \rangle$

$\therefore$ $(G,*)$ is cyclic group.

Corollary 2.62: Every group of order less than 6 is commutative.

Proof:

Let $(G, *)$ be a finite group $\ni o(G) < 6$

$o(G) = 1$ or 2 or 3 or 4 or 5

If $o(G) = 1 \Rightarrow G = \{e\} \Rightarrow$ G is commutative

If $o(G) = 2$ or 3 or 5

By corollary (2.61) of Lagrange theorem G is cyclic $\Rightarrow$ G is commutative

If $o(G) = 4$

$\therefore\ o(a) = 1$ or 2 or 4

If $o(a) = 1 \Rightarrow a = e$

If $o(a) = 2 \quad \forall\ a \in G \Rightarrow a^2 = e \Rightarrow a = a^{-1} \quad \forall\ a \in G$

$\therefore$ G is commutative group

If $o(a) = 4 \Rightarrow o(a) = o(G) \Rightarrow G = \langle a \rangle$

$\therefore$ G is cyclic $\Rightarrow$ G is commutative group.

Exercises (2): **(Home work 6)**

(1) Find all subgroups of $(Z_5, +_5)$.

(2) Let $(Z_8, +_8)$ be a group and $H = \langle \overline{2} \rangle$. Is H a subgroup of Z_8?

(3) If $H = \{\overline{0}, \overline{6}, \overline{12}, \overline{18}\}$, show that $(H, +_{24})$ is a cyclic subgroup of $(Z_{24}, +_{24})$. Also list the elements of each coset of H in Z_{24}.

Chapter Three : Normal Subgroups and Quotient Groups
الفصل الثالث : الزمر الجزئية الطبيعية وزمر القسمة

Definition 3.1: Let (G, *) be a group and a, b ∈ G, then

" **a is conjugate to b** ", denoted by $a \sim b$ iff $\exists\, x \in G \ni b = x*a*x^{-1}$ and

$b \sim a$ iff $\exists\, x \in G \ni a = x*b*x^{-1}$.

$a \not\sim b \Leftrightarrow b \neq x*a*x^{-1}\ \forall x \in G$.

Example 3.2: In (S_3, o). Show that $f_3 \sim f_2$. (or, Is $f_3 \sim f_2$?).

Solution:

$f_3 \sim f_2 \Leftrightarrow \exists\, x \in S_3 \ni f_2 = x\ o\ f_3\ o\ x^{-1}$

If $x = f_1 \Rightarrow f_1\ o\ f_3 o\ f_1^{-1} = f_3 \neq f_2$

If $x = f_2 \Rightarrow f_2\ o\ f_3\ o\ f_2^{-1} = f_1\ o f_2^{-1} = f_3 \neq f_2$

If $x = f_3 \Rightarrow f_3\ o\ f_3\ o\ f_3^{-1} = f_2\ o\ f_2 = f_3 \neq f_2$

If $x = f_4 \Rightarrow f_4\ o\ f_3\ o\ f_4^{-1} = f_5\ o\ f_4 = f_2$

If $x = f_5 \Rightarrow f_5\ o\ f_3\ o\ f_5^{-1} = f_6\ o\ f_5 = f_2$

If $x = f_6 \Rightarrow f_6\ o\ f_3\ o\ f_6^{-1} = f_4\ o\ f_6 = f_2$

$\therefore \exists\, x \in S_3 \ni x\ o\ f_3\ o\ x^{-1} = f_2$

$\therefore f_3 \sim f_2$

Is $f_1 \sim f_2$ and $f_1 \sim f_1$? **(H.W)**

Example 3.3: In $(Z_4, +_4)$. Is $\bar{1} \sim \bar{2}$?

Solution:

$\bar{1} \sim \bar{2} \Leftrightarrow \exists\, x \in Z_4 \ni \bar{2} = \bar{x} +_4 \bar{1} +_4 (\bar{x})^{-1}$

If $x = \bar{1} \Rightarrow \bar{1} +_4 \bar{1} +_4 (\bar{1})^{-1} = \bar{2} + \bar{3} = \bar{5} = 1 \neq \bar{2}$

If $x = \bar{2} \Rightarrow \bar{2} +_4 \bar{1} +_4 (\bar{2})^{-1} = \bar{3} +_4 \bar{2} = \bar{5} = \bar{1} \neq \bar{2}$

If $x = \bar{3} \Rightarrow \bar{3} +_4 \bar{1} +_4 (\bar{3})^{-1} = \bar{0} +_4 \bar{1} = \bar{1} \neq \bar{2}$

If $x = \bar{0} \Rightarrow \bar{0} +_4 \bar{1} +_4 (\bar{0})^{-1} = \bar{1} \neq \bar{2}$

$\therefore \quad \bar{1} \not\sim \bar{2}$

Remark 3.4: If (G, *) is abelian group and a, b ∈ G , then $a \sim b \Leftrightarrow a = b$

Proof: Suppose $a \sim b \Leftrightarrow \exists\, x \in G \ni b = x*a*x^{-1}$

$\Leftrightarrow b = x * x^{-1} * a = e * a$

$\Leftrightarrow b = a$

Theorem 3.5: The relation (Conjugate) is an equivalent relation.

Proof:

(1) Reflexive (الانعكاس)

Let $a \in G$. To prove, $a \sim a$

$\exists\ e \in G \ni a = e*a*e^{-1}$

$\therefore\ a \sim a$

(2) Symmetric (التناظر)

Let $a, b \in G$ and $a \sim b$. To prove, $b \sim a$

$a \sim b \Rightarrow \exists\ x \in G \ni\ b = x*a*x^{-1}$

$\Rightarrow x^{-1}*b = a*x^{-1}$

$\Rightarrow x^{-1}*b*x = a$

$\Rightarrow b \sim a$

(3) Transitive (التعدي)

Let $a, b, c \in G$ s.t. $a \sim b \wedge b \sim c$. To prove, $a \sim c$

$a \sim b \Rightarrow \exists\ x \in G$ s.t. $b = x*a*x^{-1}$ .....(1)

$b \sim c \Rightarrow \exists\ y \in G$ s.t. $c = y*b*y^{-1}$ .....(2)

put (1) in (2)

$c = y*(x * a * x^{-1})*y^{-1}$

$c = (y * x) * a * (y * x)^{-1}$

$c = z * a * z^{-1}$ (where $z = y * x \in G$)

$\therefore a \sim c$

Definition 3.6: Let $(G, *)$ be a group and $a \in G$, then the set of all elements conjugate to a is called conjugate class of a, denoted by c(a), and defined as:

$c(a) = \{b \in G: a \sim b\}$ (مجموعة العناصر التي ترافق a)

or $c(a) = \{b \in G: b = x * a * x^{-1}\}$

or $c(a) = \{x * a * x^{-1}, \forall\ x \in G\}$.

Example 3.7: In Example 3.2, $c(f_3) = \{f_4, f_5, f_6\}$.

Example 3.8: Find the conjugate class of each element in the following group: $(G = \{1, -1, i, -i\}, \cdot) \ni i^2 = -1$

Solution: $c(i) = \{x.i.x^{-1}, \forall x \in G\}$

$= \{1.i.1^{-1}, -1.i.(-1)^{-1}, i.i.i^{-1}, -i.i.(-i)^{-1}\}$

$= \{1.i.1, -1.i.-1, i.i.-i, -i.i.i\}$

$= \{i, i, i, i\} = \{i\}$

$\therefore$ $c(1) = \{1\}$, $c(-1) = \{-1\}$, $c(-i) = \{-i\}$.

(2) $(S_3, \circ)$ **(H.W)**

(3) $(G_S, \circ)$ **(H.W)**

Example 3.9: Find $c(\bar{3})$ in $(Z_4, +_4)$

Solution:

$c(\bar{3}) = \{\bar{0}, +_4\bar{3}+_4\bar{0}^{-1}, \bar{1}+_4\bar{3}+_4\bar{1}^{-1}, \bar{2}+_4\bar{3}+_4\bar{2}^{-1}, \bar{3}+_4\bar{3}+_4\bar{3}^{-1}\}$

$= \{\bar{0}+_4\bar{3}+_4\bar{0}, \bar{1}+_4\bar{3}+_4\bar{3}, \bar{2}+_4\bar{3}+_4\bar{2}, \bar{3}+_4\bar{3}+_4\bar{1}\}$

$= \{\bar{3}, \bar{3}, \bar{3}, \bar{3}\}$

$\therefore$ $c(\bar{3}) = \{\bar{3}\}$ (by remark if G is comm. group and $a \sim b$ then $a = b$)

فقط في الزمر الابداليه (العنصر يرافق نفسه).

Remark 3.10: Let $(G, *)$ be a group and $a \in G$, then $c(a)$ need not be a subgroup of $(G, *)$.

For example: In (S_3, o), $c(f_3) = \{f_4, f_5, f_6\}$ is not subgroup of S_3

Theorem 3.11: Let $(G, *)$ be a group and $a, b \in G$, then

(1) $a \in c(a)$ and $c(a) \neq \varphi$, $\forall a \in G$.

(2) $c(a) = c(b) \Leftrightarrow a \sim b$ $\forall a, b \in G$.

(3) $c(a) \cap c(b) = \phi$ iff $a \not\sim b$. **(H.W.)**

(4) $c(a) \cap c(b) = \phi$ or $c(a) = c(b)$. **(H.W.)**

(5) $b \in c(a) \Leftrightarrow c(a) = c(b)$.

(6) $c(a) = \{a\}$ $\forall a \in G \Leftrightarrow$ G is a comm. group.

(7) $c(a) = \{a\} \Leftrightarrow a \in Cent(G)$. **(H.W.)**

(8) $c(e) = \{e\}$. **(H.W.)**

Proof (1):

Since $a \sim a$ $\forall a \in G$ ($\sim$ is ref.)

$\Longrightarrow a \in c(a) \Rightarrow c(a) \neq \phi$

Proof (2):

($\Rightarrow$) Suppose c(a) = c(b). To prove, $a \sim b$

By (1) ,$a \in c(a) = c(b) \Rightarrow a \in c(b) \Rightarrow a \sim b$

($\Leftarrow$) Suppose $a \sim b$. To prove, c(a) = c(b)

(i.e.) $c(a) \subseteq c(b) \wedge c(b) \subseteq c(a)$?

Let $x \in c(a) \Rightarrow x \sim a \wedge a \sim b \Rightarrow x \sim b$

$\Rightarrow x \in c(b) \Rightarrow c(a) \subseteq c(b)$ .....(1)

Let $x \in c(b) \Rightarrow x \sim b \wedge a \sim b$

$\Rightarrow x \sim a \Rightarrow x \in c(a) \Rightarrow c(b) \subseteq c(a)$ .....(2)

By (1) and (2) $\Rightarrow$ c(a) = c(b)

Proof (5): $\mathbf{b \in c(a) \Leftrightarrow c(a) = c(b)}$

($\Rightarrow$) Let $b \in c(a) \Rightarrow b \sim a \Rightarrow c(a) = c(b)$(by 2)

($\Leftarrow$) $c(a) = c(b) \Rightarrow a \sim b \Rightarrow b \sim a \Rightarrow b \in c(a)$.

Proof (6): $\mathbf{c(a) = \{a\} \ \forall\, a \in G \Leftrightarrow}$ **G is a comm. group.**

$c(a) = \{a\} \ \forall\, a \in G$

$\Leftrightarrow x * a * x^{-1} = a \ \ \forall\, x \in G$

$\Leftrightarrow x * a = a * x$

$\Leftrightarrow$ G is a comm. group.

Definition 3.12: Let (G, $*$) be a group and $a \in G$, then **the normalizer of a** is denoted by N(a) and defined as:

$$N(a) = \{x \in G: x * a = a * x\}$$ (a مع تتبادل التي العناصر مجموعة)

Example 3.13: In $(Z_8, +_8)$. Find $N(\bar{3})$

Solution: $N(\bar{3}) = \{\bar{x} \in Z_8: \bar{x} +_8 \bar{3} = \bar{3} +_8 \bar{x}\} = \{\bar{0},\bar{1},\bar{2},\bar{3},\bar{4},\bar{5},\bar{6},\bar{7}\} = Z_8$.

Theorem 3.14: Let (G, $*$) be a group and $a \in G$, then

(1) (N(a) , $*$) is a subgroup of (G, $*$).

(2) Cent(G) = $\cap$ N(a) $\forall\, a \in G$. **(H.W.)**

(3) $N(a) = G \ , \forall\, a \in G \Leftrightarrow (G,*)$ is a comm.

(4) $N(a) = G \Leftrightarrow a \in G$. **(H.W.)**

(5) The Cardinal number of c(a) = the index of N(a) in G.

(6) If (G, $*$) is finite group, then o (c(a)) \ o(G).

Proof (1): **$(N(a), *)$ is a subgroup of $(G, *)$**

$N(a) = \{x \in G : x * a = a * x\} \subseteq G$

Since $e * a = a * e \Rightarrow e \in N(a) \Rightarrow N(a) \neq \phi$

(i) Closure: Let $x, y \in N(a)$. To prove, $x*y \in N(a)$

Since $x \in N(a) \Rightarrow x * a = a * x$

Since $y \in N(a) \Rightarrow y * a = a * y$

$(x * y) * a = x * (y * a) = x * (a * y)$

$= (x * a) * y = (a * x) * y = a * (x * y)$

$\therefore x * y \in N(a)$

(ii) Inverse: Let $x \in N(a)$. To prove, $x^{-1} \in N(a)$

Since $x \in N(a) \Rightarrow x * a = a * x$

$\Rightarrow x * a * x^{-1} = a$

$\Rightarrow a * x^{-1} = x^{-1} * a$

$\Rightarrow x^{-1} \in N(a)$

$\therefore (N(a), *)$ is a subgroup .

Proof (3): **$N(a) = G \quad , \forall a \in G \Leftrightarrow (G, *)$ is a comm.**

$(\Rightarrow)$ Suppose $N(a) = G \ \forall a \in G$. To prove, G is a comm.

$\forall x \in G = N(a) \Rightarrow x \in N(a) \ \forall a \in G$

$\Rightarrow x \in N(a) \ \forall x, a \in G$

$\Rightarrow x * a = a * x \ \forall x, a \in G$

$\therefore (G, *)$ is a comm. group .

$(\Leftarrow)$ Suppose $(G, *)$ is a comm. group. To prove, $N(a) = G$

(i. e. ,) To prove, $N(a) \subseteq G \ \wedge \ G \subseteq N(a)$

$N(a) \subseteq G$ (by def.) ..... (1)

To prove, $G \subseteq N(a)$

Let $x \in G \wedge$ G is a comm. $\Rightarrow x * a = a * x \quad \forall x, a \in G$

$\Rightarrow x \in N(a) \ \forall a \in G$

$\Rightarrow G \subseteq N(a)$ ..... (2)

From (1) and (2) $\Rightarrow N(a) = G \ \forall a \in G$

Proof (5): **The Cardinal number of c(a) = the index of N(a) in G**

To prove, $c(a) = [G: N(a)]$

$c(a) = \{x * a * x^{-1} : \forall x \in G\}$, $[G: N(a)] = \{ x * N(a) , \forall x \in G\}$

Define $f : [G:N(a)] \rightarrow c(a)$ s.t. $f(x*N(a)) = x * a * x^{-1} \ \forall\ x \in G$

To prove, f is map, f is 1-1 , f is onto

To prove, f is map ??

Let $x * N(a) = y*N(a)$. To prove, $f(x*N(a)) = f(y*N(a))$

Since $x*N(a) = y*N(a) \Rightarrow x^{-1} *y \in N(a)$ by $(a*H=b*H \Rightarrow a^{-1}*b \in H)$

$\Rightarrow (x^{-1}*y) *a = a* (x^{-1}*y)$

$\Rightarrow x*x^{-1}*y*a*y^{-1} = x*a*x^{-1}*y*y^{-1}$

$\Rightarrow y*a*y^{-1} = x*a*x^{-1}$

$\Rightarrow f(y*N(a)) = f(x*N(a)) \Rightarrow$ f is map.

To prove, f is 1-1 ??

Let $f(x*N(a) = f(y*N(a))$. To prove, $x*N(a) = y*N(a)$

(i.e.,) To prove, $x^{-1}*y \in N(a) \Rightarrow$ To prove, $(x^{-1}*y) *a=a* (x^{-1}*y)$

Since, $f(x*N(a)) = f(y*N(a))$

$\Rightarrow x*a*x^{-1} = y*a*y^{-1}$

$\Rightarrow x^{-1}*x*a*x^{-1}*y = x^{-1}*y*a*y^{-1}*a*y^{-1}*y$

$\Rightarrow a * (x^{-1}*y) = (x^{-1}*y) *a$

$\Rightarrow x^{-1}* y \in N(a) \Rightarrow x* N(a) = y * N(a) \Rightarrow$ f is 1-1.

To prove, f is onto ??

$R_f = \{f(x*N(a) \ \forall\ x \in G\}$

$= \{x*a*x^{-1} \ \forall\ x \in G\} = c(a) \Rightarrow$ f is onto

Hence, f is map, f is 1-1 , f is onto $\Rightarrow c(a) = [G: N(a)]$

<u>Proof (6):</u> If (G,∗) is finite group, then o(c(a)) \ o(G).

by (1) $\Rightarrow$ (N(a),∗) is a subgroup of G.

by Lag. Th. $\Rightarrow$ o(N(a)) \ o(G)

$o(G) = o(N(a)) .[G:N(a)]$

$= o(N(a)) . o(c(a))$ (by 5)

$\therefore o(c(a)) / o(G).$

Definition 3.15: Let $(H, *)$, $(K, *)$ be two subgroups of $(G, *)$, then **H is a conjugate subgroup of K** iff $\exists\, x \in G \ni K = x * H * x^{-1}$ and denoted by $H \sim K$.

$H \not\sim K \Leftrightarrow K \neq x * H * x^{-1} \quad \forall\, x \in G$.

Example 3.16: In (S_3, o), $H = \{f_1, f_6\}$, $K = \{f_1, f_5\}$. Is $H \sim K$?

Solution:

(i.e.,) Is $\exists\, x \in S_3$ such that $xo\, Ho\, x^{-1} = K$?

If $x = f_1 \Rightarrow f_1 o\{f_1,f_6\} o f_1^{-1} = \{f_1 o f_1 o f_1^{-1}, f_1 o f_6 o f_1^{-1}\} = \{f_1,f_6\} \neq K$

If $x = f_2 \Rightarrow f_2 o\{f_1,f_6\} o f_2^{-1} = \{f_2 o f_1 o f_2^{-1}, f_2 o f_6 o f_2^{-1}\} = \{f_1,f_5\} = K$

$\therefore \exists\, x = f_2 \in S_3$ such that $H \sim K$.

Example 3.17: In $(Z_{12}, +_{12})$, $H = \{\bar{0},\bar{4},\bar{8}\}$, $K = \{\bar{0},\bar{3},\bar{6},\bar{9}\}$. Is $H \sim K$?

Solution:

(i.e.,) $\exists\, \bar{x} \in Z_{12}$ such that $\bar{x} +_{12} H +_{12} \bar{x}^{-1} = K$

If $\bar{x} = \bar{1} \Rightarrow \bar{1} +_{12} \{\bar{0},\bar{4},\bar{8}\} +_{12} \bar{1}^{-1} = \bar{1} +_{12} \{\bar{0},\bar{4},\bar{8}\} +_{12} \overline{11} = H = \{\bar{0},\bar{4},\bar{8}\} \neq K$

(i.e.,) $\bar{1} +_{12} \{\bar{0},\bar{4},\bar{8}\} +_{12} \bar{1}^{-1} = \bar{1} +_{12} \bar{1}^{-1} +_{12} \{\bar{0},\bar{4},\bar{8}\} = \{\bar{0},\bar{4},\bar{8}\} = H$

$\therefore H \not\sim K \quad \forall\, \bar{x} \in Z_{12}$

Since $\bar{x} +_{12} H +_{12} \bar{x}^{-1} = \bar{x} +_{12} \bar{x}^{-1} +_{12} H = H \neq K$, so $H \sim K$.

Example 3.18: In (G_s, o), let $H = \{r_1, r_4\}$, $K = \{r_1, r_2\}$. Is $H \sim K$? **(H.W.)**

Theorem 3.19: Let $(H, *)$, $(K, *)$ be two finite subgroups of $(G, *)$ and $H \sim K$, then $o(H) = o(K)$.

Proof:

Since $H \sim K \Rightarrow \exists\, x \in G \ni K = x * H * x^{-1}$

To prove, $o(H) = o(K) = o(x * H * x^{-1})$

Define $f : (H,*) \to (x * H * x^{-1}, *)$ s.t. $f(h) = x * h * x^{-1} \quad \forall\, h \in H$

To prove, f is a map ?

Let $h_1 = h_2$. To prove, $f(h_1) = f(h_2)$

Since $h_1 = h_2 \Rightarrow x * h_1 * x^{-1} = x * h_2 * x^{-1}$

$\Rightarrow f(h_1) = f(h_2) \quad \therefore f$ is a map.

To prove, f 1-1 ?

Let $f(h_1) = f(h_2) \Rightarrow x * h_1 * x^{-1} = x * h_2 * x^{-1}$

$\Rightarrow h_1 = h_2 \quad \therefore$ f is 1-1.

To prove, f onto ?

$R_f = \{f(h): \forall h \in H\} = \{x * h * x^{-1}: \forall h \in H\} = x * H * x^{-1}$ المدى = المستقر

$\therefore$ f is onto,

$\therefore o(H) = o(x * H * x^{-1}) = o(K)$.

Theorem 3.20: Let $(H, *)$ be a subgroup of $(G, *)$ and $x \in G$, then $(x*H*x^{-1}, *)$ is a subgroup of $(G, *)$.

Proof:

Since $e*H*e^{-1} = H \neq \emptyset \Rightarrow x*H*x^{-1} \neq \emptyset$

$x*H*x^{-1} = \{x * h * x^{-1} : \forall h \in H\} \subseteq G$

Let $a, b \in x * H * x^{-1}$. To prove, $a*b^{-1} \in x * H * x^{-1}$

Since $a \in x * H * x^{-1} \Rightarrow a = x * h_1 * x^{-1} \ni h_1 \in H$

Since $b \in x * H * x^{-1} \Rightarrow b = x * h_2 * x^{-1} \ni h_2 \in H$

$a * b^{-1} = (x * h_1 * x^{-1}) * (x * h_2 * x^{-1})^{-1}$

$= (x * h_1 * x^{-1}) * (x * h_2^{-1} * x^{-1})$

$= (x * h_1) * (x^{-1} * x) * (h_2^{-1} * x^{-1})$

$= x * (h_1 * h_2^{-1}) * x^{-1} \in x * H * x^{-1}$

$\therefore (x * H * x^{-1})$ is a subgroup of $(G, *)$.

Remark 3.21: The relation "conjugate" is an equivalent relation on the set of all subgroups of G. **(H.W.)**

Definition 3.22: Let $(H, *)$ be a subgroup of $(G, *)$, then **the conjugate class of H** is denoted by C(H) and defined as:

$C(H) = \{x * H * x^{-1} : \forall x \in G\}$ (مجموعة الزمر الجزئية التي ترافق H)

Example 3.23: In (S_3, o), $H = \{f_1, f_4\}$, find C(H)

Solution:

$C(H) = \{xoHox^{-1} : \forall x \in S_3\}$

$= \{f_1o\{f_1,f_4\}of_1^{-1}, f_2o\{f_1,f_4\}o f_2^{-1}, \ldots., f_6o\{f_1,f_4\}of_6^{-1}\}$

$= \{\{f_1,f_4\}, \{f_1,f_6\}, \ldots., \{f_1,f_5\}\}$

Example 3.24: $(G = \{e, a, b, c\}, *)$ is a four Klien group.

G is comm. group , $a^2=b^2=c^2=e$. $H = \{e, a\} \subseteq G$. Find C(H)

Solution: $C(H) = \{x * H * x^{-1} : \forall x \in G\}$

$= \{x * x^{-1} * H : \forall x \in G\} = \{H\}$.

Definition 3.25: Let (H, $*$) be a subgroup of (G, $*$), then **the normalizer of H** is denoted by N(H) and defined as:

$$N(H) = \{x \in G : x * H = H * x\}.$$

Example 3.26: In (G_s, o) , $H=\{r_2,r_3\}$. Find N(H)

Solution: $N(H) = \{x \in G_s \ni xoH = Hox\}$

If $x = r_1 \Rightarrow r_1oH = H \circ r_1$

If $x = r_2 \Rightarrow r_2oH = H \circ r_2 \ldots \rightarrow \ldots..$

$\Rightarrow N(H) = \{r_1, r_2, r_3, r_4, h, v, D_1, D_2\} = Gs$

Exercises (1): Find C(H), N(H) to each of the following:

(1) (S_3, o), $H_1 = \{f_1,f_5\}$, $H_2 = \{f_1,f_4\}$.

(2) (G_5, o), $H_1 = \{r_3, r_1, v, h\}$, $H_2 = \{r_1, D_1\}$.

(3) $(Z_{12}, +_{12})$, $H = \{\bar{0}, \bar{4}, \bar{8}\}$.

Theorem 3.27: Let (H, $*$) be a subgroup of a group (G, $*$), then

(1) (N(H), $*$) is a subgroup of (G, $*$) contianing H.

(2) If (G, $*$) is a commutative group, then N(H) = G.

(3) The cardinal number of C(H) = the index of N(H) in G. **(H.W.)**

(4) If (G, $*$) is finite group, then o(C(H))/(o(G)). **(H.W.)**

Proof (1):

Since $e* H = H * e \Rightarrow e \in N(H) \neq \varphi$

$N(H) = \{x \in G \ni x * H = H * x\} \subseteq G$

Let a, b $\in$ N(H). To prove, $a * b^{-1} \in N(H)$

(i.e.,) $(a * b^{-1}) * H = H * (a * b^{-1})$

Since $a \in N(H) \Rightarrow a * H = H * a$

$b \in N(H) \Rightarrow b * H = H * b$

$b * H * b^{-1} = H \Rightarrow H * b^{-1} = b^{-1} * H \Rightarrow b^{-1} \in N(H)$

Now, $(a * b^{-1}) * H = a * (b^{-1} * H)$

$$= a * (H * b^{-1}) \qquad (b^{-1} \in N(H))$$
$$= (a * H) * b^{-1}$$
$$= (H * a) * b^{-1}$$
$$= H * (a * b^{-1})$$

$\Rightarrow a * b^{-1} \in N(H) \Rightarrow$ $(N(H),*)$ is a subgroup of $(G,*)$

To prove, $H \subseteq N(H)$

Let $a \in H \Rightarrow a * H = H \wedge H * a = H$

$\therefore a * H = H * a \Rightarrow a \in N(H)$

$\therefore H \subseteq N(H)$

Proof (2): If $(G, *)$ is a commutative group, then $N(H) = G$.

Suppose G is comm. To prove, $N(H)=G$ (i.e.,) $N(H) \subseteq G \wedge G \subseteq N(H)$.

By definition $N(H) \subseteq G$. ….. (1)

Let $x \in G$ and G is comm. gp $\Rightarrow x * H = H * x$

$\Rightarrow x \in N(H) \Rightarrow G \subseteq N(H)$ …..(2)

From (1) and (2) $\Rightarrow$ $G = N(H)$.

Remark 3.28: If $N(H) = G$, then $(G, *)$ is comm. group ? **(H.W.)**

Definition 3.29: A subgroup $(H, *)$ is called **self-conjugate** iff $C(H) = H$.

(i.e.,) $x * H * x^{-1} = H \quad \forall x \in G$.

Example 3.30: In (S_3, o), $H_1 = \{f_1,f_2,f_3\}$, $H_2 = \{f_1,f_5,f_6\}$

$C(H_1) = H_1 \Rightarrow H_1$ is self-conjugate.

$C(H_2) \neq H_2 \Rightarrow H_2$ is not self-conjugate.

Definition 3.31: A subgroup $(H, *)$is called **normal subgroup** of $(G, *)$ and denoted by $H \Delta G \Leftrightarrow H$ is self-conjugate

or $H \Delta G \Leftrightarrow x * H * x^{-1} = H \quad \forall x \in G$.

$H \not\Delta G \Leftrightarrow \exists x \in G \ni x*H*x^{-1} \neq H$

Example 3.32:

(1) If (G_s, o), $H = \{r_1,r_4,v,h\}$, then $C(H) = H \Rightarrow H \Delta G_s$

(2) If (S_3, o), $H_1 = \{f_1,f_5\}$, $H_2 = \{f_1,f_2,f_3\}$

$C(H_1) \neq H_1 \Longrightarrow H \not\Delta S_3$, and $C(H_2) = H_2 \Longrightarrow H_2 \Delta S_3$

(3) If $(Z_4, +_4)$, $H = \{\bar{0},\bar{2}\}$, then $C(H) = H \Rightarrow H \Delta Z_4$.

Theorem 3.33: Let $(H, *)$ be a subgroup of $(G, *)$, then

(1) $H \Delta G \Leftrightarrow x * H = H * x \quad \forall x \in G.$

(2) $H \Delta G \Leftrightarrow N(H) = G.$

(3) $H \Delta G \Leftrightarrow c(a) \subseteq H \quad \forall a \in H.$

(4) $H \Delta G \Leftrightarrow (x * H) * (y * H) = (x * y) * H \quad \forall x, y \in G.$

Proof (1):

$H \Delta G \Leftrightarrow x * H * x^{-1} = H \quad \forall x \in G$

$\Leftrightarrow x * H = H * x \quad \forall x \in G.$

Proof (2): $H \Delta G \Leftrightarrow N(H) = G.$

($\Rightarrow$) Suppose that $H \Delta G$. To prove, $N(H) = G$

(i.e.,) To prove, $N(H) \subseteq G \quad \wedge \quad G \subseteq N(H)$

$N(H) \subseteq G$ (by definition) ..... (1)

Let $x \in G$ and $H \Delta G \Rightarrow x * H = H * x$, $\forall x \in G$

$\Rightarrow x \in N(H) \Longrightarrow G \subseteq N(H)$ ..... (2)

From (1) and (2) $\Rightarrow G = N(H)$.

($\Leftarrow$) Suppose $N(H) = G$, To prove, $H \Delta G$

$\forall x \in G \Rightarrow x \in N(H) \Rightarrow \quad x * H = H * x \quad \forall x \in G \Rightarrow H \Delta G$ (by(1))

Proof (3): $H \Delta G \Leftrightarrow c(a) \subseteq H \quad \forall a \in H.$

($\Rightarrow$) Suppose $H \Delta G$. To prove, $c(a) \subseteq H \quad \forall a \in H$

Since $H \Delta G \Longrightarrow x * H * x^{-1} = H$ (by definition)

$\Longrightarrow x * H * x^{-1} \subseteq H$

$\therefore c(a) = \{x * a * x^{-1} \quad \forall a \in H \} \subseteq H$

($\Leftarrow$) Suppose $c(a) \subseteq H \quad \forall a \in H$. To prove, $H \Delta G$.

(i.e., To prove, $x * H * x^{-1} \subseteq H \quad \wedge \quad H \subseteq x * H * x^{-1}$

Since, $c(a) \subseteq H \Rightarrow x * H * x^{-1} \subseteq H$ .....(1)

Let $b \in H \Longrightarrow b = e * b * e^{-1}$

$\Longrightarrow b = (x * x^{-1}) * b * (x * x^{-1})$

$= x * (x^{-1} * b * x) * x^{-1}$

$b = x * h * x^{-1} \in x * H * x^{-1}$ (where $h = x^{-1} * b * x$)

$\therefore$ $H \subseteq x * H * x^{-1}$ …….. (2)

From (1) and (2) $\Rightarrow$ $H = x * H * x^{-1}$ $\forall x \in G$

$\therefore$ $H \Delta G$

Proof (4): $\mathbf{H \Delta G \Leftrightarrow (x * H) * (y * H) = (x * y) * H \quad \forall x, y \in G.}$

($\Rightarrow$) $(x * H) * (y * H) = (x * H * y) * H$

$= x * (H * y) * H$

$= x * (y * H) * H$ (since $H \Delta G$)

$= (x * y) * (H * H)$

$= (x * y) * H$

($\Leftarrow$) Suppose $H \not\Delta G \Rightarrow \exists\, x \in G \ni x * H * x^{-1} \neq H$

$\Rightarrow (x * H) * (x^{-1} * H) \neq H * H$

$\Rightarrow (x * x^{-1}) * H \neq H$

$\Rightarrow e * H \neq H$ C!!!!! (تناقض) $\therefore H \Delta G.$

Theorem 3.34: Let $(G, *)$ be a group, then

(1) $\{e\} \Delta G.$

(2) $G \Delta G$

(3) $Cent(G) \Delta G$.

Proof: **(H.W.)**

Theorem 3.35: Every subgroup of a comm. group is a normal subgroup.

Proof: Let $(G, *)$ be a comm. group and $(H, *)$ be a subgroup of $(G, *)$.

To prove, $x * H * x^{-1} = H \quad \forall x \in G$

$x * H * x^{-1} = (x * x^{-1}) * H = e * H = H \quad \forall x \in G$

$\therefore$ $H \Delta G.$

Remark 3.36: The converse of this theorem is not true.

For example: Take $(G = (\pm 1, \pm i, \pm j, \pm k), .) \ni i^2 = j^2 = k^2 = -1$

$ij = k, \quad ji = -k \Rightarrow ij \neq ji \implies$ G is not a comm.

The subgroup of G are :$\{1\}$, $G, \{\pm 1\}, \{1, -1, i, -i\}, \{1, -1, j, -j\}, \{1, -1, k, -k\}$.

Theorem 3.37: Let $(H, *)$ be a subgroup of $(G, *)$ such that$[G:H] = 2$, then $H \Delta G$.

Proof:

Since $[G:H] = 2$, then there are two distinct left (right) cosets of H in G.

H and $a*H \ni a \in G - H$ (left cosets of H in G)

H and $H*a \ni a \in G - H$ (right cosets of H in G)

$H \cup a * H = G \wedge H \cap a * H = \emptyset$ .....(1)

$H \cup H * a = G \wedge H \cap H * a = \emptyset$ .....(2)

If $a \in H \Rightarrow a * H = H = H * a \Rightarrow a * H = H * a \quad \forall a \in H$

If $a \in G - H \Rightarrow a * H = G - H = H * a \Rightarrow a * H = H * a \quad \forall a \in H$

$\therefore a * H = H * a \quad \forall a \in H$

$\therefore H \Delta G$

Remark 3.38: The converse of this theorem is not true

For example :

Take, (G_s, o), $H = \{r_1, r_4\}$

$H \Delta G_s$, but $[G_s:H] = 4 \neq 2$.

Remark 3.39: If $(H, *)$ and $(K, *)$ are two subgroups of $(G,*)$ and $H \Delta G$, then $(H \cap K) \trianglelefteq G$ and $(H*K) \trianglelefteq G$.

Example 3.40:

(1) Consider (S_3, o) and $H = \{f_1\} \Delta S_3$ and $K = \{f_1, f_4\} \trianglelefteq S_3$

$\Rightarrow H*K = \{f_1, f_4\} \trianglelefteq S_3$

(2) Consider (G_s, o) and $H = \{r_1, r_3, h, v\} \Delta G$ and $K = \{r_1, v\} \trianglelefteq G$

$\Rightarrow H \cap K = \{r_1, v\} \trianglelefteq G_s$, since $C(H*K) \neq H \cap K$

Definition 3.41: A group $(G, *)$ is called **simple group** iff G has no proper normal subgroup.

Example 3.42:

(1) (S_3, o) is not simple group, since $H = \{f_1, f_2, f_3\}$ is a proper subgroup and $H \Delta S_3$

(2) (G_s, o) is not simple group, since $H = \{r_1, r_3, v, h\}$ is a proper subgroup and $H \Delta G_s$.

(3) $(Z_6, +_6)$ is not simple group, since $H = \{\bar{0}, \bar{3}\}$ is a proper subgroup and $H \Delta Z_6$

(4) $(Z_3, +_3)$ is simple group, since Z_3 has no proper subgroup.
Also, $\{0\} \Delta Z_3$ and $Z_3 \Delta Z_3$.

Definition 3.43: Let $H \Delta G$ and $G|H = \{x * H : x \in G\}$ define $\otimes$ on $G|H$ as follows:

$$(x * H) \otimes (y * H) = (x * y) * H \quad \forall x, y \in G$$

$(G|H, \otimes)$ is called **quotient group of G by H** .

Theorem 3.44: Let $H \Delta G$, then $(G|H, \otimes)$ is a group.

Proof:

$G|H = \{a * H : a \in G\}$

Since $e * H = H \in G|H \neq \emptyset$

Closure: Let $a * H, b * H \in G|H$

$$(a * H) \otimes (b * H) = (a * b) * H \quad \forall \ a * H, b * H \in G|H$$

Asso. : Let $a * H, b * H, c * H \in G|H$

$$[(a * H) \otimes (b * H)] \otimes (c * H) = [(a * b) * H] \otimes (c * H)$$
$$= ((a * b) * c) * H$$
$$= (a * (b * c)) * H$$
$$= (a * H) \otimes [(b * c) * H]$$
$$= (a * H) \otimes](b * H) \otimes (c * H)].$$

Identity : $e * H = H \in G|H$

$$(a * H) \otimes (e * H) = (a * e) * H = a * H \quad \forall \ a * H \in G|H$$

and $(e * H) \otimes (a * H) = (e * a) * H = a * H \quad \forall \ a * H \in G|H$

$\therefore$ $e * H$ is an identity element of $G|H$.

Inverse : Let $a * H \in G|H$, To prove, $(a * H)^{-1} = a^{-1} * H$

$(a * H) \otimes (a^{-1} * H) = (a * a^{-1}) * H = e * H = H$

$(a^{-1} * H) \otimes (a * H) = (a^{-1} * a) * H = e * H = H$

$\therefore \forall \ a * H \in G|H \quad \exists \ a^{-1} * H \in G|H.$

$\therefore$ $(G|H, \otimes)$ is a group.

Example 3.45: In $(Z_6, +_6)$, $H = \{\bar{0},\bar{3}\}$. Find $Z_6|H$ **(if exist)**

Solution:

$\because$ $H \Delta Z_6 \Rightarrow Z_6|H$ exist

$\bar{0}+_6H = H$,

$\bar{1}+_6H = \{\bar{1}, \bar{4}\}$,

$\bar{2}+_6H = \{\bar{2}, \bar{5}\}$

$\bar{3}+_6H = \{\bar{3},\bar{0}\} = H$,

$\bar{4}+_6H = \{\bar{4},\bar{1}\} = \bar{1}+_6H$,

$\bar{5}+_6H = \{\bar{5},\bar{2}\} = \bar{2}+_6H$

So, $Z_6|H = \{H,\bar{1}+_6H,\bar{2}+_6H\}$

$o(Z_6|H) = 3$

$(Z_6|H, \otimes)$ is a quotient group.

H is an identity.

$(\bar{1}+_6H)^{-1} = (\bar{1})^{-1}+_6H = \bar{5}+_6H = \bar{2}+_6H$

$(\bar{2}+_6H)^{-1} = (\bar{2})^{-1}+_6H = \bar{4}+_6H = \bar{1}+_6H$

$\otimes$	H	$\bar{1}+_6H$	$\bar{2}+_6H$
H	H	$\bar{1}+_6H$	$\bar{2}+_6H$
$\bar{1}+_6H$	$\bar{1}+_6H$	$\bar{2}+_6H$	H
$\bar{2}+_6H$	$\bar{2}+_6H$	H	$\bar{1}+_6H$

Example 3.46:

(1) In $(Z_{20}, +_{20})$, $H = <\bar{5}>$. Find $Z_{20}|H$ (if exist) **(H.W.)**

(2) In (S_3, o), $H = \{f_1,f_2,f_3\}$. Find $S_3|H$ (if exist)
And if $H = \{f_1,f_4\}$. Find $S_3|H$ (if exist)

Solution:

Since $H \Delta S_3 \Rightarrow S_3|H$ (exist)

$f_1 o H = H$

$f_2 o H = \{f_2,f_3,f_1\} = H$

$f_3 o H = \{f_3,f_1,f_2\} = H$

$f_4 o H = \{f_4,f_6,f_5\}$

$f_5 o H = \{f_5,f_4,f_6\} = f_4oH$

$f_6 o H = \{f_6,f_5,f_4\} = f_4oH$

$\therefore$ $S_3|H = \{H, f_4o H\}$

But if $H = \{f_1,f_4\}$, $H \not\Delta S_3$

$\therefore$ $S_3|H$ is not exist

Theorem 3.47: The quotient group of comm. group is comm.

Proof: Suppose $(G, *)$ is a comm. group and $(H, *)$ is a subgroup of $(G,*)$ such that $H \Delta G$

$\therefore$ $G|H$ is a group.

Let $a * H , b * H \in G|H$

$$(a * H)\otimes(b * H) = (a * b) * H$$
$$= (b * a) * H \quad \text{(since G is a comm.)}$$
$$= (b * H)\otimes(a * H)$$

$\therefore$ $(G|H, \otimes)$ is a comm. group.

Theorem 3.48: If $(G, *)$ is a cyclic group, then $(G|H, *)$ is a cyclic group.

Proof:

Suppose $(G, *)$ is cyclic, H is a subgroup of G.

$\therefore \exists\ a \in G \ni G = < a > = \{a^k : k \in Z\}$

Since G is cyclic $\Rightarrow$ G is comm $\Rightarrow$ $H \Delta G \Rightarrow G|H$ is a group.

To prove, $G|H$ is cyclic group.

(i.e.,) To prove, $\exists\ a * H \in G|H \ni G|H = < a * H > = \{(a*H)^k : k \in Z\}$

(i.e.,) To prove, $G|H \subseteq < a * H > \ \wedge\ <a *H> \subseteq G|H$

Let $x * H \in G|H \Rightarrow x \in G = <a> \Rightarrow x = a^r \ni r \in Z$

$$x * H = a^r * H = (\underbrace{a * a * \dots \dots * a}_{\text{r- times}}) * H = (\underbrace{a * H)\otimes \dots \dots \otimes(a}_{\text{r- times}} * H)$$

$$= (a * H)^r \in < a * H >$$

$\Rightarrow x* H \in < a * H > \Rightarrow G|H \subseteq < a * H >$ ……. (1)

Let $y*H \in < a * H >$

$y * H = (a * H)^s \ni s \in Z$

$y * H = a^s * H \in G|H$

$\therefore$ $y * H \in G|H \Rightarrow <a*H> \subseteq G|H$ …….. (2)

From (1) and (2) $\Rightarrow$ $G|H = <a * H>$

Remark 3.49: The converse of this theorem is not true.

For example:

Take, (S_3, o), $H = \{f_1, f_2, f_3\} \Delta S_3$

$\therefore$ $S_3|H$ is a group

$S_3|H = \{H, f_4 o H\}$

$o(S_3|H) = 2$ (prime order)

$S_3|H$ is a cyclic group but (S_3, o) is not cyclic.

$S_3|H = \langle f_4 o H \rangle = \{f_4 \text{ o } H, (f_4 o H)^2\} = \{f_4 o H, f_1 o H\}$.

Theorem 3.50: Let $(G, *)$ be a group and $(G|cent(G), \otimes)$ is a cyclic group. Then $(G, *)$ is comm. (بدون برهان)

Remark 3.51: The converse of this theorem is not true.

For example:

Take, $G = \{e, a, b, c\} \ni a^2 = b^2 = c^2 = e$

G is comm. (not cyclic)

$Cent(G) = G \Rightarrow G|cent(G) = (G|G) = \{G\} = \{e, a, b, c\}$

$\therefore$ G|Cent(G) is not cyclic.

Chapter Four : Isomorphic Groups
الفصل الرابع : الزمر المتشاكلة او تشاكل الزمر

Definition 4.1: Let $(G, *)$ and $(G', .)$ be two groups and $f : (G, *) \to (G', .)$ be a mapping, then f is called a homomorphism iff

$$f(x * y) = f(x).f(y), \ \forall x, y \in G.$$

Example 4.2: Let $f : (R, +) \to (R^+, .)$, s.t. $f(a) = 2^a, \ \forall a \in R$.
Is f a homomorphism map.?

Solution:

Let $a, b \in R$ To Prove $f(a + b) = f(a).f(b)$?

$$f(a + b) = 2^{a+b} = 2^a.2^b = f(a).f(b)$$

$\therefore f$ is a homomorphism map.

Example 4.3: Let $f : (Z, +) \to (Z, +)$, such that $f(x) = 3x + 2, \ \forall x \in Z$.
Is f a homomorphism map.?

Solution:

Let $x, y \in Z$ To Prove $f(x + y) = f(x) + f(y)$?

$$\Rightarrow f(x + y) = 3(x + y) + 2 = 3x + 3y + 2 \quad \ldots\ldots (1)$$

$$f(x) + f(y) = (3x + 2) + (3y + 2) = 3x + 3y + 4 \ldots\ldots (2)$$

$$\Rightarrow (1) \neq (2)$$

$$\Rightarrow f(x + y) \neq f(x) + f(y)$$

$\therefore f$ is not a homomorphism map.

Example 4.4: Let $f : (Z, +) \to (\{1, -1\}, .)$, such that $f(a) = \begin{cases} 1 & if\ a\ is\ even \\ -1 & if\ a\ is\ odd \end{cases}, \ \forall a \in Z$. Is f a homomorphism map.?

Solution:

To Prove $f(a + b) = f(a).f(b)$

Let $a, b \in Z \Rightarrow a, b \in E \ \ or \ \ a, b \in O \ \ or \ \ a \in E \wedge b \in O$

(1) If $a, b \in E \Rightarrow$ a + b ∈ E

$$f(a + b) = 1 = 1 \ . \ 1 = f(a).f(b)$$

(2) If $a, b \in O \Rightarrow a + b \in E$

$f(a + b) = 1 = -1.-1 = f(a).f(b)$

(3) If $a \in E \wedge b \in O \Rightarrow a + b \in O$

$f(a + b) = -1 = 1.-1 = f(a).f(b)$

In all cases $f(a + b) = f(a).f(b)$

$\therefore f$ is a homomorphism map.

Example 4.5: Let $g : (S_3, \circ) \to (S_3, \circ)$, such that $g(x) = x, \ \forall x \in S_3$.
Is g a homomorphism map.? **(H.W.)**

Example 4.6: Let $f : (Z_6, +_6) \to (Z_6, +_6)$, such that $f(\bar{x}) = \bar{x}, \ \forall \bar{x} \in Z_6$.
Is f a homomorphism map.? **(H.W.)**

Example 4.7: Let $f : (G, *) \to (G, *)$, such that $f(a) = x * a * x^{-1}, \forall a \in G$.
Is f a homomorphism map.?

Solution:

Let $a, b \in G$

$f(a * b) = x * (a * b) * x^{-1}$ ..... (1)

$f(a) * f(b) = (x * a * x^{-1}) * (x * b * x^{-1})$

$= x * a * (x^{-1} * x) * b * x^{-1}$

$= x * (a * b) * x^{-1}$ ..... (2)

$\Rightarrow (1) = (2)$,

$\therefore f$ is a homomorphism map.

Example 4.8: Let $f : (G, *) \to (G', \circ)$, such that $f(a) = e', \ \forall a \in G$.
Is f a homomorphism map.?

Solution:

Let $a, b \in G$

$\Rightarrow f(a * b) = e'$ ..... (1)

And $f(a) \circ f(b) = e' \circ e' = e'$ ..... (2)

$\Rightarrow (1) = (2)$.

Then f is called a trivial homomorphism map.

Example 4.9: Let $H \Delta G$ and $f : (G,*) \to (\frac{G}{H}, \otimes)$, such that $f(a) = a * H, \ \forall a \in G$. Is f a homomorphism map.?

Solution:

Let $a, b \in G$

$$\Rightarrow f(a * b) = (a * b) * H \quad \ldots\ldots (1)$$

And $f(a) \otimes f(b) = (a * H) \otimes (b * H) = (a * b) * H \quad \ldots\ldots (2)$

$\Rightarrow (1) = (2)$

$\therefore f$ is a homomorphism map.

Definition 4.10: Let $(G,*)$ and $(G',\circ)$ be two groups and $f : (G,*) \to (G',\circ)$ be a mapping, then

(1) f is called a monomorphism (mono.) iff f is a homomorphism and (1-1).

(2) f is called an epimorphism (epi.) iff f is a homomorphism and (onto) map.

(3) f is called an isomorphism (iso.) iff f is a homomorphism, (1-1) and (onto).

Definition 4.11: Any two groups $(G,*)$ and $(G',\circ)$ are called isomorphic iff there exist an isomorphism map between them and denoted by $G \cong G'$.

(i.e.) $G \cong G' \Leftrightarrow \exists\, f : (G,*) \to (G',\circ)$ and f is an isomorphism.

Example 4.12: Let $(G = \{2^x : x \in Z\}, .)$, show that $(Z, +) \cong (G, .)$.

Solution:

Define $f : (Z, +) \to (G, .)$ such that $f(x) = 2^x, \ \forall x \in Z$

homo.?

Let $x, y \in Z$, then

$f(x + y) = 2^{x+y} = 2^x . 2^y = f(x) . f(y).$

$\therefore f$ is homo.

(1-1) ?

Let $f(x) = f(y)$. To prove $x = y$

$f(x) = f(y) \Rightarrow 2^x = 2^y \Longrightarrow x = y \Longrightarrow f$ is (1-1)

(onto)?

$R_f = \{f(x): x \in Z\} = \{2^x: x \in Z\} = G$

$\therefore f$ is (onto)

$\therefore f$ is an isomo.

So, $(Z,+) \cong (G,.)$.

Theorem 4.13: The relation "isomorphic" is an equivalent relation.

Proof:

Reflective ? To prove $(G,*) \cong (G,*)$

Since $\exists\ i : (G,*) \to (G,*)\ \ni\ i(x) = x\ \ \forall x \in G$

And i is homo., (1-1), onto.

$\therefore i$ is isomo. $\Longrightarrow (G,*) \cong (G,*)$.

Symmetric ? Let $(G,*) \cong (G',.)$, To prove $(G',.) \cong (G,*)$

Since $(G,*) \cong (G',.) \Longrightarrow \exists\ f : (G,*) \to (G',.)\ \ \ni f\ is\ isomo.$

$f\ is\ bij. \Longrightarrow \exists\ f^{-1}: (G',.) \to (G,*)$

Since $f\ is$ (1-1) and onto $\Longrightarrow f^{-1}\ is$ (1-1) and onto

To prove f^{-1} is homo.

Let $a, b \in G'\ \wedge f$ is onto $\Longrightarrow \exists x, y \in G$ s.t. $f(x) = a\ , f(y) = b$

$f^{-1}(a.b) = f^{-1}\big(f(x).f(y)\big)$

$= f^{-1}\big(f(x*y)\big)$

$= x * y$

$= f^{-1}(a) * f^{-1}(b)$

$\therefore f^{-1}$ is homo. $\Longrightarrow f^{-1}$ is isomo. $\Longrightarrow (G',.) \cong (G,*)$.

Transitive ? Let $(G,*) \cong (G',.) \wedge (G',.) \cong (G'',\odot)$,

To prove $(G,*) \cong (G'',\odot)$

Since $G \cong G' \Longrightarrow \exists\ f : (G,*) \to (G',.)\ \ \ni f\ is\ isomo.$

$G' \cong G'' \Longrightarrow \exists\ g : (G',.) \to (G'',\odot)\ \ \ni g\ is\ isomo.$

$\Longrightarrow \exists\ g \circ f: (G,*) \to (G'',\odot)$

Since f, g are bij. $\Longrightarrow g \circ f$ is bij.

To prove $g \circ f$ is homo.

Let , $b \in G$, then

$(g \circ f)(a * b) = g[f(a * b)]$

$= g[f(a).f(b)]$
$= g(f(a)) \odot g(f(b))$
$= (g \circ f)(a) \odot (g \circ f)(b)$

$\therefore$ $g \circ f$ is homo. $\Longrightarrow$ $g \circ f$ is isomo. $\Longrightarrow G \cong G^{"}$

$\therefore$ $\cong$ is an equivalent relation.

Theorem 4.14: Let $f : (G,*) \to (G',.)$ be an isomorphism map. Then

(1) $f(e) = e'$, such that e is an identity of G and e' is an identity of G'.

(2) $f(a^{-1}) = (f(a))^{-1}$, $\forall a \in G$.

(3) If $(H, *)$ is a subgroup of a group $(G, *)$, then $(f(H), .)$ is a subgroup of a group $(G', .)$.

(4) If $(K, .)$ is a subgroup of a group $(G', .)$, then $(f^{-1}(K), *)$ is a subgroup of a group $(G, *)$.

(5) If $H \Delta G$ and f is onto , then $f(H) \Delta G'$.

(6) If $K \Delta G'$, then $f^{-1}(K) \Delta G$.

Proof.

(1): $f(e) = e'$, such that e is an identity of G and e' is an identity of G'.

Proof:

Let $a \in G \Rightarrow a * e = a$ (Def. of idenitity)

$\Rightarrow f(a * e) = f(a)$ (f is map)

$\Rightarrow f(a).f(e) = f(a)$ (f is homo.).....(1)

Let $f(a) \in G'$

$\Rightarrow f(a).e' = f(a)$ (Def. of identity).....(2)

$(1) = (2)$, then

$f(a).f(e) = f(a).e'$

$\therefore f(e) = e'$ (By cancellation law).

(2): $f(a^{-1}) = (f(a))^{-1}$, $\forall a \in G$.

Proof:

Let $a \in G \Rightarrow a * a^{-1} = e$ (Def. of inverse)

$\Rightarrow f(a * a^{-1}) = f(e) = e'$

$\Rightarrow f(a).f(a^{-1}) = f(e) = e'$ ... ... (1)

Let $f(a) \in G'$

$\Rightarrow f(a).(f(a))^{-1} = e'$ ... ... (2) (Def. of inverse)

$\Rightarrow (1) = (2)$, then

$f(a).f(a^{-1}) = f(a).\big(f(a)\big)^{-1}$

$\therefore f(a^{-1}) = (f(a))^{-1}$ (By cancellation law).

(3) If $(H, *)$ is a subgroup of a group $(G, *)$, then $(f(H), .)$ is a subgroup of a group $(G', .)$.

Proof:

$f(H) = \{f(x): x \in H\} \subseteq G'$

$f(e) = e' \in f(H) \Rightarrow f(H) \neq \varphi$

Let $f(x), f(y) \in f(H)$. To prove $f(x).(f(y))^{-1} \in f(H)$

$f(x).f(y)^{-1} = f(x).f(y^{-1})$ (by (2))

$= f(x * y^{-1})$ (f is homo.)

$since(H,*)$ is subgroup, then $x * y^{-1} \in H \Rightarrow f(x * y^{-1}) \in f(H)$

So, $f(x).f(y)^{-1} \in f(H)$

$\therefore (f(H),.)$ is a subgroup of a group $(G',.)$

(4) If $(K, .)$ is a subgroup of a group $(G', .)$, then $(f^{-1}(K), *)$ is a subgroup of a group $(G, *)$.

Proof.

$f^{-1}(K) = \{x \in G: f(x) \in K\} \subseteq G$

Since $(K,.)$ is a subgroup of a group G'

$\Rightarrow e' = f(e) \in K \Rightarrow e \in f^{-1}(K)$. So, $f^{-1}(K) \neq \varphi$

Let $x, y \in f^{-1}(K)$. To prove $x * y^{-1} \in f^{-1}(K)$

$x \in f^{-1}(K) \Rightarrow f(x) \in K$

$y \in f^{-1}(K) \Rightarrow f(y) \in K$

Since $(K,.)$is a subgroup of a group G'

$\Rightarrow f(x).f(y)^{-1} \in K$

$\Rightarrow f(x).f(y^{-1}) \in K$

$\Rightarrow f(x * y^{-1}) \in K \Rightarrow x * y^{-1} \in f^{-1}(K)$

$\therefore (f^{-1}(K),*)$ is a subgroup of a group $(G,*)$.

(5) If $H \Delta G$ and f is onto, then $f(H) \Delta G'$.

Proof:

Suppose that $H \Delta G$ and f is onto, To Prove $f(H) \Delta G'$

By (3), $(f(H),.)$ is a subgroup of a group $(G',.)$.

Let $y \in G' \wedge a \in f(H)$, To prove $y.a.y^{-1} \in f(H)$

$y \in G'$ and f is onto, then $\exists\, x \in G \;\; s.t. \; f(x) = y$

$a \in f(H)$, then $a = f(h) \;\; s.t. \; h \in H.$

$$y.a.y^{-1} = f(x).f(h).f(x)^{-1} = f(x).f(h).f(x^{-1}) = f(x * h * x^{-1})$$

Since $H \,\Delta\, G$, then $x * h * x^{-1} \in H.$

It follows that $f(x * h * x^{-1}) \in f(H)$

$\therefore y.a.y^{-1} \in f(H) \Rightarrow f(H) \,\Delta\, G'.$

(6) If $K \,\Delta\, G'$, then $f^{-1}(K) \,\Delta\, G$.

Proof:

Suppose that $K \,\Delta\, G'$, To prove $f^{-1}(K) \,\Delta\, G$

By (4), $(f^{-1}(K),*)$ is a subgroup of a group $(G,*)$.

Let $x \in G \wedge a \in f^{-1}(K)$, To prove $x * a * x^{-1} \in f^{-1}(K)$

$x \in G \Rightarrow f(x) \in G'$

$a \in f^{-1}(K) \Rightarrow f(a) \in K$.

$f(x) \in G' \wedge f(a) \in K$ and $K \,\Delta\, G'$

$\Longrightarrow f(x).f(a).f(x)^{-1} \in K$

$\Longrightarrow f(x).f(a).f(x^{-1}) \in K$

$\Longrightarrow f(x * a * x^{-1}) \in K$

$\Longrightarrow x * a * x^{-1} \in f^{-1}(K)$

$\therefore f^{-1}(K) \,\Delta\, G$

Theorem 4.15. Prove that

(1) Every two finite cyclic groups of the same order are isomorphic.

(2) Every finite cyclic group is isomorphic to $(Z_n, +_n)$.

(3) Every two infinite cyclic groups are isomorphic.

(4) Every infinite cyclic group is isomorphic to $(Z, +)$.

Proof (1):

Let $(G, *), (G', .)$ be two finite cyclic groups such that $o(G) = o(G') = n$

To prove, $(G,*) \cong (G', .)$

G is cyclic

$\Rightarrow \exists\ a \in G\ \ni\ G = < a > = \{ a^k : k \in Z\} = \{a^1, a^2, \dots, a^n = e\}$

and

G' is cyclic $\Rightarrow \exists\ b \in G' \ni\ G' = < b > = \{ b^k : k \in Z\} = \{b^1, b^2, \dots, b^n = e\}$

Define $f : (G,*) \to (G', .)\ \ni f(a^k) = b^k\ ,\ \forall\ k \in Z,\ a \in G$

Is f mapping?

Let $a^r = a^s$ To prove $f(a^r) = f(a^s)$

$a^r = a^s \ \Rightarrow\ r \equiv_n s\ (mode\ n)$

$$\Rightarrow r - s = ng \quad \ni g \in Z$$
$$\Rightarrow r = ng + s$$
$$\Rightarrow b^r = b^{ng+s} = (b^n)^g . b^s$$
$$\Rightarrow b^r = b^s$$
$$\Rightarrow f(a^r) = f(a^s)$$

So, f is mapping.

Is f (1-1) ?

Let $f(a^r) = f(a^s)$ To prove $a^r = a^s$

$f(a^r) = f(a^s) \Rightarrow b^r = b^s \Rightarrow\ r \equiv_n s$ (G is finite)

$$\Rightarrow r - s = ng$$
$$\Rightarrow r = ng + s$$
$$\Rightarrow a^r = (a^n)^g * a^s$$
$$\Rightarrow a^r = a^s$$

So, f is 1-1

Is f onto ?

$R_f = \{ f(a^k) : \forall\ k \in\ Z\} = \{b^k : \forall\ k \in\ Z\} = G'$

So, f is onto

Is f homo. ?

$f(a^r * a^s) = f(a^{r+s}) = b^{r+s} = b^r . b^s = f(a^r) . f(a^s)$

so, f is homo.

Thus, f is isomo and $(G,*) \cong (G', .)$.

(2) Every finite cyclic group is isomorphic to $(Z_n, +_n)$.

Proof:

Let $(G,*)$ be a finite cyclic group such that $o(G) = m$

$$G = < a >= \{a^1, a^2, \dots, a^m = e\}$$

(1) If $m > n \Rightarrow o(G) > o(Z_n) \Rightarrow f$ is not (1-1) $\Rightarrow (G,*) \ncong (Z_n, +_n)$.
(2) If $m < n \Rightarrow o(G) < o(Z_n) \Rightarrow f$ is not onto $\Rightarrow (G,*) \ncong (Z_n, +_n)$.
(3) If $m = n \Rightarrow o(G) = o(Z_n)$ To prove $(G,*) \cong (Z_n, +_n)$.
Define $f: (G,*) \to (Z_n, +_n) \ni f(a^k) = [k], \ \forall \ k \in Z^+, a \in G$

Is f mapping?

Let $a^r = a^s$ To prove $f(a^r) = f(a^s)$
$a^r = a^s \ \Rightarrow \ r \equiv_n s \Rightarrow [r] = [s]$

$$\Rightarrow f(a^r) = f(a^s)$$

So, f is mapping.

Is f (1-1) ?

Let $f(a^r) = f(a^s)$ To prove $a^r = a^s$
$f(a^r) = f(a^s) \ \Rightarrow [r] = [s] \Rightarrow \ r \equiv_n s$ (G is finite)

$$\Rightarrow r - s = ng$$
$$\Rightarrow r = ng + s$$
$$\Rightarrow a^r = (a^n)^g * a^s$$
$$\Rightarrow a^r = a^s$$

So, f is 1-1

Is f onto ?

$R_f = \{ f(a^k): \forall \ k \in \ Z\} = \{[k]: \forall \ k \in \ Z\} = Z_n$

So, f is onto

Is f homo. ?

$f(a^r * a^s) = f(a^{r+s}) = [r + s] = [r] +_n [s] = f(a^r) +_n f(a^s)$
so, f is homo.
Thus, f is isomo and $(G,*) \cong (Z_n, +_n)$.

(3) Every two infinite cyclic groups are isomorphic.

Proof:

Let $(G,*)$ and $(G',.)$be two infinite cyclic groups, then
$G = < a >= \{\dots, a^{-2}, a^{-1}, a^0, a^1, a^2, \dots\}$
$G' = < b >= \{\dots, b^{-2}, b^{-1}, b^0, b^1, b^2, \dots\}$

To prove $(G,*) \cong (G',.)$

Define $f:(G,*) \to (G',.) \ \ni f(a^k) = b^k \ , \ \forall k \in Z, a \in G$

Is f map.? , Is f (1-1) ? , Is f onto ? , Is f homo. ? (H.W.)

(4) Every infinite cyclic group is isomorphic to $(Z,+)$.

Proof:

Let $(G,*)$ be an infinite cyclic group, then

$$G =< a >= \{\dots, a^{-2}, a^{-1}, a^0, a^1, a^2, \dots\}$$

$$Z = \{\dots, -2, -1, 0, 1, 2, \dots\}$$

To prove $(G,*) \cong (Z,+)$

Define $f : (G,*) \to (Z,+) \ \ni f(a^k) = K \ , \ \forall \ k \in Z, a \in G$

Is f map.? , Is f (1-1) ? , Is f onto ? , Is f homo. ? (H.W.)

Definition 4.16: Let $(G, *)$ be a group, then

(1) The Homomorphism of G, denoted by Hom(G) and define as:
$Hom(G) = \{f \ ; \ f : (G, *) \to (G, *) \ \ni f \ is \ homo.\}$ تشاكل

(2) The Automorphism of G, denoted by Aut(G) and define as:
$Aut(G) = \{f \ ; \ f : (G, *) \to (G, *) \ \ni f \ is \ isomo.\}$ تشاكل تقابلي

Theorem 4.17: Let $(G, *)$ be a group, then

(1) $(Hom(G), \circ)$ is semigroup with identity.

(2) $(Aut(G), \circ)$ is a group **(H.W.)**

(3) $(Aut(G), \circ)$ is a subgroup of $(symm(G),\circ)$.

Proof: (1) $Hom(G) = \{f \ ; \ f : (G,*) \to (G,*) \ \ni f \ is \ homo.\}$

$\exists \ i : (G,*) \to (G,*) \ \ni \ i(x) = x \ \ \forall \ x \in G$, and i is homo.

$\therefore \ Hom(G) \neq \varphi.$

Closure: let $f, g \in Hom(G)$ To prove $f \circ g \in Hom(G)$

Since $f, g \in Hom(G) \Rightarrow \exists \ f : (G,*) \to (G,*) \ \ni f \ is \ homo.$ and

$$\exists \ g : (G,*) \to (G,*) \ \ni g \ is \ homo.$$

So, $f \circ g : (G,*) \to (G,*) \ \ is \ homo.$

$\therefore f \circ g \in Hom(G)$

Asso. Is true since $(f \circ g) \circ h = f \circ (g \circ h)$

Identity: $\exists\ i \in Hom(G)$ and $f \circ i = i \circ f = f \quad \forall\ f \in Hom(G)$

It follows that $(Hom(G),\ \circ)$ is semigroup with identity.

(3) To Prove $(Aut(G),\circ)$ is a subgroup of $(symm(G),\circ)$.

Proof:

$Aut(G) = \{f\ ;\ f : (G,*) \to (G,*)\ \ni f\ is\ isomo.\}$

$Symm(G) = \{f\ ; f : (G,*) \to (G,*)\ \ni f\ is\ bij.\}$

Since $\exists\ i : (G,*) \to (G,*)\ \ni\ i(x) = x\ \ \forall\ x \in G$, and i is $isomo$.

$\therefore Aut(G) \neq \varphi\ ,\ Aut(G) \subseteq Symm(G)$ and $(Aut(G),\ \circ)$ is a subgroup.

$\therefore (Aut(G),\ \circ)$ is a subgroup of $(symm(G),\ \circ)$.

Definition 4.18: Let $(G,\ *)$ be a group and $\in G$.

Define $f_x : (G,*) \to (G,*)\ \ni f_x(a) = x * a * x^{-1}\ \ \forall\ a \in G.$

Then f_x is called an inner automorphism of G and the set

$Inn(G) = \{\ f_x : \forall x \in G\}$ or $I(G) = \{\ f_x : \forall x \in G\}$ تشاكل تقابلي داخلي ( )

Theorem 4.19: Let $(G,\ *)$ be a group and $x \in G$, then

(1) f_x is an isomorphism map.

(2) $(I(G),\ \circ)$ is a subgroup of $(Aut(G),\circ)$

(3) $I(G)\ \Delta\ Aut(G)$.

Proof:

(1) $f_x : (G,*) \to (G,*)\ \ni f_x(a) = x * a * x^{-1}\ \ \forall\ a \in G$

To preove f_x is (1-1), onto and homo.

Let $f_x(a) = f_x(b),\ \ \forall\ a, b \in G$, then

$x * a * x^{-1} = x * b * x^{-1} \quad \Rightarrow a = b$

So, f_x is (1-1)

$R_{f_x} = \{\ f_x(a) : \forall\ a \in\ G\} = \{x * a * x^{-1} : \forall\ a \in\ G\} = G$

So, f_x is onto

$f_x(a) * f_x(b) = (x * a * x^{-1}) * (x * b * x^{-1})$

$$= x * a * (x^{-1} * x) * b * x^{-1}$$
$$= x * a * b * x^{-1} = f_x(a * b)$$

So, f_x is homo.

Thus, f_x is an isomo. map.

(2) $(I(G),\ \circ)$ is a subgroup of $(Aut(G),\ \circ)$

Proof:

To prove $(I(G),\ \circ)$ is a subgroup of $(Aut(G),\ \circ)$

$$I(G) = \{f_x\ ;\ f_x : (G,*) \to (G,*)\ \ni f_x \quad is\ an\ isomo.\}$$

$$Aut(G) = \{f\ ; f : (G,*) \to (G,*)\ \ni f\ is\ an\ isomo.\}$$

Since $e \in G \Rightarrow\ f_e \in I(G) \neq \varphi$

$$f_e(a) = e * a * e^{-1} = a$$

$\therefore I(G) \subseteq Aut(G)$

Closure: Let $f_x\ ,\ f_y \in I(G)$, To prove $f_x \circ f_y \in I(G)$

$$(f_x \circ f_y)(a) = f_x\left(f_y(a)\right) = f_x(y * a * y^{-1})$$

$$= x * (y * a * y^{-1}) * x^{-1}$$
$$= (x * y) * a * (x * y)^{-1}$$
$$= f_{x*y}(a)\ \in I(G)$$

Inverse: Let $f_x \in I(G)$

Since $x^{-1} \in G \Rightarrow\ f_{x^{-1}} \in I(G)$

$$f_x \circ f_{x^{-1}} = f_{x*x^{-1}} = f_e \Rightarrow f_{x^{-1}} \circ f_x = f_{x^{-1}*x} = f_e$$

$\therefore (f_x)^{-1} = f_{x^{-1}}$

So, $(I(G),\circ)$ is a subgroup of $(Aut(G),\circ)$.

(3) $I(G)\ \Delta\ Aut(G)$.

Proof:

We have $(I(G),\circ)$ is a subgroup of $(Aut(G),\circ)$ and

$Aut(G) = \{g\ ; g : (G,*) \to (G,*)\ \ni g\ is\ an\ isomo.\}$,

$I(G) = \{f_x\ ; f_x : (G,\ *) \to (G,\ *) \quad is\ an\ isomo.\}$.

Let $g \in Aut(G),\ f_x \in I(G)$ To prove $g \circ f_x \circ g^{-1} \in I(G)$

$$(g \circ f_x \circ g^{-1})(a) = g \circ f_x\left(g^{-1}(a)\right)$$

$$= g[\,f_x\left(g^{-1}(a)\right)]$$
$$= g(x * g^{-1}(a) * x^{-1})$$
$$= g(x) * a * g(x^{-1})$$
$$= f_{g(x)}(a)\ \in I(G).\ \text{So, } I(G)\ \Delta\ Aut(G).$$

Definition 4.20: Let $f:(G,\ *)\to(G',\ .)$ be a homomorphism, then the **kernel** of f is denoted by $kerf$ and defined as:

$$kerf=\{x\in G\mid f(x)=e'\}.$$

Example 4.21: Find $kerf$ for the following mappings:

(1) $f:(R,+)\to(R^+,.)\quad \ni f(x)=3^x$

Solution: f is homo. (Check)

$\Rightarrow kerf$ exist

$kerf=\{x\in R: f(x)=1\}=\{x\in R: 3^x=1\}=\{0\}.$

(2) $f:(G,*)\to(G',.)\ \ni f$ **is a trivial homo.**

Solution: $f(x)=e'\quad \forall\ x\in G$

Since f is homo., then $kerf$ is exist

$kerf=\{x\in G\mid f(x)=e'\}=G.$

(3) $f:(Z,+)\to(Z_3,+_3)\quad \ni f(x)=\bar{x}\ \forall\ x\in Z$

Solution: f is homo. (Check)

$$kerf=\{x\in Z:\ f(x)=\bar{0}\}=\{x\in Z:\ \bar{x}=\bar{0}\}$$

$$=\{x\in Z:\ x\equiv_3 0\ (mode3)\}$$
$$=\{x\in Z:\ x=0+3k\ \forall\ k\in Z\}$$
$$=\{0,\pm3,\pm6,\dots\}\subseteq Z.$$

Theorem 4.22: Let $f:(G,\ *)\to(G',\ .)$ be a homomorphism, then

(1) $(kerf,\ *)$ is a subgroup of $(G,\ *)$

(2) $kerf\ \Delta\ G$

(3) $kerf=\{e\}$ iff f is (1-1).

Proof: (1) $kerf=\{x\in G\mid f(x)=e'\}\subseteq G$

Since $f(e)=e'\Rightarrow e\in kerf\neq\varphi$

Let $a,b\in kerf$ To prove $a*b^{-1}\in kerf$ (i.e., To prove $f(a*b^{-1})=e'$)

$$f(a*b^{-1})=f(a).f(b^{-1})$$
$$=f(a).\left(f(b)\right)^{-1}$$
$$=e'.(e')^{-1}=e'$$

$\therefore\ f(a*b^{-1})=e'\Rightarrow\ a*b^{-1}\in kerf$

So, $(kerf,\ *)$ is a subgroup of $(G,\ *)$.

(2) $kerf \ \Delta \ G$

Proof:

To prove $kerf \ \Delta \ G$

By (1), $(kerf, *)$ is a subgroup of $(G, *)$

Let $x \in G$ and $a \in kerf$ To prove $x * a * x^{-1} \in kerf$

(i.e.) To prove $f(x * a * x^{-1}) = e'$

$$f(x * a * x^{-1}) = f(x).f(a).f(x^{-1})$$

$$= f(x).e'.\left(f(x)\right)^{-1}$$

$$= e'$$

So, $x * a * x^{-1} \in kerf$

Thus, $kerf \ \Delta \ G$.

(3) $kerf = \{e\}$ iff f is (1-1).

Proof:

($\Rightarrow$) $Suppose \ kerf = \{e\}$ To prove f is (1-1)

Let $f(a) = f(b) \Rightarrow f(a).\left(f(b)\right)^{-1} = e'$

$$\Rightarrow f(a).f(b^{-1}) = e'$$

$$\Rightarrow f(a * b^{-1}) = e' \quad \text{(since } f \text{ is a homo.)}$$

$$\Rightarrow a * b^{-1} \in kerf$$

Since $kerf = \{e\} \Rightarrow a * b^{-1} = e \Rightarrow a = b$

So, f is (1-1)

($\Leftarrow$) Suppose f is (1-1) To prove $kerf = \{e\}$

Let $a \in kerf$ To prove $a = e$

Since f is (1-1) and $f(a) = f(e) \Rightarrow a = e$

then, $kerf = \{e\}$.

The first fundamental theorem of isomorphism 4.23:

(النظرية الأساسية الأولى للتشاكل)

Let $f:(G,\ *)\to(G',\ .)$ be an onto and homomorphism mapping, then

$$\left(\frac{G}{kerf},\otimes\right)\cong(G',.)\ .$$

Proof:

Since f is onto $\Rightarrow R_f=\{\,f(a):a\in G\}=G'$

Since $kerf\ \Delta\ G\Rightarrow\left(\frac{G}{kerf},\otimes\right)$ is a group.

Define $g:\left(\frac{G}{kerf},\otimes\right)\to(G',.)\ ;\ g(a*kerf)=f(a)\ ,\ \forall a\in G$

To prove g is map., (1-1), onto and homo.

T.P. g is map. ?

Let $a*kerf=b*kerf\Rightarrow a^{-1}*b\in kerf$

$$\Rightarrow f(a^{-1}*b)=e'$$
$$\Rightarrow f(a^{-1}).f(b)=e'$$
$$\Rightarrow (f(a))^{-1}.f(b)=e'$$
$$\Rightarrow f(b)=f(a)$$
$$\Rightarrow g(b*kerf)=g(a*kerf)$$

So, g is map.

T.P. g is 1-1 ?

Let $g(a*kerf)=g(b*kerf)\Rightarrow f(a)=f(b)$

$$\Rightarrow e'=(f(a))^{-1}.f(b)$$
$$\Rightarrow e'=f(a^{-1}).f(b)$$
$$\Rightarrow e'=f(a^{-1}*b)$$
$$\Rightarrow a^{-1}*b\in kerf$$
$$\Rightarrow a*kerf=b*kerf$$

So, g is 1-1

T.P. g is onto ?

$R_g=\{\ g(a*kerf):a\in G\}=\{f(a):a\in G\}=G'$

So, g is onto

g is homo. ?

$g[(a*kerf)\otimes(b*kerf)]=g[(a*b)*kerf]$

$$= f(a * b)$$
$$= f(a).f(b)$$
$$= g(a * kerf).g(b * kerf)$$

So, g is homo.

Thus, g is isomo.

Hence, $\left(\frac{G}{kerf}, \otimes\right) \cong (G', .)$.

Example 4.24: Let $f : (Z, +) \to (\{1, -1\}, .)$ such that

$$f(a) = \begin{Bmatrix} 1 & if\ a\ is\ even \\ -1 & if\ a\ is\ odd \end{Bmatrix}, \quad \forall a \in Z.$$

Show that $(Z_2, +_2) \cong (\{1, -1\}, .)$ by two ways.

Solution:

(1) Since $o(Z_2) = o(\{1, -1\}) = 2$ and $(Z_2, +_2), (\{1, -1\}, .)$ are cyclic groups. Then $(Z_2, +_2) \cong (\{1, -1\}, .)$

(2) By using the first fundamental theorem of isomo.

It is clear that f is homo.

$R_f = \{ f(a) : \ a \in Z\} = \{1, -1\} = Codf$

So, f is onto

Since f is homo. and onto, then by the first fundamental theorem of isomo. $\Rightarrow \left(\frac{Z}{kerf}, \otimes\right) \cong (\{1, -1\}, .)$

$kerf = \{a \in Z : f(a) = 1\} = E$

$\therefore \left(\frac{Z}{E}, \otimes\right) \cong (\{1, -1\}, .)$

$(Z, +)$ is cyclic group, then $\left(\frac{Z}{E}, \otimes\right)$ is cyclic.

We have, $o\left(\frac{Z}{E}\right) = 2 \Rightarrow (Z_2, +_2) \cong \left(\frac{Z}{E}, \otimes\right)$

$\therefore \ (Z_2, +_2) \cong (\{1, -1\}, .)$.

Corollary 4.25: Let $(G, *)$ be a group, then $\left(\frac{G}{cent(G)}, \otimes\right) \cong (I(G), \circ)$.

Proof:

Define $g : (G, *) \to (I(G), \circ) \ni g(x) = f_x \quad \forall x \in G$

$I(G) = \{ f_x : x \in G\}$

T.P. g is map. ?

Let $x = y \Rightarrow x * a = y * a \Rightarrow x * a * x^{-1} = y * a * y^{-1}$

$\Rightarrow f_x(a) = f_y(a)$

$\Rightarrow g(x) = g(y)$. So, g is map.

T.P. g is onto ?

$R_g = \{g(x) : x \in G\} = \{f_x : \forall x \in G\} = I(G)$

So, g is onto

T.P. g is homo. ?

$g(x * y) = f_{x*y} = f_x \circ f_y = g(x) \circ g(y)$

$\therefore$ g is homo.

By the first fundamental theorem of isomo. $\Rightarrow \left(\frac{G}{kerg}, \otimes\right) \cong (I(G), \circ)$.

$kerg = \{x \in G : g(x) = f_e\} = \{x \in G : f_x(a) = f_e(a) \quad \forall a \in G\}$

$= \{x \in G : x * a * x^{-1} = a \quad \forall a \in G\}$

$= \{x \in G : x * a = a * x \quad \forall a \in G\}$

$= cent(G)$

$\therefore \left(\frac{G}{cent(G)}, \otimes\right) \cong (I(G), \circ)$.

The second fundamental theorem of isomorphism 4.26:

(النظرية الأساسية الثانية للتشاكل)

Let $(H, *)$ and $(K, *)$ be two subgroups of $(G, *)$ such that , $(H * K, *)$ is subgroup of $(G, *)$, $K \Delta (H * K)$ and $(H \cap K) \Delta H$. Then

$$\left(\frac{H*K}{K}, \otimes\right) \cong \left(\frac{H}{H \cap K}, \otimes\right).$$

Proof:

Since $K \Delta (H * K)$, then $\left(\frac{H*K}{K}, \otimes\right)$ is a group.

And since $(H \cap K) \Delta H$, then $\left(\frac{H}{H \cap K}, \otimes\right)$ is a group.

Define $f:(H*K,*)\to\left(\frac{H}{H\cap K},\otimes\right)$ such that

$$f(a*b)=a*(H\cap K)\qquad \forall\, a\in H, b\in K$$

f is map.?

Let $a*b=c*d$ such that $a,c\in H, b,d\in K$

$\Rightarrow c^{-1}*a=d*b^{-1}$

$\Rightarrow c^{-1}*a\in H\ \wedge\ c^{-1}*a\in K$

$\Rightarrow c^{-1}*a\in H\cap K$

$\Rightarrow c*(H\cap K)=a*(H\cap K)$

$\Rightarrow f(c*d)=f(a*b)$

$\therefore$ f is map.

f is onto ?

$$R_f=\{f(a*b):\ \forall a\in H\}=\{a*(H\cap K):\forall a\in H\}=\frac{H}{H\cap K}$$

$\therefore$ f is onto

f is homo. ?

$$f[(a*b)*(c*d)]=f[(a*(c*c^{-1})*b)*(c*d)]$$
$$=f[(a*c)*(c^{-1}*b*c)*d]$$

Since $c\in G\ \wedge\ b\in K\ \wedge\ K\Delta G$, then $(c^{-1}*b*c)\in K$

Let $(c^{-1}*b*c)=r\in K$

$\therefore f[(a*b)*(c*d)]=f[(a*c)*(r*d)]$

$=(a*c)*(H\cap K)$

$=[a*(H\cap K)]\otimes[c*(H\cap K)]$

$=f(a*b)\otimes f(c*d)$

$\therefore$ f is homo.

By the first fundamental theorem of isomo. $\Rightarrow\left(\frac{H*K}{kerf},\otimes\right)\cong\left(\frac{H}{H\cap K},\otimes\right)$.

$$kerf=\{a*b\in H*K: f(a*b)=H\cap K\}$$
$$=\{a*b\in H*K: a*H\cap K=H\cap K\}$$
$$=\{a*b\in H*K: a\in H\cap K\}$$
$$=\{a*b\in H*K: a\in H\ \wedge a\in K\}$$
$$=\{a*b\in H*K: a\in k\ \wedge b\in K\}=K$$

$\therefore$ $\left(\frac{H*K}{K},\otimes\right)\cong\left(\frac{H}{H\cap K},\otimes\right)$.

The third fundamentaltheorem of isomorphism 4.27:

(النظرية الأساسية الثالثة للتشاكل)

Let $(H,*)$ and $(K,*)$ be two normal subgroups of $(G,*)$ such that $H \subseteq K$, then

(1) $H \Delta K$,

(2) $\left(\frac{K}{H},\otimes\right) \Delta \left(\frac{G}{H},\otimes\right)$

(3) $\left(\frac{\frac{G}{H}}{\frac{K}{H}},\otimes\right) \cong \left(\frac{G}{K},\otimes\right)$

Proof:

(1) To prove $H \Delta K$

Since $(H,*)$ and $(K,*)$ are two subgroups and $H \subseteq K$

$\therefore (H,*)$ is a subgroup of $(K,*)$

Let $x \in K, a \in H$ To prove $x * a * x^{-1} \in H$

$x \in K \subseteq G \Rightarrow x \in G, a \in H$ and $H \Delta G \Rightarrow x * a * x^{-1} \in H$

$\therefore H \Delta K$

(2) $\left(\frac{K}{H},\otimes\right) \Delta \left(\frac{G}{H},\otimes\right)$

Since , then $\left(\frac{K}{H},\otimes\right)$ is a group.

And since $H \Delta G$, then $\left(\frac{G}{H},\otimes\right)$ is a group.

$$\frac{K}{H} = \{a * H : a \in K\} \subseteq \{a * H : a \in G\} = \frac{G}{H}$$

$\frac{K}{H} \subseteq \frac{G}{H} \Rightarrow \left(\frac{K}{H},\otimes\right)$ is a sub group of $\left(\frac{G}{H},\otimes\right)$

Let $x * H \in \frac{G}{H}$, $a * H \in \frac{K}{H}$

To Prove $(x * H) \otimes (a * H) \otimes (x * H)^{-1} \in \frac{K}{H}$

$$(x * H) \otimes (a * H) \otimes (x * H)^{-1} = ((x * a) * H) \otimes (x^{-1} * H)$$
$$= ((x * a * x^{-1}) * H)$$

$\therefore \ (x * a * x^{-1}) * H \in \frac{K}{H} \Rightarrow \left(\frac{K}{H},\otimes\right) \Delta \left(\frac{G}{H},\otimes\right)$.

(3) *T.P.* $\left(\frac{\frac{G}{H}}{\frac{K}{H}},\otimes\right) \cong \left(\frac{G}{K},\otimes\right)$

Since $\frac{K}{H} \Delta \frac{G}{H} \Rightarrow \left(\frac{\frac{G}{H}}{\frac{K}{H}},\otimes\right)$ is a group.

Since $K \Delta G \Rightarrow \left(\frac{G}{K},\otimes\right)$ is a group.

Define $f:\left(\frac{G}{H},\otimes\right)\longrightarrow\left(\frac{G}{K},\otimes\right)$ such that $f(a*H)=a*K \quad \forall a\in G$

f is map.?

Let $a*H=b*H$ To Prove $f(a*H)=f(b*H)$

$$a*H=b*H\Rightarrow a^{-1}*b\in H\subseteq K$$
$$\Rightarrow a^{-1}*b\in K$$
$$\Rightarrow a*K=b*K$$
$$\Rightarrow f(a*H)=f(b*H)$$

$\therefore$ f is map.

f is onto ?

$$R_f=\{\ f(a*H):a\in G\}=\{a*K:a\in G\}=\frac{G}{K}$$

$\therefore$ f is onto

f is homo. ?

$$f[(a*H)\otimes(b*H)]=f[(a*b)*H]$$
$$=(a*b)*K$$
$$=(a*K)\otimes(b*K)=f(a*H)\otimes f(b*H)$$

$\therefore$ f is homo.

By the first fundamental theorem of isomo.

$$\Rightarrow\left(\frac{\frac{G}{H}}{kerf},\otimes\right)\cong\left(\frac{G}{K},\otimes\right).$$

$$kerf=\left\{a*H\in\frac{G}{H}:f(a*H)=e'\right\}$$
$$=\{a*H\in\frac{G}{H}:a*K=K\}$$
$$=\{a*H\in\frac{G}{H}:a\in K\}$$
$$=\frac{K}{H}$$

$\therefore$ $\left(\frac{\frac{G}{H}}{\frac{K}{H}},\otimes\right)\cong\left(\frac{G}{K},\otimes\right).$