Group theory

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

4) مقدمة في الجبر المجرد الحديث

تاليف ديفيد بيرتون وترجمه عبد العالي جاسم

Chapter one

Binary Operations

Definition 1.1

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).

Example 1.2

1) The operations $\{+, -, \times\}$ are binary operations on R, Z, Q, C. But " $-$ " is not binary operation on N.

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

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

Example 1.3

Let $a * b = a + b + 2, \forall a, b \in Z^+$**.** Is $*$ abinary 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: $a, b, c, d \in A$ 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 1.4

Let$a * b = a^b, a, b \in Z$. Show that$*$is abinary operation on Z.

Solution:

1) Closure: if $a = 3$ and $b = -1$. Then $a * b = 3^{-1} = \frac{1}{3} \notin Z \Rightarrow *$ is not a binary operation on Z.

Remark 1.5: Some time we used the symbols $*, \circ, \#, \odot$, ... to denote abinary operation.

Exercises: 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) $a \# b = a + b - 3, \forall a, b \in N$.

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

Definition 1.7 (Associative)

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

(a $*$b) $*$c = a $*$(b $*$c) $\forall$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 $a * b = a + b - ab$, then $*$ is commutative and associative.

Solution:

(i) $a * b = a + b - ab = b + a - ba = b * a$

Which implies that $*$ is commutative.

(ii) Let $a, b, c \in R$, then

$$(a * b) * c = (a + b - ab) * c = (a + b - ab) + c - (a + b - ab)c$$

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

$$a * (b * c) = a * (b + c - bc)$$

$$= a + (b + c - bc) - a(b + c - bc)$$

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

$\Rightarrow$ (1)=(2)

$\Rightarrow *$ is an associative.

Exercises: which of the following binary operations is a comm., asso.?

(i) $a * b = a - b, \forall a, b \in Z.$

(ii) $a \odot b = 2ab, \forall a, b \in E.$

(iii) $a \# b = a^3 + b^3 \forall a, b \in R.$

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

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.

(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

i. $(Z,+),(E,+),(Q,+),(N,\times),(C,+)$ are commutative groups .

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

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

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

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

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

Example 1.20

Let $G=\{a,b,c,d\}$ be a set. Define a binary operation $*$ on G by the following table.

$*$	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 ….$\rightarrow$

$\Rightarrow*$ is asso.

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

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

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

(4) The inverse:

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

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

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

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

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

(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 abinary operation.

Is $(G, .)$ a group ?

Solution:

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

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

$\therefore$ (G , .) is a comm.group.

Example 1.22

Let G = Z , $a * b = a + b + 2$, show that (G , $*$) is a comm . group.

Solution:

1- Closure : let a, b $\in$Z , Then

$a * b = a + b + 2 \in Z \rightarrow$Closure is true

2- asso. Low : Let a, b, c $\in$Z , then

$a *(b * c) = a * (b + c + 2)$= a + (b + c + 2) + 2

= a + b + c + 4 ……..(1)

$(a * b) * c = (a + b + 2) * c$= (a + b + 2) + C + 2

= a + b + c + 4 …….(2)

$\therefore$ (1) = (2) $\Rightarrow *$ is asso .

3- Identity : let e $\in$**Z** $\ni$ $a * e = e * a = a$, then

$a * e = a + e + 2 = a \Longrightarrow e = -2$

$e * a = e + a + 2 = a \Longrightarrow e = -2$

$\therefore$ -2 is an identity element of G.

4- Inverse : let a , b $\in$ Z $\ni$ $a * b = b * a = e$

$a * b = a + b + 2 = -2 \Longrightarrow b = -a - 4$

$b * a = b + a + 2 = -2 \Longrightarrow b = -a - 4$

$\therefore a^{-1} = -(a+4) \in Z$

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

5- Comm. To prove $a * b = b * a \ \forall a, b \in Z$

$a * b = a + b + 2 = b + a + 2 = b * a$

$\therefore (G, *)$ is a comm. Group.

Example 1.25

Let (G , *) be an arbitrary group .The set of the function from G in to G with the composition (F_G, o) is forms a group , where

$F_G = \{ f_a : a \in G \}$, $f_a: G \to G$ s.t .

$f_a(x) = a * x$, $x \in G$, prove that

Proof : (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 FG, 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 a Comm . group, then (F_G, o) is a comm. group .

(Exercises): Determine the systems $(G , *)$ described abelian (comm..) group

1) $G= Z , a * b = a+b+3$
2) $G = R \times R = \{ (a, b) : a , b \in R\}$ s.t
   $(a, b) * (c,d) = (a+b, b+d + 2bd)$.
3) $(G = \{f_1 , f_2, f_3, f_4, f_5, f_6 \}, o)$, where
   $f_1(x) = x$, $f_2 (x) = \frac{1}{x}$, $f_3 (x) =1-x$, $f_4(x) = \frac{x-1}{x}$, $f_5(x) = \frac{x}{x-1}$, $f_6(x) = \frac{1}{1-x}$
4) $G = \{ (a,b) : a, b \in R , a \neq 0 , b \neq 0 \}$ s.t.
   $(a,b) * (c,d) = (ac,bd)$
5) $(G = \{ an : n \in z \} , +)$
6) $G = Q^+ , a * b = \frac{ab}{2}$.

Some properties of Groups:

Theorem (1) : If G is a group with a binary operation $*$, then the left and right cancellation laws hold in G , that is:

1) $a * b = a * c$ implies $b = c$
2) $b * a = c* a$ implies $b = c$

For all $a, b, c \in G$.

Proof :

1) suppose $a*b = a*c$

$\exists\ a^{-1} \in G$ s . t . $a^{-1} * (a * b) = a^{-1} * (a * c)$

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

$e * b = e * c$

$\therefore b = c$

2) H.W

Theorem(2): In a group (G , $*$), there is only one element e in G such that $e * a = a * e = a$, $\forall\, a \in G$.

Proof:

Suppose that G has two identity elements e and e' that mean $\forall a \in G$. Then

$a * e = e * a = a$ 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)

and

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

It follows that $e' = e$.

Theorem(3): 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(4): If (G , $*$) is group , then

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

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

Proof :

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

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

Proof :

$(\Longrightarrow)$ Let $(G, *)$ be a group and $(a * b)^{-1} = a^{-1} * b^{-1}$. To prove G is comm.

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

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

$= (b^{-1} * a^{-1})^{-1}$ $\quad$ (by Th.4)

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

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

$\therefore$ G is comm. gp.

$(\Longleftarrow)$ Let $(G, *)$ is a comm . gp. To prove $(a * b)^{-1} = a^{-1} * b^{-1}$

$(a * b)^{-1} = b^{-1} * a^{-1}$ (by Th.4)

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

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

proof :

Let $a = a^{-1}$ T. P. $a * b = b * a$, $\forall a, b \in G$

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

$= b^{-1} * a^{-1}$ (by Th.4)

$= b * a$

$\therefore$ G is a comm. Group.

The converse of this part is not true.

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

For example:

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

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

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

Give another example (H. W.)

Theorem (6): In a group (G , $*$) , the equations $a * x = b$ and $y * a = b$ have a unique solution.

Definition.(**The integral powers of *a***)

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

1- $a^n = \underbrace{a * a \ldots * a}_{n-times}$

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) 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:

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

Definition: ((The **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: (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.) $|a| = n$ if $a^n = e$, $n \in Z^+$

Example (1): (Z , +) is an infinite group

Example (2): the trivial group G = { 0 }

| G | = 1 , G is the only group of order 1.

Example (3): find the order of G and the order of each element of (G, .) . Such that G = { 1, -1 , i, -i}.

Ans.

| G | = 4 and

| *a* | : *a* = 1 , then | *a* | = | 1 | = 1 (since *e* = 1)

If *a* = -1, then | -1 | : $(-1)^2 = 1 \Longrightarrow$ | -1 | = 2

If *a* = i , then | i | : $i^2 = -1$, $i^4 = 1 \Longrightarrow$ | i | = 4

If *a* = -i , then |- i | : $-i^2 = -1$, $-i^3 = i$, $-i^4 = 1$

$\therefore$ | -i | = 4

((The group of integers modulo *n*))

Definition: Let *a* , *b* $\in$ Z , *n* $>$ 0 . Then *a* is congruent to *b* modulo *n* if *a* – *b* = *nk* , *k* $\in$ Z and denoted by *a* $\equiv$ *b* or *a* $\equiv$ *b* (mod *n*)

1- 17 $\equiv$ 5 (mod 6) , sine 17 – 5 = 12 = (6) (2)
2- 8 $\equiv$ 4 (mod 2) , since 8 – 4 = 4= (2) (2)
3- -12 $\equiv$3 (mod 3) , since -12 -3 = -15 = (3) (-5)
4- 5 $\not\equiv$ 2 (mod 2), since 5 – 2 = 3 $\neq$ (2)(*k*) , $\forall$ *k* $\in$ Z

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

Definition:

Let a $\in$ Z , n $>$ o . The congruence class of a module *n*, denoted by [a] is the set of all integers that are congruent to a module *n* .

(i.e.)

$[a] = \{ z \in Z : z \equiv a \pmod n \}$

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

Example(1):

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

$[0] = \{ z \in Z : z \equiv 0 \pmod 2 \}$

$= \{ z \in Z : z = 0 + 2K , K \in Z \}$

$= \{ 0 , \mp 2 , \mp 4 , \ldots\ldots\ldots \}$

$[1] = \{ z \in Z : z \equiv 1 \pmod 2 \}$

$= \{ z \in Z : z = 1 + 2k , k \in \}$

$= \{ \mp 1 , \mp 3 , \mp 5 , \ldots . \}$.

Example(2):

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

$[1] = \{ z \in Z : z \equiv 1 \pmod 3 \}$

$= \{ 1 , 1 \mp 3, 1 \mp 6 \ldots . \}$

$= \{ 1 , -2 , 4 , 7 , -5 , \ldots . \}$.

$[7]$ (H. W.)

Definition:

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

$Z_n = \{ [0] , [1] , [2] , \ldots\ldots , [n-1] \}$, or

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

Z_n has *n* elements.

Example:

$Z_1 = \{\bar{0}\}$

$Z_2 = \{ \bar{0}, \bar{1} \}$

$Z_3 = \{\bar{0}, \bar{1}, \bar{2}\}$

Now, we define addition on Z_n (write $+_n$) by the following : For any [a] , [b] $\in Z_n$ $[a] +_n [b] = [a +_n b]$

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

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

It is easy to see that $(Z_n , +_n)$ 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 .

Also, $(Z_n , ._n)$ is abelian semi group with identity [1] . It is called the multiplicative semi group of integers modulo n.

Example (1): $(Z_4, +_4)$

$Z_4 = \{ \bar{0} , \bar{1} , \bar{2} , \bar{3} \}$

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

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

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

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

Example (2): $(Z_4, \cdot_4)$

$\cdot_4$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
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. Since the number $\bar{1}$ is identity but the numbers $\bar{0}$ and $\bar{2}$ have no inverse. It follows that

$(Z_4, \cdot_4)$ is not a group, but it is semi group.

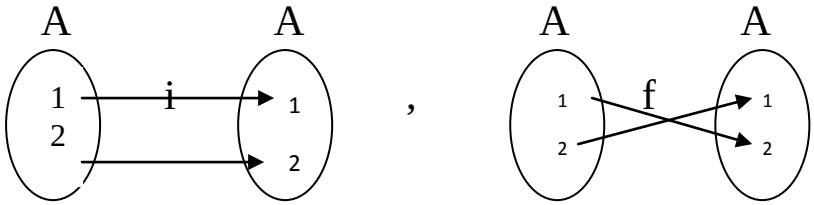
The Permutations : (التباديل)

Definition: A Permutation or 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 permutation on A . If A is the finite set $\{1,2,\ldots, n\}$, then the set of all permutation of A is denoted by S_n or P_n and $o(S_n) = n!$, where $n! = n(n-1) \ldots (3)(2)(1)$

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



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

Example (2): Let A = { 1, 2, 3} . Write all Perm. on A.

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

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

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

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

<u>Theorem :</u> If $A \neq \varphi$, then the set of all permutation on A Forms agroup with composition of Mapps.

(i.e.) Let $\neq \varphi$, then (Symm(A) , o) is a group.

Proof :

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

T.P. (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 $fof^{-1} = f^{-1}of = i_A$

$\therefore$ (Symm(A), o) is a group.

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

Example: 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.

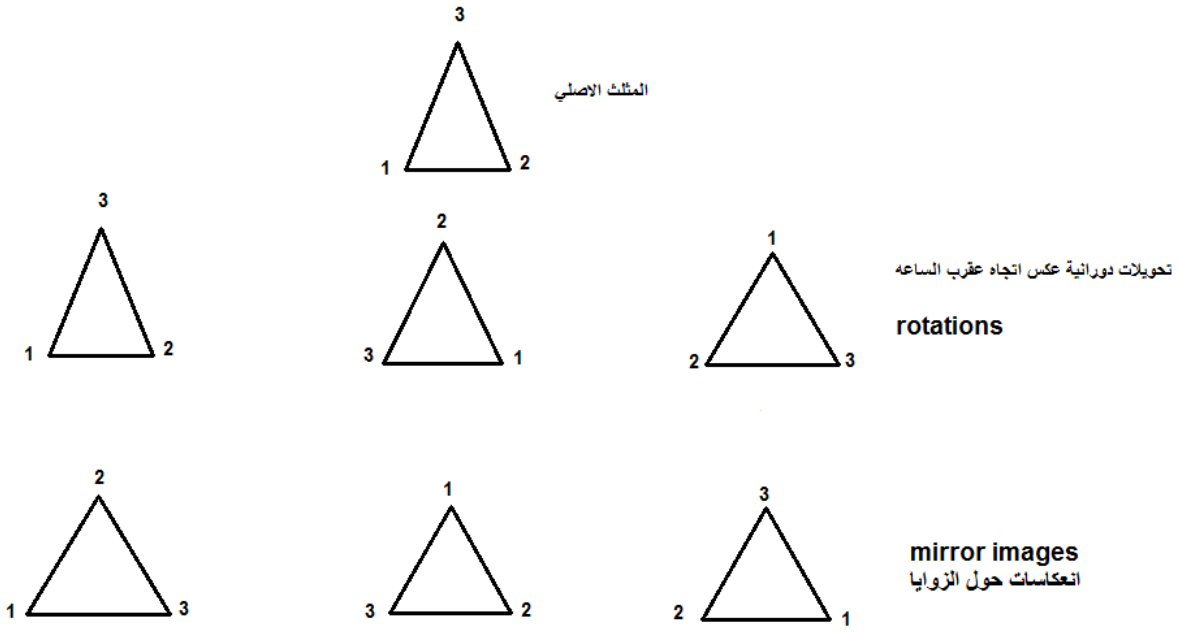
This group is called symmetric group.

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

(S_3 , o) is not Comm. Group.

Also (S_3,o) is called the group of symmetries of on equilateral triangle .

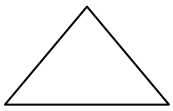
(زمرة تناظر المثلث متساوي الساقين)



Definition : (**The dihedral group D_n of order $2n$**)

The n^{th} dihedral group is the group of symmetries of the regular n-gon. $o(D_n) = 2n$

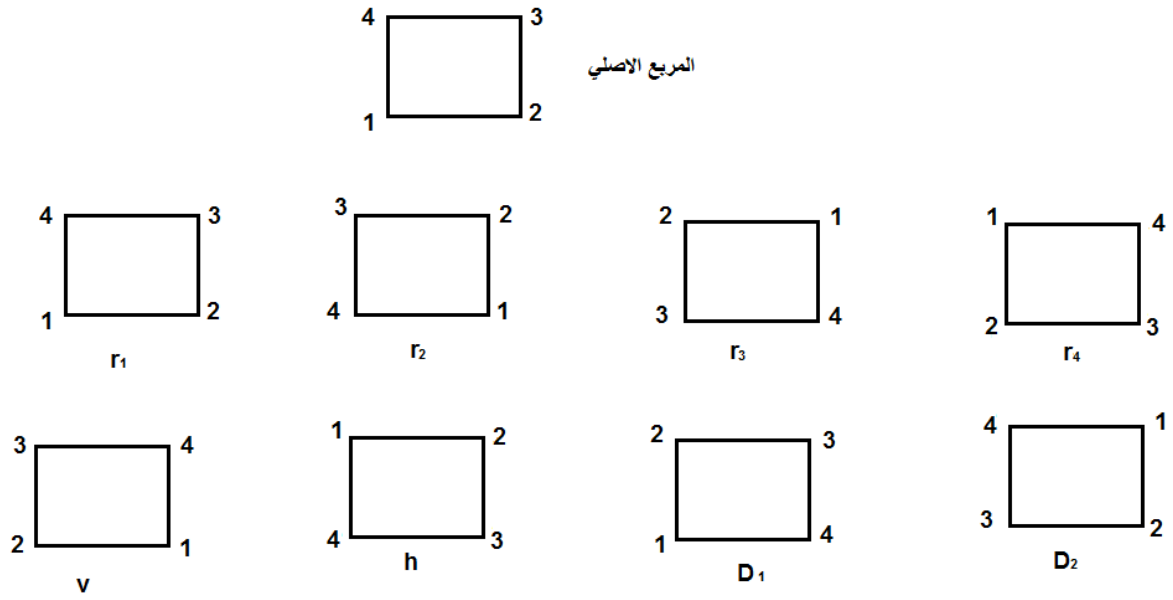
D_3 : is the third dihedral group.

 , O (D_3) = (2) (3) = 6 elements

Example . The group of symmetries of square D_4 or Gs, o (D_4)= 8

$G_s = D_4 = \{r_1, r_2, r_3, r_4, v, D_1, D_2\}$, 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: 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: 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: (2) 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: Every permutation f of a finite set A is a product of disjoint cycles.

Definition: A cycle of length 2 is a transposition.

Example: The permutation

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

Property: any permutation can be expressed as the product of transpositions.

(i.e.) $(a_1a_2 \dots a_n) = (a_1a_2)\,(a_1a_3)$ $\dots..(a_1a_n)$

Therefore any cycle is a product of transpositions.

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

Definition: 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) Let $f = \begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix} \in P_3$

Is f even or odd permutation .

Ans. $f = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ = (1 3 2) = (13) (12)

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

Example(2): Determine an even and odd permutations of P_4.

(H.W)

Definition: "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): 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

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

Example(2): Find A_4 from S_4

(H. W.)

Chapter Two

Subgroups and Cyclic Groups الزمر الجزئية والزمر الدائرية

Definition (1):

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

Definition (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 element of H. e∈G⇒ e∈H

(3)∀a∈H⇒a^{-1}∈H

Remark (1):

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

Examples (1):

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

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

3. H={$\bar{0}, \bar{2}$}⊆Z_4

   (H,+$_4$) is a proper subgroup of (Z_4,+$_4$). But {$\bar{0}, \bar{3}$} is not subgroup of (Z_4,+$_4$). Since $\bar{3}+_4\bar{3} = \bar{6}$ (Mod4) $= \bar{2} \notin \{\bar{0}, \bar{3}\}$, it follows that closure is not true in {$\bar{0}, \bar{3}$}.

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

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

Proof:

(⇒) let (H,∗) be a subgroup and a,b ∈ H, then

$a,b^{-1}\in H \Rightarrow a*b^{-1}\in H$ (since ∗closure)

(⇐) Let $a*b^{-1}\in H$ T.P. (H,∗) is subgroup

(1) Since H≠ϕ⟹∃ b∈H s.t. $b*b^{-1}\in H \Rightarrow e\in H$.

(2) Since b∈H and $e\in H \Rightarrow e*b^{-1}\in H \Rightarrow b^{-1}\in H$

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

∴By definition (2) (H,∗) is a subgroup of (G,∗)

Example (2): Let (Z,+) be a group and H={5a: a∈Z}. Show that (H,+) is a subgroup of (Z,+)

Solution: By The above, let x , y ∈ H, T.P. $x+y^{-1}\in H$

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

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

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

⟹ (H,+) is a subgroup of (Z,+)

Theorem (2): If (H_i,∗) is the collection of subgroups of (G,∗), then ($\cap H_i$,∗)) is also subgroup of (G,∗)

Proof:

(1) Since ∃ e∈ H_i ,∀i ⟹e ∈ $\cap H_i \Rightarrow \cap H_i \neq \phi$

(2) Let x, y ∈$\cap H_i$ T.P. $x*y^{-1}\in \cap H_i$

Since x ,y∈ $\cap H_i \Rightarrow$ x,y ∈H_i ∀i

$\Rightarrow x*y^{-1}\in H_i$, ∀i (since H_i subgroups)

$\Rightarrow x*y^{-1}\in \cap H_i$

∴ ($\cap H_i$,∗) is subgroup of (G,∗)

Theorem (3): Let $(H_i,*)$ is the collection of subgroups of $(G,*)$ and let H_k and $H_j \in \{H_i\}$ 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. (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 $H_\ell$subgroup)

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

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

Theorem (4): Let $(H_1,*)$ and $(H_2,*)$ are two subgroupsof $(G,*)$ then $(H_1 \cup H_2,*)$, is asubgroup of $(G,*)$ iff $H_1 \subseteq H_2$ or $H_2 \subseteq H_1$.

Proof. $(\Rightarrow)$ Let$(H_1 \cup H_2,*)$ is a subgroup, T.P. $H_1 \subseteq H_2$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 $\exists\ b \in H_2$, $b \notin H_1$

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

$\Longrightarrow a * b^{-1} \in H_1$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 $H_2 \subseteq H_1$T.P. $(H_1 \cup H_2,*)$ 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): $(H_1 \cup H_2,*)$ 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 (3): Let $(G,*)$ be a group and $(H,*)$, $(K,*)$ be two subgroups of G, then the product of H and K is the set:

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

Notes(1):

(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 (5): 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 $(G,*)$. (منطوق فقط)

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 $b\in K\subseteq G$

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

$$\Longrightarrow a*b =x\in G$$

$$\therefore H*K \subseteq G$$

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

$\Longrightarrow x\in H*K$

$$\therefore H\subseteq H*k$$

Similarly $K \subseteq H*K$

(3) (⇒) suppose (H∗K,∗) is asubgroup of (G,∗) T.P. H∗K=K∗H

(i.e.) H∗K ⊆ K∗H ∧ K∗H ⊆H∗K

Let x ∈ H∗K ⟹x =a∗b ∋ a∈H ∧ b ∈ K

Since H∗K is subgroupof G⟹x^{-1}∈ H∗K

Let x^{-1}= c ∗ d ∋ c ∈H∧ d∈K

x =$(x^{-1})^{-1}$ = $(c*d)^{-1}$ = $d^{-1}*c^{-1}$∋d^{-1} ∈K ∧c^{-1}∈ H

∴x = $d^{-1}*c^{-1}$∈ K∗H

∴H∗K⊆K∗H

K∗H ⊆ H∗K **(H.W.)**

(⇐) Let H∗K=K∗H T.P.(H∗K,∗) is subgroup of(G,∗)

H∗K≠ ϕand H∗K⊆G (by 1)

Let x,y ∈H∗K T.P.x∗y^{-1}∈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}= $(a*b)*(c*d)^{-1}$

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

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

∴$(b*d^{-1})*c^{-1}$∈ K∗H=H∗K

∴$(b*d^{-1})*c^{-1}$∈ H∗K

⇒∃ p∈ H , ℓ ∈K ∋ $(b*d^{-1})*c^{-1}$ = p∗ℓ

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

∴x∗y^{-1}∈H∗k

∴(H∗K,∗) is subgroup of (G,∗)

Example (3): In $(Z_8,+_8)$, Let $H=\{\bar{0},\bar{4}\}$ and $K=\{\bar{0},\bar{2},\bar{4},\bar{6}\}$. Find $H+_8K$

Solution: $H+_8K=\{\bar{0},\bar{2},\bar{4},\bar{6}\}$.

Notes (2): Let $(H,*)$ and $(K,*)$ are two subgroupof $(G,*)$, then :

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

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

Exercises: Is $(H,*)$ a subgroup of $(G,*)$ each of the following:

(1) $(Z_8, +_8)$, $H=\{\bar{0},\bar{6}\}$. Find H^2.

(2) $(Z_4, +_4)$, $H=\{\bar{0},\bar{1},\bar{2}\}$. Find H^2.

Definition (4): The center of a group $(G,*)$ denoted by cent(G) or C(G) is the set $C(G)=\{c\in G: c*x=x*c, \forall x\in G\}$ العناصر التي تتبادل مع كل عناصر الزمرة

Note (3): $C(G)\neq\phi$, since $\exists e\in G$ s.t.

$e*x=x*e \ \forall x\in G \Rightarrow e\in C(G)$

Examples (4):

(1) The group $(R\backslash\{0\}, .)$

$C(R)=R$ since R with multiplication is commutative

(2) The group $(S_3,\circ)$, $C(S_3)=\{f_1\}$

Since $C(S_3)=\{f\in S_3: f\circ g=g\circ f \ \forall g\in S_3\}=\{f_1\}$

Theorem (6): Let $(G,*)$ be a group. Then $(cent(G),*)$ is a subgroup of $(G,*)$.

Proof:

$cent(G)\neq\phi$ (by note (3))

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

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

$a\in cent(G)\Rightarrow a*x=x*a, \forall x\in G$

$b\in cent(G)\Rightarrow b*x=x*b, \forall x\in G$

T.P. $(a*b^{-1})*x=x*(a*b^{-1}) \ \forall x\in G$

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

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

$=a*(b*x^{-1})^{-1}$ (since b ∈ cent (G))

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

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

$=(x*a)*b^{-1}$ (since b ∈ cent (G))

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

∴ $(a*b^{-1}) \in$ cent (G)

∴ (cent (G),∗) is a subgroup of (G,∗).

Theorem(7): Let (G,∗) be a group. Then

cent(G)=G⇔G is a commutative group.

Proof.

(⇒) ∀a∈G ⇒a∈ cent(G)

∴ a∗x =x∗a, ∀x∈G

∴ a∗x =x∗a, ∀x, a∈G

∴ G is commutative group

(⇐) suppose that G is commutative group T.P. cent(G) =G

(i.e) T.P. cent (G) ⊆G∧G⊆ cent(G)

By definition of cent(G) we have cent(G)⊆G.

T.P. G⊆ cent(G)

Let x∈G, G is commutative group ⇒x∗a = a ∗x, ∀a∈G

∴x∈ cent(G)⇒G⊆ cent(G)

∴ cent G=G

Cyclic Groups الزمر الدوارة أو (الزمر الدائرية)

Definition (5): Let (G,∗) be a group and $a \in G$, the cyclic subgroup of G generated by the a is denoted by $\langle a \rangle$ and defined as

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

G=$\langle a \rangle$ is called cyclic group.

- تسمى الزمرة دائرية او دوارة اذا امكن توليدها من عنصر واحد او اذا وجد عنصر يولدها

Definition (6):A group (G,∗) is called cyclic group generated by a iff $\exists a \in G$ such that

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

Examples (5): In $(Z_9,+_9)$find the cyclic subgroup generated by$\bar{2},\bar{3},\bar{1}$

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

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

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

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

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

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

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

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

Examples (6): In (Z,+) fined a cyclic group generated by 1, 2, – 1

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

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

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

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

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

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

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

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

Examples (7): Is $(S_3,\circ)$ cyclic group ?

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

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

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

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

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

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

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

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

Examples (8): In$(Z_6,+_6)$ find cyclic group generated by$\bar{1},\bar{2},\bar{5}$**(H.W.)**

Theorem (8): Every cyclic group is commutative.

Proof: Let (G,∗) be acyclic group

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

(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 (9):$<a>=<a^{-1}>\forall a\in$G

Proof:

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

$=\{ (a^{-1})^m \because$m $= -$ k$\in Z\}$

$=<a^{-1}>$

Theorem (10): If (G,∗) is a finite group of order *n* generated by *a*, then G= $<a>=\{a^k : k\in Z\} = \{a^1, a^2, \ldots\ldots, a^n = e\}$such that *n* is least positive integer $\ni a^n = e\,, (i.e.)$

o(*a*)=*n*= o(G) (رتبة العنصر الذي يولد الزمرة = رتبة الزمرة)

Examples (9): Show that (Z_n,+$_n$) is cyclic group.

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

بما ان الزمرة مرتبهية فتكتب بالشكل :

o(Z_n) = *n* ,T.P. $Z_n . =<\bar{1}>$

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

$=\{\bar{1}, \bar{2}, \bar{3}, \ldots, \bar{n} = \bar{0}\}=Z_n$

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

Definition (7):(Division Algorithm for Z) **خوارزمية القسمة**

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

a =bq + r where $0 \le r < b$

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

Examples (10): Find the quotient q and remainder r when 38 is divided by 7 according to the division algorithm.

Answer: 38=7(5)+3 $0\le 3\le 7$

∴q =5 and r=3.

Examples (11):a=23 ,b=7

23=7(3)+2 $0\le 2\le 7$

q =3 , r=2.

Examples (12): a=15 , b=2

15=(2)(7)+1 $0\leq 1\leq 2$

q =7 , r=1

Theorem (11): A subgroup of acyclic group is cyclic.(للاطلاع)

Corollary (1): 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, then o(G)=*n*

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

Let (H,∗)be a subgroup of (G,∗). Then (H,∗) is cyclic (by Theorem 11) such that H=<a^m>

T.P. *m*|*n*(*n*=*m*g , g ∈ Z)

e ∈H ⇒a^n∈H,a^m∈H, by division algorithm of *n* and *m*

⇒*n*=*m*g+r $0\leq r<m$

r =n – mg⇒$a^r = a^n * (a^m)^{-g}$

⇒$a^r = (a^m)^{-g}$∈H

But $0\leq r<m$

⇒ If r=0 ⇒*n*=*m*g

∴*m*|*n*

Examples (13): Find all subgroup of (Z_{15},$+_{15}$)

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

H=<$(\bar{1})^m$>∋*m*|15

m=1,3,5,15

If *m*=1 ⇒H_1=<$\bar{1}$>= Z_{15}

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

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

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

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

Corollary (2): 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

∴H=< a^m>∋m|p⇒m = 1 or m = p

If m=1 ⇒ H=<a>= G (not proper subgroup)

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

∴G has no proper subgroup.

Examples (14): Find all subgroup of (Z_7,$+_7$)

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

∴ m=1 , m =7

If m=1 ⇒H_1=<$\bar{1}$>= Z_7

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

Definition (8): [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|x ∧c|y

(2) if a|x ∧a|y ⇒a|c

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

Examples (15): Find (g.c.d.(12,18))

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

(1) 6|12 ∧ 6|18

(2) 3|12 ∧ 3|18 ⇒ 3|6

or 2|12 ∧2|18 ⇒2|16

Remark (3): 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 (16): Find all generators of $(Z_6,+_6)$

Answer: 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)$\neq$ 1$\Rightarrow Z_6\neq<(\bar{1})^2>=<\bar{2}>$

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

k=4$\Rightarrow$ g.c.d(4,6)$\neq$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 $\{\bar{1},\bar{5}\}$

Theorem (12): 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.

Definition (9): **المجموعات المشاركة للزمرة الجزيئة H**

Let $(H,*)$ be a subgroup of a group $(G,*)$.The set

$a*H=\{a*h : h\in H\}$of G is the left coset of H containing a , while the subset $H*a=\{h*a : h\in H\}$ is the right coset of H containing a.

Examples (17): If $(Z_6,+_6)$,a=$\bar{1}$, H=$\{\bar{0},\bar{2},\bar{4}\}$, then

$\bar{1}+_6H=\{\bar{1},\bar{3},\bar{5}\}$, $H+_6\bar{1}=\{\bar{1},\bar{3},\bar{5}\}$

$\bar{3}+_6H=\{\bar{3},\bar{5},\bar{1}\}$, $H+_6\bar{3}=\{\bar{3},\bar{5},\bar{1}\}$.

Notes(4):

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

(2) $a*H \neq H*a$ 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 (13): Let $(H,*)$ be a subgroup of $(G,*)$ and $a\in G$, then

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

Proof: (1) $e\in G$, $e*H=\{e*h:h\in H\}=H$

(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: $a=a*e\in a*H$

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

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

$(\Leftarrow)$ Suppose $a\in H$ T.P. $a*H=H$

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

T.P. $a*H\subseteq H$

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

$\therefore a*H\subseteq H$

T.P.$H\subseteq a*H$

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

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

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

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

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

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

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

$\Rightarrow b*H=a*H$

Remark (4): Every coset (left or right) of a subgroup H of a group $(G,*)$ has the same number of elements as H.

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

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

Proof: T.P. $G=\cup_{a\in G} a* H$ and $a_i*H \cap a_j*H = \phi$

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

$\therefore a_i*H \cap a_j*H = \phi$ T.P. $G=\cup_{a\in G} a* H$

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

$\Rightarrow \cup_{a\in G} a* H \subseteq G \quad \ldots(1)$

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

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

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

Example (17): The group $(Z_6,+_6)$ is abelian. Find the partition of Z_6 into coset of the subgroup $H=\{\bar{0},\bar{3}\}$

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

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

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

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

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

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

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

∴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.

Example (18):(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 (10): 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 (5): If $(G,*)$ is a finite group. Then $[G:H]=\frac{o(G)}{o(H)}$.

Example (19):$(S_3,\circ)$,H= $\{f_1,f_2, f_3\}$

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

Example (20):$(Z_6,+_6)$, H=$\{\bar{0},\bar{3}\}$

∴$[Z_6:H]=\frac{6}{2} =3$

Theorem (14): (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 ∋o(G)=n and H be a subgroup of G ∋ o(H)=m.

T.P. o(H) | o(G) (T.P. m|n , n=mk)

Since G is finite⇒[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 (1): 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 $o(a) = m$ T.P.$o(a)| o(G)$.

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): If $(G,*)$ is a finite group, then $a^{0(G)} = e \quad \forall a \in G$.

Proof.

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

By Corollary (1) of Lagrange theorem⇒o(a) | o(G)

⇒m|n

⇒ n=mk

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

$\therefore a^{0(G)} = e \forall a \in G$.

Corollary (3): Every group of prime order is cyclic.

Corollary (4): Every group of order less than 6 is commutative.

Exercises:

(1) Find all subgroupsof $(Z_5,+_5)$.

(2) Let $(Z_8,+_8)$ be agroup and $H=<\bar{2}>$. Is H a subgroup of Z_8?

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

Chapter Three

Normal Subgroups and Quotient Groups

(الزمر الجزئية الطبيعية وزمر القسمة)

Def (1). Let (G,*) be a group and $a, b \in G$, then "a is conjugate to b " and denoted by $a \sim b$ iff $\exists x \in G \ni b = x*a*x^{-1}$ and $b \sim a$ iff $\exists x \in G \ni a = x*b*x^{-1}$.

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

ex.(1) In (S_3,o) . Is $f_3 \sim f_2$?

Ans. $f_3 \sim f_2 \Leftrightarrow \exists x \in S_3 \ni f_2 = x \ o \ f_3 \ o x^{-1}$

$x=f_1 \Rightarrow f_1 \ o \ f_3 o \ f_1^{-1}=f_3 \neq f_2$

$x=f_2 \Rightarrow f_2 \ o \ f_3 \ o f_2^{-1}=f_1 \ o f_2^{-1}=f_3 \neq f_2$

$x=f_3 \Rightarrow f_3 \ o \ f_3 \ o \ f_3^{-1}=f_2 \ o \ f_2=f_3 \neq f_2$

$x=f_4 \Rightarrow f_4 \ o \ f_3 o f_4^{-1}=f_5 \ o \ f_4=f_2$

$x=f_5 \Rightarrow f_5 \ o \ f_3 \ o f_5^{-1}=f_6 \ o \ f_5=f_2$

$x=f_6 \Rightarrow f_6 \ o \ f_3 \ o \ f_6^{-1}=f_4 \ o \ f_6=f_2$

$\therefore \exists x \in S_3 \ni x o \ f_3 \ o \ x^{-1}=f_2$

$\therefore f_3 \sim f_2$

IS $f_1 \sim f_2$ and $f_1 \sim f_1$? (H.W)

ex.(2) In $(z_4,+_4)$. Is $\bar{1} \sim \bar{2}$? $\bar{2} = \bar{x} +_4 \bar{1} +_4 x^{-1}$

$x = \bar{1} \Rightarrow \bar{1} +_4 \bar{1} +_4 (\bar{1})^{-1} = \bar{2} +_4 \bar{3} = \bar{5} = \bar{1} \neq \bar{2}$

$x=\bar{2} \Rightarrow \bar{2}+_4\bar{1}+_4(\bar{2})^{-1}=\bar{3}+_4\bar{2}=\bar{5}=\bar{1}\neq\bar{2}$

$x=\bar{3} \Rightarrow \bar{3}+_4\bar{1}+_4(\bar{3})^{-1}=\bar{0}+_4\bar{1}=\bar{1}\neq\bar{2}$

$x=\bar{0} \Rightarrow \bar{0}+_4\bar{1}+_4(\bar{0})^{-1}=\bar{1}\neq\bar{2}$

$\therefore \bar{1}\neq\bar{2}$

Remark(1): if (G,*) is a belian group and a,b ∈ G , then a~ b ⇔ a=b

Proof: Suppose a~b⇔ $\exists x \in G \ni b=x*a*x^{-1}$

⇔b= $x * x^{-1} * a = e * a$

⇔ b=a

Theorem (1): The relation (Conjugate) is an equivalent relation.

Proof: (1) Reflexive (الانعكاسية)

Let $a \in$G , T.P $a \sim a$

∃ e ∈ G ∋ a=e*a*e^{-1}

$\therefore a \sim a$

(2) Symmetric (التناظر)

Let a,b ∈ G and a~b ,T.P b ~a

a~b⇒ ∃ x ∈ G ∋ b=$x*a*x^{-1}$

⇒ x^{-1}*b=$a*x^{-1}$

⇒ x^{-1}*b*x=a

⇒b~a

(3) Transitive (متعدية)

Let a,b,c ∈ G s.t.a~b∧ b~c ,T.P a~c

a~b ⇒ ∃x ∈ G s.t b=x*a*x^{-1}……(1)

b~c⇒ ∃y ∈ 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=$y * x$ ∈ G)

∴ a~c

Def(2). Let (G,*) be a group and a ∈ G , then the conjugate of a is denoted by c(a) and defined as

c(a)={b∈ G: a~b} (a مجموعة العناصر التي ترافق)

or c(a)={b∈ G:b=$x * a * x^{-1}$ }

or c(a)={$x * a * x^{-1}$,∀x ∈ G} .

The set of all elements conjugate to a is called the conjugate class of a.

Ex(3). Find the conjugate class of each element in the following groups:

1) (G={1,-1,i,-i},·) ∋ i^2= -1

Ans. c(i)={x.i.x^{-1}, ∀x ∈ 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)**

Ex(4). Find $c(\bar{3})$ in $(z_4,+_4)$

Ans. $c(\bar{3}) = \{\bar{0}, +_4\bar{3}+_4\bar{0}^{-1}\ , \bar{1}+_4\bar{3}+_4\bar{1}^{-1}, \bar{2}+_4\bar{3}+_4\bar{2}^{-1}, \bar{3}+_4\bar{3}+_4\bar{3}^{-1}\}$

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

$= \{\bar{3}, \bar{3}, \bar{3}, \bar{3}\}$

$\therefore$ $c(\bar{3})=\{\bar{3}\}$ (by remark if G is comm. group and a$\sim b$ then a=b)

Note. 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)

$c(f_3)=\{f_2,f_3\}$ is not subgroup of S_3

Theorem(2): Let $(G,*)$be a group and a,b$\in G$,then

1) $a \in c(a)\ \forall a \in G$
2) $c(a)=c(b) \Leftrightarrow a\sim b\ \forall a,b \in G$
3) $c(a)\cap c(b)=\emptyset$ iff $a\sim b$ **(H.W)**
4) $c(a)\cap c(b)=\emptyset$ 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}⇔ a ∈cent (G) **(H.W)**

8) c(e) ={e} **(H.W)**

Proof: (1) a ∈ c(a) ∀a ∈G

Since $a\sim a$ ∀a ∈G (~ is ref.)

⟹ a ∈ c(a)⇒ c(a)≠Ø

(2) c(a)=c(b) ⇔ $a\sim b$ ∀a,b ∈ G

(⇒) Suppose c(a)=c(b) T.P $a\sim b$

By (1) ,a ∈ c(a)=c(b)⇒ $a \in c(b) \Rightarrow a\sim b$

(⇐) suppose $a\sim b$ T.P c(a)=c(b)

(i.e.) c(a) ⊆c(b) ∧ c(b) ⊆ c(a) ?

Let x ∈ c(a)⇒ x~a ∧ $a\sim b$ ⇒ x~b

⇒ x∈ c(b) ⇒ c(a)⊆c(b) ……(1)

Let x ∈ c(b) ⇒ x~b ∧ $a\sim b$

⇒ x~a ⇒ x ∈c(a) ⇒ c(b)⊆ c(a) .....(2)

By (1) and (2)⇒ c(a)=c(b)

(5) b∈ c(a)⇔ c(a)=c(b)

(⇒) Let b ∈c(a)⇒ b~a ⇒c(a)=c(b)(by Th.)

(⇐) c(a)=c(b)⇒ $a\sim b$ ⇒ b~a ⇒ b∈ c(a).

(6) c(a) ={a} ∀a ∈ G⇔ G is a comm. group.

c(a)=$\{a\}$ $\forall a \in$ G

$\Leftrightarrow x * a * x^{-1}=a \quad \forall x \in G$

$\Leftrightarrow x * a = a * x$

$\Leftrightarrow$ G is a comm. group.

Def(3). Let (G,$*$) be a group and $a \in G$, then the normalizer of a is denoted by N(a) and defined as: N(a) $= \{x \in G: x * a = a * x\}$

(مجموعة العناصر التي تتبادل مع a)

Ex 5. In (z_8,$+_8$) . find N($\bar{3}$)

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): Let (G,$*$) be a groub 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 (منطوق فقط)
6) If (G,$*$) is a finite group, then o (c(a)) / o(G)). (منطوق فقط)

Proof: (1)N(a) $= \{x \in G : x * a = a * x\} \subseteq$ G

Since $e * a = a * e \Rightarrow$ e$\in$ N(a)

$\therefore$ N(a)$\neq \emptyset$

(i) Closure: Let x, y $\in$ N(a) T. P x$*$y $\in$ N(a)

$x \in N(a) \Rightarrow x * a = a * x$

$y \in N(a) \Rightarrow y * a = a * y$

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

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

$\therefore x * y \in N(a)$

(ii) $Let\ x \in N(a)\ T.P.\ x^{-1} \in N(a)$

$Since\ x \in N(a) \Rightarrow x * a = a * x$

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

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

$\Rightarrow x^{-1} \in N(a)$

$\therefore (N(a), *)\ is\ a\ subgroup$.

(3)($\Rightarrow$) Suppose $N(a) = G \forall a \in G$ T.P G is a comm.

$\forall x \in G = N(a) \Rightarrow x \in N(a)\ \ \forall a \in G$

$\Rightarrow x \in N(a) \forall x, a \in G$

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

$\therefore (G, *)\ is\ a\ comm.\ group$.

($\Leftarrow$)$Suppose (G, *)\ is\ a\ comm.group \quad T.P. \quad N(a) = G$

$T.P. \quad N(a) \subseteq G \ \wedge \ G \subseteq N(a)$

$N(a) \subseteq G \quad (bydef.)$

$T.P.\ \ G \subseteq N(a)$

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$\subseteq N(a) \ \Rightarrow \ N(a) = G \ \ \forall a \in G.$

Def(4). Let (H,$*$), (K,$*$) be two subgroups of (G,$*$), then H is a conjugate subgroup K iff $\exists x \in G \ni K = x * H * x^{-1}$ and denoted by $H \sim K$.

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

Ex.(6) In (S_3,o), H={f_1,f_6}, K ={f_1,f_5} . Is $H \sim K$?

Ans.(i.e.) Is $\exists x \in S_3 \ni x$o Ho x^{-1} =K ?

$x=f_1 \Rightarrow f_1$ o{f_1,f_6} o f_1^{-1}={f_1o f_1o f_1^{-1},f_1o f_6o f_1^{-1}}={f_1,f_6}$\neq K$

$x=f_2 \Rightarrow f_2$o{f_1,f_6} o f_2^{-1}={f_2o f_1o f_2^{-1},f_2o f_6o f_2^{-1}}={f_1,f_4}$\neq K$

$x = f_3 \Rightarrow$ f_3o{f_1,f_6} o f_3^{-1}={ f_3o f_1o f_3^{-1}, f_3o f_6o f_3^{-1}}={f_1,f_5}$=K$

$\therefore \exists x = f_3 \ni H \sim K$.

ex(7): In (Z_{12},$+_{12}$), H={$\bar{0},\bar{4},\bar{8}$}, K ={$\bar{0},\bar{3},\bar{6},\bar{9}$} Is H$\sim K$?

Ans. (i.e.) $\exists \bar{x} \in Z_{12} \ni \bar{x} +_{12}$ H$+_{12} \bar{x}^{-1}$=K

$\bar{x}=\bar{1} \Rightarrow \bar{1} +_{12} \{\bar{0},\bar{4},\bar{8}\} +_{12} \bar{1}^{-1} = \bar{1} +_{12} \{\bar{0},\bar{4},\bar{8}\} +_{12} \overline{11}$=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 $\ \forall \bar{x} \in Z_{12}$

Since $\bar{x} +_{12}$ H$+_{12} \bar{x}^{-1} = \bar{x} +_{12} \bar{x}^{-1} +_{12}$ H= H $\neq$ K

ex.(8): In (G_s,o) , let $H=\{r_1,r_4\}$, $K=\{r_1,r_2\}$. Is $H\sim K$? **(H.W)**

Theorem (4) : Let $(H,*)$, $(K,*)$be two finite subgroups of$(G,*)$ and $H\sim K$, then $o(H)=o(K)$. (منطوق فقط)

Theorem(5) : 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 $a,b\in x*H*x^{-1}$ T.P $a*b^{-1}\in x*H*x^{-1}$

$a\in x*H*x^{-1}\Rightarrow a=x*h_1*x^{-1}\ni h_1\in H$

$b\in x*H*x^{-1}\Rightarrow b=x*h_2*x^{-1}\ni h_2\in H$

$a*b^{-1}=(x*h_1*x^{-1})*(x*h_2*x^{-1})^{-1}$

$=(x*h_1*x^{-1})*(x*h_2^{-1}*x^{-1})$

$=(x*h_1)*(x^{-1}*x)*(h_2^{-1}*x^{-1})$

$=x*(h_1*h_2^{-1})*x^{-1}\in x*H*x^{-1}$

$\therefore (x*H*x^{-1})$ is a subgroup of $(G,*)$.

Remark(2): The relation "conjugate" is an equivalent relation on the set of all subgroups of G. **(H.W)**

Def(5). 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 ترافقH)

Ex(9). (S_3,o), $H=\{f_1,f_4\}$, find C(H)

Ans. $C(H)=\{xoHox^{-1} : \forall x \in S_3\}$

$=\{f_1o\{f_1,f_4\}of_1^{-1},f_2o\{f_1,f_4\}o\ f_2^{-1},\ldots.,f_6o\{f_1,f_4\}of_6^{-1}\}$

$=\{\ \{f_1,f_4\},\{f_1,f_6\},\ldots..,\{f_1,f_5\}\ \}$

Ex.(10) : $(G=\{e,a,b,c\},*)$ is a four Klien group.

G is comm. group , $a^2=b^2=c^2=e$.

$H=\{e,a\}\subseteq G$, find C(H)

Ans. $C(H)=\{x*H*x^{-1} : \forall x \in G\}$

$=\{x*x^{-1}*H : \forall x \in G\ \}=\{H\}$

Def(6). Let $(H,*)$ be a subgroup of $(G,*)$, then the normalizer of H is denoted by N(H) and defined as: $N(H)=\{x \in G : x*H=H*x\}$

Ex(11). (Gs,o) , $H=\{r_2,r_3\}$, find N(H)

$N(H)=\{x \in G_5 \ni xoH=Hox\}$

$x=r_1 \Rightarrow r_1oH=H\ o\ r_1$

$x=r_2 \Rightarrow r_2oH=H\ o\ r_2$ …. → N(H) = { r_1, r_2, r_3, r_4, h, v, D_1, D_2 } = Gs

Exercises: 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(6): 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∗ $H = H * e \Rightarrow e \in N(H) \neq \emptyset$

$$N(H) = \{x \in G \ni x * H = H * x\} \subseteq G$$

Let a,b ∈ $N(H), to\ prove\ a * b^{-1} \in N(H)$

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

Since a∈ $N(H) \Rightarrow a * H = H * a$

b∈ $N(H) \Rightarrow b * H = H * b$

$b * H * b^{-1}$=H

$H * b^{-1}$=$b^{-1} * H$

∴$b^{-1} \in N(H)$

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

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

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

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

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

$\Rightarrow a * b^{-1} \in N(H) \Rightarrow (N(H),*)$ is a subgroup of (G,$*$) T.P $H \subseteq N(H)$

Let a$\in H \Rightarrow a * H = H \ \wedge H * a = H$

$\therefore a * H = H * a \Rightarrow$ a$\in N(H)$

$\therefore$H$\subseteq N(H)$

(2) Suppose G is comm. To prove N(H)=G i.e. N(H) $\subseteq G \wedge G \subseteq N(H)$.

By definition N(H) $\subseteq G$.

Let x$\in G \Rightarrow x * H = H * x \Rightarrow x \in N(H)$

$\therefore G \subseteq N(H)$, $\therefore$G=N(H)

Note : If N(H)=G, then (G,$*$) is comm. group ? **(H.W)**

Def(7). A subgroup (H,$*$) is called self-conjugate iff C(H)=H.

(i.e.) $x * H * x^{-1}$=H $\forall x \in G$.

Ex(12). 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.

Def(8). : A subgroup (H,$*$) is called normal subgroup of(G,$*$) and denoted by H$\Delta G \Leftrightarrow$H is self-conjugate

Or H$\Delta G \Leftrightarrow x * H * x^{-1}=H \ \forall x \in G$.

H$\not\Delta$G $\Leftrightarrow \exists x \in G \ \ni$ x*H*x$^{-1}\neq$H

Ex(13). (1) (G_s,o) , $H = \{r_1,r_4,v,h\}$

$C(H)=H \Rightarrow H \Delta G_s$

(2) $(S_3,o), \Rightarrow H_1=\{f_1,f_5\}$, $H_2=\{f_1,f_2,f_3\}$

$C(H_1)\neq H_1 \Leftrightarrow H \not\Delta S_3$, $C(H_2)=H_2 \Rightarrow H_2 \Delta S_3$

1) $(Z_4,+_4)$, $H=\{\bar{0},\bar{2}\}$

$C(H)=H \Rightarrow H \Delta Z_4$

Theorem(7): 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) $H \Delta G \Leftrightarrow (x * H) * (y * H) = (x * y) * H \quad \forall x,y \in$ (منطوق فقط)

Proof: (1) $H \Delta G \Leftrightarrow x * H * x^{-1}=H \quad \forall x \in G$

$\Leftrightarrow x * H = H * x \quad \forall x \in G$

(2) ($\Rightarrow$) Suppose that $H \Delta G$ T.P. $N(H)=G$

T.P. $N(H) \subseteq G \quad \wedge \quad G \subseteq N(H)$

$N(H) \subseteq G$ by definition

T.P. $G \subseteq N(H)$

Let $x \in G \Rightarrow x * H = H * x \Rightarrow x \in N(H)$

$\therefore G \subseteq N(H)$

$\Rightarrow G=N(H)$

($\Leftarrow$) Suppose $N(H)=G$, T.P. $H \Delta G$

$\forall x \in G \Rightarrow x \in N(H) \Rightarrow \quad x * H = H * x \ \forall x \in G \Rightarrow H \Delta G$ (by(1))

(3) ($\Rightarrow$) Suppose $H \Delta G$. T.P. c(a) $\subseteq H \quad \forall a \in H$

Since $H \Delta G$ so by definition

$x * H * x^{-1} = H$

$x * H * x^{-1} \subseteq H$

$\therefore c(a) = \{x * a * x^{-1} \forall\ a \in H\ \} \subseteq H$

($\Leftarrow$) Suppose c(a) $\subseteq H \quad \forall a \in H$ T.P. $H \Delta G$ (i.e.) $x*H*x^{-1} = H$

T.P. $x*H*x^{-1} \subseteq H \wedge H \subseteq x * H * x^{-1}$

c(a) $\subseteq H \Rightarrow x * H * x^{-1} \subseteq H$ …..(1)

T.P. $H \subseteq x*H*x^{-1}$

Let $b \in H \Rightarrow b = e * b * e^{-1}$

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

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

$b = x * h * x^{-1} \in x * H * x^{-1} \qquad (h = x^{-1} * b * x)$

$\therefore H \subseteq x * H * x^{-1}$…….(2)

From (1) and (2) $\Rightarrow H = x * H * x^{-1} \quad \forall x \in G \quad \Rightarrow H \Delta G$

Theorem(8): Let $(G,*)$ be agroup , then

1) $\{e\} \Delta G$

2) $G \Delta G$

3) cent (G) ΔG .

Theorem(9): 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 $\quad \therefore$H$\Delta\, G$

Note: The converse of this theorem is not true

For example:

(G=$[\pm 1, \pm i, \pm j, \pm k]$,.) $\ni$ $i^2=j^2=k^2=-1$

ij=K , ji= -K $\Rightarrow$ ij$\neq$ji

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}and

All subgroup of G are normal of G, since $C(H_i) = H_i \ \ \forall i$

Theorem(10): Let (H,$*$) be a subgroup of (G,$*$) such that[G:H]=2 , then HΔG.

(منطوق فقط)

Note: The converse of this theorem is not true

For example : (G_s,o) , H=$\{r_1, r_4\}$

H Δ G_s but $[G_s:H] = 4 \neq 2$

Remark(3): If H Δ G, then H$\cap$ K$\not\Delta$ G $\wedge$ (H$*$K)$\not\Delta$ G

Where H and K are two subgroups of the group (G,$*$)

Consider (S_3,o)

$H=\{f_1\} \Delta S_3$, $K=\{f_1,f_4\} \not\Delta S_3$, then

$H*K=\{f_1,f_4\} \not\Delta S_3$

In (G_s,o) , $H=\{r_1,r_3,h,v\}$, $K=\{r_1,v\}$ s.t. $H\Delta G_s$, $K \not\Delta G_s$, then

$H\cap K=\{r_1,v\} \not\Delta G_s$.

Def(9). A group $(G,*)$ is called simple group iff G has no proper normal subgroup.

Ex(14).

1) (S_3,o) is not simple $H=\{f_1,f_2,f_3\} \Delta s_3$

2) (G_s,o) not simple since $H=\{r_2,r_4,v,h\}$ proper subgroup and $H\Delta G_s$.

3) $(Z_6,+_6)$ is not simple , $H=\{\bar{0},\bar{3}\} \Delta Z_6$

4) $(Z_3,+_3)$ is simple group since Z_3 has no proper normal subgroup. $\{0\} \Delta Z_3$ and $Z_3 \Delta Z_3$.

Def(10). Let $H\Delta G$ and $G\backslash H=\{x*H: x\in G\}$ 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(10): Let $H\Delta G$, then $(G|H,\otimes)$ is a group .

Proof: $G|H=\{a*H: a\in G\}$

Since $e*H=H\in G|H\neq\varphi$

Closure: Let $a * H , b * H \in G|H$

$$(a * H)\otimes(b * H) = (a * b) * H \quad \forall x, y \in G|H$$

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: $e * H = H \in G|H$

$$(a * H)\otimes(e * H) = (a * e) * H = a * H \quad \forall a * H \in G|H$$

$$(e * H)\otimes(a * H) = (e * a) * H = a*H$$

$\therefore$ e *H is an identity element of G|H.

Inverse: Let a* $H \in G|H$ $T.P.(a * H^{-1})=a^{-1}* H$

$(a * H) \otimes (a^{-1}* H) = (a * a^{-1}) * H = e * H = H$

$(a^{-1}* H) \otimes (a * H)=(a^{-1}* a) * H = e * H = H$

$\therefore \forall a * H \in G|H \quad \exists a^{-1}* H \in G|H.$

$\therefore$(G|H,$\otimes$) is a group.

Ex(15). (Z_6,$+_6$) , H={$\bar{0},\bar{3}$} , find Z_6|H **(if exist)**

$\because H\Delta\ Z_6 \Rightarrow Z_6|H$ 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.

$\otimes$	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	$\bar{1}+_6H$

H is an identity .

$(\bar{1}+_6H)^{-1}=(\bar{1})^{-1}+_6H=\bar{5}+_6H= \bar{2}+_6H$

$(\bar{2}+_6H)^{-1}=(\bar{2})^{-1}+_6H=\bar{4}+_6H=\bar{1}+_6H$

Ex(16). 1) $(Z_{20},+_{20})$, $H=<\bar{5}>$

Find $Z_{20}|H$ (if exist) **(H.W)**

2) (S_3,o) ,$H=\{f_1,f_2,f_3\}$

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 oH= {f_6,f_5,f_4}=f_4oH

∴S_3|H={H,f_4o H}

But if H={f_1,f_4} , H⊿S_3

∴S_3|H is not exist

Theorem(11): The quotient group of comm. group is comm.

Proof: Suppose (G,∗) is a comm. group and (H,∗) is a subgroup of (G,∗) such that HΔG.

∴G|H is a group.

Let $a * H , b * H \in G|H$

$(a * H)\otimes(b * H) = (a * b) * H$

$= (b * a) * H$ (since G is comm.)

$= (b * H)\otimes(a * H)$

∴ (G|H,∗) is a comm. group.

Theorem(12): If (G,∗) is a cyclic group , then (G|H,∗) is a cyclic group. منطوق فقط

The converse of this theorem is not true.

For example: (S_3,0) , H={f_1,f_2,f_3}ΔS_3

$\therefore S_3|H$ is a group.

$S_3|H=\{H, f_4 oH\}$

$o(S_3|H)=2$ (prime order)

$S_3|H$ is a cyclic group but $(S_3,0)$ is not cyclic.

$S_3|H=<f_4 oH>=\{f_4 \text{ o } H, (f_4 oH)^2\}$

$=\{f_4 oH, f_1 oH\}$

Theorem(13): Let $(G,*)$ be a group and $(G\backslash cent(G),\otimes)$ is a cyclic group. Then $(G,*)$ is comm. (بدون برهان)

The converse of this theorem is not true.

For example:

$G=\{e,a,b,c\} \ni a^2=b^2=c^2=e$

G is comm. (not cyclic)

$Cent(G)=G \Rightarrow G\backslash cent(G)= (G\backslash G) =\{G\}=\{e,a,b,c\}$

$\therefore G\backslash cent(G)$ is not cyclic.

Chapter 4

Isomorphic groups

(الزمر المتشاكلة او تشاكل الزمر)

Definition(1). Let $(G,*)$ and $(G',\circ)$ be two groups and $f:(G,*)\to(G',\circ)$ be a mapping, then f is called a homomorphism iff

$$f(\chi*\gamma)=f(\chi)\circ f(\gamma),\ \forall\chi,\gamma\in G.$$

Example(1). Let $f:(R,+)\to(R^+,.)$, s.t. $f(a)=2^a,\forall a\in R$. Is f a homomorphism map.?

Ans. Let $a,b\in R\Rightarrow f(a+b)=2^{a+b}=2^a.2^b=f(a).f(b)$

$\therefore f$ is a homomorphism map.

Example(2). Let $f:(Z,+)\to(Z,+)$, s.t. $f(x)=3x+2,\forall x\in Z$. Is f a homomorphism map.?

Ans. Let $x,y\in Z\Rightarrow f(x+y)=3(x+y)+2=3x+3y+2$ ... ... (1)

$$f(x)+f(y)=(3x+2)+(3y+2)=3x+3y+4\ldots..(2)$$

$$\Rightarrow(1)\neq(2)$$

$$\Rightarrow f(x+y)\neq f(x)+f(y)$$

$\therefore f$ is not a homomorphism map.

Example(3). Let $g:(S_3,\circ)\to(S_3,\circ)$, s.t. $g(x)=x,\forall x\in S_3$. Is g a homomorphism map.? **(H.W.)**

Example(4). Let $f:(Z_6,+_6)\to(Z_6,+_6)$, s.t. $f(\bar{x})=\bar{x},\forall x\in Z_6$. Is f a homomorphism map.? **(H.W.)**

Example(5). Let $f:(\mathrm{Z},+)\to(\{1,-1\},.)$, s.t.

$f(a)=\begin{cases}1 & if\ a\ is\ even\\ -1 & if\ \ a\ is\ odd\end{cases}\},\forall a\in Z$. Is f a homomorphism map.?

Ans. 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 $a,b\in E$:

$f(a+b)=1\quad$ (since $a+b\in E$)

$f(a).f(b)=1.1=1$

(2) If $a,b\in O\ \Rightarrow a+b\in E$

$f(a+b)=1$

$f(a).f(b)=-1.-1=1$

(3) If $a\in E\wedge b\in O\Rightarrow a+b\in O$

$f(a+b)=-1$

$f(a).f(b)=1.-1=-1$

In all cases $f(a+b)=f(a).f(b)$

$\therefore f$ is a homomorphism map.

Example(6). Let $f:(\mathrm{G},*)\to(\mathrm{G},*)$, s.t. $f(a)=x*a*x^{-1},\forall a\in G$. Is f a homomorphism map.?

Ans. Let $a,b\in G\Rightarrow f(a*b)=x*(a*b)*x^{-1}$ ... ... (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(7). Let $f:(\mathrm{G},*)\to(\mathrm{G}',\circ)$, s.t. $f(a)=e',\forall a\in G$. Is f a homomorphism map.?

Ans. Let $a, b \in G \Rightarrow f(a * b) = e' \ldots\ldots(1)$

And $f(a) \circ f(b) = e' \circ e' = e' \ldots\ldots(2)$

Then f is a trivial homomorphism map.

Example(8). Let HΔG and $f : (G,*) \to (G/H, \otimes)$, s.t.

$f(a) = a * H, \forall a \in G$. Is f a homomorphism map.?

Ans. Let $a, b \in G \Rightarrow f(a * b) = (a * b) * H \ldots\ldots(1)$

And $f(a) \otimes f(b) = (a * H) \otimes (b * H) = (a * b) * H \ldots\ldots(2)$

$\Rightarrow (1) = (2)$

$\therefore f$ is a homomorphism map.

Definition(2). 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) map.

(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) map.

Definition(3). 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(9). Let $(G = \{2^x : x \in Z\}, .)$, show that $(Z, +) \cong (G, .)$.

Ans. Define $f : (Z, +) \to (G, .) \quad s.t. \quad f(x) = 2^x, \forall x \in Z$

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 $f(x) = f(y)$ T.P. $x = y$

$f(x) = f(y)$

$2^x = 2^y \Longrightarrow x = y \Longrightarrow f$ 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.

$\therefore (Z, +) \cong (G, .)$.

Theorem(1). Let $f : (G, *) \to (G', .)$ be an isomorphism map. Then

(1) $f(e) = e'$, s.t. 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 Δ G and f is onto , then $f(H)$ Δ G′.

(6) If K Δ G′, then $f^{-1}(K)$ Δ G.

Proof.

(1) $f(e) = e'$

Let $a \in G \Rightarrow a * e = a$

$\Rightarrow f(a*e)=f(a)$ (f is map)

$\Rightarrow f(a).f(e)=f(a)$ (f is homo.).....(1)

Let $f(a)\in \mathrm{G}'$

$\Rightarrow f(a).e'=f(a)$ (def. of identity).....(2)

$(1)=(2)$, then

$f(a).f(e)=f(a).e'$

$\therefore f(e)=e'$ (by cancellation law).

... ...

(2) $f(a^{-1})=(f(a))^{-1}, \forall a\in G.$

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 $f(a)\in \mathrm{G}'$

$\Rightarrow f(a).\big(f(a)\big)^{-1}=e'$ ... ... (2)

$(1)=(2)$, 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 $(\mathrm{G},*)$, then $(f(\mathrm{H}),.)$ is a subgroup of a group $(\mathrm{G}',.)$.

Proof. $f(H)=\{f(x): x\in H\}\subseteq \mathrm{G}'$

$f(e)=e'\in f(H)\Rightarrow f(H)\neq \varphi$

Let $f(x),f(y)\in f(H)$ T.P. $f(x).f(y)^{-1}\in f(H)$

$f(x).f(y)^{-1}=f(x).f(y^{-1})$ (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, $f(x).f(y)^{-1} \in f(H)$

$\therefore$ $(f(\mathrm{H}),.)$ is a subgroup of a group $(\mathrm{G}',.)$.

… … … … … … … … … ..

(4)If $(K,.)$ is a subgroup of a group $(\mathrm{G}',.)$, then $(f^{-1}(\mathrm{K}),*)$ is a subgroup of a group $(\mathrm{G},*)$.

Proof. $f^{-1}(K) = \{x \in G: f(x) \in K\} \subseteq G$

Since $(K,.)$is a subgroup of a group $\mathrm{G}' \Rightarrow e' = f(e) \in K \Rightarrow e \in f^{-1}(K)$

So, $f^{-1}(K) \neq \varphi$

Let $x, y \in f^{-1}(\mathrm{K})$ T.P. $x * y^{-1} \in f^{-1}(K)$

$x \in f^{-1}(K) \Rightarrow f(x) \in K$

$y \in f^{-1}(K) \Rightarrow f(y) \in K$

Since $(K,.)$is a subgroup of a group G'

$\Rightarrow f(x).f(y)^{-1} \in K$

$\Rightarrow f(x).f(y^{-1}) \in K$

$\Rightarrow f(x * y^{-1}) \in K \Rightarrow x * y^{-1} \in f^{-1}(K)$

$\therefore$ $(f^{-1}(\mathrm{K}),*)$ is a subgroup of a group $(\mathrm{G},*)$.

… … … … … … … … … ..

(5)If $H \Delta \mathrm{G}$ and f is onto, then $f(\mathrm{H}) \Delta \mathrm{G}'$.

Proof. Suppose that $H \Delta \mathrm{G}$ and f is onto T.P. $f(H) \Delta \mathrm{G}'$

By (3), $(f(\mathrm{H}),.)$ is a subgroup of a group $(\mathrm{G}',.)$.

Let $y \in \mathrm{G}' \wedge a \in f(H)$ T.P. $y.a.y^{-1} \in f(H)$

$y \in \mathrm{G}'$ and f is onto, then $\exists x \in G \;\; s.t. \;\; f(x) = y$

$a \in f(\mathrm{H})$, 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 $H \;\Delta\; \mathrm{G}$, then $x * h * x^{-1} \in H$. It follows that $f(x * h * x^{-1}) \in f(H)$

$\therefore y.a.y^{-1} \in f(H) \Rightarrow f(\mathrm{H}) \;\Delta\; \mathrm{G}'.$

… … … … … … … … … ..

Theorem(2). The relation "isomorphic" is an equivalent relation.

Theorem(3).

(1) Every two finite cyclic groups of the same order are isomorphic.

(2) Every finite cyclic group is isomorphic to $(\mathrm{Z_n}, +_{\mathrm{n}})$.

(3) Every two infinite cyclic groups are isomorphic.

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

Definition(4). Let $(\mathrm{G},*)$ be a group, then

(1) $Hom(G) = \{ f \mid f: (\mathrm{G},*) \to (\mathrm{G},*) \;\ni f \; is \; homo. \}$

(2) $Aut(G) = \{ f \mid f: (\mathrm{G},*) \to (\mathrm{G},*) \;\ni f \; is \; isomo. \}$

Theorem (4). Let $(\mathrm{G},*)$ be a group, then

(1) $(Hom(G),\circ)$ is a 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) $Hom(G) = \{ f \mid f: (\mathrm{G},*) \to (\mathrm{G},*) \;\ni f \; is \; homo. \}$

$\exists \;\; i: (\mathrm{G},*) \to (\mathrm{G},*) \;\; \ni \;\; i(x) = x \;\; \forall x \in G$, and i is homo.

$\therefore \; Hom(G) \neq \varphi.$

Closure: let $f, g \in Hom(G)$ T.P. $f \circ g \in Hom(G)$

Since $f:(\mathrm{G},*)\to(\mathrm{G},*)\ \ni f\ is\ homo.$ and

$g:(\mathrm{G},*)\to(\mathrm{G},*)\ \ni g\ is\ homo.$

$\therefore\ f\circ g:(\mathrm{G},*)\to(\mathrm{G},*)\ \ is\ homo.$

$\therefore f\circ g\in Hom(G)$

Asso. Is true since $(f\circ g)\circ h=f\circ(g\circ h)$

Identity: $\exists\ i\in Hom(G)$ and $f\circ i=i\circ f=f\ \ \forall f\in Hom(G)$

It follows that $(Hom(G),\circ)$ is semigroup with identity.

… … … … … … … … ..

(3) $T.P.(Aut(G),\circ)$ is a subgroup of $(symm(G),\circ)$.

$Aut(G)=\{f|\ f:(\mathrm{G},*)\to(\mathrm{G},*)\ \ni f\ is\ isomo.\}$

$Symm(G)=\{f|f:(\mathrm{G},*)\to(\mathrm{G},*)\ \ni f\ is\ bij.\}$

Since $\exists\ i:(\mathrm{G},*)\to(\mathrm{G},*)\ \ni\ i(x)=x\ \ \forall x\in G$, and i is homo.

$\therefore Aut(G)\neq\varphi\ ,\ Aut(G)\subseteq Symm(G)$ and by (2) $(Aut(G),\circ)$ is a group.

$\therefore (Aut(G),\circ)$ is a subgroup of $(symm(G),\circ)$.

Definition(5). Let $(\mathrm{G},*)$ be a group and $x\in\mathrm{G}$. Define

$f_x:(\mathrm{G},*)\to(\mathrm{G},*)\ \ni f_x(a)=x*a*x^{-1}\ \ \forall a\in G$. Then f_x is called an inner automorphism of G and the set

$Inn(\mathrm{G})=\{f_x:\forall x\in\mathrm{G}\}$ or $I(\mathrm{G})=\{f_x:\forall x\in\mathrm{G}\}$ (تشاكل تقابلي داخلي)

Theorem (5). Let $(\mathrm{G},*)$ be a group and $x\in\mathrm{G}$, then

(1) f_x is an isomorphism map.

(2) $(I(\mathrm{G}),\circ)$ is a subgroup of $(Aut(G),\circ)$

(3) $I(\mathrm{G})\ \Delta\ Aut(G)$.

Proof. (1)T.P. f_x is (1-1) , onto and homo.

Let $f_x(a) = f_x(b),\ \forall a, b \in G$, then

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

$\Rightarrow a = b$ $\quad\therefore$ f_x is (1-1)

$R_{f_x} = \{ f_x(a): \forall\ a \in G\} = \{x * a * x^{-1}: \forall\ a \in G\} = G$

$\therefore$ f_x is onto

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

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

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

$\therefore$ f_x is homo. $\Rightarrow$ f_x is an isomo. Map.

… … … … … … … … ..

(2) $(I(\mathrm{G}),\circ)$ is a subgroup of $(Aut(G),\circ)$

Proof. T.P. $(I(\mathrm{G}),\circ)$ is a subgroup of $(Aut(G),\circ)$

$I(\mathrm{G}) = \{ f_x | f_x: (\mathrm{G},*) \to (\mathrm{G},*) \quad is\ an\ isomo. \}$

$Aut(G) = \{ f | f: (\mathrm{G},*) \to (\mathrm{G},*)\ \ni f\ is\ an\ isomo. \}$

Since $e \in \mathrm{G} \Rightarrow f_e \in I(G) \neq \varphi$

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

$\therefore I(\mathrm{G}) \subseteq Aut(\mathrm{G})$

Closure: Let f_x , $f_y \in I(\mathrm{G})$, T.P. $f_x \circ f_y \in I(\mathrm{G})$

$(f_x \circ f_y)(a) = f_x\left(f_y(a)\right) = f_x(y * a * y^{-1})$

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

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

$$= f_{x*y}(a) \in I(\mathrm{G})$$

Inverse: Let $f_x \in I(\mathrm{G})$

Since $x^{-1} \in G \Rightarrow f_{x^{-1}} \in I(\mathrm{G})$

$f_x \circ f_{x^{-1}} = f_{x*x^{-1}} = f_e \Rightarrow f_{x^{-1}} \circ f_x = f_{x^{-1}*x} = f_e$

$\therefore (f_x)^{-1} = f_{x^{-1}}$ $\therefore (I(\mathrm{G}),\circ)$ is a subgroup of $(Aut(G),\circ)$.

… … … … … … … … ..

(3) $I(\mathrm{G}) \Delta Aut(G)$.

Proof. We have $(I(\mathrm{G}),\circ)$ is a subgroup of $(Aut(G),\circ)$ and

$Aut(G) = \{ g | g: (\mathrm{G},*) \to (\mathrm{G},*) \ \ni g \ is \ an \ isomo. \}$,

$I(\mathrm{G}) = \{ f_x | f_x: (\mathrm{G},*) \to (\mathrm{G},*) \quad is \ an \ isomo. \}$.

Let $g \in Aut(G)$, $f_x \in I(\mathrm{G})$ T.P. $g \circ f_x \circ g^{-1} \in I(\mathrm{G})$

$(g \circ f_x \circ g^{-1})(a) = g \circ f_x\left(g^{-1}(a)\right)$

$= g[\, f_x\left(g^{-1}(a)\right)]$

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

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

$= f_{g(x)}(a) \in I(\mathrm{G})$

$\therefore I(\mathrm{G}) \Delta Aut(G)$

Definition(6). Let $f: (\mathrm{G},*) \to (\mathrm{G}',.)$ be a homomorphism, then the kernel of f is denoted by $kerf$ and defined as follows $kerf = \{x \in G | \ f(x) = e'\}$.

Example(9). Find $kerf$ for the following mappings:

(1) $f:(\mathrm{R},+)\to(\mathrm{R}^{+},.)\quad \ni f(x)=3^{x}$

Ans. f is homo. (Check)

$\Rightarrow kerf$ exist

$kerf=\{x\in R: f(x)=1\}=\{x\in R: 3^{x}=1\}=\{0\}.$

(2) $f:(\mathrm{G},*)\to(\mathrm{G}',.)\ \ni f$ is a trivial homo.

$f(x)=e'\quad \forall x\in G$

Since f is homo., then $kerf$ is exist

$kerf=\{x\in G\mid f(x)=e'\}=G$

(3) $f:(\mathrm{Z},+)\to(\mathrm{Z}_3,+_3)\quad \ni f(x)=[x]\ \forall x\in Z$

Ans. f is homo. (Check)

$kerf=\{x\in Z: f(x)=[0]\}=\{x\in Z: [x]=[0]\}$

$=\{x\in Z: x\equiv_3 0\}$

$=\{x\in Z: x=0+3k\ \forall k\in Z\}$

$=\{0,\bar{+}3,\bar{+}6,\ldots\}\subseteq Z$

Theorem (6). Let $f:(\mathrm{G},*)\to(\mathrm{G}',.)$ be a homomorphism, then

(1) $(kerf,*)$ is a subgroup of $(\mathrm{G},*)$

(2) $kerf\ \Delta\ \mathrm{G}$

(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 $a,b\in kerf$ T.P. $a*b^{-1}\in kerf$ T.P. $f(a*b^{-1})=e'$

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

$= f(a).\big(f(b)\big)^{-1}$

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

$\therefore\ f(a * b^{-1}) = e' \Rightarrow a * b^{-1} \in kerf$

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

(2) T. P. $kerf\ \Delta\ G$

By (1), $(kerf,*)$ is a subgroup of $(G,*)$

Let $x \in G$ and $a \in kerf$ T.P. $x * a * x^{-1} \in kerf$

(i.e.) T.P. $f(x * a * x^{-1}) = e'$

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

$= f(x).e'.\big(f(x)\big)^{-1}$

$= e'$

$\therefore\ x * a * x^{-1} \in kerf \Rightarrow kerf\ \Delta\ G$

(3) $kerf = \{e\}$ iff f is (1-1).

($\Rightarrow$) Suppose $kerf = \{e\}$ T.P. f is (1-1)

Let $f(a) = f(b)$

$\Rightarrow f(a).(f(b))^{-1} = f(b).(f(b))^{-1}$

$\Rightarrow f(a).f(b^{-1}) = e'$

$\Rightarrow f(a * b^{-1}) = e'$ (since f is a homo.)

$\Rightarrow a * b^{-1} \in kerf$

Since $kerf = \{e\} \Rightarrow a * b^{-1} = e \Rightarrow a = b$

$\therefore$ f is (1-1)

($\Leftarrow$) Suppose f is (1-1) T.P. $kerf = \{e\}$

Let $a \in kerf$ T.P. $a = e$

Since f is (1-1) , then $f(a) = f(e) \Rightarrow a = e$

$\therefore$ $kerf = \{e\}$.

The first fundamental theorem of isomorphism:

(النظرية الأساسية الأولى للتشاكل)

Let f: (G,$*$) $\rightarrow$ (G$'$,.) be an onto and homomorphism mapping, then

(G/$kerf$,$\otimes$) $\cong$ (G$'$,.) .

Proof. Since f is onto $\Rightarrow R_f = \{ f(a): a \in G\} =$ G$'$

Since $kerf$ Δ G $\Rightarrow$ (G/$kerf$,$\otimes$) is a group.

Define g: (G/$kerf$,$\otimes$) $\rightarrow$ (G$'$,.), such that $g(a * kerf) = f(a)$, $\forall a \in G$

T.P. g is map., (1-1), onto and homo.

g is map.

Let $a * kerf = b * kerf \Rightarrow a^{-1} * b \in kerf$

$\Rightarrow f(a^{-1} * b) = e'$

$\Rightarrow f(a^{-1}).f(b) = e'$

$\Rightarrow (f(a))^{-1}.f(b) = e'$

$\Rightarrow f(b) = f(a)$

$\Rightarrow g(b * kerf) = g(a * kerf)$

$\therefore$ g is map.

g is 1-1 ?

Let $g(a * kerf) = g(b * kerf)$

$\Rightarrow f(a) = f(b)$

$\Rightarrow e' = (f(a))^{-1}.f(b)$

$\Rightarrow e' = f(a^{-1}).f(b)$

$\Rightarrow e' = f(a^{-1} * b)$

$\Rightarrow a^{-1} * b \in kerf$

$\Rightarrow a * kerf = b * kerf$

$\therefore$ g is 1-1

g is onto ?

$R_g = \{\ g(a * kerf) : a \in G\} = \{f(a) : a \in G\} = G'$

$\therefore$ g is onto

g is homo. ?

$$g[(a * kerf) \otimes (b * kerf)] = g[(a * b) * kerf]$$

$$= f(a * b)$$

$$= f(a).f(b)$$

$$= g(a * kerf).g(b * kerf)$$

$\therefore$ g is homo.

$\therefore$ g is isomo.

$\Rightarrow (\mathrm{G}/ker f, \otimes) \cong (\mathrm{G}', .)$.

... ...

Corollary: Let $(\mathrm{G},*)$ be a group, then $(\mathrm{G}/cent(G), \otimes) \cong (\mathrm{I}(\mathrm{G}),\circ)$.

The second theorem of isomorphism:

Let $(H,*)$ and $(K,*)$ be two subgroups of $(G,*)$ such that $K \Delta G$, $(H * K,*)$ is subgroup of $(G,*)$, $K \Delta (H * K)$ and $(H \cap K) \Delta H$. Then

$(H * K/K, \otimes) \cong (\mathrm{H}/H \cap K, \otimes)$.

Proof. Since $K \Delta (H * K)$, then $(H * K/K, \otimes)$ is a group.

And since $(H \cap K) \Delta H$, then $(\mathrm{H}/H \cap K, \otimes)$ is a group.

Define $f: (H * K,*) \to (\mathrm{H}/H \cap K, \otimes)$ such that

$f(a * b) = a * (H \cap K) \quad \forall a \in H, b \in K$

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 ?

$R_f = \{\ f(a*b): \forall a \in H\} = \{a*(H\cap K): \forall a \in H\} = \mathrm{H}/H\cap K$

$\therefore\ f$ 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 theorem of isomo.

$\Rightarrow (H*K/kerf\ ,\otimes) \cong (\mathrm{H}/H\cap K\ ,\otimes)$.

$kerf = \{a*b \in H*K: f(a*b) = H\cap K\}$

$= \{a*b \in H*K: a*H\cap K = H\cap K\}$

$= \{a*b \in H*K: a \in H\cap K\}$

$= \{a*b \in H*K: a \in H\ \wedge a \in K\}$

$= \{a*b \in H*K: a \in k\ \wedge b \in K\} = K$

$\therefore \ (H * K/K, \otimes) \cong (\mathrm{H}/H \cap K, \otimes)$.

The third theorem of isomorphism:

Let $(H,*)$ and $(K,*)$ be two normal subgroups of $(G,*)$ such that $H \subseteq K$, then

(1) $H \Delta K$,

(2) $(\mathrm{K}/H, \otimes)\Delta(\mathrm{G}/H, \otimes)$

(3) $\left(\mathrm{G}/H \Big/ \mathrm{K}/H, \otimes\right) \cong (\mathrm{G}/K, \otimes)$.