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

2) The operations $\{+, -\}$arenotbinary operations onO **(**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 abinary 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 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 $(N, -), (R, \div), (O, +, -)$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) $(O, +), (Z, -), (E, -), (R\backslash\{0\}, \div)$ 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) ?

a∗ d=b ∗ c

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 $\exists e \in G\ \ s.t. a * e = e * a = a, \forall a \in G$.

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

$\Rightarrow e = a$ 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

$a * b = a + b + 2 \in Z$ →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 1.23:

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

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

Solution:

$\circ$	f_1	f_2	f_3	f_4
f_1	f_1	f_2	f_3	f_4
f_2	f_2	f_1	f_4	f_3
f_3	f_3	f_4	f_1	f_2
f_4	f_4	f_3	f_2	f_1

1- Closure is true.

For example: $f_1 \circ f_2 (x) = f_1(f_2(x))$

$= f_1(-x)$

$= - x = f_2$

2- Asso. is true. (H .W)

3- The identity : the identity element of G is f_1 , since

$f_1 \circ f_1 = f_1$, $f_2 \circ f_1 = f_2$, $f_3 \circ f_1 = f_3$, $f_4 \circ f_1 = f_4$.

4- The inverse:

$f_1^{-1} = f_1$, $f_2^{-1} = f_2$, $f_3^{-1} = f_3$, $f_4^{-1} = f_4$

Is (G , ∗) Comm . ??

Example 1.24

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

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

Prove that (G , ∗) is not comm . group

Solution:

1- Closure : let $(a, b), (c, d) \in G \Rightarrow a \neq 0, \; c \neq 0 \Rightarrow ac \neq 0$

$(a, b) * (c, d) = (ac, bc + d) \in G \;\; ac \neq 0$

2- Asso. : Let $(a, b), (c, d), (e, f) \in G$, 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-*Identity*: *Let* $(a, b), (x, y) \in G \ni$

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

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

$\therefore$ ax = a $\rightarrow x = 1$

$$bx + y = b \rightarrow b + y = b \rightarrow y = 0$$

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

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

$\therefore xa = a \rightarrow x = 1$

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

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

$$\therefore (1,0) \text{ is an identity element of } G$$

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

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

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

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

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

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

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

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

$(4,6) * (3,5) = (12, 23)$

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 $f_a, f_b \in F_G$, $a,b \in G$

$(f_a \circ f_b)(x) = f_a(f_b(x)) = f_a(b * x)$

$= a * (b * x)$

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

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

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

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

Since * is asso. on G

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

(3) identity : f_e is an identity of FG, since

$f_a \circ f_e = f_{a*e} = f_{e*a} = f_e \circ f_a = f_a$

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

$F_a \circ f_a^{-1} = f_{a*a^{-1}} = f_{a^{-1}*a} = f_a^{-1} \circ f_a = f_e$

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

<u>**(Exercises):**</u> 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 $e * a = a * e = a, \quad \forall a \in G$.

Proof:

Suppose that G has two identity elements e and $e^{/}$ that mean $\forall a \in G$.

$a * e = e * a = a$ 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

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

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 $a * x = x * a = e$
$a * x' = x' * a = e$

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

$\therefore \quad x = x' \Longrightarrow$ 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- $(a * b)^{-1} = a^{-1} * b^{-1} \Longleftrightarrow$ 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 ∈ G . To prove $a * b = b * a , \forall a , b \in G$

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

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

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

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

∴ 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 Th.4)

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

ii) if $a = a^{-1}$ then G is 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 $a * b \in G \Rightarrow (a * b) = (a * b)^{-1}$

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

$= b * a$

$\therefore$ G is comm. Group.

The converse of this part is not true.

(i-e.) if $(G, *)$ is comm . $\not\Rightarrow$ $a = a^{-1}$

For example:

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

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

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

Give another example (H. W.)

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

proof : we take

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

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

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

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

To show the solution is a unique

Let x' $\in$ G s.t. a $*$ x' = b

$\Longrightarrow$ a $*$ x' = a $*$ x

$\Longrightarrow$ x' = x (by com. law)

By same way, we prove $y * a = b$ has Solution $y = b * a^{-1}$.

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- $a^{n+1} = a^n * a \quad , n \in Z^+$.

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 ∈ Z , then :

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

Proof :

2- T.P. $(a^n)^m = a^{nm}$, $\forall n, m \in Z^+$

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

T.P. is true $\forall m \in Z^+$

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

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

∴ $(a^n)^k = a^{nk}$

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 - T.P. $a^{-n} = (a^{-1})^n = (a^n)^{-1}$, $\forall$ 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) : $(a^{-1})^{k+1} = (a^{k+1})^{-1}$?

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

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

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

4-($\Longrightarrow$) If n = 2 $\Longrightarrow$ $(a * b)^2 = a^2 * b^2$, T.P. G is 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 comm . group.

($\Longleftarrow$) Let G be comm . group . T.P $(a * b)^n = (a^n * b^n)$, $\forall$ n $\in$ Z.

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

I f n = 1 $\Longrightarrow (a * b)^1 = a^1 * b^1$ 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) : $(a * b)^{k+1} = (a * b)^k * (a * b)^1$

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

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

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

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

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

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

Definition: ((**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 $a \equiv b \pmod{n}$

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- $5 \not\equiv 2$ (mode2), 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.

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 $a \equiv b \pmod{n}$, T. P. $b \equiv a \pmod{n}$

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

T. P. $a \equiv c \pmod{n}$

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

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:

Let $a \in Z$, $n > o$. 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.)

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

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

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 ∈ Z : z ≡ 1 (mod 3) }

= { 1 , 1 ∓ 3, 1 ∓ 6 …. }

= { 1 , -2 , 4 , 7 , -5 , ….}.

[7] (H. W.)

Definition:

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

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

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] ∈ Z_n [a] $+_n$ [b] = [a $+_n$ b]

Similarly, we define multiplication on Z_n (write "$\cdot_n$ " by the following :

[a] $\cdot_n$ [b] = [a $\cdot_n$ b] , ∀ [a] , [b] ∈ Z_n

It is easy to see that (Z_n , $+_n$) is an abelian group with identity [0] and for every [a] ∈Z_n , $[a]^{-1}$ = [*n* – a] . This group is called the Additive Group of integers modulo *n* .

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

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

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

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

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

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

↓

$\therefore (Z_4, +_4)$ 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.

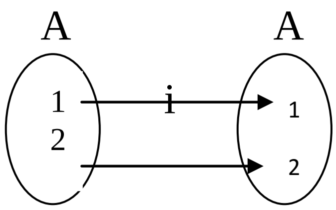
The Permutations : (التباديل)

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.

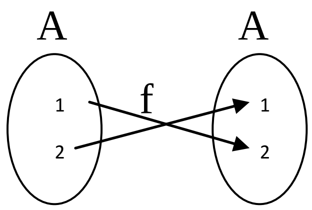
$$f : A \xrightarrow{1-1, onto} A$$

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

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) $\Rightarrow$ Symm(A) $\neq \varphi$.

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

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

$\Rightarrow fog: A \xrightarrow{1-1, onto} A \Rightarrow fog \in$ 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.

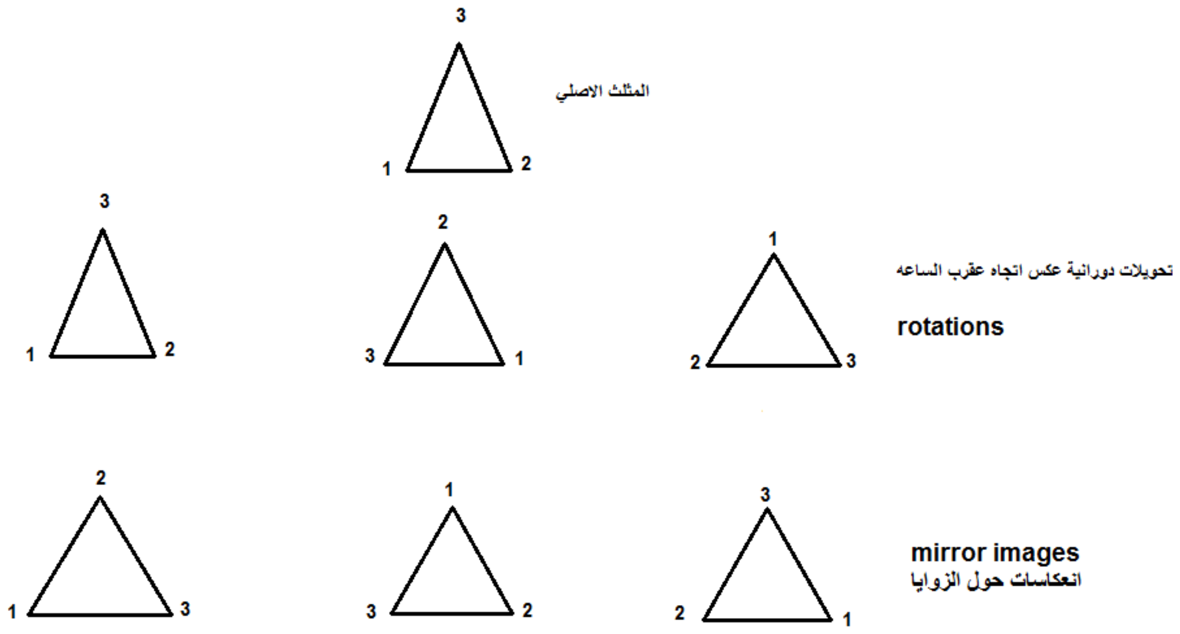
This group is called symmetric group.

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 .

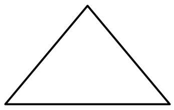
(زمرة تناظر المثلث متساوي الساقين)



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

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.

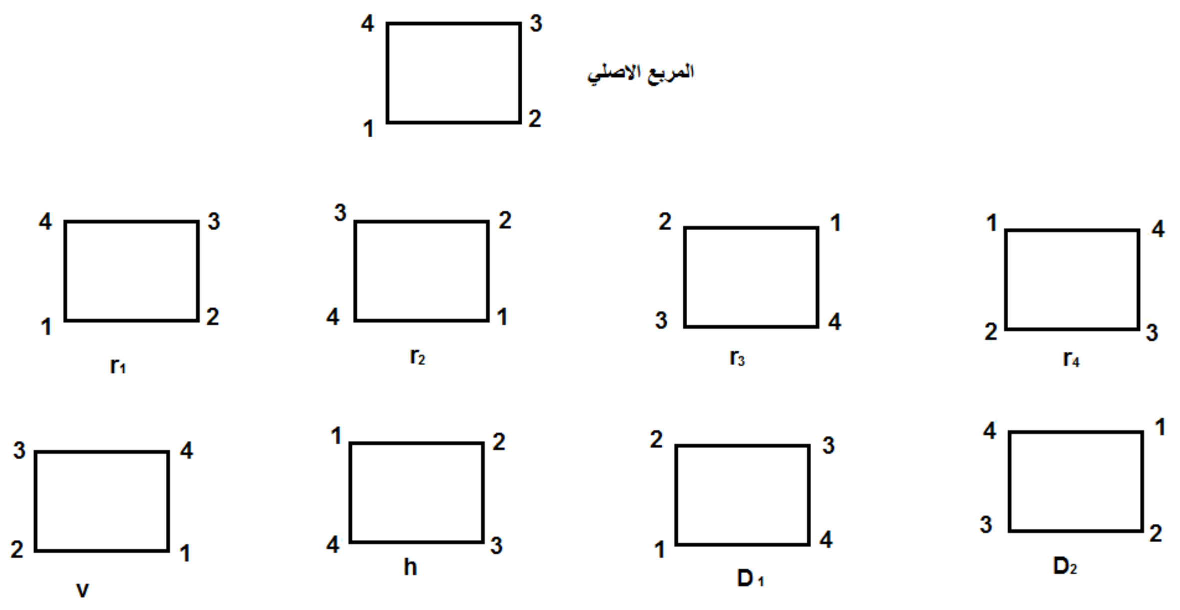


, $O(D_3) = (2)(3) = 6$ elements.

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.) $(a_1 a_2 \ldots a_n) = (a_1 a_2)(a_1 a_3) \quad \ldots..(a_1 a_n)$

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 agroup 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 agroup 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,$+_4$).

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 $a*b^{-1} \in H, \forall\, a, b \in H$

Proof:

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

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

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

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

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

(3) Let a∈ H and $b^{-1} \in H$ (by2) $\Longrightarrow a*(b^{-1})^{-1} \in H \Longrightarrow a*b \in H$

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

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

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

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

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

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

⟹(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 $\exists\, e \in H_i, \forall i \Longrightarrow e \in \cap H_i \Longrightarrow \cap H_i \neq \phi$

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

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)

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

∴ $(\cap H_i,*)$ 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 $i \Rightarrow e \in \cup H_i \Rightarrow \cup H_i \neq \phi$

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

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

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

$\therefore$ $(\cup H_i,*)$ 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 $\exists\ b \in H_2$, $b \notin H_1$

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

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

$\Rightarrow a, b \in H_1$ 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 asubgroup

If $H_1 \subseteq H_2 \Rightarrow H_1 \cup H_2 = H_2$ is asubgroup.

If $H_2 \subseteq H_1 \Rightarrow H_1 \cup H_2 = H_1$ is asubgroup

$\therefore H_1 \cup H_2$ is asubgroup 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 asubgroup of $(G,*)$.

Proof:

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

$$\therefore H*K \neq \phi$$

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

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

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

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

(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,∗)

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

Proof: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

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

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

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

$=a*(b*)*d^{-1}$(∗ is associative)

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

∴$x*y^{-1}$∈ H∗K

∴(H∗K,∗) is a 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 $+_8$K

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

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

(1)H∗K≠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∈G: c∗x =x∗c, ∀x∈G}   العناصر التي تتبادل مع كل عناصر الزمرة

Note (3):C(G)≠ϕ, since ∃e∈G s.t.

e∗x=x∗e ∀x∈G ⇒e∈ 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 agroup. Then $(cent(G),*)$ is a subgroupof $(G,*)$.

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 $b \in cent (G)$)

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

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

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

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

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

$\therefore$ (cent (G),$*$) is asubgroupof $(G,*)$

Theorem(7): Let $(G,*)$ be agroup. Then

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

Proof:

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

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

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

$\therefore$G is commutativegroup

($\Leftarrow$) suppose that G is commutative group T.P. cent(G) =G

(i.e) T.P. cent(G) $\subseteq G \wedge G \subseteq$ cent(G)

By definitionof cent(G) we havecent(G)$\subseteq$G.

T.P. 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 (5): Let (G,$*$) be agroup and $a \in G$, the cyclic subgroup of G generated by the a is denoted by $<a>$ and defined as

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

G=$<a>$ 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 groupgenerated 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 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 cyclic groupgenerated by $\bar{1}$

Examples (6): In (Z,+) fined cyclic groupgenerated by1, 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 groupgenerated 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 commutativegroup

The convers 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 commutativegroup

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 afinite group of order$n$generated by$a$, then G= $< a >$={a^k:k∈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 منتهية فتكتب بالشكل :

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

<$\bar{1}$>={$(\bar{1})^k$:k∈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. =<$\bar{1}$>ando(Z_n)= o($\bar{1}$)=n.

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

If a and b are integers with b>0, then there is a unique pair of integersqandr such that:

a =bq + r where 0 ≤ 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 quotientq and remainder r when 38 is divided by 7 according to the division algorithm.

Answer: 38=7(5)+3 0≤3≤7

∴q =5 and r=3

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

23=7(3)+2 0≤2≤7

q =3 ,r=2

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

15=(2)(7)+1 0≤1≤2

q =7 ,r=1

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

Proof: Let G be acyclic group generated by $a$and let H be asubgroup of G.

If H={e}, then H =<e>is cyclic

If H≠{e} and H≠G (H is proper subgroup)

Then

x∈H ⇒ x=a^m , m∈Z

x^{-1}∈H ⇒x^{-1} =a^{-m} , – m∈Z

Let m be aleast positive integer, such that $a^m \in H$

T.P. H=$<a^m> = \{(a^m)^g : g \in Z\}$

T.P. H⊆$<a^m>$∧$<a^m>$⊆H

Let y∈ H⇒y=a^s , s∈Z

By division algorithmof sand m

s =mg+r ⇒r=s – mg

∴$a^r = a^{s-mg} = a^s * (a^{-m})^g$ 0≤r≤m

∴a^r∈ H but 0≤r<m

r=0⇒s=mg

$$a^s = (a^m)^g \in < a^m >$$

∴y=$a^s \in <a^m>$⇒H⊆$<a^m>$

T.P.$<a^m>$⊆H

Let x∈$< a^m >$⇒x=$(a^m)^g$, g∈Z

$a^m \in H \Rightarrow (a^m)^g$ ∈H

∴x∈H⇒$<a^m>$⊆H

∴(H,∗) is cyclic subgroup.

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 afinite, o(G)=n

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

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

T.P.$m|n$(n=mg , g ∈ Z)

e ∈H ⇒a^n∈H,a^m∈H, by division algorithmof $n$and$m$

⇒n=mg+r   0≤r<m

r =n – mg⇒$a^r = a^n * (a^m)^{-g}$

⇒$a^r = (a^m)^{-g}$∈H

But 0≤r<m

⇒ If r=0 ⇒n=mg

∴$m|n$

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 finite groupsuch 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 1|12∧1|18 ⇒ 1|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.

Proof(1):

Suppose G=<a> T.P.G=<a^{-1}>

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

Let b$\in$ G $\ni$ G=<b>=$\{\ldots.,b^{-2},b^{-1},b^0,b^1,b^2,\ldots\}$

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

b$\in$G=<a>$\Rightarrow$ b=a^s,s $\in$ z …(2)

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

1=rs $\Rightarrow$ r=s=1 or r=s= – 1

If r=s=1 $\Rightarrow a$=b $\Rightarrow$ G=<a>

If r=s= – 1$\Rightarrow$ b=$a^{-1}$$\Rightarrow$ G=<a^{-1}>

Proof (2): Let (H,∗)be a subgroupof (G,∗) ∋ H≠ {e}T.P.(H,∗)is infinite

Suppose that (H,∗)is finite ∋o(H)=k

(H,∗)is cyclic subgroup

$H=<a^m>=\{(a^m)^1,(a^m)^2,\dots,(a^m)^k=e\}$

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

∴o(a)=o(G) c! متناقضه (G=<a>,G is finite)

∴(H,∗)is infinite.

Definition (9):H المجموعات المشاركة للزمرة الجزيئة

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

a∗H= {a ∗ h : h ∈ H}of G is the left coset of H containing a , while the subset

a∗H= {a ∗ h : h ∈ H} is the right cosetof 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 = H ∗ain 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∈G,then

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

Proof: e ∈ G, e∗H={e∗h:h ∈ 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 subgroupH of a group $(G,*)$ has the same number of elements as H.

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

Proof: Suppose $(a*H) \cap (b*H)=\phi$

T.P.$a*H = b*H$

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

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

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

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

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

or supposea$* H \neq b*H$ T.P.$(a*H) \cap (b*H)=\phi$

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

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

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

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

$\Rightarrow a*H = b*H$ 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: 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: $Z_6=\{\bar{0},\bar{1},\bar{2},\bar{3},\bar{4},\bar{5}\}$

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

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

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

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

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

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

$\therefore$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.

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 cosetsof H in G is called the index of H in G and denotedby [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):(LagrangeTheorem)

Let H be a subgroup of a finite group (G,∗).Then the order of H is adivisor of the order of G .

Proof:

Let G be afinite 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 $a_1* H,a_2*H, \dots,a_k*H$ are left cosets of H

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

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

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

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

mk=n ⇒ m|n ⇒o(H)| o(G)

Corollary (1): If $(G,*)$ is finite group, then the order of any element of G divides the orderof 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 afinite 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 $\Rightarrow o(a) | o(G)$

$\Rightarrow m | n$

$\Rightarrow n = mk$

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

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

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

Proof: Let $(G,*)$ be finite $\ni o(G) = p$

By corollary (1)of Lagrange theorem $\Rightarrow o(a) | p \quad \forall\, a \in G$.

$o(a) = 1$ 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 (4): Every group of order less than 6 is commutative.

Proof:

Let(G,*) be a finite group ∋o(G)<6

o(G)=1or 2 or 3 or4 or 5 or6

If o(G)=1 ⇒G={e} ⇒ G is commutative

If o(G)=2or 3 or 5

By corollary (3) of Lagrange theoremG is cyclic⇒G is commutative

Ifo(G)=4

∴ o(a) = 1 or 2 or 4

If o(a)=1 ⇒ a=e

If o(a) =2 ∀ a ∈ G⇒ a^2 =e ⇒a=a^{-1} ∀ a ∈ G

∴G is commutative group

If o(a)=4 ⇒o(a)= o(G) ⇒ G=<a>

∴G is cyclic ⇒ G is commutative group.

Exercises:

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

(2) Let (Z_8,$+_8$) be agroup and H=<$\overline{2}$>. 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 subgroupof (Z_{24},$+_{24}$). Also list the elements of each coset of H in Z_{24}.