محاضرات جبر الزمر

المرحلة الثانية

اعداد

م.م. هديل حازم سامي

Definition: Let S be a nonempty set, a binary operation * is a function from the Cartesian product **S × S into S**.

Mathematically: Let $S \neq \emptyset$ and $*: S \times S \to S$ is a function s.t. $*(a, b) = a * b$, $\forall a, b \in S$.

Example1: Let $+: N \times N \to N$ is a function that is a binary operation on N since $\forall a, b \in N$: $+(a, b) = a + b \in N$.

Example2: $.: R \times R \to R$ is a binary operation on R.

Example3: $\div: Z \times Z \to Z$ is not binary operation since $\forall a, b \in Z$: $\div(a, b) = a \div b \notin Z$.

Definition: a mathematical system (mathematical structure), is a nonempty set of elements with one or more binary operations defined on this set.

Example: (N,+,.) is a math. sys., (R,.,÷) is a math. sys. (Z,.,÷) is not math. sys.,

Question1: let S={1,-1,i,-i} s.t. $i^2=-1$. Is (S,.) construct a math. system where (.) is an ordinary multiplication?

Question2: If Z_e and Z_O denote the even and odd integers respectively, are $(Z_e,+,.)$ &$(Z_o,+,.)$ constitute mathematical system?

Definition: The operation * defined on the set S is said to be associative if, $(a * b) * c = a * (b * c)$: $a, b, c \in S$.

Example1: + is an associative operation on N,Z,Q and R. also (.). but (-) is not asso. operation on R.

Example2: Let * be an operation defined on Z s.t. $a * b = a + b + ab$: $a, b \in Z$. Show whether that * is an associative operation on Z.

Sol. Let $a, b, c \in Z$

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

L.S. $(a * b) * c = (a + b + ab) * c$

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

$$= a + b + ab + c + ac + bc + abc$$

R.S. $a * (b * c) = a * (b + c + bc)$

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

$$= a + b + c + bc + ab + ac + abc$$

$\because$ L.S = R.S.

$\therefore$ * is an ass. operation on Z

Definition: A semi group is a pair (S,*) consisting of a nonempty sets together with an associative binary operation * defined on S.

Example: Let Q be the rational numbers, define $a * b = \frac{1}{2}(a + b): a, b \in Q$.

prove if (Q,*) is a semi group or not?

Solution: $a * b = \frac{1}{2}(a + b): a, b \in Q$ then $a * b \in Q$

$\therefore *$ is closed

let $a, b, c \in Q$

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

L.S./ $a * (b * c) = a * \left[\frac{1}{2}(b + c)\right]$

$$= \frac{1}{2}[a + \left[\frac{1}{2}(b + c)\right] = \frac{1}{2}a + \frac{1}{4}b + \frac{1}{4}c$$

R.S./ $(a * b) * c = \frac{1}{2}(a + b) * c = \frac{1}{2}\left[\frac{1}{2}(a + b) + c\right]$

$$= \frac{1}{4}a + \frac{1}{4}b + \frac{1}{2}c$$

$\because$ L. S. $\neq$ R. S.

$\therefore$ * is not associative

Then (Q,*) is not semi group.

Definition: The system (S,*) is said to have a (two- sides) identity element for the operation * if there exists an element e in S such that:

$a * e = e * a = a$ for every $a \in S$

Example: (0) is the identity element for the systems (Z,+),(Q,+),(R,+) and (1) for (N,.),(Z,.),(Q,.),(R,.).

$(Z_e,.)$ has not identity element

Example2: Let $S = \{a + b\sqrt{2} : \quad a, b \in Z\}$ is the system $(S,.)$ has an identity element?

Sol. $\forall\ a + b\sqrt{2} \in S \quad \exists\ e_1 + e_2\sqrt{2} \in S$, s.t.

$$(a + b\sqrt{2})(e_1 + e_2\sqrt{2}) = (e_1 + e_2\sqrt{2})(a + b\sqrt{2}) = (a + b\sqrt{2})$$

L.S. / $(a + b\sqrt{2})(e_1 + e_2\sqrt{2}) = a + b\sqrt{2}$

$$ae_1 + 2be_2 + (ae_2 + be_1)\sqrt{2} = a + b\sqrt{2}$$

$$ae_1 + 2be_2 = a \ldots \ (1) \quad \rightarrow e_1 = \frac{a - 2be_2}{a} \ \ldots (3)$$

$$ae_2 + be_1 = b \ \ldots \ (2)$$

Substitute 3 in 2 we get

$$ae_2 + \frac{ba - 2b^2e_2}{a} = b$$

$a^2e_2 + ba - 2\,b^2e_2 - ba = 0$

$(a^2 - 2\,b^2)e_2 = 0$

$\rightarrow e_2 = 0$

$\rightarrow e_1 = 0$

R.S./ Similar

H.W. Is $(Z^+,.)$ has identity?

Definition: Let **(S,*)** be a mathematical system with identity element e. An element $a \in S$ is said to have a (two – sides) inverse under the operation * if there exists some number $a^{-1} \in S$ such that:

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

In particular, since e*e=e we may infer that $e^{-1} = e$.

Example: Consider the set G={1,2,3}, and * is a function defined by the operation table. Find the inverse for each element?

*	1	2	3
1	1	2	3
2	2	3	1
3	3	1	2

Definition: A group is a pair (G,*) consisting of a nonempty set G and a binary operation * defined on G, satisfying the following conditions:

1) G is closed under the operation *.
2) The operation * is associative.
3) G contains an identity element e for the operation *.
4) Each element a of G has an inverse $a^{-1} \in G$ relative to *.

Definition : The pair (G,*) is a group if and only if (G,*) is a semi group with identity in which element of G has an inverse.

Example1: (Z,+) ,(Q,+),(R,+), (Q-{0},.), (R-{0},.) are all groups.

Example2: G=R/{1}, a* b=a + b – ab , show that (G, *) is a group.

Sol.: 1) Since $a + b - ab \in G$ then $a * b \in G \rightarrow$ $(G,*)$is a mathematical system.

2) let $a, b, c \in G \rightarrow (a * b) * c = a * (b * c)$

L.S./ $(a * b) * c = (a + b - ab) * c = (a + b - ab) + c - (a + b - ab)c$

$$= a + b - ab + c - ac - bc + abc$$

R.S./ $a * (b * c) = a * (b + c - bc) = a + (b + c - bc) - a(b + c - bc)$

$$= a + b + c - bc - ab - ac + abc$$

$\therefore$ * is an associative operation on G.

3) a*e=e*a=a

$\text{L.S.})\ a * e = a \rightarrow a + e - ae = a$ (by cancellation law

$\rightarrow (1 - a)e = 0 \rightarrow e = 0 \in G$

$\text{R.S.})\ e * a = a \rightarrow e + a - ea = a$ (by cancellation law

$\rightarrow e(1-a)=0 \rightarrow e=0 \in G$

∴ (G,*) has an identity element e=0.

4) $a * a^{-1} = a^{-1} * a = e$

L.S.) $a * a^{-1} = e \rightarrow a * a^{-1} = 0 \rightarrow a + a^{-1} - aa^{-1} = 0$

$\rightarrow (1-a)a^{-1} = -a$

$\rightarrow a^{-1} = \frac{-a}{1-a}$

R.S.) $a^{-1} * a = e \rightarrow a^{-1} * a = 0 \rightarrow a^{-1} + a - a^{-1}a = 0$

$\rightarrow a^{-1}(1-a) = -a$

$\rightarrow a^{-1} = \frac{-a}{1-a} \in G$

∴ (G,*) is a group

<u>Example2</u>: let $G = \{(x,y): x,y \in R\}$ and $*$ defined on G as:

$$\forall (x,y),(a,b) \in G \text{ then } (x,y) * (a,b) = (x+a, y+b)$$

Show that (G,*) is a group.

Sol: 1) $R \neq \emptyset \rightarrow G \neq \emptyset$

Let $(x,y),(a,b) \in G$ *such that* $a,b,x,y \in R$

$$\rightarrow (x,y) * (a,b) = (x+a, y+b) \in G$$

Since $x+a, y+b \in R$

∴ G is a closed under *.

2) let $(x,y),(a,b),(c,d) \in G$, $x,y,a,b,c,d \in R$

L.S.) $[(x,y)*(a,b)]*(c,d) = (x+a, y+b)*(c,d) = (x+(a+c), y+(b+d))$

$$= \big(x+(a+c), y+(b+d)\big) = (x,y)*(a+c, b+d)$$

$$= (x,y)*[(a,b)*(c,d)] = R.S$$

∴ * is associative on G.

3) Let $(x,y) \in G$, $x,y \in R$ s.t.

$(x,y)*(e_1,e_2) = (x,y) \rightarrow (x+e_1, y+e_2) = (x,y)$

$\rightarrow x + e_1 = x \ , y + e_2 = y$

$\rightarrow e_1 = x - x \ \ , e_2 = y - y$

$\rightarrow \ e_1 = 0, e_2 = 0$

$\rightarrow (e_1, e_2) = (0,0) \in G$

Similarly $(e_1, e_2) * (x, y) = (x, y)$

$\therefore (e_1, e_2) = (0,0) \in G$ is an identity element.

4)let $(a, b) \in G$, $a, b \in R$ and

$$(a, b) * (c, d) = (e_1, e_2)$$

$$\rightarrow \ (a, b) * (c, d) = (0,0)$$

$$\rightarrow (a + c, b + d) = (0,0)$$

$$\rightarrow a + c = 0 \ , \ \ b + d = 0$$

$$\rightarrow c = -a \ , \quad d = -b$$

$$\rightarrow (c, d) = (-a, -b)$$

$\therefore (-a, -b)$ is the inverse element of (a,b).

Then (G,*) is a group.

<u>Definition</u>: If A is an arbitrary set, then the set whose elements are all the subsets of A is known as the power set of A and denoted by P(A):

$P(A) = \{B : B \subseteq A\}, P(A) = 2^n$.

<u>Note</u>: 1) If $A = \emptyset \rightarrow P(A) = \{\emptyset\}$

2) If $x \in A \rightarrow \{x\} \subseteq A \rightarrow \{x\} \in P(A)$.

3) Since $\emptyset \subseteq A$ and $A \subseteq A$ we always have $\{\emptyset, A\} \subseteq P(A)$.

4) If A is a finite set with (n) elements then P(A) is itself a finite set having 2^n elements.

<u>Example</u>: Suppose the set A={1,2,3}, then P(A) $=\{\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\}$.

<u>Example</u>: Suppose the set A={a,b} and Δ is a symmetric difference operation defined on A. Is (P(A),Δ) constitute a group?

Δ	∅	{a}	{b}	{a,b}

$\emptyset$	$\emptyset$	$\{a\}$	$\{b\}$	$\{a,b\}$
$\{a\}$	$\{a\}$	$\emptyset$	$\{a,b\}$	$\{b\}$
$\{b\}$	$\{b\}$	$\{a,b\}$	$\emptyset$	$\{a\}$
$\{a,b\}$	$\{a,b\}$	$\{b\}$	$\{a\}$	$\emptyset$

H.w.

1) prove if $(P(A),\cup)$ is a group or not?

2) suppose that $a \in R - \{0,1\}$ and consider the set $G = \{a^k : k \in Z\}$. Is (G,.) constitute a group.

Theorem1: Let (G,*) be a group , $a \in G$ and $m, n \in Z$. the powers of a obey the following laws of exponents:

1) $a^n * a^m = a^{n+m} = a^m * a^n$
2) $(a^n)^m = a^{nm} = (a^m)^n$
3) $a^{-n} = (a^n)^{-1}$
4) $e^n = e$

Definition: the operation * defined on the set S is called commutative if a*b=b*a for every pair of elements $a, b \in S$.

Example1: Let S=Z , a*b=a+b-1

Solution: let $a, b \in Z$ S.T:

a*b=a+b-1=b+a-1=b*a

$\therefore *$ is a commutative.

Example2: Let S=R/{0} , a*b $= \frac{a}{b}$ then * is not comm. operation.

Definition: Let (G,*) be a group, if * is a commutative operation on G then (G,*) is called a commutative group.

Example: (Z,+), (R,+), (Q,+), (Q/{0},.),(R/{0},.) are comm. group.

Example2: Take the set G as consisting of the six function $f_1, f_2, \ldots f_6$, where for all $x \in R - \{0,1\}$ we define $f_1(x) = x$, $f_2(x) = \frac{1}{x}$, $f_3(x) = 1 - x$, $f_4(x) = \frac{x-1}{x}$, $f_5(x) = \frac{x}{x-1}$, $f_6(x) = \frac{1}{1-x}$

Is $(G,\circ)$ be a commutative group.?

Solution:

$\circ$	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_1	f_6	f_5	f_4	f_3
f_3	f_3	f_4	f_1	f_2	f_6	f_5
f_4	f_4	f_3	f_5	f_6	f_2	f_1
f_5	f_5	f_6	f_4	f_3	f_1	f_2
f_6	f_6	f_5	f_2	f_1	f_3	f_4

From the table:

1) $(G,_o)$ is a math. sys.
2) $_o$ is as associative operation on G.
3) $e = f_1$
4) $(f_1)^{-1} = f_1, (f_2)^{-1} = f_2, (f_3)^{-1} = f_3, (f_4)^{-1} = f_6, (f_5)^{-1} = f_5, (f_6)^{-1} = f_4.$

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

5) L. S) $(f_2 \,_o\, f_3)(x) = f_2[f_3(x)]$

$$= f_2[1-x] = \frac{1}{1-x} = f_6(x)$$

R. S) $(f_3 \,_o\, f_2)(x) = f_3[f_2(x)]$

$$= f_3\left(\frac{1}{x}\right) = 1 - \frac{1}{x} = \frac{x-1}{x} = f_4(x)$$

$\because$ L. S $\neq$ R. S

$\therefore (f_2 \,_o\, f_3) \neq (f_3 \,_o\, f_2)$

$\therefore$ $_o$ is not comm. operation on G.

$\therefore$ the group $(G,_o)$ is not commutative.

H.W). Let $M = \{\begin{bmatrix} a & b \\ c & d \end{bmatrix}, a, b, c, d \in R\}$ and * define on M as:

$\forall \begin{bmatrix} a & b \\ c & d \end{bmatrix}, \begin{bmatrix} x & y \\ z & w \end{bmatrix} \in M$ then

$\begin{bmatrix} a & b \\ c & d \end{bmatrix} * \begin{bmatrix} x & y \\ z & w \end{bmatrix} = \begin{bmatrix} a+x & b+y \\ c+z & d+w \end{bmatrix}$ show that (M,*) is a commutative group?

<u>**Theorem2**</u>: The identity element of a group (G,*) is unique, and each element of a group has inverse element.

Proof: Let (G,*) be a group has two identity element e_1 and e_2 then $\forall\ a \in G$:

$a * e_1 = e_1 * a = a\ \ldots(1)$

and

$a * e_2 = e_2 * a = a\ \ldots(2)$

Equality (1) and (2) we have

$a * e_1 = a * e_2 \to e_1 = e_2$

So, the identity element of a group (G,*) is unique.

To show that an element of a group (G,*) has exactly one inverse, we assume that $a \in G$ such that a has two inverse element a_1^{-1} *and* a_2^{-1} then

$a * a_1^{-1} = a_1^{-1} * a = e \ldots(3)$

$a * a_2^{-1} = a_2^{-1} * a = e \ldots(4)$

Equality (3) and (4) we have

$a * a_1^{-1} = a * a_2^{-1} \ldots.(5)$

Multiply both sides of (5) from the left by a_1^{-1} *or* a_2^{-1} we have

$(a_1^{-1} * a) * a_1^{-1} = (a_1^{-1} * a) * a_2^{-1}$

$\to e * a_1^{-1} = e * a_2^{-1}$

$\to a_1^{-1} = a_2^{-1}$

$\therefore$ each element of a group (G,*) has exactly one inverse element.

Corollary: If (G,*) is a group then $(a^{-1})^{-1} = a\ \ \forall\ a \in G$.

Proof: Let $a \in G,$ since (G,*) is a group then $\exists\ a^{-1} \in G\ s.t.$

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

Now, since $a^{-1} \in G, then\ \exists\ (a^{-1})^{-1} \in G\ s.t.$

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

From (1) and (2) we have

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

$\to a^{-1}$ has two inverse elements a and $(a^{-1})^{-1}$

But from (theorem 2) each element of a group (G,*) has exactly one inverse element.

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

Example : let G={1,-1,i,-i} s.t. $i^2=-1$ and (.) is a binary operation on G. find $i^{-1}, (-1)^{-1}, (i^{-1})^{-1}, (-i^{-1})^{-1}$

Lemma: If $a, b, c, d \in G$ and (G,*) is a semi group then (a*b)*(c*d)=a*((b*c)*d)

Proof: L.S.) (a*b)*(c*d)

Let m=c*d

⇒(a*b)*(c*d)= (a*b)*m =a*(b*m) [since * associative]

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

R.S.) a*((b*c)*d)= a*((b*(c*d)) [since * associative]

Let m=c*d

⇒ a*(b*m) = (a*b)*m [since * associative]

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

∴ (a*b)*(c*d)=a*((b*c)*d)

Theorem3: If (G,*) is a group, then $(a * b)^{-1} = b^{-1} * a^{-1}\ \forall\, a, b \in G$.

Proof: ⇒ clearly $(a * b) * (a * b)^{-1} = (a * b)^{-1} * (a * b) = e$

⇐ $(a * b) * (b^{-1} * a^{-1}) = \big((a * b) * b^{-1}\big) * a^{-1}$ [*from the lemma*]

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

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

Corollary: If (G,*) is a commutative group, then $(a * b)^{-1} = a^{-1} * b^{-1}\ \ \forall\, a, b \in G$.

Proof: Since (G,*) is a group then $(a * b)^{-1} = b^{-1} * a^{-1}$ [by th.3]

But $b^{-1} * a^{-1} = a^{-1} * b^{-1}$ [* comm. operation]

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

H.W. Let G denotes the set of all ordered pairs of real numbers. If the binary operation * is defined on the set G by the rule

$(a, b) * (c, d) = (ac, bc + d)$ then show that (G,*) is not commutative group? And find

$((1,3) * (2,4))^{-1}$, $(2,4)^{-1} * (1,3)^{-1}$

Theorem4: (Cancellation law)

If a,b and c are elements of a group (G,*) such that either a*c=b*c or c*a=c*b then a=b.

Proof: since $c \in G$ and (G,*) is a group then $c^{-1} \in G$ exists

Multiplying the equation a*c=b*c both of sides from the right by c^{-1} we obtain

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

Then by associative law this becomes $a*(c*c^{-1}) =b*(c*c^{-1})$

$\Rightarrow$ a * e=b*e

$\Rightarrow$ a=b

Similarly we can show that c*a=c*b implies a=b.

Theorem5: In a group (G,*) the equation a*x=b and y*a=b have a unique solution.

Proof: Let $x = a^{-1} * b$

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

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

To show the solution is unique, let $x' \in G$ such that $a * x' = b$

$\Rightarrow a * x' = a * x$ [by cancellation law]

$\Rightarrow x' = x$

Corollary : In a multiplication table for a group, each element appears exactly once in each row and column.

Proof: let $a, b \in \mathrm{G}$ and let $x_1 \neq x_2 \in \mathrm{G}$ s.t.

$$a * x_1 = b$$

$$a * x_2 = b$$

$$\therefore a * x_1 = a * x_2$$

By theorem (5) we get $x_1 = x_2$.

Problems

1) Given a,b are element of a group (G,*) with a*b=b*a show that $(a * b)^k = a^k * b^k \; for \;\; k \; \in Z.$

   Proof:

   If k=1

   $\Rightarrow (a * b)^1 = a * b$

   If k=2

   $\Rightarrow (a * b)^2 = (a * b) * (a * b)$

   $= a * a * b * b \quad (since \; a * b = b * a)$

   $= a^2 * b^2$

Let k=r is true

$\Rightarrow (a * b)^r = a^r * b^r$

Now , we will prove when k=r+1

$\Rightarrow (a * b)^{r+1} = a^{r+1} * b^{r+1}$

$= a^r * b^r * a * b$

$= a^r * a * b^r * b \quad (since \; a * b = b * a)$

$= \; a^{r+1} * b^{r+1}$

$\therefore \; (a * b)^k = a^k * b^k$

2) Given $a^2 = e$ for every element a of the group (G,*). show that the group must be a commutative.

   Proof: let $a, b \in G \; \ni a^2 = e \, , b^2 = e$

   $a^2 * b^2 = e * e = e \ldots (1)$

   $\because a \in G \, , b \; \in G \; \Rightarrow a * b \; \in G$ ($*$ is closed)

   $(a * b)^2 = e \ldots (2)$

   $from$ (1)&(2)$we \; get$

   $a^2 * b^2 = (a * b)^2$

   $a * a * b * b = (a * b) * (a * b)$

   $a * (a * b * b) = a * \big(b * (a * b)\big) \quad (by \; cancellation \; law)$

   $(a * b) * b = (b * a) * b$

   $a * b = b * a$

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

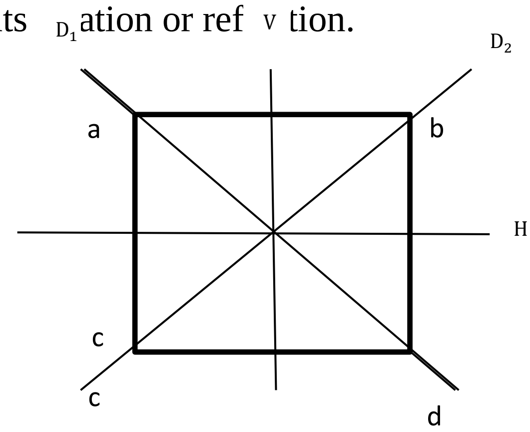
3) Suppose that $G = \{1, \frac{-1+\sqrt{3}\,i}{2}, \frac{-1-\sqrt{3}\,i}{2}\}$ and (.) is the ordinary multiplicative operation show whether that (G,.) constitutes a group or not?

   Sol.:

.	1	$\frac{-1+\sqrt{3}\,i}{2}$	$\frac{-1-\sqrt{3}\,i}{2}$
1	1	$\frac{-1+\sqrt{3}\,i}{2}$	$\frac{-1-\sqrt{3}\,i}{2}$
$\frac{-1+\sqrt{3}\,i}{2}$	$\frac{-1+\sqrt{3}\,i}{2}$	$\frac{-1-\sqrt{3}\,i}{2}$	1
$\frac{-1-\sqrt{3}\,i}{2}$	$\frac{-1-\sqrt{3}\,i}{2}$	1	$\frac{-1+\sqrt{3}\,i}{2}$

The group of symmetries of a square

The eight symmetries of the square are
$G = \{R_{360}, R_{90}, R_{180}, R_{270}, H, V, D_1, D_2\}$ and (o) is an operation on G represents D_1 ation or ref V tion.



o	R_{90}	R_{180}	R_{270}	R_{360}	H	V	D_1	D_2
R_{90}	R_{180}	R_{270}	R_{360}	R_{90}	D_1	D_2	V	H
R_{180}	R_{270}	R_{360}	R_{90}	R_{180}	V	H	D_2	D_1
R_{270}	R_{360}	R_{90}	R_{180}	R_{270}	D_2	D_1	H	V
R_{360}	R_{90}	R_{180}	R_{270}	R_{360}	H	V	D_1	D_2
H	D_2	V	D_1	H	R_{360}	R_{180}	R_{270}	R_{90}
V	D_1	H	D_2	V	R_{180}	R_{360}	R_{90}	R_{270}
D_1	H	D_2	V	D_1	R_{90}	R_{270}	R_{360}	R_{180}
D_2	V	D_1	H	D_2	R_{270}	R_{90}	R_{180}	R_{360}

⇨ (G, o) is a group but is not comm. Group.

(Permutation) or Symmetric

Definition: Let A be a non-empty set, then every (1-1) and onto map is called (permutation)or symmetric on A and denoted by:

$$\mathrm{symm}(A) = \left\{ f : f : A \underset{(onto)}{\overset{(1-1)}{\longrightarrow}} A \right\} \text{the set of all permute on A.}$$

Example: Let A={x,y} write all permute on A.

Solution: $\mathrm{symm}(A) = \left\{ f : f : A \underset{(onto)}{\overset{(1-1)}{\longrightarrow}} A \right\}$

$$\mathrm{symm}(A) = \{i_A, f\} = \{\begin{pmatrix} x & y \\ x & y \end{pmatrix}, \begin{pmatrix} x & y \\ y & x \end{pmatrix}\}$$

Remark:

1) If A is a finite set, then $\mathrm{symm}(A)$ is a finite.
2) If A contains n elements (finite), then $\mathrm{symm}(A)$ contains n! elements.
3) We shall written $\mathrm{symm}(A)$ as S_n or P_n where A contains (n) elements.
4) The identity element for (P_n, o) is the permutation $\begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix}$.
5) The multiplicative inverse of any permutation $f \in S_n$ is described by $f^{-1} = \begin{pmatrix} f(1) & \dots & f(n) \\ 1 & \dots & n \end{pmatrix}$.

Example: If A={1,2,3} write all permute on A. then show (P_3, o) is a group of symmetric.

Solution: $P_n = P_3 = 3! = 6$

$$f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, f_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, f_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, f_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix},$$

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

$$\therefore P_3 = \{\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, f_6 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}\}$$

(P_3, o) is a group ? H.W

Definition: Let $n_1, n_2, \dots, n_k$ distinct integers between 1 and n. if a permutation $f \in S_n$ such that:
$f(n_i) = n_{i+1}$ for $1 \le i < k$
$f(n_k) = n_1$ and $f(n) = n \quad \forall\, n \notin (n_1, n_2, \dots, n_k)$

Then f is said to be a k- cycle or a cycle of length k.

In the symmetric group (P_5, o)

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 2 & 4 & 3 \end{pmatrix} = (2 \quad 5 \quad 3) \qquad 3-\text{cycle}$$

also

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 2 & 3 & 5 \end{pmatrix} = (1 \quad 4 \quad 3 \quad 2) \qquad 4-\text{cycle}$$

- The cycles can be multiplied by the functional composition operation thus in (P_5, o)we have

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

$f(1)=5$, $f^2(1) = f\big(f(1)\big) = f(5) = 3$

$f^3(1) = f\big(f^2(1)\big) = f(3) = 1$

Find $f^2(2)$.

Definition : the simplest of permutation are $2-$cycle this called transposition.

$1-$cycle $\rightarrow$ Identity permutation.

Corollary: every permutation may be expressed as the product of transpositions that is:

(1,2,…,k0=(1k)(1k-1)…(12)

Example: $f = (1 \quad 2 \quad 4 \quad 3) = (13)(14)(12)$

Note: A permutation of a finite set is even or odd a according to weather it can be expressed as a product of an even number of transposition or the product of an odd number of transposition.

Example: (123)=(13)(12) even

Definition : A group (G,*) is said to be cyclic if there exists an element $a \in G$ such that every element of G is of the form a^k for some integer k.

Such that an element a is called a generator of the group. The cyclic group G is denoted by G=(a). that is

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

Note: if the binary operation is (+) then the cyclic group is written by $G = \{ka : k \in Z\}$.

Example1: (Z,+) is a cyclic group generated by 1 &-1. that is

$$Z = \{k(1): k \in Z\} \quad \& \; Z = \{k(-1): k \in Z\}.$$

Example 2: let G={1,-1,I,-i} and (.) is an ordinary multiplicative operation. Show that (G,.) is a cyclic group?

Solution: (G,.) is a group

(G,.) is a cyclic group generated by I &-i

The Group Of Integers Modulo n :

Definition: let n be a fixed positive integer. Two integers a and b are said to be congruent modn, written: $a \equiv b\,(\text{mod} n)$ if and only if the difference (a-b) is divisible by n. that is

$$a \equiv b(\text{mod} n) \leftrightarrow a - b = kn \text{ for some } k \in Z$$

For example, if n=7 we have $3 \equiv 24(\text{mod} 7) \rightarrow 3 - 24 = 7k \text{ for some } k \in Z$

$$\rightarrow k = \frac{-21}{7} = -3$$

Example2: $10 \not\equiv 4(\text{mod} 5)$ since $10 - 4 \neq 5k$ for some $k \in Z$

Note/if a-b is not divisible by n we say that a is in congruent to b modulo n and in this case, write $a \not\equiv b(\text{mod} n)$

Definition: Division algorithm

Let a and b be integers with b>0 then there exist unique integers q and r with property that a=bq+r where $0 \leq r < b$.

If b/a then r=0 that is a=bq.

Example: let a=19 & b=5 then 19=5(3)+4 $\quad 0 \leq 4 < 5$

Theorem6: let n be a fixed positive integer and a,b be arbitrary integers. Then $a \equiv b \pmod n$ iff a and b have the same remainder when divided by n.

Proof: suppose that $a \equiv b \pmod n$

⇨ a=b+kn for some integer k.

On division by n,b leaves a certain remainder r :

b=qn+r where $0 \leq r < n$, $q \in Z$.

thus a=b+kn = (qn+r)+kn

=(q+k)n+r

Which shows a has the same remainder as b.

Conversely:

Let $a = q_1 n + r$ and $b = q_2 n + r$ with the same remainder $0 \leq r < n$.

Then

$a - b = (q_1 n + r) - (q_2 n + r) = (q_1 - q_2)n$ with $(q_1 - q_2) \in Z$

Hence, n is a factor of a-b and so $a \equiv b \pmod n$

Theorem7: let n be a fixed positive integer and a,b,c arbitrary integers. Then

1) $a \equiv a \pmod n$
2) if $a \equiv b \pmod n$ then $b \equiv a \pmod n$
3) if $a \equiv b \pmod n$ and $b \equiv c \pmod n$ then $a \equiv c \pmod n$.
4) if $a \equiv b \pmod n$ and $c \equiv d \pmod n$ then $a + c \equiv b + d \pmod n$, $ac \equiv bd \pmod n$
5) if $a \equiv b \pmod n$, then , $ac \equiv bc \pmod n$.
6) if $a \equiv b \pmod n$, then $a^k \equiv b^k \pmod n$ for every positive integer k.

proof(1): for any integer a, since a-a=0.n $0 \in Z$

⇨ $a \equiv a \pmod n$

Proof(2): if $a \equiv b \pmod n$ then a-b=kn, $k \in Z$

⇨ a-b=kn] (-1)

⇨ - (a-b)=-kn

⇨ - (a+b)=(-k)n

⇨ b-a =(-k)n where $-k \in Z$

⇨ $b \equiv a \pmod{n}$

Proof(3): if $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$ then a-b=kn and b-c=hn, for some $k, h \in Z$

⇨ a-b=kn … (1)

b-c=hn …(2)

a-c= kn+hn

⇨ a-c =(k+h)n , $(k+h) \in Z$

⇨ $a \equiv c \pmod{n}$

Proof(4): if $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$ then $a - b = k_1 n$ & $c - d = k_2 n$ for some integers $k_1, k_2 \in Z$.

Now (a+c)-(b+d)= (a-b)+(c-d)

= $k_1 n + k_2 n = (k_1 + k_2)n$, $(k_1 + k_2) \in Z$

⇨(a+c)-(b+d)= $(k_1 + k_2)n$

⇨ $(a + c) \equiv (b + d) \pmod{n}$

Also/ $ac = (b + k_1 n)(d + k_2 n)$

$$= bd + (bk_2 + dk_1 + k_1 k_2 n)n$$

Since $(bk_2 + dk_1 + k_1 k_2 n)$ is integer

∴ $ac = bd + k_3 n$ where $k_3 = bk_2 + dk_1 + k_1 k_2 n$

⇨ $ac = bd = k_3 n$

⇨ $ac \equiv bd \pmod{n}$.

Proof(5): if $a \equiv b \pmod{n}$ then a-b=kn, $k \in Z$

and $c \equiv c \pmod{n}$ for $0 \in Z$ then ac - bc=(a-b)c

= knc

= (kc)n , $kc \in Z$

∴ $ac \equiv bc \pmod{n}$.

Proof(6): we prove (6) by inductive argument

Since $a \equiv b \pmod{n}$ ⇨ $a^1 \equiv b^1 \pmod{n}$

⇨ the statement true for k=1.

Assuming it holds for an arbitrary k, we must show that it also holds for k+1.

Since $a^k \equiv b^k \pmod{n}$ and $a \equiv b \pmod{n}$ from (4)

⇨ $a^k a \equiv b^k\, b \pmod{n}$

⇨ $a^{k+1} \equiv b^{k+1} \pmod{n}$

$\therefore\ a^k \equiv b^k \pmod{n} \quad , k \in Z^+.$

Definition: Congruence class

Let $a \in Z$ the set of all integers congruent to a module n is denoted by [a] where

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

$$[a] = \{x \in Z : x \equiv a + kn,\ k \in Z\}$$

[a] is called the congruence class of a.

Example: suppose that we are dealing with congruence modulo 3. Then find [0], [1], [-7].

Solution:

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

$$= \{x \in Z : x = 3k\ ,\ \ k \in Z\}$$

$$= \{\dots, -9, -6, -3, 0, 3, 6, 9, \dots\}$$

Theorem 8: Let $n \in N$ then there is n of equivalent classes.

i.e. there is [0], [1], [2],…,[n-1] of equivalent classes.

Note: the set of all congruence classes is denoted by Z_n where

Z_n= {[0], [1], [2],…,[n-1]}

For example, if n=4 then Z_4= {[0], [1], [2],[3]} s.t.

$$[0] = \{\dots, -8, -4, 0, 4, 8, 12, \dots\}$$

find [1], [2], [3]

Theorem 9: Len n be a positive integer and Z_n be defined as $Z_n = \{[0], [1], [2], \ldots, [n-1]\}$,

then:

1) For each $[a] \in Z_n$, $[a] \neq \emptyset$.
2) If $[a] \in Z_n$ and $[b] \in Z_n$, then $[a] = [b]$ that is, any element of the congruence class [a] determines the class.
3) For any $[a], [b] \in Z_n$ where $[a] \neq [b]$ then $[a] \cap [b] = \emptyset$.
4) $\cup \{[a] : a \in Z\} = Z$.

Definition: A binary operation $(+_n)$ may be defined on Z_n as follows:

For each $[a], [b] \in Z_n \Rightarrow [a] +_n [b] = [a + b]$

Theorem10: For each positive integer n, the mathematical system $(Z_n, +n)$ forms a commutative group, known is the (group of integers module n).

Proof: let $[a], [b] \in Z_n$

1) $[a] +_n [b] = [a + b] \in Z_n$
   $\therefore (Z_n , +_n)$ is a mathematical system
2) $[a] +_n ([b] +_n [c]) = [a] +_n ([b + c]$

$$= [a + (b + c)] = [(a + b) + c]$$

$$= [a + b] +_n [c] = ([a] +_n [b] +_n [c]$$

$\therefore +_n$ is associative operation on Z_n.

3) $\forall [a] \in Z_n, \exists [0] \in Z_n$ s.t.
   $[a] +_n [0] = [a + 0] = [a] = [0 + a] = [0] +_n [a]$
   $\therefore [0]$ is the identity element of $+_n$
4) If $[a] \in Z_n$, then $[n - a] \in Z_n$ and $[a] +_n [n - a] = [a + +(n - a)] = [n] = [0]$
   So that $[a]^{-1} = [n - a]$
5) $[a] +_n [b] = [a + b] = [b + a] = [b] +_n [a]$
   $\therefore (Z_n , +_n)$ is a commutative group.

Example: show that $(Z_4 , +_4)$ is a comm. group.

Note: for simplicity, it is convenient remove the brackets in the designation of the congruence classes of Z_n. thus we often write $Z_n = \{\{0,1,2, \ldots , n - 1\}$

H.W./ Let $G = \{(a, b) : (a, b^n) \in Z_2\}$show that $(G, +)$is a group?

Subgroups

Definition: Let (G,*) be a group and $\emptyset \neq H \subseteq G$. The pair (H,*) is said to be a subgroup of (G,*) if (H,*) is itself a group.

Example1: If Z_e and Z_o denote the sets of even and odd integers respectively then (Z_e,+) is a subgroup of the group (Z,+) while (Z_o,+) is not.

Example2: consider $(Z_6, +_6)$ the group of integers modulo 6. If H={0,2,4} then $(H, +_6)$ *is* a subgroup of $(Z_6, +_6)$.

Note: each group (G,*) has at least two subgroups ({e},*) and (G,*), these subgroups are known trivial subgroup and any subgroup different from these subgroup known proper subgroup.

Theorem11: Let (G,*) be a group and $\emptyset \neq H \subseteq G$ then (H,*) is a subgroup of (G,*) iff $a, b \in H$ implies $a * b^{-1} \in H$.

Proof: ⇒) Let (H,*) is a subgroup of (G,*) we have prove $a * b^{-1} \in H$

Let $a, b \in H$ then $a, b^{-1} \in H$

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

⇦) Let $a * b^{-1} \in H$ then

1) The operation * in H is a associative binary operation because H subset of G.
2) Let $a, b \in H \Rightarrow a * b^{-1} \in H$
   If a=b $\Rightarrow b * b^{-1} \in H \Rightarrow e \in H$
3) $\because b \in H$ and $e \in H \Rightarrow e * b^{-1} \in H \Rightarrow b^{-1} \in H$
4) Let $a \in H$ and $\because\ b^{-1} \in H \Rightarrow a * (b^{-1})^{-1} \in H \Rightarrow a * b \in H$

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

Example: $(Z_{12}, +_{12})$ is a group let H={0,4,8} then $(H, +_{12})$ is a subgroup of $(Z_{12}, +_{12})$ according (theorem11) since::

$\mathbf{(0)^{-1} = 0}$ $\mathbf{, (4)^{-1} = 8,}$ $\mathbf{(8)^{-1} = 4}$

$0 * (4)^{-1} = 0 +_{12} 8 = 8 \in H$

$0 * (8)^{-1} = 0 +_{12} 4 = 4 \in H$

$\vdots$

That is $a, b \in H$ $a +_{12} b^{-1} \in H$

Center of a group

Definition : let (G,*) be a group the center of G is the center(G) and denoted by cent (G) s.t. :

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

Note: $\text{cent}(G) \neq \emptyset$ since $\exists$ $e \in G$ s.t.

$$e * x = x * e, \forall\, x \in G \rightarrow e \in \text{cent}(G)$$

Theorem 12: Let (G,*) be a group then cent (G)=G iff G is a comm. group .

Theorem 13: let (G,*) be a group then (cent(G),*) is a subgroup of (G,*).

Proof: $\text{cent}(G) \neq \emptyset$ since $e \in \text{cent}(G)$

Let $a, b \in \text{cent}(G)$

$\therefore$ a*x = x*a , b*x = x*b $\forall\, x \in G$ [by definition of cent(G)]

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

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

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

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

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

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

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

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

Theorem 14: If (H_i, *) is the collection of subgroups of (G,*) then $(\cap H_i, *)$ is also subgroup of G.

Proof: 1) $\cap H_i \neq \emptyset$ since $\exists$ $e \in H_i$, $\forall i$

$\Rightarrow e \in \cap H_i$

2) let $x, y \in \cap H_i \Rightarrow x, y \in H_i$, $\forall i$

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

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

$\Rightarrow (\cap H_i, *)$ is also subgroup of G.

Example: $(Z_{15}, +_{15})$ is a group and $H_1 = \{0,3,6,9,12\}, H_2 = \{0,5,10\}$ are subgroups of Z_{15} then

$H_1 \cap H_2 = \{0\} \rightarrow (H_1 \cap H_2, +_{15})$ is subgroups of Z_{15}

$H_1 \cup H_2 = \{0,3,5,6,9,10,12\}$

$(H_1 \cup H_2, +_{15})$ is not subgroups of Z_{15}

<u>Theorem15</u>: Let $(H_1,*)$ and $(H_2,*)$ are two subgroups of $(G,*)$. Then $(H_1 \cup H_2,*)$ is a subgroup of $(G,*)$ if and only if $H_1 \subseteq H_2$ or $H_2 \subseteq H_1$.

<u>Proof</u>: $\Rightarrow$) Let $H_1 \subseteq H_2$ and let $a, b \in H_1$

$\therefore a * b^{-1} \in H_1$ (since $(H_1,*)$ is a subgroup)

$\therefore a * b^{-1} \in H_1$ (since $H_1 \subseteq H_2$)

Similarly if $H_2 \subseteq H_1$

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

$\Leftarrow$) Let $(H_1 \cup H_2,*)$ is a subgroup and let $H_1 \nsubseteq H_2$ or $H_2 \nsubseteq H_1$

Let $a \in H_1$ and $a \notin H_2$ $(a \in H_1 - H_2)$

$b \in H_2$ and $b \notin H_1$ $(b \in H_2 - H_1)$

Now let $a * b \in H_1$ (since $(H_1,*)$ is a subgroup)

$\therefore a^{-1} * (a*b) \in H_1$

$(a^{-1} * a) * b \in H_1$

$e * b \in H_1 \rightarrow b \in H_1$ C!

also $a * b \in H_2$ (since $(H_2,*)$ is a subgroup)

$\therefore$ $(a * b) * b^{-1}) \in H_2 \rightarrow a \in H_2$ C!

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

Example: (Z,+) is a group , ((2),+) and ((4),+) are subgroups of the group (Z,+).

Since $((4),+) \subseteq ((2),+)$ then (by the. 15) $\big((2) \cup (4), +\big) = ((2), +)$ is subgroup of the group (Z,+).

<u>Definition</u>: If $(G,*)$ is a group and $a \in G$ write $(a) = \{a^k : k \in Z\}$, then $((a),*)$ is called the cyclic subgroup of the group $(G,*)$ generated by a.

Example1: (Z,+) is a group and $(2) = \{2k : k \in Z\}$

⇨ (2)={ …, -4,-2,0,2,4,6,…}

Then ((2),+) is a cyclic subgroup of (Z,+).

Example2: $(Z_{12},+_{12})$ is a group ,

$(3) = \{3k \bmod 12 \ , k \in Z\}$

={0,3,6,9} thus $((3),+_{12})$ is a cyclic subgroup of $(Z_{12},+_{12})$.

Example3: the group of symmetries of the square is not cyclic but the subgroup:

$(R_{90})= \{ R_{90}, R_{180}, R_{270}, R_{360}\}$ is cyclic generated by the element R_{90}.

Theorem16: If ((a),*) is a finite cyclic group of order n then $(a)=\{e,a,a^2,\dots, a^{n-1}\}$.

Example: $(Z_{15},+_{15})$ is a group

$(5)= \{ 5^k , k \in Z\}$

$=\{5k : k \in Z\}$

$=\{0,5^1,5^2\}$

={0,5,10}

⇨$((5), +_{15})$ is a cyclic group.

Theorem17: Every subgroup of a cyclic group is a cyclic.

Example: (Z,+) is a cyclic group generated by 1, -1 so Z=(1)=(-1)

Then by the **theorem 16** ((4),+) is a cyclic subgroup of (Z,+) also ((2),+), ((3),+) and in general ((n),+) is a cyclic subgroup of (Z,+)where $n \in Z^+ \cup \{0\}$.

Definition: let (G,*) be a group and (H,*), (K,*) are two subgroups of G then the product of H and K is the set $H * K = \{h * k: h \in H, k \in K\}$.

Remark:

1) $H*H= H^2$
2) If H={a} then H*K=a*K, if K={b} then H*K= H*b.
3) $H*K \subseteq G$
4) $H \cup K \subseteq H*K$.

Example: In the group of symmetries of the square, consider the subgroups $H=\{R_{360}, D_1\}$ and $K=\{R_{360},V\}$ then

$H*K = \{ R_{360} \circ R_{360}, R_{360} \circ V, D_1 \circ R_{360}, D_1 \circ V \}$

$= \{ R_{360}, V, D_1, R_{270} \}$

(H*K, o) is not subgroup of G.

<u>Theorem18:</u> Let (G,*) be a group and (H,*), (K,*) are two subgroup of (G,*) then (H*K, *) is

a subgroup of (G,*) iff H*K= K*H.

<u>Proof</u>: suppose (H*K, *) is a subgroup of (G,*)

to prove H*K= K*H we should prove $H*K \subseteq K*H$ and $K*H \subseteq H*K$

let $x \in H*K \Rightarrow x = a*b \ni a \in H, b \in K$

$\because H*K$ is a subgroup of G.

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

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

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

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

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

Let $y \in K*H \Rightarrow y = f*g \ni f \in K, g \in H$

$\because K*H$ is a subgroup of G.

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

$y^{-1} = h*l \ni h \in K \wedge l \in H$

$y = (y^{-1})^{-1} = (h*l)^{-1} = l^{-1}*h^{-1} \ni l^{-1} \in H \wedge h^{-1} \in K$

$y = l^{-1}*h^{-1} \in H*K$

$\Rightarrow$ H*K= K*H

Conversely: let H*K= K*H

1) $H*K \neq \emptyset$ since $e=e*e \in H*K$
   Also $H*K \subseteq G$

Now, let $x,y \in H*K$, T. P. $x*y^{-1} \in H*K$

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

$y \in H * K \Rightarrow y = c*d \ni c \in H \wedge d \in K$

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

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

$\because$(H,*), (K,*) are two subgroup of (G,*) $\Rightarrow b*d^{-1} \in K$ & $c^{-1} \in H$

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

But H*K= K*H

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

Now, $a * (b*d^{-1}) * c^{-1} = (a * p) * q \in H * K$

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

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

Example: $(Z_{12},+_{12})$ is a comm. Group, H={0,6} and K={0,4,8} such that $(H,+_{12})$and $(K,+_{12})$ are subgroups of $(Z_{12},+_{12})$ show that $(H*K, +_{12})$ is a subgroup of $(Z_{12},+_{12})$.

$H+_{12}K=\{0,2,4,6,8,10\}$

$\therefore (H*K, +_{12})$ is a subgroup of $(Z_{12},+_{12})$.

Definition: Let (H,*) be a subgroup of the group (G,*) and let $a \in G$ then the set $a * H = \{a * h : h \in H\}$ is called a left coset of H in G and $H * a = \{h * a : h \in H\}$ is called right coset of H in G and a representative $a * H$ and $H * a$.

If the group (G,*) is commutative then $a * H = H * a$.

Example: let $(Z_{10},+_{10})$ be a group and H={0,5} be a subgroup of $(Z_{10},+_{10})$ find all cosets of H in Z_{10}.

Theorm19: let (H,*) be a subgroup of (G,*) and $a \in G$ then :

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

Proof: since $e \in G$

$\Rightarrow e * H = \{e * h : h \in H\} = H$

2) IF ((G,*) is a belian 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.

Example: (S_3, o) , $H=\{f_1,f_5,f_6\}$, $a = f_4$

f_4 o $H= \{ f_4, f_2, f_3\}$, H o $f_4=\{f_4, f_2, f_3\}$

$\Rightarrow f_4$ o $H= H$ o f_4

but (S_3, o) is not a belain group

3) $a\in a * H$
Proof: since $e\in H$
$\Rightarrow a=a*e\in a * H$

Theorem20: If $(H,*)$ is a subgroup of the group $(G,*)$ then $a*H=H$ if and only if $a \in H$.

Proof: suppose that $(H,*)$ is a subgroup of the group $(G,*)$ such that $a*H=H$ since $e \in H$ and for every $a \in G$ we have $a = a * e \in a * H$.

But $a*H=H$ hence $a \in H$.

Conversely: Let $a \in H$ to prove that $a*H=H$.

Let $x\in a*H\Rightarrow x=a*h$ for some $h \in H$

Since $a \in H$ and $h \in H \Rightarrow a * h \in H$ {(H,*) is a subgroup}

Hence $x \in H$

$\therefore a * H \subseteq H$ ... (1)

Now, Let $h \in H \Rightarrow h = e * h = (a * a^{-1}) * h = a * (a^{-1} * h)$

Since $a \in H \Rightarrow a^{-1} \in H$ {(H,*) is a subgroup}

$\Rightarrow a^{-1} * h \in H$

Then $a * (a^{-1} * h) \in a * H$

Hence $h \in a * H$

$\therefore H \subseteq a*H$ … (2)

From (1) & (2) we have $a*H=H$.

Theorem21: If $(H,*)$ is a subgroup of the group $(G,*)$ then $a*H=b*H$ if and only if $a^{-1} * b \in H$.

Proof : Let $a*H=b*H$ then we have to prove $a^{-1} * b \in H$ that mean

$\exists\, h_1, h_2 \in H$

$\Rightarrow a * h_1 = b * h_2$

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

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

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

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

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

Conversely: Let $a^{-1} * b \in H$ we have to prove that a*H=b*H

$\Rightarrow a^{-1} * b * H = H$ (By theorem 20)

$\Rightarrow$ let $h_3, h_4 \in H$

$\Rightarrow a^{-1} * b * h_3 = h_4$

$\Rightarrow (a * a^{-1}) * b * h_3 = a * h_4$

$\Rightarrow b * h_3 = a * h_4$

$\Rightarrow b * H = a * H$

Theorem22:

If (H,*) is a subgroup of the group (G,*) then left(right) cosets of H in G form a partition of the set G.

Example: consider (Z_{12},$+_{12}$) the group of integer modulo 12. If we take H={0,4,8}, Then (H, $+_{12}$) is a subgroup of (Z_{12},$+_{12}$) the left cosets of H in Z_{12} are

$$0 +_{12} H = H = 4 +_{12} H = 8 +_{12} H$$

$$1 +_{12} H = \{1,5,9\} = 5 +_{12} H = 9 +_{12} H$$

$$2 +_{12} H = \{2,6,10\} = 6 +_{12} H = 10 +_{12} H$$

$$3 +_{12} H = \{3,7,11\} = 7 +_{12} H = 11 +_{12} H$$

$$H \cup 1 +_{12} H \cup 2 +_{12} H \cup 3 +_{12} H = Z_{12}$$

Also

$$H \cap 1 +_{12} H \cap 2 +_{12} H \cap 3 +_{12} H = \emptyset$$

Thus the left (cosets) of H in Z_{12} form a partition of the set Z_{12}.

Definition : If (H,*) is a subgroup of (G,*) the index of H is the number of coset (left or right) of H in G which is denoted by r.

Definition : the number of elements in a group (G,*) is called the order of G.

Theorem23: (Lagrang theorem)

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

That is order (G)=index(H). order(H)

Or o(G)=o(H).r

Proof: suppose G be a finite group ∋ $o(G) = n$ and H be a subgroup of G ∋ $o(H) = m$.

Let r is the index of H in G

Let $a_1 * H, a_2 * H, \dots, a_r * H$ are left cosets of H.

$$a_1 * H \cup a_2 * H \cup \dots \cup a_r * H = G$$

and

$$a_1 * H \cap a_2 * H \cap \dots \cap a_r * H = \emptyset$$

$$o(a_1 * H) + o(a_2 * H) + \cdots + o(a_r * H) = o(G)$$

$$m + m + \cdots + m = n$$

$$\Rightarrow rm = n$$

$$\Rightarrow r.o(H)=o(G)$$

Example: let G={1,-1,i,-i} , (G,.) is a group and H={1,-1} where (H,.) is a subgroup of (G,.). The left cosets of H are

1.H={1,-1}=H

-1.H={-1,1}=H

i.H={i,-i}

-i.H={i,-i}

∴ the distinct left cosets of H are {1.H, i.H}

∴index H=2 and by Lagrange's theorem

o(G)=o(H).r

$$r=\frac{o(G)}{o(H)}=\frac{4}{2}=2$$

Definition: A subgroup (H,*) of the group (G,*) is said to be normal (or invariant) in (G,*)iff every left coset of H in G is also a right coset of H in G that is a*H=H*a for every a ∈ G.

Example: The subgroup ((4),$+_{12}$) is normal in Z_{12} since:

Left H=(4)={0,4,8}

$$0+_{12} H = H \quad , H+_{12} 0 = H$$

$$1+_{12} H = \{1,5,9\}, \quad H+_{12} 1 = \{1,5,9\}$$

$$2+_{12} H = \{2,6,10\}, \quad H+_{12} 2 = \{2,6,10\}$$

$$\vdots$$

$$\therefore a+_{12} H = H+_{12} a \qquad \text{for every } a \in H$$

Remarks:

1) Every subgroup of a commutative group is normal.
2) We denote for any normal subgroup (H,*) of (G,*) by HΔG.
3) {e}ΔG.
4) cent(G)ΔG.

Definition: If (H,*) is a normal subgroup of the group (G,*) then we shall denote the collection of distinct cosets of H in G by G/H:

$$G/H = \{a * H : a \in G\}$$

A rule of composition ⊗ may be defined on G/H by the formula

(a*H) ⊗ (b*H)=(a*b)*H $\quad \forall a, b \in G$

∴ (G/H,⊗) is called quotient group of G by H.

Theorem 24: let HΔG. then (G/H,⊗) is quotient group.

Proof: 1) $\forall\, a, b \in G$ s.t:

(a*H) &(b*H) ∈ G/H

Then (a*H) ⊗ (b*H)=(a*b)*H ∈ G/H

Since $a * b \in G$ [(G,∗)is a group]

$\therefore$ $(G/H,\otimes)$ is a mathematical system.

2) Let $a, b, c \in G$ s.t.:

$$[(a*H) \otimes (b*H)] \otimes (c*H) = (a*H) \otimes [(b*H) \otimes (c*H)]$$

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

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

$\therefore \otimes$ is associative operation on G/H.

3) Identity $e*H=H \in G/H \quad \forall\ a*H \in G/H$

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

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

4) $\forall\ a*H \in G/H\ \exists\ a^{-1}*H \in G/H$

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

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

$\therefore$ $(G/H,\otimes)$ is quotient group

Example: Let $(Z_6, +_6)$ and H={0,3} find Z_6/H? then prove $(Z_6/H, \otimes)$ is a quotient group.

Sol./ Z_6/H={H,1+H, 2+H}

$\otimes$	H	1+H	2+H
H	H	1+H	2+H
1+H	1+H	2+H	H
2+H	2+H	H	1+H

Homomorphism

Definition: Let (G,*) and (G',o) be two groups and f is a function from G into G' i.e $f: G \to G'$ then f is said to be a homomorphism from (G,*) into (G',o) if and only if

$$f(a*b)=f(a) \text{ o } f(b)$$

$$\text{where } a, b \in G$$

Example1: Define the function $f: (R, +) \to (R-\{0\}, .)$ by $f(a) = 2^a\ \ \forall a \in R$

Is f homo.?

Sol./ $f(a+b) = 2^{a+b}$

$= 2^a . 2^b$

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

$\Rightarrow$ f is homo.

Example2: Define the function f: $(Z,+) \to (Z,+)$ by $f(x)=x$ $\forall x \in Z$, is f homo.?

Sol.: L.s/ $f(x+y)=x+y=f(x)+f(y)$

$\Rightarrow$ f is homo.

Example3: Define the function f: $(R^+,.) \to (R,+)$ by $f(x)=e^x$ $\forall x \in R^+$, is f homo

Sol.: let $x, y \in R^+$

$\Rightarrow f(x+y)=e^{x.y}$

$\neq e^x + e^y$

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

$\therefore$ f is not homo.

Example4: Suppose that (G,*) and (G',o) are two subgroups with identity elements e and e' respectively. The function $f: G \to G'$ given by f(a)=e' for each $\forall a \in G$ is a homo.

f(a*b)=e'=e' o e'=f(a) o f(b)

$\therefore$ f is trivial homo.

Example5: let f: $(G,*) \to (G,*)$ defined by $f(a)=x*a*x^{-1}$ $\forall a \in G$, prove that f is a homo.

Sol. Let $a, b \in G$ then

L.S./ $f(a*b)= x*(a*b)* x^{-1}$

R.S/ $f(a)*f(b)=(x*a*x^{-1})*(x*b*x^{-1})$

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

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

$\therefore$ f is a homo.

H.w. In the following situations determine whether the indicated function f is homo. from the first group into the second group.

a) $f(a)=-a$, f: $(R,+) \to (R,+)$.

b) $f(a)=|a|$, f: $(R-\{0\},.) \to (R^+,.)$.

c) $f(a)=a+1$, $f: (Z,+) \to (Z,+)$.

d) $f(a)= a^2$, $f: (R-\{0\},.) \to (R^+,.)$.

e) $f(a)=na$ (n a fixed integer) , $f: (Z,+) \to (Z,+)$.

Theorem25: If f is a homo. from the group (G,*) into the group (G',o) then :

1) f(e)=e' where e' is an identity element of G'.
2) $f(a^{-1}) = (f(a))^{-1} \quad \forall a \in G$.

Theorem 26: Let f be a homo. From the group (G,*) into the group (G′,o) then :

1) For each subgroup (H,*) of (G,*) the pair (f(H), o) is a subgroup of (G′,o).
2) For each subgroup (H′,o) of (G′,o) the pair $((f(H'))^{-1}, *)$ is a subgroup of (G,*).

Proof: 1) $f(H) \neq \emptyset$ since $f(e) = e' \in f(H)$

Let $f(a),f(b) \in f(H)$

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

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

$\therefore$ (f(H), o) is a subgroup of (G′,o).

Proof: 2) $(f(H'))^{-1} \neq \emptyset$ since $e \in (f(H'))^{-1}$

Let $a, b \in (f(H'))^{-1} \ni f(a), f(b) \in H'$

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

$= f(a) \circ (f(b))^{-1} \in H'$

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

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

Definition: Let f be a homomorphism from the group (G,*) into the group (G′,o) and let e′ be the identity element of (G′,o). The kernel of f denoted by ker(f) is the set:

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

Example1: consider the function:

$f: (Z, +) \to (\{1, , -1, I, -I\}, .)$ defined by $f(n) = i^n$ for $n \in Z$, find ker(f).

sol:/ $f(n_1 + n_2) = i^{n_1+n_2}$

$= i^{n_1}.i^{n_2} = f(n_1).f(n_2)$

∴ f is a homo.

To find the kernel, we have

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

$$= \{n \in Z: f(n) = 1\}$$

$$= \{n \in Z: i^n = 1\}$$

$$= \{\dots, -8, -4, 0, 4, 8, \dots\}$$

Example2: Let $f: (R, +) \to (R - \{0\}, .)$ is a homo. and defined by $f(a) = 2^a$ for $a \in R$, find ker(f).

Sol:/

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

$$= \{a \in R: f(a) = 1\}$$

$$= \{a \in R: 2^a = 1\}$$

$$= \{a \in R: 2^a = 2^0\} = \{0\}$$

Example3: Let $f: (Z, +) \to (\{1, -1\}, .)$ such that:

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

Show that:

1) f is a homo.
2) find kernel (f).

sol.: 1) if $a, b \in Z_e$

$\Rightarrow f(a+b) = f(a).f(b)$

$\Rightarrow$L.S/ $f(a+b) = 1 \quad , a+b \in Z_e$

R.S / $f(a).f(b) = 1$

2) if $a, b \in Z_O$

$\Rightarrow f(a+b) = f(a).f(b)$

$\Rightarrow$L.S/ $f(a+b) = 1 \quad , a+b \in Z_e$

R.S / $f(a).f(b) = 1$

3) if $a \in Z_e$ & $b \in Z_o$

$\Rightarrow f(a+b) = f(a).f(b)$

$\Rightarrow$L.S/ $f(a+b) = -1 \quad , a+b \in Z_o$

R.S / $f(a).f(b) = -1$

$\therefore$ f is a homo.

$$\ker(f) = \{a \in Z : f(a) = e'\}$$
$$= \{a \in Z : f(a) = 1\}$$
$$= \{Z_e\}$$

Theorem 27: let $f: (G,*) \to (G', o)$ be a group homo. then $(\ker(f),*)$ is a subgroup of $(G,*)$.

Proof:

$$\ker(f) = \{x \in G : f(x) = e'\} \subseteq G$$
$$\because f(e) = e' \Rightarrow e \in \ker(f) \neq \emptyset$$

Let $a, b \in \ker(f)$

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

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

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

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

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

Theorem 28: let f: $(G,*) \to (G', o)$ be a group homo. then ker(f)={e} iff f is one to one.

Proof:

$\Rightarrow$ suppose ker(f)={e} T.p. f is one to one

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

$\Rightarrow f(a)\ o\ \left(f(b)\right)^{-1} = f(b)\ o\left(f(b)\right)^{-1}$

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

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

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

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

$\Rightarrow$ a=b

$\therefore$ f is 1-1

$\Leftarrow$ suppose f is (1-1) T.p. ker(f) ={e}

Let $a \in \ker(f) \Rightarrow f(a)= e'$

Since $f(e) = e'$

$\Rightarrow f(a)= f(e) \Rightarrow a=e$ [since f is 1-1]

$\therefore$ ker(f)={e}.

Reference

Introduction to modern abstract Algebra by :Dvaid M. Burton , 1978