Unit - 4

Algebraic Structures

Binary Operation : Let S be a ~~non-empty~~ non-empty set. An operation * is called binary operation on set S if following two condition holds.

(1) The operation * must be well-defined for any two elements a and b in S.

(2) The resulting element i.e. a * b must belong to set S.

For eg :-

(i) The operation of usual addition "+" is binary on the set of natural no.s N, real no.s R, rational numbers Q, integers Z, postive integers Z^+.

(ii) The operation of usual multiplication "·" is binary on the set of natural no. 'N', real no. 'R', rational no.s 'Q', integer 'Z', postive integers 'Z^+'

(iii) The operation of usual addition "+" is binary on the set of all 2×2 matrices, but not binary on the set of all matrices of any arbitary order.

Ex: The operation of usual addition '+' & usual multiplication '*' is binary on the set of all real functions. $F(x)$ defined on domain A.

Properties of binary operation :

Let S be a non-empty set and * be a binary operation on S. Then

Closure property ⇒ for $a, b \in S$; $a * b \in S$

associative property ⇒ for $a, b, c \in S$;

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

Commutative property ⇒ for $a, b \in S$;

$$a * b = b * a$$

Remark:

Closure property is obviously satisfied by binary relation * from its definition.

Ex:- Determine whether the operation given below is binary or not. Justify with valid reason.

(i) On Z^+, defined * by $a * b = a - b$

On Z^+, defined * by $a * b = a^b$

On R, defined * by $a * b = a - b$

(i) On Z^+, define $*$ by $a*b = c$, where c is the smallest integer greater than both a & b.

(ii) On Z^+, defined $*$ by $a*b = c$, where c is the atleast 5 more than $a+b$.

(iii) On Z^+, defined $*$ by $a*b = c$, where c is the largest integer less than the product of a & b.

Q-2 Determine whether the binary operation $*$ is commutative or associative.

(i) On Z, define $*$ by $a*b = a-b$

(ii) On Q, define $*$ by $a*b = ab+1$

(iii) On Q, define $*$ by $a*b = \frac{ab}{2}$

(iv) On Z^+, define $*$ by $a*b = 2^{ab}$

(v) On Z^+, define $*$ by $a*b = a^b$

(i) It is not binary because on $1*3 = 1-3 = -2 \notin Z^+$

(ii) It is binary.

(iii) It is binary

(iv) It is binary.

(v) It is binary.

(vi) No, it is not binary as

$1 * 1 = 0 \notin Z^+$

(2)

(a) Not associative

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

$= a - (b - c)$

$= a - b + c$

Also,

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

$= a - b - c$

$a * (b * c) \neq (a * b) * c$

Not Commutative

$a * b = a - b$

$b * a = b - a$

$= -(a - b)$

$a * b \neq b * a$

$ab + 1 = b'a + 1$

Hence $\otimes$ is commutative $\otimes$.

Algebraic Structure Definition

Let G be a non-empty set & $*$ be a binary operation defined on it. Then the set together with binary operation is called an algebraic structure denoted by $(G, *)$

For eg: $(Z, +)$; $(R, +)$; $(R, \cdot)$ etc are algebraic structures.

Group :

An algebraic structure $(G, *)$ is called a group if it satisfies the following axioms (properties)

(1) Closure axiom : $\forall a, b \in G$; $a * b \in G$

(2) Associative axiom : $\forall a, b, c \in G$; $a * (b * c) = (a * b) * c$

(3) Identity axiom : $\forall$ for each element $a \in G$, there exist a unique element $e \in G$ such that

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

then e is called the identity element.

(4) Inverse axiom : $\forall$ element $a \in G$, there exist a unique element $a^{-1} \in G$ such that

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

Remarks:

1. If $(G, *)$ satisfies only closure axiom then it is a groupoid.
2. If $(G, *)$ satisfies the closure & associative axiom then it is semi-group.
3. If $(G, *)$ satisfies closure, associative & identity axioms then we call it monoid.
4. If $(G, *)$ satisfies the commutative axiom in addition to the above 4 axioms, then it is called an abelian group.

Ex: Show that the algebric structure $(Z, +)$ is a group. Is it a abelian?

Sol^n:

Closure axiom:

For $x, y \in Z$, obviously $x+y$ is an integer.

i.e. $x+y \in Z$

Associative: Addition of integers is always associative

i.e. $x+(y+z) = (x+y)+z$

$\forall\ x, y, z \in Z$

Identity element

Clearly $0 \in Z$ is the additive identity i.e.

$$x+0 = 0x = 0+x \quad \forall x \in Z$$

Inverse Axiom:

For any $x \in Z$, we have $-x \in Z$ such that $x+(-x) = 0 = (-x)+x$

Therefore, $(Z,+)$ is a group.

(5) Commutative Axiom:

Clearly for $x, y \in Z$ we have

$$x+y = y+x$$

Addition is always commutative.

$(Z,+)$ is an abelian group.

Ex: Show that $(R,\cdot)$ is an abelian group.

Q. Consider an operation $*$ on the set $\mathbb{Q}$ of rational numbers defined as follows:

$$a * b = a + b + 1$$

Prove that $(\mathbb{Q}, *)$ is an abelian group.

(a) Closure Axiom:

For all $a, b \in \mathbb{Q}$ we have $a * b = a + b + 1 \in \mathbb{Q}$

(b) Associative axiom:

$$(a * b) * c = (a + b + 1) * c$$

$$= a + b + 1 + c + 1$$

$$= a + b + c + 2$$

$$a * (b * c) = a * (b + c + 1)$$

$$= a + b + c + 1 + 1$$

$$= a + b + c + 2$$

$$\boxed{(a * b) * c = a * (b * c)}$$

(c) Identity: Let $e \in \mathbb{Q}$ be the identity element.

$$a * e = a$$

$$a + e + 1 = a$$

$$\boxed{e = -1}$$

-1 is the identity

Theorem: Let a^{-1} be the inverse of $a \in \mathbb{Q}$

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

$a + a^{-1} + 1 = -1$

$a + a^{-1} = -2$

$\boxed{a^{-1} = -2 - a} \in \mathbb{Q}$

Commutative

$a * b = a + b + 1$

$b * a = b + a + 1$

$\boxed{a * b = b * a}$

$(\mathbb{Q}, *)$ is an abelian group

Consider an operation $*$ on set of rational no $\mathbb{Q}$ defined as $a * b = a + b - 1$

Prove that $(\mathbb{Q}, *)$ is an abelian group.

(a) Closure:

$\forall \; a, b \in \mathbb{Q}$

$a + b \in \mathbb{Q}$

$\Rightarrow a + b - 1 \in \mathbb{Q}$

(b) Associative

$(a * b) * c$

$(a + b - 1) * c$

$a + b - 1 + c - 1 = a + b + c - 2$

$a * (b * c)$

$a * (b + c - 1)$

$a + b + c - 1 - 1$

$a + b + c - 2$

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

(i) Identity: let e be the identity element

$$a * e = a$$
$$a + e - 1 = a$$
$$\boxed{e = 1}$$

(ii) Inverse: let a' be the inverse

$$a * a' = e$$
$$a + a' - 1 = 1$$
$$a + a' = 2$$
$$\boxed{a' = 2 - a}$$

(iii) Commutative

$$a * b$$
$$a + b - 1$$
$$b * a$$
$$\therefore b + a - 1$$
$$a + b - 1$$
$$a * b = b * a$$

To prove that the set $G = \left\{ \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}, a \in R, b \in R \right\}$ is a group under matrix addition

Closure Axiom:

Let $A = \begin{bmatrix} a_1 & 0 \\ 0 & b_1 \end{bmatrix}$ and $B = \begin{bmatrix} a_2 & 0 \\ 0 & b_2 \end{bmatrix} \in G$

Then $A + B = \begin{bmatrix} a_1 + a_2 & 0 \\ 0 & b_1 + b_2 \end{bmatrix} \in G$

Associative Axiom:

Matrix addition is always associative

i.e. $(A + B) + C = A + (B + C)$

for $A, B, C \in G$

Identity Axiom:

Clearly O (Null Matrix) $\in G$ such that

$A + O = A = O + A$ for all $A \in G$

Hence O is the identity element of G.

Inverse

Clearly

Let $A = \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \in G$

Clearly $A^{-1} = \begin{bmatrix} -a & 0 \\ 0 & -b \end{bmatrix} = -A \in G$

is the inverse of A.

Therefore G is a group under matrix addition.

Ex Let $G = \left\{ \begin{bmatrix} a & c \\ 0 & b \end{bmatrix} : a \in R, b \in R, c \in R, a \neq 0, b \neq 0 \right\}$

Prove that G is a group under matrix multiplication.

Set of Integers modulo n:

The set of integers modulo n wrt addition is defined as.

Z_n $\{0, 1, 2, 3, \ldots, n-1\}$ wrt $+_n$.

Eg: Z_2 $\{0, 1\}$ wrt $+_2$

Z_3 $\{0, 1, 2\}$ wrt $+_3$ etc

Note: $a +_n b = r$, where r is the remainder obtained by dividing the sum $a+b$ by n.

Similarly, the set of integers modulo n wrt multiplication is defined as

Z_n $\{1, 2, 3, \ldots, n-1\}$ wrt $\times_n$

Eg: Z_3 $\{1, 2\}$ wrt $\times_3$

Z_4 $\{1, 2, 3\}$ wrt $\times_4$ etc

Note: $a \times_n b = r$, where r is the remainder obtained by dividing the product ab by n.

1. P.T the set $Z_4 = \{0, 1, 2, 3\}$ is a group wrt $+_4$. Is Z_4 abelian

2. For finite groups, we use cayley table

	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

(1) Closure Axiom:
Since all the entries of the table belong to the set Z_4 itself, hence closure axiom is satisfied.

(2) Associative Axiom:
Let $a=1, b=2, c=3$

$= 1 +_4 (2 +_4 3)$

$= 1 +_4 1$

$= 2$

$(1 +_4 2) +_4 3$

$3 +_4 3$

$= 2$

Therefore Associative Axiom holds

(3) Identity Axiom:

Since the top border row is identical to the first row of the table hence the element at its extreme left is the identity element i.e., 0 is the identity element

(4) Inverse Axiom:

Inverse of $0 \to 0$

$1 \to 3$

$2 \to 2$

$3 \to 1$

Commutative

Since the first row is identical to the first column hence commutative axiom holds.

Therefore Z_4 is an abelian group.

P.T $Z_5 = \{0, 1, 2, 3, 4\}$

T_5	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Q. P.T, Set $Z_4 = \{1, 2, 3\}$ is not a group wrt X_4.

X_4	1	2	3
1	1	2	3
2	2	0	2
3	3	2	1

Since one of entry is zero which does not belong to set Z_4 hence Closure axiom is not satisfied. Therefore Z_4 is not a group wrt X_4.

Q. P.T Set $Z_8 = \{1, 2, 3, 4, 5, 6, 8\}$ is a group wrt X_8.

X_8	1	2	3	4	5	6
1	1	2	3			
2	2	4				
3	3	6				
4	4	1				
5	5	3				
6	6	5				

Since 1 is the identity element. Therefore

$O(1) = 1$

$(-1)^2 = 1, \quad O(-1) = 2$

$(i)^4 = 1 \quad \therefore O(i) = 4$

$(-i)^4 = 1 \quad \therefore O(-i) = 4$

Remarks :

(i) The order of an element divides the order of a group i.e. if $a \in G$ then $O(a)$ divides $O(G)$

(ii) If $a \in G$, then $O(a) = O(a^{-1})$

(iii) If $a \in G$ & there exist no such positive integer satisfying $a^n = e$, then $O(a)$ is taken as infinite.

For eg: $(Z, +)$ is a group.

Here $2 \in Z$ & there exist no positive n such that $2^n = 0$ is satisfied.

Hence $O(2)$ is infinite.

Find the order of each element of the group $(Z_6, +_6)$

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

(a) $O(0) = 1$; $\therefore e = 0$ is identity.

$\because (1)^1 = 1$; $(1)^2 = 1 +_6 1 = 2$; $(1)^3 = 1 +_6 1 +_6 1 = 3$

$(1)^4 = 1 +_6 1 +_6 1 +_6 1 = 4$; $(1)^5 = 1 +_6 1 +_6 1 +_6 1 +_6 1 +_6 1$

$(1)^6 = 5 +_6 (1)^1 = 0$

$\therefore O(1) = 6$

(c) $(2)^1 = 2$; $(2)^2 = 2 +_6 2 = 4$; $(2)^3 = 4 +_6 (2)^1 = 0$

$\therefore O(2) = 3$

(d) $(3)^1 = 3$, $(3)^2 = 3 +_6 3 = 0$

$\therefore (3) = 2$

(e) $O(4) = O(4^{-1}) = O(2) = 3$

(f) $O(5) = O(5^{-1}) = O(1) = 6$

Q: Find the order of each element of the group $(Z_7, \times_7)$

$Z_7 = \{1, 2, 3, 4, 5, 6\}$

(a) $O(1) = 1$ $\because$ as 1 is the identity

(b) $(2)^1 = 2$; $(2)^2 = 2 \times_7 2 = 4$; $(2)^3 = 4 \times_7 2 = 1$

$\therefore O(2) = 3$

(b) (3

(c)

(d)

(e) (6

Let G

oper

For

$(3)^1 = 3$, $(3)^2 = 3 \times_7 3 = 2$, $(3)^3 = 2 \times_7 3 = 6$,
$(3)^4 = 6 \times_7 3 = 4$, $(3)^5 = 4 \times_7 3 = 5$

$(3)^6 = 5 \times_7 3 = 1$

$\therefore O(3) = 6$

$O(4) = O(4^{-1}) = O(2) = 3$

$O(5) = O(5^{-1}) = O(3) = 6$

$(6)^1 = 6$; $(6)^2 = 6 \times_7 6 = 1$

$O(6) = 2$

Subgroup

Let $(G, *)$ be a group. A subset H of G is called a subgroup wrt the induced operation $*$ if H itself is a group.

For eg: $Z_6 = \{0, 1, 2, 3, 4, 5\}$ is a group wrt $+_6$. If $H = \{0, 2, 4\}$ then H is a subgroup of Z_6 wrt $+_6$ as follows

$+_6$	0	2	4
0	0	2	4
2	2	4	0
4	4	0	2

Clearly, H is closed, associative, has identity element 0 and $0^{-1}=0$, $2^{-1}=4$, & $4^{-1}=2$.

Hence, H is a subgroup of G.

Remark:

(i) Not every subset of a given group is a subgroup.
For eg: $H=\{0,3,5\}$ is not a group of Z_6 wrt $+_6$ because $3+_6 5=2 \notin H$. Hence, H is not closed.

(ii) For a given group G the subgroups $H=\{e\}$ and $H=G$ are called trivial subgroups.
A subgroup other than these two trivial subgroup is called non-trivial subgroup

For eg: $H=\{0\}$
$H=\{0,1,2,3\}$ are trivial subgroups of Z_4. and $H=\{0,2\}$ is a non-trivial subgroup of Z_4.

Necessary & sufficient Condition for a subset H to be a Subgroup of G:
Let $(G,*)$ be a group. A subset H of G is a subgroup if and only if
$a\in H,\ b\in H \Rightarrow a*b^{-1}\in H$

Prove that $H = \{1, -1\}$ is a subgroup of $G = \{1, -1, i, -i\}$ wrt multiplication

$1 \in H \Rightarrow 1.(-1)^{-1} = 1.(-1) = -1 \in H$

$-1 \in H \Rightarrow -1.(-1)^{-1} = -1.1 = -1 \in H$

$1 \in H, 1 \in H \Rightarrow 1.1^{-1} = 1 \in H$

$-1 \in H, -1 \in H \Rightarrow -1(-1)^{-1} = 1 \in H$

$\therefore a \in H, b \in H \Rightarrow a * b^{-1} \in H$ is satisfied $\forall a, b \in H$

$\therefore H$ is a subgroup of G.

Let Z be a group wrt addition Prove that its subset $3Z$ is a subgroup of Z.

Sol^n: Here $Z = \{\ldots\ldots -3, -2, -1, 0, 1, 2, 3 \ldots\ldots\}$ is a group wrt $+$.

Its subset $3Z = \{\ldots\ldots -9, -6, -3, 0, 3, 6, 9 \ldots\}$

Let $3x \in 3Z, 3y \in 3Z$ where $x, y \in Z$

Then $3x + (3y)^{-1} = 3x - 3y = 3(x-y) \in 3Z$.

Prove that the intersection of two subgroups of a group is again a subgroup.

Given: H_1 & H_2 are two subgroups of group G.

To prove: $H_1 \cap H_2$ is a subgroup of G i.e. $a \in H_1 \cap H_2, b \in H_1 \cap H_2 \Rightarrow a * b^{-1} \in H_1 \cap H_2$

for subgroup $a * b^{-1} \in$

Proof: Let $a \in H_1 \cap H_2$ & $b \in H_1 \cap H_2$

$(a \in H_1 \& a \in H_2) \& (b \in H_1 \& b \in H_2)$

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

$\because H_1$ & H_2 are subgroups of G

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

$\therefore H_1 \cap H_2$ is a subgroup of G.

Q: Prove that the union of two subgroups is not necessarily a subgroup of G.

Sol: Consider $\mathbb{Z} = \{\ldots -3, -2, -1, 0, 1, 2, 3, \ldots\}$ is a group wrt addition.

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

& $3\mathbb{Z} = \{\ldots -9, -6, -3, 0, 3, 6, 9, \ldots\}$

are subgroups of $\mathbb{Z}$.

by $2\mathbb{Z} \cup 3\mathbb{Z} = \{\ldots -9, -6, -4, -3, -2, 0, 2, 3, 4, 6, 8, 9, \ldots\}$

is not a subgroup as

$2 \in 2\mathbb{Z} \cup 3\mathbb{Z}$ & $3 \in 2\mathbb{Z} \cup 3\mathbb{Z}$

but $2 + 3^{-1} = 2 + (-3) = -1 \notin 2\mathbb{Z} \cup 3\mathbb{Z}$

Hence, the union of two subgroups

is not necessarily a subgroup.

Cyclic Group :-

Let G be a group w.r.t operation $*$.
Group G is called cyclic if there exist an element $g \in G$ such that $G = \{g^r : r \in Z\}$
Then G is called generator of group G.

For eg: In the multiplicative group $G = \{1, -1, i, -i\}$, we have two generators i & $-i$.

$\because$

$(i)^1 = i$ & $(-i)^1 = -i$
$(i)^2 = -1$ $(-i)^2 = -1$
$(i)^3 = -i$ $(-i)^3 = i$
$(i)^4 = 1$ $(-i)^4 = 1$

Hence, G is a cyclic group.

Remarks:

1. If $g \in G$ is a generator then $O(g) = O(G)$
2. If g is a generator of group G then g^{-1} is also a generator.
3. For $\phi(n)$ is used to count the number of generators in a cyclic group of order n.
4. $\phi(n)$ is defined as $\phi(p) = p-1$, if p is prime

(iii) $\phi(p^n) = p^n - p^{n-1}$, if p is prime

also $\phi(p_1^{n_1} \cdot p_2^{n_2}) = \phi(p_1^{n_1}) \phi(p_2^{n_2})$ where p_i is prime

Q. Find all the generators of cyclic group $Z_4 = \{0, 1, 2, 3\}$ wrt $+_4$.

Sol: Clearly $\phi(4) = \phi(2^2)$

$= 2^2 - 2^1 = 2$ generators.

Remember that if g is a generator of Z_4 then $O(g) = 4$

$(1)^1 = 1$

$(1)^2 = 2$

$(1)^3 = 1 +_4 1 = 2 +_4 1 = 3$

$(1)^4 = 3 +_4 1 = 0$

Order of 1 is 4.

1 is a generator.

Since $1^{-1} = 3$

Therefore 3 is also a generator.

$= \phi(2)\left(\frac{9}{2}\right)$

Find all the generators of cyclic groups of Z_{11}.

$Z_{11} = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$

Clearly

$\phi(10) = \phi(2 \times 5)$

$= \phi(2) \times \phi(5)$

$= (2-1) \times (5-1)$

$= 4$

Clearly if g is a generator of Z_{11} then $O(g) = 10$

$(2)^1 = 2$
$(2)^2 = 4$
$(2)^3 = 8$
$(2)^4 = 5$
$(2)^5 = 10$
$(2)^6 = 9$
$(2)^7 = 7$
$(2)^8 = 3$
$(2)^9 = 6$
$(2)^{10} = 1$ (identity)

$(8)^1 = 8$
$(8)^2 = 9$
$(8)^3 = 6$
$(8)^4 = 7$
$(8)^5 = 10$
$(8)^6 = 3$
$(8)^7 = 2$
$(8)^8 = 5$
$(8)^9 = 7$
$(8)^{10} = 1$ (identity)

Since $O(2) = 10$
Therefore 2 is a generator.
Since $2^{-1} = 6$
Therefore 6 is also a generator.

Since $O(8) = 10$
Therefore 8 is a generator. Since $8^{-1} = 7$
Therefore 7 is also a generator.

Q. Find all the generators of the cyclic group $G = \{a^0, a, a^2, a^3, a^4, a^5, a^6, a^7\}$

Sol: 1, 5, 7 are co-prime to 8

a, a^3, a^5, a^7 are also generators.

Subgroup of a Cyclic Group :-

Let H be a subgroup of a cyclic group G. Then every subgroup H is itself a cyclic. i.e. H is also a cyclic subgroup.

Theorem

Find all the proper subgroups of cyclic group $Z_8 = \{0,1,2,3,4,5,6,7\}$ w.r.t $+_8$.

Clearly no. of generators of $Z_8 = \phi_8 = \phi(2^3) = 2^3 - 2^2 = 8-4 = 4$

Clearly 1, 7, 3, 5 are generators of Z_8.

Therefore, proper subgroups will be generated by 0, 2, 4, 6.

$0 \in Z_8$; $H = \{0\}$

$2 \in Z_8$, $H_2 = \{0, 2, 4, 6, 0\}$

$4 \in Z_8$, $H_3 = \{4, 0\}$

$6 \in Z_8$, $H_4 = \{6, 4, 2, 0\}$

Same (why??) Since $2^{-1} = 6$

Q: Find all the proper subgroups of cyclic groups Z_{12} = {1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12} and X_{12}.

Sol: Clearly, no. of generators in Z_{12} = $\phi(12)$

$= \phi(2^2 \times 3)$

$= \phi(2^2) \times \phi(3)$

$= (2^2 - 2^1) \times (3 - 1)$

$= (4 - 2) \times 2$

$= 4$

X_{12}

Co-sets:

Let $(G, *)$ be a group & H be its subgroup. for $a \in G$, the set defined as $a * H = \{a * h, h \in H\}$ is called left coset of H generated by 'a' in G.

Similarly; $H * a = \{h * a, h \in H\}$ is right coset of H generated by 'a' in G.

For ex: $G = \{1, -1, i, -i\}$ is a multiplicative group & $H = \{1, -1\}$ is a subgroup of G.

Then ~~cosets~~ left cosets of G are given by =

(a) $1 \in G$; $1.H = \{1, -1\}$
(b) $-1 \in G$, $(-1)H = \{-1, 1\}$
(c) $i \in G$, $(i)i.H = \{i, -i\}$
(d) $-i \in G$; $(-i)H = \{-i, i\}$

Similarly,

The right cosets of H in G are as follows

(a) $1 \in G$ $H.1 = \{1, -1\}$
(b) $-1 \in G$ $H(-1) = \{-1, 1\}$
(c) $i \in G$ $Hi = \{i, -i\}$
(d) $-i \in G$ $H(-i) = \{-i, i\}$

Remarks:

(i) If group G is abelian then $a*H = H*a$ for all $a \in G$ and H is a subgroup.

(ii) Two cosets are either disjoint or identical.

(iii) $a \in (a*H)$

(iv) If $a \in (b*H)$ & $b \in (a*H)$, then $a*H = b*H$

(v) Union of all distinct cosets is equal to group G.

Let $(Z, +)$ be a group of integers & $3Z$ is a subgroup of it. Find all (left) cosets of $3Z$ in Z. How many of them are distinct. Show that the union of all distinct cosets is equal to Z.

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

$3Z = \{ \ldots\ldots -9, -6, -3, 0, 3, 6, 9 \ldots\ldots \}$

$0 \in Z$, $0+3Z = \{\ldots -9, -6, -3, 0, +3, 6, 9 \ldots\} = 3Z$

$1 \in Z$, $1+3Z = \{\ldots -8, -5, -2, 1, 4, 7, 10 \ldots\}$

$2 \in Z$, $2+3Z = \{\ldots -7, -4, -1, 2, 5, 8, 11 \ldots\}$

$3 \in Z$, $3+3Z = \{\ldots -6, -3, 0, 3, 6, 9 \ldots\} = 3Z$

$4 \in Z$, $4+3Z = \{\ldots -5, -2, 1, 4, 7, 10 \ldots\} = 1+3Z$ etc.

Clearly $(0+3Z) \cup (1+3Z) \cup (2+3Z) = Z$

Lagrange's theorem

The order of this subgroup divides the order of the group. i.e.

Let H be a subgroup of G such that $O(G) = n$ & $O(H) = m$. Then m divides n.

Proof:

Let $G = \{a_1, a_2, \ldots\ldots a_n\}$ be a group and $H = \{h_1, h_2, \ldots\ldots h_m\}$ be a sub group of G.

For $a_i \in G$; the left coset is given by $a_i * H = \{a_i * h_1, a_i * h_2, \ldots, a_i * h_m\}$ where $i = 1, 2, \ldots, n$

Clearly, the members of above cosets are all distinct because

if $a_i * h_r = a_i * h_t$

$h_r = h_t$ (by left cancellation)

(a contradiction)

Clearly, out of total n cosets, only k (say) will be distinct.

Then the union of these k distinct cosets will be equal to G.

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

$$\Rightarrow \boxed{m.k = n}$$

Therefore, m divides n.

Hence Lagrange's theorem is proved in general.

THE END.