Unit→9
Group & Subgroups:

Unary operation → कुनै set बाट एउटा variable लिएर operation गरि एउटा value दिन्छ त्यहि set मा पर्ने।

Binary operation → दुई variable कुनै set बाट लिएर operation गरि एउटा value दिन्छ त्यहि set मा पर्ने।

A binary operation on a set S is simply represented by symbol $*$ (astrik) or $\circ$ (circle) etc.

Example 1: Consider the set $Z^+ = \{1, 2, 3, \ldots\}$
(a) under operation '+'.
(b) under subtraction '−'.

Solution:

(a) Clearly, addition (sum) of two positive integers is again a positive integer.
i.e., $\forall a, b \in Z^+$, $a+b \in Z^+$.
$\therefore$ + operation satisfies closure property on Z^+.
Hence, + is a binary operation on Z^+.

(b) Clearly, there exist $1, 2 \in Z^+$ such that $1-2=-1 \notin Z^+$.
$\therefore$ Closure property is not satisfied under subtraction operation. Hence '−' is not a binary operation on Z^+.

Note: यो भनेर देखाउनु पर्दा for all ($\forall$) हुनुपर्छ हैन भनेर देखाउदा कुनै एउटा condition false भएको देखाउदा पुग्छ।

Some Properties:

i) **Closure property** → Any operation $*$ defined on a non-empty set S is said to satisfy closure property if $\forall a, b \in S$, $a*b \in S$. For example The set Z of integers is closed under addition.

ii) **Associative property** → An operation $*$ defined on set S is said to satisfy associative property if $\forall a, b, c \in S$, $a*(b*c) = (a*b)*c$.
For example: The operation '+' satisfies associative property on Z.

iii) Commutative property: An operation $*$ on a set S is said to satisfy commuative property if $\forall a,b \in S,\ a*b = b*a$.

iv) Existence of identity: Let $*$ be a binary operation on S. We say existence of identety holds on S under $*$ if $\exists$ an element $e \in S$ such that $\forall a \in S\ a*e = a = e*a$.

Example. Consider the set $\mathbb{Z}$ of integers under the operation $+$,
We see that $\exists e = 0 \in \mathbb{Z}$ such that $\forall a \in \mathbb{Z}$,
$$a + 0 = a = 0 + a.$$
$\therefore$ Existence of identity holds.

v) Existence of inverse: Let $*$ be a binary operation on S with identity element e. We say existence of inverse holds on S under $*$ if $\forall a \in S, \exists a^{-1} \in S$ such that
$$a * a^{-1} = e = a^{-1} * a.$$

Example:- Consider $\mathbb{Z}$ under addition $+$. ($\mathbb{Z}$ is set of integers)
Then $e = 0$ is identity element.
Now, $\forall a \in \mathbb{Z}, \exists a^{-1} = -a \in \mathbb{Z}$. such that $a + (-a) = 0 = -a + a$
$\therefore$ Existence of inverse holds.

$\mathbb{N} \rightarrow$ represents set of natural numbers.
$\mathbb{Z}^+ \rightarrow$ represents set of positive integers.
$\mathbb{Z}^- \rightarrow$ set of negative integers.
$\mathbb{Z} \rightarrow$ set of all integers.
$\mathbb{Q} = \{p/q : p,q \in \mathbb{Z},\ q \neq 0\}$ set of rational numbers.
$\mathbb{R} \rightarrow$ set of all real numbers.
$\mathbb{C} \rightarrow \{a + bi : a,b \in \mathbb{R}\}$ set of all complex numbers.

Example 1: Determine whether $a*b = ab+1$ defined for all $a,b \in \mathbb{Q}$ is

(a) Commutative

(b) Associative.

Solution:

Consider the set $\mathbb{Q}$ of rational numbers under operation $a*b = ab+1$ on $\mathbb{Q}$.

(a) We see that, $\forall a,b \in \mathbb{Q}$,

$$a*b = ab+1$$
$$= ba+1 \quad (\because \text{multiplication is commutative on } \mathbb{Q})$$
$$= b*a$$

$\therefore$ $*$ is commutative on $\mathbb{Q}$.

(b) We see that, $\exists$ 1,2,3 $\in \mathbb{Q}$ such that

$$1*(2*1) = 1*(\overset{ab+1}{2\cdot 3+1}) = 1*7 = \overset{a\ b}{1\cdot 7}+1 = 8$$
and $$(1*2)*3 = (1\cdot 2+1)*3 = 3*3 = 3\cdot 3+1 = 10.$$

Example 2: Determine whether $*$ is binary operation on given sets.

Sol^n

i) Consider $a*b = a-b$ on $\mathbb{Z}$.

Here, We see that $\forall a,b \in \mathbb{Z}$, $a*b = a-b \in \mathbb{Z}$.

$\therefore$ Closure property hold. Hence $*$ is binary operation $\mathbb{Z}$. ($\because$ difference of two integers is also an integer.)

ii) Consider $a*b = a^b$ on $\mathbb{Z}^+$

Here, We see that $\forall a,b \in \mathbb{Z}^+$
$$a*b = a^b \in \mathbb{Z}^+ \quad (\because \text{Positive integer power of positive integer is also +ve integer})$$

$\therefore$ $*$ is binary operation on $\mathbb{Z}^+$.

iii) Consider $a*b = a-b$ on $\mathbb{R}$.

Sol^n We see that, $\forall a,b \in \mathbb{R}$, $a*b = a-b \in \mathbb{R}$.

($\because$ difference of two real numbers is also an real number)

iv) Consider $a*b = c$ where c is at least 5 more than $a+b$, defined on $\mathbb{Z}^+$.

Sol^n

The operation is not well defined since

$1*2 = 1+2+5$
and also, it may be $1+2+6$ } Not unique value

$\therefore$ It is not binary operation.

v) Consider $a*b = c$, where c is smallest integer greater than a & b, defined on $\mathbb{Z}^+$

Sol^n Here,

Consider $\mathbb{Z}^+ = \{1,2,3,4,\ldots\}$ under given operation.

We see that $\forall\, a,b \in \mathbb{Z}^+$,

$$a*b = \begin{pmatrix}\text{smallest integer}\\ \text{greater than } a,b\end{pmatrix} \in \mathbb{Z}^+$$

$\left[\because \forall\, a,b \in \mathbb{Z}^+,\ a*b = \max\{a,b\}+1 \in \mathbb{Z}^+\right]$

$\therefore *$ is a binary operation on $\mathbb{Z}^+$.

Side work

$1*2$ = smallest int greater than 1&2 $=3$.

Similarly

$1*1=2$

$2*10=11$.

Example 3: Determine whether given binary operation $*$ is commutative or associative on given sets.

ⓐ. Given $a*b = a-b$ on $\mathbb{Z}$.

Soln

For commutative

We see that $\exists\, 1,2 \in \mathbb{Z}$ such that $\left.\begin{array}{l} 1*2 = 1-2 = -1 \\ \text{and } 2*1 = 2-1 = 1 \end{array}\right\}$ not equal

i.e, $1*2 \neq 2*1$.

$\therefore *$ is not commutative on $\mathbb{Z}$.

For associative

We see that $\exists\, 1,2,3 \in \mathbb{Z}$ such that,

$$1*(2*3) = 1*(2-3) = 1-(+2-3) = 2$$

and $(1*2)*3 = (1-2)*3 = \cancel{1}*3 = -1-3 = -4$

i.e, $1*(2*3) \neq (1*2)*3$

$\therefore *$ is not associative on $\mathbb{Z}$.

Sidework

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

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

ⓑ Given $a*b = \dfrac{ab}{2}$ on set $\mathbb{Q}$.

Soln

For commutative

We see that $\forall\, a,b \in \mathbb{Q}$,

$$\left.\begin{array}{l} a*b = \dfrac{ab}{2} \\ \& \ b*a = \dfrac{ba}{2} \end{array}\right\} \text{equal}$$

i.e, $a*b = b*a$ [since multiplication of rational numbers is commutative]

$\therefore *$ is commutative on $\mathbb{Q}$.

Side work

$a*b = \dfrac{ab}{2}$

$b*a = \dfrac{ba}{2}$

For associative

We see that $\forall\, a,b,c \in Q$,

$$a*(b*c) = a*\left(\frac{bc}{2}\right) = \frac{abc}{4}$$

and $$(a*b)*c = \left(\frac{ab}{2}\right)*c = \frac{abc}{4}$$

i.e, $a*(b*c) = (a*b)*c$

$\therefore$ $*$ is associative on Q.

Side work

$$a*(b*c) = a*\frac{bc}{2} = \frac{a\left(\frac{bc}{2}\right)}{2} = \frac{abc}{4}$$

$$(a*b)*c = \frac{\left(\frac{ab}{2}\right)c}{2} = \frac{abc}{4}$$

(c). Given $a*b = 2^{ab}$ on Z^+

Soln

For commutative

We see that, $\forall\, a,b \in Z^+$,

$$\left.\begin{aligned} a*b &= 2^{ab} \\ b*a &= 2^{ba} \end{aligned}\right\} \text{equal.}$$

($\because$ multiplication is commutative on Z^+)

i.e, $a*b = b*a$.

$\therefore$ $*$ is commutative on Z^+.

Side work

$a*b = 2^{ab}$

$b*a = 2^{ba}$

For associative

We see that, $\exists\, 1,2,3 \in Z^+$ such that

$$1*(2*3) = 1*2^{2\cdot 3} = 1*64 = 2^{1\cdot 64} = 2^{64}$$

and $$(1*2)*3 = (2^{1\cdot 2})*3 = 4*3 = 2^{4\cdot 3} = 2^{12}$$

i.e, $1*(2*3) \neq (1*2)*3$.

$\therefore$ $*$ is not associative on Z^+

Exam मा a,b,c तिनवटै सँगै सोध्दैन कुनै एउटा long मा 'आर दुई सम्म मात्र सोध्छ. So, a,b,c seperate question हुन्

Example 4: For $a, b \in Z$, define $a*b = \frac{ab}{2}$ that Z is not closed under $*$. Also show that set E of even integers is closed under $*$.

Soln

1st part → Consider the operation $a*b = \frac{ab}{2}$ on Z.

We see that, $\exists\, 1, 3 \in Z$ such that $1*3 = \frac{1\cdot 3}{2}$
$= \frac{3}{2} \notin Z$.

$\therefore$ Z is not closed under $*$.

2nd part → Consider $a*b = \frac{ab}{2}$ on set, $E = \{0, \pm 2, \pm 4, \pm 6, \ldots\}$

We see that $\forall\, a, b \in E$,
$a*b = \frac{ab}{2} \in E$

$\therefore$ Set E of even integers is closed under $*$.

[multiple of 2 of some integer being even
$\because a = 2m$ & $b = 2n$ being even. So, $\frac{ab}{2} = \frac{(2m)(2n)}{2}$
$= 2mn$
m & n are integer so on multiplying integers by 2 we get even]

Example 5. Show $S = Q - \{0\}$ is commutative, associative or not under $x*y = x/y$.

Soln

For commutative

We see that $\exists\, 4, 5 \in S$.
such that, $4*5 = 4/5$ and $5*4 = 5/4$ } Not equal
i.e, $4*5 \neq 5*4$
$\therefore$ $*$ is not commutative on S.

Side work.
$x*y = x/y$
$y*x = y/x$.

For associative

We see that $\exists\, 1, 2, 3 \in S$.
such that, $1*(2*3) = 1*(2/3) = \frac{1}{(2/3)} = \frac{3}{2}$
and $(1*2)*3 = \left(\frac{1}{2}\right)*3 = \frac{1/2}{3} = 1/6$ } Not equal.
i.e, $1*(2*3) \neq (1*2)*3$.
$\therefore$ $*$ is not associative on S.

Side work
$a*(b*c) = a*b/c$
$= \frac{a}{(b/c)}$
$= a \times \frac{c}{b}$
$(a*b)*c = \frac{a/b}{c}$
$= a/bc$

Example 6 :- Consider set $\mathbb{Q}$ of rationals under $x*y = \frac{x+y}{3}$

Soln

For commutative

We see that $\forall x, y \in \mathbb{Q}$

$$\left.\begin{aligned} x*y &= \frac{x+y}{3} \\ \text{and } y*x &= \frac{y+x}{3} \end{aligned}\right\} \text{equal} \quad \left[\because \text{Addition is commutative on } \mathbb{Q}\right]$$

i.e, $x*y = y*x$

$\therefore$ $*$ is commutative on $\mathbb{Q}$.

For associative

We see that $\exists\, 1, 2, 3 \in \mathbb{Q}$ such that

$$\left.\begin{aligned} 1*(2*3) &= 1*\left(\frac{2+3}{3}\right) = \left(\frac{1+5/3}{3}\right) = 8/9 \\ \text{and } (1*2)*3 &= \left(\frac{1+2}{3}\right)*3 = \frac{1+3}{3} = \frac{4}{3} \end{aligned}\right\} \text{Not equal}$$

$\therefore$ $*$ is not associative on $\mathbb{Q}$.

Side work

$$x*(y*z) = x*\left(\frac{y+z}{3}\right) = \frac{x+\left(\frac{y+z}{3}\right)}{3} = \frac{3x+y+z}{9}$$

$$(x*y)*z = \left(\frac{x+y}{3}\right)*z = \frac{\frac{x+y}{3}+z}{3} = \frac{x+y+3z}{9}.$$

Algebraic Structure:

A non-empty set S together with one or more binary operations on it is called an algebraic structure.

If S is algebraic structure with $*$ we denote it by $(S, *)$. If S is algebraic structure with $*$ and $\cdot$, we denote it by $(S, *, \cdot)$.

Definition of Group:

A non-empty set G together with binary operation $*$ is said to form a group if the following four properties are satisfied.

i) Closure property: $\forall a, b \in G$, $a*b \in G$.

ii) Associative property: $\forall a, b, c \in G$, $a*(b*c) = (a*b)*c$

iii) Existence of identity: $\exists$ an element $e \in G$ such that
$$a*e = a = e*a \ \forall a \in G.$$

iv) Existence of inverse: $\forall a \in G$, $\exists a^{-1} \in G$ such that
$$a*a^{-1} = 1 = a^{-1}*a.$$

Example: Show that the set $\mathbb{Z}$ is a group under usual addition operation.

Solution:

Consider set $\mathbb{Z} = \{0, \pm1, \pm2, \pm3, \ldots\}$ of all integers under addition '+'.

i) **Closure property:** We see that $\forall a, b \in \mathbb{Z}$, $a+b \in \mathbb{Z}$. ($\because$ Sum of two integers is also an integer).

$\therefore$ Closure property holds.

ii) **Associative property:** We see that $\forall a, b, c \in \mathbb{Z}$.

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

iii) **Existence of identity:** We see that, $\exists e = 0 \in \mathbb{Z}$ such that

$$a+0 = a = 0+a \quad \forall a \in \mathbb{Z}.$$

$\therefore$ 0 is identity.

iv) **Existence of inverse:**

We see that, $\forall a \in \mathbb{Z}$, $\exists a^{-1} = -a \in \mathbb{Z}$, such that,

$$a+(-a) = 0 = -a+a$$

$\therefore$ $-a$ is inverse of a, $\forall a \in \mathbb{Z}$.

All the four properties are hold.

Hence $(\mathbb{Z}, +)$ is a group.

Cayley's table:

It is a table that contains all possible results of an operation on a finite set. More precisely, we the following example.

Example: - Construct Cayley's table for addition on $\{-1, 0, 1\}$.

Solution:

Consider $S = \{-1, 0, 1\}$ under addition.

Cayley's table

+	-1	0	1
-1	-2	-1	0
0	-1	0	1
1	0	1	2

Important One Additional Question: - $G = \{1, -1, i, -i\}$ is a group of order 4. Solve it. [Kec publication book, example no. 25, page no 238].