(1) Let S be a set having exactly one element. How many different binary operations can be defined on S?

Answer the question has exactly 2 elements; 3 elements ; n elements.

Ans Let the element is a, i.e $S = \{a\}$

Now if n be the possible different binary operations ; for which a is the identity element.

Then n many different binary operation can be defined on S.

Ans Let A and B be two finite set, such that $|A| = m$ and $|B| = n$

Then if $(a, b) \in (A \times B)$

then $|A \times B| = mn$

Let us define a function —

$f: A \times B \to C$ and $|C| = C$

Then the number of possible mapping —

$= \prod_{i=1}^{mn} C$

$= C^{mn}$

Now a binary operation defined on a set S is essentially a mapping —

$$f: S \times S \to S$$

Then if $|S| = n$

Then number of possible binary operation —

$$N = n^{n^2}$$

(i) if $n = 1$, $N = 1$

(ii) if $n = 2$, $N = 2^4 = 16$

(iii) if $n = 3$, $N = 3^9 = 19683$

(iv) if $n = n$, $N = n^{n^2}$

---

(2) How many different commutative binary operations can be defined on a set of 2 element ? Or a set of 3 elements ? Or a set of n elements.

(Ans) Previously we had for non-commutative binary operation on set S, the number of possible different binary operation —

$$N = n^{n^2} \quad (|S| = n)$$

Now we can put the whole domain set in a $n \times n$ matrix, such that $A = [a_{ij}] = [(a_i \times a_j)]$

$$a_i \in S \; ; \; a_j \in S \qquad 1 \le i \le n \qquad 1 \le j \le n$$

Now for a commutative binary operation

$$a_i * a_j = a_j * a_i$$

Then the effective domain set lies in the upper triangular part of matrix A.

Since if a_{ij} lies in the upper trangular part of A then a_{ji} will lie in lower trangular part.

Then number of elements in upper triangular part —

$$= n + (n-1) + (n-2) + \cdots 1$$

$$= \frac{n(n+1)}{2}$$

Then number of possible commutative binary operation —

$$N_c = n^{\frac{n(n+1)}{2}}$$

(i) for $n = 2$, $N_c = 2^{\frac{2(2+1)}{2}}$

$= 8$

(ii) for $n = 3$, $N_c = 3^{\frac{3(3+1)}{2}}$

$= 3^6 = 729$

---

(3) Determine wheather * defined as follows gives a binary operation on the set or not. If not, then justify.

(a) On $\mathbb{Z}^+$, define * by $a * b = a - b$

(b) On $\mathbb{Z}^+$, define * by $a * b = a^b$

(c) On $\mathbb{R}$, define * by $a * b = a - b$

(d) On $\mathbb{R}$, define * by $a * b = |a| + |b|$

(e) On $\mathbb{Z}$, define * by $a * b = |a| b$

(f) On $\mathbb{Q}$, define * by $a * b = ab + 3$

For the binary operations above determine wheather they are associative or commutative? find the identity elements in each of the structures above if these exist.

(a) On $\mathbb{Z}^+$, * defined by $a * b = a - b$

Here * is not an binary operation on $\mathbb{Z}^+$

given $a * b = a - b \quad a, b \in \mathbb{Z}^+$

Now if $b > a$, $a - b \notin \mathbb{Z}^+$

Thus it is not a binary operation.

(b) On $\mathbb{Z}^+$, * defined by $a * b = a^b$

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

Since $\forall\, a, b \in \mathbb{Z}^+$

$\Rightarrow a^b \in \mathbb{Z}^+$

and $a * b = a^b$ is unique element.

(i) Commutativity $\Rightarrow$

If * is commutative —

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

$a * b = b * a$

$\Rightarrow a^b = b^a$

which is not possible for $a = 2, b = 3$

$\therefore$ * is not commutative.

(ii) Associativity $\Rightarrow$ If * is associative—

$(a*b)*c = a*(b*c)$ $\forall a,b,c \in \mathbb{Z}^+$

$\Rightarrow (a^b)^c = a^{(b^c)}$

$\Rightarrow a^{bc} = a^{bc}$

which is not always possible.

$\therefore$ $*$ is not associative.

(iii) Identity

Let e be the identity.

Then $a*e = e*a = a$ $\forall a \in \mathbb{Z}^+$, $e \in \mathbb{Z}^+$

$\Rightarrow a^e = e^a = a$

~~$\Rightarrow a^{e-1} = 1$ and $\frac{e^a}{a} = 1$~~

i.e, $a^{e-1} = 1$ and $\frac{e^a}{a} = 1$ must be satisfied simultaneously.

for first expression —

$e-1 = 0 \Rightarrow e = 1$

But $e = 1$ doesn't satisfy $\frac{e^a}{a} = 1$ for all $a \in \mathbb{Z}^+$

$\therefore$ Identity doesn't exist.

(c) On $\mathbb{R}$, $*$ defined by $a*b = a-b$

$*$ is a binary operation —

since, $a*b = a-b \in \mathbb{R}$ $\forall a,b \in \mathbb{R}$

and $a*b = a-b$ is unique for every $(a,b) \in \mathbb{R} \times \mathbb{R}$

(i) Associativity

If $*$ is associative —

then $(a*b)*c = a*(b*c)$ $\forall a,b,c \in \mathbb{R}$

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

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

$\Rightarrow a-b-c = a-b+c$

which is not always possible.

(ii) Commutativity

If $*$ is commutative —

then $a*b = b*a$ $\forall a,b \in \mathbb{R}$

$\Rightarrow a-b = b-a$

this is not always possible for $\forall a,b \in \mathbb{R}$

Then * is not commutative.

(iii) Identity ⇒

If e be the identity $e \in \mathbb{R}$

Then, $a * e = e * a = a \quad \forall a \in \mathbb{R}$

$\Rightarrow a - e = e - a = a$

Then $a - e = a$ and $e - a = a$ must satisfy simultaneously.

for first part, $e = 0$

for second ", $e = 2a$

Which is not possible for $\forall a \in \mathbb{R}$.

∴ Identity doesn't exist.

(d) On $\mathbb{R}$, * is defined by $a * b = |a| + |b|$

* is certainly a binary operation.

(i) Associativity ⇒ If * is associative -

$(a * b) * c = a * (b * c) \quad \forall a, b, c \in \mathbb{R}$

$\Rightarrow (|a| + |b|) * c = |a| * (|b| + |c|)$

$\Rightarrow ||a| + |b|| + |c| = |a| + ||b| + |c||$

$\Rightarrow |a| + |b| + |c| = |a| + |b| + |c|$

$\because a, b, c \in \mathbb{R}$

∴ * is associative.

(ii) Commutativity ⇒

If * is commutative —

$a * b = b * a \quad \forall a, b \in \mathbb{R}$

$\Rightarrow |a| + |b| = |b| + |a|$

Which is true for $\forall a, b \in \mathbb{R}$

∴ * is commutative.

(iii) Identity ⇒

Let e be identity element. $e \in \mathbb{R}$

$\therefore a * e = e * a = a$

$\Rightarrow |a| + |e| = |e| + |a| = a$

Now e can't be uniquely determined.

∴ Identity doesn't exist.

(e) On $\mathbb{Z}$, $*$ defined by $a*b = |a|b$

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

(i) Associativity ⇒

If $*$ is associative —

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

$$\Rightarrow (|a|b)*c = a*(|b|c)$$

$$\Rightarrow ||a|b|c = |a||b|c$$

$$\Rightarrow |a||b|c = |a||b|c$$

This is possible for all $a,b,c \in \mathbb{Z}$

$\therefore$ $*$ is associative.

(ii) Commutative ⇒

If $*$ is commutative —

$$a*b = b*a \quad \forall\ a,b \in \mathbb{Z}$$

$$\Rightarrow |a|b = |b|a$$

This is not possible for $\forall\ a,b \in \mathbb{Z}$

$\therefore$ $*$ is not commutative.

(iii) Identity ⇒

Let e be identity element. $e \in \mathbb{Z}$

$$\therefore \quad a*e = e*a = a \quad \forall\ a \in \mathbb{Z}$$

$$\Rightarrow |a|e = |e|a = a$$

We can't uniquely determine the element e.

$\therefore$ Identity doesn't exist.

(f) On $\mathbb{Q}$, $*$ is defined by $a*b = ab+3$

$*$ is a binary operation on $\mathbb{Q}$

(i) Associativity ⇒

If $*$ is associative —

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

$$\Rightarrow (ab+3)*c = a*(ab+3)$$

$$\Rightarrow (ab+3)c+3 = a(ab+3)+3$$

$$\Rightarrow abc+3c+3 = a^2b+3a+3$$

Which is not possible for $\forall\ a,b,c \in \mathbb{Q}$

$\therefore$ $*$ is not associative.

(ii) Commutativity :

If $*$ is commutative —

$$a * b = b * a \quad \forall\ a, b \in \mathbb{Q}$$

$$\Rightarrow ab + 3 = ba + 3$$

It is true for $\forall\ a, b \in \mathbb{Q}$

$\therefore *$ is commutative.

(iii) Identity :

Let e be the identity element.

Then $a * e = e * a = a \quad \forall a \in \mathbb{Q},\ e \in \mathbb{Q}$

$$\Rightarrow ae + 3 = ea + 3 = a$$

$$\Rightarrow e = \frac{a - 3}{a}$$

e is not uniquely determinable.

$\therefore$ Identity doesn't exist.

(4) Either prove the following statement or give a counterexample:

(a) Every binary operation on a set consisting of a single element is both commutative and associative.

(b) Every commutative binary operation on a Set having just two elements is associative.

(a) Let the single element is $a \in S$

$\therefore S = \{a\}$

Let $*$ be the binary operation.

Then $a * a = a$ ($\because$ only one element available)

Now, $a * (a * a) = a * a = a$

And $(a * a) * a = a * a = a$

$\therefore a * (a * a) = (a * a) * a$

$\therefore *$ is Associative in S.

Now, $a * a = a = a * a$

$\therefore *$ is commutative in S.

Thus the given statement is proved.

(b) Let elements of S be a, b.

$\therefore S = \{a, b\}$

Then $a * (a * b) = a * a$ (Let $a * b = a$)

and, $(a * a) * b = b * b$ (Let $a * a = b$)

Now we choose $b * b = a$

Then $a * (a * b) = a * a = b \neq a = (a * a) * b$

$\therefore$ This is not associative.

(5) In the following cases determine wheather the binary * gives a group structure on the given set or not. If not, justify

(a) $\langle \mathbb{Z}, * \rangle$, * given by $a*b = ab$

(b) $\langle 2\mathbb{Z}, * \rangle$, * given by $a*b = a+b$

(c) $\langle \mathbb{R}^+, * \rangle$, * given by $a*b = \sqrt{ab}$

(d) $\langle \mathbb{R}^+, * \rangle$, * given by $a*b = \frac{a}{b}$

(e) $\langle \mathbb{C}, * \rangle$, * given by $a*b = |ab|$

(f) $\langle \mathbb{Q}[\sqrt{2}], + \rangle$ where $\mathbb{Q}[\sqrt{2}] = \{a+b\sqrt{2} : a,b \in \mathbb{Q}\}$

(g) $\langle P(X), \Delta \rangle$ where $P(X)$ is the power set of X and Δ is the symmetric difference.

(h) $\langle \mathbb{Q}[\sqrt{2}] - \{0\}, * \}$, '*' is the usual product.

(i) $\langle G, * \rangle$, where $G = \left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} : a \in \mathbb{R} - \{0\} \right\}$ and * is the matrix multiplication.

(a) Given $\langle \mathbb{Z}, * \rangle$, * is defined by

$a*b = ab$

This is not a Group.

Since

(i) Inverse of every element doesn't belong to Set $\mathbb{Z}$

e.g $2^{-1} = \frac{1}{2} \notin \mathbb{Z}$

(ii) For $a = 0 \in \mathbb{Z}$ there exists no inverse element.

(b) Given $\langle 2\mathbb{Z}, * \rangle$, * given by $a*b = a+b$

Let us check where $\langle 2\mathbb{Z}, * \rangle$ satisfies all the requirements to be a group

(i) Associativity ⇒

Let $a, b, c \in 2\mathbb{Z}$

$\therefore a*(b*c) = a*(b+c)$

$= a+b+c$

And, $(a*b)*c = (a+b)*c = a+b+c$

Since, $a*(b*c) = (a*b)*c \quad \forall a,b,c \in 2\mathbb{Z}$

Then * is associative in $2\mathbb{Z}$

(ii) Identity element ⇒

Let e be the identity element.

Then $a*e = e*a = a \quad a \in 2\mathbb{Z}$

$\Rightarrow \quad a+e = e+a = a$

Then $\quad e = 0 \in 2\mathbb{Z}$

$\therefore$ Identity element exists. $e = 0$

(iii) Inverse element $\Rightarrow$

Let $\quad a \in 2\mathbb{Z}$

Then if a^{-1} be its inverse element.

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

$$\Rightarrow a+a^{-1} = 0 = a^{-1}+a$$

$$\therefore \quad a^{-1} = -a \in 2\mathbb{Z}$$

$\because a \in 2\mathbb{Z}$

$\therefore$ for every element in $2\mathbb{Z}$, inverse is present in $2\mathbb{Z}$.

Now $*$ is binary operation, so the closure property comes with it.

$\therefore \langle 2\mathbb{Z}, * \rangle$ forms a Group.

(c) $\langle \mathbb{R}^+, * \rangle$, $*$ given by $a*b = \sqrt{ab}$

Let us check weather $\langle \mathbb{R}^+, * \rangle$ satisfies all the requirements to be a Group.

(i) Associativity $\Rightarrow$

Let, $\quad a, b, c \in \mathbb{R}^+$

$$\therefore \quad (a*b)*c = (\sqrt{ab})*c$$

$$= \sqrt{\sqrt{ab}\cdot c}$$

And, $\quad a*(b*c) = a*\sqrt{bc}$

$$= \sqrt{a\sqrt{bc}}$$

Now, $\quad (a*b)*c \neq a*(b*c) \quad \forall a,b,c \in \mathbb{R}^+$

$\therefore \langle \mathbb{R}^+, * \rangle$ doesn't have the associative property.

$\therefore \quad \langle \mathbb{R}^+, * \rangle$ doesn't form a Group.

(d) $\langle \mathbb{R}^+, * \rangle$, $*$ given by $a*b = \frac{a}{b}$

Let us check weather $\langle \mathbb{R}^+, * \rangle$ satisfies all the requirements to be a Group.

(i) Associativity $\Rightarrow$

Let $a, b, c \in \mathbb{R}^+$

$\therefore a * (b * c) = a * \left(\frac{b}{c}\right)$

$= \frac{a}{\frac{b}{c}} = \frac{ac}{b}$

Now, $(a * b) * c = \frac{a}{b} * c$

$= \frac{\frac{a}{b}}{c}$

$= \frac{a}{bc}$

Now, $a * (b * c) \neq (a * b) * c \quad \forall\ a, b, c \in \mathbb{R}^+$

$\therefore \langle \mathbb{R}^+, * \rangle$ doesn't form a group.

(e) $\langle \mathbb{C}, * \rangle$, $*$ is given by $a * b = |ab|$

Let us check whether $\langle \mathbb{C}, * \rangle$ satisfies all the requirements to be a group.

(i) Associativity :

Let, $a, b, c \in \mathbb{C}$.

$\therefore (a * b) * c = |ab| * c$

$= ||ab|c|$

Now, $a * (b * c) = a * |bc| = |a|bc||$

Now let

$a = d + ie$
$b = f + ig$
$c = h + ij$

($d, e, f, g, h, i, j \in \mathbb{R}$, $i = \sqrt{-1}$)

[Since every element of $\mathbb{C}$ can be written in the form $a = b + ic$ where $a \in \mathbb{C}$, $b, c \in \mathbb{R}$]

$\therefore ab = (df - eg) + i(dg + ef)$

$\therefore |ab| = \sqrt{(df - eg)^2 + (dg + ef)^2}$

$\therefore ||ab|c| = \sqrt{h^2[(df - eg)^2 + (dg + ef)^2] + j^2}$

$\therefore ||ab|c| = \sqrt{h^2 + j^2} \cdot \sqrt{(df - eg)^2 + (dg + ef)^2}$

Similarly, $|a|bc| = \sqrt{d^2 + e^2} \cdot \sqrt{(fh - gi)^2 + (fi + gh)^2}$

$\therefore ||ab|c| \neq |a|bc|| \quad \forall\ a, b, c \in \mathbb{C}$

$\therefore \langle \mathbb{C}, * \rangle$ doesn't have associative property.

$\therefore \langle \mathbb{C}, * \rangle$ doesn't form a group.

---

(8) $\langle \mathbb{Q}[\sqrt{2}], + \rangle$, where $\mathbb{Q}[\sqrt{2}]$
$= \{a+b\sqrt{2} : a,b \in \mathbb{Q}\}$

Let us check all the requirements of $\langle \mathbb{Q}[\sqrt{2}], + \rangle$ to be a group.

(i) Associativity ⇒

Let, $x, y, z \in \mathbb{Q}[\sqrt{2}]$

and, $x = a+b\sqrt{2} : a,b \in \mathbb{Q}$
$y = c+d\sqrt{2} : c,d \in \mathbb{Q}$
$z = e+f\sqrt{2} : e,f \in \mathbb{Q}$

$\therefore (x*y)*z$
$= (a+b\sqrt{2} + c+d\sqrt{2}) + (e+f\sqrt{2})$
$= (a+b+c) + (b+d+f)\sqrt{2}$

And, $x*(y*z)$
$= (a+b+c) + (b+d+f)\sqrt{2}$

$\because a,b,c,d,e,f \in \mathbb{Q}$.

Then $(x+y)+z = x+(y+z)$

$\therefore +$ is associative over $\mathbb{Q}[\sqrt{2}]$.

(ii) Identity element ⇒

Let e be the identity.

$\therefore x+e = e+x = x$

$\forall x \in \mathbb{Q}[\sqrt{2}]$
$\therefore x = a+b\sqrt{2}$
$a,b \in \mathbb{Q}$

$e = e_1 + e_2\sqrt{2}$
$e_1, e_2 \in \mathbb{Q}$

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

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

$\therefore e_1 = e_2 = 0 \in \mathbb{Q}$

$\therefore e = 0+0\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$

$\therefore$ Identity element exists.

(iii) Inverse element ⇒

Let $x \in \mathbb{Q}[\sqrt{2}]$ has inverse x^{-1}.

$x = a+b\sqrt{2}$; $a,b \in \mathbb{Q}$.

Let $x^{-1} = c + d\sqrt{2}$

Then we have —

$$x + x^{-1} = x^{-1} + x = e$$

$$\Rightarrow (a+c) + (b+d)\sqrt{2} = (c+a) + (d+b)\sqrt{2} = 0 + 0\sqrt{2}$$

$$\therefore c = -a \in \mathbb{Q}$$

$$d = -b \in \mathbb{Q}.$$

$$\therefore x^{-1} \in \mathbb{Q}[\sqrt{2}]$$

∴ for every element in $\mathbb{Q}[\sqrt{2}]$ inverse element exists in $\mathbb{Q}[\sqrt{2}]$,

$$\therefore \langle \mathbb{Q}[\sqrt{2}], + \rangle \text{ forms a group.}$$

(8) $\langle \overline{P(x)}, \Delta \rangle$ where $\overline{P(x)}$ is the power set of x and Δ is the symmetric difference.

Let, $X = \{a, b, c\}$

Then $P(X) = \{\{\phi\}, \{a\}, \{b\}, \{c\}, \{a,b\}, \{b,c\}, \{c,a\}, \{a,b,c\}\}$

Now, $(\{a,b\} \Delta \{b,c\}) \Delta \{a,c\}$

Now, $\{a,b\} \Delta \{b,c\}$

$= \{\{a,b\} - \{b,c\}\} \cup \{\{b,c\} - \{a,b\}\}$

$= \{a\} \cup \{c\}$

$= \{a,c\}$

$\therefore (\{a,b\} \Delta \{b,c\}) \Delta \{a,c\}$

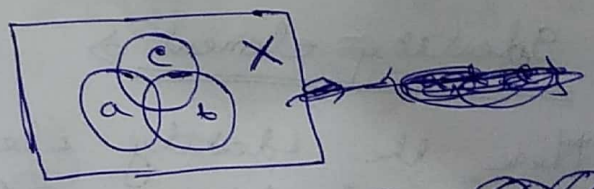
$= \{a,c\} \Delta \{a,c\}$

Let us check all the requirements of $\langle P(x), \Delta \rangle$ to be a group.

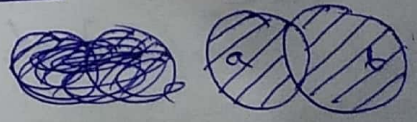
① Associativity ⇒

Let, $a, b, c \in P(X)$

Then venn diagram becomes arbitrarily —

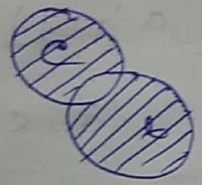


Then $a \Delta b$ is ⇒

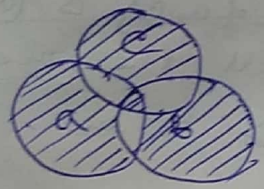


Now, $(a \Delta b) \Delta c$ is —

Now, $b \Delta c$ is —



Then $a \Delta (b \Delta c)$ is —



$\therefore (a \Delta b) \Delta c = a \Delta (b \Delta c)$

$\therefore \Delta$ over $P(X)$ is associative.

(ii) Identity element ⇒

Here the identity element is —

$\{\phi\} \in P(X)$

(iii) Inverse element

for $\forall\, a \in P(X)$

The inverse is $X - a \in P(X)$

$\therefore \langle P(X), \Delta \rangle$ forms a group, since Δ is a binary operation on $P(X)$.

(h) $\langle \mathbb{Q}[\sqrt{2}] - \{0\}, * \rangle$, '$*$' is the usual product.

Let us check the requirements —

(i) Associativity ⇒

Let $x, y, z \in \mathbb{Q}[\sqrt{2}]$

$x = a + b\sqrt{2}$ $\quad a, b \in \mathbb{Q}$

$y = c + d\sqrt{2}$ $\quad c, d \in \mathbb{Q}$

$z = e + f\sqrt{2}$ $\quad e, f \in \mathbb{Q}$

$\therefore (x * y) * z$

$= \left((ac + 2bd) + (ad + bc)\sqrt{2}\right) * (e + f\sqrt{2})$

$= f\left((ace + 2bde + 2adf + 2bcf)\right)$

$$= (ace + 2bde + 2adf + 2bcf) + (acf + 2bdf + ade + bce)\sqrt{2}$$

Now, $x * (y * z)$

$$= (a + b\sqrt{2}) * ((ce + 2fd) + (cf + de)\sqrt{2})$$

$$= (ace + 2fda + 2cfb + 2bde) + (bec + 2fdb + acf + ade)\sqrt{2}$$

$$\therefore (x * y) * z = x * (y * z) \quad \forall\ x, y, z \in \mathbb{Q}[\sqrt{2}]$$

$\therefore$ $*$ is Associative in $\mathbb{Q}[\sqrt{2}]$

(ii) Identity element $\Rightarrow$

Let $e = e_1 + e_2\sqrt{2}$ be identity.

$\therefore$ for $a = b + c\sqrt{2}$ $\quad a \in \mathbb{Q}[\sqrt{2}]$, $b, c \in \mathbb{Q}$

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

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

Then $e_1 b + e_2 c = b$ ... (i)

$e_1 c + e_2 b = c$ ... (ii)

by (i) $\times c$ − (ii) $\times b$ we get :-

$$e_2 c^2 - e_2 b^2 = bc - cb$$

$$\Rightarrow e_2 = \frac{b^2 - c^2}{c^2 - b^2} = -1$$

Again by, (i) $\times b$ − (ii) $\times c$ we get −

$$e_1 b^2 - e_1 c^2 = b^2$$

$$e_2 = \frac{\quad}{\quad} \in \mathbb{Q} \quad (\because c^2 - b^2 \neq 0 \ \forall\ b, c \in \mathbb{Q})$$

Again by (i) $\times b$ − (ii) $\times c$ we get −

$$e_1 b^2 - e_1 c^2 = b^2 - c^2$$

$$\Rightarrow e_1 = 1 \in \mathbb{Q}$$

$$\therefore e = 1 \in \mathbb{Q}[\sqrt{2}]$$

$\therefore$ Identity exists.

(iii) Inverse element $\Rightarrow$

Let a^{-1} be inverse element of $a \in \mathbb{Q}[\sqrt{2}]$

If $a = b + c\sqrt{2}$ $\quad [b, c, d, e \in \mathbb{Q}]$

$a^{-1} = d + e\sqrt{2}$

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

$\Rightarrow (bd + 2ce) + (be + cd)\sqrt{2} = 1$

$\therefore \quad be + cd = 0 \quad \ldots (i)$

$bd + 2ce = 1 \quad \ldots (ii)$

(i) × d, (ii) × e we get

$cd - 2ce^2 = -e$

By (i) × b − (ii) × c we get —

$b^2e - 2c^2e = -c$

$e = \frac{-c}{b^2 - 2c^2}$

Now if $b^2 = 2c^2$

then e is undefined.

$\therefore a^{-1}$ doesn't exist for $a = b + c\sqrt{2}$ if $b^2 = 2c^2$

$\therefore \langle \mathbb{Q}\sqrt{2} - \{0\}, + \rangle$ is not a Group.

(i) $\langle G, + \rangle$, where $G = \left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} : a \in \mathbb{R} - \{0\} \right\}$ and * is matrix multiplication.

Now for any $g \in G$

$|g| = 0$

$\therefore g^{-1}$ can't exist.

$\therefore \langle G, + \rangle$ doesn't form group.

(6) Give an example of an abelian group G where G has exactly 1000 elements.

Let $\mathbb{Z}_{1000}$ be the residue class set of 1000.

Let us define * be binary operation in $\mathbb{Z}_n$ such that $a * b = (a+b) \bmod 1000$ $(a, b \in \mathbb{Z}_{1000})$

Then $\langle \mathbb{Z}_{1000}, + \rangle$ forms a Group, which

has exactly 1000 elements.

---

(7) Let G be a group with finite number of elements. Show that for any $a \in G$, there exists an $n \in \mathbb{Z}^+$ such that $a^n = e$.

Proof Let the number of elements in G is, $|G| = m$ (finite)

Let us choose an arbitary element $a \in G$.

Now there must be at least two $p, n \in \mathbb{Z}^+$ such that — $(p \neq n)$

$$a^p = a^n$$

Since G contains only m distinct elements and m is finite.

$$\Rightarrow a^p = a^n$$

$$\Rightarrow a^p * a^{-n} = a^n * a^{-n} \quad (\text{let } p > n)$$

$$\Rightarrow a^{p-n} = e$$

$\therefore (p-n) = s \in \mathbb{Z}^+$ for which

$$a^{p-n} = e$$

Since we have picked a arbitarily.

Then for any $a \in a$ there exists some integer (say n) $\in \mathbb{Z}^+$ such that $a^n = e$

$\therefore$ The statement is proved.

---

(8) Suppose that a group G has an element x such that $ax = x$ for all $a \in G$. Show that G contains only identity element.

Proof Given —

$$ax = x \qquad \boxed{\begin{array}{l} x \in G \\ \forall a \in G \end{array}}$$

Since G is a group and $x \in G$ then $x^{-1} \in G$.

Post operating both sides with x^{-1} —

$$axx^{-1} = xx^{-1}$$

$$\Rightarrow ae = e \quad (\text{By Associativity})$$

$$\Rightarrow a = e \quad (e = \text{Identity})$$

Now this is true for all $a \in G$.

Then G contains only one element. And it is the identity element.

---

(9) Let G be a group, $a, b \in G$. Show that $(aba^{-1})^n = ab^n a^{-1}$ iff $b = b^n$

Proof Let $b = b^n$

Then, $(aba^{-1})^n$

~~$(aba^{-1})(aba^{-1}) \cdots (aba^{-1})$~~

$= (aba^{-1})(aba^{-1}) \cdots$ nth term

$= ab(a^{-1}a)b(a^{-1}a) \cdots (a^{-1}a)ba^{-1}$

$= abebe \cdots ebe a^{-1}$ $(a^{-1}a = e = \text{identity})$

$= ab^n a^{-1}$

$= aba^{-1}$ $(\because b = b^n)$

$\therefore (aba^{-1})^n = aba^{-1}$

Conversely let $(aba^{-1})^n = ab^n a^{-1}$

Similarly by previous manner we get –

$(aba^{-1})^n = ab^n a^{-1}$

$\therefore ab^n a^{-1} = aba^{-1}$

pre operating both sides by a^{-1} we get –

$a^{-1}a\, b^n a^{-1} = a^{-1}a\, b\, a^{-1}$

$\Rightarrow b^n a^{-1} = ba^{-1}$

$\Rightarrow b^n = b$ (RCL)

~~$ab \cdots (aba)$~~

$\therefore$ Hence our statement is proved.

---

(10) An element $a \in G$ is called idempotent if $a^2 = a$. Show that the only idempotent element in G is the unit element

Proof Given $a \in G$ and —

$a^2 = a$

post operating both sides with a^{-1}.

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

$\Rightarrow a = e$ (e = identity)

Since the identity element in a group is unique.

Then $a \in G$ is also unique.

Hence our statement is proved.

(12). If G is a group such that $a^2 = e$ for every $a \in G$. Show that G is abelian. Is it true if $a^3 = e, \forall a \in G$

Proof

Given $a^2 = e \quad \forall a \in G$

$\Rightarrow a^2 a^{-1} = e a^{-1}$

$\Rightarrow a = a^{-1} \quad \forall a \in G$

Now, for $a, b \in G$ ——

$ab = (ab)^{-1} \quad (\because ab \in G)$

$\Rightarrow ab = b^{-1} a^{-1}$

$\Rightarrow ab = ba \quad (\because a^{-1} = a \ \forall a \in G$

$\therefore G$ is abelian since for any arbitrarily chosen $a, b \in G$ —

$ab = ba.$

Hence our statement is proved.

But the statement is not true if $a^3 = e, \forall a \in G.$

(13) Show that G is abelian iff $(ab)^2 = a^2 b^2$ $\forall a, b \in G$.

Proof Let $(ab)^2 = a^2 b^2 \quad \forall a, b \in G$

$\Rightarrow (ab)(ab) = (aa)(bb)$

$\Rightarrow a(ba)b = a(ab)b$ (Associativity)

$\Rightarrow a^{-1}a(ba)bb^{-1} = a^{-1}a(ab)bb^{-1}$

(pre operating both sides by a^{-1} and post " " " " b^{-1})

$\Rightarrow e(ba)e = e(ab)e$ (e = identity)

$\Rightarrow \boxed{ba = ab}$

Conversely Let $ba = ab \quad \forall a, b \in G$

$\therefore (ab)^2 = (ab)(ab)$

$= (ab)(ba) \quad (\because ab = ba)$

$= a b^2 a$ (Associativity)

$= aab^2$ (By assumption)

$\Rightarrow \boxed{(ab)^2 = a^2 b^2}$

Hence G is abelian if and only $(ab)^{-1} = a^{-1}b^{-1} \quad \forall\, a, b \in G$

(14) Let G be a finite group with even number of elements. Show that there is at least one $a \in G$ such that $a^2 = e$

Since $e \in G$.

and $e^{-1} = e$

Then there is at least one $a \in G$ for which $a^{-1} = e$.

(15) Give an example to show that union of two subgroups may not be a subgroup.

(Ans) Let us have a set $S = \{1, 2, 4, 5\}$,

And we define a binary operation $*$ on S, such that

$$a * b = (ab) \bmod 6 \quad (a, b \in S)$$

Then $\{1, 5\}$ forms a subgroup.

And $\{1, 4\}$ also forms a subgroup.

But the union of these, i.e $\{1, 4, 5\}$ doesn't form a subgroup.

since, $4 * 5 = 20 \bmod 6$

$= 2 \notin \{1, 4, 5\}$

Thus our statement is correct.

(16) If K is a subgroup of H and H is a subgroup of G, show that K is a subgroup of G.

(Ans) Let us pick two arbitary elements

$a, b \in K$.

Since K is a subgroup of H.

Then $ab^{-1} \in K \subseteq H$

$\therefore \quad ab^{-1} \in H$

Again H is a subgroup of G.

$\therefore \quad H \subseteq G$

$\therefore \quad ab^{-1} \in G$

So we have picked up two arbitary elements a, b from K and shown that ab^{-1} also belongs to K.

And a, b, ab^{-1} also belongs to G.

$\therefore$ K is also a subgroup of G.

---

(15) Give an example to show that union of two subgroups may not be a subgroups.

Let us consider the set $\mathbb{Z}_6$ (residue class set of 6).

Under addition modulo 6 operation it forms a group.

Let $H_1 = \{[0], [2], [4]\}$

$H_2 = \{[0], [3]\}$

Now H_1 and H_2 are subgroups of $(\mathbb{Z}_6, +_6)$

But $H_1 \cup H_2 = \{[0], [2], [3], [4]\}$

doesn't forms a group, since —

$[2] +_6 [3] = [5] \notin H_1 \cup H_2$

$\therefore$ Our statement is proved.

(17) If G is an abelian group, show that $H = \{a : a \in G, a^2 = e\}$ is a subgroup of G.

Proof Let us pick two elements $a, b \in H$

Then $a^2 = b^2 = e$

Now, $e^2 = e \in G$ (e = identity)

$\therefore e \in H$

Now, $a^2 = e$

$\Rightarrow a^2 a^{-1} = a^{-1}$

$\Rightarrow a^{-1} = a \in H$

i.e for any arbitary element $a \in H$, a^{-1} also lies in H.

Now we have $a, b \in H$

Then $ab^{-1} = ab$ ($\because \forall a \in H$, $a^{-1} = a$)

Now we have to show $ab \in H$

We have $a^2 = b^2 = e \in H$

$\therefore a^2 b^2 = e \in H$

$\Rightarrow a(ab)b = e \in H$

~~$a^{-1}a(ab)bb^{-1} \in a^{-1}eb^{-1} \in H$~~

$\Rightarrow (ab)ab = e$ $(\because G$ is abelian$)$

$\Rightarrow (ab)^2 = e$

$\therefore ab \in H$

$\therefore ab^{-1} \in H \quad \forall a, b \in H$

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

(18) Show that a group can not be expressed as a union of two proper subgroups.

Ans As we have done in Q-15.

We pick set $\mathbb{Z}_6$ (the residue class set of 6).

Let $H_1 = \{[0], [2], [4]\}$

$H_2 = \{[0], [3]\}$

Here H_1 and H_2 is proper subgroup of $\langle \mathbb{Z}_6, +_6 \rangle$

But $H_1 \cup H_2 \neq \mathbb{Z}_6$

Since $[5] \notin H_1 \cup H_2$

But $[5] \in \mathbb{Z}_6$.

Hence the statement is proved.

(19) Give an example of a group which is not cyclic but every proper subgroup of which is cyclic.

Ans Let us have a set, $G = \{1, -1, i, -i\}$ where $i = \sqrt{-1}$

Ans Let us consider a Klein four group G

The Cayley table is given by –

*	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Here e is the identity element.

This group G is non cyclic since

every element, but the identity, has order 2.

But total number of elements = 4.

But the proper subgroups of G are –

$H_1 = \{e\}$

$H_2 = \{e, a\}$

$H_3 = \{e, b\}$

$H_4 = \{e, c\}$

All of these subgroups are cyclic and proper.

Thus this is the required example.

---

(20) Let $a, b \in G$ such that $b = xax^{-1}$ for some $x \in G$. Show that $O(a) = O(b)$

(Ans) Let us assume $O(a) = n$

$O(b) = m$

If $n > m$ then ——

$b^m = (xax^{-1})^m$

$\Rightarrow e = xa(x^{-1}ax)a(x^{-1}ax)\cdots$ m times

$\Rightarrow e = xa^m x^{-1}$

$\Rightarrow x^{-1}ex = x^{-1}xa^m x^{-1}x$

$\Rightarrow x^{-1}x = eae$

$\Rightarrow a^m = e$

This is a contradiction to our assumption that $O(a) = n > m$.

Let us assume $n < m$ then —

$b^n = (xax^{-1})^n$

$\Rightarrow b^n = xa^n x^{-1}$ (By previous manner)

$\Rightarrow b^n = xx^{-1}$ ($\because O(a) = n$)

$\Rightarrow b^n = e$

This is again contradiction to the assumption that $O(b) = m > n$.

$\therefore m = n$

$\therefore O(a) = O(b)$ (proved)

(21) Let $a, b \in G$. Show that ~~$o(ab) = o(ba)$~~
$o(ab) = o(ba)$

Proof Let us assume $o(ab) = n$
$o(ba) = m$

If $n > m$ then ——

$(ba)^m = (ba)(ba) \cdots$ m times

$\Rightarrow (ba)^m = b(ab)(ab) \cdots (ab)a$

$\Rightarrow e = b(ab)^{m-1}a \quad (\because o(ba) = m)$

$\Rightarrow aeb = ab(ab)^{m-1}ab$

$\Rightarrow ab = (ab)^{m+1}$

$\Rightarrow (ab)^m = e$

Which is a contradiction to our assumption $o(ab) = n > m$.

Similarly, assuming $m > n$ we can reach to the contradiction that-

$o(ba) = m$

$\therefore n = m$

$\therefore o(ab) = o(ba)$ (proved)

(22) Write all complex roots of $x^6 = 1$. Show that they form a group under the usual complex multiplication

(Ans) Let us write $x = a(\cos\theta + i\sin\theta)$

$\therefore |x^6| = 1$

$\Rightarrow a^6 = 1$

$\Rightarrow a = 1$ (a = const)

$\therefore (\cos\theta + i\sin\theta)^6 = 1$

By De-Moivre's theorem —

$\cos 6\theta + i\sin 6\theta = 1$

$\Rightarrow \cos 6\theta = 1$ (comparing real part)

$\Rightarrow 6\theta = 2n\pi \quad (n = 0, 1, 2 \cdots)$

$\Rightarrow \theta = 0, \frac{2\pi}{6}, \frac{4\pi}{6}, \frac{6\pi}{6}, \frac{8\pi}{6}, \frac{10\pi}{6}$

$\therefore$ roots are given by —

$x_0 = \cos 0 + i \sin 0 = 1$

$x_1 = \cos \frac{2\pi}{6} + i \sin \frac{2\pi}{6}$

$x_2 = \cos \frac{4\pi}{6} + i \sin \frac{4\pi}{6}$

$x_3 = \cos \frac{6\pi}{6} + i \sin \frac{6\pi}{6}$

$x_4 = \cos \frac{8\pi}{6} + i \sin \frac{8\pi}{6}$

$x_5 = \cos \frac{10\pi}{6} + i \sin \frac{10\pi}{6}$

In general we can write —

$x_p = \cos\left(\frac{2\pi p}{6}\right) + i \sin\left(\frac{2\pi r}{6}\right)$

$= e^{\frac{2\pi i r}{6}}$

Let us check whether $G = \{x_0, x_1, \ldots x_5\}$ forms a group or not.

(i) Associativity $\Rightarrow$

Let $x_r, x_p, x_q \in G$

$\therefore (x_r \cdot x_p) x_q$

$= \left(e^{\frac{2\pi i r}{6}} \cdot e^{\frac{2\pi i p}{6}}\right) \cdot e^{\frac{2\pi i q}{6}}$

$= e^{\frac{2\pi i (r+p)}{6}} \cdot e^{\frac{2\pi i q}{6}}$

$= e^{\frac{2\pi i (r+q+q)}{6}}$

Then, $x_r \cdot (x_p \cdot x_q)$

$= e^{\frac{2\pi i r}{6}} \cdot e^{\frac{2\pi i (p+q)}{6}}$

$= e^{\frac{2\pi i (r+p+q)}{6}}$

$\therefore (x_r \cdot x_p) x_q = x_r \cdot (x_p \cdot x_q)$

$\therefore$ Multiplication operation in G is Associative.

(ii) Identity $\Rightarrow$ $x_0 = 1$ is identity.

$1 \in G$

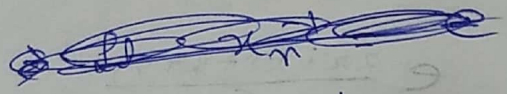
$\therefore$ Identity lies within G.

(iii) Inverse element $\Rightarrow$

Let us choose $x_r \in G$ $(0 \le r \le 5)$

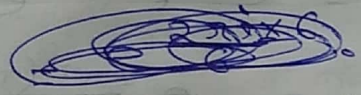
Let, x_r^{-1} be inverse of x_r.

$\therefore \quad x_r \cdot x_r^{-1} = x_r^{-1} \cdot x_r = 1$



$\therefore \quad x_r^{-1} = \dfrac{1}{x_r}$

$= e^{-\frac{2\pi i r}{6}}$



Now, $e^{\frac{2\pi i \times 6}{6}} = e^{2\pi i} = 1$

Then, $e^{-\frac{2\pi i r}{6}} = e^{2\pi i} \cdot e^{-\frac{2\pi i r}{6}}$

$= e^{\frac{2\pi i}{6}(6-r)}$

$\therefore \quad 0 \le r \le 5$

Then, $1 \le 6-r \le 6$

Now if $6-r = 6$, then

$x_r^{-1} = 1 = e$

So we can conclude $x_r^{-1} \in G$.

(iv) Closure property:

As we have proved x_r^{-1} lies in G.

In the similar fashion we can prove-

$x_r \cdot x_p \in G \quad \forall\ r, p \in G$.

$\therefore$ G forms a group. (proved)

---

(23) Let $G = \{a \in \mathbb{R}, -1 < a < 1\}$. Define a binary operation $*$ on G by

$a * b = \dfrac{a+b}{1+ab}$, $\forall\ a, b \in G$. Show that $(G, *)$ is a group.

Proof

Let us check all the requirements so that $(G, *)$ be a group.

(i) Associativity: Let $a, b, c \in G$.

Then, $(a * b) * c$

$= \left(\dfrac{a+b}{1+ab}\right) * c = \dfrac{\frac{a+b}{1+ab} + c}{1 + \frac{ac+bc}{1+ab}}$

$$= \frac{\frac{a+b+c+abc}{1+ab}}{\frac{1+ab+bc+ca}{1+ab}}$$

$$= \frac{(a+b+c+abc)(1+ab)}{(1+ab+bc+ca)(1+ab)}$$

$(\because -1 < a, b < 1,\ ab \neq -1)$

Again $a * (b * c)$

$$= a * \left(\frac{b+c}{1+bc}\right)$$

$$= \frac{a + \frac{b+c}{1+bc}}{1 + \frac{ab+ac}{1+bc}}$$

$$= \frac{a+b+c+abc}{1+ab+bc+ca} \quad (\because -1 < b, c < 1,\ bc \neq -1)$$

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

$\therefore *$ is associative in G.

(ii) **Identity element** $\Rightarrow$

Let e be the identity.

Then $a * e = e * a = a \quad \forall a \in G$

$$\Rightarrow \frac{a+e}{1+ae} = \frac{e+a}{1+ea} = a$$

$$\Rightarrow a + e = a + a^2 e$$

$$\Rightarrow e = 0$$

$e = 0 \in G$.

$\therefore$ Identity, $e = 0$ lies in G.

(iii) **Inverse element**

Let us choose c be the inverse of $a \in G$.

Then, $a * c = c * a = e$

$$\Rightarrow \frac{a+c}{1+ac} = \frac{c+a}{1+ca} = 0$$

$$\Rightarrow a + c = 0$$

$$\Rightarrow c = -a$$

Since $a \in G$ i.e $-1 < a < +1$

then $-1 < -a < 1$

$\therefore -a \in G$

$\therefore \forall a \in G$, a^{-1} exists in G.

Now given $*$ is binary operation in G.

Then closure property comes with that.

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

---

(24) Let $\langle G, * \rangle$ be a group and $a, b \in G$. Suppose that $a^2 = e$ and $a * b * a = b^7$. Prove that $b^{48} = e$

(Ans) Given $b^7 = a * b * a$

Then operating b^7, 7 times —

$$(b^7)^7 = (a * b * a)^7$$

$$\Rightarrow b^{49} = a * b * (a * a) * b * \ldots$$
$$(a * a) * b * a$$

$$\Rightarrow b^{49} = a\, b^7\, a \quad (\because a * a = a^2 = e)$$

$$\Rightarrow b^{49} = a(a * b * a)\, a \quad (\because b^7 = a * b * a)$$

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

$$\Rightarrow b^{49} = e * b * e$$

$$\Rightarrow b^{48} = e \quad \text{(proved)}$$

---

(25) Let $\langle G, * \rangle$ be a group such that $(a * b)^{-1} = a^{-1} * b^{-1}$ $\forall\, a, b \in G$, show that G is a commutative group.

(Ans) Let $a \in G$.

$b^{-1} * a^{-1}$ Let

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

$b^{-1} * a^{-1}$ $\Rightarrow$ $a^{-2} = a$

(Ans) To show that the group G is commutative we have to show that

$$a * b = b * a \quad \forall\, a, b \in G$$

Let us choose two arbitary elements $a, b \in G$.

Then, $a^{-1} \in G$ and $b^{-1} \in G$.

Now we know for any group —

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

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

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

Now by given property —

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

$= a * b \quad \ldots (2)$

Then equating eq (1) & eq (2)

$a * b = b * a$

We had chosen $a, b \in G$ arbitarily.

And shown that $a * b = b * a$

$\therefore$ G is commutative group.

---

(26) Prove that a group $(G, *)$ is commutative if $(a*b)^n = a^n * b^n$, for any three consecutive integers n and for all $a, b \in G$.

(Ans) Let a & b be any two elements of G.

Suppose $n, n+1, n+2$ be three consecutive integers such that —

$(ab)^n = a^n . b^n \quad \ldots (i)$

$(ab)^{n+1} = a^{n+1} . b^{n+1} \quad \ldots (ii)$

$(ab)^{n+2} = a^{n+2} . b^{n+2} \quad \ldots (iii)$

Then eq (ii) can be written as —

$(ab)(ab)^n = a(a^n)\, b(b^n)$

$\Rightarrow (ab)(a^n b^n) = a * a^n * b * b^n$ (By eq (i))

$\Rightarrow abab^n = aa^n bb^n$

$\Rightarrow ba^n = a^n b \quad \ldots (iv)$ (By RCL & LCL)

Again by eq (iii) we get —

$(ab)(ab)^{n+1} = a . a^{n+1} . b . b^{n+1}$

$\Rightarrow (ab)(a^{n+1} b^{n+1}) = aa^{n+1} bb^{n+1}$

$\Rightarrow ba^{n+1} = a^{n+1} b$ (By RCL & LCL)

$\Rightarrow ba^n . a = a^n ab$

$\Rightarrow a^n ba = a^n ab$ (by eq (iv))

$\Rightarrow ba = ab$ (LCL)