Swastik Nandi
CSE-'A' Roll-1751007

1) Let S be a set having exactly one element. How many different binary operations can be defined on S? Answer when S has exactly 2 elements, 3 elements, n elements.

Sol$^{n}$: No. of binary operations possible on a set of n elements is given by the formula $n^{n^2}$ (ans)

∴ for a set having exactly 1 element we get $= 1^{1^2} = 1$.

∴ for a set having exactly 2 elements we get $= 2^{2^2} = 16$.

∴ for a set having exactly 3 elements we get $= 3^{3^2} = 19683$

2. How many different commutative binary operations can be defined on a set of 2 elements? On a set of 3 elements? On a set of n elements?

Sol$^{n}$: Number of diff. commutative operations on a set of 'n' elements is given by formula $n^{\frac{n(n+1)}{2}}$

∴ for a set of 2 elements; no. of commutative binary operations are $2^{\frac{2\times3}{2}} = 2^3 = 8$

∴ for a set of 3 elements; no. of commutative binary operations are $3^{\frac{3\times4}{2}} = 3^6 = 729$.

3. Determine whether * defined as follows gives a binary operation on the set or not. If not justify. For following binary operations determine whether they are associative or commutative? Find identity element in each if they exist.

a) On $Z^+$, define $*$ by $a*b = a-b$.

Sol: Clearly $\exists\ a,b \in Z^+$ s.t when $b>a$

$a*b = a-b < 0$

$\therefore a*b \notin Z^+$

$\therefore$ Not binary operation.

| $*$ is a binary operation on a set S if,
| i) $a*b$ is unique $\forall a,b \in S$
| ii) $a*b$ exists, $\forall a,b \in S$
| iii) $a*b \in S$ $\forall a,b \in S$
| [closure].

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

Sol: All 3 properties are satisfied. So it is binary operation

Commutativity: Clearly $a*b = a^b \neq b^a = b*a$ $\forall a,b \in Z^+$

eg: $2^3 \neq 3^2$, So not commutative.

Associativity: $a*(b*c) = a^{b*c} = a^{(b^c)}$

& $(a*b)*c = (a^b)*c = (a^b)^c = a^{bc}$

[eg: $2^{3\cdot 4} = 2^{12} \neq 2^{3^4} = 2^{81}$]

Not Associative

Identity element: Assuming $\oplus$ 1 to be identity

$1*a = 1^a = 1 \neq a$.

$\therefore$ No identity exists.

c) On R, define $*$ by $a*b = a-b$

Sol: All 3 properties are satisfied. So it is a binary operation

Commutativity: $a*b = a-b \neq b-a = b*a$

$\therefore$ Not commutative.

Associativity: $a*(b*c) = a*(b-c) = a-(b-c)$
$= a-b+c$

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

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

$\therefore$ not associative.

Identity: Lets assume 0 to be identity.

$0*a = 0-a \neq a-0 = a*0$

$\therefore$ No identity exists.

(d) On R define * by $a*b = |a| + |b|$

Sol$^n$: All 3 properties satisfy. So it is a binary operation.

Commutativity: $a*b = |a| + |b| = |b| + |a| = b*a$

$\therefore$ It is commutative.

Associativity: $a*(b*c) = a*(|b| + |c|) = |a| + |b| + |c|$

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

$\therefore$ Associative.

Identity does not exist i.e. '0' might be good choice but $a \neq |a|$ if a is -ve.

Hence not possible to find identity $\forall a \in R$.

e) On Z, define * by $a*b = |a| \cdot b$

Sol$^n$: All 3 properties satisfy. Hence binary operation.

Commutativity: $a*b = |a| \cdot b \neq |b| \cdot a = b*a \quad \forall a, b \in Z$.

eg: if $a = 2$ & $b = -3$ then

$a*b = -6 \qquad b*a = 6$

$\therefore a*b \neq b*a$

$\therefore$ Not commutative.

f) Associativity: $a*(b*c) = |a| * (b*c)$
$= |a| \cdot |b| \cdot c$

$(a*b)*c = |\,|a| \cdot b| \cdot c = |a| \cdot |b| \cdot c$

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

Hence associative.

Identity does not exist i.e no 'e' exist such that $a*e = e*a = a$
(1) might seem good choice but $|a| \neq a \quad \forall a \in Z$.

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

All 3 properties satisfy. So it is a binary operation.

Commutativity : $a*b = ab+3 = ba+3 = b*a$

$\Rightarrow$ commutative

Associativity: $a*(b*c) = a*(bc+3) = abc+3a+3$ &

$(a*b)*c = (ab+3)*c = abc+3c+3$

Clearly not associative as $a*(b*c) = (a*b)*c$

Let 'e' be the identity w.r.t $*$ on $\mathbb{Q}$.

then $a*e = e*a = ae+3$

We need,

$ae+3 = a$

$\Rightarrow ae - a = 3$

$\Rightarrow ae = a+3 \Rightarrow e = +\frac{(3+a)}{a}$

Now we can see that identity is specific for each element $a \in \mathbb{Q}$ which should not be.

$\therefore$ No identity exists.

4) Either prove the following statements or give a counter-example.

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

Sol$^n$: A binary operation on a set must satisfy 3 cond$^n$s:

i) $a*b$ is unique $\forall a,b \in S$

ii) $a*b$ exists $\forall a,b \in S$

iii) $a*b \in S$ $\forall a,b \in S$ [closure]

By 3 we can say for a set S with one element (say 'a') can have only one operation defined on it.

i.e. $a*a = a$.

So clearly $a*a = a = a*a$ [commutative]

& $a*(a*a) = a*a = a = a*a = (a*a)*a$

$\Rightarrow$ Associative.

$\therefore$ Statement is true.

b) Every commutative binary operation on a set having just 2 elements is associative.

Sol^n: Counter example: Let S be a set having 2 elements 'a' & 'b'. Let * be a commutative binary operation on S; that has the following composition table:

| * | a | b |
|---|---|---|
| a | b | a |
| b | a | a |

→ this follows all 3 properties of a binary operation

→ also * is commutative; ie $a*b = b*a$

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

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

$\therefore (a*a)*b \neq a*(a*b)$ $\therefore$ Not associative.

Hence disproved.

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

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

a) closure: clearly $a*b = ab \in \mathbb{Z}$ $\forall a, b \in \mathbb{Z}$

b) Associativity: let $a, b, c \in \mathbb{Z}$

Then $a*(b*c) = a*bc = abc$ ✓

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

Hence associative

c) $1 \in \mathbb{Z}$ is the identity

$\because 1*a = a = a*1$

d) Let b be the inverse of $a \in \mathbb{Z}$.

$\therefore a*b = 1 \Rightarrow b = 1/a$

When $a=0$ b is undefined moreover $b \in \mathbb{Q}$ if $a \neq 1$. Thus inverse does not exist.

$\therefore \langle \mathbb{Z}, * \rangle$ not a group.

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

Sol$^n$ $2\mathbb{Z} = \{ \ldots, -2, 0, 2, 4, \ldots \}$

a) Closure: Clearly sum of 2 even is even.

$\therefore$ Closure satisfied.

b) Associativity: $a*(b*c) = a*(b+c) = a+b+c$

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

$\therefore$ Associativity holds.

c) Existence of identity: $0 \in 2\mathbb{Z}$ is the identity element

This is because $a*0 = a+0 = a = 0+a = 0*a \quad \forall a \in 2\mathbb{Z}$

$\therefore 0$ is the identity element.

d) Inverse: 'a' & 'b' $\in 2\mathbb{Z}$ such that b is the inverse of a

$\therefore a*b = b*a = 0$

$\Rightarrow a+b = 0 \Rightarrow b = -a$.

b is well defined $\forall a \in 2\mathbb{Z}$.

$\therefore$ Inverse exists $\forall a \in 2\mathbb{Z}$.

$\therefore \langle 2\mathbb{Z}, * \rangle$ is a group.

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

Note we are taking $a*b = \sqrt{ab}$ not $\pm\sqrt{ab}$

a) Closure: Let $a, b \in \mathbb{R}^+$, Clearly $ab \in \mathbb{R}^+$

and $\sqrt{ab}$ is thus defined $\forall a, b \in \mathbb{R}^+$

$\therefore a*b = \sqrt{ab} \in \mathbb{R}^+ \quad \forall a, b \in \mathbb{R}^+$

$\therefore$ Closure satisfied.

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

Then $a*(b*c) = a*(\sqrt{bc}) = \sqrt{a\sqrt{bc}}$

& $(a*b)*c = (\sqrt{ab})*c = \sqrt{\sqrt{ab} \cdot c}$

$\therefore$ Associativity fails.

$\Rightarrow \langle \mathbb{R}^+, * \rangle$ is not a group.

iv) $\langle R^*, * \rangle$ , $*$ given by $a * b = \frac{a}{b}$

a) Closure:

Clearly division is possible $\forall a, b \in R^*$ &

$a * b = \frac{a}{b} \in R^*$ $[R^* = R / \{0\}]$

$\therefore$ Closure satisfied.

b) Associativity:

Let $a, b, c \in R^*$.

Now $a * (b * c) = a * (b / c) = \frac{a}{b/c} = \frac{ac}{b}$ &

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

$\therefore$ Associativity fails.

$\therefore$ $\langle R^*, * \rangle$ is not a group.

v) $\langle C, * \rangle$ , $*$ is given by $a * b = |ab|$

Sol$^{n}$: It is easier to show no identity exists hence we are skipping closure & associativity parts.

Let $e$ be the identity for all $a \in C$ . we have.

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

Now $a * e = |a \cdot e| \rightarrow$ which is always a real number.

[As we take $|x+iy| = \sqrt{x^2+y^2}$]

$\therefore$ $a * e \neq a$

$\therefore$ Identity does not exist.

$\therefore$ $\langle C, * \rangle$ is not a group.

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

a) closure

Let 'i', 'j' $\in Q[\sqrt{2}]$ s.t $i = a + b\sqrt{2}$ and $j = c + d\sqrt{2}$

$[a, b, c, d \in Q]$

$\therefore i + j = (a+c) + (b+d)\sqrt{2}$

$[\because (a+c), (b+d) \in Q]$ ; so $i + j \in Q[\sqrt{2}]$

$\therefore$ closure satisfied.

b) associativity:

Let $i, j, k \in Q[\sqrt{2}]$ $\quad a, b, c, d, e, f \in Q$

s.t $i = a + b\sqrt{2}$

$j = c + d\sqrt{2}$

$k = e + f\sqrt{2}$

Now $(i+j)+k = [(a+c) + (b+d)\sqrt{2}] + e + f\sqrt{2}$

$= (a+c+e) + (b+d+f)\sqrt{2}$

& $i + (j+k) = a + b\sqrt{2} + [(c+e) + (d+f)\sqrt{2}]$

$= (a+c+e) + (b+d+f)\sqrt{2}$

$\therefore$ associativity holds.

c) Identity element:

$e = 0 + 0\sqrt{2}$ is the identity element $[0 \in Q]$

$i + e = e + i = i \quad [i = a + b\sqrt{2}]$

$\therefore$ identity exists.

d) Inverse: Let $i = a + b\sqrt{2} \quad i \in Q[\sqrt{2}]$

$j = c + d\sqrt{2}$ ; inverse of $i$

$\therefore i + j = j + i = e$

$\Rightarrow c = -a$ & $d = -b$

$c, d \in Q$ hence $j \in Q[\sqrt{2}]$ $\forall$ $i \in Q[\sqrt{2}]$.

$\therefore$ Inverse exists.

$\therefore \langle Q\sqrt{2}, + \rangle$ is a group.

vii) $\langle P(x), \Delta \rangle$ where $P(x)$ is the power set of $x$ and $\Delta$ is the symmetric difference. (4)

Soln: $x$ is a set. Then the power set $P(x)$ contains all subsets of $x$ including null set & $x$ itself.

$A \Delta B$ is defined as $A \Delta B = (A \cup B) - (A \cap B)$

a) Closure: $P(x)$ is the set of all subsets of $x$, so it must contain any possible set resulting from the symmetric difference b/w any set in $P(x)$

i.e $\forall$ sets $a, b \in P(x)$

$a \Delta b \subseteq x \Rightarrow a \Delta b \in P(x)$

$\therefore$ Closure satisfied.

b) Associativity (from Venn diagram):

$a \Delta b \rightarrow$  now $(a \Delta b) \Delta c \rightarrow$ 

similarly $a \Delta (b \Delta c)$ will lead to same fig.

Associativity holds.

c) Identity

The null set $\phi \in P(x)$ is the identity element

$\forall a \in P(x)$; $a \Delta \phi = (a \cup \phi) - (a \cap \phi) = a - \phi = a = \phi \Delta a$.

$\therefore$ Identity exists.

d) Inverse:

Every element $\in P(x)$ is its own inverse.

say $\forall a \in P(x)$

$a \Delta a = (a \cup a) - (a \cap a)$

$= a - a = \phi$

$\therefore$ Inverse $\forall a \in P(x)$.

$\therefore \langle P(x), \Delta \rangle$ is a group.

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

a) Closure:

Let $x, y \in Q[\sqrt{2}] - \{0\}$ : $x = a_1 + b_1\sqrt{2}$, $y = a_2 + b_2\sqrt{2}$ } $a_1, a_2, b_1, b_2 \in Q - \{0\}$

Then $x * y = (a_1 + b_1\sqrt{2})(a_2 + b_2\sqrt{2})$

$= (a_1a_2 + 2b_1b_2) + \sqrt{2}(a_2b_1 + a_1b_2)$

$a_1a_2 + 2b_1b_2$, $a_2b_1 + a_1b_2 \in Q - \{0\}$

$\therefore$ [let us suppose $a_1a_2 + 2b_1b_2 = 0 = a_2b_1 + a_1b_2$

So $a_1a_2 = -2b_1b_2$ ...(i) & $a_2b_1 = 0 - a_1b_2$ (ii)

$-a_1b_2 = a_2b_1$ ...(ii)

(i) ÷ (ii) $= \frac{a_1}{b_1} = 2\frac{b_1}{a_1}$

$\Rightarrow a_1 = \pm\sqrt{2}\, b_1$ .. (iv)

Now (i) ÷ (iii) $\Rightarrow \frac{a_2}{b_2} = 2\frac{b_2}{a_2} \Rightarrow a_2 = \pm\sqrt{2}\, b_2$ —(v)

Clearly (iv) & (v) contradict our assumption that $a_1, a_2, b_1, b_2 \in Q - \{0\}$

So; $(a_1a_2 + 2b_1b_2)$ & $(a_2b_1 + a_1b_2)$ cannot be simultaneously 0.

$\therefore$ Closure satisfied.

b) Associativity:

Let $x, y, z \in Q[\sqrt{2}] - \{0\}$

$x = a_1 + b_1\sqrt{2}$ ; $y = a_2 + b_2\sqrt{2}$ ; $z = a_3 + b_3\sqrt{2}$

$\therefore x * (y * z) = x * [(a_2a_3 + 2b_2b_3) + \sqrt{2}(a_3b_2 + a_2b_3)]$

$= (a_1a_2a_3 + 2a_1b_2b_3 + 2a_3b_2b_1 + 2a_2b_3b_1) +$

$\sqrt{2}(a_1a_3b_2 + a_1a_2b_3 + a_2a_3b_1 + 2b_2b_3b_1)$

$(x * y) * z = (a_1a_2a_3 + 2a_1b_2b_3 + 2a_3b_2b_1 + 2a_2b_3b_1) +$

$\sqrt{2}(a_1a_3b_2 + a_1a_2b_3 + a_2a_3b_1 + 2b_2b_3b_1)$

$\therefore$ associativity holds.

c) Identity: $e = 1 + 0\sqrt{2}$ is the identity element $\{1 \in Q^*\}$

Let $x = a_1 + \sqrt{2}b_1$,

$e * x = a_1 + \sqrt{2}b_1 = x * e$.

$\therefore$ Identity exists.

d) Let $x = a + \sqrt{2}b \in Q[\sqrt{2}] - \{0\}$

Since operation is multiplication, $e = 1$.

We have $x \cdot \left(\frac{1}{x}\right) = e \Rightarrow x^{-1} = \frac{1}{x}$

Now $x^{-1} = \frac{1}{x} = \frac{1}{a + \sqrt{2}b} = \frac{a - \sqrt{2}b}{(a + \sqrt{2}b)(a - \sqrt{2}b)}$

$= \frac{a}{a^2 - 2b^2} + \sqrt{2}\left(\frac{b}{2b^2 - a^2}\right)$

$\therefore$ Inverse exists $a \neq \sqrt{2}b$

$\therefore$ So it is a group.

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

Sol$^n$: Closure:

Let $g_1, g_2 \in G$: $g_1 \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$; $g_2 = \begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix}$; $a, b \in R^*$

Now $g_1 * g_2 = \begin{pmatrix} ab & 0 \\ 0 & 0 \end{pmatrix}$ Clearly $ab \in R^*$

$\therefore g_1 * g_2 \in G$ $\therefore$ Closure satisfied.

Associativity:

Let $g_1, g_2, g_3 \in G$: $g_1 = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$ $g_2 = \begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix}$ $g_3 = \begin{pmatrix} c & 0 \\ 0 & 0 \end{pmatrix}$

$a, b, c \in R^*$

Now $g_1 * (g_2 * g_3) = g_1 * \begin{pmatrix} bc & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} abc & 0 \\ 0 & 0 \end{pmatrix}$

$(g_1 * g_2) * g_3 = \begin{pmatrix} ab & 0 \\ 0 & 0 \end{pmatrix} * g_3$

$= \begin{pmatrix} abc & 0 \\ 0 & 0 \end{pmatrix}$

$\therefore$ Associativity holds.

c) Identity :

The identity matrix is $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \rightarrow e$

Clearly $\forall g_1 = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \in G_1 \; ; \; a \in R^* \; ;$

$g_1 * e = e * g_1 = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} = g_1$

d) Existence of inverse

Let $g_1 \in G_1 = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$

Clearly $g_1 * g_1^{-1} = g_1^{-1} * g_1 = e = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$

Hence $g_1^{-1} = \begin{pmatrix} 1/a & 0 \\ 0 & 0 \end{pmatrix} \rightarrow$ which is always defined and $\in G_1$ [because $a \in R^*$]

$\therefore$ Inverse exists for all elements (matrices) of $G_1$.

$\therefore \langle G_1, * \rangle$ is a group

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

Sol^n: Example of an abelian group G which has exactly 1000 elements can be $(Z_{1000}, +_{1000})$. Now $(Z_{1000}, +_{1000})$ is an example of an abelian group because:

i) satisfies closure property as any number modulus 1000 lies in the range 0 to 999.
ii) Addition is associative.
iii) Identity element exists (The element is 0)
iv) Every element as its inverse. Inverse of any element can be found out using $(a+b) \bmod 1000 = 0$. where a = the number and b its inverse.
v) Addition is commutative.

$\therefore$ $(Z_{1000}, +_{1000})$ is an example of abelian group having exactly 1000 elements.

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

Sol^n: Let a be an element of the finite group G. Let us consider all positive powers of a, namely

$$a, a^2, a^3, a^4, \ldots$$

Everyone of the powers must belong to G. But as G is finite, all of these elements cannot be different. Let us consider

$$a^s = a^r$$
$$\Rightarrow a^s \cdot a^{-r} = a^r \cdot a^{-r}$$
$$\Rightarrow a^{s-r} = a^0 = e$$

$\therefore$ $a^t = e$, putting $s - r = t > 0$

Thus there is a +ve integer t for which $a^t = e$.

8. Suppose that a group $G_1$ has an element $x$ such that $ax = x$ for all $a \in G_1$. Show that $G_1$ contains only identity element.

Sol$^n$: Given $ax = x$ where $a * x \in G_1$.

$\because G_1$ is a group so inverse of each element exists.

$\Rightarrow axx^{-1} = ax^{-1}$

$\Rightarrow ae = e \Rightarrow a = e$ where $e$ is the identity element

$\therefore$ The group only contains identity element.

9. Let $G_1$ be a group, $a, b \in G_1$. Show that $(aba^{-1})^n = aba^{-1}$ iff $b = b^n$.

Sol$^n$: First let us take $b = b^n$.

Given Now, $(aba^{-1})^n = aba^{-1}aba^{-1}aba^{-1} \ldots$ n times.

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

$= ab.b. \ldots b\,a^{-1}$

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

as $b = b^n$

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

Now let us consider

$(aba^{-1})^n = aba^{-1}$, we are to show $b = b^n$

$aba^{-1}aba^{-1} \ldots = aba^{-1}$

$\Rightarrow abbb \ldots a^{-1} = aba^{-1}$

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

Applying left and right cancellation property successively we get

$b = b^n$

Hence 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.

Sol$^{n}$:- An element is said to be idempotent if $a^2 = a$.

Now $a^2 = a$

$\Rightarrow a \cdot a = a$

Since $G$ is a group, identity element exists.

$\therefore a \cdot a = a \cdot e$

Through left cancellation law to get,

$a = e$

$\therefore$ The only idempotent element in $G$ is the identity element.

11. Find a solution of the equation $ax = b$ in $S_3$ where $a = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$ and $b = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$

correct solution is given in last page.

Sol$^{n}$:- Given $ax = b$

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

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

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

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

Sol$^{n}$:- Let $a \in G$, $b \in G$

Then $(a \cdot b) \in G$.

$\therefore (a \cdot b)^2 \in G$.

Now as per question

$(a \cdot b)^2 = e$.

$\therefore a\cdot b\cdot a\cdot b = e$

$\Rightarrow a\cdot b\cdot a\cdot b\cdot b = e\,b$

$\Rightarrow a\cdot b\cdot a\cdot e = eb$

$\Rightarrow a\cdot b\cdot a = b$

$\Rightarrow a\cdot b\cdot a\cdot a = b\cdot a$

$\Rightarrow a\cdot b\cdot e = b\cdot a \Rightarrow a\cdot b = b\cdot a.$

$\therefore G$ is abelian if $a^2 = e$.

When $(a\cdot b)^3 = e$

$a\cdot b\cdot a\cdot b\cdot a\cdot b = e$

$\Rightarrow a\cdot b\cdot a\cdot b\cdot a\cdot b\cdot b = e\cdot b$

$\Rightarrow a\cdot b\cdot a\cdot b\cdot a = e\cdot b$

$\Rightarrow a\cdot b\cdot a\cdot b\cdot a\cdot a = b\cdot a$

$\Rightarrow abab = ba$

$\Rightarrow ababb = bab.$

$\Rightarrow aba = bab.$

$\Rightarrow ab = baba.$

$\therefore$ Using (1) we get,

$ab = a\cdot b \neq b\cdot a.$

$\therefore G$ is not abelian if $a^3 = e$.

& $(b\cdot a)^3 = e$

$b\cdot a\cdot b\cdot a\cdot b\cdot a = e$

$\Rightarrow b\cdot a\cdot b\cdot a\cdot b\cdot a\cdot a = e\cdot a$

$\Rightarrow b\cdot a\cdot b\cdot a\cdot b = a$

$\Rightarrow b\cdot a\cdot b\cdot a\cdot b\cdot b = a\cdot b$

$\Rightarrow b\cdot a\cdot b\cdot a = a\cdot b.$ — (1)

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

Sol$^{n}$: First let $(G, \cdot)$ be abelian — (1)

Now $(a\cdot b)^2 = (a\cdot b)\cdot(a\cdot b)$

$= a\cdot(b\cdot a)\cdot b = a\cdot(a\cdot b)\cdot b$

[As $G$ is abelian $ab = ba$]

$= (a\cdot a)\cdot(b\cdot b)$ [Using associativity].

$= a^2\cdot b^2$

Next let $(a\cdot b)^2 = a^2\cdot b^2 \quad \forall\ a,b \in G$.

Then $(a\cdot b)^2 = a^2\cdot b^2$

$\Rightarrow (a\cdot b)\cdot(a\cdot b) = (a\cdot a)\cdot(b\cdot b)$

$\Rightarrow a\cdot(b\cdot a)\cdot b = a\cdot(a\cdot b)\cdot b$ [Using associativity].

Using left and right cancellation property successively we get, $b\cdot a = a\cdot b$

Hence $(G,\cdot)$ is abelian.

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

Sol$^{n}$: Let $A = \{g \in G \mid g \neq g^{-1}\} \subseteq G$.

$\therefore e \notin A$.

If $g \in A$, then $g^{-1}$ should also belong to $A$. As a result of which all the elements in $A$ occur in pair. Thus $A$ is an even set.

Now $e \cup A$ is an odd set.

Since the no: of elements in $G$ is even & $e \cup A \subseteq G$

$\exists\ a \in G$, s.t $a \notin \{e\} \cup A$

Hence there exists $a \in G$, where $a = a^{-1}$ since $G$ is a group & every element should have inverse.

$\therefore a = a^{-1} \Rightarrow a^2 = e$. (proved).

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

Sol$^{n}$: Let $G = \langle \mathbb{Z}, + \rangle$ and $H = \langle 2\mathbb{Z}, + \rangle$ $K = \langle 3\mathbb{Z}, + \rangle$

Now $H$ & $K$ are subgroups of $G$.

Clearly $2 \in H$, $3 \in K$ $\therefore 2, 3 \in H \cup K$ but $2+3 = 5 \notin H \cup K$

$\therefore$ It violets closure property.

Hence $H \cup K$ is not a subgroup.

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

Sol$^{n}$:- Given K is a subgroup of H.

& H is a subgroup of G.

Now $K \subset H \subset G$.

The closure of K is not changed and it holds in both ways. Now as K is a subgroup of H thus

$$e_K = e_H \quad \text{also} \quad e_H = e_G$$

$$\Rightarrow e_K = e_H = e_G$$

$$\therefore e_K = e_G$$

Associativity is inherited.

Let $a \in K$, $a^{-1} \in K$.

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

as H is a subgroup of G.

$$\Rightarrow a^{-1} \in G.$$

$\therefore$ inverse of a also exists in G.

$\therefore$ K is a subgroup of G (proved)

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

Sol$^{n}$:- Let $H = \{x : x^2 = e\}$

Now $x^2 = e \Rightarrow x = x^{-1}$

$\therefore$ If $x \in H$, $x^{-1} \in H$

Further, $e^2 = e$

$\therefore$ Identity element of G also belongs to H.

Let $x, y \in H$

As per question,

$$xy = yx$$

Now $y = y^{-1}$ & $x = x^{-1}$

$$\Rightarrow xy = y^{-1}x^{-1} = (xy)^{-1} \quad [\text{as G is abelian}]$$

$\therefore xy \in H$. $\Rightarrow$ H is a subgroup of G

$\therefore$ Closure is satisfied.

Now associativity is inherited from G.

$\Rightarrow$ H is a subgroup of G (proved)

18) Show that a group cannot be expressed as a union of two proper subgroups.

Sol$^n$: Let us consider that union of 2 proper subgroups is a subgroup.

Since $H_1 \not\subset H_2$, $\exists\ a \in H_1$ s.t $a \notin H_2$

Similarly $H_2 \not\subset H_1$, $\exists\ b \in H_2$ s.t $b \notin H_1$

As we are assuming $H_1 \cup H_2$ is a subgroup

$$a \cdot b \in H_1 \cup H_2$$

$\Rightarrow$ Either $a \cdot b \in H_1$ or $a \cdot b \in H_2$

If $a \cdot b \in H_1$, then we have

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

As both $a^{-1}$ & $a \cdot b$ belongs to $H_1$, b should also belong to $H_1$. This contradicts our choice of element b.

Similarly $(a \cdot b) \in H_2$ we have

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

This contradicts our choice of a.

In either case it is a contradiction. Thus $H_1 \cup H_2$ is not a subgroup of G.

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

Sol$^n$: Example of a group not cyclic is $S_3$.

The elements of $S_3$ are $s_0, s_1, s_2, s_3, s_4, s_5$ where

$s_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = e$; $s_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1\,2\,3)$; $s_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (1\,3\,2)$

$\rho_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (1\ 3)$ ; $\rho_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = (1\ 2)$

$\rho_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = (2\ 3)$

Now all the cyclic subgroups of $S_3$ are

$\langle \rho_0 \rangle = \{\rho_0\}$ ; $\langle \rho_1 \rangle = \{\rho_0, \rho_1, \rho_2\}$ $(\because \rho_1^2 = \rho_2 \ \ \rho_1^3 = \rho_0)$

$\langle \rho_2 \rangle = \{\rho_0, \rho_1, \rho_2\}$ $(\because \rho_2^2 = \rho_1 \ \ \rho_2^3 = \rho_0)$

$\langle \rho_3 \rangle = \{\rho_0, \rho_3\}$ $(\because \rho_3^2 = \rho_0)$

$\langle \rho_4 \rangle = \{\rho_0, \rho_4\}$ $(\because \rho_4^2 = \rho_0)$

$\langle \rho_5 \rangle = \{\rho_0, \rho_5\}$ $(\because \rho_5^2 = \rho_0)$

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

Sol$^{n}$: Let us assume that $O(a) = n$ $O(b) = m$ such that $n \neq m$. i.e $m$ and $n$ are least positive integers such that $[n, m \in Z^+]$

$a^n = e$ & $b^m = e$ respectively

Now, $b = xax^{-1}$ for some $x \in G$.

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

$\Rightarrow (xax^{-1})(xax^{-1}) \ldots$ $m$ times $= e$.

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

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

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

$\Rightarrow xa^m = x$

$\Rightarrow a^m = e$.

$\therefore$ If $m < n$

then $O(a) = m$ → a contradiction as $O(a) = n$.

If $r < m$

$$b^n = x a^n x^{-1} = x e x^{-1} = x x^{-1} = e.$$

which is a contradiction as $o(b) = m$.

Hence we have $m = n$

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

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

Sol$^n$: Let order of $ab = t$.

$\therefore (ab)^t = e$

$\Rightarrow (a\cdot b)(a\cdot b)(a\cdot b) \ldots$ $t$ times $= e$.

$\Rightarrow a\cdot(b\cdot a)\cdot(b\cdot a) \ldots b = e$

($\hookrightarrow t-1$ times)

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

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

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

$\Rightarrow (b\cdot a)^{t-1} \cdot b \cdot b^{-1} = a^{-1} \cdot b^{-1} = (ba)^{-1}$

$\Rightarrow (b\cdot a)^{t-1} = (ba)^{-1}$

$\Rightarrow (b\cdot a)^{t-1} \cdot (ba)^1 = (ba)^{-1} \cdot (ba)^1$

$\Rightarrow (b\cdot a)^{t-1+1} = e$

$\Rightarrow (b\cdot a)^t = e.$

$\therefore$ order of $ba = t$.

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

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

Sol$^n$: We have:

$x^6 - 1 = 0$

$\Rightarrow (x^3-1)(x^3+1) = 0$

$\Rightarrow [(x-1)(x^2+x+1)][(x+1)(x^2-x+1)] = 0$

Now $(x-1)=0$

$\Rightarrow x = +1 + 0i \quad \ldots (i)$

Also $x+1=0$

$\Rightarrow x = -1 + 0i \quad \ldots (ii)$

also $(x^2+x+1)=0$

$\Rightarrow x = \frac{-1 \pm \sqrt{-3}}{2}$

$\Rightarrow x = -\frac{1}{2} \pm \frac{\sqrt{3}}{2} i \quad \ldots (iii)$

or $x = -\frac{1}{2} - \frac{\sqrt{3}}{2} i \quad \ldots (iv)$

and $(x^2-x+1)=0$

$\Rightarrow x = \frac{1 \pm \sqrt{-3}}{2} \Rightarrow x = \frac{1}{2} + \frac{\sqrt{3}}{2} i \quad \ldots (v)$

or $x = \frac{1}{2} - \frac{\sqrt{3}}{2} i \quad \ldots (vi)$

(i) to (vi) are all complex roots of $x^6 = 1$.

Let $S = \{(i), (ii), (iii) \ldots (vi)\}$

Let us examine the algebraic str. $\langle G, \cdot \rangle$ • implies usual complex multiplication.

a) Closure

Let 'x' and 'y' $\in S$ be chosen randomly.

$\therefore x = 1^{1/6}$ and $y = 1^{1/6}$

Now $x \cdot y = (1)^{1/6} \cdot (1)^{1/6} = (1)^{2/6} = (1)^{1/6}$

$\therefore$ S contains 6th roots of unity so $x \cdot y \in S$.

$\therefore$ closure satisfied.

b) Associativity

Inherited from complex no: set.

c) Existence of Identity

$e = 1 + 0i$ ; we can check $\alpha \cdot e = e \cdot \alpha = \alpha \quad \forall \alpha \in S$.

d) Inverse

Let '$x$' $\in S$. Let $y$ be it's inverse such that:

$yx = xy = 1$

$\Rightarrow xy = 1 \Rightarrow y = \frac{1}{x}$

$\Rightarrow y^6 = \frac{1}{x^6} = 1.$

$\Rightarrow y = (1)^{1/6}$

$\Rightarrow y \in S.$

$\therefore \forall x, \exists y \in S$ ; s.t $xy = e$ $\therefore$ Inverse exists.

Hence $\langle S, \cdot \rangle$ is a group satisfying all 4 properties.

2) Let $G = \{a \in R, -1 < a < 1\}$. Define a binary operation $*$ on $G$ by $a * b = \frac{a+b}{1+ab}$ $\forall a, b \in G$. Show that $\langle G, * \rangle$ is a group.

Sol$^{n}$:

a) Closure

Let $x, y \in G \Rightarrow x^2 < 1$ and $y^2 < 1$

$1 - x^2 > 0$ & $1 - y^2 > 0$

$(1-x^2)(1-y^2) > 0 \cdots$ (i) $\Rightarrow -[(1-x^2)(1-y^2)] < 0 \cdots$ (ii)

Now $(x+y)^2 - (1+xy)^2$

$= x^2 + y^2 + 2xy \mp 1 \mp x^2y^2 - 2xy$

$= -[1 - x^2 - y^2 + x^2y^2]$

$= -[1(1-x^2) - y^2(1-x^2)]$

$= -[(1-x^2)(1-y^2)]$

$\therefore (x+y)^2 - (1+xy)^2 < 0$ - (using ii)

$\Rightarrow (x+y)^2 < (1+xy)^2$

$\Rightarrow \left(\frac{x+y}{1+xy}\right)^2 < 1$ $\therefore -1 < \frac{x+y}{1+xy} < 1$

$-1 < x+y < 1$

$\therefore x + y \in G$ ; closure satisfied.

b) Associativity

Let $a, b, c \in G$

Now $(a*b)*c = \left(\frac{a+b}{1+ab}\right)*c = \frac{\frac{a+b}{1+ab} + c}{1 + \frac{a+b}{1+ab}.c} = \frac{a+b+c+abc}{1+ab+bc+ca}$ ... (i)

& $a*(b*c) = a*\left(\frac{b+c}{1+bc}\right) = \frac{a + \frac{b+c}{1+bc}}{1 + \frac{b+c}{1+bc}.a} = \frac{a+b+c+abc}{1+ab+bc+ca}$ ... (ii)

∴ From (i) & (ii) we see that it is associative.

c) Existence of identity

Let e be the identity $a*e = e*a = a \quad \forall a \in G$.

Now $a*e = e*a = \frac{a+e}{1+ae} = a$.

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

$\Rightarrow e = a^2e$

Now as $a \neq 1$ or $-1$ so we can't cancel e from both sides

∴ 0 is the identity element.

d) Inverse

Let $a \in G$, $a^{-1}$ be the inverse.

$a * a^{-1} = e = 0$

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

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

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

∴ $\langle G, * \rangle$ is a group.

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

Sol$^n$: We have $a^2 = e$ i.e $a * a = e$ i.e $a = a^{-1}$.

Now $a * b * a = b^7$

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

$\Rightarrow b = a * b^7 * a$ ... (i)

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

$\Rightarrow a * b * a * a * b * a \cdots$ 7 times $= b^{49}$

$\Rightarrow a * b^7 * a = b^{49}$ [as $a^2 = e$]

$\Rightarrow b = b^{49}$

$\Rightarrow b * b^{-1} = b^{49} * b^{-1}$

$\Rightarrow b^{48} = e$. (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 commutative.

Sol$^n$: Since $G$ is a group; by closure $a * b \in G$; and hence

$\forall a, b \in G$

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

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

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

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

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

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

$\Rightarrow a * b = b * a$.

$\therefore G$ is commutative.

26) Prove that a group $(G,*)$ is commutative if $(a*b)^n = a^n * b^n$ for any 3 consecutive integers $n$ & $\forall a, b \in G$.

Soln: According to the problem we have

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

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

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

Now $(a\cdot b)^{n+2} = (a\cdot b)^{n+1} \cdot (a\cdot b)$

$\Rightarrow a^{n+2} \cdot b^{n+2} = a^{n+1} \cdot b^{n+1} \cdot a \cdot b$ by (ii) & (iii)

$\Rightarrow a\cdot(a^{n+1} \cdot b^{n+1}) \cdot b = a\cdot(a^n \cdot b^n)\cdot(b\cdot a)\cdot b$

$\Rightarrow a^{n+1} \cdot b^{n+1} = (a^n \cdot b^n)\cdot(b\cdot a)$

Using LCL & RCL respectively.

$\Rightarrow (a\cdot b)^{n+1} = (a\cdot b)^n \cdot (b\cdot a)$ .. using (i) & (ii)

$\Rightarrow (a\cdot b)^n \cdot (a\cdot b) = (a\cdot b)^n \cdot (b\cdot a)$

$\Rightarrow a\cdot b = b\cdot a$ by LCL.

$\therefore (G,*)$ is commutative.

Soln of 11 (corrected)

$$ax = b$$

$$\Rightarrow x = a^{-1}\cdot b$$

Now $a = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$ ; $a^{-1} = \begin{pmatrix} 3 & 2 & 1 \\ 1 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$

$$\therefore x = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \rightarrow (\text{dns})$$

—x—