Solution Model

1a) $M = \left\{ \begin{pmatrix} a & a \\ b & b \end{pmatrix} : a+b \neq 0 \ \& \ a,b \in \mathbb{R} \right\}$

For semigroup, M must satisfy closure & associative property.

Let $A = \begin{pmatrix} a & a \\ b & b \end{pmatrix}$, $A' = \begin{pmatrix} c & c \\ d & d \end{pmatrix} \in M$

$\Rightarrow a+b \neq 0$; $c+d \neq 0$ & $a,b,c,d \in \mathbb{R}$

Now, $A \circ A' = \begin{pmatrix} a & a \\ b & b \end{pmatrix} \cdot \begin{pmatrix} c & c \\ d & d \end{pmatrix} = \begin{pmatrix} a(c+d) & a(c+d) \\ b(c+d) & b(c+d) \end{pmatrix}$

Now, $a(c+d) + b(c+d) = (a+b)(c+d) \neq 0$ $\left[\because \begin{matrix} a+b \neq 0 \\ \& \ c+d \neq 0 \end{matrix} \right]$

Also, $a(c+d)$ & $b(c+d) \in \mathbb{R}$ $\because a,b,c,d \in \mathbb{R}$.

$\Rightarrow A \circ A' \in M$ $\Rightarrow$ M is <u>closed</u> under $\circ$.

For associativity, let us take $A'' = \begin{pmatrix} e & e \\ f & f \end{pmatrix} \in M$

Then, $(A \circ A') \circ A'' = \left(\begin{pmatrix} a & a \\ b & b \end{pmatrix} \circ \begin{pmatrix} c & c \\ d & d \end{pmatrix} \right) \circ \begin{pmatrix} e & e \\ f & f \end{pmatrix} = \begin{pmatrix} a(c+d) & a(c+d) \\ b(c+d) & b(c+d) \end{pmatrix} \begin{pmatrix} e & e \\ f & f \end{pmatrix}$

$$= \begin{pmatrix} a(c+d)(e+f) & a(c+d)(e+f) \\ b(c+d)(e+f) & b(c+d)(e+f) \end{pmatrix}$$

Also, $A \circ (A' \circ A'') = \begin{pmatrix} a & a \\ b & b \end{pmatrix} \circ \left(\begin{pmatrix} c & c \\ d & d \end{pmatrix} \circ \begin{pmatrix} e & e \\ f & f \end{pmatrix} \right)$

$$= \begin{pmatrix} a(c+d)(e+f) & a(c+d)(e+f) \\ b(c+d)(e+f) & b(c+d)(e+f) \end{pmatrix}$$

$\because (A \circ A') \circ A'' = A \circ (A' \circ A'')$

$\Rightarrow$ M is <u>associative</u> under '$\circ$'.

$\Rightarrow$ M is a semigroup.

a ii) Let $\begin{pmatrix} a & x \\ y & y \end{pmatrix} \in M$ s.t

$$\begin{pmatrix} x & x \\ y & y \end{pmatrix} \circ \begin{pmatrix} a & a \\ b & b \end{pmatrix} = \begin{pmatrix} a & a \\ b & b \end{pmatrix}$$

$$\Rightarrow \begin{pmatrix} x(a+b) & x(a+b) \\ y(a+b) & y(a+b) \end{pmatrix} = \begin{pmatrix} a & a \\ b & b \end{pmatrix}$$

$$\Rightarrow x(a+b) = a \ ; \ y(a+b) = b$$

$$\Rightarrow \frac{x}{y} = \frac{a}{b} \ \& \ x+y = 1 \quad [\because a+b \neq 0$$

$$\Rightarrow \frac{x}{1-x} = \frac{a}{b}$$

$$\therefore x = \frac{a}{a+b} \ \& \ y = \frac{b}{a+b}$$

$\because$ x & y depends on a & b, the value differs as a, b differs. Thus left identity doesn't exists.

Right identity exists: $\begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}$ can be a right identity.

1.6

Given, $(M, \circ)$ is monoid

1. finit
2. e is the only idempotent element ie $a^2 = a \Rightarrow a = e$

Let $a \neq e \in M$

then $a, a^2, a^3 \cdots a^m \cdots \in M$

since M is finite then. $a^m = a^n$ — (1) for some $n \in \mathbb{N}$, $m \neq n$

either $m > n$ or $m < n$.

Without loss of generality let $n > m$.

Then $\boxed{a^m = a^{m+(n-m)}}$ — (11) from (1) $n - m \neq 0$

$\Rightarrow$ Now, $a^{m+2(n-m)} = a^{m+(n-m)} \cdot a^{n-m}$

$= a^{m+(n-m)}$ as by (11)

$= a^m$ by (11)

Similarly, $a^{m+k(n-m)} = a^m$ — (111) for all $k > 1$

Let $t = m + k_1(n-m)$ where k_1 is an integer such that $t > 2m$

$\Rightarrow a^t = a^m$ by (111)

we can multiply a^{t-2m} as $t - 2m > 0$

$\Rightarrow a^t \cdot a^{t-2m} = a^m \cdot a^{t-2m}$

$\Rightarrow a^{2t-2m} = a^{t-m}$

$\Rightarrow a^{2(t-m)} = a^{t-m}$

$\Rightarrow$ this implies a^{t-m} is idempotent.

as e is the idempotent $\Rightarrow a^{t-m} = e \Rightarrow a a^{t-m-1} = a^{t-m-1} \cdot a = e$

$\Rightarrow a^{t-m-1}$ is inverse of a

1c) Yes $(G, \circ)$ is a commutative group as —

Closure: $r_\theta \circ r_\phi = r_{\theta+\phi} \in G$ as $\theta, \phi \in \mathbb{R} \Rightarrow \theta + \phi \in \mathbb{R}$

Associativity: $(r_\theta \circ r_\phi) \circ r_\alpha = (r_{\theta+\phi}) \circ r_\alpha = r_{\theta+\phi+\alpha} = r_\theta \circ (r_\phi \circ r_\alpha)$

Identity: $r_0 \circ r_\theta = r_{0+\theta} = r_\theta = r_{\theta+0} = r_\theta \circ r_0$; r_0 = identity elem

Inverse: $r_\theta \circ r_{-\theta} = r_0 = r_{-\theta} \circ r_\theta$

$\Rightarrow r_{-\theta}$ is the inverse of r_θ.

Commutativity: $r_\theta \circ r_\phi = r_{\theta+\phi}$, $r_\phi \circ r_\theta = r_{\phi+\theta}$

$\because \theta + \phi = \phi + \theta$

$\Rightarrow r_{\theta+\phi} = r_{\phi+\theta}$

$\Rightarrow r_\theta \circ r_\phi = r_\phi \circ r_\theta$

2a:

$o(a) = 3$

$\Rightarrow a^3 = e$

Given, $a \circ b \circ a^{-1} = b^2$

$(a \circ b \circ a^{-1}) \circ (a \circ b \circ a^{-1}) = b^4$

$\Rightarrow a \circ b^2 \circ a^{-1} = b^4$

$\Rightarrow a \circ (a \circ b \circ a^{-1}) \circ a^{-1} = b^4$

$\Rightarrow a^2 \circ b \circ a^{-2} = b^4.$

$\Rightarrow (a^2 \circ b \circ a^{-2}) \circ (a^2 \circ b \circ a^{-2}) = b^4 \circ b^4$

$\Rightarrow (a^2 \circ b^2 \circ a^{-2}) = b^4 \circ b^4$

$\Rightarrow a^2 \circ (a \circ b \circ a^{-1}) \circ a^{-2} = b^4 \circ b^4$

$\Rightarrow a^3 \circ b \circ a^{-3} = b^4 \circ b^4$

$\Rightarrow b = b^8$

$\Rightarrow b^7 = e$

$\Rightarrow o(b) = 7.$ [$\because$ 7 is a prime] we have

2 a ii) $a^{-1}b^2a = b^3$

$\Rightarrow b^2a = ab^3$

$\Rightarrow b^2ab^{-2} = ab$. —①

$\Rightarrow b^2a^3b^{-2} = (ab)^3$

$\Rightarrow b^2(b^{-1}a^2b)b^{-2} = (ab)^3$.

$\Rightarrow b\,a^2b^{-1} = (ab)^3$ —②

Also

$b^{-1}a^2b = a^3$.

Also, from ① we have

$b^2a^2b^{-2} = (ab)^2$.

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

So, from ② we have

$b(b^{-2}(ab)^2b^2)b^{-1} = (ab)^3$.

$\Rightarrow b^{-1}(ab)^2b = (ab)^3$.

$\Rightarrow (ab)^2 = (ba)^3$.

Similarly we can show that $(ba)^2 = (ab)^3$. —③

Now, $(ab)^2 = (ba)^3$

$= (ba)(ab)^3.$

$\Rightarrow baab = e$

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

Similarly we can show from ③ that

$ab^2a = e.$

Now $a^{-1} b^2 a = b^3.$

$b^2 a = a b^3$

$\Rightarrow a b^2 a = a^2 b^3$

$\Rightarrow \underline{a^2 b^3 = e}.$

$a b^2 a = e$

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

$\Rightarrow b^2 = a^{-2}.$

$\Rightarrow \underline{a^2 b^2 = e}.$

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

$\Rightarrow \boxed{b = e.}$

Similarly we can show that $\underline{a = e}.$

2b i. $G = \langle a \rangle \quad O(a) = 30.$

$a^{30} = e$

Let $H = \langle a^{18} \rangle$

$$O(a^{18}) = \frac{O(a)}{\gcd(18, 30)} = \frac{30}{6} = 5$$

$\therefore |H| = 5$

b ii) $|H| = 6$

$$O(a^{\alpha}) = \frac{O(a)}{\gcd(\alpha, 30)} = 6$$

$\Rightarrow \gcd(\alpha, 30) = 5$

$\Rightarrow \alpha = 5$

$\therefore H = \{a^5, a^{10}, a^{15}, a^{20}, a^{25}\}$

generators are : a^5 & a^{25}

2c i) $(ab)\cdot(ab)$

$= ab \cdot ba \quad [\because a$ & b commute$]$

$= ab^2a \quad [\because b^2 = e]$

$= a^2$

$= e \quad [\because a^2 = e]$

$\therefore O(ab) = 2$

c ii) $(aba^{-1})(aba^{-1})$

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

$= aea^{-1}$

$= aa^{-1}$

$= e$

$\Rightarrow O(aba^{-1}) = 2$

c iii) If G is abelian, then by (2c i), ab is another element of order 2 & if G is non abelian then by (2c ii), aba^{-1} is another element of order 2.

3. a)

Let G be a group of order 8

ie $o(G) = 8$

and let H is a subgroup of G, then $o(H) \mid o(G)$

So. $o(H) = 1, 2, 4, 8$.

Hence if H is proper subgroup then $o(H) = 1, 2, 4$.

if $o(H) = 1$ then trival group. ie. cyclic

if $o(H) = 2$ then H is cyclic as 2 is prime

if $o(H) = 4$ then, let a bie an element of H.

the $o(a) = 1, 2, 4$.

Case 1| Let $\exists$ an element $a \in H$ s.t $o(a) = 4$

then this is cyclic $\Rightarrow$ H is commutative

Case 2| if there does exist no element of order 4 in H

then all non-identity element is self inverse of itself

Hence in this case also H is commutative.

b) $$gHg^{-1} = \{ghg^{-1} \mid h \in H\}$$

wher G is a group & H is subgroup of G.

th $gHg^{-1} \subset G$ and e = identity of G is in gHg^{-1}

So. gHg^{-1} is non-empty subset of G.

Let $a = gh_1g^{-1}$ where $h_1 \in H$

then $a \in gHg^{-1}$

and let $b = gh_2g^{-1}$ where $h_2 \in H$

$\Rightarrow b \in gHg^{-1}$

Now
$$\boxed{\begin{aligned} ab &= gh_1g^{-1} \cdot gh_2g^{-1} \\ &= gh_1h_2g^{-1} \in gHg^{-1} \end{aligned}} \quad \text{— (1)}$$
as H is subgroup so $h_1h_2 \in H$

and $a^{-1} = (gh_1g^{-1})^{-1} = gh_1^{-1}g^{-1}$

then $\boxed{a^{-1} \in gHg^{-1}}$ — (ii) as H is subgroup so $h_1^{-1} \in H$

from (i) & (ii) we can conclude gHg^{-1} is subgroup of G.

c) $H = \{ax + by : x, y \in \mathbb{Z}\}$

$H \subset \mathbb{Z}$ & $\mathbb{Z}$ is group & $0 \in H$.

& let $g_1 = ax_1 + by_1$, $g_2 = ax_2 + by_2$

then $g_1 + g_2 = a(x_1 + x_2) + b(y_1 + y_2) \in H$

& $-g_1 = -ax_1 - by_1 \in H$

Hence H is a subgroup of $\mathbb{Z}$.

& let $d = \gcd(a,b)$

$\Rightarrow$ $d \mid a$ & $d \mid b$ — (i)

Let $g = ax + by$ any element of H.

then $d \mid (ax + by)$ [from (i))

Hence $ax + by = d\, d_1$ for some integer $d_1 \in \mathbb{Z}$.

$\Rightarrow$ $ax + by = d_1 \cdot \gcd(a,b)$.

Hence $H = \{ax + by : x, y \in \mathbb{Z}\}$

$= \{d_1 \gcd(a,b) : d_1 \in \mathbb{Z}\}$

$\Rightarrow$ H is cyclic group generated by $\gcd(a,b)$.

4 a) Here given $o(a) = 3 \Rightarrow a^3 = e$

& $[G : H] = 10$ & H is normal subgroup of G

$\Rightarrow$ G/H is a group of order 10.

$\Rightarrow$ $aH \in G/H$. $a \in G$

$\Rightarrow$ Since order of G/H is 10

$\Rightarrow$ $(aH)^{10} = H$ $\Rightarrow$ $a^{10} H = H$

$\Rightarrow$ $aH = H$ (as $a^3 = e$)

$\Rightarrow$ $a \in H$. proved.

4 b

$\boxed{\text{We know that } H \text{ is a normal subgroup of } G \text{ iff } \forall h \in H, g \in G \text{ then } \Rightarrow g^{-1}hg \in H.}$

Here given $x \in G \Rightarrow x^2 \in H$

Let $g \in G$ $h \in H$.

Now, $g^{-1}hg = g g^{-1} g^{-1} g h g$

$= (g^{-1})^2 h^{-1} h g h g$

$= (g^{-1})^2 h^{-1} (hg)^2$

Since $g^{-1} \in H$, $h^{-1} \in H$ & $(hg)^2 \in H$

$\Rightarrow g^{-1}hg \in H$.

Hence H is normal subgroup of G.

Since $a^2 \in H$

$\Rightarrow a^2 H = H$

$\Rightarrow aH = a^{-1}H$.

Now,

$aH \cdot bH = abH$

$(ab)^2 H = H$

$\Rightarrow abH = (ab)^{-1} H$

$= b^{-1} \cdot a^{-1} H$

$= b^{-1}H \cdot a^{-1} H$

$= bH \cdot aH$

Hence $aH \cdot bH = bH \cdot aH$

$\Rightarrow G/H$ is abelian.