a] let $G_1 = \left\{ \begin{bmatrix} a & a \\ a & a \end{bmatrix} : a \in R,\ a \neq 0 \right\}$

Show that G_1 is Group under matrix multiplication.

Sol^n :- Closure property :-

let $x = \begin{bmatrix} a & a \\ a & a \end{bmatrix}$, $y = \begin{bmatrix} b & b \\ b & b \end{bmatrix}$, $a, b \in R$

$$x \cdot y = \begin{bmatrix} a & a \\ a & a \end{bmatrix} \begin{bmatrix} b & b \\ b & b \end{bmatrix}$$

$$= \begin{bmatrix} ab+ab & ab+ab \\ ab+ab & ab+ab \end{bmatrix}$$

$$= \begin{bmatrix} 2ab & 2ab \\ 2ab & 2ab \end{bmatrix} \quad \left\{ \begin{array}{l} \because a, b \in R \\ 2ab \in R \end{array} \right.$$

$\therefore x \cdot y \in G_1$

associativity :- let $z = \begin{bmatrix} c & c \\ c & c \end{bmatrix}$ $\because c \in R$

$$(x \cdot y) z = \left(\begin{bmatrix} a & a \\ a & a \end{bmatrix} \begin{bmatrix} b & b \\ b & b \end{bmatrix} \right) \begin{bmatrix} c & c \\ c & c \end{bmatrix}$$

$$= \begin{bmatrix} 2ab & 2ab \\ 2ab & 2ab \end{bmatrix} \begin{bmatrix} c & c \\ c & c \end{bmatrix}$$

$$(x \cdot y) z = \begin{bmatrix} 4abc & 4abc \\ 4abc & 4abc \end{bmatrix} \quad \text{---(1)}$$

$$(x)(y.z) = \begin{bmatrix} a & a \\ a & a \end{bmatrix} \cdot \left(\begin{bmatrix} b & b \\ b & b \end{bmatrix} \begin{bmatrix} c & c \\ c & c \end{bmatrix} \right)$$

$$= \begin{bmatrix} a & a \\ a & a \end{bmatrix} \begin{bmatrix} 2bc & 2bc \\ 2bc & 2bc \end{bmatrix}$$

$$= \begin{bmatrix} 4abc & 4abc \\ 4abc & 4abc \end{bmatrix}$$

$\therefore (x \cdot y) \cdot (z) = (x) \cdot (yz)$

Identity:-

Let $e \in G \Rightarrow e = \begin{bmatrix} x & x \\ x & x \end{bmatrix} \; x \in R$

$x \cdot e = x$

$\therefore \begin{bmatrix} a & a \\ a & a \end{bmatrix} \cdot e = \begin{bmatrix} a & a \\ a & a \end{bmatrix}$

$$\begin{bmatrix} a & a \\ a & a \end{bmatrix} \begin{bmatrix} x & x \\ x & x \end{bmatrix} = \begin{bmatrix} a & a \\ a & a \end{bmatrix}$$

$$\begin{bmatrix} 2ax & 2ax \\ 2ax & 2ax \end{bmatrix} = \begin{bmatrix} a & a \\ a & a \end{bmatrix}$$

$\therefore 2ax = a$

$\therefore x = 1/2$

$\therefore e = \begin{bmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{bmatrix}$ is identity.

Let $x, y \in R$ s.t. $x \neq 0$

$x \cdot y = e$

$$\therefore \begin{bmatrix} a & a \\ a & a \end{bmatrix} \begin{bmatrix} b & b \\ b & b \end{bmatrix} = \begin{bmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{bmatrix}$$

$$\therefore \begin{bmatrix} 2ab & 2ab \\ 2ab & 2ab \end{bmatrix} = \begin{bmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{bmatrix}$$

$\therefore 2ab = 1/2$

$b = \frac{1}{4a}$ $\quad \because a \neq 0$

$\therefore b$ is well defined.

$$\therefore y = x^{-1} = \begin{bmatrix} 1/4a & 1/4a \\ 1/4a & 1/4a \end{bmatrix}$$

b] Let F be a Field of order 32 show that the only subfield of F are F itself and {0,1}

Sol?

Result:- Let $\mathbb{F}_q$ be Finite field with $q = p^n$ elements. then every subfield of $\mathbb{F}_q$ has order p^m, where m is a positive divisor of n. conversly, if m is a positive divisor of n, then there is exactly one subfield of $\mathbb{F}_q$ with p^m elements.

In ours case $|F| = 32 = 2^5$
only possible divisor of 5 are 1 and 5

∴ only posible subfield are F and {0,1}

6] Prove or disprove that $(\mathbb{R}, +)$ and $(\mathbb{R}^+, \cdot)$ are isomorphic groups where $\mathbb{R}^+$ denots set of all positive Real no. - (3)

Soln:-

Let $f: \mathbb{R} \to \mathbb{R}^+$

$$f(x) = e^x$$

to prove f is well defined.

$$x = y$$
$$\Rightarrow e^x = e^y$$
$$\Rightarrow f(x) = f(y)$$

conversly we can prove

$$f(x) = f(y)$$
$$\Rightarrow e^x = e^y$$
$$\Rightarrow x = y$$

$\therefore$ f is one-one.

$\forall \; y \in \mathbb{R}^+ \quad \exists \; x \in \mathbb{R} \ni$

$$f(x) = y$$
$$\Rightarrow e^x = y$$
$$\Rightarrow x = \log y$$

$\therefore$ f is onto.

$$f(x+y) = e^{x+y}$$
$$= e^x \cdot e^y$$
$$= f(x) \cdot f(y)$$

$\therefore$ f is one-one-onto and homomorphism

$\therefore$ f is isomorphic

from $(\mathbb{R}, +) \to (\mathbb{R}^+, \cdot)$

a] Show that zero and unity are only idempotents of Z_n if $n = p^r$ where p is a prime. --- (13)

Soln We know $Z_n \cong \frac{Z}{\langle n \rangle}$

Let $\langle n \rangle + m$ be an idempotent of $\frac{Z}{\langle n \rangle}$.

then $(\langle n \rangle + m)^2 = \langle n \rangle + m$

$\Rightarrow \langle n \rangle + m^2 = \langle n \rangle + m$

$\Rightarrow m^2 - m \in \langle n \rangle$

$\Rightarrow n \mid m^2 - m = m(m-1)$

$\Rightarrow p^r \mid m(m-1)$

$\because$ g.c.d $(m, m-1) = 1$

$\therefore p^r \mid m$ or $p^r \mid m-1$

If $n = p^r \mid m$, then

$\langle n \rangle + \langle m \rangle = \langle n \rangle$

if $n = p^r \mid m-1$ then

$m - 1 = nK$

$\Rightarrow \langle n \rangle + m = \langle n \rangle + nK + 1$

$= \langle n \rangle + 1$

$\therefore$ zero and unity are the only idempotents of $\frac{Z}{\langle n \rangle}$ when $n = p^r$