Answer on Question #44738 – Math – Abstract Algebra:

Let $S = \left\{\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \mid a, b \in \mathbb{Z}\right\}$.

(a) Check that S is a subring of $M_2(\mathbb{R})$ and it is a commutative ring with identity.
(b) Is S an ideal of $M_2(\mathbb{R})$? Justify your answer.
(c) Is S an integral domain? Justify your answer.
(d) Find all the units of the ring S.
(e) Check whether $I = \left\{\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \in S \mid 2|a\right\}$is an ideal of S.
(f) Show that S is congruent to $\mathbb{Z} \times \mathbb{Z}$ where the addition and multiplication operations are componentwise addition and multiplication.

Solution.

(a)

We need to check the following properties:

$$\forall A, B \in S: A + B, A \cdot B \in S;$$
$$\forall A, B \in S: A \cdot B = B \cdot A;$$
$$\exists e \in S: \forall A \in S: A \cdot e = A;$$

So:

$$A, B \in S \Longrightarrow A = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}, B = \begin{pmatrix} c & 0 \\ 0 & d \end{pmatrix} \Longrightarrow \begin{cases} A + B = \begin{pmatrix} a + c & 0 \\ 0 & b + d \end{pmatrix} \in S \\ A \cdot B = \begin{pmatrix} ac & 0 \\ 0 & bd \end{pmatrix} \in S \end{cases};$$

$$B \cdot A = \begin{pmatrix} ca & 0 \\ 0 & db \end{pmatrix} = \begin{pmatrix} ac & 0 \\ 0 & bd \end{pmatrix} = A \cdot B;$$

$$e = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in S, A = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \Longrightarrow A \cdot e = \begin{pmatrix} a \cdot 1 & 0 \\ 0 & b \cdot 1 \end{pmatrix} = A.$$

So, S is a commutative ring with identity e.

(b)

Prove that S is not ideal of $M_2(\mathbb{R})$.

Assume the contrary.

$$S \text{ is an ideal} \Longrightarrow \forall A \in M_2(\mathbb{R}), \forall X \in S: A \cdot X \in S;$$
$$e \in S \Longrightarrow \forall A \in M_2(\mathbb{R}): A \cdot e = A \in S \Longrightarrow S = M_2(\mathbb{R});$$

But, for example, $A = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \notin S.$

So, our assumption doesn't hold and S is not ideal.

(c)

S is not an integral domain, because:

$$A = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \neq 0, B = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \neq 0, A \cdot B = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = 0.$$

(d)

Assume that $x = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$ is a unit of the ring S. So:

$$\exists y = \begin{pmatrix} c & 0 \\ 0 & d \end{pmatrix} \in S: x \cdot y = e;$$

$$x \cdot y = \begin{pmatrix} ac & 0 \\ 0 & bd \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \Longrightarrow ac = bd = 1;$$

$$a, c \in \mathbb{Z}, ac = 1 \Longrightarrow \left[\begin{array}{l} a = c = 1 \\ a = c = -1 \end{array}\right.;$$

Hence:

$$a, b = \pm 1 \Longrightarrow x \in \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \right\}.$$

So, there are 4 units in S: $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$.

(e)

$$A \in S, B \in I \Longrightarrow A = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}, B = \begin{pmatrix} 2n & 0 \\ 0 & m \end{pmatrix} \Longrightarrow A \cdot B = \begin{pmatrix} 2an & 0 \\ 0 & bm \end{pmatrix} \in I.$$

So, I is an ideal of S.

(f)

We need to show that the mapping $f: S \to \mathbb{Z} \times \mathbb{Z}, f\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} = (a, b)$ is an isomorphism of rings.

Note that f is bijective. Show that f saves both operations:

$$A, B \in S \Longrightarrow A = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}, B = \begin{pmatrix} c & 0 \\ 0 & d \end{pmatrix};$$

$$f(A \cdot B) = f\begin{pmatrix} ac & 0 \\ 0 & bd \end{pmatrix} = (ac, bd) = (a, b)(c, d) = f(A)f(B);$$

$$f(A + B) = f\begin{pmatrix} a + c & 0 \\ 0 & b + d \end{pmatrix} = (a + c, b + d) = (a, b) + (c, d) = f(A) + f(B);$$

$$f(0_S) = (0,0) = 0_{\mathbb{Z} \times \mathbb{Z}};$$

$$f(e_S) = (1,1) = e_{\mathbb{Z} \times \mathbb{Z}}.$$

So, f is an isomorphism of rings.