Consider \( \mathbb{R} \times \mathbb{R} \) with its usual coordinate-wise addition and a new multiplication given by
\[
(a, b) \cdot (c, d) = (ac - bd, ad + bc).
\]

Show that \( \mathbb{R} \times \mathbb{R} \) is a field.

**Proof:**

Closed under \( \cdot \): \((a, b) \cdot (c, d) = (ac - bd, ad + bc) \in \mathbb{R} \times \mathbb{R} \).

Associative under \( \cdot \): clear.

Zero: \((0, 0) \in \mathbb{R} \times \mathbb{R} \).

Additive inverse: \(- (a, b) = (-a, -b)\).

Commutative +: clear.

Commutative \( \cdot \): clear from the definitions above.

Associative \( \cdot \):
\[
(a, b) \cdot ((c, d) \cdot (e, f)) = (ac - bd, ad + bc) \cdot (e, f)
= ((ac - bd)e - (ad + bc)f, (ac - bd)f + (ad + bc)e)
= (ace - bde - adf - bcg, ace - bde - adf - bcg + ade + bce)
= (a(ce - df) - b(de + cf) - a(cf + de) + b(cf - de), (a, b) \cdot (ce - df, cf + de) = (a, b) \cdot (ce - df, cf + de) = (a, b) \cdot (ce - df, cf + de) = (a, b) \cdot (ce - df, cf + de))
\]

Distributive:
\[
(a, b) \cdot ((c, d) + (e, f)) = (a, b) \cdot (c + e, d + f)
= (a(c + e) - b(d + f), a(d + f) + b(c + e))
= (ac + ae - bd - bf, ad + a f + bc + be)
= (ac - bd, ad + bc) + (ae - bf, a f + be)
= (a, b)(c, d) + (a, b)(e, f),
\]

Commutative -: clear since \( ac - bd = ca - db \).

One: \((1, 0) \cdot (a, b) = (a, b) = (a, b)(1, 0)\).

Multiplicative inverse \( I \): \((a, b) \neq (0, 0), \) then \((a, b)^{-1} = \left(\frac{a}{a^2 + b^2}, \frac{-b}{a^2 + b^2}\right) \) (check).
An element $e \in R$ is idempotent if $e^2 = e$.

(a) Find some idempotent elements in $M(2 | R)$.

\[
\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \text{ and } \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}
\]

are clearly idempotent.

Less clear are the following two:

\[
\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}; \quad \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}
\]

Examples of idempotent linear transformations come from projection onto a subspace.

(b) Find all idempotents in $\mathbb{Z}_4$.

\[
\begin{align*}
0 \cdot 0 &= 0 & 5 \cdot 5 &= 5 & 10 \cdot 10 &= 10 \\
1 \cdot 1 &= 1 & 6 \cdot 6 &= 6 & 11 \cdot 11 &= 11 \\
2 \cdot 2 &= 2 & 7 \cdot 7 &= 7 \\
3 \cdot 3 &= 3 & 8 \cdot 8 &= 8 & \text{Answer:} \{0, 1, 4, 9\}
\end{align*}
\]

(c) Prove that the only idempotents in an integral domain are $0_R$ and $1_R$.

Proof: If $e \in R$ and $e^2 = e$. Then,

\[
e(e - 1_R) = e - e = 0_R \quad \Rightarrow \quad e = 0_R
\]

or \[e - 1_R = 0_R.
\]

Therefore, $e = 1_R$ or $e = 0_R$. \( \square \)
# 5 in 3.2  Let $S, T$ be subrings of a ring $R$.
(a) Is $S \cup T$ a subring?
Yes: closure of $+:
\begin{align*}
a \in S, b \in T &\implies a+b \in S \cup T \\
a, b \in S &\implies a+b \in S \\
0 \in S &\implies 0 \in S \cup T \\
\text{additive inverse: } -a \in S &\implies (-a) \in S \cup T.
\end{align*}
\text{Closure of $\cdot$: } a, b \in S \implies a,b \in S \cup T.

(In fact, an intersection of an arbitrary collection of subrings of $R$ is a subring.)

(b) Is $S \cap T$ a subring?
No: Example $\mathbb{Z} = \{0, \pm 2, \pm 4, \ldots \} \subset \mathbb{Z}$
is a subring. And $3 \mathbb{Z} = \{0, \pm 3, \pm 6, \ldots \} \subset \mathbb{Z}$
is a subring. But $2+3 = 5 \notin (2\mathbb{Z} \cup 3\mathbb{Z})$, so it fails closure under $+$.

# 7 in 3.2
(a) Let $S = \{ r \in \mathbb{Z}_{10} : 5r = 0 \}$ List the elements of $S$. Is $S$ a subring of $\mathbb{Z}_{10}$?

$S = \{0, 2, 4, 6, 8\}$. This is clearly a subring (multiples of two).

(b) Let $B = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$. And let $S = \{ A \in M(R) : AB = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \}$ What does a typical element look like? Is it a subring of $M(R)$?
\[(a, b)(1, 0) = (b, 0) = (0, 0) \iff b = a = 0\]

So, \[S = \{ (a, 0) : a, c \in \mathbb{R} \}\]

This is a subring. Clearly, closed under +, has zero and has additive inverses.

Closed under \*: \[(a, 0)(a', 0) = (aa', 0)\]

(c) Let \(R\) be a ring, and let \(b \in R\). Let \[S = \{ r \in R : rb = 0R \}\]

Prove that \(S\) is a subring of \(R\).

Proof: Choose \(r, s \in S\) \[rb = 0R, \quad sb = 0R \]

So, \(r + s \in S\).

Zero: \(0R \cdot b = 0R \)

Additive inverses: If \(rb = 0R\), then since \(-0R = 0R\), \(-rb = 0R\).

By Theorem 3.5(2), \(-rb = (-r)b\)

Therefore \((r - s)b = 0R\). Hence \((r - s) \in S\).

\[S\text{ is called the subring of } R \text{ ""annihilated by } b\]""

which ""annihilates \(b\). When \(R\) is noncommutative, you need to differentiate between right and left annihilators.
#8 in 3.2 Let R be a ring, and let
\[ C = \{ a \in R : ra = ar \text{ for every } r \in R \} \]

(a) When \( R = M(2, \mathbb{R}) \), find at least one element that is not in \( C \) and at least three elements that are in \( C \).

\[ a = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad ; \quad \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \]
\[ \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix} \]
\( \therefore \) Not equal.

So \( a \notin C \).

But \( \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \text{ and } \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \) are in \( C \).

(b) If \( R \) is any ring, prove that \( C \) is a subring of \( R \).

Closure under +: \( a, b \in C \Rightarrow a \in R \).

Then \( (a+b)R = aR + bR = 2a + 2b = 2(a+b) \).

\[ \therefore (a+b) \in C \quad ; \quad \text{zero or } 0 \in R \Rightarrow 0 \in C \quad ; \quad \text{additive inverses: } \quad a \in C \Rightarrow -a \in R \Rightarrow \]
\[ 2a = -(2a) \Rightarrow -2a = -(2a) \quad \Rightarrow \]
\[ \therefore 2(-a) = (-a)R \quad \Rightarrow \quad a \in C \]

Multiplication: \( a, b \in C \Rightarrow aR \Rightarrow \)
\[ (ab)R = a(bR) = a(b)R = (ab)(R) \]
\[ = (2a)(b) = 2(ab) \quad \Rightarrow \quad abR \Rightarrow \]
\[ (C \text{ is called the center of the ring } R) \]

#10 in 3.2 Is the set of units in a ring of 1 a subring?

No. \( \text{ (units of } \mathbb{Z} ) = \{ 1, -1 \} \). \( 1 + 1 \) is not a unit.