A: Suppose that $R$ is a commutative ring with identity. Prove that $R$ is a field if and only if $\{0_R\}$ is a maximal ideal of $R$

**SOLUTION:** Assume that $R$ is a commutative ring with identity. We denote the additive and multiplicative identities $0_R$ and $1_R$ of $R$ by 0 and 1, respectively. We will prove that $R$ is a field if and only if $\{0\}$ is a maximal ideal of $R$.

First of all, assume that $R$ is a field. Let $I = \{0\}$. By definition, a field $R$ contains at least two elements (since $1 \neq 0$) and so we have $I \neq R$. Furthermore, suppose that $J$ is any ideal of $R$ containing $I$, but not equal to $I$. Then $J$ contains at least one nonzero element $a$. Since $R$ is a field, $a$ is a unit of $R$, and hence $ba = 1$ for some $b \in R$. Thus, $1 \in J$. Then, for any $r \in R$, we have $r = r \cdot 1 \in J$. It follows that $J = R$. We have verified that $I = \{0\}$ is indeed a maximal ideal of $R$.

Now assume that $\{0\}$ is a maximal ideal of $R$. In particular, $\{0\} \neq R$. Hence $R$ has at least one nonzero element $a$. Since $1 \cdot a = a$ and $0 \cdot a = 0$, it follows that $1 \cdot a \neq 0 \cdot a$, and therefore $1 \neq 0$. It remains to prove that every nonzero element of $R$ is a unit of $R$.

For that purpose, suppose that $a \in R$ and $a \neq 0$. Consider $I = Ra$, the principal ideal generated by $a$. This ideal $I$ contains $a$ and hence $I \neq \{0\}$. But $0 \in I$ and so we have $\{0\} \subseteq I$. Since $I \neq \{0\}$ and we are assuming that $\{0\}$ is a maximal ideal of $R$, it follows that $I = R$. That is, $Ra = R$. Hence there exists an element $r \in R$ such that $ra = 1$. We also have $ar = 1$ since $R$ is a commutative ring. Therefore, $a$ is indeed a unit of $R$. We have proved that $R$ is a field.

Alternatively, one can use the result stated in class. Suppose that $R$ is a commutative ring with identity. Then $\{0\}$ is a maximal ideal of $R$ if and only if $R/\{0\}$ is a field. Since $R/\{0\}$ is isomorphic to $R$, it again follows that $R$ is a field if and only if $\{0\}$ is a maximal ideal of $R$.

B: Suppose that $R$ is an integral domain. Suppose that $a, b \in R$. Prove that $(a) = (b)$ if and only if $b = ua$ where $u \in U(R)$.

**SOLUTION:** Suppose that $R$ is an integral domain. Suppose that $a, b \in R$. Consider the principal ideals $(a)$ and $(b)$ of the ring $R$ generated by $a$ and $b$, respectively. Note that, if $c, d \in R$, then

$$\text{(1)} \quad (c) \subseteq (d) \iff c \in (d) \iff c = dr \text{ for some } r \in R.$$
Therefore, if \((a) = (b)\), then we obtain two equations: \(a = br\) for some \(r \in R\) and \(b = as\) for \(s \in R\). Therefore, we have

\[
(2) \quad a = br = (as)r = a(sr) .
\]

We now consider two cases. First, assume that \(a = 0\). Then \(b = as = 0s = 0\). Thus, \(b = a = 0\). We then have \(a = 1 \cdot b\). Note that \(1 \in U(R)\).

Now we consider the case where \(a \neq 0\). By equation (2), we have \(a \cdot 1 = a = a(sr)\). Thus, we have \(a \cdot 1 = a \cdot (sr)\). Since \(R\) is an integral domain and \(a \neq 0\), we can use the cancellation law to conclude that \(1 = sr\). Hence \(r \in U(R)\). Thus, we have \(a = br\) and \(r\) is a unit of \(R\).

In both cases, we have proved that \((a) = (b)\) implies that \(a = ub\), where \(u \in U(R)\).

Now we prove the converse. Suppose that \(a = ub\) where \(u \in U(R)\). Since \(u \in R\), equation (1) then implies that \((a) \subseteq (b)\). Since \(u\) is a unit of \(R\), there exists a \(v \in R\) such that \(vu = 1\). The equation \(a = ub\) implies that \(va = vub = 1b = b\). Thus, \(b = va\) where \(v \in R\) and so we can use equation (1) again to conclude that \((b) \subseteq (a)\). Thus, we have proved that \((a) \subseteq (b)\) and that \((b) \subseteq (a)\). Therefore, \((a) = (b)\). We have now proved that if \(a = ub\) where \(u \in U(R)\), then \((a) = (b)\).

C: Let \(R\) be the ring of continuous real-valued functions on the interval \((0, 1)\). Let

\[
I = \{ f \in R \mid f(1/2) = 0 \text{ and } f(1/3) = 0 \} .
\]

Prove that \(I\) is an ideal of \(R\). Prove that \(I\) is not a prime ideal of \(R\).

SOLUTION: This problem concerns the ring \(R\) of continuous real-valued functions on the interval \((0, 1)\). Let

\[
I = \{ f \in R \mid f(1/2) = 0 \text{ and } f(1/3) = 0 \} .
\]

We will prove that \(I\) is an ideal of \(R\). One can prove this in a rather direct way using the definition of \(I\). Here is an alternative approach. Define a map \(\varphi\) from \(R\) to the ring \(\mathbb{R} \times \mathbb{R}\) as follows:

\[
\varphi(f) = (f(1/2), f(1/3))
\]

for all \(f \in R\). We will verify that \(\varphi\) is a ring homomorphism. to see this, suppose that \(f, g \in R\). We have
\[ \varphi(f + g) = ( (f + g)(1/2), (f + g)(1/3) ) = ( f(1/2) + g(1/2), f(1/3) + g(1/3) ) \]
\[ = ( f(1/2), f(1/3) ) + ( g(1/2), g(1/3) ) = \varphi(f) + \varphi(g) \]
and also
\[ \varphi(fg) = ( (fg)(1/2), (fg)(1/3) ) = ( f(1/2)g(1/2), f(1/3)g(1/3) ) \]
\[ = ( f(1/2), f(1/3) ) ( g(1/2), g(1/3) ) = \varphi(f)\varphi(g) . \]
thus, \( \varphi \) is a ring homomorphism. We know that \( \text{Ker}(\varphi) \) is an ideal in \( R \). By definition, we have
\[ \text{Ker}(\varphi) = \{ f \in R \mid ( f(1/2), f(1/3) ) = (0, 0) \} \]
\[ = \{ f \in R \mid f(1/2) = 0 \text{ and } f(1/3) = 0 \} = I . \]
Therefore, \( I \) is an ideal of \( R \).

To show that \( I \) is not a prime ideal of \( R \), just take \( f \) and \( g \) defined by
\[ f(x) = x - 1/2 \quad \text{and} \quad g(x) = x - 1/3 \]
for all \( x \in (0, 1) \). Note that \( f \) and \( g \) are continuous functions on \( (0, 1) \) and so \( f, g \in R \). Note also that \( f(1/3) \neq 0 \) and so \( f \notin I \). Also, \( g(1/2) \neq 0 \) and so \( g \notin I \). However, \( (fg)(1/2) = f(1/2)g(1/2) = 0 \) and \( (fg)(1/3) = f(1/3)g(1/3) = 0 \). Hence \( fg \in I \). Therefore, \( I \) is not a prime ideal of \( R \).

D: This question concerns idempotents in a ring \( R \). Suppose that \( R \) is a commutative ring with identity. As usual, let \( 1_R \) denote the multiplicative identity element in \( R \). Suppose that \( e \) is an idempotent in \( R \). Thus, \( e \in R \) and \( e^2 = e \).

(a) Let \( f = 1_R - e \). Show that \( f \) is an idempotent element of \( R \). Furthermore, show that \( ef = 0_R \) and \( fe = 0_R \).

SOLUTION: In this problem, \( R \) is a commutative ring with identity \( 1_R \). For brevity, we will write \( 1 \) for \( 1_R \) and \( 0 \) for \( 0_R \). We assume that \( e \) is an idempotent in \( R \). Thus, \( e^2 = e \).

Consider \( f = 1 - e \). We will use elementary facts about rings. We have
\[ f^2 = ff = (1-e)(1-e) = (1-e)1-(1-e)e = 1-e-(e-e^2) = 1-e-e+e^2 = 1-e+e = 1-e = f . \]
We have used the fact that \( e^2 = e \) in this calculation. Thus, we indeed have \( f^2 = f \) and so \( f \) is an idempotent in \( R \).
Finally, note that
\[ ef = e(1 - e) = e - e^2 = e - e = 0_R \quad \text{and} \quad fe = (1 - e)e = e - e^2 = e - e = 0_R , \]

exactly as stated in the problem.

(b) Let \( S = Re \) and \( T = Rf \). Thus, \( S \) is the principal ideal of \( R \) generated by \( e \) and \( T \) is the principal ideal of \( R \) generated by \( f \). In particular, \( S \) and \( T \) are subrings of \( R \). Prove that \( S \) and \( T \) are commutative rings with identity.

**SOLUTION:** As pointed out in the problem, \( S \) and \( T \) are subrings of the commutative ring \( R \). Therefore, it is clear that multiplication in \( S \) and \( T \) is commutative. We must just show that \( S \) and \( T \) have an identity element. Both arguments are the same and so we just give the argument for \( S \).

Note that \( S \) contains \( re \) for all \( r \in R \). In particular, \( S \) contains \( 1e = e \). We will show that \( e \) is an identity element for \( S \). Suppose that \( s \in S \). Thus, \( s = re \) for some \( r \in R \). We have
\[
se = (re)e = re = r(e^2) = re = s
\]
Since \( S \) is a commutative ring, we also have \( es = s \). Thus, for all \( s \in S \), we have \( se = s \) and \( es = s \). This shows that \( e \) is indeed an identity element for \( S \). Of course, as we have shown, the identity element for a ring (if it exists) is unique and so \( e \) is the identity element for the ring \( S \).

A similar argument works for \( T \). The identity element in \( T \) is \( f \).

(c) Prove that \( S \cap T = \{ 0_R \} \).

**SOLUTION:** Clearly, \( S \cap T \) contains \( 0_R \). Now suppose that \( a \in S \cap T \). Since \( a \in S \), we have \( ae = a \). Since \( a \in T \), we have \( af = a \). Therefore,
\[
a = af = (ae)f = a(ef) = a(0_R) = 0_R .
\]
Therefore, \( S \cap T = \{ 0_R \} \), as stated.

(d) Find all the idempotent elements in the ring \( R = \mathbb{Z} \times \mathbb{Z} \).

**SOLUTION:** Suppose that \( a, b \in \mathbb{Z} \) and that \( (a, b)^2 = (a, b) \). This means that \( (a^2, b^2) = (a, b) \). Hence \( a^2 = a \) and \( b^2 = b \). Thus, \( a \) and \( b \) are idempotents in the ring \( \mathbb{Z} \). It is clear that \( a = 0 \) or \( a = 1 \) are the only possibilities. (Recall a previous homework problem which
asserts that the only idempotents in any integral domain are the additive and multiplicative identities.) Thus, the idempotents in the ring \( \mathbb{Z} \times \mathbb{Z} \) are

\[
(0, 0), \quad (1, 0), \quad (0, 1), \quad (1, 1).
\]

E: Give an example of a ring which has exactly three distinct ideals.

**SOLUTION:** One such example is the ring \( R = \mathbb{Z}/25\mathbb{Z} \). The two obvious ideals are \( R \) itself and \( \{0_R\} \). Since \( R \) is a commutative ring with identity, we can also consider principal ideals. One such ideal is \( R\alpha \), where \( \alpha = 5 + 25\mathbb{Z} \). One sees easily that this ideal consists of the elements \( 5k + 25\mathbb{Z} \), where \( k \in \{0, 1, 2, 3, 4\} \). Thus, \( R\alpha \) is an ideal with 5 elements, and so is different than the two other ideals mentioned before.

No other ideals exist in the ring \( R \). This is because an ideal of \( R \) must be a subgroup of the underlying additive group of \( R \). Since the underlying additive group of \( R \) is a cyclic group of order 25, we know from group theory that the only subgroups of \( R \) have orders 1, 5, and 25, and that there is a unique subgroup of each of those possible orders. Hence \( R \) cannot have more than the three ideals already described.

F: Consider the ring \( R = \mathbb{Z}[i] \). Let \( I = (5) \), the principal ideal of \( R \) generated by 5. Show that the quotient ring \( R/I \) is not a field.

**SOLUTION:** The ideal \( I \) can be described explicitly as follows:

\[
I = (5) = \{ r5 \mid r \in R \} = \{ 5(a + bi) \mid a, b \in \mathbb{Z} \} = \{ 5a + 5bi \mid a, b \in \mathbb{Z} \}
\]

Let \( \alpha = 2 + i \) and \( \beta = 2 - i \). From the above description, we see that \( \alpha \) and \( \beta \) are not in \( I \). Therefore, \( \alpha + I \) and \( \beta + I \) are nonzero elements of the quotient ring \( R/I \). Notice that \( \alpha\beta = 5 + 0i \) is in the ideal \( I \). Hence

\[
(\alpha + I)(\beta + I) = \alpha\beta + I = I,
\]

which is the additive identity element of \( R/I \). Therefore, the ring \( R/I \) has zero-divisors.

In any field \( F \), every nonzero element is a unit of \( F \). As proved in class, the set of units form a group and is therefore closed under multiplication. Thus, a product of nonzero elements in \( F \) is also nonzero. Therefore, a field \( F \) cannot have zero-divisors.

Since \( R/I \) has zero-divisors, it follows that \( R/I \) is not a field.
Let \( R \) be a commutative ring. Let \( N \) denote the set of nilpotent elements in \( R \). As explained in class, \( N \) is an ideal of \( R \). Prove that the quotient ring \( R/N \) has no nonzero nilpotent elements.

**SOLUTION:** Consider the quotient ring \( R/N \). Every element of \( R/N \) has the form \( a + N \), where \( a \in R \). Suppose that \( \alpha \) is a nilpotent element of \( R/N \). We have \( \alpha = a + N \) where \( a \in R \). Since \( \alpha \) is nilpotent, we have \( \alpha^n = 0_{R/N} \) for some positive integer \( n \). Now

\[
\alpha^n = (a + N)^n = a^n + N
\]

and so the fact that \( \alpha^n = 0_{R/N} \) means that \( a^n + N = 0 + N = N \). Therefore, we have \( a^n \in N \).

Since \( a^n \in N \), it follows that \( a^n \) is a nilpotent element of \( R \). Thus, we have \( (a^n)^m = 0_R \) for some positive integer \( m \). Now \( (a^n)^m = a^{nm} \) and so we have \( a^{nm} = 0_R \). Of course, \( nm \) is a positive integer and therefore \( a \) is a nilpotent element of \( R \). It follows that \( a \in N \). Therefore, \( \alpha = a + N = N \). That is, we have \( \alpha = 0_{R/N} \). We have proved that the only nilpotent element in the ring \( R/N \) is the zero element of that ring.