1. **(Hungerford 3.1.6 b)** Let \( k \) be a fixed integer. Show that the set of multiples of \( k \) is a subring of \( \mathbb{Z} \).

**Solution.** Let \( k\mathbb{Z} = \{kn : n \in \mathbb{Z}\} \) denote the set of multiples of \( k \).

Let \( a, b \in k\mathbb{Z} \). Then, \( a = km \) and \( b = kn \) for some \( m, n \in \mathbb{Z} \). We have that
\[
a + b = km + kn = k(m + n) \in k\mathbb{Z} \quad \text{(closure of +)}
\]
\[
ab = (km)(kn) = k(kmn) \in k\mathbb{Z} \quad \text{(closure of \cdot)}
\]

By properties of 0, we have that \( 0 = k0 \in k\mathbb{Z} \).

Let \( a \in k\mathbb{Z} \) and write \( a = km \). Then, \( -a = -km = k(-m) \in k\mathbb{Z} \).

Therefore, applying the subring theorem we have shown that \( k\mathbb{Z} \) is a subring of \( \mathbb{Z} \).

2. **(Hungerford 3.1.11 and 41)** Let \( S \subset M_2(\mathbb{R}) \) be the set of matrices of the form \( \begin{pmatrix} a & a \\ b & b \end{pmatrix} \).

(a) Prove that \( S \) is a ring.

(b) Show that \( J = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \) is a right identity (that is, \( AJ = A \) for all \( A \in S \)). Show that \( J \) is not a left identity by finding a matrix \( B \in S \) such that \( JB \neq B \).

(c) Prove that the matrix \( \begin{pmatrix} x & x \\ y & y \end{pmatrix} \) is a right identity in \( S \) if and only if \( x + y = 1 \).

**Solution.**

(a) Recall that \( M_2(\mathbb{R}) \) with standard matrix addition and multiplication is a ring. We will show that \( S \subset M_2(\mathbb{R}) \) is a subring, and thus is itself a ring.

Let \( M, N \in S \) and write \( M = \begin{pmatrix} a & a \\ b & b \end{pmatrix} \) and \( N = \begin{pmatrix} c & c \\ d & d \end{pmatrix} \) for some \( a, b, c, d \in \mathbb{R} \). It follows that
\[
M + N = \begin{pmatrix} a & a \\ b & b \end{pmatrix} + \begin{pmatrix} c & c \\ d & d \end{pmatrix} = \begin{pmatrix} a + c & a + c \\ b + d & b + d \end{pmatrix} \in S \quad \text{(closure of +)}
\]
\[
MN = \begin{pmatrix} a & a \\ b & b \end{pmatrix} \begin{pmatrix} c & c \\ d & d \end{pmatrix} = \begin{pmatrix} ac + ad & ac + ad \\ bc + bd & bc + bd \end{pmatrix} \in S \quad \text{(closure of \cdot)}
\]

Let \( a = 0 \) and \( b = 0 \), then \( 0 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \in S \).
Let $M \in S$ and write $M = \begin{pmatrix} a & a \\ b & b \end{pmatrix}$. Then,

$$\begin{pmatrix} a & a \\ b & b \end{pmatrix} + \begin{pmatrix} -a & -a \\ -b & -b \end{pmatrix} = 0,$$

so that $-M = \begin{pmatrix} -a & -a \\ -b & -b \end{pmatrix} \in S$.

Therefore, by the subring theorem $S$ is a subring of $M_2(\mathbb{R})$ and furthermore, is a ring on its own.

(b) Let $M = \begin{pmatrix} a & a \\ b & b \end{pmatrix}$. It follows that

$$\begin{pmatrix} a & a \\ b & b \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a \cdot 1 + a \cdot 0 & a \cdot 1 + a \cdot 0 \\ b \cdot 1 + b \cdot 0 & b \cdot 1 + b \cdot 0 \end{pmatrix} = \begin{pmatrix} a & a \\ b & b \end{pmatrix},$$

so that $J$ is a right identity.

However,

$$\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$$

so $J$ is not a left identity.

(c) (\implies) Suppose $\begin{pmatrix} x & x \\ y & y \end{pmatrix}$ is a right identity. Then, for all $M = \begin{pmatrix} a & a \\ b & b \end{pmatrix} \in S$ we have that

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

Multiplying the left hand side we get,

$$\begin{pmatrix} ax + ay & ax + ay \\ bx + by & bx + by \end{pmatrix} = \begin{pmatrix} a & a \\ b & b \end{pmatrix}.$$

Equating the entries of the matrices leaves the equations $ax + ay = a$ and $bx + by = b$. By cancellation, $a(x + y) = a$ implies that $x + y = 1$.

(\impliedby) Suppose $x + y = 1$. By matrix multiplication, it follows that

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

Therefore, $J$ is a right identity.

3. (Hungerford 3.1.21) Show that the subset $R := \{0, [2], [4], [6], [8]\} \subset \mathbb{Z}_{10}$ is a subring of $\mathbb{Z}_{10}$ and that $R$ is a ring with identity.

Solution. Notice that $[a] \in R$ if and only if $a$ when divided by 10 leaves an even remainder.

Let $[a], [b] \in R$, and write $a = 10k + 2j$ and $b = 10k' + 2j'$ for some $j = 0, 1, 2, 3, 4$. By the Division Algorithm, there exist unique $q, r \in \mathbb{Z}$ such that $a + b = 10q + r$ with $0 \leq r < 10$. By substitution, we see that $a + b = 10(k + k') + 2(j + j') = 10q + r$. Therefore, $r = 10(k + k' - q) + 2(j + j') = 2(5(k + k' - q) + (j + j'))$ which implies that $2|r$. We conclude that $[a] + [b] \in R$ (closure of $+$).

Similarly, we can write $ab = 10q + r$ with $0 \leq r < 10$. By substitution it follows that $ab = (10k + 2j)(10k' + 2j') = 10q + r$. Solving for $r$ we see that $2|r$. We conclude that $[a][b] \in R$ (closure of $\cdot$).

By definition $[0] \in R$.

Let $[a] \in R$ and write $a = 10k + 2j$ where $0 \leq 2j \leq 8$. Then, $-a = -10k - 2j = -10(k + 1) + 2(5 - j)$ and $0 \leq 2(5 - j) \leq 8$, which shows that $-a$ has an even remainder. Therefore, $[-a] \in R$.

By the subring theorem, $R$ is a subring of $\mathbb{Z}_{10}$.
Notice that

\[
\begin{align*}
4. & \quad [6][2] = [12] = [2] \\
6. & \quad [6][6] = [36] = [6]
\end{align*}
\]

Thus, [6] is an identity for \( R \).

4. \textbf{(Hungerford 3.1.26)} Let \( L = \{ a \in \mathbb{R} : a > 0 \} \). Define a new addition and multiplication on \( L \) by

\[
a \oplus b = ab \quad \text{and} \quad a \otimes b = a^{\ln b}.
\]

Prove that \( L \) is a commutative ring with identity. (Note there was a mistake in the original problem that is corrected here)

\textbf{Solution.}\ First, we show that \((L, \oplus, \otimes)\) is a ring. We freely use the properties of normal + and \( \cdot \) on \( \mathbb{R} \). Let \( a, b, c \in L \)

(a) \text{(closure for} \( \oplus \)) If \( a > 0 \) and \( b > 0 \) then \( ab > 0 \). Thus, \( a \oplus b = ab > 0 \) and \( a \oplus b \in L \).

(b) \text{(associative} \( \oplus \)) \( (a \oplus b) \oplus c = (ab) \oplus c = (ab)c = abc \) and \( a \oplus (b \oplus c) = a \oplus (bc) = ab = abc \).

Therefore \( (a \oplus b) \oplus c = a \oplus (b \oplus c) \).

(c) \text{(commutative} \( \oplus \)) \( a \oplus b = ab = ba = b \oplus a \).

(d) \text{(zero)} \( 1 \in L \) and \( a \oplus 1 = a1 = a = 1a = 1 \oplus a \). Therefore, \( 1 = 0_L \) is the zero element.

(e) \text{(inverse} \( \oplus \)) Let \( a \in L \). Then, \( a > 0 \) so that \( 1/a > 0 \) and \( 1/a \in L \). Thus, \( a \oplus (1/a) = a(1/a) = 1 = 0_L \) and similarly, \( (1/a) \oplus a = (1/a)(a) = 1 = 0_L \). Therefore, \( -a = (1/a) \) in \( L \).

(f) \text{(closure for} \( \otimes \)) If \( a > 0 \) and \( b > 0 \) then \( ab > 0 \). Thus, \( a \otimes b = a^{\ln b} \in L \).

(g) \text{(associative} \( \otimes \)) \( (a \otimes b) \otimes c = (a^{\ln b})^{\ln c} = a^{\ln b \cdot \ln c} \) and \( a \otimes (b \otimes c) = a \otimes (b^{\ln c}) = a^{\ln b \cdot \ln c} \).

(h) \text{(distribution)} \( a \otimes (b \oplus c) = a \otimes (bc) = a^{\ln (bc)} = a^{\ln b + \ln c} \) and \( (a \otimes b) \oplus (a \otimes c) = a^{\ln b} \oplus a^{\ln c} = a^{\ln b + \ln c} \).

Let \( e \in L \) be the unique base of the natural log, that is, \( e^{\ln a} = a \) and \( \ln e = 1 \). It follows that \( a \otimes e = a^{\ln e} = a^1 = a \) and \( e \otimes a = e^{\ln a} = a \). Therefore, \( L \) is a ring with identity \( 1_L = e \).

Let \( a, b \in L \). \( a \otimes b = a^{\ln b} = e^{\ln (a^{\ln b})} = e^{\ln b \cdot \ln a} \) and \( b \otimes a = b^{\ln a} = e^{\ln (b^{\ln a})} = e^{\ln a \cdot \ln b} \).

Therefore, \( a \otimes b = b \otimes a \) and \( L \) is a commutative ring.

5. \textbf{(Hungerford 3.2.8)} Let \( R \) be a ring and \( b \in R \) be fixed and define \( T := \{ rb : r \in R \} \). Prove that \( T \subset R \) is a subring.

\textbf{Solution.}\ Let \( x, y \in T \) and write \( x = r_1b \) and \( y = r_2b \) for some \( r_1, r_2 \in R \). Then, \( x + y = r_1b + r_2b = (r_1 + r_2)b \) where \( r_1 + r_2 \in R \). Thus, \( x + y \in T \) (closure of +). Further, \( x \cdot y = (r_1b)(r_2b) = (r_1r_2)b \) where \( r_1r_2 \in R \). Thus, \( x \cdot y \in T \) (closure of \( \cdot \))

We have that \( b \cdot 0_R = 0_R \). Thus, \( 0_R \in T \).

From basic ring properties, \(-x = -(r_1b) = (-r_1)b \) where \( -r_1 \in R \). Thus, \( -x \in T \).

Therefore, by the subring theorem \( T \) is a subring of \( R \).

6. \textbf{(Hungerford 3.2.25)} Let \( S \subset R \) be a subring and suppose \( R \) is an integral domain. Prove that if \( S \) is an integral domain then the identities are equal \( 1_S = 1_R \). (Note there was a mistake in the original problem that is corrected here.)
Solution. Since $S$ is an integral domain, $S$ is a ring with identity call it $1_S$. Let $s \in S$ be nonzero. It follows that

$$0_R = s - s = s1_R - s1_S = s(1_R - 1_S).$$

Since $R$ is an integral domain and $s \in S \subseteq R$ is nonzero, we conclude that $1_R - 1_S = 0_R$. Therefore, $1_S = -(1_R) = 1_R$.

7. **(Hungerford 3.2.31)** A Boolean ring is a ring $R$ with identity in which $x^2 = x$ for every $x \in R$. If $R$ is a Boolean ring prove that $R$ is commutative. [Hint: Expand $(a + b)^2$.]

**Solution.** Let $a, b \in R$. Then since $R$ is a Boolean ring we have that $(a + b)^2 = a + b$ Following the hint, expand the product

$$(a + b)^2 = a^2 + ab + ba + b^2 = a + ab + ba + b.$$  

By substitution, $a + b = a + ab + ba + b$. By subtraction, $0_R = ab + ba$ and further, $ab = -ba$.

Apply the above the case $a = b = 1_R$ we have that $1_R 1_R = -1_R 1_R$ or simply $1_R = -1_R$.

Therefore, $ab = -ba = (-1_R)ba = (1_R)ba = ba$. We conclude that $R$ is commutative.

8. **(Hungerford 3.3.9)** If $f : \mathbb{Z} \rightarrow \mathbb{Z}$ is an isomorphism, prove that $f$ is the identity map. [Hint: What is $f(1)$, $f(1 + 1)$, ...?]

**Solution.** Let $f : \mathbb{Z} \rightarrow \mathbb{Z}$ be an isomorphism. Since $\mathbb{Z}$ is a ring with identity 1, basic ring homomorphism properties of Theorem 3.10 imply that $f(0) = 0$, $f(1) = 1$ and $f(-1) = -1$.

Let $k \in \mathbb{Z}$ and $k > 0$. We can write $k = 1 + 1 + \cdots + 1$ adding $1$ $k$ times. Since $f$ respects addition we have that

$$f(k) = f(1 + 1 + \cdots + 1) = f(1) + f(1) + \cdots + f(1) = 1 + 1 \cdots + 1 = k.$$  

Thus, if $k > 0$ then $f(k) = k$.

If $k < 0$ then $-k > 0$. Since $f$ respects multiplication we have that $f(-k) = f(-1)f(k) = (-1)(k) = -k$.

We conclude $f(k) = k$ for all $\mathbb{Z}$ and thus $f$ is the identity map.

9. **(Hungerford 3.3. 27 and 29)** If $g : R \rightarrow S$ and $f : S \rightarrow T$ are homomorphisms, show that $f \circ g : R \rightarrow T$ is a homomorphism. If $f$ and $g$ are isomorphisms, show that $f \circ g$ is an isomorphism.

**Solution.** Let $a, b \in R$. We have that

$$f \circ g(a + b) = f(g(a + b))$$  

$$= f(g(a) + g(b)) \quad (g \text{ respects } +)$$  

$$= f(g(a)) + f(g(b)) \quad (f \text{ respects } +)$$  

and similarly,

$$f \circ g(a \cdot b) = f(g(ab))$$  

$$= f(g(a)g(b)) \quad (g \text{ respects } \cdot)$$  

$$= f(g(a))f(g(b)) \quad (f \text{ respects } \cdot)$$  

$$= (f \circ g(a))(f \circ g(b)).$$  

Thus, $f \circ g$ is a homomorphism of rings.

Further, suppose $f$ and $g$ are isomorphisms. Then, $f$ and $g$ are both injective and surjective.
Suppose that \( f \circ g(a) = f \circ g(b) \) which we write as \( f(g(a)) = f(g(b)) \). Then, since \( f \) is injective we have that \( g(a) = g(b) \). Since \( g \) is injective \( a = b \). Thus, \( f \circ g \) is injective.

Let \( t \in T \). Since \( f \) is surjective there exists \( s \in S \) such that \( f(s) = t \). Since \( g \) is surjective there exists \( r \in R \) such that \( g(r) = s \). By substitution, we have that \( f \circ g(r) = f(g(r)) = t \). Thus, \( f \circ g \) is surjective.

We have shown that \( f \circ g \) is bijective. Since we have already shown that \( f \circ g \) is a homomorphism, we conclude that \( f \circ g \) is an isomorphism.

10. (Hungerford 3.3.41) Let \( m, n \in \mathbb{Z} \) be positive with \( \gcd (m, n) = 1 \) and define the map \( f : \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n \) by \( f([a]_{mn}) = ([a]_m, [a]_n) \).

(a) Show that \( f \) is well-defined, that is, if \([a]_{mn} = [b]_{mn}\) then \([a]_m = [b]_m\) and \([a]_n = [b]_n\).

(b) Prove that \( f \) is an isomorphism.

**Solution.**

(a) Let \([a]_{mn}, [b]_{mn} \in \mathbb{Z}_{mn}\) and suppose that \([a]_{mn} = [b]_{mn}\). Congruence classes are equal if and only if their representatives are congruent, that is, \(a \equiv b \mod mn\). Thus, \(a - b = mnk\) for some \(k\).

Thus, \(a - b = mnk\) which implies \([a]_m = [b]_m\) and \(a - b = nmk\) which implies \([a]_n = [b]_n\).

(b) First, let’s show that \( f \) is a homomorphism. Let \([a]_{mn}, [b]_{mn} \in \mathbb{Z}_{mn}\). Then,

\[
\begin{align*}
  f([a]_{mn} + [b]_{mn}) &= f([a + b]_{mn}) \\
  &= ([a + b]_m, [a + b]_n) \\
  &= ([a]_m + [b]_m, [a]_n + [b]_n) \\
  &= ([a]_m, [a]_n) + ([b]_m, [b]_n) \\
  &= f([a]_{mn}) + f([b]_{mn})
\end{align*}
\]

and

\[
\begin{align*}
  f([a]_{mn}[b]_{mn}) &= f([ab]_{mn}) \\
  &= ([ab]_m, [ab]_n) \\
  &= ([a]_m[b]_m, [a]_n[b]_n) \\
  &= ([a]_m, [a]_n)([b]_m, [b]_n) \\
  &= f([a]_{mn})f([b]_{mn}).
\end{align*}
\]

Therefore, \( f \) is a homomorphism for any \(m, n\).

Next, we will use the fact that \( \gcd (m, n) = 1 \) to show that \( f \) is bijective.

Suppose \( f([a]_{mn}) = f([b]_{mn}) \). Then, \(([a]_m, [a]_n) = ([b]_m, [b]_n)\), and by equating entries,

\[
\begin{align*}
  [a]_m &= [b]_m \quad \implies \quad a - b = mk \text{ for some } k \in \mathbb{Z} \\
  [a]_n &= [a]_n \quad \implies \quad a - b = nj \text{ for some } j \in \mathbb{Z}
\end{align*}
\]

By substitution, \(mk = nj\). Thus, \(m|nj\) and \( (m, n) = 1 \) from which we conclude that \(m|j\). Write \(j = ml\) for some \(l \in \mathbb{Z}\). Back substitution gives \(a - b = nj = nml\) which implies \([a]_{mn} = [b]_{mn}\).

Thus, \( f \) is injective.

We know that the cardinality of the sets satisfies \(|\mathbb{Z}_{mn}| = mn = |\mathbb{Z}_m \times \mathbb{Z}_n|\). Thus, \( f \) is an injective function from two finite sets of the same cardinality. We conclude that \( f \) must be bijective.