Solutions to Homework Problems from Chapter 3

§3.1

3.1.1. The following subsets of $\mathbb{Z}$ (with ordinary addition and multiplication) satisfy all but one of the axioms for a ring. In each case, which axiom fails.

(a) The set S of odd integers.

- The sum of two odd integers is a even integer. Therefore, the set S is not closed under addition. Hence, Axiom 1 is violated. ∎

(b) The set of nonnegative integers.

- If a is a positive integer, then there is no solution of $a + x = 0$ that is also positive. Hence, Axiom 5 is violated. ∎

3.1.2

(a) Show that the set R of all multiples of 3 is a subring of $\mathbb{Z}$.

(b) Let k be a fixed integer. Show that the set of all multiples of k is a subring of $\mathbb{Z}$.

- Clearly, (b) implies (a); so let us just prove (b). Let
$$S = \{z \in \mathbb{Z} \mid z = nk \quad \text{for some} n \in \mathbb{Z}\} \quad .$$
In general, to show that a subset S of a ring R, is a subring of R, it is sufficient to show that
(i) S is closed under addition in R
(ii) S is closed under multiplication in R;
(iii) $0_R \in S$;
(iv) when $a \in S$, the equation $a + x = 0_R$ has a solution in S.
Let $a, b, c \in S \subset \mathbb{Z}$ with $a = rk$, $b = sk$, $c = tk$.

(i)
$$a + b = rk + sk = (r + s)k \in S$$

(ii)
$$ab = (rk)(sk) = (rsk)k \in S$$

(iii)
$$0_{\mathbb{Z}} = 0 = 0 \cdot k \in S$$

(iv)
$$a = rs \in S \quad \Rightarrow \quad x = -rs \in S \text{ is a solution of} a + x = 0_S$$

Thus, S is a subring of $\mathbb{Z}$. ∎

3.1.3. Let $R = \{0, e, b, c\}$ with addition and multiplication defined by the tables below:

$+$	0	e	b	c	$\cdot$	0	e	b	c
0	0	e	b	c	0	0	0	0	0
e	e	0	c	b	e	0	e	b	c
b	b	c	0	e	b	0	b	e	c
c	c	b	e	0	c	0	c	c	0

Assume distributivity and associativity and show that R is a ring with identity. Is R commutative?

Axioms (1) and (6) are satisfied by virtue of the tables above. We are also allowed to assume that Axioms (2), (7) and (8) hold. Axiom (3), commutatively of addition, is also evident from the symmetry of the addition table. Similarly, the symmetry of the multiplication table implies that multiplication is commutative for this set. From the addition table it is also clear that $0+a=a$ for any $a \in R$; so Axiom (4) is satsified.. It remains to verify Axiom (5). Thus, we need to find a solution in R of

$$a+x=O$$

for each $a \in R$. From the addition table we have

$$\begin{array}{cccc} a=0 & , & x=0 & \Rightarrow & a+x=0 \\ a=e & , & x=e & \Rightarrow & a+x=0 \\ a=b & , & x=b & \Rightarrow & a+x=0 \\ a=c & , & x=c & \Rightarrow & a+x=0 \quad , \end{array}$$

so Axiom (5) is also verified.

3.1.4. Let $F=\{0,e,a,b\}$ with addition and multiplication defined by the tables below:

$+$	0	e	a	b
0	0	e	a	b
e	e	0	b	a
a	a	b	0	e
b	b	a	e	0

$\cdot$	0	e	a	b
0	0	0	0	0
e	0	e	a	b
a	0	a	b	e
b	0	b	e	a

Assume distributivity and associativity and show that R is a field.

We first show that F is a ring:

Axioms (1) and (6) are satisfied by virtue of the tables above. We are also allowed to assume that Axioms (2), (7) and (8) hold. Axiom (3), commutatively of addition, is also evident from the symmetry of the addition table. Similarly, the symmetry of the multiplication table implies that multiplication is commutative for this set. From the addition table it is also clear that $0+s=a$ for any $s \in R$; so Axiom (4) is satsified.. It remains to verify Axiom (5). Thus, we need to find a solution in R of

$$s+x=O$$

for each $a \in R$. From the addition table we have

$$\begin{array}{cccc} s=0 & , & x=0 & \Rightarrow & s+x=0 \\ s=e & , & x=e & \Rightarrow & s+x=0 \\ s=a & , & x=a & \Rightarrow & s+x=0 \\ s=b & , & x=b & \Rightarrow & s+x=0 \quad , \end{array}$$

so Axiom (5) is also verified. We also note that $s \cdot e = s$ for any $s \neq 0$ in F. Thus, F is a commutative ring with identity.

To show that F is a field we need to show further that F is a division ring; i.e., for each $s \neq 0_F$ in F, the equations $sx = 1_F \equiv e$ has a solution in F. From the multiplication table we see

$$\begin{array}{cccc} s=e & , & x=e & \Rightarrow & sx=e \\ s=a & , & x=b & \Rightarrow & sx=e \\ s=b & , & x=a & \Rightarrow & sx=e \quad , \end{array}$$

So F is a commutative division ring; i.e., a field.

3.1.5. Which of the following five sets are subrings of $M(\mathbb{R})$. Which ones have an identity?

(a)

$$A=\left\{\begin{pmatrix} 0 & r \\ 0 & 0 \end{pmatrix} \mid r \in \mathbb{Q}\right\}$$

This is a subring since

$$\begin{aligned}\begin{pmatrix} 0 & r \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & r' \\ 0 & 0 \end{pmatrix} &= \begin{pmatrix} 0 & r+r' \\ 0 & 0 \end{pmatrix} \in A \\ \begin{pmatrix} 0 & r \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & r' \\ 0 & 0 \end{pmatrix} &= \begin{pmatrix} 0 & rr' \\ 0 & 0 \end{pmatrix} \in A\end{aligned}$$

It does not have an identity, however.

(b)

$$B = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid a, b, c \in \mathbb{Z} \right\}$$

This is a subring since

$$\begin{aligned}\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} + \begin{pmatrix} a' & b' \\ 0 & c' \end{pmatrix} &= \begin{pmatrix} a+a' & b+b' \\ 0 & c+c' \end{pmatrix} \in B \\ \begin{pmatrix} a & b \\ 0 & b \end{pmatrix} \begin{pmatrix} a' & b' \\ 0 & c' \end{pmatrix} &= \begin{pmatrix} aa' & ab'+bc' \\ 0 & bc' \end{pmatrix} \in B\end{aligned}$$

It does have an identity, namely,

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad .$$

$$C = \left\{ \begin{pmatrix} a & a \\ b & b \end{pmatrix} \mid a, b \in \mathbb{R} \right\}$$

This is a subring since

$$\begin{aligned}\begin{pmatrix} a & a \\ b & b \end{pmatrix} + \begin{pmatrix} a' & a' \\ b' & b' \end{pmatrix} &= \begin{pmatrix} a+a' & a+a' \\ b+b' & b+b' \end{pmatrix} \in C \\ \begin{pmatrix} a & a \\ b & b \end{pmatrix} \begin{pmatrix} a' & a' \\ b' & b' \end{pmatrix} &= \begin{pmatrix} aa'+ab' & aa'+ab' \\ ba'+bb' & ba'+bb' \end{pmatrix} \in C\end{aligned}$$

It does not have an identity, however.

(c)

$$D = \left\{ \begin{pmatrix} a & 0 \\ a & 0 \end{pmatrix} \mid a \in \mathbb{R} \right\}$$

This is a subring since

$$\begin{aligned}\begin{pmatrix} a & 0 \\ a & 0 \end{pmatrix} + \begin{pmatrix} a' & 0 \\ a' & 0 \end{pmatrix} &= \begin{pmatrix} a+a' & \\ a+a' & \end{pmatrix} \in D \\ \begin{pmatrix} a & 0 \\ a & 0 \end{pmatrix} \begin{pmatrix} a' & 0 \\ a' & 0 \end{pmatrix} &= \begin{pmatrix} aa' & 0 \\ aa' & 0 \end{pmatrix} \in D\end{aligned}$$

It does have an identity however. For $\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} \in D$ and

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

$$D = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \mid a \in \mathbb{R} \right\}$$

This is a subring since

$$\begin{aligned}\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} + \begin{pmatrix} a' & 0 \\ 0 & a' \end{pmatrix} &= \begin{pmatrix} a+a' & 0 \\ 0 & a+a' \end{pmatrix} \in D \\ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \begin{pmatrix} a' & 0 \\ 0 & a' \end{pmatrix} &= \begin{pmatrix} aa' & 0 \\ 0 & aa' \end{pmatrix} \in D\end{aligned}$$

It does have an identity, namely,

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad .$$

3.1.6. Let R and S be rings. Show that the subset $\bar{R} = \{(r, 0_S) \mid r \in R\}$ is a subring of $R \times S$. Do the same for the set $\bar{S} = \{(0_R, s) \mid s \in S\}$.

Proof. Clearly, $\bar{R}$ is a subset of $R \times S$. By Theorem 3.1, $R \times S$ is a ring. To show that $\bar{R}$ is a subring of $R \times S$ we must verify

(i) $\bar{R}$ is closed under addition
(ii) $\bar{R}$ is closed under multiplication
(iii) $0_{R\times S} \in \bar{R}$
(iv) When $a \in \bar{R}$, the equation $a + x = 0_{R\times S}$ has a solution in $\bar{R}$

Let $a = (r, 0_S)$ and $b = (t, 0_S)$ be arbitrary elements of $\bar{R}$.

(i)
$$a + b = (r, 0_S) + (t, 0_S) = (r + t, 0_S + 0_S) = (r + t, 0_S) \in R$$

(ii)
$$ab = (r, 0_S)(t, 0_S) = (rt, 0_S \cdot 0_S) = (rt, 0_S) \in R$$

(iii)
$$0_{R\times S} = (0_R, 0_S) \in \bar{R}$$

(iv) Let $a = (r, 0_S)$ be an arbitrary element of $\bar{R}$ and let u be a solution of $r + x = 0_R$ in R. If we set $\bar{u} = (u, 0_S)$, then $\bar{u} \in \bar{R}$ and we have

$$a + \bar{u} = (r, 0_S) + (u, 0_S) = (r + u, 0_S + 0_S) = (0_R, 0_S) = 0_{R\times S} \quad .$$

So if a is any element of $\bar{R}$, there is a solution of $a + x = 0_{R\times S}$ in $\bar{R}$.

The proof that $\bar{S}$ is a subring of $R \times S$ is similar. ∎

3.1.7 If R is a ring, show that $R^* = \{(r, r) \mid r \in R\}$ is a subring of $R \times R$.

Proof. We verify the four properties of a subring (as listed in the previous problem).

(i)
$$(r, r) + (r', r') = (r + r', r + r') \in R^*$$

(ii)
$$(r, r)(r', r') = (rr', rr') \in R^*$$

(iii)
$$0_{R\times R} = (0_R, 0_R) \in R^*$$

(iv)

If u is a solution of $r + x = 0_R$ in R, then $u^* = (u, u)$ is a solution of $(r, r) + u^* = 0_{R\times R}$ lying in R^*; for

$$(r, r) + u^* = (r, r) + (u, u) = (r + u, r + u) = (0_R, 0_R) = 0_{R\times R} \quad .$$

∎

3.1.8. Is $\{1, -1, i, -i\}$ a subring of $\mathbb{C}$?

No, since $i + i = 2i \notin \{1, -1, i, -i\}$, this subset is not closed under addition; hence it is not a subring. Also, $0 = 0_{\mathbb{C}} \notin \{1, -1, i, -i\}$. ∎

3.1.9. Let p be a positive prime and let R be the set of all rational numbers that can be written in the form $\frac{r}{p^i}$ with $r, i \in \mathbb{Z}$. Show that R is a subring of $\mathbb{Q}$.

Proof. We again verify properties (i) - (iv) of a subring.

(i) $$\frac{r}{p^i}+\frac{r'}{p^j}=\frac{rp^j+p^ir'}{p^ip^j}=\frac{rp^j+r'p^i}{p^{i+j}}\in R$$

(ii) $$\frac{r}{p^i}\cdot\frac{r'}{p^j}=\frac{rr'}{p^ip^j}=\frac{rr'}{p^{i+j}}\in R$$

(iii) $$0_{\mathbb{Q}}=0=\frac{0}{p}\in R$$

(iv) There is always a solution of $\frac{r}{p^i}+x=0_{\mathbb{Q}}=0$ in R; namely $x=\frac{-r}{p^i}$. ∎

3.1.10. Let T be the ring of continuous functions from $\mathbb{R}$ to $\mathbb{R}$ and let f,g be given by

$$f(x)=\begin{cases} 0 & \text{if } x\leq 2\\ x-2 & \text{if } 2<x\end{cases}\quad,\quad g(x)=\begin{cases} 2-x & \text{if } x\leq 2\\ 0 & \text{if } 2<x\end{cases}\quad.$$

Show that $f,g\in T$ and that $fg=0_T$, and therefore that T is not an integral domain.

Well, f and g are certainly continuous on the intervals $(-\infty,2)$ and $(2,+\infty)$ since they are prescribed by polynomial functions there. f and g are also continuous at $x=2$ since

$$\lim_{x\to 2^-}f(x)=\lim_{x\to 2^+}f(x)=0=\lim_{x\to 2^-}g(x)=\lim_{x\to 2^+}g(x)\quad.$$

Therefore, $f,g\in T$. The product of f and g is then the function defined by

$$(fg)(x)=f(x)g(x)=\begin{cases}(0)(2-x)=0 & \text{if } x\leq 2\\ (x-2)(0)=0 & \text{if } 2<x\end{cases}\quad.$$

Hence $fg(x)=0$ for all x. But this function is just the additive identity of T. Thus, $fg=0_T$. Since $f,g\neq 0_T$, but $fg=0_T$, T can not be an integral domain. ∎

3.1.11. Let

$$\mathbb{Q}(\sqrt{2})=\left\{r+s\sqrt{2}\mid r,s\in\mathbb{Q}\right\}\quad.$$

Show that $\mathbb{Q}(\sqrt{2})$ is a subfield of $\mathbb{R}$.

Proof. To prove that a subset S of a field F is a subfield, one must show that S is a subring of F and that

(v) $1_F\in S$
(vi) If $s\in S$, then the equation $sx=1_F$ always has a solution in S.

$\mathbb{Q}(\sqrt{2})$ is certainly a subset of $\mathbb{R}$. Consider two arbitrary elements $r+s\sqrt{2}$, $r'+s'\sqrt{2}\in\mathbb{Q}(\sqrt{2})$. We have

(i) $$\left(r+s\sqrt{2}\right)+\left(r'+s'\sqrt{2}\right)=(r+r')+(s+s')\sqrt{2}\in\mathbb{Q}(\sqrt{2})$$

(ii) $$\left(r+s\sqrt{2}\right)\left(r'+s'\sqrt{2}\right)=(rr'+2ss')+(rs'+sr')\sqrt{2}\in\mathbb{Q}(\sqrt{2})$$

(iii) $$0_{\mathbb{R}}=0=0+0\cdot\sqrt{2}\in\mathbb{Q}$$

Also,

(iv) $$r+s\sqrt{2}\in\mathbb{Q}(\sqrt{2})\quad\Rightarrow\quad -r+(-s)\sqrt{2}\in\mathbb{Q}(\sqrt{2})$$

so every equation of the form $a+x=0_{\mathbb{R}}$ with $a\in\mathbb{Q}(\sqrt{2})$ has a solution in $\mathbb{Q}(\sqrt{2})$. We also have

(v) $$1_{\mathbb{R}}=1=1+0\cdot\sqrt{2}\in\mathbb{Q}(\sqrt{2})S\quad.$$

Finally, we have (recalling that if $r,s\in\mathbb{Q}$ then $r^2-2s^2\neq 0$ unless $r=s=0$)

$$0\neq r+s\sqrt{2}\in\mathbb{Q}(\sqrt{2})\quad\Rightarrow\quad\frac{r}{r^2-2s^2}-\frac{s}{r^2-2s^2}\sqrt{2}\in\mathbb{Q}(\sqrt{2})$$

and

$$\text{(vi)} \qquad \left(r+s\sqrt{2}\right)\left(\frac{r}{r^2-2s^2}-\frac{s}{r^2-2s^2}\sqrt{2}\right)=\frac{\left(r+s\sqrt{2}\right)\left(r-s\sqrt{2}\right)}{r^2-2s^2}=\frac{r^2-2s^2}{r^2-2s^2}=1 \quad ,$$

so every non-zero element of $\mathbb{Q}(\sqrt{2})$ is a unit. ▮

3.1.12. Let $\mathbb{H}$ be the set of real quaterions and 1, **i**, **j**, and **k** the matrices

$$1=\begin{pmatrix}1&0\\0&1\end{pmatrix} \quad , \quad \mathbf{i}=\begin{pmatrix}i&0\\0&-i\end{pmatrix} \quad , \quad \mathbf{j}=\begin{pmatrix}0&1\\-1&0\end{pmatrix} \quad , \quad \mathbf{k}=\begin{pmatrix}0&i\\i&0\end{pmatrix} \quad .$$

(a) Prove that

$$\begin{aligned}\mathbf{i}^2 &= \mathbf{j}^2=\mathbf{k}^2=-1\\ \mathbf{jk} &= -\mathbf{kj}=\mathbf{i}\\ \mathbf{ij} &= -\mathbf{ji}=\mathbf{k}\\ \mathbf{ki} &= -\mathbf{ik}=\mathbf{j}\end{aligned}$$

ı These identities are all proved by direct calculation; e.g.,

$$\mathbf{i}^2=\begin{pmatrix}i&0\\0&-i\end{pmatrix}\begin{pmatrix}i&0\\0&-i\end{pmatrix}=\begin{pmatrix}-1&0\\0&-1\end{pmatrix}=-1$$

(b) Show that $\mathbb{H}$ is a noncommutative ring with identity.

ı Let us parmeterize $\mathbb{H}$ as follows.

$$\begin{aligned}\mathbb{H} &= \left\{\begin{pmatrix}a+ib&c+id\\-c+id&a-ib\end{pmatrix} \mid a,b,c,d\in\mathbb{R}\right\}\\ &= \left\{\begin{pmatrix}z&w\\-\bar{w}&\bar{z}\end{pmatrix} \mid z,w\in\mathbb{C}\right\} \quad .\end{aligned}$$

The latter parameterization displays $\mathbb{H}$ as a subset of the set $M_2(\mathbb{C})$ of 2×2 complex matrices. Since $M_2(\mathbb{C})$ is known to be a ring (under the usual operations of matrix addition and matrix multiplication) to show that $\mathbb{H}$ is a ring, it suffices to verify that the subset $\mathbb{H}$ of $M_2(\mathbb{C})$ i is closed under addition; ii is closed under multiplication iii contains the element $0=\begin{pmatrix}0&0\\0&0\end{pmatrix}$. iv contains the solution of $a+x=0$ if $a\in\mathbb{H}$. These properties are easily confirmed by direct calculation.

(c) Show that $\mathbb{H}$ is a division ring.

ı The multiplicative inverse of 2×2 complex matrix M exists whenever the determinant of M does not vanish. If $M\in\mathbb{H}$, then

$$\begin{aligned}det(M) &= det\begin{pmatrix}a+ib&c+id\\-c+id&a-ib\end{pmatrix}\\ &= (a+ib)(a-ib)-(c+id)(-c+id)\\ &= a^2+b^2+c^2+d^2\\ \\ &= 0 \quad \text{iff } a=b=c=d=0.\end{aligned}$$

So every nonzero element of $\mathbb{H}$ has a multiplicative inverse; so $\mathbb{H}$ is a division ring.

(d) Show that the equation $x^2=-1$ has infinitely many solutions in $\mathbb{H}$.

3.1.13. Prove Theorem 3.1. If R and S are rings, then we can give the Cartesian product $R \times S$ the structure of a ring by setting

$$\begin{aligned} (r,s)+(r',s') &= (r+r', s+s') \\ (r,s)(r',s') &= (rr', ss') \\ 0_{R\times S} &= (0_R, 0_S) \quad . \end{aligned}$$

If R and S are both commutative, then so is $R \times S$. If R and S each have an identity, then so does $R \times S$.

We must confirm that the 8 axioms of a ring are satisfied.

(1) Closure under addition in $R \times S$ is guaranteed by its definition above.

(2) Associativity of addition:

$$\begin{aligned} (r,s)+((r',s')+(r'',s'')) &= (r,s)+(r'+r'', s'+s'') \\ &= (r+r'+r'', s+s'+s'') \\ &= (r+r', s+s')+(r'',s'') \\ &= ((r,s)+(r',s'))+(r'',s'') \end{aligned}$$

(3) Commutativity of addition:

$$(r,s)+(r',s') = (r+r', s+s') = (r'+r, s'+s) = (r',s')+(r,s)$$

(4) Existence of $0_{R\times S}$

Set $0_{R\times S} = (0_R, 0_S)$. Then

$$(r,s)+0_{R\times S} = (r,s)+(0_R,0_S) = (r+0_R, s+0_S) = (r,s)$$

for all $(r,s) \in R \times S$.

(5) Existence of a solution of $(r,s)+x = 0_{R\times S}$ for any $(r,s) \in R \times S$.

$x = (-r,-s)$ is a solution of

$$(r,s)+x = 0_{R\times S}$$

since

$$(r,s)+(-r,-s) = (r-r, s-s) = (0_R, 0_S) = 0_{R\times S}.$$

(6) Closure of multiplication in $R \times S$ is guaranteed by its definition above.

(7) Associativity of multiplication:

$$\begin{aligned} (r,s)\left((r',s')(r'',s'')\right) &= (r,s)(r'r'', s's'') \\ &= (rr'r'', ss's'') \\ &= (rr', ss')(r'',s'') \\ &= \left((r,s)(r',s')\right)(r'',s'') \end{aligned}$$

(8) Distributive laws:

$$\begin{aligned}(r,s)\left((r',s')+(r'',s'')\right) &= (r,s)(r'+r'',s'+s'')\\ &= (r(r'+r''),s(s'+s''))\\ &= (rr'+rr'',ss'+ss'')\\ &= (rr',ss')+(rr'',ss'')\\ &= (r,s)(r',s')+(r,s)(r'',s'')\end{aligned}$$

$$\begin{aligned}\left((r,s)+(r',s')\right)(r'',s'') &= (r+r',s+s')(r'',s'')\\ &= ((r+r')r'',(s+s')s'')\\ &= (rr''+r'r'',ss''+s's'')\\ &= (rr'',ss'')+(r'r'',s's'')\\ &= (r,s)(r'',s'')+(r',s')(r'',s'')\end{aligned}$$

If R and S are commutative, then

$$(r,s)(r',s')=(rr',ss')=(r'r,s's)=(r',s')(r,s)$$

so $R\times S$ is commutative.

If R and S have identity, then $1_{R\times S}=(1_R,1_S)$ is an identity for $R\times S$; since

$$(1_R,1_S)(r,s)=(1_Rr,1_Ss)=(r,s)=(r1_R,s1_S)=(r,s)(1_R,1_S)\quad .$$

▮

3.1.14 Prove or disprove: If R and S are integral domains, then $R\times S$ is an integral domain.

Disproof: Consider, $a=(r,0_S)$, with $r\neq 0_R$ and $b=(0_R,s)$, with $s\neq 0_S$. Then $a,b\neq(0_R,0_S)\equiv 0_{R\times S}$, but

$$ab=(r,0_S)(0_R,s)=(r\cdot 0_R,0_S\cdot s)=(0_R,0_S)=0_{R\times S}\quad .$$

Hence, $R\times S$ has divisors of zero and so it is not an integral domain.

3.1.15 Prove or disprove: If R and S are fields, then $R\times S$ is a field.

Disproof: Consider a non-zero element of $R\times S$ of the form $(r,0_S)$. We claim there is no solution in $R\times S$ of the equation

$$(r,0_S)x=1_{R\times S}\quad .$$

For any $x\in R\times S$ must have the form (r',s') with $r\in R$ and $s\in S$, but

$$(r,0_S)(r',s')=(rr',0_S\cdot s')=(rr',0_S)\neq(1_R,1_S)=1_{R\times S}$$

since $0_S\neq 1_S$. ▮

§3.2

3.2.1 If R is a ring and $a, b \in R$ then
(a) $(a+b)(a-b) = ?$
(b) $(a+b)^3 = ?$
(c) What are the answers to (a) and (b) if R is commutative?

$$\begin{aligned}(a+b)(a-b) &= (a+b)a-(a+b)b\\ &= aa+ba-ab-bb\\ \\ &= a^2-b^2 \quad \text{if } R \text{ is commutative.}\end{aligned}$$

$$\begin{aligned}(a+b)^3 &= (a+b)(a+b)(a+b)\\ &= (a+b)(a+b)a+(a+b)(a+b)b\\ &= (a+b)(aa+ba)+(a+b)(ab+bb)\\ &= (a+b)aa+(a+b)ba+(a+b)ab+(a+b)bb\\ &= aaa+baa+aba+baa+aab+bab+abb+bbb\\ \\ &= a^3+3a^2b+3ab^2+b^3 \quad \text{if } R \text{ is commutative.}\end{aligned}$$

3.2.2 An element e of a ring R is said to be **idempotent** if $e^2 = e$.
(a) Find four idempotent elements of the ring $M_2(\mathbb{R})$.
(b) Find all idempotents in $\mathbb{Z}_{12}$.

(a)

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

(b) For [a] to be an idempotent in $\mathbb{Z}_{12}$, we need

$$[a][a] = [a^2] = [a] \quad .$$

Since any congruence class [a] in $\mathbb{Z}_{12}$ can be represented by a number $a \in \{0, 1, 2, \ldots, 11\}$, we simply check for which of these numbers a^2 is congruent to a; i.e., for which $a \in \{0, 1, \ldots, 11\}$

$$a^2 - a = 12k \quad , \quad k \in \mathbb{Z} \quad .$$

It is easily confirmed that the only solutions of this equation are $a = \{0, 1, 4, 9\}$; so the idempotents of $\mathbb{Z}_{12}$ are [0], [1], [4], and [9]. ▮

3.2.3 Prove that the only idempotents in an integral domain R are 0_R and 1_R.

By definition, if R is an integral domain, then $ab = 0_R$ implies $a = 0_R$ or $b = 0_R$. Let R be an integral domain, and suppose $a^2 = a$. If $a = 0_R$, there is nothing to prove. If $a \neq 0_R$, then Theorem 3.7 says that since $a \cdot a = a = a \cdot 1_R$, we must have $a = 1_R$. ▮

3.2.4 Prove or disprove: The set of units in a ring R with an identity is a subring of R.

Disproof: Consider the ring $\mathbb{Z}$. The element 1 is certainly a unit but $1+1=2$ is not a unit in $\mathbb{Z}$. Therefore, the set of units in $\mathbb{Z}$ is not closed under addition; hence it cannot be a subring. ▮

3.2.5 (a) If a and b are units in a ring R with identity, prove tha ab is a unit and $(ab)^{-1} = b^{-1}a^{-1}$.
(b)Give an example to show that if a and b are units, then $(ab)^{-1}$ may not be the same as $a^{-1}b^{-1}$. (Hint: consider the matrices $\mathbf{i}$ and $\mathbf{k}$ in the quaterion ring $\mathbb{H}$.)

(a) A short calculation proves both statements.

$$\left(b^{-1}a^{-1}\right)(ab) = b^{-1}a^{-1}ab = b^{-1}(a^{-1}a)b = b^{-1}1_R b = b^{-1}b = 1_R$$
$$(ab)\left(b^{-1}a^{-1}\right) = abb^{-1}a^{-1} = a\left(bb^{-1}\right)a^{-1} = a1_R a^{-1} = aa^{-1} = 1_R$$

Since $(ab)x = 1_R = x(ab)$ has a solution $x = b^{-1}a^{-1}$, ab is a unit and $(ab)^{-1} = b^{-1}a^{-1}$.

(b) Let

$$a = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \quad \Rightarrow \quad a^{-1} = \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix} \quad ,$$
$$b = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \quad \Rightarrow \quad b^{-1} = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix} \quad .$$

Then

$$b^{-1}a^{-1} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = a^{-1}b^{-1} \quad .$$

▮

3.2.6 Prove that a unit in a commutative ring cannot be a zero divisor.

Let R be a commutative ring with identity and let a be a unit in R. Then there is an element $b \in R$ such that $ab = 1_R$. If a is also a zero divisor then there is an element $c \neq 0_R$ in R such that $ca = 0_R$. But then

$$c = c \cdot 1_R = cab = 0_R \cdot b = 0_R \quad ;$$

i.e., we have a contradiction. Therefore, a cannot be a zero divisor. ▮

3.2.7
(a) If ab is a zero divisor in a commutative ring R, prove that a or b is a zero divisor.

(b) If a or b is a zero divisor in a commutative ring R and $ab \neq 0_R$, prove that ab is a zero divisor.

(a) If ab is a zero divisor, then $ab \neq 0_R$ and there is a non-zero element $c \in 0_R$ such that $abc = 0_R$. Since $ab \neq 0_R$ we must have $a \neq 0_R$ and $b \neq 0_R$ or else we would have a contradiction. There are two cases. Case (i): Suppose $bc \neq 0_R$. Then $abc = 0_R$ implies a is a zero divisor. Case (ii): Suppose $bc = 0$, then since $c \neq 0_R$ by hypothesis, b must be a zero divisor. ▮

(b) Suppose a is a zero divisor in R; i.e., there exists $c \neq 0_R$ in R such that $ca = 0_R$. But then $c(ab) = (ca)b = 0_R b = 0_R$. Hence, if $ab \neq 0_R$, ab is a zero divisor (by hypothesis, $ab \neq 0_R$. Similarly, if b is a zero divisor there exists $d \neq 0_R$ such that $bd = 0_R$. But then $(ab)d = a(bd) = a0_R = 0_R$ then so is ab is a zero divisor (by hypothesis, $ab \neq 0_R$). ▮

3.2.8 Let S be a non-empty subset of a ring R. Prove that S is a subring if and only if for all $a, b \in S$, both $a - b$ and ab are in S.

$\Rightarrow$ Suppose S is a subring of R. Then $0_R \in S$ and there is always a solution in S to the equation $a + x = 0_R$. In fact, that this solution is unique by Theorem 3.2, so we can denote it uniquely by $-a \in S$. Now we argue as follows, if $a, b \in S$, then $-b \in S$ (by the preceding argument), hence $a + (-b) \in S$ (since a subring is closed under addition), hence $a - b \in S$ (by the definition of subtraction). Since S is a subring it is also closed under multiplication. We conclude that S must be closed under both subtraction and multiplication.

$\Leftarrow$

By hypothesis, S is closed under multiplication. To show that S is a subring of R, we must show

(i) $0_R \in S$
(ii) Every equation $a + x = 0_R$ has a solution in S.
(iii) S is closed under addition.

If $a - b \in S$ for all $a, b \in S$ then certainly $0_R \in S$ since $a - a \equiv 0_R$. Since $0_R \in S$, then for any $a \in S$, $-a \in S$, since $0_R - a = -a$ must be in S. This in turn implies that the equation $a + x = 0_R$ always has a solution in S. Also the fact $a \in S \Rightarrow -a \in S$, implies that if $a, b \in S$, then $a, -b \in S$, and so $a - (-b) = a + b \in S$. Thus, S is closed under addition. ∎

3.2.9 Let R be a ring with identity. If there is a smallest integer n such that $n1_R = 0_R$, then n is said to have *characteristic* n. If no such n exists, R is said to have *characteristic zero*. Show that $\mathbb{Z}$ has characteristic zero, and that $\mathbb{Z}_n$ has characteristic n. What is the characteristic of $\mathbb{Z}_4 \times \mathbb{Z}_6$?

In $\mathbb{Z}_n$

$$n1_R = n[1] = [1] + [1] + \cdots + [1] = [n]$$

so the smallest value of n such that $n1_R = 0_R = [0]$ is n. ∎

In $\mathbb{Z}_4 \times \mathbb{Z}_6$, we have

$$\begin{aligned} n1_R &= n\left([1]_4, [1]_6\right) \\ &= ([1]_4, [1]_6) + ([1]_4, [1]_6) + \cdots + ([1]_4, [1]_6) \\ &= ([n]_4, [n]_6) \end{aligned}$$

so we need to find the smallest n such that

$$0_R = ([0]_4, [0]_6) = ([n]_4, [n]_6) \quad .$$

This means n must be the smallest number divisible by both 4 and 6. Thus, $n = 12$; so the $\mathbb{Z}_4 \times \mathbb{Z}_6$ has characteristic 12. ∎

§3.3

3.3.1 Let R be a ring and let R^* be the subring of $R \times R$ consisting of all elements of the form (a, a), $a \in R$. Show that the function $f : R \to R^*$ given by $f(a) = (a, a)$ is an isomorphism.

(i) f is surjective; since every $(a, a) \in R\ ^*$ can be written as $f(a)$.

(ii) f is injective; since if $f(a) = f(a')$, then we must have

$$(a, a) = (a', a') \quad \Rightarrow \quad a = a' \quad .$$

(iii) f is a ring homomorphism since

$$\begin{aligned} f(a + a') &= (a + a', a + a') = (a, a) + (a', a') = f(a) + f(a') \\ f(aa') &= (aa', aa') = (a, a)(a', a') = f(a)f(a') \qquad . \end{aligned}$$

Thus, f is a ring isomorphism. ▮

3.3.2. If $f : \mathbb{Z} \to \mathbb{Z}$ is an isomorphism, prove that f is the identity map.

Since 0 is the (unique) additive identity in $\mathbb{Z}$ and 1 is the (unique) multiplicative identity in $\mathbb{Z}$, Theorem 3.10 tells us that we must have $f(0) = 0$ and $f(1) = 1$ for any isomorphism $f : \mathbb{Z} \to \mathbb{Z}$. But then for any $n \neq 0$

$$f(n) = f \quad (\underbrace{1 + 1 + \cdots + 1}_{n \text{ summands}}) = f(1) + f(1) + \cdots f(1) = 1 + 1 + \cdots + 1 = n$$

Thus, $f(n) = n$ for all n, so f is the identity map. ▮

3.3.3. Show that the map $f : \mathbb{Z} \to \mathbb{Z}_n$ given by $f(a) = [a]$ is a surjective homomorphism but not an isomorphism.

Well, since

$$\mathbb{Z}_n = \{[0], [1], [2], \ldots, [n-1]\} = \{f[0], f[1], f[2], \ldots, f[n-1]\}$$

the map f is certainly onto. It is also a homomorphism by the definition of addition and multiplication in $\mathbb{Z}_n$

$$\begin{aligned} f(a) + f(b) &= [a] + [b] \equiv [a + b] = f(a + b) \\ f(a)f(b) &= [a][b] = [ab] = f(ab) \qquad . \end{aligned}$$

However, the map f is not injective since, for example,

$$f(n) = [n] = [0] = f(0) \quad .$$

▮

3.3.4. If R and S are rings and $f : R \to S$ is a ring homomorphism, prove that

$$f(R) = \{s \in S \mid s = f(a) \text{ for some} a \in R\}$$

is a subring of S

By Theorem 3.10, $f(0) = 0_S$, so $0_S \in f(R)$. $f(R)$ is also closed under addition and multiplication; for if $f(r)$ and $f(r')$ are arbitrary elements of $f(R)$, then because f is a ring homomorphsim

$$\begin{aligned} f(r) + f(r') &= f(r + r') \in f(R) \quad , \\ f(r)f(r') &= f(rr') \in f(R) \qquad . \end{aligned}$$

Finally, Theorem 3.10 tells us that

$$-f(r) = f(-r) \in R$$

so every equation of the form

$$f(r) + x = 0_S$$

has a solution in $f(R)$. ▮

3.3.5.

(a) If $f : R \to S$ and $g : S \to T$ are ring homomorphisms, show that $g \circ f : R \to T$ is a ring homomorphism.

(b) If $f : R \to S$ and $g : S \to T$ are ring isomorphisms, show that $g \circ g : R \to T$ is also a ring isomorphism.

(a)

$$\begin{aligned} g \circ f(a+b) &= g\left(f(a+b)\right) \\ &= g\left(f(a) + f(b)\right) \\ &= g\left(f(a)\right) + g\left(f(b)\right) \\ &= g \circ f(a) + g \circ f(b) \end{aligned}$$

$$\begin{aligned} g \circ f(ab) &= g\left(f(ab)\right) \\ &= g\left(f(a) \cdot f(b)\right) \\ &= g\left(f(a)\right) \cdot g\left(f(b)\right) \\ &= g \circ f(a) \cdot g \circ f(b) \end{aligned}$$

(b) Suppose f and g are ring isomorphisms, then f and g are bijections. By Theorem B.1, both $f^{-1} : S \to R$ and $g^{-1} : T \to S$ exist. But then

$$(g \circ f)^{-1} = f^{-1} \circ g^{-1}$$

exists, so $f \circ g$ is a bijection. ▮

3.3.6. If $f : R \to S$ is an isomorphism of rings, which of the following properties are preserved by this isomorphism? Why?

(a) $a \in R$ is a zero divisor.
(b) R is an integral domain.
(c) R is a subring of $\mathbb{Z}$.
(d) $a \in R$ is a solution of $x^2 = x$.
(e) R is a ring of matrices.

(a) Yes. If a is a zero divisor in R, then by definition there must be an element $b \neq 0_R$ such that $ab = 0_R$. But then

$$f(a)f(b) = f(ab) = f(0_R) = 0_R$$

by Theorem 3.10. Moreover, since f is surjective, $f(b) \neq 0_S$ unless $b = 0_R$. Therefore, if a is a zero divisor in R, then $f(a)$ is a zero divisor in S. ▮

(b) Yes. Suppose R is an integral domain and S is not an integral domain. Then there exists $a, b \neq 0_S$ such that $ab = 0_S$. But since f is a bijection f^{-1} exists and is also an isomorphism. But then (a) implies that $f^{-1}(a)$ is a zero divisor in R; a contradiction. ▮

(c) No. Consider the ring $R \subset \mathbb{Z}$ consisting of even integers let S be the set of 2×2 matrices of the form

$$S = \left\{ \left(\begin{array}{cc} 2z & 0 \\ 0 & 0 \end{array} \right) \mid z \in \mathbb{Z} \right\} \quad .$$

One easily verifies that the map

$$f : R \to S \quad , \quad a \to \left(\begin{array}{cc} a & 0 \\ 0 & 0 \end{array} \right)$$

is an isomorphism; but the set S is not a subset of the set of integers. ▮

(d) Yes. Suppose $a^2 = a$ in R and $f : R \to S$ is an isomorphism. Then

$$f(a) \cdot f(a) = f(a^2) = f(a) \quad .$$

∎

(e) No. This is similar to (c). ∎

3.3.7. Use the properties that are preserved by ring isomorphism to show that the first ring is not isomorphic to the second.

(a) E (the set of even integers) and $\mathbb{Z}$.
(b) $\mathbb{R} \times \mathbb{R} \times \mathbb{R} \times \mathbb{R}$ and $M_2(\mathbb{R})$.
(c) $\mathbb{Z}_4 \times \mathbb{Z}_{14}$ and $\mathbb{Z}_{16}$.
(d) $\mathbb{Q}$ and $\mathbb{R}$.
(e) $\mathbb{Z} \times \mathbb{Z}_2$ and $\mathbb{Z}$.
(f) $\mathbb{Z}_4 \times \mathbb{Z}_4$ and $\mathbb{Z}_{16}$.

(a) $\mathbb{Z}$ has identity, while E does not. Therefore, $\mathbb{Z}$ cannot be isomorphic to E. ∎

(b) Muliplication in $\mathbb{R} \times \mathbb{R} \times \mathbb{R} \times \mathbb{R}$ is commutative (Theorem 3.1) but multiplication in $M_2(\mathbb{R})$ is not. Therefore, $\mathbb{R} \times \mathbb{R} \times \mathbb{R} \times \mathbb{R}$ cannot be isomorphic to $M_2(\mathbb{R})$. ∎

(c) $\mathbb{Z}_4 \times \mathbb{Z}_{14}$ has $4 \times 14 = 56$ elements, but $\mathbb{Z}_{16}$ has only 16 elements. Therefore, $\mathbb{Z}_4 \times \mathbb{Z}_{16}$ cannot be isomorphic. ∎

(d) Suppose there is a isomorphism $f : \mathbb{R} \to \mathbb{Q}$. Then

$$f(2) = f(1) + f(1) = 1 + 1 = 2$$

and

$$f(2) = f\left(\sqrt{2}\right) f\left(\sqrt{2}\right) \quad .$$

But we know the equation $x^2 = 2$ has no solution in $\mathbb{Z}$. Therefore, $\mathbb{R}$ cannot be isomorphic to $\mathbb{Z}$. ∎

(e) Consider the multiplicative identity $([1]_4, [1]_4)$ in $\mathbb{Z}_4 \times \mathbb{Z}_4$. If f were an isomorphism from $\mathbb{Z}_4 \times \mathbb{Z}_4$ to $\mathbb{Z}_{16}$ we would have

$$f\left(4\left([1]_4, [1]_4\right)\right) = f(4) f\left([1]_4, [1]_4\right) = f(4) \cdot 1_{\mathbb{Z}_{16}} = f(4)$$

on the one hand, but also

$$f\left(4\left([1]_4, [1]_4\right)\right) = f\left([4]_4, [4]_4\right) = f\left(\left([0]_4, [0]_4\right)\right) = 0_{\mathbb{Z}_{16}}.$$

But $f(4) \neq 0_{\mathbb{Z}_{16}}$ since f is surjective. Thus, we have a contradiction. Hence, a map f from $\mathbb{Z}_4 \times \mathbb{Z}_4$ to $\mathbb{Z}_{16}$ cannot be an isomorphism. ∎