MATH 3613

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.

• Consider closure under addition or existence of additive identity.
(b) The set of nonnegative integers.

• Consider existence of additive identity.

3.1.2.
(a) Show that the set R of all multiples of 3 is a subring of $\mathbb{Z}$.

• Check that R is closed under addition, multiplication, and taking additive inverses.
(b) Let k be a fixed integer. Show that the set of all multiples of k 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
0	0	e	b	c
e	e	0	c	b
b	b	c	0	e
c	c	b	e	0

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

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

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.

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

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

• subring w/o identity

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

• subring with identity

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

• subring w/o identity

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

• subring with identity

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

• subring with identity.

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 $\bar{S} = \{(0_R, s) \mid s \in S\}$.

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

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

• Consider closure under addition

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 $\mathbb{Q}$.

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.

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 $\mathbb{R}$.

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

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

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

• Show that $\mathbb{H}$ is a subring of $M_{2,2}(\mathbb{C})$ (the set of 2×2 matrices with entries in $\mathbb{C}$)
(c) Show that $\mathbb{H}$ is a division ring.

• Show that if $\mathbf{0} \neq h \in \mathbb{H}$, then $h^{-1} \in \mathbb{H}$.
(d) Show that the equation $x^2 = -1$ has infinitely many solutions in $\mathbb{H}$.

•

$$x^2 = \begin{pmatrix} a^2 - b^2 - c^2 - d^2 - 2iab & 2ac + 2iad \\ -2ac + 2iad & a^2 - b^2 - c^2 - d^2 + 2iab \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \Longrightarrow \begin{cases} a^2 - b^2 - c^2 - d^2 = -1 \\ 2ab = 0 \\ 2ac = 0 \\ 2ad = 0 \end{cases}$$

Notice that if $a = 0$, then the only condition on b, c, d

$$b^2 + c^2 + d^2 = 1$$

which clearly has an infinite number of solution (e.g., take $b = \sin\theta$, $c = \cos\theta$, $d = 0$, $\theta \in [0, 2\pi]$).

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

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

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

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

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

§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?

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 $\mathbb{Z}_{12}$.

$$[0]_{12}\,, [1]_{12}\,, [4]_{12}\,, [9]_{12}$$

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

$$e^2 = e \quad \Longrightarrow \quad e\,(e - 1_R) = 0_R \quad \Longrightarrow \quad e = 0_R \text{ or } e = 1_R \text{ since } R \text{ is an I.D.}$$

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

false: consider closure under addition

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 **i** and **k** in the quaterion ring $\mathbb{H}$.)

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

If $aa^{-1} = 1 = a^{-1}a$ and $\exists\, b \neq 0_R$ such that $ab = 0_R$, then

$$1 = aa^{-1} \quad \Longrightarrow \quad b \cdot 1 = b\left(aa^{-1}\right) \quad \Longrightarrow \quad b = (ba)\,a^{-1} = (ab)\,a^{-1} = 0_R a^{-1} = 0 \text{ (contradiction)}$$

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.

$$\begin{aligned} a \text{ is a zero divisor} \quad &\Longrightarrow \quad \exists\, c \neq 0_R \text{ s.t. } ac = 0_R \quad \Longrightarrow \quad c\,(ab) = (ca)\,b = 0_R b = 0_R \\ &\Longrightarrow \quad ab \text{ is a zero divisor} \end{aligned}$$

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.

• Demonstrate that these two conditions are sufficient to guarantee the three conditions
(i) $a, b \in S \quad \Longrightarrow \quad a + b \in S$,
(ii) $a, b \in S \quad \Longrightarrow \quad ab \in S$
(iii) $a \in S \quad \Longrightarrow \quad -a \in S$

for S to be a subring of R.

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 $\mathbb{Z}_4 \times \mathbb{Z}_6$?

• Look for the smallest integer such that $[n]_4 = [0]_4$ and $[n]_6 = [0]_6$

§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.

• Show that f is a ring homomorphism ($f\,(a + b) = f\,(a) + f\,(b)$ and $f\,(ab) = f\,(a)\,f\,(b)$) and that it is both injective and surjective.

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

• If f is a ring isomorphism then $f\,(0) = 0$ and $f\,(1) = 1$ (because we need $f\,(n) = f\,(0 + n) = f\,(0) + f\,(n)$, and $f\,(n) = f\,(1 \cdot n) = f\,(1)\,f\,(n)$). But then $f\,(n) = f\,(1 + 1 + 1 + \cdots + 1) = f\,(1) + f\,(1) + \cdots + f\,(1) = 1 + 1 + \cdots + 1 = n$

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.

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

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 $g \circ f : R \to T$ is also a ring isomorphism.

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.

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 $\mathbb{Z}$.

(consider multiplicative identity)
(b) $\mathbb{R} \times \mathbb{R} \times \mathbb{R} \times \mathbb{R}$ and $M_2(\mathbb{R})$.

(commutativity of multiplication)
(c) $\mathbb{Z}_4 \times \mathbb{Z}_{14}$ and $\mathbb{Z}_{16}$.

$|\mathbb{Z}_4 \times \mathbb{Z}_{14}| = 56 \neq 16 = |\mathbb{Z}_{16}|$
(d) $\mathbb{Q}$ and $\mathbb{R}$.

$$f(2) = f(1) + f(1) = 2$$
$$f(2) = f\left(\sqrt{2}\right) f\left(\sqrt{2}\right) \neq q^2 \text{ for any } q \in \mathbb{Q}$$

(e) $\mathbb{Z} \times \mathbb{Z}_2$ and $\mathbb{Z}$.

$$\mathbb{Z} \times \mathbb{Z}_2 \text{ has zero divisors (e.g., } (0, [1]_2) * (1, [0]_2) = (0, [0]_2)\text{)}$$

(f) $\mathbb{Z}_4 \times \mathbb{Z}_4$ and $\mathbb{Z}_{16}$.

$$f(4([1]_4, [1]_4)) = f([4]_4, [4]_4) = f(([0]_4, [0]_4)) = [0]_{16}$$
$$\neq 4f([1]_4, [1]_4) = 4 \cdot [1]_{16}$$