Indira Gandhi National Open University
School of Sciences

BMTC-134
ALGEBRA

Volume-II
RING THEORY

Unitised Course Outline

Volume I Group Theory

Block 1 Introduction to Groups

Unit 1: Some Preliminaries

Unit 2: Groups

Unit 3: Subgroups

Unit 4: Cyclic Groups

Block 2 Normal Subgroups and Group Homomorphisms

Unit 5: Lagrange's Theorem

Unit 6: Normal Subgroups

Unit 7: Quotient Groups

Unit 8: Group Homomorphisms

Unit 9: Permutation Groups

Volume II Ring Theory

Block 3 Introduction to Rings

Unit 10: Rings

Unit 11: Subrings

Unit 12: Ideals

Unit 13: Ring Homomorphisms

Block 4 Integral Domains

Unit 14: Integral Domains and Fields

Unit 15: Polynomials Rings

Unit 16: Roots and Factors of Polynomials

March, 2021

ISBN-8]-

Further information on the Indira Gandhi National Open University courses, may be obtained from the University's office at Maidan Garhi, New Delhi-110 068 and IGNOU website www.ignou.ac.in.

Printed and published on behalf of the Indira Gandhi National Open University, New Delhi by Prof. Sujatha Varma, School of Sciences.

BMTC-134
ALGEBRA

Indira Gandhi National Open University
School of Sciences

Block

3

INTRODUCTION TO RINGS

Course Design Committee*

Prof. Rashmi Bhardwaj
G.G.S. Indraprastha University, Delhi

Dr. Sunita Gupta
University of Delhi

Prof. Amber Habib
Shiv Nadar University
Gautam Buddha Nagar

Prof. S. A. Katre
University of Pune

Prof. V. Krishna Kumar
NISER, Bhubaneswar

Dr. Amit Kulshreshtha
IISER, Mohali

Prof. Aparna Mehra
I.I.T., Delhi

Prof. Rahul Roy
Indian Statistical Institute, Delhi

Prof. Meena Sahai
University of Lucknow

Dr. Sachi Srivastava
University of Delhi

Prof. Jugal Verma
I.I.T., Mumbai

Faculty members
School of Sciences, IGNOU

Prof. M. S. Nathawat (Director)

Dr. Deepika

Mr. Pawan Kumar

Prof. Poornima Mital

Prof. Parvin Sinclair

Prof. Sujatha Varma

Dr. S. Venkataraman

* The Committee met in August, 2016. The course design is based on the recommendations of the Programme Expert Committee and the UGC-CBCS template.

Block Preparation Team

Prof. Parvin Sinclair (*Editor and Writer*)
School of Sciences
IGNOU

Course Coordinator: Prof. Parvin Sinclair

Acknowledgement:

i) To **Prof. Parvati Shastri**, Mumbai University, and **Dr. Indrakshi Dutta**, Jesus and Mary College, University of Delhi, for their detailed comments.

ii) To Sh. S. S. Chauhan, for the CRC, of this block.

iii) Some material of the earlier IGNOU undergraduate course, Abstract Algebra (MTE-06), has been used in this block.

BLOCK INTRODUCTION

In the first two blocks of this course, you studied various aspects of group theory. In the four units of this block, we will introduce you to another algebraic structure. It consists of a set along with **two** binary operations defined on it. We will call such a system a **ring** if it satisfies certain axioms that you will find in Unit 10.

The notion of a ring is due to the mathematicians Richard Dedekind (1831-1916) and Leopold Kronecker (1823-1891). Kronecker called such a system an 'order'. The mathematician, David Hilbert introduced the term 'ring' in 1897 for this algebraic system. The current definition of an abstract ring appears to be due to the 'mother of algebra', Emmy Noether, who used it extensively in her paper published in 1921.

As you go through the block, you will see that a ring is an abelian group with some extra properties. You will realise that we can very naturally generalise many of the concepts of group theory to ring theory. Thus, whatever you have studied about groups will help you to study this block, and the next one.

Your study of ring theory will follow the path that we used for introducing you to group theory. We will start by defining different types of rings. Then we shall introduce you to subrings (the analogue of subgroups) and ideals (an analogue of normal subgroups). As in Unit 7, this will lead to quotient rings, the analogue of quotient groups. In the last unit of this block, we shall discuss ring homomorphisms and isomorphisms. You will discover that the extremely useful isomorphism theorems for groups can be carried over to ring isomorphisms. This helps us greatly in analysing the structure of rings.

As in the previous blocks, we shall help you to digest the material by exposing you to plenty of examples and exercises. The exercises are as important as the rest of the material in the unit. So please attempt each exercise as and when you come to it, and move further only after solving it.

As in the earlier blocks, you will find an additional set of examples and exercises at the end of the block. These miscellaneous problems cover the material in this block mainly, and assume a knowledge of the previous blocks too. The reason for giving you these problems is to give you more of an opportunity to exercise your mind on basic ring theory. You would enjoy doing them too!

NOTATIONS AND SYMBOLS (used in Block 3)

The list is further to those given in Blocks 1 and 2.

$(R, +, \cdot)$	a ring R w.r.t. the operations of $+$ and $\cdot$
$C[a, b]$	the ring of continuous functions from $[a, b]$ to $\mathbb{R}$
$\text{End } A$	the ring of endomorphisms of a group A
$U(R)$	the group of units of a ring R
$\mathbb{H}$	the ring of real quaternions
$C(R)$	the centre of the ring R
$< a >$	the principal ideal generated by a
$< a_1, \ldots, a_n >$	the ideal generated by $a_1, a_2, \ldots, a_n$

UNIT 10

RINGS

Structure | Page Nos.

10.1 INTRODUCTION

In this course so far, you have studied about a variety of groups and their properties. Some groups also have other binary operations defined on them. For instance, $(\mathbb{C}, +)$ is a group, with multiplication also being a binary operation on $\mathbb{C}$. With this unit, you will start the study of such sets, with two binary operations defined on them, each satisfying certain properties. $\mathbb{Z}$, $\mathbb{Q}$ and $\mathbb{R}$ are examples of such an algebraic system, as you will see.

Now, you know that both addition and multiplication are binary operations on $\mathbb{R}$. Further, you have seen that $\mathbb{R}$ is an abelian group under addition, though it is not a group with respect to multiplication. However, multiplication is associative in $\mathbb{R}$. Also, addition and multiplication are related by the distributive laws, i.e.,
$a(b+c) = ab + ac$, and $(a+b)c = ac + bc$ for all real numbers a, b and c.

We generalise these very properties of the binary operations on $\mathbb{R}$ to define an algebraic system called a ring, in Sec.10.2. This definition is due to the famous algebraist Emmy Noether, also called 'the mother of algebra'.

Fig.1: Emmy Noether (1882-1935)

In Sec.10.3, you shall study several properties of rings that follow directly from the definition.

Throughout these sections, you will be considering several examples of rings. However, in Sec.10.4, we shall specifically focus on some generic rings, like matrix rings and polynomial rings. Of course, in the next block, you will study polynomial rings in detail.

As the contents suggest, this unit lays the foundation for the rest of this course. So study it carefully, including attempting every exercise as you come to it. This will help you ensure that you have attained the following learning objectives of this unit.

Objectives

After studying this unit, you should be able to:

- define, and give examples, of rings;
- derive some elementary properties of rings from the defining axioms of a ring;
- decide whether or not a ring is commutative, and/or has identity.

10.2 WHAT IS A RING?

You are familiar with $\mathbb{Z}$, the set of integers. You also know that it is a group with respect to addition. Is it a group with respect to multiplication too? No, but it is a semigroup with respect to multiplication, since multiplication is associative. Also, multiplication distributives over addition in $\mathbb{Z}$. These properties of addition and multiplication of integers allow us to say that the system $(\mathbb{Z}, +, \cdot)$ is a ring, according to the following definition.

The name 'ring' was given to this algebraic system by the famous mathematician, David Hilbert, in 1897.

Definition: An algebraic system $(R, +, \cdot)$, where R is a non-empty set with two **binary** operations defined on it, usually called addition (denoted by +) and multiplication (denoted by $\cdot$), is called a **ring** if the following axioms are satisfied:

R1) $a + b = b + a$ for all a, b in R, i.e., addition is commutative.

R2) $(a + b) + c = a + (b + c)$ for all a, b, c in R, i.e., addition in R is associative.

R3) There exists an element (denoted by 0) of R such that $a + 0 = a = 0 + a$ for all a in R, i.e., R has an additive identity.

R4) For each a in R, there exists x in R such that $a + x = 0 = x + a$, i.e., every element of R has an additive inverse.

R5) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all a, b, c in R, i.e., multiplication in R is associative.

R6) **(Distributive Laws):** For all a, b, c in R,
$a \cdot (b + c) = a \cdot b + a \cdot c$ (left distributive law), and
$(a + b) \cdot c = a \cdot c + b \cdot c$ (right distributive law).
i.e., multiplication **distributes** over addition from the left as well as the right.

Now, look carefully at the axioms R1 - R4. What do they tell us about $(R, +)$? Don't they say that $(R, +)$ is an abelian group? So, from Unit 2, you know that the additive identity, 0, is unique, and each element a of R has a unique additive inverse (denoted by $-a$). We call the element 0 the **zero element** of the ring.

Now, what does Unit 2 tell you about what the axiom R5 says? Doesn't it tell us that that $(R, \cdot)$ is a semigroup? Hence, we can abbreviate R1 - R6 in the definition of a ring as follows:

Definition: An algebraic system $(R, +, \cdot)$ is called a **ring** if:

$R1'$) $(R, +)$ is an abelian group,

$R2'$) $(R, \cdot)$ is a semigroup, and

$R3'$) for all a, b, c in R,

$a \cdot (b + c) = a \cdot b + a \cdot c$, and $(a + b) \cdot c = a \cdot c + b \cdot c$.

Note that $R1'$ above requires R to be a non-empty set and '+' to be a binary operation on R. Similarly, $R2'$ requires '$\cdot$' to be a binary operation on R.

Before going further we would like to make a remark about notational conventions.

Remark 1: Recall that in the case of groups, we decided to use only the notation G for $(G, *)$, for convenience. Here too, in future, we shall **use only the notation R for $(R, +, \cdot)$**, for convenience, if $+$ and $\cdot$ are understood. We shall, also, usually denote the product of two elements a and b of R by ab instead of $a \cdot b$.

Let us look at some examples of rings now. You have already seen that $\mathbb{Z}$ is a ring. Our brief discussion in Sec.10.1 shows why $(\mathbb{R}, +, \cdot)$ is a ring. What about the sets $\mathbb{Q}$ and $\mathbb{C}$? Do $(\mathbb{Q}, +, \cdot)$ and $(\mathbb{C}, +, \cdot)$ satisfy the axioms $R1$-$R6$ (or $R1'$-$R3'$)? You should check that they do. Therefore, these systems are rings.

Now, a word of caution!

Remark 2: Note that though a ring R has two operations defined on it, their order is important. Thus, if $(R, +, \cdot)$ is a ring, it **does not mean** that $(R, \cdot, +)$ is a ring. For instance, $(\mathbb{Z}, +, \cdot)$ is a ring, but $(\mathbb{Z}, \cdot, +)$ is not because, for example, $(\mathbb{Z}, \cdot)$ does not satisfy $R1'$. (Why?)

Let us now look at some examples that actually provide us with infinitely many examples of rings.

Example 1: Show that $(n\mathbb{Z}, +, \cdot)$ is a ring, where $n \in \mathbb{Z}$.

Solution: From Block 1, you know that $n\mathbb{Z} = \{nm \mid m \in \mathbb{Z}\}$ is an abelian group with respect to addition. Thus, $n\mathbb{Z}$ satisfies $R1'$.
You also know that multiplication in $n\mathbb{Z}$ is associative. Thus, $n\mathbb{Z}$ satisfies $R2'$.
Finally, multiplication distributes over addition from the right as well as the left in $n\mathbb{Z}$. Thus, $n\mathbb{Z}$ satisfies $R3'$.
Hence, $n\mathbb{Z}$ is a ring w.r.t the usual addition and multiplication of integers.

***

Example 2: Show that $(\mathbb{Z}_n, +, \cdot)$ is a ring, for $n \in \mathbb{N}$.

Solution: You already know that $(\mathbb{Z}_n, +)$ is an abelian group, and that multiplication is associative in $\mathbb{Z}_n$. Thus, $\mathbb{Z}_n$ satisfies $R1'$ and $R2'$.
Now, for any $\bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}_n$,

$$\bar{a} \cdot (\bar{b} + \bar{c}) = \overline{a \cdot (b + c)} = \overline{a \cdot b + a \cdot c} = \overline{a \cdot b} + \overline{a \cdot c} = \bar{a} \cdot \bar{b} + \bar{a} \cdot \bar{c}.$$

Thus, $\bar{a} \cdot (\bar{b} + \bar{c}) = \bar{a} \cdot \bar{b} + \bar{a} \cdot \bar{c}$.
Similarly, $(\bar{a} + \bar{b}) \cdot \bar{c} = \bar{a} \cdot \bar{c} + \bar{b} \cdot \bar{c}$ $\forall$ $\bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}_n$.

Hence, $\mathbb{Z}_n$ satisfies $R3'$.

So, $(\mathbb{Z}_n, +, \cdot)$ satisfies the axioms $R1' - R3'$, or $R1 - R6$. Therefore, it is a ring.

***

Example 3: Consider the set
$\mathbb{Z}[i] = \mathbb{Z} + i\mathbb{Z} = \{m + in \mid m \text{ and } n \text{ are integers}\}$, where $i^2 = -1$.
We define '+' and '·' in $\mathbb{Z} + i\mathbb{Z}$ to be the usual addition and multiplication of complex numbers. Thus, for $m + in$ and $s + it$ in $\mathbb{Z} + i\mathbb{Z}$,
$(m + in) + (s + it) = (m + s) + i(n + t)$, and
$(m + in) \cdot (s + it) = (ms - nt) + i(mt + ns)$.
Prove that $\mathbb{Z} + i\mathbb{Z}$ is a ring w.r.t this addition and multiplication. (This ring is called the ring of **Gaussian integers**, after the mathematician Carl Friedrich Gauss.)

Solution: You should prove that $(\mathbb{Z} + i\mathbb{Z}, +)$ is a subgroup of $(\mathbb{C}, +)$. Thus, the axioms $R1 - R4$ (or $R1'$) are satisfied.

You also know that multiplication is associative in $\mathbb{C}$. Hence, it is so in $\mathbb{Z}[i]$. This shows that $R5$ (or $R2'$) is also satisfied.

Finally, since the right and left distributive laws hold in $\mathbb{C}$, they also hold for $\mathbb{Z}[i]$.
Thus, $(\mathbb{Z} + i\mathbb{Z}, +, \cdot)$ is a ring.

***

In Example 3, note how we have used the properties of the binary operations in $\mathbb{C}$ to prove them for a subset, $\mathbb{Z}[i]$, on which these operations are closed.

In the examples above, you can see that $\mathbb{Z}_n$ is finite, while $n\mathbb{Z}$ is infinite. This leads us to the following definition, which should not surprise you.

Definition: A ring $(R, +, \cdot)$ is called **finite** if R is a finite set, and is called **infinite** otherwise.

Are there any finite rings, apart from $\mathbb{Z}_n$? Consider the following examples.

Example 4: Check whether or not $\mathbb{M}_3(\mathbb{Z}_4)$ is a finite ring w.r.t. the usual matrix addition and multiplication.

Solution: Firstly, in Unit 2, you have seen that $(\mathbb{M}_3(\mathbb{Z}_n), +)$ is an abelian group for $n \geq 1$.

Further, you have seen in Unit 1, that matrix multiplication is associative.

Next, let $A = [a_{ij}]$, $B = [b_{ij}]$, $C = [c_{ij}]$ be any three elements of $\mathbb{M}_3(\mathbb{Z}_4)$.
Then $A \cdot (B + C) = [a_{k\ell}] \cdot [(b_{ij} + c_{ij})] = [d_{kj}]$, where k, ℓ, i, j vary over 1, 2, 3,
and $d_{kj} = a_{k1}(b_{1j} + c_{1j}) + a_{k2}(b_{2j} + c_{2j}) + a_{k3}(b_{3j} + c_{3j})$
$= (a_{k1}b_{1j} + a_{k2}b_{2j} + a_{k3}b_{3j}) + (a_{k1}c_{1j} + a_{k2}c_{2j} + a_{k3}c_{3j})$
$=$ sum of the (k, j)th elements of AB and AC.

Hence, $A(B+C) = AB + AC$.
Similarly, you should prove that $(A+B)C = AC + BC \ \forall\ A, B, C \in \mathbb{M}_3(\mathbb{Z}_4)$.
Thus, the distributive laws are satisfied.

Hence, $(\mathbb{M}_3(\mathbb{Z}_4), +, \cdot)$ is a ring.

Finally, each element of $\mathbb{M}_3(\mathbb{Z}_4)$ has 9 entries, each of which is an element of $\mathbb{Z}_4$. Hence, each of these entries has 4 possibilities, $\overline{0}, \overline{1}, \overline{2}, \overline{3}$. Thus, the total number of elements in $\mathbb{M}_3(\mathbb{Z}_4)$ is 4^9. Hence, $\mathbb{M}_3(\mathbb{Z}_4)$ is a finite ring.

***

The next example is related to Example 10 of Unit 2. The operations that we consider in it are not the usual addition and multiplication.

Example 5: Let X be a non-empty set, $\wp(X)$ be the collection of all subsets of X, and Δ denote the symmetric difference operation. Show that $(\wp(X), \Delta, \cap)$ is a ring.

Solution: For any two subsets A and B of X, $A \Delta B = (A \setminus B) \cup (B \setminus A)$.
In Example 10 of Unit 2, you studied that $(\wp(X), \Delta)$ is an abelian group.
You also know that $\cap$ is associative.
Now let us see if $\cap$ distributes over Δ.
Let $A, B, C \in \wp(X)$. Then

$$\begin{aligned} A \cap (B \Delta C) &= A \cap [(B \setminus C) \cup (C \setminus B)] \\ &= [A \cap (B \setminus C)] \cup [A \cap (C \setminus B)], \text{ since } \cap \text{ distributes over } \cup. \\ &= [(A \cap B) \setminus (A \cap C)] \cup [(A \cap C) \setminus (A \cap B)], \text{ since } \cap \text{ distributes} \\ &\qquad \text{over complementation.} \\ &= (A \cap B) \Delta (A \cap C). \end{aligned}$$

So, the left distributive law holds.
Similarly, you should check that the right distributive law holds also.
Therefore, $(\wp(X), \Delta, \cap)$ is a ring.

Now, if X is finite, say $|X| = 10$, then $|\wp(X)| = 2^{10}$. So $(\wp(X), \Delta, \cap)$ is a finite ring. However, if X is infinite, then $(\wp(X), \Delta, \cap)$ is an infinite ring.

***

Now, that you have studied several examples of rings, let us look at $R6$ of the definition of a ring. In that axiom, we have written two equations. Why do both have to be checked? If $a \cdot (b + c) = a \cdot b + a \cdot c$, doesn't it follow that $(a + b) \cdot c = a \cdot c + b \cdot c$? That is, does the fact that the left distributive law holds imply that the right distributive law holds? Consider the following remark about this.

Remark 3: So far you have seen examples of several rings. Are both the operations defined on the ring commutative? What about in Example 4? For instance, is $\begin{bmatrix} \overline{1} & \overline{1} & \overline{1} \\ \overline{0} & \overline{0} & \overline{0} \\ \overline{0} & \overline{0} & \overline{0} \end{bmatrix} \begin{bmatrix} \overline{0} & \overline{0} & \overline{0} \\ \overline{1} & \overline{1} & \overline{1} \\ \overline{0} & \overline{0} & \overline{0} \end{bmatrix} = \begin{bmatrix} \overline{0} & \overline{0} & \overline{0} \\ \overline{1} & \overline{1} & \overline{1} \\ \overline{0} & \overline{0} & \overline{0} \end{bmatrix} \begin{bmatrix} \overline{1} & \overline{1} & \overline{1} \\ \overline{0} & \overline{0} & \overline{0} \\ \overline{0} & \overline{0} & \overline{0} \end{bmatrix}$? Not so.

Thus, multiplication in $\mathbb{M}_3(\mathbb{Z}_4)$ is not commutative. In fact, more generally, **multiplication over $\mathbb{M}_n(\mathbb{C})$ is not commutative, for $n \geq 2$.** So, we can't assume that if the left distributive law holds, then the right distributive law holds in this case. We need to check the validity of both the laws separately. (You will study about sets of matrices being non-commutative in general in more detail in the course, 'Linear Algebra'.)

Remark 3 leads us to the following definition.

Definitions: 1) Two elements a and b, in a ring $(R, +, \cdot)$, are said to **commute with each other** w.r.t. multiplication if $a \cdot b = b \cdot a$.

2) A ring $(R, +, \cdot)$ is called a **commutative ring** if $\cdot$ is commutative over R, i.e., if $a \cdot b = b \cdot a$ for all $a, b \in R$.

Thus, a ring R is commutative iff a and b commute with each other w.r.t. multiplication, $\forall\ a, b \in R$.

For example, $\mathbb{Z}$, $\mathbb{Q}$ and $\mathbb{R}$ are commutative rings, while $\mathbb{M}_n(\mathbb{C})$ is not, for $n \geq 2$. Consider another example, in some detail.

Example 6: Show that $(\wp(X), \Delta, \cap)$ is a commutative ring, where X is a non-empty set.

Solution: In Example 5, you have studied why $(\wp(X), \Delta, \cap)$ is a ring.
Now, from Calculus, you know that $A \cap B = B \cap A\ \forall\ A, B \in \wp(X)$.
Thus, $\cap$ is commutative.
Hence, $(\wp(X), \Delta, \cap)$ is a commutative ring.

***

Now consider the following remark, that adds to the point made in Remark 3.

Remark 4: Let R be a set with the binary operations $+$ and $\cdot$ defined on it. Suppose $\cdot$ is commutative on R. Then, to check whether R6 holds or not for $(R, +, \cdot)$, it is enough to check one distributive law only. Why? Well, if $a \cdot (b + c) = a \cdot b + a \cdot c\ \forall\ a, b, c \in R$, then
$(a + b) \cdot c = c \cdot (a + b) = c \cdot a + c \cdot b = a \cdot c + b \cdot c\ \forall\ a, b, c \in R$.
So, in this case, the other distributive law will hold also.

Try the following exercises now.

E1) Write out the Cayley tables for addition and multiplication in $\mathbb{Z}_6^*$, the set of non-zero elements of $\mathbb{Z}_6$. Looking at these tables, decide whether $(\mathbb{Z}_6^*, +, \cdot)$ is a ring or not.

E2) Show that $\{0\}$ is a ring with respect to the usual addition and multiplication. (This is called the **trivial ring**.)
Further, show that the only singleton that is a ring is $\{0\}$.

E3) Show that the set $\mathbb{Q}[\sqrt{2}] = \mathbb{Q} + \sqrt{2}\mathbb{Q} = \{p + \sqrt{2}q \mid p, q \in \mathbb{Q}\}$ is a commutative ring with respect to addition and multiplication of real numbers.

E4) Let $R = \left\{ \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \middle| a, b \in \mathbb{R} \right\}$. Show that R is a ring with respect to matrix addition and multiplication. Is R a commutative ring? Why, or why not?

E5) Let $R = \left\{ \begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix} \middle| a, b \text{ are real numbers} \right\}$. Prove that R is a ring under matrix addition and multiplication. Is R a commutative ring? Why?

E6) Which of the following are rings? Give reasons for your answers.

i) $(\wp(X), \cup, \cap)$, where X is a non-empty set,

ii) $(\mathbb{R}^*, \cdot, +)$,

iii) $\mathbb{M}_{2\times 3}(\mathbb{R})$, w.r.t. matrix addition and multiplication.

E7) Let $(R, +, \cdot)$ be a ring, where $R = \{a, b, c\}$. Complete the Cayley tables below, explaining your reasoning behind each new entry.

$+$	a	b	c
a	a		
b		c	
c			b

$\cdot$	a	b	c
a			
b		a	
c			

E8) Check whether or not $(\mathbb{Z}, \oplus, \odot)$ is a ring, where
$\oplus(m, n) = \text{g.c.d}(m, n)$ and $\odot(m, n) = \text{l.c.m}(m, n)\ \forall\ m, n \in \mathbb{Z}$.

Let us now look at rings whose elements are functions that you have studied in the course, Calculus.

Example 7: Consider $C[0, 1]$, the set of all continuous real-valued functions defined on the closed interval $[0, 1]$. For f and g in $C[0, 1]$ and $x \in [0, 1]$, we define $f + g$ and $f \cdot g$ by
$(f + g)(x) = f(x) + g(x)$ (i.e., pointwise addition), and
$(f \cdot g)(x) = f(x) \cdot g(x)$ (i.e., pointwise multiplication).
Show that $C[0, 1]$ is a ring with respect to $+$ and $\cdot$.

$C[0, 1]$ is called the **ring of continuous functions on [0, 1].**

Solution: From Calculus, you know that if f and $g \in C[0, 1]$, then both $f + g$ and $f \cdot g$ are in $C[0, 1]$.
Next, using the fact that addition in $\mathbb{R}$ is associative and commutative, you should check that $C[0, 1]$ satisfies $R1$ and $R2$.
The additive identity of $C[0, 1]$ is $\mathbf{0} : [0, 1] \to \mathbb{R} : \mathbf{0}(x) = 0$.
The additive inverse of $f \in C[0, 1]$ is $(-f)$, where $(-f)(x) = -f(x)\ \forall\ x \in [0, 1]$.
Thus, $(C[0, 1], +)$ is an abelian group.

Again, you should use the fact that multiplication in $\mathbb{R}$ is associative, to verify that multiplication in $C[0, 1]$ satisfies $R5$.

Now let us see if the axiom $R6$ holds.

To prove $f \cdot (g + h) = f \cdot g + f \cdot h$, we consider $(f \cdot (g + h))(x)$ for $x \in [0, 1]$.

Now $(f \cdot (g + h))(x) = f(x)(g + h)(x)$

$= f(x)(g(x) + h(x))$

$= f(x)g(x) + f(x)h(x)$, since $\cdot$ distributes over $+$ in $\mathbb{R}$.

$= (f \cdot g)(x) + (f \cdot h)(x)$

$= (f \cdot g + f \cdot h)(x)$

Hence, $f \cdot (g + h) = f \cdot g + f \cdot h$.

Since multiplication is commutative in $\mathbb{R}$, it is commutative in $C[0, 1]$. Hence, by Remark 4, the other distributive law also holds. Thus, $R6$ holds for $C[0, 1]$.

Therefore, $(C[0, 1], +, \cdot)$ is a ring.

***

The next example shows us one way of defining a ring from a given abelian group.

Example 8: Let $(A, +)$ be an abelian group. Consider $\text{End } A$, the set of all endomorphisms of A. For $f, g \in \text{End } A$, and $a \in A$, define $f + g$ and $f \cdot g$ by

$$\left.\begin{aligned}(f + g)(a) &= f(a) + g(a), \text{ and} \\ (f \cdot g)(a) &= f \circ g(a) = f(g(a)).\end{aligned}\right\} \quad \ldots(1)$$

Show that $(\text{End } A, +, \cdot)$ is a ring. (This ring is called the **endomorphism ring of A**.)

Solution: From Unit 8, you know that

$$\text{End } A = \{f : A \to A \mid f(a + b) = f(a) + f(b) \ \forall \ a, b \in A\}.$$

Let us first check that $+$ and $\cdot$, as defined in (1), are binary operations on $\text{End } A$.

For all $a, b \in A$,

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

$= (f(a) + f(b)) + (g(a) + g(b))$, since $f, g \in \text{End } A$.

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

$= (f + g)(a) + (f + g)(b)$, and

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

$= f(g(a) + g(b))$, since $g \in \text{End } A$.

$= f(g(a)) + f(g(b))$, since $f \in \text{End } A$.

$= (f \cdot g)(a) + (f \cdot g)(b)$.

Thus, $f + g$ and $f \cdot g$ are in $\text{End } A$.

Now let us see if $(\text{End } A, +, \cdot)$ satisfies $R1 - R6$.

Since addition in the abelian group A is associative and commutative, so is addition in $\text{End } A$.

The zero endomomorphism on A is the zero element of $\text{End } A$.

$(-f)$ is the additive inverse of $f \in \text{End } A$, where $(-f)(a) = -f(a) \ \forall \ a \in A$.

Thus, $(\text{End } A, +)$ is an abelian group.

You also know that the composition of functions is an associative operation in general, and hence, it is so in $\text{End } A$.

Finally, to check $R6$, we look at $f \cdot (g + h)$ for any $f, g, h \in \text{End } A$.

For any $a \in A$,

$$\begin{aligned}[f \cdot (g+h)](a) &= f((g+h)(a)) \\ &= f(g(a)+h(a)) \\ &= f(g(a)) + f(h(a)), \text{ since } f \in \text{End } A. \\ &= (f \cdot g)(a) + (f \cdot h)(a) \\ &= (f \cdot g + f \cdot h)(a).\end{aligned}$$

$\therefore f \cdot (g+h) = f \cdot g + f \cdot h.$

You should similarly prove that $(f+g) \cdot h = f \cdot h + g \cdot h.$

Here note that $\cdot$ in $\text{End } A$ is not commutative, since $f \circ g$ need not be equal to $g \circ f$ for $f, g \in \text{End } A.$

Thus, R1 - R6 are true for $\text{End } A.$

Hence, $(\text{End } A, +, \cdot)$ is a ring.

***

You should solve the following exercises now.

E9) Let X be a non-empty set and $(R, +, \cdot)$ be a ring. Let $\text{Map}(X, R)$ be the set of all functions from X to R, that is,

$\text{Map}(X, R) = \{f \mid f : X \to R\}.$

Define $+$ and $\cdot$ in $\text{Map}(X, R)$ by pointwise addition and multiplication. Show that $(\text{Map}(X, R), +, \cdot)$ is a ring.

Under what conditions on X and R will $\text{Map}(X, R)$ be a commutative ring?

E10) You know that $(\mathbb{R}, +, \cdot)$ is a ring. Now, check whether or not $(\mathbb{R}, \oplus, \odot)$ is a ring, where $\oplus$ and $\odot$ are defined by

$a \oplus b = a + b + 1,$ and $a \odot b = a \cdot b + a + b$ for all $a, b \in \mathbb{R}.$

(Here $+$ and $\cdot$ denote the usual addition and multiplication of real numbers.)

E10 tells us that a given set can be an underlying set of many different rings.

E11) Let R be a ring. Prove that $\mathbb{M}_2(R)$ is a ring with respect to matrix addition and multiplication. (In fact, $\mathbb{M}_n(R)$ is a ring $\forall\ n \in \mathbb{N}.$)

Now, in Unit 2 you have seen that the Cartesian product of groups forms a group called their direct product. Let us see if this happens with the Cartesian product of rings.

Example 9: Let $(A, +, \cdot)$ and $(B, \boxplus, \boxdot)$ be two rings. Show that their Cartesian product, $A \times B,$ is a ring with respect to $\oplus$ and $*,$ defined by

$(a, b) \oplus (a', b') = (a + a', b \boxplus b'),$ and

$(a, b) * (a', b') = (a \cdot a', b \boxdot b'),$

for all $(a, b), (a', b')$ in $A \times B.$

[The ring $(A \times B, \oplus, *)$ is called the **external direct product** (or simply, the **direct product**) of the rings $(A, +, \cdot)$ and $(B, \boxplus, \boxdot)$.]

Solution: In Unit 2, you have seen that $(A \times B, \oplus)$ is a group. Further, this is an abelian group since $(A, +)$ and $(B, \boxplus)$ are abelian groups.

Since the multiplications in A and B are associative, $*$ is associative in $A \times B$.

Again, using the fact that $R6$ holds for A and B, you should prove that $R6$ holds for $A \times B$.

Thus, $(A \times B, \oplus, *)$ is a ring.

***

If you have understood the example above, you will be able to solve the following exercises.

E12) Write down the addition and multiplication tables for the direct product $\mathbb{Z}_2 \times \mathbb{Z}_3$. Hence decide if this ring is commutative or not.

E13) Show that $\mathbb{R}^2$ and $\mathbb{C}^3$ are rings.

Generalising from E13, you can see why $\mathbb{R}^n$ and $\mathbb{C}^n$ are rings $\forall\ n \geq 2$.

By now you would be familiar with several examples of rings. So let us begin discussing some basic properties of rings.

10.3 ELEMENTARY PROPERTIES

In this section, we will prove, and apply, some basic properties of rings. These properties are immediate consequences of the definition of a ring. As we go along, you must not forget that for any ring $R, (R, +)$ is an abelian group. Hence, the notation and the results obtained for groups in the earlier units of this course are applicable to the abelian group $(R, +)$ too. In particular, note that

i) the additive identity, 0, is unique, and the additive inverse of any element $a \in R$ is $(-a)$;

ii) $-(-a) = a\ \forall\ a \in R$;

iii) the cancellation law holds for addition, i.e., $\forall\ a, b, c \in R,\ a + c = b + c \Rightarrow a = b$;

iv) $a - b = a + (-b)\ \forall\ a, b \in R$.

We will use the facts above, off and on, while proving some basic results in this section.

So let us begin with some properties which follow from the axiom $R6$, mainly. You know that, for any $m, n \in \mathbb{Z}$, $m \cdot 0 = 0$, and $m(-n) = -mn = (-m)n$. The following theorem tells us that these properties, and some others, hold true for any ring R.

Theorem 1: Let R be a ring. Then, for any $a, b, c \in R$,

i) $a \cdot 0 = 0 = 0 \cdot a$,

ii) $a(-b) = (-a)b = -(ab)$,

iii) $(-a)(-b) = ab$,

iv) $a(b-c) = ab - ac$ and $(b-c)a = ba - ca$.

Proof: i) Now, $0 + 0 = 0$

$\Rightarrow a(0+0) = a \cdot 0$, for any $a \in R$.

$\Rightarrow (a \cdot 0) + (a \cdot 0) = a \cdot 0$, applying the left distributive law.

$= a \cdot 0 + 0$, since 0 is the additive identity.

$\Rightarrow a \cdot 0 = 0$, by the cancellation law for $(R, +)$.

Using the right distributive law, you should similarly show that $0 \cdot a = 0$.

(Note that here we cannot assume $0 \cdot a = a \cdot 0$, since R may not be a commutative ring.)

Thus, $a \cdot 0 = 0 = 0 \cdot a$ for all $a \in R$.

ii) For $a, b \in R$,

$0 = a \cdot 0$, from (i) above.

$= a(b + (-b))$, as $0 = b + (-b)$.

$= ab + a(-b)$, by distributivity.

Now, $ab + [-(ab)] = 0$ and $ab + a(-b) = 0$.

But, as you know, the additive inverse of an element is unique.

Hence, we get $[-(ab)] = a(-b)$.

In the same manner, using the fact that $a + (-a) = 0$, you should show that $[-(ab)] = (-a)b$.

Thus, $a(-b) = (-a)b = -(ab)$ for all $a, b \in R$.

iii) For $a, b \in R$,

$(-a)(-b) = -(a(-b))$, from (ii) above.

$= -[-(ab)]$, from (ii) above.

$= ab$, since $-(-x) = x$ for $x \in R$.

iv) For $a, b, c \in R$,

$a(b-c) = a(b + (-c))$

$= ab + a(-c)$, by distributivity.

$= ab + (-(ac))$, from (ii) above.

$= ab - ac$.

You should similarly prove that $(b-c)a = ba - ca$. ■

You can use these properties to solve some exercises now.

E14) Prove that the only ring R in which the two operations are equal (i.e., $a + b = ab \ \forall \ a, b \in R$) is the trivial ring.

E15) Let R be a ring. For $a_1, a_2, \ldots, a_n \in R$, where $n \in \mathbb{N}$, define $(a_1 + a_2 + \cdots + a_n) = (a_1 + \cdots + a_{n-1}) + a_n$, i.e., recursively.

Now, using the principle of induction, prove that if $a, b_1, \ldots, b_n \in R$, where $n \in \mathbb{N}$, then $a(b_1 + b_2 + \cdots + b_n) = ab_1 + ab_2 + \cdots + ab_n$, and $(b_1 + b_2 + \cdots + b_n)a = b_1a + b_2a + \cdots + b_na$.

Let us extend what you have done in E15. We shall look at the sum and the product of three or more elements of a ring. We define them recursively, as we did in the case of groups (see Unit 2).

Definitions: If $k \in \mathbb{N}, k \geq 2,$ is such that the sum of k elements in a ring R is defined, we define **the sum of $(k+1)$ elements** $a_1, a_2, \ldots, a_{k+1}$ in $R,$ taken in that order, as

$a_1 + \cdots + a_{k+1} = (a_1 + \cdots + a_k) + a_{k+1}.$

In the same way, if $k \in \mathbb{N}, k \geq 2,$ is such that the product of k elements in R is defined, we define **the product of $(k+1)$ elements** $a_1, a_2, \ldots, a_{k+1}$ (taken in that order) as

$a_1 \cdot a_2 \ldots a_{k+1} = (a_1 \cdot a_2 \ldots a_k) \cdot a_{k+1}.$

As we did for groups in Unit 2, you can obtain laws of indices (LIs) for rings also with respect to both $+$ and $\cdot$. In fact, you should prove the following results for any ring R.

LI 1) If m and n are **positive** integers and $a \in R,$ then
$a^m \cdot a^n = a^{m+n},$ and $(a^m)^n = a^{mn}.$

LI 2) For $m, n \in \mathbb{Z}$ and $a, b \in R,$

i) $(n+m)a = na + ma,$

ii) $(nm)a = n(ma) = m(na),$

iii) $n(a+b) = na + nb,$

iv) $m(ab) = (ma)b = a(mb),$ and

v) $(ma)(nb) = mn(ab) = (mna)b.$

LI 3) (Generalised distributive law): For $m, n \in \mathbb{N},$ if
$a_1, a_2, \ldots, a_m, b_1, \ldots, b_n \in R,$ then
$(a_1 + \cdots + a_m)(b_1 + \cdots + b_n)$
$= a_1b_1 + \cdots + a_1b_n + a_2b_1 + \cdots + a_2b_n + \cdots + a_mb_1 + \cdots + a_mb_n,$
and the order of addition can be changed since addition is commutative in R.

Try solving some related exercises now.

E16) If R is a ring and $a, b \in R$ such that $ab = ba,$ then use induction on $n \in \mathbb{N}$ to derive the **binomial expansion**
$(a+b)^n = a^n + {}^nC_1 a^{n-1}b + \cdots + {}^nC_k a^{n-k}b^k + \cdots + {}^nC_{n-1}ab^{n-1} + b^n,$ where
${}^nC_k = \dfrac{n!}{k!(n-k)!}.$

E17) Prove LI 1, i.e., $a^m \cdot a^n = a^{m+n}$ $\forall$ $a \in R,$ $m, n \in \mathbb{N},$ where R is a ring. Is this true for m and n with $m, n \leq 0$? Why, or why not?

E18) Prove LI 2(v), that is, if R is a ring, then
$(ma)(nb) = mn(ab)$ $\forall$ $m, n \in \mathbb{Z},$ $a, b \in R.$

There are several other properties of rings that we will be discussing throughout this block. For now, let us look closely at some rings, which are classified according to the properties of the multiplication defined on them.

10.4 RINGS WITH IDENTITY

The definition of a ring guarantees that the binary operation, multiplication, is associative. We also know that $\cdot$ and $+$ satisfy the distributive laws. Nothing more is said about the properties of multiplication. If we place restrictions on this operation, we get several types of rings. For instance, you know that if multiplication is commutative, we get a commutative ring. Let us see what happens if we insist that $(R, \cdot)$ should satisfy $G2$ (of Sec.2.2, Unit 2).

Definition: A ring $(R, +, \cdot)$ is called a **ring with identity** (or a **ring with unity**) if R has an identity element with respect to multiplication, i.e., if there exists an element e in R such that $ae = ea = a$ for all $a \in R$.

Can you think of such a ring? Aren't $\mathbb{Z}$, $\mathbb{Q}$ and $\mathbb{R}$ examples of a ring with identity? The element 1 serves the purpose of an identity in each case.

Looking at all these examples, you may be wondering if every ring is a ring with unity. Consider the following example now.

Example 10: Show that the ring $5\mathbb{Z}$ is not a ring with identity.

Solution: We shall prove this by contradiction. Suppose $5\mathbb{Z}$ has identity, e.
Then $e = 5n$, for some $n \in \mathbb{Z}$.
Now $5e = 5 \Rightarrow 5 \cdot 5n = 5$, which is not possible since $n \in \mathbb{Z}$.
Hence, we reach a contradiction.
Thus, $5\mathbb{Z}$ is not a ring with identity.

***

Why don't you solve some quickies before we go to our next definition?

E19) Prove that if a ring R has an identity element with respect to multiplication, then this **identity is unique**. (We usually denote this **unique identity element** in R by the symbol $\mathbf{1}$.)

E20) Check whether $n\mathbb{Z}$ is a ring with identity or not, where $n \in \mathbb{N} \setminus \{1\}$.

Because of E19, we now can say **the** identity of a ring, when it exists.

Now, consider $\mathbb{Z}$. You have seen that $\mathbb{Z}$ is a ring with identity and is commutative. Thus, $\mathbb{Z}$ is an example of a type of ring we shall now define. Again, this nomenclature would not surprise you.

Definition: A ring $(R, +, \cdot)$ is called a **commutative ring with identity** (or **unity**), if it is a commutative ring and has the multiplicative identity.

Thus, the rings $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are all commutative rings with unity. The integer 1 is the unity, i.e., the multiplicative identity, in all these rings. Let us look at one example in detail.

Example 11: Show that $S = \mathbb{Z}[\sqrt{5}] = \{a + b\sqrt{5} \mid a, b \in \mathbb{Z}\}$ is a ring w.r.t. the addition and multiplication defined as follows:
$(a + b\sqrt{5}) + (c + d\sqrt{5}) = (a + c) + \sqrt{5}(b + d)$, and
$(a + b\sqrt{5}) \cdot (c + d\sqrt{5}) = (ac + 5bd) + \sqrt{5}(ad + bc)$.
Further, is S commutative? Does S have identity? Give reasons for your answers.

Solution: As in the case of Gaussian integers, you should check that both addition and multiplication are binary operations on S, and are the same operations as in $(\mathbb{R}, +, \cdot)$.

Next, using the fact that $\mathbb{Z}$ satisfies $R1$ and $R2$, you should prove that S satisfies $R1$ and $R2$.
Further, $0 \in S$ is the additive identity, and $(-a) + \sqrt{5}(-b)$ is the additive inverse of $a + \sqrt{5}b$.
Thus, $(S, +)$ is an abelian group.

Also, since multiplication is associative and commutative in $\mathbb{R}$, it is associative and commutative in S.

Finally, for $a + b\sqrt{5}, c + d\sqrt{5}, m + n\sqrt{5} \in S$,
$$(a + b\sqrt{5})[(c + d\sqrt{5}) + (m + n\sqrt{5})]$$
$$= (a + b\sqrt{5})[(c + m) + \sqrt{5}(d + n)]$$
$$= a(c + m) + 5b(d + n) + \sqrt{5}[a(d + n) + b(c + m)]$$
$$= [ac + 5bd + \sqrt{5}(ad + bc)] + [am + 5bn + \sqrt{5}(an + bm)]$$
$$= (a + b\sqrt{5})(c + d\sqrt{5}) + (a + b\sqrt{5})(m + n\sqrt{5}).$$
Thus, the left distributive law holds.
Since multiplication in S is commutative, the right distributive law also holds.

Thus, $(S, +, \cdot)$ is a commutative ring.

Finally, $1 \in S$ s.t. for $(a + b\sqrt{5}) \in S$, $(a + b\sqrt{5}) \cdot 1 = a + b\sqrt{5}$.
Hence, S is a commutative ring with identity, 1.

***

What you have seen in Example 11 is true more generally, i.e.,
$\mathbb{Z}[\sqrt{n}] = \mathbb{Z} + \sqrt{n}\mathbb{Z}$ is a commutative ring with identity for any integer n which is not a square. [Of course, if n is a square, say $n = m^2, m \in \mathbb{Z}$, then $\sqrt{n} = \pm m$. So $\mathbb{Z}[\sqrt{n}] = \mathbb{Z} + m\mathbb{Z} = \mathbb{Z}$, in these cases.]
Thus, $\mathbb{Z}[\sqrt{-5}], \mathbb{Z}[\sqrt{2}], \mathbb{Z}[\sqrt{-2}]$ are all commutative rings with identity.

We can also find commutative rings which are not rings with identity. For example, the ring in Example 10 is commutative, but it has no multiplicative identity. What about the converse? That is, if R is with identity, must it be commutative? Let's see.

Example 12: Is every ring with identity commutative? Why, or why not?

Solution: Consider $\mathbb{M}_2(\mathbb{R})$. Since

$A\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix} = A = \begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}A \ \forall \ A \in \mathbb{M}_2(\mathbb{R})$, $\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}$ is the unity of $\mathbb{M}_2(\mathbb{R})$.

However, if $A = \begin{bmatrix}1 & 0\\ 2 & 0\end{bmatrix}$ and $B = \begin{bmatrix}0 & 1\\ 0 & 2\end{bmatrix}$, then

$AB = \begin{bmatrix}1 & 0\\ 2 & 0\end{bmatrix}\begin{bmatrix}0 & 1\\ 0 & 2\end{bmatrix} = \begin{bmatrix}0 & 1\\ 0 & 2\end{bmatrix}$, and

$BA = \begin{bmatrix}0 & 1\\ 0 & 2\end{bmatrix}\begin{bmatrix}1 & 0\\ 2 & 0\end{bmatrix} = \begin{bmatrix}2 & 0\\ 4 & 0\end{bmatrix}$.

Thus, $AB \neq BA$.

Thus, $\mathbb{M}_2(\mathbb{R})$ is not commutative.

***

Now, let us look at the ring you studied in Example 9. How does this behave regarding commutativity and multiplicative identity? Let's see.

Example 13: Let A and B be rings. Show that

i) $A \times B$ is commutative if and only if both the rings A and B are commutative,

ii) $A \times B$ has unity if and only if both A and B have unity.

We say a ring R **has unity** if it is with unity.

Solution: For convenience we will denote the operations in all three rings, A, B and $A \times B$, by $+$ and $\cdot$.

i) Let (a, b) and $(a', b') \in A \times B$. Then

$(a, b)\cdot(a', b') = (a', b')\cdot(a, b)$

$\Leftrightarrow (a\cdot a', b\cdot b') = (a'\cdot a, b'\cdot b)$

$\Leftrightarrow a\cdot a' = a'\cdot a$ and $b\cdot b' = b'\cdot b$.

Thus, $A \times B$ is commutative iff both A and B are commutative rings.

ii) You should, similarly, show that $A \times B$ is with unity iff A and B are both with unity. If A and B has identities e_1 and e_2, respectively, then the identity of $A \times B$ is (e_1, e_2).

***

Why don't you solve an exercise now?

E21) Which of the rings in Examples 2-8 are rings with unity? Give reasons for your answers.

Now, can the trivial ring be a ring with identity? It seems not, because $0 \neq 1$ in $\mathbb{Z}$, in our minds.

But, $0\cdot 0 = 0$.

So, 0 is also the multiplicative identity for this ring.

Thus, **the trivial ring is a ring with identity in which the additive and multiplicative identities coincide**.

But, if R is not the trivial ring, we have the following result.

Theorem 2: Let R be a ring with identity 1. If $R \neq \{0\}$, then the elements 0 and 1 are distinct.

Proof: Since $R \neq \{0\}$, $\exists\ a \in R$ s.t. $a \neq 0$.
Now suppose $0 = 1$.
Then $a = a \cdot 1 = a \cdot 0 = 0$, by Theorem 1.
i.e., $a = 0$, a contradiction.
Thus, our supposition must be wrong.
Hence, $0 \neq 1$. ■

Now for some related exercises for you!

E22) Check whether or not the ring in E10 is a commutative ring with identity.

E23) Check whether or not $X = \left\{ \begin{bmatrix} x & x \\ x & x \end{bmatrix} \middle| x \in \mathbb{R} \right\}$ is a commutative ring with unity, with respect to the usual matrix addition and multiplication.

E24) Let R be a non-trivial **Boolean ring** (i.e., $a^2 = a\ \forall\ a \in R$). Show that $a = -a\ \forall\ a \in R$. Hence show that R must be commutative.

Fig.2: W. R. Hamilton

Now let us consider an important example of a non-commutative ring with identity. This is the ring of **real quaternions**. It was first described by the Irish mathematician, William Rowan Hamilton (1805 1865). This ring plays an important role in geometry, number theory and the study of mechanics. Later, in Remark 5, we shall consider the relationship of this ring with the group of quaternions, Q_8, that you studied in the earlier units.

Example 14: Let $\mathbb{H} = \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{R}\}$, where i, j, k are symbols that satisfy $i^2 = -1 = j^2 = k^2$, $ij = k = -ji$, $jk = i = -kj$, $ki = j = -ik$.

The elements of $\mathbb{H}$ are also called **real Hamiltonians**, after the creator of $\mathbb{H}$.

We define addition and multiplication in $\mathbb{H}$ by
$(a + bi + cj + dk) + (a_1 + b_1 i + c_1 j + d_1 k)$
$= (a + a_1) + (b + b_1)i + (c + c_1)j + (d + d_1)k$, and
$(a + bi + cj + dk) \cdot (a_1 + b_1 i + c_1 j + d_1 k) = (aa_1 - bb_1 - cc_1 - dd_1) +$
$(ab_1 + ba_1 + cd_1 - dc_1)i + (ac_1 - bd_1 + ca_1 + db_1)j + (ad_1 + bc_1 - cb_1 + da_1)k$.
(This multiplication may seem complicated. But it is not so. It is simply performed as you have done for polynomials in Calculus, keeping the relationship between i, j and k in mind.)

Show that $\mathbb{H}$ is a non-commutative ring with identity.

Solution: You should prove that

i) $(\mathbb{H}, +)$ is an abelian group in which the additive identity is $0 = 0 + 0i + 0j + 0k$,

ii) multiplication in $\mathbb{H}$ is associative, (this may get a bit messy, but don't get put off by that!)

iii) the distributive laws hold, and

iv) $1 = 1 + 0i + 0j + 0k$ is the unity in $\mathbb{H}$.

Thus, $\mathbb{H}$ is a ring with unity.

Would you agree that $\mathbb{H}$ is not a commutative ring? You would, if you remember that $ij \neq ji$, for example.

***

Consider the following important comment about quaternions now.

Remark 5: In E29, Unit 2, you were introduced to Q_8, the group of quaternions. Over there, if we put $i = A$, $j = B$, $k = C$ and $1 = I$, then you can see that i, j, k satisfy the same relations as A, B, C.
So $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ is a subset of $\mathbb{H}$, where i, j, k satisfy the relations given in Example 14.
In fact, $Q_8 = < i > \times < j >$, as you have seen in Block 2.
On the other hand, the group $\mathbb{H}$ is $\mathbb{R} + \mathbb{R}i + \mathbb{R}j + \mathbb{R}k$.
Thus, the group of quaternions is **not** the group $(\mathbb{H}, +)$.
Further, $Q_8 \not< \mathbb{H}$ either, since Q_8 is a group w.r.t. multiplication, while $\mathbb{H}$ is a group w.r.t. addition.

Now, let us consider an interesting aspect about rings with unity. Some elements in such rings are invertible w.r.t. multiplication. For instance, consider $\mathbb{Z}$. Here $1 \cdot 1 = 1$, $(-1) \cdot (-1) = 1$. Thus, both 1 and (-1) are invertible. However, no other element of $\mathbb{Z}$ is invertible because if $x \in \mathbb{Z}$ s.t. $xy = 1$ for some $y \in \mathbb{Z}$, then $x = 1$ or -1.
On the other hand, $\mathbb{R}$ is a ring with unity in which every element of $\mathbb{R}^*$ is invertible.

These examples lead us to a definition.

Definition: Let $(R, +, \cdot)$ be a ring with identity. An element r of R is called a **unit** if there is an $s \in R$ s.t. $rs = 1 = sr$. In this case, s is called an **inverse** of r. (Note that s is also a unit in this case!)

What the definition above says is that a unit is an invertible element of a ring with unity. For example, the identity is a unit in every ring with identity, since $1 \cdot 1 = 1$. Similarly, every non-zero element of $\mathbb{C}$ is a unit. So there can be several units in a ring with unity. Consider the following comment in this regard.

Remark 6: Note the difference between ‘unit’ and ‘unity’. A unit is any invertible element, while the unity is unique, and is the multiplicative identity in the ring concerned. Thus, in a ring with identity, the unity is a unit, but there can be many units apart from the unity.

Now, just as an additive inverse is unique, can we expect a multiplicative inverse of a unit to be unique? Let’s see.

Theorem 3: If r is a unit in R, a ring with identity, then there is a **unique** $s \in R$ s.t. $rs = 1$, i.e., r has a unique inverse in R.

The proof is just as in Theorem 2, Unit 2. We leave it to you to prove (see E25). ■

You have seen that the set of units in a ring with identity can be finite or infinite. In fact, it has more properties, as the following theorem tells us.

Theorem 4: Let R be a ring with identity. The set of units in R is a group with respect to multiplication. (This group is called the **group of units of R**, and is denoted by **U(R)**.)

Proof: First, since $1 \in U(R)$, $U(R) \neq \phi$.

Next, if $r_1, r_2 \in U(R)$, then $\exists\ s_1, s_2 \in R$ s.t. $r_1s_1 = s_1r_1 = 1$, $r_2s_2 = s_2r_2 = 1$.
Hence, $(r_1r_2)(s_2s_1) = r_1(r_2s_2)s_1 = r_1 \cdot 1 \cdot s_1 = r_1s_1 = 1$.
Thus, multiplication is closed in $U(R)$.

Also, $1 \in U(R)$ is the identity.

Further, for any $r \in U(R)$, the unique $s \in U(R)$ s.t. $rs = 1 = sr$ is the inverse of R.

Hence, $(U(R), \cdot)$ is a group. ■

Let us consider some examples.

Example 15: Find $U(R)$, where R is

i) $\mathbb{Z}[i]$, ii) $C[0, 1]$.

Solution: i) $a + ib$ is a unit in $\mathbb{Z}[i]$ iff $\exists\ c + id \in \mathbb{Z}[i]$ such that

$(a + ib)(c + id) = 1$, i.e., $(ac - bd) + i(ad + bc) = 1$,

i.e., $ac - bd = 1$, $ad + bc = 0$. …(2)

Now, if $a = 0$, then (2) implies $bd = -1$ and $bc = 0$,

so that $c = 0$ and $b, d \in U(\mathbb{Z}) = \{1, -1\}$.

Hence, $a = 0 \Rightarrow b = \pm 1$. …(3)

If $a \neq 0$, then

$a = a \cdot 1 = a(ac - bd)$, by (2).

$= a^2c - bad = (a^2 + b^2)c$, since (2) gives $ad = -bc$.

So $(a^2 + b^2) \mid a$.

This is possible only if $b = 0$ and $a^2 = |a|$, since $a^2 \geq a$.

$\therefore ad = 0$ and $a^2 = \pm a \neq 0$. Thus, $d = 0$, so that $ac = 1$, by (2).

Thus, $a = \pm 1$, so that $c = \pm 1$.

So $a \neq 0 \Rightarrow a = \pm 1$ and $b = 0$. …(4)

From (3), we get $\pm i \in U(\mathbb{Z}[i])$.

From (4), we get $\pm 1 \in U(\mathbb{Z}[i])$.

These are the only possibilities.

Hence, $U(\mathbb{Z}[i]) = \{\pm 1, \pm i\}$.

ii) $f \in U(C[0, 1])$

$\Leftrightarrow \exists\ g \in C[0, 1]$ s.t. $f(x)g(x) = 1\ \forall\ x \in [0, 1]$

$\Leftrightarrow f(x) \neq 0\ \forall\ x \in [0, 1]$.

Hence, $U(C[0, 1]) = \{f \in C[0, 1] \mid f(x) \neq 0\ \forall\ x \in [0, 1]\}$.

***

Example 16: Let $\mathbb{R}[x]$ be the set of polynomials with coefficients in $\mathbb{R}$ (refer to Block 1, Calculus). Show that $(\mathbb{R}[x], +, \cdot)$ is a commutative ring with identity. Also find $U(\mathbb{R}[x])$.

You will study polynomial rings in detail in Block 4.

Solution: Firstly, for $f(x)$ and $g(x)$ in $\mathbb{R}[x]$, recall from Calculus that $f(x) = a_0 + a_1x + \cdots + a_rx^r$, $g(x) = b_0 + b_1x + \cdots + b_sx^s$ for some non-negative integers r and s, and $a_i, b_j \in \mathbb{R}\ \forall\ i = 1,\ldots,r,\ j = 1,\ldots,s$.

Now, either $r \le s$ or $r \ge s$. Without loss of generality, we can assume $r \ge s$. Then

$$f(x) + g(x) = (a_0 + b_0) + (a_1 + b_1)x + \cdots + (a_s + b_s)x^s + a_{s+1}x^{s+1} + \cdots + a_rx^r \in \mathbb{R}[x],$$

and $$f(x)g(x) = a_0b_0 + (a_1b_0 + a_0b_1)x + \cdots + \left(\sum_{i+j=k} a_ib_j\right)x^k + \cdots + a_rb_sx^{r+s} \in \mathbb{R}[x].$$

Thus, $+$ and $\cdot$ are binary operations on $\mathbb{R}[x]$.

You should prove that $(\mathbb{R}[x], +)$ is an abelian group, with additive identity 0 and the additive inverse of $\sum_{i=0}^{m} a_ix^i$ being $\sum_{i=0}^{m} (-a_i)x^i$.

Next, you should show that multiplication is associative in $\mathbb{R}[x]$. (This can get a bit messy, but try it for polynomials upto degree 3 first, to get a hang of what is happening.)

Finally, let us prove that the distributive laws are satisfied. Let $f(x) = \sum_{i=0}^{r} a_ix^i$, $g(x) = \sum_{j=0}^{s} b_jx^j$ and $h(x) = \sum_{k=0}^{t} c_kx^k$. Also, let us assume $t \le s$, without loss of generality, and put $c_{t+1} = c_{t+2} = \cdots = c_s = 0$.

Then $$f(x)(g(x) + h(x)) = \left(\sum_{i=0}^{r} a_ix^i\right)\left(\sum_{j=0}^{s} (b_j + c_j)x^j\right)$$

$$= \sum_{k=0}^{r+s}\left[\sum_{i+j=k} a_i(b_j + c_j)\right]x^k$$

$$= \sum_{k=0}^{r+s}\left[\sum_{i+j=k} (a_ib_j + a_ic_j)\right]x^k$$

$$= \sum_{k=0}^{r+s}\left(\sum_{i+j=k} a_ib_j\right)x^k + \sum_{k=0}^{r+s}\left(\sum_{i+j=k} a_ic_j\right)x^k$$

$$= f(x)g(x) + f(x)h(x).$$

Thus, the left distributive law holds for $\mathbb{R}[x]$.

Note that since $\mathbb{R}$ is a commutative ring, $f(x)g(x) = g(x)f(x)$ $\forall\ f(x), g(x) \in \mathbb{R}[x]$. Thus, multiplication in $\mathbb{R}[x]$ is commutative. Hence, the right distributive law also holds for $\mathbb{R}[x]$.

Hence, $\mathbb{R}[x]$ is a commutative ring.

Also, the constant polynomial $1 \in \mathbb{R}[x]$ is the unity of $\mathbb{R}[x]$, since $1 \cdot f(x) = f(x)\ \forall\ f(x) \in \mathbb{R}[x]$.
Hence, $\mathbb{R}[x]$ has unity.

Now, if $f(x) \in \mathbb{R}[x]$ is a unit, then $\exists\ g(x) \in \mathbb{R}[x]$ such that $f(x)g(x) = 1$. So

$$\deg f(x) + \deg g(x) = \deg 1 = 0. \quad \ldots(5)$$

But $\deg f(x) \geq 0, \deg g(x) \geq 0.$

So, (5) tells us that $\deg f(x) = 0 = \deg g(x).$

Thus, $f(x) \in \mathbb{R}^*$, $g(x) \in \mathbb{R}^*$.

Thus, $U(\mathbb{R}[x]) = U(\mathbb{R}) = \mathbb{R}^*$.

***

You should solve some exercises now.

E25) Prove Theorem 3.

E26) Show that $U(\mathbb{M}_2(\mathbb{C})) = GL_2(\mathbb{C})$.
(**Hint:** Use the determinant function.)

E27) Find $U(\mathbb{Z}[x])$.

E28) If R is a ring with identity, is

i) $(U(R), +)$ a group?

ii) $(U(R), \cdot)$ an abelian group?

In a commutative ring R an element a **divides** an element b if $\exists\ c \in R$ s.t. $a = bc$. This is denoted by $\mathbf{a \mid b}$.

E29) Show that if R is a commutative ring with identity and $a \in R$ is a unit, then $a \mid r\ \forall\ r \in R$.

Is the converse true? That is, if $\exists\ a \in R$ s.t. $a \mid r\ \forall\ r \in R$, then must a be a unit? Why, or why not?

E30) Show that the set of all differentiable functions from $\mathbb{R}$ to $\mathbb{R}$ is a ring with respect to pointwise addition and multiplication. Is this a ring with identity? Is it commutative? Give reasons for your answers.

So far, in this unit we have discussed various types of rings. You have seen examples of commutative and non-commutative rings, and rings with and without identity. We shall continue this discussion in the next unit, where we shall focus on the analogue of subgroups, for rings.

Now, let us summarise what you have studied in this unit.

10.5 SUMMARY

In this unit, we discussed the following points.

1. The axioms that define a ring, and some examples of this algebraic system. In particular, the example of the external direct product of rings.

2. Some elementary properties of a ring, like
$a \cdot 0 = 0 = 0 \cdot a,$
$a(-b) = -(ab) = (-a)b,$
$(-a)(-b) = ab,$
$a(b - c) = ab - ac,$

$(b-c)a = ba - ca,$
$\forall\ a, b, c$ in a ring R.

3. The laws of indices for addition and multiplication in a ring, and the generalised distributive law.

4. The definition, and examples, of a commutative ring, a ring with unity and a commutative ring with unity.

5. The additive and multiplicative identities are distinct in a non-trivial ring with identity.

6. The definition, and examples, of a unit in a ring with identity.

7. The set of all the units in a ring R with identity is a group w.r.t. multiplication. This group is denoted by $U(R)$.

10.6 SOLUTIONS / ANSWERS

E1) **Addition in $\mathbb{Z}_6^*$**

$+$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$
$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$

Multiplication in $\mathbb{Z}_6^*$

$\cdot$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{2}$	$\overline{2}$	$\overline{4}$	$\overline{0}$	$\overline{2}$	$\overline{4}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$
$\overline{4}$	$\overline{4}$	$\overline{2}$	$\overline{0}$	$\overline{4}$	$\overline{2}$
$\overline{5}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

From the tables above, you can see that neither addition nor multiplication are binary operations in $\mathbb{Z}_6^*$, since $\overline{0} \notin \mathbb{Z}_6^*$. Thus, $(\mathbb{Z}_6^*, +, \cdot)$ can't be a ring.

E2) Note that $+$ and $\cdot$ are binary operations on $\{0\}$. The axioms $R1\text{-}R6$ are trivially satisfied by $(\{0\}, +, \cdot)$ as you should verify.

Now, suppose a singleton $\{a\}$ is a ring. Then this must contain the additive identity 0. But $\{a\}$ has only one element. Thus, $a = 0$.
Hence, $\{a\} = \{0\}$.

E3) We define addition and multiplication in $\mathbb{Q}[\sqrt{2}]$ by
$(a + \sqrt{2}b) + (c + \sqrt{2}d) = (a + c) + \sqrt{2}(b + d)$, and
$(a + \sqrt{2}b) \cdot (c + \sqrt{2}d) = (ac + 2bd) + \sqrt{2}(ad + bc)\ \forall\ a, b, c, d \in \mathbb{Q}$.
Since $+$ is associative and commutative in $\mathbb{R}$, the same holds for $+$ in $\mathbb{Q} + \sqrt{2}\mathbb{Q}$.
Here $0 = 0 + \sqrt{2} \cdot 0$ is the additive identity and $(-a) + \sqrt{2}(-b)$ is the additive inverse of $a + \sqrt{2}b$.
Thus, $\mathbb{Q}[\sqrt{2}]$ satisfies $R1'$ (or $R1\text{-}R4$).
(Note that you could also have shown that $\mathbb{Q}[\sqrt{2}]$ satisfies $R1'$ by showing it is a subgroup of $(\mathbb{R}, +)$.)

Since multiplication in $\mathbb{R}$ is associative, R5 (or R2′) holds for $\mathbb{Q}+\sqrt{2}\mathbb{Q}$ also.

Since multiplication distributes over addition in $\mathbb{R}$, it does so in $\mathbb{Q}+\sqrt{2}\mathbb{Q}$ as well. Hence, $\mathbb{Q}[\sqrt{2}]$ satisfies R6 (or R3′).

Thus, $(\mathbb{Q}+\sqrt{2}\mathbb{Q}, +, \cdot)$ is a ring.

Further, since $\cdot$ is commutative over $\mathbb{R}$, it is commutative over $\mathbb{Q}[\sqrt{2}]$.
Hence, $\mathbb{Q}[\sqrt{2}]$ is a commutative ring.

E4) As you know, $+$ and $\cdot$ are well-defined binary operations on R.
Now, for $\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}, \begin{bmatrix} c & 0 \\ 0 & d \end{bmatrix} \in R$, $\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} - \begin{bmatrix} c & 0 \\ 0 & d \end{bmatrix} = \begin{bmatrix} a-c & 0 \\ 0 & b-d \end{bmatrix} \in R$.
Thus, $(R, +) \leq \mathbb{M}_2(\mathbb{R})$.
Hence, $(R, +)$ is an abelian group.

Also, $(R, \cdot)$ is a semigroup, as you know from Unit 1.

From Unit 1, you also know that $(R, +, \cdot)$ satisfies R6.

Hence, R is a ring.
Now, for any $\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}, \begin{bmatrix} c & 0 \\ 0 & d \end{bmatrix} \in R$,
$\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}\begin{bmatrix} c & 0 \\ 0 & d \end{bmatrix} = \begin{bmatrix} ac & 0 \\ 0 & bd \end{bmatrix} = \begin{bmatrix} ca & 0 \\ 0 & db \end{bmatrix} = \begin{bmatrix} c & 0 \\ 0 & d \end{bmatrix}\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$.
Hence, R is commutative.

E5) You should show that $+$ and $\cdot$ are binary operations on R.
You should also show that $(R, +, \cdot)$ satisfies R1-R6, as in E4.
However, $\begin{bmatrix} 1 & 0 \\ 2 & 0 \end{bmatrix}\begin{bmatrix} 3 & 0 \\ 4 & 0 \end{bmatrix} \neq \begin{bmatrix} 3 & 0 \\ 4 & 0 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 2 & 0 \end{bmatrix}$, for example.
Hence, R is not a commutative ring.

E6) i) $\cup$ and $\cap$ are well-defined binary operations on $\wp(X)$. However, for any $A \subseteq X$, $A \neq \phi$, there is no $B \subseteq X$ such that $A \cup B = \phi$, the identity with respect to $\cup$.
Hence, $(\wp(X), \cup, \cap)$ is not a ring.

ii) Since $+$ is not a binary operation on $\mathbb{R}^*$, this is not a ring.

iii) As you know from Unit 1, multiplication is not a binary operation on $\mathbb{M}_{2\times 3}(\mathbb{R})$. Hence, this is not a ring.

E7)

+	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

Since $b + b = c \neq b$, b is not the additive identity. Similarly, c is not the additive identity. Hence, a is the zero element. Hence, the first row and column in the table above are as filled.

Now, remember that since $(R, +)$ is a group, each element of R must figure once and only once in each row and column of the table.

So, since $b + c = c + b$, and the only element missing in the second row is a, $b + c = a = c + b$.

Thus, the table above is as filled.

$\cdot$	a	b	c
a	a	a	a
b	a	a	a
c	a	a	a

Since $b \cdot b = a$ and $a + b = b$, $b \cdot b = (a + b) \cdot b = a \cdot b + b \cdot b$. Thus, $a \cdot b$ is the zero element, i.e., a.

Similarly, you should see why $c \cdot b = a$, using $b + b = c$. Hence, the 2nd column of the multiplication table above has a in each cell.

Now, $a \cdot a = a \cdot (b \cdot b) = (a \cdot b) \cdot b = a \cdot b = a$.

Similarly, you should explain why

$b \cdot a = a$, $c \cdot a = a$, $a \cdot c = a$, $b \cdot c = a$, $c \cdot c = a$.

Hence, the table above is as filled.

E8) From Unit 1, you know that $(m, n) \in \mathbb{Z}$ and $[m, n] \in \mathbb{Z}$ $\forall$ $m, n \in \mathbb{Z}$.

Thus, $\oplus$ and $\odot$ are binary operations on $\mathbb{Z}$. However, $(\mathbb{Z}, \oplus)$ is not a group. This is because 0 is the identity; but given $m \in \mathbb{Z}^*$, there is no $n \in \mathbb{Z}$ s.t. $(m, n) = 0$. For example, $(1, n) \neq 0$ for any $n \in \mathbb{Z}$.

E9) Since R satisfies $R1, R2, R5$ and $R6$, so does $\text{Map}(X, R)$.

The zero element is $\mathbf{0} : X \to R : \mathbf{0}(x) = 0$.

The additive inverse of $f : X \to R$ is $(-f) : X \to R : (-f)(x) = -f(x)$.

Thus, $(\text{Map}(X, R), +, \cdot)$ satisfies $R1 - R6$. Hence, it is a ring.

For any X, $\text{Map}(X, R)$ will be commutative iff R is commutative, since $f \cdot g = g \cdot f \Leftrightarrow (f \cdot g)(x) = (g \cdot f)(x) \Leftrightarrow f(x)g(x) = g(x)f(x)$ $\forall$ $x \in X$.

E10) Firstly, you should verify that $\oplus$ and $\odot$ are well-defined binary operations on $\mathbb{R}$.

Next, let us check if $(\mathbb{R}, \oplus, \odot)$ satisfies $R1 - R6$.

Now, $\forall$ $a, b, c \in \mathbb{R}$,

R1 : $a \oplus b = a + b + 1 = b + a + 1 = b \oplus a$.

R2 : $(a \oplus b) \oplus c = (a + b + 1) \oplus c = a + b + 1 + c + 1$

$= a + (b + c + 1) + 1$

$= a \oplus (b \oplus c)$

R3 : $a \oplus (-1) = a - 1 + 1 = a$.

Thus, (-1) is the identity with respect to $\oplus$.

R4 : $a \oplus (-a - 2) = a + (-a - 2) + 1 = -1$.

Thus, $-a - 2$ is the inverse of a with respect to $\oplus$.

R5 : $(a \odot b) \odot c = (ab + a + b) \odot c = (ab + a + b)c + (ab + a + b) + c$
$= a(bc + b + c) + a + (bc + b + c)$
$= a \odot (b \odot c).$

R6 : $a \odot (b \oplus c) = a \odot (b + c + 1) = a(b + c + 1) + a + (b + c + 1)$
$= (ab + a + b) + (ac + a + c) + 1$
$= (a \odot b) \oplus (a \odot c).$

Since $a \odot b = b \odot a,$ the right distributive law also holds.

Thus, $(\mathbb{R}, \oplus, \odot)$ is a ring.

E11) Use the fact that $(R, +, \cdot)$ satisfies $R1 - R6,$ to show that $\mathbb{M}_2(R)$ satisfies the axioms. For instance, to check $R6,$ consider

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \left(\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} + \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} \right) = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \begin{bmatrix} a_1 + a_2 & b_1 + b_2 \\ c_1 + c_2 & d_1 + d_2 \end{bmatrix}$$

$$= \begin{bmatrix} a(a_1 + a_2) + b(c_1 + c_2) & a(b_1 + b_2) + b(d_1 + d_2) \\ c(a_1 + a_2) + d(c_1 + c_2) & c(b_1 + b_2) + d(d_1 + d_2) \end{bmatrix}$$

$$= \begin{bmatrix} aa_1 + bc_1 & ab_1 + bd_1 \\ ca_1 + dc_1 & cb_1 + dd_1 \end{bmatrix} + \begin{bmatrix} aa_2 + bc_2 & ab_2 + bd_2 \\ ca_2 + dc_2 & cb_2 + dd_2 \end{bmatrix},$$ since R satisfies R1 and R6.

$$= \begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} + \begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix}$$

for $\begin{bmatrix} a & b \\ c & d \end{bmatrix}, \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}, \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix}$ in $\mathbb{M}_2(R).$

E12) $\mathbb{Z}_2 = \{\bar{0}, \bar{1}\}, \mathbb{Z}_3 = \{\bar{0}, \bar{1}, \bar{2}\}.$

$\therefore \mathbb{Z}_2 \times \mathbb{Z}_3 = \{(\bar{0}, \bar{0}), (\bar{0}, \bar{1}), (\bar{0}, \bar{2}), (\bar{1}, \bar{0}), (\bar{1}, \bar{1}), (\bar{1}, \bar{2})\}.$

Note that the first component is 'mod 2', and the second component is 'mod 3', in each element of $\mathbb{Z}_2 \times \mathbb{Z}_3$.

Thus, the tables are:

+	$(\bar{0}, \bar{0})$	$(\bar{0}, \bar{1})$	$(\bar{0}, \bar{2})$	$(\bar{1}, \bar{0})$	$(\bar{1}, \bar{1})$	$(\bar{1}, \bar{2})$
$(\bar{0}, \bar{0})$	$(\bar{0}, \bar{0})$	$(\bar{0}, \bar{1})$	$(\bar{0}, \bar{2})$	$(\bar{1}, \bar{0})$	$(\bar{1}, \bar{1})$	$(\bar{1}, \bar{2})$
$(\bar{0}, \bar{1})$	$(\bar{0}, \bar{1})$	$(\bar{0}, \bar{2})$	$(\bar{0}, \bar{0})$	$(\bar{1}, \bar{1})$	$(\bar{1}, \bar{2})$	$(\bar{1}, \bar{0})$
$(\bar{0}, \bar{2})$	$(\bar{0}, \bar{2})$	$(\bar{0}, \bar{0})$	$(\bar{0}, \bar{1})$	$(\bar{1}, \bar{2})$	$(\bar{1}, \bar{0})$	$(\bar{1}, \bar{1})$
$(\bar{1}, \bar{0})$	$(\bar{1}, \bar{0})$	$(\bar{1}, \bar{1})$	$(\bar{1}, \bar{2})$	$(\bar{0}, \bar{0})$	$(\bar{0}, \bar{1})$	$(\bar{0}, \bar{2})$
$(\bar{1}, \bar{1})$	$(\bar{1}, \bar{1})$	$(\bar{1}, \bar{2})$	$(\bar{1}, \bar{0})$	$(\bar{0}, \bar{1})$	$(\bar{0}, \bar{2})$	$(\bar{0}, \bar{0})$
$(\bar{1}, \bar{2})$	$(\bar{1}, \bar{2})$	$(\bar{1}, \bar{0})$	$(\bar{1}, \bar{1})$	$(\bar{0}, \bar{2})$	$(\bar{0}, \bar{0})$	$(\bar{0}, \bar{1})$

·	$(\bar{0}, \bar{0})$	$(\bar{0}, \bar{1})$	$(\bar{0}, \bar{2})$	$(\bar{1}, \bar{0})$	$(\bar{1}, \bar{1})$	$(\bar{1}, \bar{2})$
$(\bar{0}, \bar{0})$	$(\bar{0}, \bar{0})$	$(\bar{0}, \bar{0})$	$(\bar{0}, \bar{0})$	$(\bar{0}, \bar{0})$	$(\bar{0}, \bar{0})$	$(\bar{0}, \bar{0})$
$(\bar{0}, \bar{1})$	$(\bar{0}, \bar{0})$	$(\bar{0}, \bar{1})$	$(\bar{0}, \bar{2})$	$(\bar{0}, \bar{0})$	$(\bar{0}, \bar{1})$	$(\bar{0}, \bar{2})$
$(\bar{0}, \bar{2})$	$(\bar{0}, \bar{0})$	$(\bar{0}, \bar{2})$	$(\bar{0}, \bar{1})$	$(\bar{0}, \bar{0})$	$(\bar{0}, \bar{2})$	$(\bar{0}, \bar{1})$
$(\bar{1}, \bar{0})$	$(\bar{0}, \bar{0})$	$(\bar{0}, \bar{0})$	$(\bar{0}, \bar{0})$	$(\bar{1}, \bar{0})$	$(\bar{1}, \bar{0})$	$(\bar{1}, \bar{0})$
$(\bar{1}, \bar{1})$	$(\bar{0}, \bar{0})$	$(\bar{0}, \bar{1})$	$(\bar{0}, \bar{2})$	$(\bar{1}, \bar{0})$	$(\bar{1}, \bar{1})$	$(\bar{1}, \bar{2})$
$(\bar{1}, \bar{2})$	$(\bar{0}, \bar{0})$	$(\bar{0}, \bar{2})$	$(\bar{0}, \bar{1})$	$(\bar{1}, \bar{0})$	$(\bar{1}, \bar{2})$	$(\bar{1}, \bar{1})$

Look at the multiplication table above. The entries in it are symmetric about the diagonal of the table from $(\bar{0}, \bar{0})\cdot(\bar{0}, \bar{0})$ to $(\bar{1}, \bar{2})\cdot(\bar{1}, \bar{2})$.
Thus, $\mathbb{Z}_2 \times \mathbb{Z}_3$ is a commutative ring.

E13) Since $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$, by Example 9 it is a ring w.r.t component-wise addition and multiplication.
Similarly, $\mathbb{C}^2$ is a ring. Hence, $\mathbb{C}^3 = \mathbb{C}^2 \times \mathbb{C}$ is a ring.

E14) We know that $a + 0 = a \ \forall \ a \in R$.
Since $a + 0 = a \cdot 0$, we find that $a \cdot 0 = a \ \forall \ a \in R$.
But, by Theorem 1, you know that $a \cdot 0 = 0$.
Thus, $a = 0 \ \forall \ a \in R$, that is, $R = \{0\}$.

E15) Let $P(n)$ be the following predicate:
$a(b_1 + \cdots + b_n) = ab_1 + \cdots + ab_n$ for $a, b_1, \ldots, b_n \in R$.
Now $P(1)$ is true, since $a(b_1) = ab_1$.
Assume that $P(k)$ is true for some $k \in \mathbb{N}$.
Now consider

$$\begin{aligned} a(b_1 + \cdots + b_k + b_{k+1}) &= a[(b_1 + \cdots + b_k) + b_{k+1}], \text{ by definition.} \\ &= a(b_1 + \cdots + b_k) + ab_{k+1}, \text{ by R6.} \\ &= (ab_1 + \cdots + ab_k) + ab_{k+1}, \text{ since } P(k) \text{ is true.} \\ &= ab_1 + \cdots + ab_k + ab_{k+1}, \text{ by definition.} \end{aligned}$$

Thus, $P(k+1)$ is true.
Hence, $P(n)$ is true for every $n \in \mathbb{N}$.

You should similarly prove the second equality.

E16) Since $(a+b)^1 = a^1 + b^1$, the given expansion is true for $n = 1$.
Assume that the expansion is true for some $m \in \mathbb{N}$, i.e.,
$(a+b)^m = a^m + {}^mC_1 a^{m-1}b + \cdots + {}^mC_{m-1}ab^{m-1} + b^m$.
Now, $(a+b)^{m+1} = (a+b)(a+b)^m = (a+b)\left(\sum_{k=0}^{m} {}^mC_k a^{m-k}b^k\right)$

$$= \sum_{k=0}^{m} {}^mC_k a^{m-k+1}b^k + \sum_{k=0}^{m} {}^mC_k a^{m-k}b^{k+1}, \text{ by distributivity.}$$

$$\begin{aligned} &= (a^{m+1} + {}^mC_1 a^{m+1-1}b + {}^mC_2 a^{m+1-2}b^2 + \cdots + {}^mC_m ab^m) \\ &\quad + ({}^mC_0 a^m b + {}^mC_1 a^{m-1}b^2 + \cdots + {}^mC_{m-1}ab^m + b^{m+1}) \\ &= a^{m+1} + ({}^mC_1 + {}^mC_0)a^{m+1-1}b + \cdots + ({}^mC_k + {}^mC_{k-1})a^{m+1-k}b^k + \cdots + b^{m+1} \\ &= a^{m+1} + {}^{m+1}C_1 a^{m+1-1}b + \cdots + {}^{m+1}C_k a^{m+1-k}b^k + \cdots + {}^{m+1}C_m ab^m + b^{m+1} \end{aligned}$$

(since ${}^mC_k + {}^mC_{k-1} = {}^{m+1}C_k$).
Thus, the equality is true for $n = m + 1$ also.
Hence, by the principle of induction, it is true for all $n \in \mathbb{N}$.

E17) By definition, $a^m = a \cdot a \ldots a (m \text{ times})$
Now, let us fix an $m \in \mathbb{N}$, and let $P(n)$ be the predicate that
$a^m \cdot a^n = a^{m+n}$, $n \in \mathbb{N}$.
Then, $P(1)$ is true, by definition.
Assume that $P(k)$ is true for some $k \in \mathbb{N}$.

Then, $a^m \cdot a^{k+1} = a^m \cdot (a^k \cdot a)$, by definition.

$= (a^m \cdot a^k) \cdot a$, by R5.

$= a^{m+k} \cdot a$, since $P(k)$ is true.

$= a^{m+(k+1)}$, by definition.

Hence, $P(k+1)$ is true.

Thus, by the PMI, $P(n)$ is true $\forall\ n \in \mathbb{N}$.

Since $(R, \cdot)$ is not a group, a^0 or a^{-1} may not exist. For instance, 2^{-1} does not exist in $\mathbb{Z}$. Similarly, $a^0 = 1$ does not exist in $2\mathbb{Z}$.

Hence, a^m and a^n need not exist if $m, n \leq 0$.

Hence, the equality cannot be extended to non-positive integers.

E18) Let $m, n > 0$. Then

$ma = a + a + \cdots + a (m \text{ times})$ and $nb = b + \cdots + b (n \text{ times})$.

So, by applying the generalised law of distributivity, extending E15,

$(ma)(nb) = (a + \cdots + a)(b + \cdots + b) = ab(mn \text{ times})$

$= mn(ab)$. …(6)

Now, let $m < 0, n > 0$. Then $-m > 0$.

Also $(-m)(-a) = (-a) + (-a) + \cdots + (-a)[(-m) \text{ times}]$

So $(-m)(-a)(nb) = (-mn)(-ab)$, by Theorem 1 and (6).

$= -(-mn)(ab)$, by Theorem 1.

$= (mn)(ab)$.

Similarly, you should prove the cases $m < 0, n < 0$ and $m > 0, n < 0$.

E19) This can be proved as in Theorem 2, Unit 2.

E20) As in Example 10, show that $n\mathbb{Z}$ cannot have identity, for $n \geq 2$.

E21) $\mathbb{Z}_n$ has identity $\bar{1}$, since $\bar{a} \cdot \bar{1} = \bar{a} = \bar{1} \cdot \bar{a}\ \forall\ \bar{a} \in \mathbb{Z}_n$.

$\mathbb{Z}[i]$ has identity $1 + i0$. (Why?)

$\mathbb{M}_3(\mathbb{Z}_4)$ has identity $I = \begin{bmatrix} \bar{1} & \bar{0} & \bar{0} \\ \bar{0} & \bar{1} & \bar{0} \\ \bar{0} & \bar{0} & \bar{1} \end{bmatrix}$, since $AI = IA = A\ \forall\ A \in \mathbb{M}_3(\mathbb{Z}_4)$.

$\wp(X)$ has identity X, since $A \cap X = A = X \cap A\ \forall\ A \subseteq X$.

$C[0, 1]$ has identity $g : [0, 1] \to \mathbb{R} : g(x) = 1$, since

$(f \cdot g)(x) = f(x) \cdot g(x) = f(x)$, and $(g \cdot f)(x) = f(x)\ \forall\ x \in [0, 1]$.

Note that g is continuous on $[0, 1]$ as it is a constant function.

End A has identity $I_A : A \to A : I_A(x) = x$. (Why?)

E22) Since $a \odot b = b \odot a\ \forall\ a, b \in \mathbb{R}$, $\odot$ is commutative.

Also, $a \odot 0 = a\ \forall\ a \in \mathbb{R}$.

Thus, 0 is the multiplicative identity. (Note that the additive identity here is not zero.)

Hence, $(\mathbb{R}, \oplus, \odot)$ is a commutative ring with identity.

E23) You must first check that $+$ and $\cdot$ are closed on X. Then check that X satisfies R1-R6.

Note that $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ is the additive identity.

Then you should check that $AB = BA$ for any two elements A and B.

Thus, the ring is commutative.

It has identity $\begin{bmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{bmatrix}$, which you should prove.

E24) For any $a \in R$, $a^2 = a$. In particular,

$(2a)^2 = 2a$

$\Rightarrow 4a^2 = 2a \Rightarrow 4a = 2a$, since $a^2 = a$.

$\Rightarrow 2a = 0 \Rightarrow a + a = 0$

$\Rightarrow a = -a.$ …(7)

Now, for any $a, b \in R$, $a + b \in R$.

$\therefore (a+b)^2 = a + b$

$\Rightarrow a^2 + ab + ba + b^2 = a + b$

$\Rightarrow a + ab + ba + b = a + b$, since $a^2 = a$ and $b^2 = b$.

$\Rightarrow ab = -ba$, by cancellation.

$\Rightarrow ab = ba$, since $-ba = ba$, by (7).

Thus, R is commutative.

E25) By definition, $\exists\ s \in R$ s.t. $rs = 1 = sr$.

Now suppose $\exists\ t \in R$ s.t. $rt = 1 = tr$.

Then $s = s \cdot 1 = s(rt) = (sr)t = 1 \cdot t = t$.

Thus, the inverse is unique.

E26) As in Example 12, $\mathbb{M}_2(\mathbb{C})$ has identity $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$.

Now, $A \in U(\mathbb{M}_2(\mathbb{C}))$ iff $\exists\ B \in \mathbb{M}_2(\mathbb{C})$ s.t. $AB = I$.

Then $\det(AB) = \det(I) = 1$.

Thus, $\det(A)\det(B) = 1$.

So $\det(A) \neq 0$, i.e., $A \in GL_2(\mathbb{C})$.

Hence, $U(\mathbb{M}_2(\mathbb{C})) \subseteq GL_2(\mathbb{C})$. …(8)

Conversely, if $A \in GL_2(\mathbb{C})$, then $\exists\ B$ s.t. $AB = I = BA$, since $(GL_2(\mathbb{C}), \cdot)$ is a group.

Thus, $A \in U(\mathbb{M}_2(\mathbb{C}))$.

Hence, $GL_2(\mathbb{C}) \subseteq U(\mathbb{M}_2(\mathbb{C}))$. …(9)

By (8) and (9), $U(\mathbb{M}_2(\mathbb{C})) = GL_2(\mathbb{C})$.

E27) As in Example 16, show that if $f(x) \in U(\mathbb{Z}[x])$, then $f(x) \in \mathbb{Z}$ and $\exists\ n \in \mathbb{Z}$ s.t. $f(x) \cdot n = 1$.

Thus, $f(x) = \pm 1$.
Hence, $U(\mathbb{Z}[x]) = \{\pm 1\}$.

E28) i) No. For instance, $U(\mathbb{Z}) = \{\pm 1\}$ is not a group w.r.t addition. (Why?)

ii) $(U(R), \cdot)$ is a group, by Theorem 4. But it need not be abelian. For instance, if $R = \mathbb{M}_2(\mathbb{C})$, then $U(R) = GL_2(\mathbb{C})$, which is not abelian.

E29) Since $a \in U(R)$, $\exists\ b \in R$ s.t. $ab = 1$.
Then $r = 1 \cdot r = (ab)r = a(br)$.
Thus, $a \mid r$.

Conversely, if $a \in R$ s.t. $a \mid r\ \forall\ r \in R$, then $a \mid 1$.
So $\exists\ b \in R$ s.t. $ab = 1$. Thus, $a \in U(R)$.

E30) Let $\mathcal{D} = \{f : \mathbb{R} \to \mathbb{R} : f$ is differentiable$\}$.
From Calculus, you know that the sum and product of differentiable functions is differentiable. So $+$ and $\cdot$ are binary operations on $\mathcal{D}$.
Use the fact that $\mathbb{R}$ satisfies $R1, R2, R5, R6,$ to prove that $\mathcal{D}$ satisfies these axioms too.
Next, show that the zero function, $\mathbf{0}$, is the additive identity, and $-f : \mathbb{R} \to \mathbb{R}$ is the additive inverse of $f \in \mathcal{D}$.
So, $(\mathcal{D}, +, \cdot)$ is a ring.

The constant function $g : \mathbb{R} \to \mathbb{R} : g(x) = 1$ is in $\mathcal{D}$, and is the identity. (Why?)

Since $\mathbb{R}$ is a commutative ring, so is $\mathcal{D}$.

UNIT 11

SUBRINGS

Structure | Page Nos.

11.1 INTRODUCTION

In this unit, we take the discussion on rings further. Here the focus is on the analogue, in ring theory, of what you studied in Unit 3. In other words, the discussion here is on various aspects of subrings, a concept that corresponds to that of a subgroup of a group. As you have seen, a ring is also a group. So, it may not surprise you to know that a subring is also a subgroup. Because of this, you will find Unit 3 often being referred to during the discussion on subrings. So it may be a good idea for you to quickly revise Unit 3 before getting into this unit.

Our discussion will begin in Sec.11.2. Here we will introduce you to what a subring is. Of course, as always, you will study several examples of subrings too.

In the next section, Sec.11.3, you will study the criteria for a subset of a ring to be a subring. Here we shall use what you studied in Sec.3.3, Unit 3. You will also see, in this section, that a subring of a ring has many algebraic properties that the ring has. It also can differ from the ring algebraically, in many aspects, as you will find.

Finally, in Sec.11.4, you will study about whether the intersection, union, sum and Cartesian product of subrings of a ring are subrings or not. Here too, you will find a lot of similarity with the results for set operations on subgroups, discussed in Unit 3.

We have given below the broad learning expectations around which this unit is created. If you study the sections carefully, and do every exercise yourself, you would be able to meet these objectives. Only then will you be comfortable in understanding the further units of this course.

Objectives

After studying this unit, you should be able to:

- define, and give examples of, a subring of a ring;
- check whether a subset of a ring is a subring or not;
- prove, and apply, the conditions for the intersection, union, sum or Cartesian product of subrings of a ring to be a subring;
- prove that the direct product of subrings is a subring of the direct product of the rings concerned.

11.2 WHAT IS A SUBRING?

When you hear the word 'subring', what comes to mind? With your experience of Block 1 and Unit 10, you would probably think that this is a subset of a ring that is a ring itself. If so, then you are right.
In the previous unit you saw that, not only is $\mathbb{Z} \subseteq \mathbb{Q}$, but $\mathbb{Z}$ and $\mathbb{Q}$ are rings with respect to the **same operations**. This shows that $\mathbb{Z}$ is a subring of $\mathbb{Q}$, as you will now see.

Definition: Let $(R, +, \cdot)$ be a ring and S be a non-empty subset of R. S is called a **subring** of R, if $(S, +, \cdot)$ is itself a ring, i.e., S is a ring with respect to the operations w.r.t. which R is a ring.

So, $(\mathbb{Z}, +, \cdot)$ is a subring of $(\mathbb{Q}, +, \cdot)$. Also, $(\mathbb{Q}, +, \cdot)$ is a subring of $(\mathbb{R}, +, \cdot)$. Further, using Example 1, Unit 10, you can see that $2\mathbb{Z}$, the set of even integers, is a ring with respect to the operations which make $\mathbb{Z}$ a ring. Hence $(2\mathbb{Z}, +, \cdot)$, is a subring of $(\mathbb{Z}, +, \cdot)$.

Similarly, from Example 11, Unit 10, you can see that $(\mathbb{Z}[\sqrt{5}], +, \cdot)$ and $(\mathbb{Z}[\sqrt{-5}], +, \cdot)$ are subrings of $(\mathbb{C}, +, \cdot)$.

Consider the following remarks regarding this concept.

Remark 1: If $(S, +, \cdot)$ is a subring of $(R, +, \cdot)$, we shall just say that S is a subring of R, unless the operations concerned need to be stressed.

Remark 2: Note that **the operations of S and R have to be the same** if S is to be a subring of R. For example, $(\mathbb{R}, \oplus, \odot)$ of E10, Unit 10, is **not** a subring of $(\mathbb{C}, +, \cdot)$, since $\oplus$ and $\odot$ are different from $+$ and $\cdot$, respectively.

Before giving more examples, let us analyse the definition of a subring. The definition says that a subring of a ring R is a ring with respect to the operations which make R a ring. Now, the distributive, commutative and associative laws for these operations hold good in R. Therefore, they hold good in any subset of R also. So, to prove that a subset S of R is a ring we don't need to check all the 6 axioms $R1$-$R6$ (of Unit 10) for S. It is enough to check that

i) S is closed under both $+$ and $\cdot$,

ii) $0 \in S$, and

iii) for each $a \in S$, $-a \in S$.

If S satisfies these three conditions, then S is a subring of R. So we have the following alternative definition for a subring.

Definition: Let S be a non-empty subset of a ring $(R, +, \cdot)$. S is called a **subring** of R if

S1) S is closed under $+$ and $\cdot$, i.e., $a + b, a \cdot b \in S$ whenever $a, b \in S$;

S2) $0 \in S$; and

S3) for each $a \in S$, $-a \in S$.

Note that S1-S3, together with Theorem 1 of Unit 3, tells us that a subset S of R is a subring of R if $(S, +) \leq (R, +)$, and $\cdot$ is a binary operation on S.

Let us consider some more examples of subrings now.

Example 1: Let R be a ring. Show that $\{0\}$ and R are subrings of R. (The trivial ring, $\{0\}$, is called the **trivial subring** of R.)

A non-trivial ring has two subrings at least.

Solution: Since $\{0\}$ is closed under $+$ and $\cdot$, and $-0 = 0$, $\{0\}$ satisfies S1-S3 in the definition above. Hence, $\{0\}$ is a subring of R.

Since $(R, +, \cdot)$ is a ring and $R \subseteq R$, R is a subring of R.

***

Example 1 leads us to the following definitions, analogous to those for subgroups.

Definitions: Let R be a ring. A subring S of R is called

i) a **proper subring** if $S \neq R$;

ii) a **non-trivial subring** if $S \neq \{0\}$.

Let us, now, consider some examples of proper non-trivial subrings.

Example 2: Show that $\mathbb{Q}[\sqrt{p}] = \{a + b\sqrt{p} \mid a, b \in \mathbb{Q}\}$ is a subring of $\mathbb{R}$, where p is a square-free integer.

Solution: Firstly, $\mathbb{Q} \subseteq \mathbb{Q}[\sqrt{p}]$. Hence, $\mathbb{Q}[\sqrt{p}] \neq \emptyset$.

Secondly, for $a, b, c, d \in \mathbb{Q}$,

$(a + b\sqrt{p}) + (c + d\sqrt{p}) = (a + c) + \sqrt{p}(b + d) \in \mathbb{Q}[\sqrt{p}]$, and

$(a + b\sqrt{p}) \cdot (c + d\sqrt{p}) = (ac + pbd) + \sqrt{p}(ad + bc) \in \mathbb{Q}[\sqrt{p}]$.

Thus, $\mathbb{Q}[\sqrt{p}]$ satisfies S1.

Next, $0 = 0 + 0\sqrt{p} \in \mathbb{Q}[\sqrt{p}]$, so that $\mathbb{Q}[\sqrt{p}]$ satisfies S2.

Finally, for $a + b\sqrt{p} \in \mathbb{Q}[\sqrt{p}], (-a) + (-b)\sqrt{p} \in \mathbb{Q}[\sqrt{p}]$ s.t.

$(a + b\sqrt{p}) + [(-a) + (-b)\sqrt{p}] = 0$.

Thus, $\mathbb{Q}[\sqrt{p}]$ satisfies S3.

Thus, by the definition, $\mathbb{Q}[\sqrt{p}]$ is a subring of $\mathbb{R}$.

***

Example 3: Check whether or not $C[0,1]$ is a subring of $\mathcal{F}$, the ring of all functions from $[0,1]$ to $\mathbb{R}$ under pointwise addition and multiplication.

Solution: From Example 7, Unit 10, you know that $C[0,1]$ is a ring under pointwise addition and multiplication.
Also $C[0,1] \subseteq \mathcal{F}$.
Hence, $C[0,1]$ is a subring of $\mathcal{F}$.

***

Example 4: Find all the subrings of $\mathbb{Z}$.

Solution: Let S be a subring of $\mathbb{Z}$. Then $(S,+) \leq (\mathbb{Z},+)$.
Hence, from Unit 4, you know that $S = n\mathbb{Z}$, for some $n \in \mathbb{Z}$.
Conversely, from Example 1, Unit 10, you know that $n\mathbb{Z}$ is a subring of $\mathbb{Z}$ $\forall$ $n \in \mathbb{Z}$.
Thus, the only subrings of $\mathbb{Z}$ are $n\mathbb{Z}$, $n \in \mathbb{Z}$.

***

Try solving some exercises now.

E1) Is $(\mathbb{Z}_n, +, \cdot)$ a subring of $\mathbb{Z}$, for $n \geq 2$? Why, or why not?

E2) Show that $\mathbb{Z}[i]$ is a subring of $\mathbb{C}$.

E3) Check whether or not $\mathbb{M}_3(\mathbb{Z})$ is a subring of $\mathbb{M}_3(\mathbb{Q})$.

E4) Is $\mathbb{Z}[x]$, the set of polynomials with coefficients in $\mathbb{Z}$, a subring of $\mathbb{R}[x]$, the ring of real polynomials? Why, or why not?

E5) Give examples to show that the conditions S1 and S3, in the definition of a subring, are necessary. Is S2 necessary? Why, or why not?

The definition of 'subring' requires you to check three conditions for a subset to be a subring. Are all these needed? As you have seen in E5, the requirement S2 follows from S1 and S3. So, can the number of conditions be cut down? This is what we shall discuss now.

11.3 SUBRING TEST

The conditions S1-S3, given in the definition of a subring in the previous section, can be improved upon. For this, recall from Unit 3 that for a non-empty subset S of a ring R, $(S,+) \leq (R,+)$ iff $a - b \in S$ whenever $a, b \in S$.
This observation allows us to cut down the number of conditions for a subset to be a subring. Consider the following theorem.

Theorem 1 (Subring Test): Let S be a non-empty subset of $(R, +, \cdot)$. Then S is a subring of R if and only if

i) $x - y \in S \ \forall \ x, y \in S$; and

ii) $xy \in S \ \forall \ x, y \in S$.

Proof: First, let us assume that S is a subring of R, i.e., S satisfies S1-S3.
Now, if $x, y \in S$, then $x, (-y) \in S$, by S3.
So, $x + (-y) = x - y \in S$, by S1, i.e., (i) is satisfied by S.
Also, (ii) is satisfied by S because of S1.

Conversely, assume that (i) and (ii) are satisfied by S, and let $x, y \in S$.
By (i), $x - x = 0 \in S$. So S satisfies S2.
Again, by (i), $0 - x = -x \in S$. So S satisfies S3.
Also, for $x, y \in S$, $x + y = x - (-y) \in S$, by (i).
Further, by (ii), S is closed under multiplication.
Thus, S satisfies S1, and hence, the definition of a subring.
So, we have proved the theorem. ■

The criteria in Theorem 1 allow us a neat way of checking whether a subset is a subring or not.

Let us look at some examples.

You have already noted that $\mathbb{Z}$ is a subring of $\mathbb{Q}$. In fact, you can use Theorem 1 to check that $\mathbb{Z}$ is a subring of $\mathbb{R}$, $\mathbb{C}$ and $\mathbb{Z}[\sqrt{n}]$ (n not a square, $n \in \mathbb{Z}$). Now for some detailed examples!

Example 5: Show that $3\mathbb{Z}_6$ is a subring of $\mathbb{Z}_6$.

Solution: Firstly, do you agree that $3\mathbb{Z}_6 = \{\bar{0}, \bar{3}\}$? Remember that $3\mathbb{Z}_6 = \{3 \cdot \bar{0}, 3 \cdot \bar{1}, ..., 3 \cdot \bar{5}\}$, and $\bar{6} = \bar{0}, \bar{9} = \bar{3}$, and so on.
Now, $\bar{0} - \bar{3} = -\bar{3} = \bar{3}$.
Thus, $x - y \in 3\mathbb{Z}_6 \ \forall \ x, y \in 3\mathbb{Z}_6$.
You should also verify that $xy \in 3\mathbb{Z}_6 \forall \ x, y \in 3\mathbb{Z}_6$.
Thus, by Theorem 1, $3\mathbb{Z}_6$ is a subring of $\mathbb{Z}_6$.

***

Example 6: Consider the ring $\wp(X)$ (given in Example 5 of Unit 10). Show that $S = \{\phi, X\}$ is a subring of $\wp(X)$.

Solution: Note that $A \Delta A = \phi \ \forall \ A \in \wp(X)$. $\therefore A = -A$ in $\wp(X)$.
Now, to apply Theorem 1, we first note that S is non-empty.
Next, $\phi \Delta \phi = \phi \in S$, $X \Delta X = \phi \in S$, $X \Delta \phi = \phi \Delta X = X \in S$,
$\phi \cap \phi = \phi \in S$, $X \cap X = X \in S$, $\phi \cap X = X \cap \phi = \phi \in S$.
Thus, by Theorem 1, S is a subring of $\wp(X)$.

***

Solving the following exercises will give you some more examples of subrings.

E6) Show that

i) $\mathbb{R}$ is a subring of $\mathbb{C}$,

ii) $\mathbb{Z}[i]$ is a subring of $\mathbb{C}$, and

iii) $\mathbb{Q}[\sqrt{2}]$ is a subring of $\mathbb{R}$.

E7) Let X be a non-empty set, $A \subsetneq X, A \neq \phi$. Show that $S = \{\phi, A, A^c, X\}$ is a subring of $\wp(X)$. Is $\wp(A)$ a subring of $\wp(X)$?

E8) Show that if A is a subring of B, and B is a subring of C, then A is a subring of C. Thus, the relation 'is a subring of', on the set of subrings of a ring, is transitive. Is this relation symmetric? Is it reflexive? Why, or why not?

E9) Check whether or not $R = \left\{ \begin{bmatrix} a & a \\ b & b \end{bmatrix} \middle| a, b \in \mathbb{Z} \right\}$ is a subring of $\mathbb{M}_2(\mathbb{Z})$.

You have already seen that $\mathbb{Z}$ has infinitely many subrings, $n\mathbb{Z}$, $n \in \mathbb{Z}$. Thus, an infinite ring can have infinitely many subrings.
Also, Example 6 and E7 show us that for each proper subset of a set X, we get a proper non-trivial subring of $\wp(X)$. So, if X has n elements, $\wp(X)$ has 2^n elements. For each of these subsets of X, except X, $\wp(X)$ has a proper subring corresponding to it. Thus, a finite ring can have several proper non-trivial subrings.

Let us now consider the behaviour of subrings of a ring with identity.

Example 7: Show that if R is a ring with identity, a subring of R may or may not be with identity.

Solution: Consider $\mathbb{Z}$. It is a ring with identity 1, but its subring $2\mathbb{Z}$ has no multiplicative identity.
On the other hand, you have seen that $\mathbb{Z}$ is a subring of $\mathbb{C}$, and both have the identity 1.

***

Example 8: Must the identity of a subring, if it exists, coincide with the identity of the ring? Why, or why not?

Solution: You know, from E7, that $\wp(A)$ is a subring of $\wp(X)$. You also know, from Example 5, Unit 10, that A and X are the respective identities of $\wp(A)$ and $\wp(X)$.
Hence, if $A \neq X$, as in E7, the two identities will not coincide.

***

Now let us look at an example which generalises the fact that $n\mathbb{Z}$ is a subring of $\mathbb{Z}$ $\forall$ $n \in \mathbb{Z}$.

Example 9: Let R be a ring and $a \in R$. Show that $aR = \{ax \mid x \in R\}$ is a subring of R.

Solution: Since $R \neq \phi, aR \neq \phi$.
Now, for any two elements ax and ay of aR,
$ax - ay = a(x - y) \in aR$, and $(ax)(ay) = a(xay) \in aR$ (since $xay \in R$).
Thus, by Theorem 1, aR is a subring of R.

***

Using Example 9, we can immediately say, for example, that $\overline{m}\mathbb{Z}_n$ is a subring of $\mathbb{Z}_n \; \forall \; \overline{m} \in \mathbb{Z}_n$. Of course, these subrings need not be distinct. For example, $\overline{3}\mathbb{Z}_5 = \mathbb{Z}_5$ and $\overline{2}\mathbb{Z}_6 = \overline{4}\mathbb{Z}_6$.

In the next example you will study a special subring.

Example 10: Let R be a ring, and $C(R) = \{x \in R \,|\, rx = xr \; \forall \; r \in R\}$. Show that $C(R)$ is a subring of R. ($C(R)$ is called the **centre** of R.)

Solution: Firstly, since $0 \in C(R)$, $C(R) \neq \phi$.
Next, for $x, y \in C(R)$ and $r \in R$, $xr = rx$ and $yr = ry$.
So, $r(x - y) = rx - ry = xr - yr = (x - y)r$.
Thus, $x - y \in C(R)$.
Also, $(xy)r = x(yr) = x(ry) = (xr)y = (rx)y = r(xy)$.
Thus, $xy \in C(R)$.
Hence, $C(R)$ is a subring of R.

***

Why don't you solve some related exercises now?

E10) Find all the subrings of $\mathbb{Z}_n$, $n \in \mathbb{N}$. How many of these are with identity?

E11) Check whether or not the following are subrings of $\mathbb{M}_2(\mathbb{R})$:

i) $S = \left\{ \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \middle| \, a, b \in \mathbb{Z} \right\}$,

ii) $T = \left\{ \begin{bmatrix} a & b \\ c & 0 \end{bmatrix} \middle| \, a, b, c \in \mathbb{R} \right\}$.

If they are subrings, do they have unity? If yes, then is the identity the same as that of $\mathbb{M}_2(\mathbb{R})$?

E12) Give an example, with justification, of a subset of a ring R which is a subgroup of $(R, +)$ but not a subring of R.

E13) Which of the following statements are true? Give reasons for your answers.

i) A subring of a commutative ring is commutative.

ii) If R has a subring with identity, then R is with identity.

iii) If R has a commutative subring, then R is commutative.

E14) Find $C(R)$ for $R = \mathbb{Z}$, $R = \mathbb{M}_2(\mathbb{R})$, $R = \mathbb{H}$ (see Example 14, Unit 10).

E15) Let $(R, +, \cdot)$ be a ring. Is the centre of the group $(R, +)$ the same as $C(R)$? Why?

E16) If R is with identity, is $C(R)$ with identity? Why, or why not?

E17) In each of the following cases, check whether or not S is a subring of R.

i) $S = \left\{ \frac{a}{b} \in \mathbb{Q} \middle| 3 \not| b \right\}$, $R = \mathbb{Q}$;

ii) $S = \left\{ \begin{bmatrix} a & 1 \\ 0 & b \end{bmatrix} \middle| a, b \in \mathbb{R} \right\}$, $R = \mathbb{M}_2(\mathbb{R})$.

Let us conclude this section with an important comment.

Remark 3: From Examples 7 and 8, and from E13, you can see that a ring and its subring can have different algebraic structures. A ring may satisfy a property that its subring may not, and vice-versa. You must keep this in mind always when dealing with rings and their subrings.

Let us now consider the behaviour of subrings under operations on the underlying sets of the subrings of a ring.

11.4 SET OPERATIONS ON SUBRINGS

In Unit 3, you found that the intersection of two subgroups of a group is a subgroup. Does the same hold for subrings? Further, is the union of subrings a subring? Is the complement of a subring a subring? The answers to these questions are very similar to the analogous questions for subgroups, as you would expect by now. In this section, we shall focus on the answers to these, and other similar, questions.

Let us begin with the answer to the first question above.

Theorem 2: Let S_1 and S_2 be subrings of a ring R. Then $S_1 \cap S_2$ is also a subring of R.

Proof: Since $0 \in S_1$ and $0 \in S_2$, $0 \in S_1 \cap S_2$. $\therefore S_1 \cap S_2 \neq \phi$.
Now, let $x, y \in S_1 \cap S_2$. Then $x, y \in S_1$ and $x, y \in S_2$.
Thus, by Theorem 1, $x - y$ and xy are in S_1 as well as in S_2, i.e., $x - y$ and xy lie in $S_1 \cap S_2$.

Thus, $S_1 \cap S_2$ is a subring of R. ■

On the same lines as the proof above, you can prove that **the intersection of three, four or more subrings of a ring R is a subring of R.**

Let us consider an example of applying Theorem 2.

Example 11: Show that the intersection of any two subrings of $\mathbb{Z}$ is $r\mathbb{Z}$ for some $r \in \mathbb{Z}$.

Solution: Let $n\mathbb{Z}$ and $m\mathbb{Z}$ be two subrings of $\mathbb{Z}$. Then, by Theorem 2, $n\mathbb{Z} \cap m\mathbb{Z}$ is a subring of $\mathbb{Z}$. Thus, by Example 4, $n\mathbb{Z} \cap m\mathbb{Z} = r\mathbb{Z}$ for some $r \in \mathbb{Z}$. In fact, you should show that r is the l.c.m of n and m, using what you studied in Unit 4.

***

Now consider the union of subrings of a ring. Do you think it will be a subring? Let's see. You must remember that the union of two subgroups need not be a subgroup!

Example 12: Show that $S = 2\mathbb{Z} \cup 3\mathbb{Z}$ is not a subring of $\mathbb{Z}$.

Solution: Note that $2 \in S$ and $3 \in S$. But $2 - 3 = -1 \notin S$, since $(-1) \notin 2\mathbb{Z}$ and $(-1) \notin 3\mathbb{Z}$. Thus, by Theorem 1, S is not a subring of $\mathbb{Z}$.

***

Solve the following related exercises now.

E18) You know that $\mathbb{Z}[i]$ and $\mathbb{Q}$ are subrings of $\mathbb{C}$. Is their union a subring of $\mathbb{C}$? Why, or why not?

E19) Under what conditions on the subrings S_1 and S_2 of R, will $S_1 \cup S_2$ be a subring of R? Give reasons for your answer.

Now let us look at the analogue of the product of two subgroups, for subrings. Remember that a ring is an abelian group.

Example 13: If S and T are subrings of a ring R, is $S + T$ a subring of R? Why, or why not?

Solution: You know that $S + T = T + S$.
Hence, by Theorem 7, Unit 3, $(S + T, +) \leq (R, +)$.
However, $S + T$ need not be closed with respect to multiplication.
For example, consider the sets

$$S = \left\{ \begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix} \middle| a, b \in \mathbb{R} \right\} \text{ and } T = \left\{ \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} \middle| a, b \in \mathbb{R} \right\}.$$

By E5, Unit 10, S and T are subrings of $\mathbb{M}_2(\mathbb{R})$. However,

$$S + T = \left\{ \begin{bmatrix} a & b \\ c & 0 \end{bmatrix} \middle| a, b, c \in \mathbb{R} \right\}$$ is not a subring of $\mathbb{M}_2(\mathbb{R})$, as you have shown in E11(ii).

***

Now let us consider the set operation of complementation. If S_1 and S_2 are subrings of a ring R, is $S_1 \setminus S_2$ a subring of R? Is $S_1 \Delta S_2$ a subring of R? Let us consider an example.

Example 14: If S_1 and S_2 are subrings of a ring R, then show that $S_1 \setminus S_2$ is never a subring of R.

Solution: Since S_2 is a subring, $0 \in S_2$. Hence, $0 \notin S_1 \setminus S_2$.

Hence, $S_1 \setminus S_2$ cannot be a subring of R.

***

Try solving an exercise now.

E20) If S_1 and S_2 are subrings of R, can $S_1 \Delta S_2$ be a subring of R, where Δ denotes the symmetric difference? Why, or why not?

Now let us look at the Cartesian product of subrings. Let us consider two subrings of the ring $\mathbb{Z}^2$.

Example 15: Show that $S = \{(n, 0) \mid n \in \mathbb{Z}\} = \mathbb{Z} \times \{0\}$ is a subring of $\mathbb{Z} \times \mathbb{Z}$. Also show that $D = \{(n, n) \mid n \in \mathbb{Z}\}$ is a subring of $\mathbb{Z} \times \mathbb{Z}$.

Solution: Recall the ring structure of $\mathbb{Z}^2$ from Example 9 of Unit 10.
Both S and D are non-empty.
Also, you should verify that both of them satisfy (i) and (ii) of Theorem 1. Thus, S and D are both subrings of $\mathbb{Z}^2$.

***

You have just seen that $\mathbb{Z} \times \{0\}$ is a subring of $\mathbb{Z} \times \mathbb{Z}$. Also $\{(0, 0)\} = \{0\} \times \{0\}$ is a subring of $\mathbb{Z}^2$. More generally, the following result tells us about **some** subrings of the direct product of rings.

Theorem 3: Let S_1 and S_2 be subrings of the rings R_1 and R_2, respectively. Then $S_1 \times S_2$ is a subring of $R_1 \times R_2$.

Proof: Since S_1 and S_2 are subrings of R_1 and R_2, $S_1 \neq \phi$ and $S_2 \neq \phi$.
$\therefore S_1 \times S_2 \neq \phi$.

Now, let (a, b) and (a', b') be in $S_1 \times S_2$. Then $a, a' \in S_1$ and $b, b' \in S_2$.
As S_1 and S_2 are subrings, $a - a', aa' \in S_1$ and $b - b', bb' \in S_2$.
(We are using $+$ and $\cdot$ for R_1, R_2 and $R_1 \times R_2$ here, for convenience.)
Hence, $(a, b) - (a', b') = (a - a', b - b') \in S_1 \times S_2$.
Also, $(a, b) \cdot (a', b') = (aa', bb') \in S_1 \times S_2$.
Thus, by Theorem 1, $S_1 \times S_2$ is a subring of $R_1 \times R_2$. ■

Theorem 3 can be generalised to the Cartesian product of three or more subrings. However, note that **not every subring of $R_1 \times R_2$ is of the form $S_1 \times S_2$** (see E21).

Let us look at an example of a subring of $R_1 \times R_2$.

Example 16: Show that $\mathbb{Z}[x] \times \mathbb{M}_3(\mathbb{Q})$ is a subring of $\mathbb{R}[x] \times \mathbb{M}_3(\mathbb{R})$. Further, give two distinct elements of this subring.

Solution: First, from E4, you know that $\mathbb{Z}[x]$ is a subring of $\mathbb{R}[x]$.

Next, let us see if $\mathbb{M}_3(\mathbb{Q})$ is a subring of $\mathbb{M}_3(\mathbb{R})$. By E11, Unit 10, you know that $\mathbb{M}_3(\mathbb{Q})$ and $\mathbb{M}_3(\mathbb{R})$ are rings w.r.t. the operations of matrix addition and multiplication. Also, since $\mathbb{Q} \subseteq \mathbb{R}$, $\mathbb{M}_3(\mathbb{Q}) \subseteq \mathbb{M}_3(\mathbb{R})$. So both these sets are rings w.r.t the same binary operations.
Therefore, $\mathbb{M}_3(\mathbb{Q})$ is a subring of $\mathbb{M}_3(\mathbb{R})$.

Thus, $\mathbb{Z}[x] \times \mathbb{M}_3(\mathbb{Q})$ is a subring of $\mathbb{R}[x] \times \mathbb{M}_3(\mathbb{R})$.

This subring is infinite. Two of its elements are $(1, I)$ and $(x, \mathbf{0})$, for example, where I and $\mathbf{0}$ are the multiplicative and additive identities of $\mathbb{M}_3(\mathbb{Q})$.
Note that $(1, I)$ and $(0, I)$ are also distinct elements, since they differ in the first component.

***

Try solving some exercises now.

E21) Obtain two proper non-trivial subrings of $\mathbb{Z} \times \mathbb{R}$.

E22) Use D in Example 15 to show that not every subring of $R_1 \times R_2$ is of the form $S_1 \times S_2$, where S_1 and S_2 are subrings of R_1 and R_2, respectively.

E23) Let R_1 and R_2 be rings, with subrings S_1 and S_2, respectively. Under what conditions on S_1 and S_2 will $S_1 \times S_2$ be a commutative ring with unity?

E24) If X and Y are two non-empty sets, give a proper non-trivial subring of $\wp(X) \times \wp(Y)$.

With this we come to the end of this discussion on subrings. In the next unit, you will study certain special subrings. For now, let us summarise what you have studied in this unit.

11.5 SUMMARY

In this unit, you studied the following points.

1. A subring of a ring R is a non-empty subset S of R such that $(S, +) \leq (R, +)$ and multiplication is closed in S.

2. Several examples, and non-examples, of subrings.

3. A subring of a ring need not have the same algebraic properties of the ring, and vice-versa.

4. The proof, and applications, of the subring test, namely, a non-empty subset S, of a ring R, is a subring of R iff $x - y \in S$ and $xy \in S \ \forall \ x, y \in S$.

5. If S_1 and S_2 are subrings of a ring R, then $S_1 \cap S_2$ is a subring of R. However, $S_1 \cup S_2$ is a subring of R iff $S_1 \subseteq S_2$ or $S_2 \subseteq S_1$. Also, $S_1 \setminus S_2$ and $S_1 \Delta S_2$ are never subrings of R.

6. If S_1 and S_2 are subrings of R_1 and R_2, respectively, then $S_1 \times S_2$ is a subring of $R_1 \times R_2$. Not every subring of $R_1 \times R_2$ is of this form, though.

11.6 SOLUTIONS / ANSWERS

E1) No, since $\mathbb{Z}_n \not\subset \mathbb{Z}$.

E2) For $a + bi,\ c + di \in \mathbb{Z}[i]$,
$(a + bi) + (c + di) = (a + c) + i(b + d) \in \mathbb{Z}[i]$, and
$(a + bi) \cdot (c + di) = (ac - bd) + i(ad + bc) \in \mathbb{Z}[i]$.
Further, $0 = 0 + i0 \in \mathbb{Z}[i]$.
Finally, for $a + ib \in \mathbb{Z}[i]$, $-(a + ib) = (-a) + i(-b) \in \mathbb{Z}[i]$.
Thus, $\mathbb{Z}[i]$ satisfies S1, S2, S3.
Hence, $\mathbb{Z}[i]$ is a subring of $\mathbb{C}$.

E3) By E11, Unit 10, $\mathbb{M}_3(R)$ is a ring w.r.t. matrix addition and matrix multiplication, where $(R, +, \cdot)$ is a ring.
Hence, $\mathbb{M}_3(\mathbb{Z})$ and $\mathbb{M}_3(\mathbb{Q})$ are rings w.r.t. the same operations.
Also, $\mathbb{M}_3(\mathbb{Z}) \subseteq \mathbb{M}_3(\mathbb{Q})$.
Hence, $\mathbb{M}_3(\mathbb{Z})$ is a subring of $\mathbb{M}_3(\mathbb{Q})$.

E4) You should show that if $f(x), g(x) \in \mathbb{Z}[x]$, then $f(x) + g(x)$ and $f(x)g(x)$ are also in $\mathbb{Z}[x]$.
Next, $0 \in \mathbb{Z}[x]$.
Finally, for $f(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Z}[x]$,
$-f(x) = (-a_0) + (-a_1)x + \cdots + (-a_n)x^n \in \mathbb{Z}[x]$.
Hence, $\mathbb{Z}[x]$ is a subring of $\mathbb{R}[x]$.

E5) **S1 is necessary:** Consider $S = \{0, 1, -1\} \subseteq \mathbb{Z}$. This satisfies S2 and S3, but not S1, regarding addition in $\mathbb{Z}$ (e.g., $1 + 1 \notin S$, though $1 \in S$).
Note that $(S, +, \cdot)$ is not a ring, since addition is not a binary operation on S. Thus, S is not a subring of $\mathbb{Z}$.

S3 is necessary: Consider the set of whole numbers, W.
$(W, +, \cdot)$ satisfies S1 and S2, but not S3 (e.g., $1 \in W$ but $(-1) \notin W$).
Note that $(W, +, \cdot)$ is not a subring of $(\mathbb{Z}, +, \cdot)$, since it does not satisfy R4 (of Unit 10), and hence is not a ring.

S2 follows from S1 and S3, taken together. So, if S2 is not included explicitly, it is inbuilt. Hence, it is necessary.

E6) i) Firstly, $\mathbb{R} \subseteq \mathbb{C}$.
Next, $\forall\ x, y \in \mathbb{R}$, $x - y \in \mathbb{R}$ and $xy \in \mathbb{R}$.
Thus, $\mathbb{R}$ is a subring of $\mathbb{C}$.

Similarly, you should check the other two cases.

E7) For any $x, y \in S$,

$x - y = x \Delta (-y) = x \Delta y$ (as pointed out in Example 6), and
$x \cdot y = x \cap y$.
So, you need to check that $x \Delta y \in S$ and $x \cap y \in S$, for each $x, y \in S$.
Once you do this, you will find that S is a subring of $\wp(X)$.
Further, in Unit 3 you have seen that $(\wp(A), \Delta) \leq (\wp(X), \Delta)$.
Also, for $x, y \in \wp(A)$, $x \cdot y = x \cap y \in \wp(A)$.
Thus, $(\wp(A), \Delta, \cap)$ is a subring of $\wp(X)$.

E8) Since A is a subring of B, $A \neq \phi$, and
$\forall\ x, y \in A$, $x - y \in A$ and $xy \in A$.
Here the addition and multiplication are those defined on B. Further, these operations are the same as those defined on C since B is a subring of C. Thus, A satisfies Theorem 1, and hence is a subring of C.

The, relation is not symmetric – e.g., $\mathbb{Z}$ is a subring of $\mathbb{Q}$, but $\mathbb{Q}$ is not a subring of $\mathbb{Z}$.

Since every ring is a subring of itself, the relation is reflexive.

E9) First, note that $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \in R$. So $R \neq \phi$.
Next, for $A = \begin{bmatrix} a & a \\ b & b \end{bmatrix}$, $B = \begin{bmatrix} c & c \\ d & d \end{bmatrix}$ in R,
$A - B = \begin{bmatrix} a-c & a-c \\ b-d & b-d \end{bmatrix} \in R$, and
$AB = \begin{bmatrix} a(c+d) & a(c+d) \\ b(c+d) & b(c+d) \end{bmatrix} \in R$.
Hence, R is a subring of $\mathbb{M}_2(\mathbb{Z})$.

E10) From Example 9, you know that $\overline{m}\mathbb{Z}_n$ is a subring of $\mathbb{Z}_n$ $\forall\ \overline{m} \in \mathbb{Z}_n$.
Also, as in Example 4, you should show that every subring of $\mathbb{Z}_n$ must be of the form $\overline{m}\mathbb{Z}_n$ for some $\overline{m} \in \mathbb{Z}_n$.
Thus, all the subrings of $\mathbb{Z}_n$ are $\overline{m}\mathbb{Z}_n$, $\overline{m} \in \mathbb{Z}_n$.

Further, $\overline{1} \in \overline{m}\mathbb{Z}_n$ iff $1 = mr + ns$ for some $r, s \in \mathbb{Z}$, i.e., iff $(m, n) = 1$, as you know from Unit 1.

E11) i) Firstly, $S \neq \phi$. (Why?)
Secondly, for any $A = \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$ and $C = \begin{bmatrix} c & 0 \\ 0 & d \end{bmatrix}$ in S,
$A - C = \begin{bmatrix} a-c & 0 \\ 0 & b-d \end{bmatrix} \in S$ and $AC = \begin{bmatrix} ac & 0 \\ 0 & bd \end{bmatrix} \in S$.
Thus, S is a subring of R.
The unity of $S = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ = the unity of R.

ii) Verify that $T \neq \emptyset$. Now, $\begin{bmatrix} 1 & 2 \\ 3 & 0 \end{bmatrix}$ and $\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \in T$. But,

$\begin{bmatrix} 1 & 2 \\ 3 & 0 \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 3 & 1 \\ 3 & 3 \end{bmatrix} \notin T$, since it does not have 0 in the $(2, 2)$th place. Thus, T is not a subring of $\mathbb{M}_2(\mathbb{R})$.

E12) Consider T in E11(ii). Check that $(T, +) \leq \mathbb{M}_2(\mathbb{R})$.
However, as given in the solution, T is not a subring of $\mathbb{M}_2(\mathbb{R})$.
You can think of many other examples.

E13) i) This is true, since the operation of multiplication on the subring is the same as that on the ring.

ii) No. For example, the trivial ring has identity, and is a subring of $2\mathbb{Z}$, which does not have identity.

iii) No. For instance, the subring S in E11(i) is commutative, but $\mathbb{M}_2(\mathbb{R})$ is not.

E14) $C(\mathbb{Z}) = \{z \in \mathbb{Z} \mid zx = xz \ \forall \ x \in \mathbb{Z}\}$
$= \mathbb{Z}$, since $\mathbb{Z}$ is commutative.

$C(\mathbb{M}_2(\mathbb{R})) = \{A \in \mathbb{M}_2(\mathbb{R}) \mid AB = BA \ \forall \ B \in \mathbb{M}_2(\mathbb{R})\}$.

Now, for any $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in C(\mathbb{M}_2(\mathbb{R}))$, and $\alpha, \beta \in \mathbb{R}, \alpha \neq \beta$,

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} \alpha & 0 \\ 0 & \beta \end{bmatrix} = \begin{bmatrix} \alpha & 0 \\ 0 & \beta \end{bmatrix}\begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

$$\Rightarrow \begin{bmatrix} a\alpha & b\beta \\ c\alpha & d\beta \end{bmatrix} = \begin{bmatrix} a\alpha & b\alpha \\ c\beta & d\beta \end{bmatrix}$$

$\Rightarrow b\beta = b\alpha, \ c\alpha = c\beta.$

$\Rightarrow b = 0, c = 0,$ since $\alpha \neq \beta$.

Now, since $\begin{bmatrix} a & 0 \\ 0 & d \end{bmatrix} \in C(\mathbb{M}_2(\mathbb{R}))$, it must commute with $\begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}$.

This gives $\begin{bmatrix} a & 0 \\ d & 0 \end{bmatrix} = \begin{bmatrix} a & 0 \\ a & 0 \end{bmatrix}$. So $a = d$.

Finally, for any $\begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix}$, $a \in \mathbb{R}$,

$$\begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix}\begin{bmatrix} b & c \\ d & r \end{bmatrix} = \begin{bmatrix} b & c \\ d & r \end{bmatrix}\begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix}, \text{ for } \begin{bmatrix} b & c \\ d & r \end{bmatrix} \in \mathbb{M}_2(\mathbb{R}).$$

$\begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix}$, $a \in \mathbb{R}$, is called a **scalar matrix over $\mathbb{R}$.**

Thus, $C(\mathbb{M}_2(\mathbb{R})) = \left\{\begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} \middle| a \in \mathbb{R}\right\} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}\mathbb{R}$, the ring of scalar matrices in $\mathbb{M}_2(\mathbb{R})$.

Since i, j, k do not commute with $j, k, i,$ respectively,
$a + ib + jc + kd \in C(\mathbb{H})$ iff $b = c = d = 0$.
Further, for any $a, b, c, d, r \in \mathbb{R}$,

$r(a+ib+jc+kd) = (a+ib+jc+kd)r.$
So $C(\mathbb{H}) = \mathbb{R}$.

E15) No. Since $(R, +)$ is abelian, you know from Unit 6 that $Z(R) = R$.
However, as you have seen in E14, $C(R) \neq R$ for all non-commutative rings R.

E16) For any $r \in R$, $1 \cdot r = r = r \cdot 1$. Thus, $1 \in C(R)$. Hence, $C(R)$ is with identity.

E17) i) Firstly, $S \subseteq \mathbb{Q}$ and $S \neq \emptyset$.

Next, for $\frac{a}{b}, \frac{c}{d} \in S$, $\frac{a}{b} - \frac{c}{d} \in S$ and $\frac{a}{b} \cdot \frac{c}{d} \in S$, since $3 \not| bd$.
Thus, S is a subring of R.

ii) Note that $\mathbf{0} \notin S$, since $\mathbf{0}$ doesn't have 1 in the $(1, 2)$th place.
Hence, S is not a subring of R.

E18) $1+i$ and $\frac{1}{2}$ are elements of the union.

But $1+i-\frac{1}{2} = \frac{1}{2}+i \notin \mathbb{Z}[i] \cup \mathbb{Q}$. Thus, $\mathbb{Z}[i] \cup \mathbb{Q}$ is not a subring of $\mathbb{C}$.

E19) Firstly, $S_1 \cup S_2$ is a subgroup of $(R, +)$ iff $S_1 \subseteq S_2$ or $S_2 \subseteq S_1$.
Once this condition is satisfied, multiplication will be closed on $S_1 \cup S_2$, by definition.
Thus, $S_1 \cup S_2$ is a subring of R iff $S_1 \subseteq S_2$ or $S_2 \subseteq S_1$.

E20) $S_1 \Delta S_2 = (S_1 \setminus S_2) \cup (S_2 \setminus S_1)$.
Since neither $S_1 \setminus S_2$ nor $S_2 \setminus S_1$ has 0, $0 \notin S_1 \Delta S_2$.
Hence, $S_1 \Delta S_2$ is never a subring of R.

E21) Since $n\mathbb{Z}$ is a subring of $\mathbb{Z}$ $\forall$ $n \in \mathbb{Z}$, and $\{0\}$ and $\mathbb{R}$ are subrings of $\mathbb{R}$, $2\mathbb{Z} \times \mathbb{R}$, $3\mathbb{Z} \times \{0\}$ are two subrings of $\mathbb{Z} \times \mathbb{R}$. You can find infinitely many examples.

E22) Consider the subring $D = \{(n, n) \mid n \in \mathbb{Z}\}$, of $\mathbb{Z} \times \mathbb{Z}$.
Suppose D is of the form $S_1 \times S_2$, where S_1, S_2 are subrings of $\mathbb{Z}$.
So $S_1 = m\mathbb{Z}$, $S_2 = s\mathbb{Z}$ for some $m, s \in \mathbb{Z}$.
Now any element of D is of the form (a, b), with $a \in S_1$ and $b \in S_2$.
So $a = mm_1$, $b = ss_1$ for some $m_1, s_1 \in \mathbb{Z}$.
As $(a, b) \in D$, $(a, b) = (n, n)$ for some $n \in \mathbb{Z}$, i.e., $(mm_1, ss_1) = (n, n)$.
So $mm_1 = n = ss_1$, i.e., $m \mid n, s \mid n$. This is true for each $n \in \mathbb{Z}$.
Thus, by E29, Unit 10, $m = \pm 1$, $s = \pm 1$.
Hence, $S_1 = \mathbb{Z} = S_2$, i.e., $D = \mathbb{Z} \times \mathbb{Z}$.
But then $\mathbb{Z} \times \mathbb{Z}$ has elements like $(1, 2)$ also, which is not in D. So we reach a contradiction. Thus, our assumption must be wrong.
Thus, $D \neq S_1 \times S_2$.

E23) $S_1 \times S_2$ will be commutative iff both S_1 and S_2 are commutative, by Example 13, Unit 10.
Similarly, $S_1 \times S_2$ has unity iff both S_1 and S_2 have unity, again by Example 13, Unit 10.

E24) $\{\phi\} \times \wp(Y)$ is an example.
This is a subring since $\{\phi\}$ is a subring of $\wp(X)$ and $\wp(Y)$ is a subring of $\wp(Y)$.
This is proper, since $\{\phi\} \subsetneq \wp(X)$.
This is non-trivial, since $\wp(Y) \neq \{\phi\}$.

UNIT 12

IDEALS

Structure | Page Nos.

12.1 INTRODUCTION

You have seen that a subring S of a ring R is a subgroup of $(R, +)$. From Unit 6, you also know that $(S, +)$ is a normal subgroup of $(R, +)$, since $+$ is commutative. Can this 'normality' be extended to both the operations, in some sense? In other words, is there a concept like a normal subring?
Recall that Galois had invented the concept of a normal subgroup in the context of defining a quotient group. So the questions that arise are – Is there a concept in ring theory analogous to that of

i) a quotient group?

ii) a normal subgroup?

Both these questions are considered in this unit.

In Sec.12.2, you will study the analogue, in ring theory, of a normal subgroup. This is the concept of 'an ideal'. You will study several examples of ideals also in this section.

In Sec.12.3, the focus will be on elementary properties of ideals. You will find out if the intersection, union or product of ideals is an ideal or not.

Finally, in Sec.12.4, you will study the analogue, in ring theory, of a quotient group. To understand the discussion here, it may be a good idea to re-look Unit 7 before studying this section.

Our discussion in this unit will be built around the following learning expectations. Please go through the unit carefully, so that you achieve these objectives.

Objectives

After studying this unit, you should be able to:

- define, and give examples of, an ideal of a ring;
- decide whether a subset of a ring is an ideal or not;
- prove, and apply, basic properties of ideals of a ring;
- define, and give examples of, a quotient ring;
- prove, and apply, some elementary properties of quotient rings.

12.2 WHAT IS AN IDEAL?

Fig.1: Dedekind (1831-1916)

In Block 2, you studied normal subgroups and the role that they play in group theory. You saw that the most important reason for the creation of normal subgroups is that they allow us to define quotient groups. In ring theory, we would like to define an analogous concept, namely, a quotient ring. In this section, you will study about a class of subrings that will help us to do so. While exploring algebraic number theory, the 19th century mathematicians Dedekind, Kronecker and others developed this concept.

Let us first consider what kind of properties a subring needs so that we can define a corresponding quotient ring.
Let us being by considering $\mathbb{Z}$. You know that this is a subring of $\mathbb{R}$. So, $(\mathbb{Z}, +) \leq (\mathbb{R}, +)$. Hence, $\mathbb{Z} \lhd \mathbb{R}$. So, $\mathbb{R}/\mathbb{Z}$ is a well-defined quotient group. Is it also a ring? Let's see.
As in Unit 7, if multiplication were defined on $\mathbb{R}/\mathbb{Z}$, then we should have $(r + \mathbb{Z}) \cdot (s + \mathbb{Z}) = rs + \mathbb{Z} \ \forall \ r, s \in \mathbb{R}$.
So, let us see if this operation is well-defined.
Firstly, you know that $\forall \ n \in \mathbb{Z}, \ n + \mathbb{Z} = \mathbb{Z}$. So $1 + \mathbb{Z} = 0 + \mathbb{Z} = \mathbb{Z}$.

Therefore, $\left(\frac{1}{5} + \mathbb{Z}\right)(1 + \mathbb{Z}) = \left(\frac{1}{5} + \mathbb{Z}\right)(0 + \mathbb{Z})$.

Thus, $\left(\frac{1}{5} \cdot 1\right) + \mathbb{Z} = \left(\frac{1}{5} \cdot 0\right) + \mathbb{Z}$, i.e., $\frac{1}{5} + \mathbb{Z} = 0 + \mathbb{Z} = \mathbb{Z}$.

So, $\frac{1}{5} \in \mathbb{Z}$, which is not true.

So we conclude that this multiplication is not well-defined in $\mathbb{R}/\mathbb{Z}$.

On the other hand, let's see what happens if we consider the subring $6\mathbb{Z}$ of $\mathbb{Z}$. Is the elementwise multiplication well-defined in $\mathbb{Z}/6\mathbb{Z}$? Let's see.
Let $r + 6\mathbb{Z} = s + 6\mathbb{Z}$ and $m + 6\mathbb{Z} = n + 6\mathbb{Z}$, where $r, s, m, n \in \mathbb{Z}$.
Then $r - s \in 6\mathbb{Z}, \ m - n \in 6\mathbb{Z}$. Let $r - s = 6t, \ m - n = 6u$, for $t, u \in \mathbb{Z}$. Then

$$\begin{aligned}(r + 6\mathbb{Z})(m + 6\mathbb{Z}) &= rm + 6\mathbb{Z} = (s + 6t)(n + 6u) + 6\mathbb{Z} \\ &= sn + 6(nt + su + 6ut) + 6\mathbb{Z} \\ &= sn + 6\mathbb{Z}, \text{ since } nt + su + 6ut \in \mathbb{Z}. \\ &= (s + 6\mathbb{Z})(n + 6\mathbb{Z}).\end{aligned}$$

Thus, the multiplication in $\mathbb{Z}/6\mathbb{Z}$ is well-defined.

Also, you should verify that, this multiplication is associative, using the fact that multiplication in $\mathbb{Z}$ is associative.

Finally, for $r, s, t \in \mathbb{Z}$,

$$(r + 6\mathbb{Z})[(s + 6\mathbb{Z}) + (t + 6\mathbb{Z})] = r(s + t) + 6\mathbb{Z}$$
$$= (rs + 6\mathbb{Z}) + (rt + 6\mathbb{Z})$$
$$= (r + 6\mathbb{Z})(s + 6\mathbb{Z}) + (r + 6\mathbb{Z})(t + 6\mathbb{Z}).$$

Thus, multiplication is distributive over addition in $\mathbb{Z}/6\mathbb{Z}$.
So, in this case, it seems we get a quotient group which is also a ring.

What was it about the subring $6\mathbb{Z}$ in $\mathbb{Z}$, that the subring $\mathbb{Z}$ in $\mathbb{R}$ didn't have? Notice that for $t \in \mathbb{Z}$ and $6n \in 6\mathbb{Z}$, $6nt \in 6\mathbb{Z}$ also. However, for $n \in \mathbb{Z}$ and $r \in \mathbb{R}$, rn need not be in $\mathbb{Z}$. It turns out that it is this property that makes all the difference, as you will see in the detailed discussion on quotient rings in Sec.12.4. For now, we will focus on subrings with the property that you have just seen. Let us begin with defining such a subring.

Definition: A subring I of a ring $(R, +, \cdot)$ is called an **ideal** of R if $ar \in I$ and $ra \in I$ for all $r \in R$ and $a \in I$.

If you study advanced ring theory, you will find that non-commutative rings have left ideals and right ideals too.

For example, as you have seen earlier in this discussion, $6\mathbb{Z}$ is an ideal of $\mathbb{Z}$, but $\mathbb{Z}$ is not an ideal of $\mathbb{R}$.

Note that, if R is a commutative ring, then the second requirement in the definition above is not needed, as $ar \in I \Rightarrow ra \in I \ \forall\ a \in I, r \in R$.

So, from the definition above, you know that **ideals are defined for any ring**. However, henceforth in this unit, **we will always assume that the rings we deal with are commutative**, **unless mentioned otherwise**. This is being done to help you get used to the concept.

Now, from the definition you know that every ideal is a subring. Is the converse true? Here is a remark about this.

Remark 1: You know that every subgroup of a commutative group is a normal subgroup. However, every subring of a commutative ring need not be an ideal. For instance, $\mathbb{R}$ is commutative, $\mathbb{Z}$ is a subring of $\mathbb{R}$, but $\mathbb{Z}$ is not an ideal of $\mathbb{R}$, as you have seen above.

Now, let us look at some examples of ideals.

Example 1: Every ring R, whether commutative or not, has at least two ideals, $\{0\}$ and R. ($\{0\}$ is called the **trivial ideal** of R.)

Solution: You have seen, in Example 1 of Unit 11, that R and $\{0\}$ are subrings of R.
Now, for any $r \in R$, $r \cdot 0 = 0 \in \{0\}$, and $0 \cdot r = 0 \in \{0\}$.
Hence, $\{0\}$ is an ideal of R.

Next, for any $r \in R$, $r \cdot s = rs \in R$ and $s \cdot r = sr \in R \ \forall\ s \in R$.
Thus, R satisfies the requirement for being an ideal.

***

Example 1 leads us to the following definition.

Definition: If an ideal I of a ring R is such that $I \neq R$, then I is called a **proper ideal** of R. Further, if $I \neq \{0\}$, I is called a **non-trivial ideal** of R.

Let us consider some proper non-trivial ideals now. You have earlier seen that $6\mathbb{Z}$ is an ideal of $\mathbb{Z}$. We generalise this in the following example.

Example 2: Show that if $n \neq 0, \pm 1$, then the subring $n\mathbb{Z}$ is a proper non-trivial ideal of $\mathbb{Z}$. Further, these are the only such ideals of $\mathbb{Z}$.

Solution: From Example 4, Unit 11, you know that $n\mathbb{Z}$ is a proper non-trivial subring of $\mathbb{Z}$ if $n \neq 0, \pm 1$.
Also, for any $z \in \mathbb{Z}$ and $nm \in n\mathbb{Z}$, $z(nm) = n(zm) \in n\mathbb{Z}$.
Hence, $n\mathbb{Z}$ is an ideal of $\mathbb{Z}$, $n\mathbb{Z} \neq \{0\}$ and $n\mathbb{Z} \neq \mathbb{Z}$.

Now, every ideal is a subring. From Example 4, Unit 11, you also know that the only subrings of $\mathbb{Z}$ are of the form $n\mathbb{Z}$, $n \in \mathbb{Z}$. Hence, the only ideals of $\mathbb{Z}$ are of the form $n\mathbb{Z}$, $n \in \mathbb{Z}$. Thus, the only proper non-trivial ideals of $\mathbb{Z}$ are $n\mathbb{Z}$, $n \neq 0, 1, -1$.

***

Example 3: Check whether or not $\mathbb{Q}[\sqrt{p}]$ is an ideal of $\mathbb{R}$, where p is a prime.

Solution: From Example 2, Unit 11, you know that $\mathbb{Q}[\sqrt{p}]$ is a subring of $\mathbb{R}$.
Now, consider $\pi \in \mathbb{R}$. Then, for $a, b \in \mathbb{Q}$,
$\pi(a + b\sqrt{p}) = \pi a + \pi b\sqrt{p} \notin \mathbb{Q}[\sqrt{p}]$, since $\pi a \notin \mathbb{Q}$.
Hence, $\mathbb{Q}[\sqrt{p}]$ is not an ideal of $\mathbb{R}$.

***

Why don't you solve some exercises now?

E1) Find a non-trivial proper ideal of the ring of functions from $[-3, 3]$ to $\mathbb{R}$ w.r.t. pointwise addition and multiplication.

E2) Is $\mathbb{Q}[\sqrt{10}]$ an ideal of $\mathbb{C}$? Why, or why not?

E3) Check whether or not

i) $\mathbb{Z}[i]$ is a proper ideal of $\mathbb{C}$,

ii) $\mathbb{R}[x]$ is an ideal of $\mathbb{C}[x]$,

iii) $\{\bar{0}, \bar{3}\}$ and $\{\bar{0}, \bar{2}, \bar{4}\}$ are proper ideals of $\mathbb{Z}_6$.

Now, from Sec.11.3, Unit 11, you know that there are criteria to decide whether a given subset of a ring is a subring or not. Can we use these to develop criteria for testing if a subset is an ideal or not? Consider the following result about this.

Theorem 1 (Ideal Test): A non-empty subset I, of a ring R (not necessarily commutative), is an ideal of R if and only if

i) $a - b \in I \ \forall \ a, b \in I$, and

ii) $ar \in I$ and $ra \in I \ \forall\ a \in I, r \in R$.

Proof: First, let I be an ideal of R. Then I is a subring of R. Thus, by the subring test, $a - b \in I \ \forall\ a, b \in I$. Hence, (i) is true.
Further, (ii) above is true, by definition.

Conversely, assume (i) and (ii) are true for I.
Then $a - b \in I$ and $ab \in I \ \forall\ a, b \in I$.
Hence, I is a subring of R.
Further, because of (ii), I satisfies the conditions in the definition of an ideal of R.
Thus, I is an ideal of R. ■

Note that if R is a commutative ring, then the condition (ii) in the ideal test reduces to '$ar \in I \ \forall\ a \in I, r \in R$'.

Let us apply this test in some cases.

Example 4: Let $S = \{a + 2bi \mid a, b \in \mathbb{Z}\}$, where $i = \sqrt{-1}$. Show that S is a subring of $\mathbb{Z}[i]$. Is S an ideal of $\mathbb{Z}[i]$? Why, or why not?

Solution: First, $2i \in S$. So, $S \neq \phi$.
Next, for $a + 2bi,\ c + 2di$ in S,
$(a + 2bi) - (c + 2di) = (a - c) + 2(b - d)i \in S$, and
$(a + 2bi)(c + 2di) = (ac - 4bd) + 2(bc + ad)i \in S$.
Thus, S is a subring of $\mathbb{Z}[i]$.

However, $ar \notin S \ \forall\ a \in S$ and $r \in \mathbb{Z}[i]$. For instance, $1 = 1 + 2 \cdot 0 \cdot i \in S$ and $i \in \mathbb{Z}[i]$ such that $1 \cdot i = i \notin S$.
Thus, S is not an ideal of $\mathbb{Z}[i]$.

***

Example 5: Let X be an infinite set. Consider I, the set of all finite subsets of X. Is I an ideal of $(\wp(X), \Delta, \cap)$? Why, or why not?

Solution: $I = \{A \mid A$ is a finite subset of $X\}$. Note that

i) $\phi \in I$, i.e., the zero element of $\wp(X)$ is in I. So $I \neq \phi$.

ii) For $A, B \in \wp(X)$, $A - B = A \Delta (-B)$
$= A \Delta B$, as $B = -B$ in $\wp(X)$.

iii) For $A, B \in \wp(X)$, $AB = A \cap B$.

Thus, if $A, B \in I$, then $A - B$ is again a finite subset of X, and hence $A - B \in I$.

Next, whenever A is a finite subset of X and B is any subset of X, $A \cap B \subseteq A$. Hence, $A \cap B$ is a finite subset of X.
Thus, if $A \in I$ and $B \in \wp(X)$, then $AB \in I$.

Hence, by the ideal test, I is an ideal of $\wp(X)$.

***

If X is an infinite set, $\wp(X)$ has infinitely many distinct ideals.

Example 6: Let X be a non-empty set and Y be a non-empty proper subset of X. Show that $I = \{A \in \wp(X) \mid A \cap Y = \phi\}$ is an ideal of $\wp(X)$.

In particular, if $Y = \{x_0\}$, where $\{x_0\} \subsetneq X$, then $I = \{A \in \wp(X) \mid x_0 \notin A\}$ is an ideal of $\wp(X)$.

Solution: Firstly, note that $I = \wp(Y^c)$, and $Y^c \neq \phi$. Thus, $I \neq \phi$.

Secondly, $\forall\ A, B \in I$,

$$\begin{aligned}(A - B) \cap Y &= (A \Delta B) \cap Y \\ &= (A \cap Y) \Delta (B \cap Y) = \phi \Delta \phi \\ &= \phi.\end{aligned}$$

Thus, $A - B \in I$.

Finally, for $A \in I$ and $B \in \wp(X)$,

$$(AB) \cap Y = (A \cap B) \cap Y = (B \cap A) \cap Y = B \cap (A \cap Y) = B \cap \phi = \phi.$$

Thus, $AB \in I$.

Thus, by Theorem 1, I is an ideal of $\wp(X)$.

***

Now consider an example which will be used in the rest of the units several times.

Example 7: Consider the ring $C[0,1]$, given in Example 7, Unit 10. Let $M = \{f \in C[0,1] \mid f(1/2) = 0\}$. Show that M is an ideal of $C[0,1]$.

Solution: The zero element $\mathbf{0}$ is defined by $\mathbf{0}(x) = 0$ for all $x \in [0, 1]$. Since $0(1/2) = 0$, $0 \in M$. Thus, $M \neq \phi$.

Also, if $f, g \in M$, then $f - g \in C[0, 1]$, and

$$(f - g)(1/2) = f(1/2) - g(1/2) = 0 - 0 = 0.$$

So, $f - g \in M$.

Next, if $f \in M$ and $g \in C[0, 1]$, then you know that $f \cdot g \in C[0, 1]$.

Also, $(fg)(1/2) = f(1/2)g(1/2) = 0 \cdot g(1/2) = 0$.

So $fg \in M$.

Thus, by Theorem 1, M is an ideal of $C[0, 1]$.

***

Now it is time for you to solve some exercises.

$C[a, b]$ has infinitely many ideals, for any closed interval $[a, b]$ in $\mathbb{R}$.

E4) Let us generalise Example 7.

i) Let $a \in [0,1]$. Show that $I_a = \{f \in C[0,1] \mid f(a) = 0\}$ is an ideal of $C[0, 1]$.

ii) For any interval $[a, b]$ in $\mathbb{R}$ and $r \in [a, b]$, show that $I_r = \{f \in C[a, b] \mid f(r) = 0\}$ is an ideal of $C[a, b]$.

iii) For $r \in [0, 1]$, is $J_r = \{f \in C[0, 1] \mid f(r) = 1\}$ an ideal of $C[0, 1]$? Why, or why not?

E5) Check whether or not $C(R)$, the centre of R, is an ideal of R.

E6) Check whether or not the following are ideals of $\mathbb{Z}[x]$:

i) The set of all polynomials over $\mathbb{Z}$ with constant term 0,

ii) $S = \left\{ \sum_{i=0}^{n} a_i x^i \;\middle|\; a_i \in 3\mathbb{Z} \;\forall\; i = 0, 1, \ldots, n \right\}$.

E7) Let R be a ring and $a \in R$. Show that Ra is an ideal of R. (Ra is called the **principal ideal** of R generated by $a \in R$.)
(Remember that R is a commutative ring!)

E8) Let R be a ring and $a, b \in R$. Show that $I = \{x \in R \mid ax \in bR\}$ is an ideal of R.

Now that you've solved E7, do you see the connection with E3(iii) and E6(i)? Note that the set in E6(i) is simply $x\mathbb{Z}[x]$.

Let us now see how we can generalise what you have proved in E7.

Example 8: For any ring R and $a_1, a_2 \in R$, show that
$Ra_1 + Ra_2 = \{x_1a_1 + x_2a_2 \mid x_1, x_2 \in R\}$ is an ideal of R.

If R is not commutative, $Ra_1 + Ra_2$ is not an ideal of R.

Solution: Firstly, $0 = 0a_1 + 0a_2$. $\therefore 0 \in Ra_1 + Ra_2$.
So, $Ra_1 + Ra_2 \neq \emptyset$.

Next, $\forall\; x_1, x_2, y_1, y_2 \in R$,
$(x_1a_1 + x_2a_2) - (y_1a_1 + y_2a_2) = (x_1 - y_1)a_1 + (x_2 - y_2)a_2 \in Ra_1 + Ra_2$.

Finally, for $r \in R$ and $x_1a_1 + x_2a_2 \in Ra_1 + Ra_2$,
$r(x_1a_1 + x_2a_2) = rx_1a_1 + rx_2a_2 \in Ra_1 + Ra_2$, since $rx_1 \in R$, $rx_2 \in R$.

Thus, by Theorem 1, $Ra_1 + Ra_2$ is an ideal of R.

***

The method of obtaining ideals in Example 8 can be extended to give ideals of the form $\{x_1a_1 + x_2a_2 + \ldots + x_na_n \mid x_i \in R\}$, for fixed elements $a_1, \ldots, a_n$ of R, for any $n \in \mathbb{N}$. Such ideals crop up again and again in ring theory. They have a special name, linked to what you studied in Sec.4.4, Unit 4.

Definition: Let $a_1, \ldots, a_n$ be given elements of a ring R, for $n \in \mathbb{N}$. Then **the ideal of R generated by $a_1, \ldots, a_n$** is
$Ra_1 + Ra_2 + \cdots + Ra_n = \{x_1a_1 + x_2a_2 + \cdots + x_na_n \mid x_i \in R\}$.

The elements $a_1, \ldots, a_n$ are called the **generators** of this ideal. We also denote this ideal by $< \mathbf{a_1, a_2, \ldots, a_n} >$.

When $n = 1$, the ideal we get is the one in E7, called a **principal ideal**. Thus, if $a \in R$, then $\mathbf{Ra} = < \mathbf{a} >$ is a principal ideal of R. In the next block, you will be working with principal ideals quite a bit.
Do you see the connection between the concepts of a principal ideal and a cyclic group? Aren't they the same if the ring is $\mathbb{Z}$? In this context, consider the following remark.

Remark 2: From Example 2, you can see that every ideal of $\mathbb{Z}$ is a principal ideal.

Now, some exercises on ideals and generators.

E9) Let R be a ring with identity. Show that $< 1 > = R$. If $u \in U(R)$, find $< u >$.

E10) Let R be a ring and $r \in R$. Find the cyclic subgroup of R generated by r. Is this the same as the principal ideal of R generated by r? Why, or why not?

E11) Find the principal ideals of $\mathbb{Z}_{10}$ generated by $\overline{3}$, and by $\overline{5}$, respectively. Also find $< \overline{2}, \overline{3} >$, and see if it is $< \overline{5} >$ or not.

E12) Show that every ideal of $\mathbb{Z}_n$, $n \in \mathbb{N}$, is a principal ideal.

E13) Let X be an infinite set, and let A be a proper non-empty subset of X. Show that the principal ideal $\wp(X)A$ is $\wp(A)$.

Let us now look at a special ideal of a ring. But, to do so, we first need to give a definition.

Definition: An element a of a ring R is called **nilpotent** if there exists a positive integer n such that $a^n = 0$.

For example, $\overline{3}$ and $\overline{6}$ are nilpotent elements of $\mathbb{Z}_9$, since $\overline{3}^2 = \overline{9} = \overline{0}$ and $\overline{6}^2 = \overline{36} = \overline{0}$.

Also, **in any ring $\mathbf{R}$, $\mathbf{0}$ is a nilpotent element**.

Now consider the following example.

Example 9: Let R be a ring. Show that the set of nilpotent elements of R is an ideal of R. (This ideal is called the **nil radical** of R.)

Solution: Let N be the set of nilpotent elements of R, i.e.,
$N = \{a \in R \mid a^n = 0$ for some positive integer $n\}$.
Also $0 \in N$. So, $N \neq \emptyset$.

Next, if $a, b \in N$, then $a^n = 0$ and $b^m = 0$ for some positive integers m and n.
Now, from E16 of Unit 10, you know that

$$(a-b)^{m+n} = \sum_{r=0}^{m+n} {}^{m+n}C_r a^r (-b)^{m+n-r}.$$

Note that, for each $r = 0, 1, \ldots, m+n$, either $r \geq n$ or $m+n-r \geq m$. Therefore, either $a^r = 0$ or $b^{m+n-r} = 0$.
Thus, the term $a^r b^{m+n-r} = 0$, for each r.
So, $(a-b)^{m+n} = 0$.
Thus, $a - b \in N$ whenever $a, b \in N$.

Finally, if $a \in N$, $a^n = 0$ for some positive integer n. So, for any $r \in R$,
$(ar)^n = a^n r^n$, since R is commutative.
$= 0$,
i.e., $ar \in N$.

Thus, N is an ideal of R.

***

Let us see what the nil radicals of some familiar rings are.
For the rings $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ or $\mathbb{C}$, $N = \{0\}$, since any positive power of any non-zero element of these rings is non-zero.

For $\mathbb{Z}_4$, $N = \{\bar{0}, \bar{2}\}$, since $\bar{1}^n = \bar{1}$, and $\bar{3}^n$ is $\bar{1}$ or $\bar{3}$ $\forall$ $n \in \mathbb{N}$.

Now, if R is a ring and $a \in R$, there is an ideal of R associated with a. We define it, and ask you to prove that it is an ideal, in one of the following exercises (see E15).

E14) Find the nil radicals of $\mathbb{Z}_8$ and $\wp(X)$, where X is a non-empty set.

E15) Let R be a ring and $a \in R$. Show that $\mathbf{Ann\ a} = \{r \in R \mid ra = 0\}$ is an ideal of R. (This ideal is called the **annihilator** of a.)
What is the annihilator of $0 \in R$? If R is with unity, what is the annihilator of $1 \in R$?

E16) Which of the following statements are true? Justify your answers.

i) $\text{Ann } a$ is a proper non-trivial ideal of R, where R is a non-trivial ring and $a \in R$.

ii) If R is a ring and $a, b \in R$ s.t. $\text{Ann } a = \text{Ann } b$, then $a = b$.

iii) If R and S are rings with the same nil radicals, then $R = S$.

By now you must be familiar with the concept of an ideal. Let us now discuss some basic properties of ideals.

12.3 PROPERTIES OF IDEALS

In this section, we shall look at several interesting aspects of ideals. We shall also discuss set operations on ideals.

Let us begin with a property that you may have got an indication about in E9. Consider all the ideals of $\mathbb{Z}$. They are given in Example 2. None of the proper ideals contain 1. Is this true only for $\mathbb{Z}$? Not so, as the following theorem will tell you.

Theorem 2: Let R be a ring with identity 1. If I is an ideal of R and $1 \in I$, then $I = R$.

Proof: You know that $I \subseteq R$. We want to prove that $R \subseteq I$.
Let $r \in R$. Since $1 \in I$ and I is an ideal of R, $r = r \cdot 1 \in I$. So, $R \subseteq I$.
Hence, $I = R$. ■

Using this result, we can immediately say that $\mathbb{Z}$ is not an ideal of $\mathbb{Q}$. How? Well, if $\mathbb{Z}$ were an ideal of $\mathbb{Q}$, wouldn't Theorem 2 imply that $\mathbb{Z} = \mathbb{Q}$? And this is not true. So, $\mathbb{Z}$ couldn't be an ideal of $\mathbb{Q}$.

Does this also tell us whether $\mathbb{Q}$ is an ideal of $\mathbb{R}$ or not? It does. Since $1 \in \mathbb{Q}$ and $\mathbb{Q} \neq \mathbb{R}$, $\mathbb{Q}$ can't be an ideal of $\mathbb{R}$.

Another important application of Theorem 2 is the following.

Example 10: Find all the ideals of $\mathbb{Q}$.

Solution: As you know, two ideals are $\{0\}$ and $\mathbb{Q}$. Are there any others? Let's find out.
Let $I \neq \{0\}$ be an ideal of $\mathbb{Q}$. Then $\exists\, x \in I,\ x \neq 0$.

Since $x \in I \subseteq \mathbb{Q}$, $\frac{1}{x} \in \mathbb{Q}$.

Since I is an ideal of $\mathbb{Q}$, $x \cdot \frac{1}{x} \in I$, i.e., $1 \in I$.

But then, by Theorem 2, $I = \mathbb{Q}$.
Hence, $\mathbb{Q}$ has no non-trivial proper ideals.

***

Try solving a related exercise now.

E17) Find all the ideals of $\mathbb{R}$ and $\mathbb{C}$.

Now let us shift our attention to binary operations on the set of ideals of a ring. In the previous section you studied that the intersection of subrings is a subring. You will now see why the intersection of ideals is an ideal.

Theorem 3: If I and J are ideals of a ring R (not necessarily commutative), then the following are ideals of R:

i) $I \cap J$, and

ii) $I + J = \{a + b \mid a \in I \text{ and } b \in J\}$.

Proof: i) From Unit 11, you know that $I \cap J$ is a subring of R.

Next, if $a \in I \cap J$, then $a \in I$ and $a \in J$.

Therefore, $ax \in I$, $xa \in I$ and $ax \in J$, $xa \in J$ for all x in R.
So, $ax \in I \cap J$ and $xa \in I \cap J$ for all $a \in I \cap J$ and $x \in R$.

Thus, $I \cap J$ is an ideal of R.

ii) Firstly, $0 = 0 + 0 \in I + J$. $\therefore I + J \neq \phi$.

Secondly, if $x, y \in I + J$, then $x = a_1 + b_1$ and $y = a_2 + b_2$ for some $a_1, a_2 \in I$ and $b_1, b_2 \in J$.
So, $x - y = (a_1 + b_1) - (a_2 + b_2) = (a_1 - a_2) + (b_1 - b_2) \in I + J$.

Finally, let $x \in I + J$ and $r \in R$. Then $x = a + b$ for some $a \in I$ and $b \in J$.
Now $ar \in I$, $ra \in I$ and $br \in J$, $rb \in J$ since I and J are ideals of R.
Therefore, $xr = (a + b)r = ar + br \in I + J$.
Also, $rx = r(a + b) = ra + rb \in I + J$, similarly.

Thus, $I + J$ is an ideal of R. ■

So, the sum of two ideals is an ideal. Here, note that the sum of two subrings need not be a subring, as you found in Unit 11.

Further, as we noted in Unit 11 in the case of subrings, **the intersection of any number of ideals of R is an ideal of R.** This can be proved along the same lines as Theorem 3(i).

Also note that Example 8 follows from Theorem 3.

Now, let us consider the product of ideals. In Unit 11, you saw that if we define $IJ = \{ab \mid a \in I, b \in J\}$, then IJ need not even be a subring, leave alone being an ideal. This is because if $x, y \in IJ$, then with this definition of IJ it is not necessary that $x - y \in IJ$. (You will study an example in Unit 15.)
However, if we define the product
$\mathbf{IJ = \{x \in R \mid x = a_1b_1 + \cdots + a_mb_m \text{ for } a_i \in I, b_i \in J \ \forall\ i = 1, \ldots, m, m \in \mathbb{N}\}}$,
then we have the following theorem.

Theorem 4: Let I and J be ideals of a ring R, whether commutative or not. Then IJ is an ideal of R.

Proof: Firstly, $IJ \neq \phi$, since $I \neq \phi$ and $J \neq \phi$.

Next, let $x, y \in IJ$. Then
$x = a_1b_1 + \cdots + a_mb_m$ and $y = a_1'b_1' + \cdots + a_n'b_n'$,
for some $a_1, \ldots, a_m, a_1', \ldots, a_n' \in I$ and $b_1, \ldots, b_m, b_1', \ldots, b_n' \in J$.

$$\therefore x - y = (a_1b_1 + \cdots + a_mb_m) - (a_1'b_1' + \cdots + a_n'b_n')$$
$$= (a_1b_1 + \cdots + a_mb_m) + (-a_1')b_1' + \cdots + (-a_n')b_n',$$

which is a finite sum of elements of the form ab with $a \in I$ and $b \in J$.
So, $x - y \in IJ$.

Finally, let $x \in IJ$, say $x = a_1b_1 + \cdots + a_nb_n$, with $a_i \in I$ and $b_i \in J$.
Then, for any $r \in R$,

$xr = (a_1b_1 + ... + a_nb_n)r = a_1(b_1r) + ... + a_n(b_nr)$, and

$rx = r(a_1b_1 + \cdots + a_nb_n) = (ra_1)b_1 + \cdots + (ra_n)b_n$.

Since I and J are ideals of R, $ra_i \in I$ and $b_ir \in J \ \forall\ i = 1, \ldots, n$.

So xr and rx are finite sums of elements of the form ab with $a \in I$ and $b \in J$.

Hence, $xr \in IJ$ and $rx \in IJ$.

Thus, IJ is an ideal of R. ■

Let us consider an example to understand what $I \cap J$, IJ and $I + J$ look like.

Example 11: For $m, n \in \mathbb{Z}$, show that

i) $n\mathbb{Z} \cap m\mathbb{Z} = \ell\mathbb{Z}$, where $\ell = [n, m]$, the l.c.m of n and m;

ii) $n\mathbb{Z} + m\mathbb{Z} = h\mathbb{Z}$, where $h = (n, m)$, the g.c.d of n and m; and

iii) $(n\mathbb{Z})(m\mathbb{Z}) = nm\mathbb{Z}$.

Solution: From Unit 1, you know that ℓ and h exist.

i) Since $\ell = [n, m]$, $\ell = nx$ and $\ell = my$, for some $x, y \in \mathbb{Z}$.
So, $\ell \in n\mathbb{Z} \cap m\mathbb{Z}$.
Hence, $\ell\mathbb{Z} \subseteq n\mathbb{Z} \cap m\mathbb{Z}$. …(1)
Conversely, let $\alpha \in n\mathbb{Z} \cap m\mathbb{Z}$.
Since $\alpha \in n\mathbb{Z}$, $n \mid \alpha$. Since $\alpha \in m\mathbb{Z}$, $m \mid \alpha$.
Hence, by definition, $\ell \mid \alpha$. So, $\alpha \in \ell\mathbb{Z}$.
Thus, $n\mathbb{Z} \cap m\mathbb{Z} \subseteq \ell\mathbb{Z}$. …(2)
From (1) and (2), we get $n\mathbb{Z} \cap m\mathbb{Z} = \ell\mathbb{Z}$.

ii) Any element of $n\mathbb{Z} + m\mathbb{Z}$ is $nr + ms$, where $r, s \in \mathbb{Z}$.
Since $(n, m) = h$, $hn_1 = n$ and $hm_1 = m$, for some $n_1, m_1 \in \mathbb{Z}$.
Then $nr + ms = h(n_1r + m_1s) \in h\mathbb{Z}$.
Therefore, $n\mathbb{Z} + m\mathbb{Z} \subseteq h\mathbb{Z}$. …(3)
Conversely, from Unit 1 you know that $h = na + mb$, for some $a, b \in \mathbb{Z}$.
Hence, $h \in n\mathbb{Z} + m\mathbb{Z}$.
So, $h\mathbb{Z} \subseteq n\mathbb{Z} + m\mathbb{Z}$. …(4)
From (3) and (4), we see that $n\mathbb{Z} + m\mathbb{Z} = h\mathbb{Z}$.

iii) For the product, note that $nm = (n \cdot 1)(m \cdot 1) \in (n\mathbb{Z})(m\mathbb{Z})$.
$\therefore nm\mathbb{Z} \subseteq (n\mathbb{Z})(m\mathbb{Z})$.
Also, any element of $(n\mathbb{Z})(m\mathbb{Z})$ is of the form

$$\sum_{i=1}^{t}(nr_i)(ms_i) = nm\left(\sum_{i=1}^{t} r_is_i\right) \in nm\mathbb{Z}.$$

So, $(n\mathbb{Z})(m\mathbb{Z}) \subseteq nm\mathbb{Z}$.
Hence, $(n\mathbb{Z})(m\mathbb{Z}) = nm\mathbb{Z}$.

***

Consider the following comment related to Example 11.

Remark 3: Note that what is proved in Example 11 is analogous to what was proved in Theorem 8, Unit 4, for cyclic groups.

Next, we want to highlight a very useful point made in Example 11. This point is used very often when dealing with $\mathbb{Z}$, as you will see in Block 4 particularly.

Example 12: Show that if n and m are coprime integers, then $n\mathbb{Z} + m\mathbb{Z} = \mathbb{Z}$.

Solution: Since n and m are coprime, $(n, m) = 1$ (see Unit 1).
Now, from Example 11, you know that
$n\mathbb{Z} + m\mathbb{Z} = (n, m)\mathbb{Z}$.
Hence the result.

***

Now let us see what IJ is like if one of I or J is a principal ideal. You have already seen this for $\mathbb{Z}$ in Example 11.

Example 13: Let R be a ring, and I and J be ideals of R such that one of them is principal. Show that $IJ = \{ab \mid a \in I, b \in J\}$.

Solution: Let $I = < a >$, and J may or may not be principal.

Then any element of IJ is $x = \sum_{i=1}^{n} a_i b_i,\ a_i \in I,\ b_i \in J.$

Let $a_i = ar_i$, where $r_i \in R\ \forall\ i = 1, \ldots, n.$

Then $x = a\left(\sum_{i=1}^{n} r_i b_i\right) = ab,$ where $b = \sum_{i=1}^{n} r_i b_i \in J,$ since J is an ideal of R.

Hence the result.

***

Try solving some exercises now.

E18) Find $I \cap J,\ I + J$ and IJ for

i) $I = < \overline{4} >$ and $J = < \overline{6} >$ in $\mathbb{Z}_{12}$;

ii) $I = \wp(Y)$ and $J = \{A \in \wp(X) \mid A \cap Y = \phi\}$ in $\wp(X)$, where X is a non-empty set and $Y \subsetneq X,\ Y \neq \phi$.

E19) If I and J are ideals of a ring R (not necessarily commutative), then show that

i) $IJ \subseteq I \cap J \subseteq I \subseteq I + J$ and $IJ \subseteq I \cap J \subseteq J \subseteq I + J$;
(This is shown schematically in Fig.2.)

ii) $I + J$ is the smallest ideal containing both the ideals I and J, i.e., if A is an ideal of R containing both I and J, then A must contain $I + J$;

iii) $I \cap J$ is the largest ideal that is contained in both I and J, i.e., if B is an ideal of R contained in both I and J, then $B \subseteq (I \cap J)$;

iv) If $1 \in R$ and $I + J = R$, then $IJ = I \cap J$, i.e., if the top two of Fig.2 are equal, then so are the lowest two.

v) If $1 \notin R$ in (iv) above, is the rest of (iv) still true? Why, or why not?

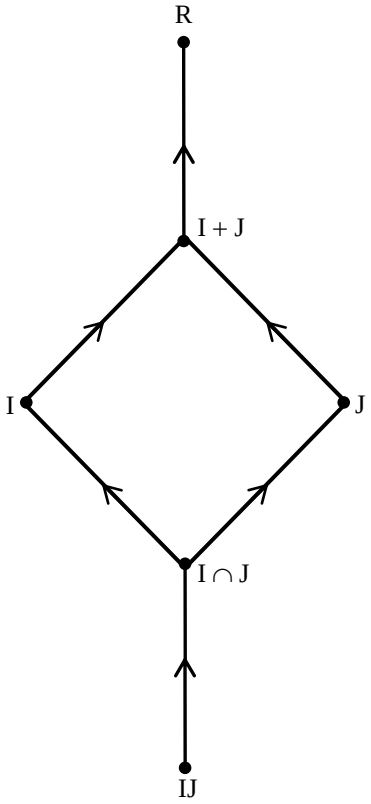

Fig. 2: The ideal hierarchy! An arrow from an ideal to another just shows that the first is contained in the second, like in the subgroup diagrams of Block 1.

Now let us look at the set operations of complementation and of union. In Unit 11, you have seen that the complement of a subring is not a subring. You have also seen the conditions under which the union of two subrings is a subring. Build on that understanding to solve the following exercises.

E20) Consider the following 'proof' of the statement, "$I_1 \setminus I_2$ is an ideal of R whenever I_1 and I_2 are distinct ideals of R."
At each step of the 'proof', decide whether the statement is true or false, and give your reasons for saying so.

Proof: 1) For $x, y \in I_1 \setminus I_2$, $x, y \in I_1$ and $x \notin I_2$, $y \notin I_2$.

2) $x - y \in I_1 \setminus I_2$.

3) For $x \in I_1 \setminus I_2$ and $r \in R$, $xr \in I_1$ and $xr \notin I_2$.

4) $xr \in I_1 \setminus I_2 \ \forall \ x \in I_1 \setminus I_2, r \in R$.

5) $I_1 \setminus I_2$ is an ideal of R.

E21) Explain why $I_1 \setminus I_2$ is not an ideal of the ring R, where I_1 and I_2 are ideals of R.

E22) i) Let $I_1 = <\overline{3}>$ and $I_2 = <\overline{5}>$ in $\mathbb{Z}_{10}$. Is $I_1 \cup I_2$ an ideal of $\mathbb{Z}_{10}$? Why, or why not?

ii) If $I_3 = <\overline{4}>$ in $\mathbb{Z}_{10}$, is $I_2 \cup I_3$ an ideal of $\mathbb{Z}_{10}$? Why, or why not?

E23) Using what you have found in E22, find the condition under which $I_1 \cup I_2$ is an ideal of a ring R, where I_1 and I_2 are ideals of R.

Let us now see whether the Cartesian product of ideals is an ideal of the direct product of the rings concerned. In Sec.6.4, Unit 6, you noted that if $H \lhd G_1$ and $K \lhd G_2$, then $H \times K \lhd G_1 \times G_2$. Does an analogous result hold true for ideals of the direct product $R_1 \times R_2$? Consider the following theorem.

Theorem 5: Let I_1 and I_2 be ideals of the rings R_1 and R_2, respectively, where R_1 and R_2 may or may not be commutative. Then $I_1 \times I_2$ is an ideal of $R_1 \times R_2$.

Proof: By Theorem 3, Unit 11, you know that $I_1 \times I_2$ is a subring of $R_1 \times R_2$.
Now, let $(a, b) \in I_1 \times I_2$ and $(x, y) \in R_1 \times R_2$.
Then $(a, b)(x, y) = (ax, by) \in I_1 \times I_2$, and
$(x, y)(a, b) = (xa, yb) \in I_1 \times I_2$. (Why?)

Thus, $I_1 \times I_2$ is an ideal of $R_1 \times R_2$. ■

Along the lines of Theorem 5, you can prove that the Cartesian product **$I_1 \times I_2 \times \ldots \times I_n$ of ideals $I_1, I_2, \ldots, I_n$ in $R_1, R_2, \ldots, R_n$, respectively, is an ideal of $R_1 \times R_2 \times \ldots \times R_n$ $\forall$ $n \geq 2$.** Let us consider an example of this, for $n = 2$.

Example 14: Find a proper non-trivial ideal of $C[0, 1] \times C[1, 2]$.

Solution: Here we will use what you proved in E4.
Let $a \in [0, 1]$ and $b \in [1, 2]$. Then I_a and I_b are ideals of $C[0, 1]$ and $C[1, 2]$, respectively. Since $f : [0, 1] \to \mathbb{R} : f(x) = 1$ does not belong to I_a, $I_a \neq C[0, 1]$.
Also $g : [0, 1] \to \mathbb{R} : g(x) = x - a$ is in I_a and $g \neq \mathbf{0}$. So $I_a \neq \{\mathbf{0}\}$.
Thus, I_a is a proper non-trivial ideal of $C[0, 1]$.
Similarly, I_b is a proper non-trivial ideal of $C[1, 2]$.
Thus, by Theorem 5, $I_a \times I_b$ is a proper non-trivial ideal of $C[0, 1] \times C[1, 2]$.

Note that $C[0, 1] \times I_b$ and $I_a \times C[1, 2]$ are also non-trivial proper ideals of $C[0, 1] \times C[1, 2]$. (Why?)

***

In Unit 11, you showed that not every subring of $R_1 \times R_2$ is a direct product of subrings. The following example shows that the same is true for ideals too.

Example 15: Let R_1 and R_2 be rings. Show that not every ideal of $R_1 \times R_2$ is of the form $I_1 \times I_2$, where I_1 is an ideal of R_1 and I_2 is an ideal of R_2.

Solution: Let A_1 and A_2 be abelian groups. Define multiplication on A_1 and A_2 by $a \odot b = 0$ $\forall$ $a, b \in A_1$, and $a' \odot b' = 0$ $\forall$ $a', b' \in A_2$.
Then, you should verify that $(A_1 \times A_2, +, \odot)$ is a ring, where $+$ and $\odot$ denote componentwise addition and multiplication.
Let us take $A_1 = A_2 = \mathbb{Z}$.

Let $I = \{(n, n) \mid n \in \mathbb{Z}\}$.

Then, in Example 15, Unit 11, you have seen that I is a subring of $\mathbb{Z} \times \mathbb{Z}$. Also, I is an ideal of $A_1 \times A_2$, since

$(n, n) \odot (a, b) = (n \odot a, n \odot b) = (0, 0) \in I \ \forall \ n \in \mathbb{Z}, (a, b) \in \mathbb{Z} \times \mathbb{Z}$.

Note that I cannot be of the form $I_1 \times I_2$, where I_1 and I_2 are ideals of $\mathbb{Z}$. Because, if it were, then the subring I would have been of the form $I_1 \times I_2$, where I_1 and I_2 are subrings of $\mathbb{Z}$. But you have proved in E22, Unit 11, that this is not so.

***

By solving the following exercises, you will get some more examples of the ideals discussed in Theorem 5. While solving them, use your experience of working with direct products of groups also.

E24) Find three distinct non-trivial proper ideals of $\mathbb{R}^4$.

E25) Let R be a non-trivial ring. Check whether or not $S = \{(x, x) \mid x \in R\}$ is an ideal of $R \times R$. (Here the multiplication on R is not the zero multiplication given in Example 15.)

E26) Find two distinct non-trivial proper ideals of $\mathbb{Q}[x] \times \mathbb{Z}[\sqrt{3}]$.

With this, let us end our discussion on set operations on ideals. We will now focus on the real reason for the creation of the concept of an ideal.

12.4 QUOTIENT RINGS

In Unit 7, you have studied quotient groups in some detail. In this section, we will discuss an analogous concept for rings. Much is similar between these two concepts. So please re-look Unit 7 before going further.

You know that the set of all cosets of a subgroup H, of a group G, forms a group only if $H \lhd G$. This group is G/H, the factor group (or the quotient group) associated with the normal subgroup H. We want to define an analogous concept for rings. But first, an important remark!

Remark 4: In this unit, you have studied the definition of an ideal of a ring – of *any ring*. There we also mentioned that we would only work with commutative rings, unless mentioned otherwise. **In this section, the theorems we prove will be valid for any ring**, commutative or not. However, the **examples** will be only of **commutative rings**, as you will be largely looking at the examples you have studied in the previous sections.

At the beginning of Sec.12.2, you noted that if $(R, +, \cdot)$ is a ring and I is a subring of R, then $I \lhd (R, +)$. So $(R/I, +)$ is a group. In fact, from Unit 7, you know that this is an abelian group. Now, if $(R/I, +, \cdot)$ is to be a ring, where $+$ and $\cdot$ are defined by

$(x + I) + (y + I) = (x + y) + I$, and

$(x + I) \cdot (y + I) = xy + I \ \forall \ x + I, \ y + I \in R/I$,

then you have seen that the subring I needs to satisfy the extra condition that $rx \in I$ and $xr \in I$ whenever $r \in R$ and $x \in I$, i.e., I should be an ideal of R.

Of course, if I is an ideal of R, then $+$ is well-defined on R/I. We need to see whether $\cdot$ is well-defined on R/I or not. Let's check this.

Let $a, a', b, b' \in R$ be such that $a + I = a' + I, b + I = b' + I$.
Now, since $a + I = a' + I, a - a' \in I$. Let $a - a' = x$.
Similarly, $b - b' \in I$, say, $b - b' = y$.
Then $ab = (a' + x)(b' + y) = a'b' + (xb' + a'y + xy)$.
$\therefore ab - a'b' \in I$, since $x \in I, y \in I$ and I is an ideal of R.
$\therefore ab + I = a'b' + I$, as you know from Unit 5.
Thus, $\cdot$ is a well-defined binary operation on R/I.

Now we are in a position to prove the following result for a ring R, which may or may not be commutative.

Theorem 6: Let R be a ring, and let I be a subring of R. The set of cosets of I in R, R/I, is a ring with respect to addition and multiplication, defined by
$(x + y) + (y + I) = (x + y) + I$, and
$(x + I) \cdot (y + I) = xy + I \ \forall \ x, y \in R$,
if and only if I is an ideal of R.

R/I is read as ' R modulo I ' or ' R mod I ', in brief.

Proof: First, let us assume that I is an ideal of R.
As you have noted earlier, $(R/I, +)$ is an abelian group. So, to prove that R/I is a ring we need to check that $\cdot$ is a binary operation on R/I, which is associative and distributive over $+$.

i) **$\cdot$ is a binary operation:** This is proved just before stating Theorem 6.

ii) **$\cdot$ is associative:** $\forall \ a, b, c \in R$,

$$\begin{aligned}((a + I) \cdot (b + I)) \cdot (c + I) &= (ab + I) \cdot (c + I) \\ &= (ab)c + I \\ &= a(bc) + I \\ &= (a + I) \cdot ((b + I) \cdot (c + I)).\end{aligned}$$

iii) **Distributive laws:** Let $a + I, b + I, c + I \in R/I$. Then

$$\begin{aligned}(a + I) \cdot ((b + I) + (c + I)) &= (a + I) \cdot [(b + c) + I] \\ &= a(b + c) + I \\ &= (ab + ac) + I \\ &= (ab + I) + (ac + I) \\ &= (a + I) \cdot (b + I) + (a + I) \cdot (c + I).\end{aligned}$$

You can, similarly, prove that $\forall \ a, b, c \in R$,
$((a + I) + (b + I)) \cdot (c + I) = (a + I) \cdot (c + I) + (b + I) \cdot (c + I)$.
Thus, multiplication distributes over addition.

Hence, R/I is a ring.

Next, to prove the converse, suppose I is not an ideal of R. Then $\exists \ x \in I$ and $r \in R$ s.t. $xr \notin I$.

Now $x + I = 0 + I = I,$ since $x \in I.$
So $(x + I) \cdot (r + I) = xr + I \neq I,$ since $xr \notin I.$
Also $(x + I)(r + I) = (0 + I)(r + I) = 0 + I = I.$
Thus, the multiplication is not well-defined on $R/I.$
Hence, $(R/I, +, \cdot)$ is not a ring. ■

Note that Theorem 6 holds **for any ring R**, commutative or not.
The ring R/I is called the **quotient ring**, or **factor ring, of R by the ideal I.**

Let us look at some examples. We start with the example that gave rise to the terminology 'R mod I'.

Example 16: Let $R = \mathbb{Z}$ and $I = n\mathbb{Z}.$ What is R/I?

Solution: In Sec.12.2, you have seen that $n\mathbb{Z}$ is an ideal of $\mathbb{Z}.$ From Unit 2, you know that $\mathbb{Z}/n\mathbb{Z} = \{n\mathbb{Z}, 1 + n\mathbb{Z}, \ldots, (n-1) + n\mathbb{Z}\}$

$$= \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\},$$

that is, the set of equivalence classes modulo n, $\mathbb{Z}_n$.
So, R/I is the ring $\mathbb{Z}_n,$ the ring of integers modulo n.

***

Now let us look at an ideal of $\mathbb{Z}_n,$ where $n = 8.$

Example 17: Let $R = \mathbb{Z}_8.$ Show that $I = \{\overline{0}, \overline{4}\}$ is an ideal of $R.$ Construct the Cayley tables for $+$ and $\cdot$ in $R/I.$

Solution: Note that $I = \overline{4}R,$ and hence, is a principal ideal of $R.$
From Unit 7, you know that the number of elements in R/I

$$= o(R/I) = \frac{o(R)}{o(I)} = \frac{8}{2} = 4.$$

You can see that these elements are the following cosets:
$\overline{0} + I = \{\overline{0}, \overline{4}\},\ \overline{1} + I = \{\overline{1}, \overline{5}\},\ \overline{2} + I = \{\overline{2}, \overline{6}\},\ \overline{3} + I = \{\overline{3}, \overline{7}\}.$

The Cayley tables for $+$ and $\cdot$ in R/I are:

$+$	$\overline{0}+I$	$\overline{1}+I$	$\overline{2}+I$	$\overline{3}+I$
$\overline{0}+I$	$\overline{0}+I$	$\overline{1}+I$	$\overline{2}+I$	$\overline{3}+I$
$\overline{1}+I$	$\overline{1}+I$	$\overline{2}+I$	$\overline{3}+I$	$\overline{0}+I$
$\overline{2}+I$	$\overline{2}+I$	$\overline{3}+I$	$\overline{0}+I$	$\overline{1}+I$
$\overline{3}+I$	$\overline{3}+I$	$\overline{0}+I$	$\overline{1}+I$	$\overline{2}+I$

$\cdot$	$\overline{0}+I$	$\overline{1}+I$	$\overline{2}+I$	$\overline{3}+I$
$\overline{0}+I$	$\overline{0}+I$	$\overline{0}+I$	$\overline{0}+I$	$\overline{0}+I$
$\overline{1}+I$	$\overline{0}+I$	$\overline{1}+I$	$\overline{2}+I$	$\overline{3}+I$
$\overline{2}+I$	$\overline{0}+I$	$\overline{2}+I$	$\overline{0}+I$	$\overline{2}+I$
$\overline{3}+I$	$\overline{0}+I$	$\overline{3}+I$	$\overline{2}+I$	$\overline{1}+I$

***

Next, let us look at an example of a polynomial ring.

Example 18: What do the elements of $\mathbb{R}[x]/\langle x \rangle$ look like? Give two distinct non-trivial elements of this ring also.

Solution: Let $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{R}[x].$ Then

$f(x) = a_0 + xg(x)$, where $g(x) = a_1 + a_2x + \cdots + a_nx^{n-1}$.

So $f(x) + < x > = a_0 + xg(x) + < x > = a_0 + < x >$, since $xg(x) \in < x >$.

Thus, any element of $\mathbb{R}[x]/< x >$ is of the form $a + < x > = \bar{a}$, where $a \in \mathbb{R}$.

Two non-trivial elements of $\mathbb{R}[x]/< x >$ are $\bar{1}$ and $\bar{2}$. They are distinct because $\bar{2} - \bar{1} = \bar{1} \neq \bar{0}$. (There are infinitely many other elements you can pick. In fact, why don't you find some others?)

***

In the examples above, note that both R and R/I are commutative, and both have identity. Is this always true? You will answer this while working on the following exercises.

E27) If R is a commutative ring and I is an ideal of R, must R/I be commutative? Why, or why not?

E28) Show that if R is a ring with identity, then R/I is a ring with identity, for any ideal I of R.

E29) Construct the Cayley tables for the quotient rings $2\mathbb{Z}/6\mathbb{Z}$ and $\mathbb{Z}_{14}/< \bar{2} >$.

E30) If R is a ring with identity 1, and I is an ideal of R containing 1, then what does R/I look like?

E31) Let X be a non-empty set and $Y \subsetneq X$, $Y \neq \phi$. Give two distinct elements of $\wp(X)/\wp(Y)$.

E32) Give two distinct non-trivial elements of $\mathbb{Z} \times \mathbb{Z}/(< 3 > \times < 5 >)$. How many elements does this ring have?

E33) Let N be the nil radical of R. Show that R/N has no non-zero nilpotent element.

E34) Let R be a ring and I be an ideal of R. Find $C(R/I)$, the centre of R/I.

Now let us see what the subrings of a quotient ring look like. From Unit 7, you know that the subgroups of the quotient group $(R/I, +)$ are of the form $(J/I, +)$, where J is a subgroup of R containing I. Also, you know that any subring of R/I is a subgroup of $(R/I, +)$. Thus, any subring of $(R/I, +)$ must be of the form $(S/I, +)$, where $I \leq S \leq R$. Is this enough for S/I to be a subring of R/I? Not so. Don't forget that S/I needs to be closed w.r.t. multiplication. Let us see what this means for S. Consider the following theorem.

Theorem 7: Let R be a ring and I be an ideal of R. There is a 1-1 correspondence between $\mathcal{S}$, the set of subrings of R/I and $\mathcal{T}$, the set of subrings of R containing I.

Proof: Let us define $\phi : \mathcal{T} \to \mathcal{S} : \phi(S) = S/I$.

ϕ is well-defined: We need to show that S/I is in $\mathcal{S}$, for S in $\mathcal{T}$.

Since $S \supseteq I$ and $S \neq \phi$, $S/I \neq \phi$.

Let $s_1 + I, s_2 + I \in S/I$. Then $s_1, s_2 \in S$. So, $s_1 - s_2 \in S$ and $s_1 s_2 \in S$.

Now $(s_1 + I) - (s_2 + I) = (s_1 - s_2) + I \in S/I$, since $(s_1 - s_2) \in S$.

Also $(s_1 + I) \cdot (s_2 + I) = s_1 s_2 + I \in S/I$, since $s_1 s_2 \in S$.

Thus, $S/I \in \mathcal{S}$.

ϕ is 1-1: Let $S_1, S_2 \in \mathcal{T}$ such that $(S_1/I) = (S_2/I)$.

Let $s \in S_1$. Then $s + I \in S_1/I = S_2/I$.

So $\exists\, s' \in S_2$ s.t. $s + I = s' + I$. Thus, $(s - s') \in I \subseteq S_2$.

Now $s - s' \in S_2$ and $s' \in S_2$, so that $s \in S_2$.

Thus, $S_1 \subseteq S_2$.

Similarly, you should show that $S_2 \subseteq S_1$.

Thus, $S_1 = S_2$.

Hence, ϕ is 1-1.

ϕ is surjective: Let A be a subring of R/I and let $S = \{s \in R \mid s + I \in A\}$.

Since $A \neq \phi$, $S \neq \phi$.

Also, for $s_1, s_2 \in S$, $s_1 + I \in A$, $s_2 + I \in A$.

Since A is a subring of R/I, $(s_1 - s_2) + I \in A$ and $s_1 s_2 + I \in A$.

Thus, $s_1 - s_2 \in S$ and $s_1 s_2 \in S$.

$\therefore S$ is a subring of R.

Now, $\forall\, x \in I$, $x + I = I$, the zero element of R/I. Hence, $x + I \in A$.

Thus, $x \in S\ \forall\, x \in I$, i.e., $S \supseteq I$.

Also, for $r + I$ in R/I, $r + I \in A \Leftrightarrow r \in S \Leftrightarrow r + I \in S/I$.

Thus, $A = S/I$.

Hence, $A = \phi(S)$, i.e., ϕ is surjective.

Thus, ϕ is a bijection.

Hence, **every subring of R/I is of the form S/I, where S is a subring of R containing I.** ■

Now, as you have seen for subrings, let us consider what the ideals of a quotient ring look like. Does Theorem 7 give you an idea? You know that an ideal of a ring R is a subring of R. Thus, if R is a ring and I is an ideal of R, then any ideal of R/I must be of the form J/I, where J is a subring of R containing I. Of course, J would need to satisfy some more properties too. So, let us see what the ideals of R/I are.

Theorem 8: Let R be a ring and I be an ideal of R. Then there is a 1-1 correspondence between $\mathcal{A}$, the set of ideals of R/I, and $\mathcal{B}$, the set of ideals of R containing I.

Proof: Define $\phi : \mathcal{B} \to \mathcal{A} : \phi(J) = J/I$.

ϕ is well-defined: Here we need to check that $J/I \in \mathcal{A}$.

Since $J \supseteq I$ and $J \neq \phi$, $J/I \neq \phi$.

Let $a+I, b+I \in J/I$. Then $a, b \in J$, and

$(a+I)-(b+I) = (a-b)+I \in J/I$, since $(a-b) \in J$.

Next, for $a+I \in J/I$ and $r+I \in R/I$, $a \in J$, $r \in R$. So,

$(a+I)(r+I) = ar+I \in J/I$, since $ar \in J$, as J is an ideal of R.

Hence, J/I is an ideal of R/I.

Hence, ϕ is well-defined.

ϕ is 1-1: Let $J_1, J_2 \in \mathcal{B}$ such that $J_1/I = J_2/I$.

As for Theorem 7, you should prove that $J_1 = J_2$, i.e., ϕ is 1-1.

ϕ is onto: Let S be an ideal of R/I, and let $J = \{s \in R \mid s+I \in S\}$.

As in the case of Theorem 7, you should prove that J is an ideal of R containing I.

Further, for $x+I \in R/I$, $x+I \in S$ iff $x+I \in J/I$, i.e., $S = J/I$.

Thus, $J \in \mathcal{B}$ s.t. $\phi(J) = S$.

Hence ϕ is 1-1 and onto, i.e., ϕ is a bijection.

Thus, **every ideal of R/I is of the form J/I, for some ideal J of R containing I**. Conversely, **for each ideal J of R containing I, J/I is an ideal of R/I**. ■

Let us consider some examples.

Example 19: Find all the subrings and ideals of $\mathbb{Z}/10\mathbb{Z}$.

Solution: First, any subring of $\mathbb{Z}$ is of the form $n\mathbb{Z}$, for $n \in \mathbb{Z}$.

Also, in Unit 7 you have seen that $10\mathbb{Z} \subseteq n\mathbb{Z}$ iff $n \mid 10$.

Thus, the only subrings of $\mathbb{Z}/10\mathbb{Z}$ are $n\mathbb{Z}/10\mathbb{Z}$, where $n = 1, 2, 5, 10$.

For $n = 1$, we get the whole ring $\mathbb{Z}/10\mathbb{Z}$.

For $n = 10$, we get the trivial subring.

The other two subrings are $<2>/<10>$ and $<5>/<10>$.

You know that every subring of $\mathbb{Z}$ is an ideal of $\mathbb{Z}$. Of course, every ideal of $\mathbb{Z}$ is a subring of $\mathbb{Z}$. By Theorems 7 and 8, this holds true for $\mathbb{Z}/10\mathbb{Z}$ also.

Thus, $\mathbb{Z}/10\mathbb{Z}$ has 4 ideals – $\mathbb{Z}/10\mathbb{Z}$, $2\mathbb{Z}/10\mathbb{Z}$, $5\mathbb{Z}/10\mathbb{Z}$ and $\{\bar{0}\}$.

***

Example 20: Find all the ideals of the ring $2\mathbb{Z}/30\mathbb{Z}$.

Solution: Any ideal of $2\mathbb{Z}/30\mathbb{Z}$ is of the form $n\mathbb{Z}/30\mathbb{Z}$, where

$30\mathbb{Z} \subseteq n\mathbb{Z} \subseteq 2\mathbb{Z}$, i.e., $2 \mid n$ and $n \mid 30$.

So, $n = 2, 6, 10$ or 30.

Hence, the required ideals are $2\mathbb{Z}/30\mathbb{Z}$, $6\mathbb{Z}/30\mathbb{Z}$, $10\mathbb{Z}/30\mathbb{Z}$, $\{\bar{0}\}$.

Note that these are all the subrings of $2\mathbb{Z}/30\mathbb{Z}$ also.

***

Example 21: Let R be a ring (not necessarily commutative), and let I be an ideal of R. Then, for any subring S of R, will S/I and $(S+I)/I$ be subrings of R/I? Under what conditions on S will $(S+I)/I$ be an ideal of R/I?
Also give an example to show that $(S+I)/I$ need not be an ideal of R/I.

Solution: By Theorem 7, you know that S/I is a subring of R/I only if $S \supseteq I$.

Here we have proved that $S+I$ is a subring of R. However, in Example 13, Unit 11, you studied that the sum of subrings need not be a subring. What do you conclude?

Next, note that $I \subseteq S+I \subseteq R$.
Further, for $s_1 + x_1,\ s_2 + x_2 \in S+I$,
$(s_1 + x_1) - (s_2 + x_2) = (s_1 - s_2) + (x_1 - x_2) \in S+I$, and
$(s_1 + x_1)(s_2 + x_2) = s_1s_2 + x_1s_2 + s_1x_2 + x_1x_2 \in S+I$, since $s_1s_2 \in S$ and $x_1s_2,\ s_1x_2,\ x_1x_2 \in I$.
Thus, $S+I$ is a subring of R containing I.
Hence, $(S+I)/I$ is a subring of R/I.

Finally, $(S+I)/I$ will be an ideal of R/I if $S+I$ is an ideal of R, by Theorem 8.
Now, for $S+I$ to be an ideal of R,
$(s+x)r = sr + xr \in S+I$, for $(s+x) \in S+I$ and $r \in R$.
Since I is an ideal of R, $xr \in I$.
Thus, $S+I$ will be an ideal of R/I iff $\forall\ s \in S$ and $r \in R$, $sr \in S+I$.
In particular, if S is an ideal of R, then $(S+I)/I$ will be an ideal of R/I.

As an example of $(S+I)/I$ not being an ideal of R/I, take $S = \mathbb{Z}$ and $I = \{0\}$ in $R = \mathbb{Q}$. Then $(S+I)/I$ is an ideal of $\mathbb{Q}/I$ iff $S+I$ is an ideal of $\mathbb{Q}$, i.e., $\mathbb{Z} + \{0\} = \mathbb{Z}$ is an ideal of $\mathbb{Q}$. You have already seen that this is not true.
Hence, $(S+I)/I$ is not an ideal of $\mathbb{Q}/I$.

***

Try solving some exercises now.

E35) Show that $<2, x>/<x>$ is an ideal of $\mathbb{Z}[x]/<x>$.

E36) Give two distinct ideals of $\mathbb{Z}/25\mathbb{Z}$.

E37) Give two distinct ideals of $\wp(X)/\wp(Y)$, where $X = \{1, 2, \ldots, 10\}$ and $Y = \{1, 2\}$.

E38) Show that if S is a subring of a ring R, and I is an ideal of R, then $S \cap I$ is an ideal of S.

(In Unit 13, you will see that $S/S \cap I$ is a subring of R/I.)

Give an example to show that $S/S \cap I$ need not be an ideal of $R/S \cap I$.

You will realise the utility and importance of quotient rings when we discuss homomorphisms in the next unit. For now, consider an important remark before we end this discussion.

Remark 5: In much of this unit you have worked with commutative rings. However, you have studied the proofs of several theorems for non-commutative rings also. You have studied quotient rings of any ring. Thus, for example, $\mathbb{M}_n(\mathbb{R})$ and $\mathbb{H}$ also have ideals and corresponding quotient rings. Similarly, Theorems 7 and 8 are true for any ring.
However, **we have defined ideals generated by n elements, $n \in \mathbb{N}$, only for commutative rings**.

Now let us briefly summarise what you have studied in this unit.

12.5 SUMMARY

In this unit, we have discussed the following points.

1. The definition of an ideal of a ring, and examples of ideals of commutative rings.

2. The criteria for a subset of a ring to be an ideal: A non-empty subset I of a ring R is an ideal of R if and only if

   i) $a - b \in I \ \forall\ a \in I, b \in I$, and

   ii) $ar \in I$ and $ra \in I \ \forall\ a \in I, r \in R$.

3. The definition of a principal ideal, and of an ideal generated by n elements, $n \geq 2$, of a commutative ring.

4. The set of nilpotent elements in a commutative ring is an ideal of the ring.

5. If I is an ideal of a ring R with identity 1, and $1 \in I$, then $I = R$.

6. If I and J are ideals of a ring R, then

   i) $I \cap J$, $I + J$ and IJ are ideals of R;

   ii) $I \cup J$ is an ideal of R iff $I \subseteq J$ or $J \subseteq I$,

   iii) $I \setminus J$ is not an ideal of R.

7. The Cartesian product of ideals is an ideal of the direct product of the corresponding rings.

8. The definition, and examples, of a quotient ring.

9. The quotient ring of a ring with identity (commutative ring, respectively) is a ring with identity (commutative ring, respectively.)

10. A subring (respectively, ideal) of a quotient ring R/I is of the form S/I, where S is a subring (respectively, ideal) of R containing I.

12.6 SOLUTIONS / ANSWERS

E1) Let $\mathcal{F}$ be the ring of functions from $[-3, 3]$ to $\mathbb{R}$, w.r.t. pointwise addition and multiplication. You know that $\mathcal{F}$ is a commutative ring.
Let $I = \{f \in \mathcal{F} \mid f(0) = 0\}$.
Using the subring test, of Sec.11.3, you should check that I is a subring of $\mathcal{F}$.
Also, for any $f \in \mathcal{F}$ and $g \in I$, $(f \cdot g)(0) = f(0)g(0) = 0$.
So $f \cdot g \in I \ \forall\ f \in \mathcal{F}$ and $g \in I$.
Thus, I is an ideal of $\mathcal{F}$.

E2) As in Example 3, show that this is not an ideal of $\mathbb{C}$.

E3) i) In Unit 11, you have seen that $\mathbb{Z}[i]$ is a subring of $\mathbb{C}$.
However, $\frac{1}{5} \in \mathbb{C}$ and $i \in \mathbb{Z}[i]$, but $\frac{1}{5}i \notin \mathbb{Z}[i]$. So $\mathbb{Z}[i]$ is not an ideal of $\mathbb{C}$.

ii) You know that $\mathbb{R}[x]$ is a subring of $\mathbb{C}[x]$, since $\mathbb{R} \subseteq \mathbb{C}$.
However, $i \in \mathbb{C}[x]$ and $x \in \mathbb{R}[x]$, but $i \cdot x = ix \notin \mathbb{R}[x]$.
So $\mathbb{R}[x]$ is not an ideal of $\mathbb{C}[x]$.

iii) Note that the two sets are $\overline{3}\mathbb{Z}_6$ and $\overline{2}\mathbb{Z}_6$. From Example 9, Unit 11, you know that they are subrings of $\mathbb{Z}_6$.
Now, by elementwise multiplication, you can check that $rx \in \overline{3}\mathbb{Z}_6 \ \forall\ r \in \mathbb{Z}_6$ and $x \in \overline{3}\mathbb{Z}_6$.
(For instance, $\overline{5} \cdot \overline{3} = \overline{15} = \overline{3} \in \overline{3}\mathbb{Z}_6$.)
You can, similarly, see that $rx \in \overline{2}\mathbb{Z}_6 \ \forall\ r \in \mathbb{Z}_6$, $x \in \overline{2}\mathbb{Z}_6$.
Thus, $\overline{3}\mathbb{Z}_6$ and $\overline{2}\mathbb{Z}_6$ are ideals of $\mathbb{Z}_6$.

E4) i) Firstly, $I_a \neq \phi$, since $0 \in I_a$.
Next, $f, g \in I_a \Rightarrow f, g \in C[0, 1]$. So, $f - g \in C[0, 1]$.
Further, $(f - g)(a) = f(a) - g(a) = 0$.
Thus, $f - g \in I_a$.

Thirdly, $f \in I_a$, $g \in C[0,1] \Rightarrow fg \in C[0, 1]$.
Also, $(fg)(a) = f(a)g(a) = 0 \cdot g(a) = 0$.
Thus, $fg \in I_a$.
$\therefore I_a$ is an ideal of $C[0,1]$.

ii) On the same lines as in (i) above, you should prove that I_r is an ideal of $C[a, b]$.

iii) Let $r = \frac{1}{2}$. Then $J_r = \{f \in C[0, 1] \mid f(\frac{1}{2}) = 1\}$.

If $f, g \in J_r$, then $(f-g)\left(\frac{1}{2}\right) = f\left(\frac{1}{2}\right) - g\left(\frac{1}{2}\right) = 0 \neq 1$. So $f - g \notin J_r$.

Thus, J_r is not a subring of $C[0, 1]$. Hence, J_r is not an ideal of $C[0, 1]$.

E5) Since R is commutative, $C(R) = R$. Hence, $C(R)$ is an ideal of R.

E6) i) Let $S = \{a_1x + a_2x^2 + \cdots + a_nx^n \mid a_i \in \mathbb{Z},\ n \in \mathbb{N}\}$.

Since $x \in S$, $S \neq \phi$.

If $f(x) = \sum_{i=1}^{n} a_i x^i$, $g(x) = \sum_{j=1}^{m} b_j x^j$ are in S, then

$f(x) - g(x) = \sum_{i=1}^{n} (a_i - b_i)x^i + \sum_{i=n+1}^{m} (-b_j)x^j$, if $n \leq m$. (If $n \geq m$, you can work this out similarly.)

So $f(x) - g(x)$ has constant term 0, i.e., $f(x) - g(x) \in S$.

Again, from Block 1 of Calculus, you know that if $f(x) \in S$, then $f(x) = 0$ or $\deg f(x) \geq 1$, and the constant term of $f(x)$ is 0.

Also, if $g(x) \in \mathbb{Z}[x]$, then $g(x) = 0$ or $g(x) \neq 0$.

If $g(x) = 0$, $f(x)g(x) = 0 \in S\ \forall\ f(x) \in S$.

If $g(x) \neq 0$, the constant term of $f(x)g(x)$ is $0 \cdot b = 0$, where b is the constant term of $g(x)$.

Also $\deg (f(x) \cdot g(x)) = \deg f(x) + \deg g(x) \geq 1$.

Thus, $f(x)g(x) \in S$.

Hence, S is an ideal of $\mathbb{Z}[x]$.

ii) Since $0 \in S$, $S \neq \phi$.

If $f(x) = \sum_{i=0}^{n} 3a_i x^i$, $g(x) = \sum_{j=0}^{m} 3b_j x^j$ are in S, then you should show why $f(x) - g(x) \in S$.

Also, if $f(x) = \sum_{i=0}^{n} 3a_i x^i$ and $g(x) = \sum_{j=0}^{m} b_j x^j \in \mathbb{Z}[x]$, then

$f(x)g(x) = \sum_{k=0}^{m+n} \left(\sum_{i+j=k} 3a_i b_j \right) x^k \in S$.

Thus, S is an ideal of $\mathbb{Z}[x]$.

E7) Ra is a subring of R (see Example 9, Unit 11).

Also, for $r \in R$ and $xa \in Ra$,

$r(xa) = (rx)a \in Ra$.

$\therefore Ra$ is an ideal of R.

E8) $I \neq \phi$. Why? Doesn't $b \in I$?

Also, for $x, y \in I$, $ax \in bR$, $ay \in bR$.

Since bR is a subring of R, $a(x - y) = ax - ay \in bR$.

$\therefore x - y \in I$.

Next, if $x \in I$ and $r \in R$,

$a(xr) = (ax)r \in bRr = bR$.

So, $xr \in I$.

Thus, I is an ideal of R.

E9) You know that $<1> \subseteq R$. So, you need to show that $R \subseteq <1>$.
Now, for any $r \in R$, $r = r \cdot 1 \in <1>$. Thus, $R \subseteq <1>$.
$\therefore R = <1>$.

Next, since $u \in U(R)$, $\exists\ v \in R$ s.t. $uv = 1$. So $1 \in < u >$.
$\therefore <1> \subseteq < u >$, i.e., $R \subseteq < u >$.
But $< u > \subseteq R$, since $u \in R$.
Thus, $< u > = R$.

E10) The **subgroup** $< \mathbf{r} >$ of $(R, +)$ **is** $\mathbb{Z}\mathbf{r}$.
However, **the principal ideal is** $\mathbf{Rr}$.
So, for example, if $R = \mathbb{R}$ and $r = 5$, then the cyclic subgroup is $5\mathbb{Z}$.
However, since $5 \in U(\mathbb{R})$, $5\mathbb{R} = \mathbb{R}$ (by E9).
Note that $5\mathbb{Z} \neq \mathbb{R}$.

E11) $\overline{3}\mathbb{Z}_{10} = \{\overline{3}x \mid x \in \mathbb{Z}_{10}\} = \{\overline{0}, \overline{3}, \overline{6}, \overline{9}, \overline{12}, \overline{15}, \overline{18}, \overline{21}, \overline{24}, \overline{27}\}$
$= \{\overline{0}, \overline{3}, \overline{6}, \overline{9}, \overline{2}, \overline{5}, \overline{8}, \overline{1}, \overline{4}, \overline{7}\}$
$= \mathbb{Z}_{10}$.
$\overline{5}\mathbb{Z}_{10} = \{\overline{0}, \overline{5}\}$.
Now $\overline{2}\mathbb{Z}_{10} + \overline{3}\mathbb{Z}_{10} = \overline{2}\mathbb{Z}_{10} + \mathbb{Z}_{10} = \mathbb{Z}_{10}$, since $\overline{2}\mathbb{Z}_{10} \subseteq \mathbb{Z}_{10}$.
Thus, $< \overline{5} > \neq < \overline{2}, \overline{3} >$.

E12) You should prove this along the lines of Example 2, using E10 of Unit 11.

E13) Any element of $\wp(X)A$ is $YA = Y \cap A \in \wp(A)$, for $Y \in \wp(X)$.
So, $\wp(X)A \subseteq \wp(A)$.
Conversely, if $S \in \wp(A)$, then $S \in \wp(X)$ and $S = S \cap A \in \wp(X)A$.
So, $\wp(A) \subseteq \wp(X)A$.
Thus, $\wp(A) = \wp(X)A$.

E14) Let the nil radical of $\mathbb{Z}_8$ be N. Then $\overline{0} \in N$.
$\overline{1} \notin N$ since $(\overline{1})^n = \overline{1} \neq \overline{0}$ for all $n \in \mathbb{N}$.
Note that $\overline{a} \in N$ iff $a^n \in 8\mathbb{Z}$ (for some $n \in \mathbb{N}$) iff $8 \mid a^n$ (for some $n \in \mathbb{N}$) iff $2 \mid a^n$ (for some $n \in \mathbb{N}$) iff $2 \mid a$ (see Unit 1).
Thus, $\overline{2}, \overline{4}, \overline{6} \in N$ and $\overline{3}, \overline{5}, \overline{7} \notin N$.
$\therefore N = \{\overline{0}, \overline{2}, \overline{4}, \overline{6}\}$.

For any $A \in \wp(X)$, $A^n = A \cap A \cap ... \cap A = A\ \forall\ n \in \mathbb{N}$.
Thus, $A^n = \phi$ iff $A = \phi$.
Thus, the nil radical of $\wp(X)$ is $\{\phi\}$, the trivial ideal.

E15) Let $I = \text{Ann } a$. Firstly, $I \neq \phi$ since $0 \in I$.
Secondly, $r,\ s \in I \Rightarrow ra = 0 = sa \Rightarrow (r - s)a = 0 \Rightarrow r - s \in I$.

Finally, $r \in I$ and $x \in R \Rightarrow (rx)a = x(ra) = x \cdot 0 = 0 \Rightarrow rx \in I$.
Thus, I is an ideal of R.

$$\text{Ann } 0 = \{r \in R \mid r \cdot 0 = 0\} = R.$$

$$\text{Ann } 1 = \{r \in R \mid r \cdot 1 = 0\} = \{0\}.$$

E16) i) False, as you have seen in E15.

ii) Take 1 and 2 in $\mathbb{Z}$. Then $\text{Ann } 1 = \{0\} = \text{Ann } 2$, but $1 \neq 2$. So, this is false.

iii) As you have seen, the nil radicals of $\mathbb{Z}$ and $\mathbb{R}$ are both $\{0\}$. But $\mathbb{Z} \neq \mathbb{R}$. So this is false.

E17) As in Example 10, show that the only ideals of $\mathbb{R}$ are $\{0\}$ and $\mathbb{R}$; and those of $\mathbb{C}$ are $\{0\}$ and $\mathbb{C}$.

E18) i) Since $<\overline{4}> = \{\overline{0}, \overline{4}, \overline{8}\}$ and $<\overline{6}> = \{\overline{0}, \overline{6}\}$, $<\overline{4}> \cap <\overline{6}> = \{\overline{0}\}$.
Also $<\overline{4}> + <\overline{6}> = \{\overline{0}, \overline{2}, \overline{4}, \overline{6}, \overline{8}\} = <\overline{2}>$.
Here $IJ = \{ab \mid a \in I, b \in J\} = \{\overline{0}\}$, since $\overline{24} = \overline{0}$.

ii) $I \cap J = \{A \in \wp(Y) \mid A \cap Y = \phi\} = \{\phi\}$.
$I + J = \{A \Delta B \mid A \in I, B \in J\} = \{A \cup B \mid A \in I, B \in J\}$, since $A \subseteq Y$ and $B \subseteq Y^c$.
$IJ = \{(A_1 \cap B_1)\Delta(A_2 \cap B_2)\Delta \ldots \Delta(A_n \cap B_n) \mid A_i \in I, B_i \in J$ for $i = 1, \ldots, n, n \in \mathbb{N}\}$
$= \{\phi\}$, since $A_i \cap B_i = \phi \ \forall \ i = 1, \ldots, n$.

E19) i) For any $a \in I$ and $b \in J$, $ab \in I$ and $ab \in J$.
Thus, $ab \in I \cap J$.
Since $I \cap J$ is an ideal, any finite sum of such elements will also be in $I \cap J$.
Thus, $IJ \subseteq I \cap J$.
By definition, $I \cap J \subseteq I$ and $I \cap J \subseteq J$.
Also, $I \subseteq I + J, J \subseteq I + J$, since $x = x + 0 \in I + J$ and $y = 0 + y \in I + J$, for $x \in I$ and $y \in J$.

ii) Let A be an ideal of R containing I as well as J.
Then, for any $x + y \in I + J$, $x \in I \subseteq A$, $y \in J \subseteq A$. So $x + y \in A$.
Thus, $I + J \subseteq A$.
Thus, (ii) is proved.

iii) Let B be an ideal of R such that $B \subseteq I$ and $B \subseteq J$. Then certainly, $B \subseteq I \cap J$.
Thus, (iii) is proved.

iv) You know that $IJ \subseteq I \cap J$. So, you need to show that $I \cap J \subseteq IJ$.
Let $x \in I \cap J$. Then $x \in I$ and $x \in J$.

Since $1 \in R = I + J$, $1 = i + j$, for some $i \in I$ and $j \in J$.
Now $ix \in IJ$ since $i \in I$ and $x \in J$. Similarly, $xj \in IJ$. Therefore,
$x = x \cdot 1 = xi + xj \in IJ$.
Thus, $I \cap J \subseteq IJ$.

v) No. For example, let $R = 2\mathbb{Z}$, $I = 4\mathbb{Z}$, $J = 6\mathbb{Z}$.
Then $1 \notin R$.
Also, from Example 11, you know that $R = I + J$, $I \cap J = 12\mathbb{Z}$ and $IJ = 24\mathbb{Z}$.
Thus, $IJ \neq I \cap J$.

E20) 1) Since $I_1 \setminus I_2 \neq \phi$, the statement is correct.

2) False, for instance, $3 \in \mathbb{Z} \setminus 2\mathbb{Z}$, $1 \in \mathbb{Z} \setminus 2\mathbb{Z}$ but $3 - 1 = 2 \notin \mathbb{Z} \setminus 2\mathbb{Z}$.

3) False, for instance, $3 \in \mathbb{Z} \setminus 2\mathbb{Z}$, but $2 \cdot 3 = 6 \in 2\mathbb{Z}$.

4) This follows from (3), but (3) is false. Hence, this is false.

5) This follows from (2) and (4), which are false. Hence, this is false.

E21) Since $I_1 \setminus I_2$ is not a subring, as you have seen in Unit 11, it cannot be an ideal.

E22) i) Yes, because $I_1 = <\overline{3}> = \mathbb{Z}_{10}$, so that $I_1 \cup I_2 = \mathbb{Z}_{10}$.

ii) No. Note that $\overline{4}, \overline{5} \in I_2 \cup I_3 = \{\overline{0}, \overline{2}, \overline{4}, \overline{5}, \overline{6}, \overline{8}\}$, but $\overline{4} + \overline{5} \notin I_2 \cup I_3$.

E23) From Unit 11, you know that $I_1 \cup I_2$ is a subring of R iff $I_1 \subseteq I_2$ or $I_2 \subseteq I_1$. Once this condition is satisfied, $I_1 \cup I_2$ will certainly be an ideal of R.

E24) For instance, $\{0\} \times \mathbb{R} \times \mathbb{R} \times \mathbb{R}$, $\mathbb{R} \times \{0\} \times \mathbb{R} \times \mathbb{R}$ and $\mathbb{R} \times \mathbb{R} \times \mathbb{R} \times \{0\}$.
These are ideals of $\mathbb{R}^4 = \mathbb{R} \times \mathbb{R} \times \mathbb{R} \times \mathbb{R}$, since $\mathbb{R}$ and $\{0\}$ are ideals of $\mathbb{R}$. Each of these is non-trivial since the trivial ideal is $\{(0, 0, 0, 0)\}$.
Each of these is a proper ideal, since one component is not $\mathbb{R}$.

E25) In Unit 11, you have seen that $S = \{(n, n) \mid n \in \mathbb{Z}\}$ is a subring of $\mathbb{Z} \times \mathbb{Z}$.
However, $(1, 1) \in S$ and $(1, 2) \in \mathbb{Z} \times \mathbb{Z}$ such that $(1, 1)(1, 2) = (1, 2) \notin S$.
Thus, S is not an ideal of $\mathbb{Z} \times \mathbb{Z}$.
Similarly, you should show that for any non-trivial ring R,
$S = \{(x, x) \mid x \in R\}$ is not an ideal of $R \times R$.

E26) For instance, $< x > \times \{0\}$ and $\mathbb{Q}[x] \times \{0\}$.

E27) If R is a commutative ring, then R/I is a commutative ring. This is because $(a + I) \cdot (b + I) = ab + I = ba + I = (b + I) \cdot (a + I)$ for all $a + I, b + I \in R/I$.

E28) $1 + I$ is the identity of R/I, where 1 is the identity of R, since $(x + I) \cdot (1 + I) = x + I = (1 + I) \cdot (x + I)\ \forall\ x \in R$.

E29) You should show that $6\mathbb{Z}$ is an ideal of $2\mathbb{Z}$, and $2\mathbb{Z}/6\mathbb{Z} = \{6\mathbb{Z},\ 2+6\mathbb{Z},\ 4+6\mathbb{Z}\}$. Then the Cayley tables are:

$+$	$\bar{0}$	$\bar{2}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{2}$	$\bar{4}$
$\bar{2}$	$\bar{2}$	$\bar{4}$	$\bar{0}$
$\bar{4}$	$\bar{4}$	$\bar{0}$	$\bar{2}$

$\cdot$	$\bar{0}$	$\bar{2}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{2}$	$\bar{0}$	$\bar{4}$	$\bar{2}$
$\bar{4}$	$\bar{0}$	$\bar{2}$	$\bar{4}$

Show that $\mathbb{Z}_{14}/\bar{2}\mathbb{Z}_{14} = \{\bar{2}\mathbb{Z}_{14},\ \bar{1}+\bar{2}\mathbb{Z}_{14}\}$.

Then the tables are:

$+$	$\bar{0}$	$\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{1}$
$\bar{1}$	$\bar{1}$	$\bar{0}$

$\cdot$	$\bar{0}$	$\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$

E30) From Theorem 2, you know that $I = R$.
$\therefore R/I = \{\bar{0}\}$, where the bar denotes the corresponding coset of I.

E31) Suppose X is finite, $|X| = n$. Then $|Y| \le n-1$.
So $o(\wp(X)/\wp(Y)) \ge (2^n/2^{n-1}) = 2$.
If X is infinite, and Y is a finite subset, then $\wp(X)/\wp(Y)$ is an infinite ring.
In either case, $\exists\ a \in X \setminus Y$. So $\{a\}\Delta\wp(Y)$ is a non-zero coset. Thus, $\overline{\phi}$ and $\overline{\{a\}}$ are two distinct element of $\wp(X)/\wp(Y)$, the bar denoting the corresponding coset of $\wp(Y)$.

E32) Any element of $R = (\mathbb{Z}\times\mathbb{Z})/(<3>\times<5>)$ is of the form $(m, n) + (<3>\times<5>)$, for $m, n \in \mathbb{Z}$.
Now $\overline{(m, n)} = \overline{(a, b)}$ iff $(a-m) \in <3>$ and $(b-n) \in <5>$.
Thus, the distinct elements of R are
$\{0+3\mathbb{Z},\ 1+3\mathbb{Z},\ 2+3\mathbb{Z}\}\times\{0+5\mathbb{Z},\ 1+5\mathbb{Z},\ 2+5\mathbb{Z},\ 3+5\mathbb{Z},\ 4+5\mathbb{Z}\}$, i.e., all the elements of $\mathbb{Z}_3\times\mathbb{Z}_5$.
Hence, R has 15 elements. For example, two of them are $(0+3\mathbb{Z},\ 0+5\mathbb{Z})$ and $(2+3\mathbb{Z},\ 1+5\mathbb{Z})$.

E33) Let $x+N \in R/N$ be a nilpotent element.
Then $(x+N)^n = N$, for some positive integer n.
$\Rightarrow x^n \in N$, for some positive integer n.
$\Rightarrow (x^n)^m = 0$, for some positive integer m.
$\Rightarrow x^{nm} = 0$, for some positive integer nm.
$\Rightarrow x \in N$
$\Rightarrow x+N = 0+N$, the zero element of R/N.
Thus, R/N has no non-zero nilpotent element.

E34) Let $\bar{x} \in C(R/I)$. Then $\bar{x}\bar{r} = \bar{r}\bar{x}\ \forall\ \bar{r} \in R/I$, i.e., $(xr - rx) \in I\ \forall\ r \in R$.
$\therefore C(R/I) = \{x+I \in R/I \mid xr - rx \in I\ \forall\ r \in R\}$.

E35) Since $< 2, x >$ is an ideal of $\mathbb{Z}[x]$, containing $< x >$, $\frac{< 2, x >}{< x >}$ is an ideal of $\mathbb{Z}[x]/< x >$.

E36) Any ideal of $\mathbb{Z}/25\mathbb{Z}$ is of the form $n\mathbb{Z}/25\mathbb{Z}$, where $n \mid 25$.
Thus, $n = 1, 5, 25$.
Thus, you can pick any two out of these, say $n = 5$ and 25. The corresponding ideals of $\mathbb{Z}/25\mathbb{Z}$ will be $5\mathbb{Z}/25\mathbb{Z}$ and $\{\bar{0}\}$.
Note that they are distinct because, for example, you can check that their orders are different.

E37) Consider $A = \{1, 2, 3\}$ and $B = \{1, 2, 6, 7\}$. Then $\wp(A)$ and $\wp(B)$ are ideals of $\wp(X)$, each containing $\wp(Y)$.
Hence, $\wp(A)/\wp(Y)$ and $\wp(B)/\wp(Y)$ are ideals of $\wp(X)/\wp(Y)$.
Note that $o(\wp(A)/\wp(Y)) = \frac{2^3}{2^2} = 2$, and $o(\wp(B)/\wp(Y)) = \frac{2^4}{2^2} = 4$.
Thus, these two ideals are distinct.

E38) Since S and I are subrings of R, so is $S \cap I$.
Since $S \cap I \subseteq S$, $S \cap I$ is a subring of S.
Further, for $x \in S \cap I$ and $s \in S$, $xs \in S$ and $xs \in I$.
So $xs \in S \cap I$.
Similarly, $sx \in S \cap I$.
Thus, $S \cap I$ is an ideal of S.

For the example, consider $S = \mathbb{Z}$, $R = \mathbb{R}$, $I = \{0\}$.
Then $S \cap I = \{0\}$, so that $S/_{S \cap I} = \mathbb{Z}/_{\{0\}}$.
Since $\mathbb{Z}$ is not an ideal of $\mathbb{R}$, $\mathbb{Z}/\{0\}$ is not an ideal of $\mathbb{R}/\{0\}$.

UNIT 13

RING HOMOMORPHISMS

Structure | Page Nos.

13.1 INTRODUCTION

In Unit 8, you studied about functions between groups that preserve the binary operation. You also saw how useful they were for studying the algebraic structure of a group, and classifying groups accordingly. In this unit, we will discuss functions between rings which preserve both the binary operations. Such functions, as you would expect, are called ring homomorphisms.

In Sec.13.2, you will study the formal definition of a ring homomorphism. Of course, you will consider several examples, and non-examples of this concept too. In this section, you will also see how homomorphisms allow us to investigate the algebraic nature of a ring.

In Sec.13.3, you will study several properties of ring homomorphisms. Most of these properties will be analogous to those of group homomorphisms, that you have studied, and applied, in Unit 8.

If a homomorphism is a bijection, it is called an isomorphism. The role of isomorphisms in ring theory, as in group theory, is to identify algebraically identical systems. That is why they are important. We will introduce them to you in Sec.13.4. Then you will study the inter-relationship between ring homomorphisms, ideals and quotient rings in the form of the Fundamental Theorem of Homomorphism for rings. You will also study its applications for proving, and using, two other isomorphism theorems.

As in group theory, homomorphisms are crucially important for ring theory. Therefore, it is important that you study this unit carefully, and solve every exercise as you come to it. This will help you to achieve the following learning objectives.

Objectives

After studying this unit, you should be able to:

- define, and give examples of, different kinds of ring homomorphisms;
- obtain the kernel and image of any ring homomorphism;
- define, and give examples of, ring isomorphisms;
- prove, and apply, some basic properties of a ring homomorphism;
- state, prove and apply the Fundamental Theorem of Homomorphism for rings.

13.2 HOMOMORPHISMS BETWEEN RINGS

In Unit 8, you studied maps between groups that preserve the group operations of the domains concerned. These functions are called group homomorphisms, as you know. Analogous to the notion of a group homomorphism, we have the concept of a ring homomorphism. So it is natural to expect a ring homomorphism to be a map between rings that preserves the ring structure of its domain. In this case there are two binary operations involved. So, you may expect the following definition of a ring homomorphism.

Definition: Let $(R_1, +, \cdot)$ and $(R_2, +, \cdot)$ be two rings. A map $f : R_1 \to R_2$ is called a **ring homomorphism** if
$f(a+b) = f(a) + f(b)$, and
$f(a \cdot b) = f(a) \cdot f(b)$,
for all a, b in R_1.

Note that the $+$ and $\cdot$ occurring on the left hand sides of the equations in the definition above are defined on R_1, while the $+$ and $\cdot$ occurring on the right hand sides are defined on R_2.
Also note the following comment about the definition above.

Remark 1: Notice that $f : R_1 \to R_2$ is a ring homomorphism if

i) the image of a sum is the sum of the images, and

ii) the image of a product is the product of the images.

Because of (i) above, the ring homomorphism f is, in particular, a group homomorphism from $(R_1, +)$ to $(R_2, +)$.
Also, you know that $(R_1, \cdot)$ and $(R_2, \cdot)$ are semigroups. What (ii) above says is that f is a semigroup homomorphism from $(R_1, \cdot)$ to $(R_2, \cdot)$.

As in the case of groups, we have different types of homomorphisms.

Definitions: Let $f : R_1 \to R_2$ be a ring homomorphism.

i) If f is 1-1, it is called a **ring monomorphism**.

ii) If f is surjective, it is called a **ring epimorphism**.

iii) If f is bijective, it is called a **ring isomorphism**.

iv) If $R_1 = R_2$, then f is called a **ring endomorphism** of R_1.

Consider a remark about the definitions above.

Remark 2: The word 'ring' in each definition, is just to emphasise that we are working in the context of rings. If this context is clear, we drop the word 'ring'. Thus, in future **we will use the term 'homomorphism' for 'ring homomorphism'**, if the context is clear. You may remember that we also did this in the case of group homomorphisms.

Let us consider some examples, and non-examples, of the functions we have just defined.

Example 1: Consider $f:\mathbb{Z}\to\mathbb{Z}: f(x)=x,\ g:\mathbb{Z}\to\mathbb{Z}: g(x)=2x,$ and let $h=-f$. Check whether f, g and h are ring homomorphisms or not.

Solution: First, you should verify that f, g and h are well-defined.

Next, for $n, m\in\mathbb{Z}, f(n+m)=n+m=f(n)+f(m),$ and
$f(nm)=nm=f(n)f(m).$
Thus, f is a ring homomorphism.

Now let us consider g.
For $n, m\in\mathbb{Z}, g(n+m)=2(n+m)=2n+2m=g(n)+g(m).$
However, $g(nm)=2nm\neq(2n)(2m).$
For instance, $g(2\cdot3)=g(6)=12.$ But $g(2)g(3)=4\cdot6=24.$
So $g(2\cdot3)\neq g(2)g(3).$
Hence, g is not a ring homomorphism.

Finally, you should verify that $(-f)$ is also not a ring homomorphism, since it does not preserve multiplication.

***

Some important points show up in the example above. We note them in the following remark.

Remark 3: Consider the three points below, about f, g and h of Example 1.

i) If f is a group homomorphism, so is $-f$. However, this is not true for ring homomorphisms.

ii) f is, in fact, bijective, and is **the identity homomorphism**. We usually denote f by $\mathbf{I}$.

iii) Though g is a group homomorphism from $(\mathbb{Z}, +)$ to $(\mathbb{Z}, +),$ it is not a ring homomorphism.

Now consider another example.

Example 2: Consider $f:\mathbb{M}_n(\mathbb{R})\to\mathbb{M}_n(\mathbb{R}): f(A)=\mathbf{0},$ the zero matrix in $\mathbb{M}_n(\mathbb{R})$. Check whether f is a ring isomorphism or not.

Solution: For $A, B\in\mathbb{M}_n(\mathbb{R}), f(A+B)=\mathbf{0}=\mathbf{0}+\mathbf{0}=f(A)+f(B),$ and
$f(AB)=\mathbf{0}=\mathbf{0}\cdot\mathbf{0}=f(A)\cdot f(B).$
Thus, f is a ring homomorphism.
However, f is not surjective, since for example, there is no $A\in\mathbb{M}_n(\mathbb{R})$ for which $f(A)=I,$ the identity matrix in $\mathbb{M}_n(\mathbb{R})$.
Therefore, f is not an isomorphism.

***

Let us now generalise some of the points made in the examples above.

Example 3: Let R be a ring. Show that $I: R \to R : I(r) = r$ and $\mathbf{0}: R \to R: \mathbf{0}(r) = 0$ are endomorphisms. (I is called the **identity homomorphism**, as noted for $\mathbb{Z}$ in Remark 3. $\mathbf{0}$ is called the **trivial homomorphism**.)

Solution: You should verify that both I and $\mathbf{0}$ preserve both the operations of R.

***

Before going further, let us consider the kernel and image of a ring homomorphism. In Unit 8, you have studied these objects for a group homomorphism. Do you expect the kernel, or image, of a ring homomorphism to be defined any differently? Actually, they are defined in the same way.

Definition: Let R_1 and R_2 be two rings, and let $f: R_1 \to R_2$ be a ring homomorphism. Then we define

Note that $\text{Im } f \subseteq R_2$ and $\text{Ker } f \subseteq R_1$.

i) the **image of f** to be the set $\mathbf{Im\ f} = \{f(x) \mid x \in R_1\}$.

ii) the **kernel of f** to be the set $\mathbf{Ker\ f} = \{x \in R_1 \mid f(x) = 0\}$.

You know that if f is an epimorphism, $\text{Im } f = R_2$.

Now let us look at some examples of the image and kernel of a ring homomorphism.

Example 4: Let R be a ring. Obtain the kernels and images of the identity homomorphism and the trivial homomorphism, defined in Example 3.

Solution: $\text{Ker } I = \{x \in R \mid I(x) = 0\} = \{x \in R \mid x = 0\}$

$= \{0\}.$

$\text{Im } I = \{I(x) \mid x \in R\} = \{x \mid x \in R\}$

$= R.$

$\text{Ker } \mathbf{0} = \{x \in R \mid \mathbf{0}(x) = 0\} = R.$

$\text{Im } \mathbf{0} = \{\mathbf{0}(x) \mid x \in R\} = \{0\}.$

***

Example 5: Let $s \in \mathbb{N}$. Show that the map $f: \mathbb{Z} \to \mathbb{Z}_s : f(m) = \overline{m}$ is a ring epimorphism. Obtain $\text{Ker } f$ also.

Solution: For any $m, n \in \mathbb{Z}$,

$f(m+n) = \overline{m+n} = \overline{m} + \overline{n} = f(m) + f(n)$, and

$f(mn) = \overline{mn} = \overline{m}\,\overline{n} = f(m)\,f(n).$

Therefore, f is a ring homomorphism.

Further, $\text{Im } f = \{f(m) \mid m \in \mathbb{Z}\}$

$= \{\overline{m} \mid m \in \mathbb{Z}\}$

$= \mathbb{Z}_s,$

showing that f is an epimorphism.

Now, $\text{Ker } f = \{m \in \mathbb{Z} \mid f(m) = \overline{0}\}$

$= \{m \in \mathbb{Z} \mid \overline{m} = \overline{0}\}$

$= \{m \in \mathbb{Z} \mid m \equiv 0 (\text{mod } s)\}$

$= s\mathbb{Z}$.

***

Example 6: Consider the maps $f: \mathbb{Z}_6 \to \mathbb{Z}_3 : f(n \,(\text{mod } 6)) = n (\text{mod } 3)$ and $g: \mathbb{Z}_3 \to \mathbb{Z}_6 : g(n(\text{mod } 3)) = n(\text{mod } 6)$. Check whether or not f and g are ring homomorphisms. If they are, find their kernels and images.

Solution: First, for $n, m \in \mathbb{Z}$,

$n(\text{mod } 6) = m(\text{mod } 6)$

$\Rightarrow 6 \mid (n - m)$

$\Rightarrow 3 \mid (n - m)$

$\Rightarrow n(\text{mod } 3) = m(\text{mod } 3)$

$\Rightarrow f(n) = f(m)$.

So, f is well-defined.

Second, for $n, m \in \mathbb{Z}$,

$$f(n(\text{mod } 6) + m(\text{mod } 6)) = f((n + m)(\text{mod } 6)) = (n + m)(\text{mod } 3)$$
$$= n(\text{mod } 3) + m(\text{mod } 3)$$
$$= f(n(\text{mod } 6)) + f(m(\text{mod } 6))$$

You should, similarly, show that

$f(n(\text{mod } 6) \cdot m(\text{mod } 6)) = f(n(\text{mod } 6)) \cdot f(m(\text{mod } 6))$.

Thus, f is a ring homomorphism.

$\text{Ker } f = \{n(\text{mod } 6) \mid n \equiv 0(\text{mod } 3)\} = \{n(\text{mod } 6) \mid n \in 3\mathbb{Z}\}$

$= \{\overline{0}, \overline{3}\}$, bar denoting '$\text{mod } 6$'.

$= \overline{3}\mathbb{Z}_6$.

$\text{Im } f = \{n(\text{mod } 3) \mid \overline{n} \in \mathbb{Z}_6\} = \mathbb{Z}_3$.

Now, let's see if g is well-defined. Note that $\overline{1} = \overline{4}$ in $\mathbb{Z}_3$, but $g(\overline{1}) \neq g(\overline{4})$ in $\mathbb{Z}_6$. Hence, g is not well-defined. Thus, there is no question of g being a homomorphism.

***

By observing the examples above, you may have observed what we are now going to note.

Remark 4: The kernel and image of a ring homomorphism f, from R_1 to R_2, are the same as the kernel and image of f, as a group homomorphism from $(R_1, +)$ to $(R_2, +)$.

Before we look at some more examples, why don't you solve some exercises? This will help you check how well you have understood what has been discussed so far.

Note that using E1 we know that $f:\mathbb{Z}\to\mathbb{Q}$ (or $\mathbb{R}$, or $\mathbb{C}$, or $\mathbb{Z}+i\mathbb{Z}$), given by $f(n) = n$, is a ring homomorphism.

E1) If S is a subring of a ring R, then S is a ring with respect to the $+$ and $\cdot$ of R. Show that the inclusion map $i:S\to R:i(x)=x$ is a homomorphism. What are $\text{Ker } i$ and $\text{Im } i$?

E2) i) Show that $\phi:\mathbb{Z}[x]\to\mathbb{Z}:\phi(f(x))=f(1)$ is a homomorphism. Find $\text{Ker }\phi$ and $\text{Im }\phi$ also. (ϕ is called the **evaluation map at $x=1$**.)

ii) For any $z\in\mathbb{C}$, show that the evaluation map $\phi_z:\mathbb{C}[x]\to\mathbb{C}:\phi_z(f(x))=f(z)$ is a homomorphism. Also find $\text{Ker }\phi_z$ and $\text{Im }\phi_z$.

E3) Consider $\phi:\mathbb{H}\to\mathbb{R}:\phi(a+ib+jc+kd)=a$. Check whether or not ϕ is a homomorphism.

E4) Consider $\psi:\mathbb{M}_2(\mathbb{C})\to\mathbb{C}:\psi(A)=\det(A)$. Check whether or not ψ is a homomorphism.

E5) Consider $f:\mathbb{Z}_3\to\mathbb{Z}_6:f(n(\text{mod }3))=4n(\text{mod }6)$. Check whether or not f is a ring homomorphism.

Now let us look at some more examples.

ϕ, in Example 7, is called the **evaluation map** at the point $x=\frac{1}{2}$.

Example 7: Consider the ring $C[0,1]$ of all real-valued continuous functions defined on the closed interval $[0,1]$. Define $\phi:C[0,1]\to\mathbb{R}:\phi(f)=f(1/2)$. Show that ϕ is an epimorphism. Is ϕ a monomorphism?

Solution: Let f and $g\in C[0,1]$. Then $+$ and $\cdot$ are defined by
$(f+g)(x)=f(x)+g(x)$, and
$(f\cdot g)(x)=f(x)g(x)$,
for all $x\in[0,1]$.
Now, $\phi(f+g)=(f+g)(1/2)=f(1/2)+g(1/2)=\phi(f)+\phi(g)$, and
$\phi(fg)=(fg)(1/2)=f(1/2)\,g(1/2)=\phi(f)\,\phi(g)$.
Thus, ϕ is a ring homomorphism.

Now, ϕ is onto because for any $r\in\mathbb{R}$, consider the constant function
$g:[0,1]\to\mathbb{R}:g(x)=r$.
From Calculus, you know that g is continuous on $[0,1]$. Also $g(1/2)=r$.
Thus, $\phi(g)=r$.
Hence, ϕ is an epimorphism.

However, ϕ is not 1-1. For example, if $f:[0,1]\to\mathbb{R}:f(x)=x-\frac{1}{2}$, and g is the zero function, then $\phi(f)=\phi(g)$, but $f\neq g$.

***

Example 8: Consider the ring $R=\left\{\begin{bmatrix}a & 0\\ 0 & b\end{bmatrix}\middle|\, a,b\in\mathbb{R}\right\}$ under matrix addition

and multiplication. Show that the map $f : \mathbb{Z} \to R : f(n) = \begin{bmatrix} n & 0 \\ 0 & n \end{bmatrix}$ is a homomorphism. Also find $\text{Ker } f$. Is f an epimorphism?

Solution: Note that f is well-defined since, if $n = m$, then $\begin{bmatrix} n & 0 \\ 0 & n \end{bmatrix} = \begin{bmatrix} m & 0 \\ 0 & m \end{bmatrix}$.

Next, for $n, m \in \mathbb{Z}$,

$f(n+m) = \begin{bmatrix} n+m & 0 \\ 0 & n+m \end{bmatrix} = \begin{bmatrix} n & 0 \\ 0 & n \end{bmatrix} + \begin{bmatrix} m & 0 \\ 0 & m \end{bmatrix} = f(n) + f(m)$, and

$f(nm) = f(n)\,f(m)$. (Verify this!)

Thus, f is a homomorphism.

$\text{Ker } f = \{n \in \mathbb{Z} \mid f(n) = \mathbf{0}\} = \{0\}$.

Finally, consider $A = \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}$. This is not in $\text{Im } f$, since its $(1, 1)$th and $(2, 2)$th elements are different. However, A is in R.

Hence, f is not an epimorphism.

***

Example 9: Consider the ring $(\wp(X), \Delta, \cap)$, where X is a non-empty set having a non-empty proper subset Y.
Define $f : \wp(X) \to \wp(Y) : f(A) = A \cap Y$. Show that f is a homomorphism.
Does $Y^c \in \text{Ker } f$? What is $\wp(Y) \setminus \text{Im } f$?

Solution: If A and B are in $\wp(X)$ s.t. $A = B$, then $A \cap Y = B \cap Y$. Thus, f is well-defined.

Now, recall from Block 1 of Calculus, that 'intersection' distributes over 'union' and over 'complementation'. We will use these properties now.

For $A, B \in \wp(X)$,

$$\begin{aligned} f(A \Delta B) &= f((A \setminus B) \cup (B \setminus A)) \\ &= ((A \setminus B) \cup (B \setminus A)) \cap Y \\ &= ((A \setminus B) \cap Y) \cup ((B \setminus A) \cap Y) \\ &= ((A \cap Y) \setminus (B \cap Y)) \cup ((B \cap Y) \setminus (A \cap Y)) \\ &= (f(A) \setminus f(B)) \cup (f(B) \setminus f(A)) \\ &= f(A) \Delta f(B), \text{ and} \end{aligned}$$

$$\begin{aligned} f(A \cap B) &= (A \cap B) \cap Y \\ &= (A \cap B) \cap (Y \cap Y), \text{ since } Y \cap Y = Y. \\ &= (A \cap Y) \cap (B \cap Y), \text{ since } \cap \text{ is associative and commutative.} \\ &= f(A) \cap f(B). \end{aligned}$$

So, f is a ring homomorphism from $\wp(X)$ to $\wp(Y)$.

Next, recall that the zero element of $\wp(Y)$ is $\emptyset$. Therefore,

$\text{Ker } f = \{A \in \wp(X) \mid A \cap Y = \emptyset\} = \{A \in \wp(X) \mid A \subseteq Y^c\} = \wp(Y^c)$.

$\therefore Y^c \in \text{Ker } f$.

Finally, to see what $\wp(Y) \setminus \text{Im } f$ is, note that

$\text{Im } f = \{A \cap Y \mid A \in \wp(X)\} \subseteq \wp(Y)$.

Now, let $B \in \wp(Y)$. Then $B \in \wp(X)$ and $f(B) = B \cap Y = B$. Thus, $B \in \text{Im } f$.

So $\wp(Y) \subseteq \text{Im } f$.

Therefore, $\text{Im } f = \wp(Y)$.

Hence, $\wp(Y) \setminus \text{Im } f = \phi$.

***

Now, you should solve the following exercises to get some more examples (and non-examples!) of homomorphisms.

E6) Let A and B be two rings. Show that the **projection map** $p : A \times B \to A : p(x, y) = x$ is a homomorphism. What are $\text{Ker } p$ and $\text{Im } p$? Is p an isomorphism?
(Similarly, $p' : A \times B \to B : p'(x, y) = y$ is a homomorphism.)

E7) Is $f : \mathbb{Z}[\sqrt{2}] \to \mathbb{Z}[\sqrt{2}] : f(a + \sqrt{2}b) = a - \sqrt{2}b$ a ring endomorphism?
Is $g : \mathbb{Q}[\sqrt{3}] \to \mathbb{Q}[\sqrt{7}] : g(a + b\sqrt{3}) = a + b\sqrt{7}$ a ring homomorphism?
Give reasons for your answers.

E8) Check whether or not $f : 3\mathbb{Z} \to 5\mathbb{Z} : f(3n) = 5n$ is a homomorphism.

E9) Check whether or not $\phi : \mathbb{C} \to R : \phi(a + ib) = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}$ is an isomorphism, where $R = \left\{ \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \middle| a, b \in \mathbb{R} \right\}$ is a subring of $\mathbb{M}_2(\mathbb{R})$.

E10) Show that the map $\phi : C[0,1] \to \mathbb{R} \times \mathbb{R} : \phi(f) = (f(0), f(1))$ is a homomorphism. Also check if ϕ is an isomorphism or not.

Having discussed many examples, let us look at some elementary properties of ring homomorphisms.

13.3 PROPERTIES OF RING HOMOMORPHISMS

Let us start this section by revisiting each of the examples of homomorphisms you have studied in the previous section. In all these cases, what is the image of the additive identity of the domain ring? Isn't it the additive identity of the co-domain? Isn't this to be expected since every ring homomorphism is also a group homomorphism? In fact, every ring homomorphism will satisfy all the properties listed in the following theorem for this reason.

Theorem 1: Let $f : R_1 \to R_2$ be a ring homomorphism. Then

i) $f(0) = 0$,

ii) $f(-x) = -f(x) \; \forall \; x \in R_1$, and

iii) $f(x - y) = f(x) - f(y) \; \forall \; x, y \in R_1$.

Proof: Since f is a group homomorphism from $(R_1, +)$ to $(R_2, +)$, you can apply Theorem 1, Unit 8, to get the result. ■

Now let us consider some properties beyond just the group homomorphism aspect of a ring homomorphism.

Theorem 2: Let R_1 be a ring with identity, and let $f: R_1 \to R_2$ be a ring **epi**morphism, where $R_2 \neq \{0\}$. Then

i) R_2 is with identity, $f(1)$; and

ii) if $u \in U(R_1)$, then $f(u) \in U(R_2)$ and $[f(u)]^{-1} = f(u^{-1})$.

Proof: Here note that R_1 is with identity and f is surjective.

i) Let $r \in R_2$. Since f is surjective, $\exists\, s \in R_1$ s.t. $f(s) = r$.
Then $r \cdot f(1) = f(s)f(1) = f(s \cdot 1) = f(s) = r$.
Similarly, $f(1)r = r$.
Hence, $f(1)$ is the identity of R_2.

ii) Let $u \in U(R_1)$. Then $\exists\, u^{-1} \in R_1$ s.t. $uu^{-1} = 1 = u^{-1}u$.
So $f(uu^{-1}) = f(1)$, that is, $f(u)f(u^{-1}) = f(1) = f(u^{-1})f(u)$.
Thus, $f(u) \in U(R_2)$ and $[f(u)]^{-1} = f(u^{-1})$. ■

Because of Theorem 2, we know that for any onto homomorphism $f: R \to \mathbb{Z}$, where R is a ring with unity, $f(1) = 1$. Similarly, if $f: R \to \mathbb{Q}$ is a ring epimorphism, where R has unity, then $f(1) = 1$.

Note that Theorem 2 need not be true if f is not surjective. For instance, take the trivial homomorphism of Example 2. Then $f(I) = \mathbf{0} \neq I$.

Now, let us look at direct and inverse images of subrings under homomorphisms.

Theorem 3: Let $f: R_1 \to R_2$ be a ring homomorphism. Then

i) if S is a subring of R_1, $f(S)$ is a subring of R_2; and

ii) if T is a subring of R_2, $f^{-1}(T)$ is a subring of R_1.

Proof: We will prove (ii) and leave the proof of (i) to you (see E11).
Firstly, since $T \neq \phi$, $f^{-1}(T) \neq \phi$.
Next, let $a, b \in f^{-1}(T)$. Then $f(a), f(b) \in T$.
$\Rightarrow f(a) - f(b) \in T$ and $f(a)f(b) \in T$, since T is a subring of R_2.
$\Rightarrow f(a - b) \in T$ (by Theorem 1), and $f(ab) \in T$.
$\Rightarrow a - b \in f^{-1}(T)$ and $ab \in f^{-1}(T)$.
$\Rightarrow f^{-1}(T)$ is a subring of R_1, by the subring test. ■

To complete the proof of Theorem 3, you need to solve E11.

E11) Prove (i) of Theorem 3.

E12) In the setting of Theorem 3, let $\mathcal{A}$ and $\mathcal{B}$ be the set of subrings of R_1 and the set of subrings of R_2, respectively. Then show that there is a correspondence $\phi : \mathcal{A} \to \mathcal{B}$. Is ϕ a bijection? Why, or why not?

Now, it is natural to expect an analogue of Theorem 3 for ideals. In fact, (ii) follows through for ideals too. But, regarding (i), consider the following remark.

Remark 5: The image of an ideal under a ring homomorphism need not be an ideal. For instance, consider the inclusion $i : \mathbb{Z} \to \mathbb{R} : i(x) = x$. You know that $\mathbb{Z}$ is an ideal of $\mathbb{Z}$. But is $i(\mathbb{Z})$ (i.e., $\mathbb{Z}$) an ideal of $\mathbb{R}$? No, as you have seen in Unit 12.

So, regarding ideals, we have the following result, for **any** two rings R_1 and R_2, commutative or not.

Theorem 4: Let $f : R_1 \to R_2$ be a ring homomorphism.

i) If f is surjective and I is an ideal of R_1, then $f(I)$ is an ideal of R_2.

ii) If I is an ideal of R_2, then $f^{-1}(I)$ is an ideal of R_1, and $\text{Ker } f \subseteq f^{-1}(I)$.

Proof: Here we will prove (i) and leave (ii) to you (see E13).
Firstly, since I is a subring of R_1, $f(I)$ is a subring of R_2, by Theorem 3.

Secondly, take any $f(x) \in f(I)$ and $r \in R_2$.
Since f is surjective, $\exists\, s \in R_1$ such that $f(s) = r$. Then
$r \cdot f(x) = f(s) f(x) = f(sx) \in f(I)$, since $sx \in I$.
Similarly, $f(x) \cdot r \in f(I)$.
Thus, $f(I)$ is an ideal of R_2. ■

The proof of Theorem 4 will be complete, once you solve E13 below.

E13) Prove (ii) of Theorem 4.

E14) Let $f : R \to S$ be a surjection. Then for any non-empty subset J of S, $f(f^{-1}(J)) = J$. In particular, if f is an onto ring homomorphism and J is an ideal of S, then $f(f^{-1}(J)) = J$.

Now, consider a ring epimorphism $f : R \to S$ and an ideal I in R. In E14, you have proved that if J is an ideal of S, then $J = f(f^{-1}(J))$. Also, in this setting, by Theorem 4 you know that $f(I)$ is an ideal of S and $f^{-1}(f(I))$ is an ideal of R. So, is $I = f^{-1}(f(I))$?
For instance, consider $f : \mathbb{Z} \to \mathbb{Z}_5 : f(m) = \overline{m}$ (see Example 5). Here f is a surjection. Take $I = 2\mathbb{Z}$. Then $5 \notin I$. But $5 \in f^{-1}(f(I))$, since $f(5) = \overline{0} \in f(I)$. So $I \neq f^{-1}(f(I))$.

But looking at the two ideals, I and $f^{-1}(f(I))$, in R, it seems that there should be some relationship between them. What could it be? You will find the answer in the following theorem.

Theorem 5: Let $f: R \to S$ be a ring homomorphism, and let I be an ideal of R. Then $f^{-1}(f(I)) = I + \text{Ker } f$.

Proof: You know that $\text{Ker } f = f^{-1}(\{0\}) \subseteq f^{-1}(f(I))$, since $0 \in f(I)$.
Also, if $x \in I$, then $f(x) \in f(I)$. So $x \in f^{-1}(f(I))$. Hence, $I \subseteq f^{-1}(f(I))$.
Thus, $I + \text{Ker } f \subseteq f^{-1}(f(I))$. …(1)

Now, to show $f^{-1}(f(I)) \subseteq I + \text{Ker } f$, let $x \in f^{-1}(f(I))$. Then
$f(x) \in f(I)$
$\Rightarrow f(x) = f(y)$, for some $y \in I$.
$\Rightarrow f(x - y) = 0$, by Theorem 1.
$\Rightarrow x - y \in \text{Ker } f$
$\Rightarrow x \in y + \text{Ker } f \subseteq I + \text{Ker } f$.
$\therefore f^{-1}(f(I)) \subseteq I + \text{Ker } f$. …(2)

From (1) and (2), we conclude that $f^{-1}(f(I)) = I + \text{Ker } f$. ■

An immediate corollary to Theorem 5 is the following.

Corollary 1: If $f: R \to S$ is a ring homomorphism, and I is an ideal of R containing $\text{Ker } f$, then $f^{-1}(f(I)) = I$.

Proof: Since $\text{Ker } f \subseteq I$, $I + \text{Ker } f = I$.
$\therefore f^{-1}(f(I)) = I$. ■

Regarding Theorem 5, consider the following important comment.

Remark 6: Note that Theorem 5 is true whether f is surjective or not. In this theorem, and in Corollary 1, we treat $f(I)$ as a subring only, by Theorem 3. If we want $f(I)$ to be an ideal, then we will have to add the condition that f is a surjection.

Now, in E12 you have seen that if $f: R \to S$ is a homomorphism, there is a correspondence between the subrings of R and the subrings of S. But this is not a 1-to-1 correspondence. Let us use Theorems 4 and 5 to see what the situation is regarding the ideals of R and S. Consider the following theorem.

Theorem 6: Let $f: R \to S$ be an **onto** ring homomorphism. Then $I \mapsto f(I)$ defines a one-to-one correspondence between the set of ideals of R containing $\text{Ker } f$ and the set of ideals of S.

Proof: Let $\mathcal{A}$ be the set of ideals of R containing $\text{Ker } f$, and $\mathcal{B}$ be the set of ideals of S.
Define $\phi: \mathcal{A} \to \mathcal{B}: \phi(I) = f(I)$.

We want to show that ϕ is a bijection.

ϕ is onto: If $J \in \mathcal{B}$, then $f^{-1}(J) \in \mathcal{A}$ and $\text{Ker } f \subseteq f^{-1}(J)$, by Theorem 4.
Now, $\phi(f^{-1}(J)) = f(f^{-1}(J)) = J$, using E14.
Hence, ϕ is surjective.

ϕ is one-one: If I_1 and I_2 are in $\mathcal{A}$, then

$$\phi(I_1) = \phi(I_2) \Rightarrow f(I_1) = f(I_2)$$
$$\Rightarrow f^{-1}(f(I_1)) = f^{-1}(f(I_2))$$
$$\Rightarrow I_1 = I_2, \text{ by Corollary 1.}$$

Thus, ϕ is bijective. ■

Let us consider an example of the utility of Theorem 6.

Example 10: Find the kernel of the homomorphism $f: \mathbb{Z} \to \mathbb{Z}_{12} : f(z) = \bar{z}$. Also find all the ideals of $\mathbb{Z}_{12}$.

Solution: $\text{Ker } f = \{n \in \mathbb{Z} \mid n \equiv 0 \pmod{12}\} = 12\mathbb{Z}$.
Now, you know that any ideal of $\mathbb{Z}$ is of the form $n\mathbb{Z}, n \in \mathbb{N}$. Thus, the ideals of $\mathbb{Z}$ containing $\text{Ker } f$ are of the form $n\mathbb{Z}$ such that $n \mid 12$, i.e., for which $n = 1, 2, 3, 4, 6, 12$. These are $\mathbb{Z}$, $2\mathbb{Z}$, $3\mathbb{Z}$, $4\mathbb{Z}$, $6\mathbb{Z}$, $12\mathbb{Z}$.
Thus, by Theorem 6, the ideals of $\mathbb{Z}_{12}$ are $\mathbb{Z}_{12}$, $\bar{2}\mathbb{Z}_{12}$, $\bar{3}\mathbb{Z}_{12}$, $\bar{4}\mathbb{Z}_{12}$, $\bar{6}\mathbb{Z}_{12}$ and $\{\bar{0}\}$.

***

Now, you should solve some related exercises.

E15) Verify Theorem 5 for $f: \mathbb{Z} \to \mathbb{Z}_5 : f(n) = n \pmod 5$, and $I = 2\mathbb{Z}$.
Also verify it for the trivial homomorphism in Example 3.

E16) What does Theorem 6 say in the context of Example 7?

E17) i) Show that $f: \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z} : f(n) = (n, n)$ is not an epimorphism.

ii) Find an ideal in $\mathbb{Z} \times \mathbb{Z}$ which is not of the form $f(I)$, where I is an ideal of $\mathbb{Z}$.

E18) Check if $g: \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z} : g(n) = (n, 0)$ is a ring homomorphism or not. Further, is g onto? Is $g(I)$ an ideal of $\mathbb{Z} \times \mathbb{Z}$, for every ideal I of $\mathbb{Z}$? Does this counter Theorem 4? Why, or why not?

E19) Is every ideal of $\mathbb{Z}_n$ a principal ideal, for any $n \in \mathbb{N}$? Use Theorem 6 to decide this.

And now let us look closely at the sets $\text{Ker } f$ and $\text{Im } f$, where f is a ring homomorphism. In Unit 8, we proved that if $f: G_1 \to G_2$ is a group homomorphism, then $\text{Ker } f$ is a normal subgroup of G_1 and $\text{Im } f$ is a

subgroup of G_2. We have an analogous result for ring homomorphisms, which you may have already realised from the examples you have studied so far.

Theorem 7: Let $f: R_1 \to R_2$ be a ring homomorphism. Then

i) $\text{Ker } f$ is an ideal of R_1, and

ii) $\text{Im } f$ is a subring of R_2.

Proof: i) Since $\{0\}$ is an ideal of R_2, by Theorem 4(ii) you know that $f^{-1}(\{0\})$ is an ideal of R_1.
As $f^{-1}(\{0\}) = \text{Ker } f$, $\text{Ker } f$ is an ideal of R_1.

ii) Since R_1 is a subring of R_1, $f(R_1)$ is a subring of R_2, by Theorem 3(i).
Thus, $\text{Im } f$ is a subring of R_2. ■

Theorem 7 is very useful for showing that certain sets are ideals. For example, from Theorem 7 and Example 9, you can immediately find a non-trivial proper ideal of $\wp(X)$, for any X having at least two elements.
Similarly, from Example 7, you can see that $\{f \in C[0, 1] \mid f(1/2) = 0\}$ is a non-trivial ideal of $C[0, 1]$.
As we go along, you will see more examples of this use of Theorem 7. For now, let us examine the kernel of a homomorphism some more. In fact, let us prove a result which is actually a corollary of Theorem 4 of Unit 8.

Theorem 8: Let $f: R_1 \to R_2$ be a homomorphism. Then f is injective iff $\text{Ker } f = \{0\}$.

Proof: Note that $f: R_1 \to R_2$ is injective iff $f: (R_1, +) \to (R_2, +)$ is an injective group homomorphism, that is, iff $\text{Ker } f = \{0\}$, by Theorem 4 of Unit 8.
Hence, the result is proved. ■

As an example of the application of Theorem 8, you can immediately tell that f (in Example 9) is not injective.

Solve the following exercises now.

E20) Which of the homomorphisms in Examples 1-8 are 1-1?

E21) Which of the homomorphisms in E1-E7 are 1-1?

E22) Check whether or not the following are ring homomorphisms. For those that are, find $\text{Ker } \phi$ and $\text{Im } \phi$. Hence decide if ϕ is an isomorphism or not.

i) $\phi: \mathbb{R} \to \mathbb{M}_2(\mathbb{R}): \phi(x) = \begin{bmatrix} x & 0 \\ -x & 0 \end{bmatrix}$,

ii) $\phi: \mathbb{Z}_3 \to \mathbb{Z}_3: \phi(\bar{n}) = \bar{n}^3$.

Now let us look at another aspect of homomorphisms. You know, from Unit 8, that given a subgroup H of $(R, +)$, you can define a group homomorphism

$f:(R,+)\to(S,+)$ with $\text{Ker } f = H$. You have also seen that given a ring homomorphism $f: R \to S$, you obtain an ideal of R corresponding to f, namely, $\text{Ker } f$. So, the question is, given an ideal I of a ring R, can you define a ring homomorphism f so that $\text{Ker } f = I$?

The following theorem answers this question. Before studying it, though, please refresh your mind about the definition of a quotient ring from Unit 12. Also remember that quotient rings are defined for any ring.

Theorem 9: If I is an ideal of a ring R, then there exists a ring S and a surjective ring homomorphism $f: R \to S$ whose kernel is I.

Proof: Let $S = R/I$, which is well-defined as I is an ideal of R. We define $f: R \to R/I : f(a) = a + I$.

Let us see if f is a well-defined homomorphism.

If $a = b$ in R, then $a + I = b + I$, i.e., $f(a) = f(b)$ in R/I.

Hence, f is well-defined.

Next, for $a, b \in R$,

$f(a+b) = (a+b) + I = (a+I) + (b+I) = f(a) + f(b)$, and

$f(ab) = ab + I = (a+I)(b+I) = f(a)\,f(b)$.

Thus, f is a homomorphism.

Further, $\text{Ker } f = \{a \in R \mid f(a) = I\}$ (Remember, I is the zero element of R/I.)

$$= \{a \in R \mid a + I = I\}$$

$$= \{a \in R \mid a \in I\}$$

$$= I.$$

$\text{Im } f = \{r + I \mid r \in R\} = R/I$.

Thus, f is surjective.

Hence, the theorem is proved. ■

The homomorphism defined in the proof above is called **the canonical** (or **natural**) homomorphism from R onto R/I. You have already studied its analogue for groups in Unit 8. As in the case of groups, you will find the theorem above used a lot in the next section.

Try a couple of related exercises now.

E23) Will the statement in Theorem 9 still be true if we replace 'ideal' by 'subring' in it? That is, if S is a subring of a ring R, can we always define a ring homomorphism whose domain is R and kernel is S? Why, or why not?

E24) Let R be a ring and I be an ideal of R. Use Theorems 4 and 9 to prove that any ideal of R/I is of the form J/I, where J is an ideal of R containing I. (You have already proved this in Unit 12, of course.)

Now let us look at the behaviour of the composition of homomorphisms. In Theorem 2, Unit 8, you studied that the composition of group homomorphisms is a group homomorphism. So, you may not find the following analogous result surprising.

Theorem 10: Let R_1, R_2 and R_3 be rings, and let $f: R_1 \to R_2$ and $g: R_2 \to R_3$ be ring homomorphisms. Then their composition $g \circ f: R_1 \to R_3 : (g \circ f)(x) = g(f(x))$ is a ring homomorphism. ■

The proof of this result is on the same lines as the proof of the corresponding result in Unit 8. We leave it to you to prove (see E25).

Now, it is time to solve the following exercises. Doing so, will help you become familiar with some properties of the composition of ring homomorphisms.

E25) Prove Theorem 10.

E26) In the situation of Theorem 10, prove that

i) if $g \circ f$ is $1\text{-}1$, then so is f.

ii) if $g \circ f$ is onto, then so is g.

iii) if $g \circ f$ is $1\text{-}1$, g need not be $1\text{-}1$.

iv) if $g \circ f$ is onto, f need not be onto.

E27) Use Theorem 10 to show that $h: \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}_r$, defined by $h((n, m)) = \overline{m}$, is a homomorphism, where $r \in \mathbb{N}$.

Now let us focus on ring isomorphisms.

13.4 THE ISOMORPHISM THEOREMS

In Sec.8.4, Unit 8, we discussed group isomorphisms and various results involving them. In this section we will do the same thing for rings.

In Sec.13.2, you have already seen that a ring isomorphism is a bijective ring homomorphism. Also, as for groups, if $f: R_1 \to R_2$ is an isomorphism, we say that **R_1 is isomorphic to R_2**, and denote this by $R_1 \simeq R_2$.
Further, as for groups, an isomorphism of a ring R onto itself is called an **automorphism** of R.

For example, every ring R has at least one automorphism, namely I, as you have studied in Examples 3 and 4.

Over here consider the following remark, akin to what you have seen for groups.

Remark 7: Two rings are isomorphic if and only if they are algebraically identical. That is, isomorphic rings must have exactly the same algebraic properties. Thus, if R is a ring with identity, then it cannot be isomorphic to a ring without identity. Similarly, if the only ideals of R are $\{0\}$ and itself, then any ring isomorphic to R must have this property too.

Let us look at a few examples that you have already worked out. Take, the case of E9. There you have shown that $\mathbb{C} \simeq \left\{ \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \middle| a, b \in \mathbb{R} \right\}$, a subring of $\mathbb{M}_2(\mathbb{R})$. From Unit 12, you know that $\mathbb{C}$ has only two ideals, $\{0\}$ and itself. Thus, the same holds for the subring of $\mathbb{M}_2(\mathbb{R})$ to which $\mathbb{C}$ is isomorphic.

Next, consider E22(i). You have seen that ϕ is a homomorphism, $\text{Ker } \phi = \{0\}$ and $\text{Im } \phi = \left\{ \begin{bmatrix} x & 0 \\ -x & 0 \end{bmatrix} \middle| x \in \mathbb{R} \right\} = S$, say.
Hence, $\mathbb{R} \simeq S$.
Therefore, S is commutative, since $\mathbb{R}$ is commutative.
Since $\mathbb{R}$ has only two ideals, $\{0\}$ and itself, the same is true for S.
Since $U(\mathbb{R}) = \mathbb{R}^*$, the same is true for S, i.e., $U(S) = S \setminus \{\mathbf{0}\}$, and so on.
Here, note that none of the properties just discussed above for S are true for $\mathbb{M}_2(\mathbb{R})$. But they are true for the subring S of $\mathbb{M}_2(\mathbb{R})$.

Let us look at a few other examples.

Example 11: Let S be the subring $\left\{ \begin{bmatrix} a & b \\ 10b & a \end{bmatrix} \middle| a, b \in \mathbb{Z} \right\}$ of $\mathbb{M}_2(\mathbb{Z})$. Check whether or not $f : \mathbb{Z}[\sqrt{10}] \to S : f(a + b\sqrt{10}) = \begin{bmatrix} a & b \\ 10b & a \end{bmatrix}$ is an isomorphism.

Solution: You should check that f is well-defined.
Next, show that $f[(a + b\sqrt{10}) + (c + d\sqrt{10})] = f(a + b\sqrt{10}) + f(c + d\sqrt{10})$, and $f[(a + b\sqrt{10})(c + d\sqrt{10})] = f(a + b\sqrt{10})\ f(c + d\sqrt{10})$.

$$\begin{aligned} \text{Ker } f &= \left\{ a + b\sqrt{10} \middle| \begin{bmatrix} a & b \\ 10b & a \end{bmatrix} = \mathbf{0},\ a, b \in \mathbb{Z} \right\} \\ &= \{0\}. \end{aligned}$$

$\text{Im } f = S$, which you should verify.

Thus, f is an isomorphism.

***

Example 12: Let R and S be rings. Prove that $R \times S$ contains a subring isomorphic to R and a subring isomorphic to S.

Solution: Define $f : R \to R \times S : f(r) = (r, 0)$ and $g : S \to R \times S : g(s) = (0, s)$.
Now, you should verify that both f and g are well-defined.
Further, $\forall\ r_1, r_2 \in R$,
$f(r_1 + r_2) = (r_1 + r_2, 0) = (r_1, 0) + (r_2, 0) = f(r_1) + f(r_2)$, and
$f(r_1 r_2) = (r_1 r_2, 0) = (r_1, 0)(r_2, 0) = f(r_1) f(r_2)$.
Thus, f is a ring homomorphism.

Similarly, you should show that g is a ring homomorphism.

Next, $\text{Ker } f = \{r \in R \mid (r, 0) = (0, 0)\} = \{0\}$, so that f is 1-1.

Also, $\text{Im } f = \{(r, 0) \mid r \in R\} = R \times \{0\}$ is a subring of $R \times S$, such that $R \simeq \text{Im } f = R \times \{0\}$.

Similarly, you should show that $S \simeq \text{Im } g = \{0\} \times S$, a subring of $R \times S$.
Thus, $R \times S$ contains a subring isomorphic to R and a subring isomorphic to S.

***

Example 13: Show that $\mathbb{C} \not\simeq \mathbb{R}$.

Recall, from Unit 8, that $\not\simeq$ denotes 'is not isomorphic to'.

Solution: We shall prove this by contradiction, as in Unit 8.
So suppose that $\mathbb{C} \simeq \mathbb{R}$. Then $\mathbb{C}$ and $\mathbb{R}$ must have the same algebraic properties. Thus, $U(\mathbb{C})$ and $U(\mathbb{R})$ must have the same properties, i.e., $\mathbb{C}^*$ and $\mathbb{R}^*$ must have the same properties.
Now, $\mathbb{C}^*$ has an element, i, of order 4. That is, $(i)^4 = 1$. But $\mathbb{R}^*$ has no element of order 4. Hence, we reach a contradiction.
Thus, $\mathbb{C} \not\simeq \mathbb{R}$.

***

Example 14: Show that if $R \simeq S$, and R is a ring with identity, then $|U(R)| = |U(S)|$, where $U(R)$ denotes the group of units of R and $|A|$ denotes the cardinality of a set A.

Solution: Let $f : R \to S$ be an isomorphism.
Firstly, since R is a ring with identity, and $R \simeq S$, S is also a ring with identity.

You also know, from Theorem 2, that if $u \in U(R)$, then $f(u) \in U(S)$.
So, $f(U(R)) \subseteq U(S)$.
We shall show that $U(S) \subseteq f(U(R))$.
So, let $s \in U(S)$. Then $s = f(t)$ for some $t \in R$, since f is surjective.
Similarly, $\exists\ r \in R$ s.t. $s^{-1} = f(r)$.
Now, $f(rt) = f(r)f(t) = s^{-1}s = 1 = f(1)$, from Theorem 2.
Thus, $rt = 1$, since f is injective.
Hence, $r \in U(R)$, so that $U(S) \subseteq f(U(R))$.
Thus, $U(S) = f(U(R))$.
Also, since f is 1-1 over R, it is 1-1 when restricted to $U(R)$.
Thus, f, restricted to $U(R)$, is a bijection from $U(R)$ to $U(S)$.
Hence, $|U(R)| = |U(S)|$.

***

Try solving the following exercises now. They will help you in becoming more familiar with isomorphisms.

E28) Which of the following functions are ring isomorphisms? Give reasons for your answers.

i) $f : \mathbb{Z} \to \mathbb{R} : f(n) = n$,

ii) $f : \mathbb{Z} \to \mathbb{Z}/10\mathbb{Z} : f(n) = \overline{5n}$,

iii) $f : \mathbb{C} \to \mathbb{C} : f(z) = \bar{z}$, the complex conjugate of z,

iv) $f : \mathbb{C} \to \mathbb{R} \times \mathbb{R} : f(z) = (|z|, \text{Arg } z)$.

$R_1 \simeq R_2$ iff $R_2 \simeq R_1$.

E29) Let $\phi : R_1 \to R_2$ be a ring isomorphism. Then you know that $\phi^{-1} : R_2 \to R_1$ is a well-defined function, since ϕ is bijective. Show that ϕ^{-1} is also an isomorphism.

E30) Show that the composition of isomorphisms is an isomorphism.

E31) Which of the following are true? Give reasons for your answers.

i) $\mathbb{Q} \simeq \mathbb{Z}$,

ii) $\mathbb{Q} \not\simeq \mathbb{R}$,

iii) $\mathbb{Z} \simeq \mathbb{M}_n(\mathbb{Z}_m)$, for some $n, m \in \mathbb{N}$,

iv) $\mathbb{Z}_3 \simeq \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$,

v) If R and S are rings such that $(R, +) \simeq (S, +)$ as groups, then R and S are isomorphic rings.

E32) Prove that $\wp(X) \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$, where $X = \{1, 2\}$.
(**Hint:** Define $f : \wp(X) \to \mathbb{Z}_2 \times \mathbb{Z}_2$ for each of the 4 elements of $\wp(X)$ in a manner that f is an isomorphism.)

And now, let us go back to Sec.8.4, Unit 8, for a moment. Over there, we proved the Fundamental Theorem of Homomorphism for groups. According to this theorem, the homomorphic image of a group G is isomorphic to a quotient group of G. Now we will prove a similar result for rings. This is known as **the first isomorphism theorem**, or **the Fundamental Theorem of Homomorphism for rings** (FTH, in brief)**.**

Theorem 11 (The Fundamental Theorem of Homomorphism): Let $f : R \to S$ be a ring homomorphism. Then $R/\text{Ker } f \simeq \text{Im } f$.

In particular, if f is surjective, then $R/\text{Ker } f \simeq S$.

Proof: First, note that $R/\text{Ker } f$ is a well-defined quotient ring, since $\text{Ker } f$ is an ideal of R. For convenience, let us write $\text{Ker } f = I$. Let us define $\psi : R/I \to S$ by $\psi(x + I) = f(x)$.

As in the case of the FTH in Unit 8, we need to check that ψ is well-defined.
Now, $x + I = y + I \Rightarrow x - y \in I = \text{Ker } f \Rightarrow f(x - y) = 0 \Rightarrow f(x) = f(y)$
$\Rightarrow \psi(x + I) = \psi(y + I)$.
Thus, ψ is well-defined.

Now let us see whether ψ is an isomorphism or not.

ψ is a homomorphism: Let $x, y \in R$. Then

$$\psi((x+I)+(y+I)) = \psi(x+y+I) = f(x+y) = f(x)+f(y)$$
$$= \psi(x+I)+\psi(y+I), \text{ and}$$
$$\psi((x+I)(y+I)) = \psi(xy+I) = f(xy) = f(x)f(y)$$
$$= \psi(x+I)\psi(y+I).$$

Thus, ψ is a ring homomorphism.

$\text{Im}\,\psi = \text{Im}\,f$: Since $\psi(x+I) = f(x) \in \text{Im } f \ \forall\ x \in R$, $\text{Im}\,\psi \subseteq \text{Im}\,f$.
Also any element of $\text{Im}\,f$ is of the form $f(x) = \psi(x+I)$ for some $x \in R$.
Thus, $\text{Im}\,f \subseteq \text{Im}\,\psi$.
So, $\text{Im}\,\psi = \text{Im}\,f$.

ψ is 1-1: Let $x, y \in R$ such that $\psi(x+I) = \psi(y+I)$.
Then $f(x) = f(y)$, so that $f(x-y) = 0$, i.e., $x - y \in \text{Ker } f = I$,
i.e., $x + I = y + I$.
Thus, ψ is 1-1.
So, we have shown that $R/\text{Ker } f \simeq \text{Im}\,f$.
Thus, if f is onto, then $\text{Im}\,f = S$, and $R/\text{Ker } f \simeq S$. ■

Note that this result says that f is the composition $\psi \circ \eta$, where η is the canonical homomorphism $\eta : R \to (R/\text{Ker } f) : \eta(a) = a + \text{Ker } f$. This is diagrammatically shown in Fig.1.

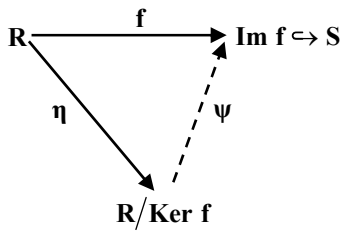

Fig.1: Given f, ∃ an isomorphism ψ s.t. $\psi \circ \eta = f$.

Let us, now, look at some examples of the application of the Fundamental Theorem.

Example 15: Show that the rings $\mathbb{Z}/m\mathbb{Z}$ and $\mathbb{Z}_m$ are isomorphic, where $m \in \mathbb{N}$.

Solution: Consider $p : \mathbb{Z} \to \mathbb{Z}_m : p(n) = \bar{n}$.
You should check that p is an epimorphism, and
$\text{Ker } p = \{n \mid \bar{n} = \bar{0} \text{ in } \mathbb{Z}_m\} = m\mathbb{Z}$.
Therefore, by Theorem 11, $\mathbb{Z}/m\mathbb{Z} \simeq \mathbb{Z}_m$.
(Note that you have often used the fact that $\mathbb{Z}/m\mathbb{Z}$ and $\mathbb{Z}_m$ are isomorphic groups.)

***

Example 16: Prove that if R_1 and R_2 are rings, then $(R_1 \times R_2)/R_2 \simeq R_1$ and

$(R_1 \times R_2)/R_1 \simeq R_2$.

Solution: Define $p : R_1 \times R_2 \to R_1 : p(a, b) = a$. Then, from E6, you know that the projection map p is an epimorphism, and its kernel is

$\text{Ker } p = \{(0, b) \mid b \in R_2\} = \{0\} \times R_2$.

Thus, by Theorem 11, $(R_1 \times R_2)/\{0\} \times R_2 \simeq R_1$.

Now define $f : \{0\} \times R_2 \to R_2 : f(0, b) = b$. Then you should prove that f is a ring isomorphism.

Thus, $\text{Ker } p \simeq R_2$.

Hence, R_2 can be treated as an ideal of $R_1 \times R_2$, and can replace $\text{Ker } p$.

Therefore, $(R_1 \times R_2)/R_2 \simeq R_1$.

You should prove that $(R_1 \times R_2)/R_1 \simeq R_2$ on the same lines.

***

Example 17: Consider the ring $R = \left\{ \begin{bmatrix} a & b \\ 0 & a \end{bmatrix} \middle| a, b \in \mathbb{R} \right\}$.

Let $I = \left\{ \begin{bmatrix} 0 & c \\ 0 & 0 \end{bmatrix} \middle| c \in \mathbb{R} \right\}$.

i) Prove that I is an ideal of R.

ii) Show that $(R/I) \simeq \mathbb{R}$.

Solution: i) Since $\mathbf{0} \in I$, $I \neq \emptyset$.

Next, for $A = \begin{bmatrix} 0 & a \\ 0 & 0 \end{bmatrix}$, $B = \begin{bmatrix} 0 & b \\ 0 & 0 \end{bmatrix}$ in I, $A - B = \begin{bmatrix} 0 & a-b \\ 0 & 0 \end{bmatrix} \in I$.

Also, for $A = \begin{bmatrix} 0 & a \\ 0 & 0 \end{bmatrix}$ in I and $C = \begin{bmatrix} c & d \\ 0 & c \end{bmatrix}$ in R,

$AC = \begin{bmatrix} 0 & ac \\ 0 & 0 \end{bmatrix} \in I$, $CA = \begin{bmatrix} 0 & ac \\ 0 & 0 \end{bmatrix} \in I$.

Thus, I is an ideal of R.

ii) Define $\pi : R \to \mathbb{R} : \pi\left(\begin{bmatrix} a & b \\ 0 & a \end{bmatrix}\right) = a$. Then π is well-defined (verify this!).

Further, prove that π is a ring homomorphism and π is surjective.

Now, $\text{Ker } \pi = \left\{ \begin{bmatrix} a & b \\ 0 & a \end{bmatrix} \middle| a, b \in \mathbb{R}, a = 0 \right\} = \left\{ \begin{bmatrix} 0 & b \\ 0 & 0 \end{bmatrix} \middle| b \in \mathbb{R} \right\} = I$.

Therefore, by the FTH, $(R/I) \simeq \mathbb{R}$.

***

Try solving some exercises now.

E33) What does the Fundamental Theorem of Homomorphism say in the case of the homomorphisms in each of the Examples 1 to 9?

E34) Prove that $\mathbb{R}[x]/_{<x>} \simeq \mathbb{R}$.

E35) Let $R = \left\{ \begin{bmatrix} a & b \\ b & a \end{bmatrix} \middle| a, b \in \mathbb{Z} \right\}$. Show that R is a commutative subring of $\mathbb{M}_2(\mathbb{Z})$, with unity.

Further, define $\phi : R \to \mathbb{Z} : \phi\left(\begin{bmatrix} a & b \\ b & a \end{bmatrix}\right) = a - b$. Show that ϕ is a ring homomorphism. What does Theorem 11 say in this case?

E36) Let R be a ring with unity. For $r \in U(R)$, define $f_r : R \to R : f_r(s) = r^{-1}sr$. Check if f_r is a homomorphism or not. If it is, what does FTH say in this case? If f_r is not a homomorphism, find an endomorphism of R.

E37) Let S be a subring of a ring R, and I be an ideal of R. In Unit 12, you have proved that $S \cap I$ is an ideal of S. Use the FTH to prove that $S/(S \cap I)$ is a subring of R/I. Is it also an ideal of R/I? Why?

Now, what E36 tells us is that if R is a ring with unity, then $f_r \in \text{Aut } R$ for each $r \in U(R)$. Are all these distinct? For example, are f_{-1} and f_1 distinct automorphisms of $\mathbb{Z}$? The answer to this lies in a very surprising result that we will now discuss. We will use Theorem 11 to prove that any ring homomorphism from a ring R onto $\mathbb{Z}$ is uniquely determined by its kernel. That is, we can't have two different ring homomorphisms from R onto $\mathbb{Z}$ with the same kernel. (Note that **this is not true for group homomorphisms**. In fact, you know that I, the identity map on $\mathbb{Z}$, and $-I$ are distinct group homomorphisms from $\mathbb{Z}$ onto itself with the same kernel, $\{0\}$.) To prove this statement we need the following result.

Theorem 12: The only non-trivial ring homomorphism from $\mathbb{Z}$ to itself is the identity map.

Proof: Let $f : \mathbb{Z} \to \mathbb{Z}$ be a non-trivial ring homomorphism. Let n be a positive integer. Then $n = 1 + 1 + \cdots + 1$ (n times).
Therefore, $f(n) = f(1) + f(1) + \cdots + f(1)$ (n times) $= n\,f(1)$.

On the other hand, if n is a negative integer, then $(-n)$ is a positive integer.
Therefore, $f(-n) = (-n)f(1)$,
i.e., $-f(n) = -nf(1)$, by Theorem 1.
Thus, $f(n) = n\,f(1)$ in this case too.
Also $f(0) = 0 = 0f(1)$, again, by Theorem 1.
Thus, $f(n) = nf(1)\ \forall\ n \in \mathbb{Z}$. …(3)
You also know that $f(1) = 1$, since f is a non-trivial ring homomorphism.
Therefore, from (3), you can see that
$f(n) = n\ \forall\ n \in \mathbb{Z}$, i.e., $f = I$. ■

This theorem has an important corollary.

Corollary 2: Let R be a ring isomorphic to $\mathbb{Z}$. If f and g are two isomorphisms from R onto $\mathbb{Z}$, then $f = g$.

Proof: The composition $f \circ g^{-1}$ is an isomorphism from $\mathbb{Z}$ onto itself.
Therefore, by Theorem 12, $f \circ g^{-1} = \mathbf{0}$ or $f \circ g^{-1} = I$.
If $f \circ g^{-1} = \mathbf{0}$, then $(f \circ g^{-1})(1) = 0 \Rightarrow f(g^{-1}(1)) = 0 \Rightarrow f(1) = 0$, a contradiction, since f is non-trivial.
Thus, $f \circ g^{-1} = I$.
Hence, $f = g$. ■

We are now in a position to prove the really surprising result we had mentioned earlier.

Theorem 13: Let R be a ring and f and g be homorphisms from R onto $\mathbb{Z}$ such that $\text{Ker } f = \text{Ker } g$. Then $f = g$.

Proof: By Theorem 11, we have isomorphisms
$\psi_f : R/\text{Ker } f \to \mathbb{Z}$ and $\psi_g : R/\text{Ker } g \to \mathbb{Z}$.
Since $\text{Ker } f = \text{Ker } g$, ψ_f and ψ_g are isomorphisms of the same ring onto $\mathbb{Z}$.
Thus, by Corollary 2, $\psi_f = \psi_g$.
Also, the canonical maps $\eta_f : R \to R/\text{Ker } f$ and $\eta_g : R \to R/\text{Ker } g$ are the same since $\text{Ker } f = \text{Ker } g$.
$\therefore f = \psi_f \circ \eta_f$, using Theorem 11
$= \psi_g \circ \eta_g$
$= g$. ■

We will now give you a chance to prove some important applications of Theorem 11! They are analogous to Theorem 12 and Theorem 14 of Unit 8.

E38) **(Second Isomorphism Theorem):** Let S be a subring and I be an ideal of a ring R. Show that $(S+I)/I \simeq S/(S \cap I)$.

E39) **(Third Isomorphism Theorem):** Let I and J be ideals of a ring R such that $J \subseteq I$. Show that $(R/J)/(I/J) \simeq R/I$.

E40) Prove that

i) $\mathbb{Z}_{15}/\overline{5}\mathbb{Z}_{15} \simeq \mathbb{Z}_5$,

ii) $\mathbb{Z}_m/\overline{n}\mathbb{Z}_m \simeq \mathbb{Z}_n$, where $m, n \in \mathbb{N}$ and $n \mid m$.

E41) How many non-trivial ring automorphisms of $\mathbb{Q}$ are there, and why?

We shall halt our discussion of ring homomorphisms and isomorphisms here, and briefly recall what we have done in this unit. Of course, we have not finished with these functions. We will be using them again and again in the units of the next block.

13.5 SUMMARY

In this unit, you have studied the following points.

1. The definition of a ring homomorphism, its kernel and its image, along with several examples.

2. The direct, and inverse, image of a subring under a homomorphism is a subring.

3. If $f: R \to S$ is a ring homomorphism, then
   i) $\text{Ker } f$ is an ideal of R,
   ii) $\text{Im } f$ is a subring of S,
   iii) $f^{-1}(I)$ is an ideal of R for every ideal I of S,
   iv) if f is surjective, then $f(I)$ is an ideal of S.

4. Let $f: R \to S$ be an onto ring homomorphism. Then $I \mapsto f(I)$ defines a one-to-one correspondence between the set of ideals of R containing $\text{Ker } f$ and the set of ideals of S.

5. A homomorphism is injective iff its kernel is $\{0\}$.

6. If I is an ideal of a ring R, then there exists a ring S and a surjective ring homomorphism $f: R \to S$ whose kernel is I.

7. The composition of homomorphisms is a homomorphism.

8. The definition, and examples, of a ring isomorphism.

9. The proof, and applications, of the **Fundamental Theorem of Homomorphism for rings**, which says that if $f: R \to S$ is a ring homomorphism, then $R/\text{Ker } f \simeq \text{Im } f$.

10. **Second Isomorphism Theorem:** Let S be a subring and I be an ideal of a ring R. Then $(S+I)/I \simeq S/(S \cap I)$.

11. **Third Isomorphism Theorem:** Let I and J be ideals of a ring R such that $J \subseteq I$. Then $(R/J)/(I/J) \simeq R/I$.

12. The only non-trivial ring homomorphism from $\mathbb{Z}$ to $\mathbb{Z}$ is the identity automorphism.

13. Let R be a ring and f and g be homorphisms from R onto $\mathbb{Z}$ such that $\text{Ker } f = \text{Ker } g$. Then $f = g$.

13.6 SOLUTIONS / ANSWERS

E1) For $x, y \in S$,

$i(x+y) = x + y = i(x) + i(y)$, and

$i(xy) = xy = i(x)\,i(y)$.

$\therefore i$ is a homomorphism.

$\text{Ker } i = \{x \in S \mid i(x) = 0\} = \{0\}$.

$\text{Im } i = \{i(x) \mid x \in S\} = S$.

E2) i) First, if $f(x) = g(x)$ in $\mathbb{Z}[x]$, then $f(1) = g(1)$ in $\mathbb{Z}$. So ϕ is well-defined.

Next, let $f(x) = \sum_{i=0}^{m} a_i x^i$, and $g(x) = \sum_{i=0}^{n} b_i x^i$ be in $\mathbb{Z}[x]$. Then

$$\phi(f(x) + g(x))$$

$$= \phi\left(\sum_{i=0}^{m} (a_i + b_i)x^i\right), \text{ assuming } m \geq n \text{ and } b_{n+1} = 0 = b_{n+2} = \cdots = b_m.$$

$$= \sum_{i=0}^{m} (a_i + b_i), \text{ putting } x = 1.$$

$$= \left(\sum_{i=0}^{m} a_i\right) + \left(\sum_{i=0}^{n} b_i\right), \text{ since } b_j = 0 \text{ for } j \geq n.$$

$$= \phi(f(x)) + \phi(g(x)).$$

If $m \leq n$, you can prove that $\phi(f(x) + g(x)) = \phi(f(x)) + \phi(g(x))$, similarly.

Also, $\phi(f(x) \cdot g(x)) = \phi\left(\sum_{k=0}^{m+n}\left(\sum_{i+j=k} a_i b_j x^{i+j}\right)\right)$

$$= \sum_{k=0}^{m+n}\left(\sum_{i+j=k} a_i b_j\right), \text{ putting } x = 1.$$

$$= f(1) \cdot g(1)$$

$$= \phi(f(x)) \cdot \phi(g(x)).$$

Thus, ϕ is a homomorphism.

$\text{Ker } \phi = \{f(x) \in \mathbb{Z}[x] \mid f(1) = 0\}$.

From Calculus, you know that if $f(x) \in \mathbb{Z}[x]$, then $f(a) = 0$ iff a is a root of the polynomial $f(x)$, where $a \in \mathbb{Z}$.

Thus, $\text{Ker } \phi = \{f(x) \in \mathbb{Z}[x] \mid f \text{ has } 1 \text{ as a root}\}$.

$\text{Im } \phi = \mathbb{Z}$, because for any $m \in \mathbb{Z}$, $f(x) = x - 1 + m \in \mathbb{Z}[x]$ s.t. $f(1) = m$.

ii) As in (i), you should prove that ϕ_z is a homomorphism.

Further, $\text{Ker } \phi_z = \{f(x) \in \mathbb{C}[x] \mid f(z) = 0\}$.

Thus, $\text{Ker } \phi_z$ is the set of all complex polynomials which have z as a root.

$\text{Im } \phi_z = \{f(z) \in \mathbb{C} \mid f(x) \in \mathbb{C}[x]\} = \mathbb{C}$, because for any
$w \in \mathbb{C}$, $x + w - z \in \mathbb{C}[x]$ s.t. $\phi_z(x + w - z) = w$.

E3) Let $\alpha = 1 + i \in \mathbb{H}$ and $\beta = 1 + 2i + j \in \mathbb{H}$.
Then $\alpha\beta = (1+i)(1+2i+j) = -1 + 3i + j + k$. (Remember the relations satisfied by i, j, k!)
So $\phi(\alpha\beta) = -1$.
But $\phi(\alpha)\phi(\beta) = 1 \cdot 1 = 1$.
Thus, $\phi(\alpha\beta) \neq \phi(\alpha)\phi(\beta)$ in $\mathbb{R}$.
Thus, ϕ is not a homomorphism.

E4) Take $A = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$, $B = \begin{bmatrix} 2 & 1 \\ 0 & 1 \end{bmatrix} \in \mathbb{M}_2(\mathbb{C})$. Then

$$\psi(A+B) = \psi\left(\begin{bmatrix} 3 & 3 \\ 3 & 5 \end{bmatrix}\right) = \det\left(\begin{bmatrix} 3 & 3 \\ 3 & 5 \end{bmatrix}\right) = 15 - 9 = 6.$$

Also $\psi(A) + \psi(B) = -2 + 2 = 0$.
Thus, ψ is not a homomorphism.

E5) You need to first check if f is well-defined.
Now, if $\bar{n} = \bar{m}$ in $\mathbb{Z}_3$, then $3 \mid (n-m)$. So $6 \mid 4(n-m)$.
i.e., $\overline{4n} = \overline{4m}$ in $\mathbb{Z}_6$.
Therefore, f is well-defined.

Next, for $\bar{n}$, $\bar{m}$ in $\mathbb{Z}_3$,

$$\begin{aligned} f(\bar{n} + \bar{m}) &= f(\overline{n+m}) = 4(n+m) \pmod 6 \\ &= 4n \pmod 6 + 4m \pmod 6 \\ &= f(\bar{n}) + f(\bar{m}). \end{aligned}$$

Also, $f(\bar{n} \cdot \bar{m}) = f(\overline{nm}) = 4nm \pmod 6$

$= 16nm \pmod 6$, since $\bar{4} = \overline{16}$ in $\mathbb{Z}_6$.

$= 4n \pmod 6 \cdot 4m \pmod 6$

$= f(\bar{n}) \cdot f(\bar{m})$.

Thus, f is a ring homomorphism.

E6) You should first show that p is well-defined.

Next, for any $(a, b), (c, d) \in A \times B$,
$p((a, b) + (c, d)) = p((a + c, b + d)) = a + c = p((a, b)) + p((c, d))$, and
$p((a, b)(c, d)) = p((ac, bd)) = ac = p((a, b))\,p((c, d))$.
So, p is a ring homomorphism.

$\text{Ker } p = \{(a,b) \in A \times B \mid a = 0\} = \{0\} \times B.$

$\text{Im } p = \{p(a,b) \mid (a,b) \in A \times B\} = \{a \mid (a,b) \in A \times B\} = A.$

If B is not the trivial ring, p is not 1-1. This is because
$\exists\, b_1, b_2 \in B, b_1 \neq b_2$, so that $(0, b_1) \neq (0, b_2)$.

But $p((0, b_1)) = 0 = p((0, b_2))$.

Hence, if $B \neq \{0\}$, p is not an isomorphism.

E7) Firstly, f is well-defined since $a - b\sqrt{2} = a + (-b)\sqrt{2} \in \mathbb{Z}[\sqrt{2}]\ \forall\ a, b \in \mathbb{Z}$.

Next, for $a, b, c, d \in \mathbb{Z}$,

$$f((a + b\sqrt{2}) + (c + d\sqrt{2})) = f(a + c + \sqrt{2}(b + d))$$
$$= (a + c) - (b + d)\sqrt{2} = (a - b\sqrt{2}) + (c - d\sqrt{2})$$
$$= f(a + b\sqrt{2}) + f(c + d\sqrt{2}).$$

Also, $f((a + b\sqrt{2})(c + d\sqrt{2})) = f(ac + 2bd + \sqrt{2}(ad + bc))$

$$= ac + 2bd - (ad + bc)\sqrt{2} = (a - \sqrt{2}b)(c - \sqrt{2}d)$$
$$= f(a + b\sqrt{2}) \cdot f(c + d\sqrt{2}).$$

Thus, f is an endomorphism.

You should check that g is well-defined. However,

$g[(1 + \sqrt{3})(1 - \sqrt{3})] = g(-2) = -2$, and

$g(1 + \sqrt{3}) \cdot g(1 - \sqrt{3}) = (1 + \sqrt{7})(1 - \sqrt{7}) = -6$. Thus, g is not a homomorphism.

E8) For $3n, 3m \in \mathbb{Z}$, $f(3n \cdot 3m) = f(9nm) = 5(3nm) \neq 5n \cdot 5m$.
Hence, f is not a homomorphism.

E9) First, you should check whether or not ϕ is well-defined.
Then prove that it is a homomorphism, 1-1 and onto.
Here, note that $\forall\ a, b, c, d \in \mathbb{R}$,

$$\phi((a + ib)(c + id)) = \phi[(ac - bd) + i(ad + bc)]$$
$$= \begin{bmatrix} ac - bd & ad + bc \\ -(ad + bc) & ac - bd \end{bmatrix} = \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \begin{bmatrix} c & d \\ -d & c \end{bmatrix}$$
$$= \phi(a + ib) \cdot \phi(c + id).$$

E10) For $f, g \in C[0, 1]$,

$$\phi(f + g) = ((f + g)(0), (f + g)(1))$$
$$= (f(0) + g(0), f(1) + g(1))$$
$$= (f(0), f(1)) + (g(0), g(1))$$
$$= \phi(f) + \phi(g), \text{ and}$$
$$\phi(fg) = (fg(0), fg(1)) = (f(0) \cdot g(0), f(1) \cdot g(1))$$
$$= (f(0, f(1))(g(0), g(1))$$
$$= \phi(f)\phi(g).$$

$\therefore \phi$ is a homomorphism.

ϕ is not injective since, for example, $f \neq \mathbf{0}$ but $\phi(f) = \phi(\mathbf{0})$, where $f : [0, 1] \to \mathbb{R} : f(x) = x(x - 1)$ is in $\mathbb{C}[0, 1]$.
Thus, ϕ is not an isomorphism.

E11) We will use Theorem 1 of Unit 11.
Firstly, $S \neq \emptyset \Rightarrow f(S) \neq \emptyset$.

Next, let $a', b' \in f(S)$. Then $\exists\ a, b \in S$ such that $f(a) = a',\ f(b) = b'$.
Now $a' - b' = f(a) - f(b) = f(a - b) \in f(S)$, since $a - b \in S$, and
$a'b' = f(a)f(b) = f(ab) \in f(S)$, since $ab \in S$.
$\therefore f(S)$ is a subring of R_2.

E12) Consider the trivial homomophism $f : \mathbb{Z} \to \mathbb{Z} : f(x) = 0$. Then, $2\mathbb{Z} \neq 3\mathbb{Z}$ in $\mathcal{A}$. But $f(2\mathbb{Z}) = \{\mathbf{0}\} = f(3\mathbb{Z})$ in $\mathcal{B}$. Thus, ϕ is not $1\text{-}1$, and hence, not a bijection.

E13) Since I is a subring of R_2, $f^{-1}(I)$ is a subring of R_1, by Theorem 3.
Now, let $a \in f^{-1}(I)$ and $r \in R_1$.
We want to show that $ar \in f^{-1}(I)$ and $ra \in f^{-1}(I)$.
Since $a \in f^{-1}(I)$, $f(a) \in I$.
$\therefore f(a)f(r) \in I$ and $f(r)f(a) \in I$, i.e., $f(ar) \in I$ and $f(ra) \in I$. (Note that R_2 need not be commutative.)
$\therefore ar \in f^{-1}(I)$ and $ra \in f^{-1}(I)$.
Thus, $f^{-1}(I)$ is an ideal of R_1.

Also, if $x \in \text{Ker } f$, then $f(x) = 0 \in I$.
$\therefore x \in f^{-1}(I)$.
$\therefore \text{Ker } f \subseteq f^{-1}(I)$.

E14) Let $x \in f(f^{-1}(J))$. Then $x = f(y)$, where $y \in f^{-1}(J)$, i.e., $f(y) \in J$, i.e., $x \in J$.
Thus, $f(f^{-1}(J)) \subseteq J$.

Now, let $x \in J$. Since f is surjective, $\exists\ y \in R$ such that $f(y) = x$.
Then $y \in f^{-1}(x) \subseteq f^{-1}(J)$. (Note that $f^{-1}(x)$ is a set, not an element.)
$\therefore x = f(y) \in f(f^{-1}(J))$.
Thus, $J \subseteq f(f^{-1}(J))$.
Hence, the result is proved.

E15) Here $f(I) = \overline{2}\mathbb{Z}_5 = \mathbb{Z}_5$, since $(2, 5) = 1$.
So $f^{-1}(f(I)) = \mathbb{Z} = \mathbb{Z} + \text{Ker } f$, since $\text{Ker } f \subseteq \mathbb{Z}$.

For any ideal I of R, in Example 3, $f(I) = \{0\}$, where $f = \mathbf{0}$. So
$f^{-1}(f(I)) = R = R + \text{Ker } f$, since $\text{Ker } f = R$.

E16) You know, from Unit 12, that the only ideals of $\mathbb{R}$ are $\{0\}$ and $\mathbb{R}$. Here
$\text{Ker } \phi = \{f \in C[0, 1] \text{ s.t. } f(1/2) = 0\}$.
So, if I is an ideal of $C[0, 1]$ s.t. $\text{Ker } \phi \subseteq I$, then $\phi(I) = \{0\}$ or $\phi(I) = \mathbb{R}$, by Theorem 6.
But, if $\phi(I) = \{0\}$, then $I \subseteq \text{Ker } \phi$, i.e., $I = \text{Ker } \phi$.
So if $I \neq \text{Ker } \phi$, then $\phi(I) = \mathbb{R}$, by Theorem 6.

E17) i) For example, $(0, 1) \notin \text{Im } f$. Hence, f is not onto.

ii) For any ideal I of $\mathbb{Z}$, $I = n\mathbb{Z}$ for some $n \in \mathbb{Z}$. So $f(I) = \{(nm, nm) \mid m \in \mathbb{Z}\}$, which is not an ideal of $\mathbb{Z} \times \mathbb{Z}$, as you have seen in Unit 12. Thus, the ideal $\mathbb{Z} \times \{0\}$ of $\mathbb{Z} \times \mathbb{Z}$ is not of the form $f(I)$, for any ideal I of $\mathbb{Z}$. In fact, no ideal of $\mathbb{Z} \times \mathbb{Z}$ can be of the form $f(I)$.

E18) You should prove that $g(m+n) = g(m) + g(n)$, and $g(mn) = g(m)g(n)$. Hence, g is a homomorphism.
However, g is not surjective – e.g., $(1, 2) \notin \text{Im } g$.

Now, let I be an ideal of $\mathbb{Z}$. So $I = n\mathbb{Z}$, for some $n \in \mathbb{N}$.
Then $g(I) = n\mathbb{Z} \times \{0\}$ is an ideal of $\mathbb{Z} \times \mathbb{Z}$, by Theorem 5, Unit 12.

This does not counter Theorem 4, as Theorem 4 says that if f is surjective, $f(I)$ should be an ideal of the co-domain. It does not say that if f is not surjective, then $f(I)$ cannot be an ideal.

E19) As in Example 10, we consider $f : \mathbb{Z} \to \mathbb{Z}_n : f(m) = \overline{m}$. Since f is an epimorphism, the ideals of $\mathbb{Z}_n$ are of the form $f(m\mathbb{Z})$, where $m \mid n$.
Thus, the ideals of $\mathbb{Z}_n$ are $\overline{m}\mathbb{Z}_n$, where $m \mid n$.
Thus, every ideal of $\mathbb{Z}_n$ is a principal ideal.

E20) The homomorphisms in Example 1, I in Example 3 (and 4), and f in Example 8 have kernel $\{0\}$. Thus, they are 1-1.

E21) The homomorphism in E1, certainly.

In E5, $\text{Ker } f = \{\overline{n} \in \mathbb{Z}_3 \mid 4n \mid 6\} = \{\overline{0}\}$. So f is 1-1.

In E7, $\text{Ker } f = \{a + b\sqrt{2} \mid a - b\sqrt{2} = 0,\ a, b \in \mathbb{Z}\}$

$= \{a + b\sqrt{2} \mid a = 0,\ b = 0\}$

$= \{0\}$.

E22) i) Firstly, if $x = y$ in $\mathbb{R}$, then $\begin{bmatrix} x & 0 \\ -x & 0 \end{bmatrix} = \begin{bmatrix} y & 0 \\ -y & 0 \end{bmatrix}$.
So $\phi(x) = \phi(y)$ in $\mathbb{M}_2(\mathbb{R})$.
Thus, ϕ is well-defined.

Next, you should check that for $x, y \in \mathbb{R}$,
$\phi(x + y) = \phi(x) + \phi(y)$ and $\phi(xy) = \phi(x)\phi(y)$.
So ϕ is a ring homomorphism.

$\text{Ker } \phi = \{x \mid \phi(x) = \mathbf{0}\} = \{0\}$. So ϕ is 1-1.

$\text{Im } \phi = \left\{ \begin{bmatrix} x & 0 \\ -x & 0 \end{bmatrix} \middle| \, x \in \mathbb{R} \right\} \neq \mathbb{M}_2(\mathbb{R})$, because, for example,

$\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \notin \text{Im } \phi$.

So ϕ is not onto.

Thus, ϕ is not an isomorphism.

ii) You should check that ϕ is well-defined and

$\phi(\bar{n}_1 \cdot \bar{n}_2) = \phi(\bar{n}_1) \cdot \phi(\bar{n}_2) \ \forall \ \bar{n}_1, \bar{n}_2 \in \mathbb{Z}_3$.

Now $\phi(\bar{n}_1 + \bar{n}_2) = \phi(\overline{n_1 + n_2}) = (\overline{n_1 + n_2})^3 = (\bar{n}_1 + \bar{n}_2)^3$

$= \bar{n}_1^3 + \bar{n}_2^3$, since $\bar{3} = \bar{0}$.

$= \phi(\bar{n}_1) + \phi(\bar{n}_2) \ \forall \ \bar{n}_1, \bar{n}_2 \in \mathbb{Z}_3$.

Thus, ϕ is a ring homomorphism.

$\text{Ker } \phi = \{\bar{n} \in \mathbb{Z}_3 \mid \bar{n}^3 = \bar{0}\} = \{\bar{0}\}$. So ϕ is 1-1.

$\text{Im } \phi = \{\bar{n}^3 \mid \bar{n} \in \mathbb{Z}_3\} = \mathbb{Z}_3$. So ϕ is onto.

Thus, ϕ is an isomorphism.

E23) No. For example, take the subring $\mathbb{Z}$ of $\mathbb{Q}$. Since $\mathbb{Z}$ is not an ideal of $\mathbb{Q}$, it can't be the kernel of any homomorphism from $\mathbb{Q}$ to another ring, because of Theorem 7.

E24) Consider f of Theorem 9. Since f is surjective, $f(J) = J/I$ is an ideal of R/I, for any ideal J of R containing I, by Theorem 4.

Conversely, let A be an ideal of R/I. Then $f^{-1}(A)$ is an ideal of R containing $\text{Ker } f = I$.

Hence, $f(f^{-1}(A)) = (f^{-1}(A)/I)$ is an ideal of R/I, by Theorem 6.

Also, from E14, you know that $A = f(f^{-1}(A))$.

Thus, $A = (f^{-1}(A)/I) = J/I$, where $J = f^{-1}(A)$.

E25) For any $x, y \in R_1$,

$g \circ f(x+y) = g(f(x+y)) = g(f(x) + f(y))$, since f is a homomorphism.

$= g(f(x)) + g(f(y))$, since g is a homomorphism.

$= g \circ f(x) + g \circ f(y)$, and

$g \circ f(xy) = g(f(xy)) = g(f(x)f(y))$, since f is a homomorphism.

$= g(f(x)) \cdot g(f(y))$, since g is a homomorphism.

$= g \circ f(x) \cdot g \circ f(y)$.

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

E26) i) $x \in \text{Ker } f \Rightarrow f(x) = 0 \Rightarrow g \circ f(x) = 0 \Rightarrow x = 0$, since $g \circ f$ is 1-1.

$\therefore \text{Ker } f = \{0\}$.

$\therefore f$ is 1-1.

ii) Let $x \in R_3$. Since $g \circ f$ is onto, $\exists \ y \in R_1$ such that $g \circ f(y) = x$,

i.e., $g(f(y)) = x$, where $f(y) \in R_2$. Thus, g is onto.

iii) For example, consider $\phi \circ i : \mathbb{Z} \to \mathbb{Z}$, where $i : \mathbb{Z} \hookrightarrow \mathbb{Z}[x] : i(m) = m$ and ϕ is the map in E2(i).
Then $\phi \circ i = I : \mathbb{Z} \to \mathbb{Z}$, which is 1-1.
But ϕ is not 1-1 since $\text{Ker } \phi \neq \{0\}$.

iv) You can use the example in (iii) above, to show this too.

E27) h is the composition of the projection map $p : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} : p(n, m) = m$ and the map $f : \mathbb{Z} \to \mathbb{Z}_r : f(m) = \overline{m}$.
Both p and f are ring homomorphisms, as you know from E6 and Example 5, respectively.
$\therefore h$ is a homomorphism.

E28) i) f is not onto, since $\frac{1}{2} \notin \text{Im } f$, for example. Hence, f is not an isomorphism.

ii) f is not an isomorphism, since $\text{Ker } f = 10\mathbb{Z} \neq \{0\}$.

iii) From Block 1, Calculus, you know that $\overline{z_1 + z_2} = \overline{z}_1 + \overline{z}_2$, and $\overline{z_1 z_2} = \overline{z}_1 \cdot \overline{z}_2$. Use this to show that f is a ring homomorphism.

Next, for any $a + ib \in \mathbb{C}$, $f(a - ib) = a + ib$. So $\text{Im } f = \mathbb{C}$.
Also, $\text{Ker } f = \{a + ib \mid a - ib = 0\} = \{0\}$.

Thus, f is an isomorphism.

iv) Note that $|z| \geq 0$. Use this to show that f is not surjective. Hence, f cannot be an isomorphism.

E29) Let $x, y \in R_2$ and $\phi^{-1}(x) = r$, $\phi^{-1}(y) = s$. Then $x = \phi(r)$ and $y = \phi(s)$.
Therefore, $x + y = \phi(r) + \phi(s) = \phi(r + s)$, and $xy = \phi(rs)$.
$\therefore \phi^{-1}(x + y) = r + s = \phi^{-1}(x) + \phi^{-1}(y)$, and
$\phi^{-1}(xy) = rs = \phi^{-1}(x) \cdot \phi^{-1}(y)$.
Thus, ϕ^{-1} is a ring homomorphism.
You already know that it is bijective.
Thus, ϕ^{-1} is an isomorphism.

E30) Let $f : R_1 \to R_2$ and $g : R_2 \to R_3$ be ring isomorphisms. From Theorem 10, you know that $g \circ f$ is a homomorphism. For the rest, proceed as you did for solving E19, Unit 8.

E31) i) Since $U(\mathbb{Q}) = \mathbb{Q}^*$ and $U(\mathbb{Z}) = \{1, -1\}$, $\mathbb{Q} \ncong \mathbb{Z}$ (by Example 14). Thus, this is false.

ii) See Example 20, Unit 8, for why this is true.

iii) Here $\mathbb{Z}$ is infinite, but $\mathbb{M}_n(\mathbb{Z}_m)$ is finite. Thus, this is false.

iv) Since $\mathbb{Z}_3$ is finite and $\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$ is infinite, this is false.

v) False. Consider $\mathbb{Z}$ and $2\mathbb{Z}$. You know that $\mathbb{Z}$ and $2\mathbb{Z}$ are isomorphic groups. However, $\mathbb{Z}$ is a ring with unity, while $2\mathbb{Z}$ does not have unity. Hence, they are not isomorphic rings.

E32) Define $f: \wp(X) \to \mathbb{Z}_2 \times \mathbb{Z}_2$ by

$f(\phi) = (0, 0), f(\{1\}) = (1, 0), f(\{2\}) = (0, 1), f(X) = (1, 1).$

Now, f is a well-defined bijection, as you can see.

You should check, case by case, that for $A, B \in \wp(X)$,

$f(A \Delta B) = f(A) + f(B)$, and $f(A \cap B) = f(A) \cdot f(B)$.

Thus, $\wp(X) \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$.

E33) Example 1: $\mathbb{Z}/\{0\} \simeq \mathbb{Z}$.

Example 2: $(\mathbb{M}_n(\mathbb{R})/\mathbb{M}_n(\mathbb{R})) \simeq \{\mathbf{0}\}$.

Example 3 and 4: $R/\{0\} \simeq R$, and $(R/R) \simeq \{0\}$, for any ring R.

Example 5: $\mathbb{Z}/s\mathbb{Z} \simeq \mathbb{Z}_s$, $\forall\ s \in \mathbb{N}$.

Example 6: $\mathbb{Z}_6/\{\bar{0}, \bar{3}\} \simeq \mathbb{Z}_3$, i.e., $(\mathbb{Z}_6/\bar{3}\mathbb{Z}_6) \simeq \mathbb{Z}_3$.

Example 7: $\text{Ker } \phi = \{f \in C[0,1] \mid f(1/2) = 0\}$, and

$\text{Im } \phi = \mathbb{R}$.

So $C[0, 1]/\text{Ker } \phi \simeq \mathbb{R}$.

Example 8: $\mathbb{Z} \simeq \{nI \mid n \in \mathbb{Z}\}$, using the fact of Example 1, i.e., $\mathbb{Z}/\{0\} \simeq \mathbb{Z}$, and Theorem 10.

Here $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$.

Example 9: $\wp(X)/\wp(Y^c) \simeq \wp(Y)$.

E34) Define $f: \mathbb{R}[x] \to \mathbb{R} : f(a_0 + a_1x + \cdots + a_nx^n) = a_0$.

Then f is the evalution map ϕ_0. As in E2, you should prove that f is a homomorphism, $\text{Ker } f = < x >$ and $\text{Im } f = \mathbb{R}$.

Hence, by FTH, $\mathbb{R}[x]/< x > \simeq \mathbb{R}$.

E35) You should show that $R \neq \phi$, and that $A - B \in R$ and $AB \in R\ \forall\ A, B \in R$.

Further, prove that $AB = BA\ \forall\ A, B \in R$. Note that $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in R$.

Next, prove that ϕ is a ring homomorphism.

After this, show that $\text{Ker } \phi = \left\{ \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} r \;\middle|\; r \in \mathbb{Z} \right\}$.

Note that $\text{Im } \phi = \mathbb{Z}$, because for any $n \in \mathbb{Z}$, $n = \phi\left(\begin{bmatrix} n & 0 \\ 0 & n \end{bmatrix} \right)$.

So FTH tells us that $R/\text{Ker } \phi \simeq \mathbb{Z}$.

E36) Since $r \in U(R)$, f_r is well-defined.

Now, for $x, y \in R$,

$$f_r(x+y) = r^{-1}(x+y)r = r^{-1}xr + r^{-1}yr$$
$$= f_r(x) + f_r(y), \text{ and}$$
$$f_r(xy) = r^{-1}xyr = (r^{-1}xr)(r^{-1}yr)$$
$$= f_r(x) \cdot f_r(y).$$

Thus, f_r is a homomorphism.

Next, $\text{Ker } f_r = \{x \in R \mid r^{-1}xr = 0\}$.

Since r is a unit, $\exists\ s \in R$ s.t. $rs = 1 = sr$.

So $r^{-1}xr = 0$ iff $s^{-1}r^{-1}xrs = s^{-1}0\ s = 0$, i.e., iff $x = 0$.

Thus, $\text{Ker } f_r = \{0\}$.

Also, for any $s \in R$, $f_r(rsr^{-1}) = s$.

So $\text{Im } f_r = R$.

Thus, f_r is an automorphism, and FTH tells us that $R/\{0\} \simeq R$.

E37) Define $f : S \to R/I : f(s) = s + I$. Show that f is a homomorphism, and $\text{Ker } f = S \cap I$.

Thus, by FTH, $(S/(S \cap I)) \simeq \text{Im } f$, a subring of R/I.

Hence, we can treat $(S/S \cap I)$ as a subring of R/I.

In E38, Unit 12, you have given an example to show that $(S/S \cap I)$ need not be an ideal of R/I.

E38) Since I is an ideal of R and $I \subseteq S + I$, it is an ideal of $S + I$.

Thus, $(S + I)/I$ is a well-defined ring.

Define $f : S \to (S + I)/I : f(x) = x + I$.

As you did in Theorem 12 of Unit 8, you should prove that f is well-defined.

Then, you should check that $f(x + y) = f(x) + f(y)$, and $f(xy) = f(x)f(y)\ \forall\ x, y \in S$.

Further, show that f is surjective and $\text{Ker } f = S \cap I$.

Thus, $S/(S \cap I) \simeq (S + I)/I$, by Theorem 11.

E39) Define $f : R/J \to R/I : f(r + J) = r + I$.

As you did in Theorem 14, Unit 8, you can check that f is well-defined.

Next, prove that f is a ring homomorphism, f is surjective and $\text{Ker } f = I/J$.

Thus, I/J is an ideal of R/J, and $(R/J)/(I/J) \simeq R/I$.

E40) i) By Example 15, $(\mathbb{Z}/m\mathbb{Z}) \simeq \mathbb{Z}_m\ \forall\ m \in \mathbb{N}$.

So $\mathbb{Z}_{15} \simeq \mathbb{Z}/15\mathbb{Z}$, $\bar{5}\mathbb{Z}_{15} \simeq \bar{5}(\mathbb{Z}/15\mathbb{Z}) = 5\mathbb{Z}/15\mathbb{Z}$.

So, by the third isomorphism theorem, $\mathbb{Z}_{15}/<\bar{5}> \simeq \mathbb{Z}/\bar{5}\mathbb{Z} \simeq \mathbb{Z}_5$.

ii) Again, as in (i) above,

$$\mathbb{Z}_m/\bar{n}\mathbb{Z}_m \simeq (\mathbb{Z}/m\mathbb{Z})\Big/(n\mathbb{Z}/m\mathbb{Z}) \simeq \mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}_n.$$

E41) Let f be an automorphism of $\mathbb{Q}$. Then, for any $\frac{p}{q} \in \mathbb{Q}$,

$f\left(\frac{p}{q}\right) = \frac{m}{n}$ for some $m, n \in \mathbb{Z}, n \neq 0$.

So $f(p) = f\left(q\frac{p}{q}\right) = qf\left(\frac{p}{q}\right) = q\frac{m}{n}$, since f is a homomorphism.

Also $f(p) = f(p \cdot 1) = pf(1)$

$= p.$

So $p = q\left(\frac{m}{n}\right)$.

$\therefore \frac{p}{q} = \frac{m}{n}$.

$\therefore f\left(\frac{p}{q}\right) = \frac{p}{q} \ \forall \ \frac{p}{q} \in \mathbb{Q}.$

i.e., $f = I$, the identity homomorphism.

Thus, the only automorphism of $\mathbb{Q}$ is I.

In fact, the only epimorphism from $\mathbb{Q}$ to $\mathbb{Q}$ is I.

MISCELLANEOUS EXAMPLES AND EXERCISES

As in the previous blocks, the few examples and exercises, given below cover the concepts and processes you have studied in this block. Studying the examples, and solving the exercises, will give you a better understanding of the concepts concerned. This will also give you more practice in solving such problems.

Example 1: Find the distinct cosets of the ideal $< 2-i >$ in $\mathbb{Z}[i]$.

Solution: Any coset of $< 2-i >$ is of the form $a+bi+< 2-i >,\ a, b \in \mathbb{Z}$.
In $R = \mathbb{Z}[i]/< 2-i >$, note that $\overline{2-i} = \bar{0}$. So $\bar{2} = \bar{i}$.
$\therefore \overline{a+ib} = \bar{a} + \bar{i}\,\bar{b} = \bar{a} + \bar{2}\,\bar{b}\ \forall\ a, b \in \mathbb{Z}$.
Also $\bar{2} = \bar{i} \Rightarrow \bar{4} = -\bar{1} \Rightarrow \bar{5} = \bar{0}$.
So, $\overline{a+ib} = \overline{a+2b} = \bar{x}$, where $a + 2b \equiv x \pmod 5$.
For example, $\overline{-2+i3} = -\bar{2} + \bar{2}\cdot\bar{3} = \bar{4}$ and $\overline{2+i3} = \bar{2} + \bar{2}\cdot\bar{3} = \bar{8} = \bar{3}$, since $8 \equiv 3 \pmod 5$.
Further, to prove that $\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}$ are distinct cosets of $< 2-i >$ in R, suppose, to the contrary that, say $\bar{1} = \bar{2}$.
Then $\bar{2} - \bar{1} = \bar{0}$, i.e., $1 \in < 2-i >$.
Then $1 = (2-i)(c+id)$ for some $c, d \in \mathbb{Z}$.
$\Rightarrow 1 = 2c + d$ and $0 = -c + 2d$.
$\Rightarrow d = 1/5$, a contradiction.
Thus, $\bar{1} = \bar{2}$.

Similarly, show that equating any of $\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}$, will lead to a contradiction.
Hence, the distinct elements of R are $\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}$.
In fact, $R \simeq \mathbb{Z}_5$.

***

Example 2: Show that no element of the set $\{3+4k \mid k \in \mathbb{Z}\}$ is a sum of the squares of two integers.

Solution: We will prove this by contradiction.
Suppose $\exists\ k, a, b \in \mathbb{Z}$ s.t.
$3 + 4k = a^2 + b^2$. …(1)
Then apply the natural homomorphism $p : \mathbb{Z} \to \mathbb{Z}_4 : p(m) = \bar{m}$, to (1). We get
$\bar{3} = \bar{a}^2 + \bar{b}^2$ for some $\bar{a}, \bar{b}$ in $\mathbb{Z}_4$. …(2)
Now $\bar{a} = \bar{0}, \bar{b} = \bar{0}$ doesn't satisfy (2). Similarly, you should check that none of the 16 possibilities for $(\bar{a}, \bar{b})$ satisfy (2).
So we reach a contradiction.
Thus, there are no $a, b \in \mathbb{Z}$ s.t. $3 + 4k = a^2 + b^2$, for any $k \in \mathbb{Z}$.

***

Example 3: Give an example, with justification, of a non-trivial subring S with unity of $\mathbb{Z}_{30}$, with S having a unity different from $\bar{1}$.

Solution: For example, take $S = 3\mathbb{Z}_{30}$. Then S is a non-trivial subring of $\mathbb{Z}_{30}$, and $\overline{1} \notin S$.
You should draw up the Cayley table for multiplication in S. From the table, you will find that $3 \cdot \overline{7} = \overline{21}$ is the unity in S.

***

Example 4: Find $U(\mathbb{Z}_{10} \times \mathbb{Z}_{15})$.

Solution: Let $U = U(\mathbb{Z}_{10} \times \mathbb{Z}_{15})$.
Now $(a(\text{mod}10), b(\text{mod}15)) \in U$
$\Leftrightarrow (a(\text{mod}10), b(\text{mod}15))(c(\text{mod}10), d(\text{mod}15)) = (1(\text{mod}10), 1(\text{mod}15))$ for some $c, d \in \mathbb{Z}$.
$\Leftrightarrow ac \equiv 1(\text{mod}10)$ and $bd \equiv 1(\text{mod}15)$ for some $c, d \in \mathbb{Z}$.
$\Leftrightarrow \overline{a} \in U(\mathbb{Z}_{10})$ and $\overline{b} \in U(\mathbb{Z}_{15})$.
Thus, $U(\mathbb{Z}_{10} \times \mathbb{Z}_{15}) = U(\mathbb{Z}_{10}) \times U(\mathbb{Z}_{15})$.

***

Example 5: Determine all ring homomorphisms from $\mathbb{Z} \times \mathbb{Z}$ to $\mathbb{Z}$.

Solution: Let $\phi : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ be a homomorphism.
If ϕ is not the zero homomorphism, then
$\phi(1, 1) = 1$, since $(1, 1)$ is the unity of $\mathbb{Z} \times \mathbb{Z}$ and 1 is the unity of $\mathbb{Z}$.
i.e., $\phi[(1, 0) + (0, 1)] = 1$, …(3)
i.e., $\phi((1, 0)) + \phi((0, 1)) = 1$.
Let $\phi((1, 0)) = m$.
Also, $\phi((1, 0)) = \phi((1, 0)(1, 0)) = \phi((1, 0))\ \phi((1, 0))$. So $m = m^2$.
Thus, m is an idempotent in $\mathbb{Z}$. $\therefore m = 0, 1$.
If $m = 0$, then $\phi((0, 1)) = 1$, and if $m = 1$, then $\phi((0, 1)) = 0$, by (3).
Now $\phi((x, y)) = \phi[x(1, 0) + y(0, 1)] = x\phi((1, 0)) + y\phi((0, 1))\ \forall\ x, y \in \mathbb{Z}$.
So, if $\phi((1, 0)) = 0$, then $\phi((x, y)) = y\ \forall\ x, y \in \mathbb{Z}$.
If $\phi((0, 1)) = 0$, then $\phi((x, y)) = x\ \forall\ x, y \in \mathbb{Z}$.
Thus, the only possible homomorphisms from $\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ are ϕ_1, ϕ_2, ϕ_3, defined by
$\phi_1((x, y)) = x$, $\phi_2((x, y)) = y$, $\phi_3((x, y)) = 0\ \forall\ x, y \in \mathbb{Z}$.

***

Example 6: Show that $S = \left\{ \frac{m}{2^n} \middle| m, n \in \mathbb{Z}, n > 0 \right\}$ is the smallest subring of $\mathbb{Q}$ containing $\frac{1}{2}$.

Solution: First, $S \subseteq \mathbb{Q}$.
Also, for $\frac{m_1}{2^{n_1}}, \frac{m_2}{2^{n_2}} \in S$, suppose $n_1 \geq n_2$. Then
$\frac{m_1}{2^{n_1}} - \frac{m_2}{2^{n_2}} = \frac{1}{2^{n_1}}(m_1 - 2^{n_1 - n_2} \cdot m_2) \in S$.

Also $\frac{m_1}{2^{n_1}} \cdot \frac{m_2}{2^{n_2}} = \frac{m_1 m_2}{2^{n_1+n_2}} \in S$.

Hence, S is a subring of $\mathbb{Q}$.

Let T be a subring of $\mathbb{Q}$ s.t. $\frac{1}{2} \in T$.

Then $\frac{m}{2^n} \in T \ \forall\ m, n \in \mathbb{Z}$ and $n > 0$.

So $S \subseteq T$.

Thus, S is the smallest subring of $\mathbb{Q}$ containing $\frac{1}{2}$.

***

Example 7: Find all the possible ring homomorphisms from $\mathbb{Z}_6$ to $\mathbb{Z}_6$.

Solution: One is the trivial homomorphism, of course. Let's look for the others.

Let $\phi : \mathbb{Z}_6 \to \mathbb{Z}_6$ be a non-trivial homomorphism.

Then $\phi(\bar{1})$ is the unity of $\text{Im}\,\phi$, say $\phi(\bar{1}) = \bar{m}$ in $\mathbb{Z}_6$, where $\bar{m} \neq \bar{0}$.

Then $\bar{m}^2 = \bar{m}$.

This is true only for $\bar{m} = \bar{1}, \bar{3}, \bar{4}$ in $\mathbb{Z}_6$.

So $\phi_1 : \mathbb{Z}_6 \to \mathbb{Z}_6 : \phi_1(\bar{n}) = \bar{n}$, (i.e., $\phi_1 = I$),

$\phi_2 : \mathbb{Z}_6 \to \mathbb{Z}_6 : \phi_2(\bar{n}) = \overline{3n}$, and

$\phi_3 : \mathbb{Z}_6 \to \mathbb{Z}_6 : \phi_3(\bar{n}) = \overline{4n}$

are the non-trivial homomorphisms.

Here, note that $\text{Im}\,\phi_1 = \mathbb{Z}_6$, $\text{Im}\,\phi_2 = \{\bar{0}, \bar{3}\}$, $\text{Im}\,\phi_3 = \{\bar{0}, \bar{2}, \bar{4}\}$; and $\{\bar{0}, \bar{3}\}$ is a subring of $\mathbb{Z}_6$, with unity $\bar{3}$; $\{\bar{0}, \bar{2}, \bar{4}\}$ is a subring of $\mathbb{Z}_6$, with unity $\bar{4}$.

***

Miscellaneous Exercises

E1) Let R be a ring. Show that $a^2 - b^2 = (a - b)(a + b)\ \forall\ a, b \in R$ iff R is commutative.

E2) Which of the following statements are true? Justify each answer.

i) $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ is a Boolean ring (ref. E24, Unit 10).

ii) $\mathbb{Z}_6$ is a subring of $\mathbb{Z}_{12}$.

iii) $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ and $\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$ commute with each other in $\mathbb{M}_2(\mathbb{Z})$.

iv) $\mathbb{Z} \times 2\mathbb{Z}$ is a ring with unity.

v) $U(\mathbb{Z} \times \mathbb{Z}) = U(\mathbb{Z})$.

E3) Draw the Cayley tables for $(\bar{2}\mathbb{Z}_{10}, +, \cdot)$. Hence decide if it is a commutative ring with unity or not.

E4) Are $2\mathbb{Z}$ and $3\mathbb{Z}$ isomorphic rings? Are $2\mathbb{Z}$ and $4\mathbb{Z}$ isomorphic rings? Give reasons for your answers.

E5) Check whether or not $S = \left\{ \begin{bmatrix} m & m-n \\ m-n & n \end{bmatrix} \middle| m, n \in \mathbb{Z} \right\}$ is a subring of $\mathbb{M}_2(\mathbb{Z})$. Is it an ideal of $\mathbb{M}_2(\mathbb{Z})$? Why?

E6) Check whether or not $S = \left\{ \begin{bmatrix} m & m+n \\ m+n & n \end{bmatrix} \middle| m, n \in \mathbb{Z} \right\}$ is a subring of $\mathbb{M}_2(\mathbb{Z})$. Is it an ideal of $\mathbb{M}_2(\mathbb{Z})$? Why?

E7) Show that $I = \mathbb{M}_2(2\mathbb{Z})$ is an ideal of $\mathbb{M}_2(\mathbb{Z})$. Also prove that $\mathbb{M}_2(\mathbb{Z}) \big/ \mathbb{M}_2(2\mathbb{Z}) \simeq \mathbb{M}_2(\mathbb{Z}_2)$.

E8) How many elements are in $\mathbb{Z}[i] / < i+3 >$? Why?

E9) Find all possible ring homomorphisms from $\mathbb{Z}_{20}$ to $\mathbb{Z}_{30}$.

E10) Prove that $\{2 + 8k \mid k \in \mathbb{Z}\}$ contains no cube of an integer.

SOLUTIONS / ANSWERS

E1) R is commutative.
$\Leftrightarrow ab = ba \ \forall\ a, b \in R$
$\Leftrightarrow a^2 - b^2 = (a-b)(a+b) \ \forall\ a, b \in R.$

E2) i) True. For any $(\bar{x}_1, \bar{x}_2, \bar{x}_3) \in \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, $\bar{x}_i = \bar{0}$ or $\bar{1} \ \forall\ i = 1, 2, 3.$
$\therefore (\bar{x}_1, \bar{x}_2, \bar{x}_3) \cdot (\bar{x}_1, \bar{x}_2, \bar{x}_3) = (\bar{x}_1^2, \bar{x}_2^2, \bar{x}_3^2) = (\bar{x}_1, \bar{x}_2, \bar{x}_3).$

ii) False. $\mathbb{Z}_6 \not\subset \mathbb{Z}_{12}$.

iii) You should check that $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \neq \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$.

iv) Since $2\mathbb{Z}$ is without unity, so is $\mathbb{Z} \times 2\mathbb{Z}$.

v) The elements of $\mathbb{Z} \times \mathbb{Z}$ are ordered pairs of elements of $\mathbb{Z}$. Hence, this is false.

E3)

$+$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{6}$	$\bar{8}$
$\bar{0}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{6}$	$\bar{8}$
$\bar{2}$	$\bar{2}$	$\bar{4}$	$\bar{6}$	$\bar{8}$	$\bar{0}$
$\bar{4}$	$\bar{4}$	$\bar{6}$	$\bar{8}$	$\bar{0}$	$\bar{2}$
$\bar{6}$	$\bar{6}$	$\bar{8}$	$\bar{0}$	$\bar{2}$	$\bar{4}$
$\bar{8}$	$\bar{8}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{6}$

$\cdot$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{6}$	$\bar{8}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{2}$	$\bar{0}$	$\bar{4}$	$\bar{8}$	$\bar{2}$	$\bar{6}$
$\bar{4}$	$\bar{0}$	$\bar{8}$	$\bar{6}$	$\bar{4}$	$\bar{2}$
$\bar{6}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{6}$	$\bar{8}$
$\bar{8}$	$\bar{0}$	$\bar{6}$	$\bar{2}$	$\bar{8}$	$\bar{4}$

From the tables, we can see that $\bar{2}\mathbb{Z}_{10}$ is closed w.r.t. addition and multiplication $(\mathrm{mod}\ 10)$.

Further, both addition and multiplication are commutative.

Next, $\bar{0}$ is the additive identity and $\bar{6}$ is the unity.

Also, every element has an additive inverse, and the multiplicative inverses are:
$\bar{2}^{-1} = \bar{8}, \bar{4}^{-1} = \bar{4}, \bar{6}^{-1} = \bar{6}, \bar{8}^{-1} = \bar{2}.$
You can also use the tables to check that the rest of the requirements for $< \bar{2} >$ to be a commutative ring with unity are satisfied.

E4) Suppose $2\mathbb{Z} \simeq 3\mathbb{Z}$. Then $\mathbb{Z}/2\mathbb{Z} \simeq \mathbb{Z}/3\mathbb{Z}$, i.e., $\mathbb{Z}_2 \simeq \mathbb{Z}_3$, a contradiction.

Suppose $\phi : 2\mathbb{Z} \to 4\mathbb{Z}$ is an isomorphism, and let $\phi(2) = 4n$, for some $n \in \mathbb{Z}$.
Then $\phi(4) = \phi(2+2) = \phi(2) + \phi(2) = 8n.$
Also $\phi(4) = \phi(2 \cdot 2) = \phi(2) \cdot \phi(2) = (4n)^2 = 16n^2.$
So $8n = 16n^2 \Rightarrow 2n = 1$, a contradiction, since $n \in \mathbb{Z}$.
$\therefore 2\mathbb{Z} \ncong 4\mathbb{Z}.$

E5) First, $S \neq \emptyset$, since $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in S$. Also $S \subseteq \mathbb{M}_2(\mathbb{Z})$.

Next, let $\begin{bmatrix} a & a-b \\ a-b & b \end{bmatrix}$ and $\begin{bmatrix} m & m-n \\ m-n & n \end{bmatrix} \in S$.

Then

$$\begin{bmatrix} a & a-b \\ a-b & b \end{bmatrix} - \begin{bmatrix} m & m-n \\ m-n & n \end{bmatrix} = \begin{bmatrix} a-m & (a-m)-(b-n) \\ (a-m)-(b-n) & b-n \end{bmatrix} \in S,$$

and

$$\begin{bmatrix} a & a-b \\ a-b & b \end{bmatrix} \cdot \begin{bmatrix} m & m-n \\ m-n & n \end{bmatrix} = \begin{bmatrix} am+(a-b)(m-n) & a(m-n)+(a-b)n \\ (a-b)m+b(m-n) & (a-b)(m-n)+bn \end{bmatrix}$$

$$= \begin{bmatrix} 2am-bm-an+bn & am-bn \\ am-bn & am-bm-an+2bn \end{bmatrix} = \begin{bmatrix} \alpha & \beta-\alpha \\ \alpha-\beta & \beta \end{bmatrix} \in S,$$

where $\alpha = 2am-bm-an+bn$ and $\beta = am-bm-an+2bn$.

So S is a subring of $\mathbb{M}_2(\mathbb{Z})$.

However, S is not an ideal of $\mathbb{M}_2(\mathbb{Z})$. For instance,

$\begin{bmatrix} 3 & 1 \\ 1 & 2 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 4 & 0 \\ 3 & 0 \end{bmatrix} \notin S$ though $\begin{bmatrix} 3 & 1 \\ 1 & 2 \end{bmatrix} \in S$.

E6) Here S is not a subring since, for example,

$\begin{bmatrix} 2 & 3 \\ 3 & 1 \end{bmatrix}, \begin{bmatrix} 2 & 2 \\ 2 & 0 \end{bmatrix} \in S$, but

$\begin{bmatrix} 2 & 3 \\ 3 & 1 \end{bmatrix} \cdot \begin{bmatrix} 2 & 2 \\ 2 & 0 \end{bmatrix} = \begin{bmatrix} 10 & 4 \\ 8 & 6 \end{bmatrix} \notin S$.

Hence, S is not an ideal either.

E7) You should show that $I = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \middle| a, b, c, d \in 2\mathbb{Z} \right\}$ is an ideal of $\mathbb{M}_2(\mathbb{Z})$.

Define $\phi : \mathbb{M}_2(\mathbb{Z}) \to \mathbb{M}_2(\mathbb{Z}_2) : \phi\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right) = \begin{bmatrix} \bar{a} & \bar{b} \\ \bar{c} & \bar{d} \end{bmatrix}$.

Check that ϕ is well-defined, and an onto ring homomorphism. Further,

$$\text{Ker } \phi = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \middle| \bar{a} = \bar{0} = \bar{b} = \bar{c} = \bar{d} \text{ in } \mathbb{Z}_2 \right\}$$

$$= \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \middle| a, b, c, d \in 2\mathbb{Z} \right\}$$

$$= \mathbb{M}_2(2\mathbb{Z}).$$

Now apply FTH to get the result.

E8) As in Example 1, show that $\overline{10} = \bar{0}$ in $\mathbb{Z}[i]/\langle i+3 \rangle$.

Also $i = -3 \Rightarrow \bar{i} = -\bar{3} = \bar{7}$.

Hence, show that $\mathbb{Z}[i]/\langle i+3 \rangle = \{\bar{0}, \bar{1}, \ldots, \bar{9}\}$.

E9) Let $\phi : \mathbb{Z}_{20} \to \mathbb{Z}_{30}$ be a ring homomorphism.

Since $\overline{1}$ generates $\mathbb{Z}_{20}$, $\phi(\overline{1})$ determines ϕ.

Let $\phi(\overline{1}) = m (\mathrm{mod}\, 30)$.

Now, in $\mathbb{Z}_{20}$, $\overline{1} = \overline{21}$. Also, $(\overline{1})^2 = \overline{1}$.

So $\phi(\overline{1}) = \phi(\overline{21}) = 21\phi(\overline{1})$, and $[\phi(\overline{1})]^2 = \phi(\overline{1})$.

Thus, $\overline{m} = 21\overline{m}$ and $\overline{m}^2 = \overline{m}$ in $\mathbb{Z}_{30}$.

So $30 \mid 20m$ and $30 \mid m(m-1)$ in $\mathbb{Z}$.

Now, $30 \mid 20m \Rightarrow 3 \mid 2m \Rightarrow 3 \mid m$.

So $\overline{m} = \overline{0}, \overline{3}, \overline{6}, \ldots, \overline{27}$ in $\mathbb{Z}_{30}$.

Now, which of these values satisfy $\overline{m}^2 = \overline{m}$? They are $\overline{0}, \overline{6}, \overline{15}, \overline{21}$.

Accordingly, there are 4 ring homomorphisms from $\mathbb{Z}_{20} \to \mathbb{Z}_{30}$, namely,

$\phi_1 \equiv \mathbf{0}$,

$\phi_2 : \mathbb{Z}_{20} \to \mathbb{Z}_{30} : \phi_2(\overline{n}) = \overline{6n}$,

$\phi_3 : \mathbb{Z}_{20} \to \mathbb{Z}_{30} : \phi_3(\overline{n}) = \overline{15n}$,

$\phi_4 : \mathbb{Z}_{20} \to \mathbb{Z}_{30} : \phi_4(\overline{n}) = \overline{21n}$.

E10) Suppose $2 + 8k = n^3$, for some $n \in \mathbb{Z}$. …(4)

Then, applying the canonical homomorphism $p : \mathbb{Z} \to \mathbb{Z}_8 : p(x) = \overline{x}$,

to (4), we get $\overline{2} = \overline{n}^3$ in $\mathbb{Z}_8$.

You should check that there is no such $\overline{n}$ in $\mathbb{Z}_8$.

So we reach a contradiction.

Thus, $\{2 + 8k \mid k \in \mathbb{Z}\}$ contains no element of the form n^3, $n \in \mathbb{Z}$.