# UNIT 9 RINGS

## Structure



## 9.1 INTRODUCTION

With this unit we start the study of algebraic systems with two binary operations satisfying certain properties, Z, Q and R are examples of such a system, which we shall call a ring.

Now, you know that both addition and multiplication are binary operations on Z. Further, Z is an abelian group under addition, Though it is not a group under multiplication, multiplication is associative. Also, addition and multiplication are related by the distributive laws

$a(b + c) = ab + ac$, and $(a + b)c = ac + bc$

for all integers a, b and c. We generalise these very properties of the binary operations to define a ring in general. This definition is due to the famous algebraist Emmy Noether.

Fig. 1 : Emmy Noether (1882-1935)

After defining rings we shall give several examples of rings. We shall also give some properties of rings that follow from the definition itself. Finally, we shall discuss certain types of rings that are obtained when we impose more restrictions on the "multiplication" in the ring.

As the contents suggest, this unit lays the foundation for the rest of this course. So make sure that you have attained the following objectives before going to the next unit.

### Objectives

After reading 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;
- define and give examples of commutative rings, rings with identity and commutative rings with identity.

## 9.2 WHAT IS A RING?

You are familiar with 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 multiplication is associative and distributes over addition. These properties of addition and multiplication of integers allow us to say that the system (Z, +, .) is a ring. But, what do we mean by a ring?

**Definition**: A non-empty set R together with two binary operations, usually called addition (denoted by +) and multiplication (denoted by .), is called a **ring** if the following axioms are satisfied :

R 1) $a + b = b + a$ for all a, b in R, i.e., addition is commutative.

R 2) $(a + b) + c = a + (b + c)$ for all a, b, c in R, i.e., addition is associative.

R 3) 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.

R 4) 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.

R 5) $(a . b).c = a.(b . c)$ for all a, b, c in R, i.e., multiplication is associative.

R 6) $a.(b + c) = a.b + a.c$, and
$(a + b).c = a.c + b.c$
for all a, b, c in R,
i.e., multiplication distributes over addition from the left as well as the right.

The axioms R1–R4 say that (R, +) is an abelian group. The axiom R5 says that multiplication is associative. Hence, we can say that the system (R, +, .) is a ring if

i) (R, +) is an abelian group,

ii) (R, .) is a semigroup, and

iii) for all a, b, c in R, $a.(b + c) = a.b + a.c$, and $(a + b).c = a.c + b.c$.

From Unit 2 you know that the addition 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.

By convention, we write $a - b$ for $a + (-b)$.

Let us look at some examples of rings now. You have already seen that **Z** is a ring. What about the sets **Q** and R? Do (Q, +, .) and (R, +, .) satisfy the axioms R1-R6? They do. Therefore, these systems are rings.

The following example provides us with another set of examples of rings

**Example 1** : Show that (n**Z**, +, .) is a ring, where $n \in Z$.

**Solution** : You know that $n\mathbf{Z} = \{nm \mid m \in Z\}$ is an abelian group with respect to addition. You also know that multiplication in n**Z** is associative and distributes over addition from the right as well as the left. Thus, n**Z** is a ring under the usual addition and multiplication.

The underlying set of a ring (R, +, .) is the set R.

So far the examples that we have considered have been **infinite rings,** that is, their underlying sets have been infinite sets. Now let us look at a **finite ring,** that is, a ring (R, +, .) where R is a finite set. Our example is the set $Z_n$, that you studied in Unit 2 (Sec. 2.5.1). Let us briefly recall the construction of $\mathbf{Z}_n$, the set of residue classes modulo n.

If a and b are integers, we say that a is congruent to b modulo n if $a - b$ is divisible by n; in symbols, $a \equiv b \pmod n$ if $n \mid (a - b)$. The relation 'congruence modulo n' is an equivalence relation in **Z.** The equivalence class containing the integer a is
$\bar{a} = \{b \in Z \mid a - b \text{ is divisible by } n\}$
$= \{a + mn \mid m \in \mathbf{Z}\}$.

It is called the **congruence class of a modulo n** or the **residue class of a modulo n.** The set of all equivalence classes is denoted by $Z_n$. So
$\mathbf{Z}_n = \{\bar{0}, \bar{1}, \bar{2}, ...., \overline{n-1}\}$.

We define addition and multiplication of classes in terms of their representatives by
$\bar{a} + \bar{b} = \overline{a + b}$ and
$\bar{a}.\bar{b} = \overline{ab}\ \forall\ \bar{a}, \bar{b} \in \mathbf{Z}_n$.

In Sec. 2.5.1 you have seen that these operations are well defined in $Z_n$. To help you regain some practice in adding and multiplying in $Z_n$, consider the following Cayley tables for $Z_5$.

**Addition in $\mathbf{Z}_5$**

| + | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ | $\bar{4}$ |
|---|---|---|---|---|---|
| $\bar{0}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ | $\bar{4}$ |
| $\bar{1}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ | $\bar{4}$ | $\bar{0}$ |
| $\bar{2}$ | $\bar{2}$ | $\bar{3}$ | $\bar{4}$ | $\bar{0}$ | $\bar{1}$ |
| $\bar{3}$ | $\bar{3}$ | $\bar{4}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ |
| $\bar{4}$ | $\bar{4}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ |

**Multiplication in $\mathbf{Z}_5$**

| | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ | $\bar{4}$ |
|---|---|---|---|---|---|
| $\bar{0}$ | $\bar{0}$ | $\bar{0}$ | $\bar{0}$ | $\bar{0}$ | $\bar{0}$ |
| $\bar{1}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ | $\bar{4}$ |
| $\bar{2}$ | $\bar{0}$ | $\bar{2}$ | $\bar{4}$ | $\bar{1}$ | $\bar{3}$ |
| $\bar{3}$ | $\bar{0}$ | $\bar{3}$ | $\bar{1}$ | $\bar{4}$ | $\bar{2}$ |
| $\bar{4}$ | $\bar{0}$ | $\bar{4}$ | $\bar{3}$ | $\bar{2}$ | $\bar{1}$ |

Now let us go back to looking for a finite ring.

**Example 2** : Show that ($\mathbf{Z}_n$, +, .) is a ring.

**Solution** : You already know that ($\mathbf{Z}_n$, +) is an abelian group, and that multiplication is associative in $\mathbf{Z}_n$. Mow we need to see if the axiom R6 is satisfied.

For any $\bar{a}, \bar{b}, \bar{c} \in Z_n$,

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

Thus, $\bar{a}.(\bar{b} + \bar{c}) = \bar{a}.\bar{b} + \bar{a}.\bar{c}$.

Similarly, $(\bar{a} + \bar{b}).\bar{c} = \bar{a}.\bar{c} + \bar{b}.\bar{c} \ \forall \ \bar{a}, \bar{b}, \bar{c} \in Z_n$.

So, $(Z_n, +, .)$ satisfies the axioms R1 – R6. Therefore, it is a ring.

Try this exercise now.

---

E 1) Write out the Cayley tables for addition and multiplication in $Z_6^*$, the set of non-zero elements of $Z_6$. Is $(Z_6^*, +, .)$ a ring? Why?

---

Now let us look at a ring whose underlying set is a subset of C.

Example 3 : Consider the set
$Z + iZ = \{ m + in \mid m$ and $n$ are integers $\}$, where $i^2 = -1$.
We define '+' and '.' in $Z + iZ$ to be the usual addition and multiplication of complex numbers. Thus, for $m + in$ and $s + it$ in $Z + iZ$,
$(m + in) + (s + it) = (m + s) + i(n + t)$, and
$(m + in) . (s + it) = (ms - nt) + i(mt + ns)$.

Verify that $Z + iZ$ is a ring under this addition and multiplication. (This ring is called the ring of Gaussian integers, after the mathematician Carl Friedrich Gauss.)

Solution : Check that $(Z + iZ, +)$ is a subgroup of $(C, +)$. Thus, the axioms R1 – R4 are satisfied. You can also check that
$((a + ib) . (c + id)) . (m + in) = (a + ib) . ((c + id) . (m + in))$
$\forall \ a + ib, c + id, m + in \in Z + iZ$.

This shows that R5 is also satisfied.

Finally, you can check that the right distributive law holds, i.e.,
$((a + ib) + (c + id)) . (m + in) = (a + ib) . (m + in) + (c + id) . (m + in)$ for any $a + ib, c + id, m + in \in Z + iZ$.

Similarly, you can check that the left distributive law holds. Thus, $(Z + iZ, +, .)$ is a ring.

The next example is related to Example 8 of Unit 2. The operations that we consider in it are not the usual addition and multiplication.

Example 4 : Let X be a non-empty set, $\wp(X)$ be the collection of all subsets of X and $\Delta$ 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 8 of Unit 2 we showed that $(\wp(X), \Delta)$ is an abelian group. You also know that $\cap$ is associative. Now let us see if $\cap$ distributes over $\Delta$.

Let $A, B, C \in \wp(X)$. Then

$A \cap (B \Delta C) = A \cap [(B \setminus C) \cup (C \setminus B)]$
$= [A \cap (B \setminus C)] \cup [A \cap (C \setminus B)]$, since $\cap$ distributes over $\cup$.
$= [(A \cap B) \setminus (A \cap C)] \cup [(A \cap C) \setminus (A \cap B)]$, since $\cap$ distributes over complementation.
$= (A \cap B) \Delta (A \cap C)$.

So, the left distributive law holds.

Also, $(B \Delta C) \cap A = A \cap (B \Delta C)$, since $\cap$ is commutative.
$= (A \cap B) \Delta (A \cap C)$
$= (B \cap A) \Delta (C \cap A)$.

Therefore, the right distributive law holds also.

Therefore, $(\wp(X), \Delta, \cap)$ is a ring.

So far you have seen examples of rings in which both the operations defined on the ring have been commutative. This is not so in the next example.

**Example** 5 : Consider the set

$$\mathbf{M_2(R)} = \left\{ \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \middle| \ a_{11}, a_{12}, a_{21} \text{ and } a_{22} \text{ are real numbers} \right\}$$

Show that $\mathbf{M_2(R)}$ is a ring with respect to addition and multiplication of matrices.

**Solution** : Just as we have solved Example 2 of Unit **3, you** can check that $(\mathbf{M_2(R)}, +)$ is an abelian group. You can also verify the associative property for multiplication. (Also see Example 5 of Unit 2.) We now show that $A.(B + C) = A.B + A.C$ for A, B, C in $\mathbf{M_2(R)}$.

$$A.(B+C) = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \left( \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix} + \begin{bmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{bmatrix} \right)$$

$$= \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \begin{bmatrix} b_{11}+c_{11} & b_{12}+c_{12} \\ b_{21}+c_{21} & b_{22}+c_{22} \end{bmatrix}$$

$$= \begin{bmatrix} a_{11}(b_{11}+c_{11}) + a_{12}(b_{21}+c_{21}) & a_{11}(b_{12}+c_{12}) + a_{12}(b_{22}+c_{22}) \\ a_{21}(b_{11}+c_{11}) + a_{22}(b_{21}+c_{21}) & a_{21}(b_{12}+c_{12}) + a_{22}(b_{22}+c_{22}) \end{bmatrix}$$

$$= \begin{bmatrix} (a_{11}b_{11}+a_{12}b_{21}) + (a_{11}c_{11}+a_{12}c_{21}) & (a_{11}b_{12}+a_{12}b_{22}) + (a_{11}c_{12}+a_{12}c_{22}) \\ (a_{21}b_{11}+a_{22}b_{21}) + (a_{21}c_{11}+a_{22}c_{21}) & (a_{21}b_{12}+a_{22}b_{22}) + (a_{21}c_{12}+a_{22}c_{22}) \end{bmatrix}$$

$$= \begin{bmatrix} a_{11}b_{11}+a_{12}b_{21} & a_{11}b_{12}+a_{12}b_{22} \\ a_{21}b_{11}+a_{22}b_{21} & a_{21}b_{12}+a_{22}b_{22} \end{bmatrix} + \begin{bmatrix} a_{11}c_{11}+a_{12}c_{21} & a_{11}c_{12}+a_{12}c_{22} \\ a_{21}c_{11}+a_{22}c_{21} & a_{21}c_{12}+a_{12}c_{22} \end{bmatrix}$$

$$= \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} . \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix} + \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} . \begin{bmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{bmatrix}$$

$$= A.B + A.C.$$

In the same way we can obtain the other distributive law, i.e., $(A + B).C = A.C + B.C \ \forall \ A, B, C \in \mathbf{M_2(R)}$.

Thus, $\mathbf{M_2(R)}$ is a ring under matrix addition and multiplication.

Note that multiplication over $M_2(R)$ is not commutative. So, we can't say that the left distributive law implies the right distributive law in this case.

Try the following exercises now.

---

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

E 3) Let $R = \left\{ \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \middle| \ a, b \text{ are real numbers} \right\}$. Show that R is a ring under matrix addition and multiplication.

E 4) 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.

E 5) Why is $(\wp(X), \cup, \cap)$ not a ring?

---

Let us now look at rings whose elements are fynctions.

**Example 6** : Consider the class of all continuous real valued functions defined on the closed interval [0, 1]. We denote this by C[0, 1]. If f and g are two continuous functions on [0, 1], we define f + g and fg as

$(f + g)(x) = f(x) + g(x)$ (i.e., pointwise addition)

and $(f.g)(x) = f(x).g(x)$ (i.e., pointwise multiplication)

for every $x \in [0, 1]$. From the Calculus course you know that the function f + g and fg are defined and continuous on [0, 1], i.e., if f and $g \in C[0, 1]$, then both f + g and f.g are in C[0, 1]. Show that C[0, 1] is a ring with respect to + and

**Solution** : Since addition in R is associative and commutative, so is addition in C[0, 1]. The additive identity of C[0, 1] is the zero function. The additive inverse of $f \in C[0, 1]$ is $(-f)$, where $(-f)(x) = -f(x) \; \forall \; x \in [0, 1]$. See Fig. 2 for a visual interpretation of $(-f)$. Thus, (C[0, 1], +) is an abelian group. Again, since multiplication in R is associative, so is multiplication in C[0, 1].

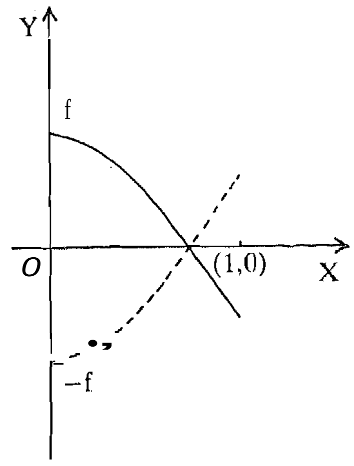


Fig 2 : The graphs of f and (− f) over [0, 1].

Now let us see if the axiom R6 holds.

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

Now $(f.(g + h))(x) = f(x)(g + h)(x)$
$= f(x)(g(x) + h(x))$
$= f(x)g(x) + f(x)h(x)$, since . distributes over + in R.
$= (f.g)(x) + (f.h)(x)$
$= (f.g + f.h)(x)$

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

Since multiplication is commutative in C[0, 1], the other distributive law also holds. Thus, R6 is true for C[0, 1]. Therefore, (C[0, 1], +, .) is a ring.

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

The next example also deals with functions.

**Example 7** : Let (A, +) be an abelian group. The set of all endomorphisms of A is

An endomorphism of a group G is a homomorphism from G into G.

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

For $f, g \in$ End A, we define $f + g$ and $f.g$ as

$(f + g)(a) = f(a) + g(a)$, and ..... (1)

$(f.g)(a) = f \circ g(a) = f(g(a)) \; \forall \; a \in A$

Show that (End A, +, .) is a ring. (This ring is called the **endomorphism ring** of A.)

**Solution** : Let us first check that + and . defined by (1) are binary operations on End A.

For all $a, b \in A$,

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

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

Thus, $f + g$ and $f.g \in$ End A.

Now let us see if (End A, +, .) satisfies R1–R6.

Since + in the abelian group **A** is associative and commutative, so is + in End **A.** The zero homomorphism on A is the zero element in End **A.** $(-f)$ is the additive inverse of $f \in$ End A. Thus, (End A, +) is an abelian group.

You also know that the composition of functions is an associative operation in End A.

Finally, to check R6 we look at $f.(g + h)$ for any $f, g, h \in$ End A. Now for any $a \in A$,

$[f.(g + h)](a) = f((g + h)(a))$
$= f(g(a) + h(a))$
$= f(g(a)) + f(h(a))$
$= (f.g)(a) + (f.h)(a)$
$= (f.g + f.h)(a)$

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

We can similarly prove that $(f + g).h = f.h + g.h$.

Thus, R1-R6 are true for End **A.**

Hence, (End A, +, .) is a ring.

Note that . is not commutative since $f \circ g$ need not be equal to $g \circ f$ for $f, g \in$ End A.

You may like to try these exercises pow.

E 6) Let X be a non-empty set and (R, +, .) be any ring. Define the set Map(X, R) to be the set of all functions from X to R. That is,
Map (X, R) = { f | f : X → R }.
Define + and . in Map (X, R) by pointwise addition and multiplication. Show that (Map (X, R), +, .) is a ring.

E 7) Show that the set R of real numbers is a ring under addition and multiplication given by $a \oplus b = a + b + 1$, and $a \odot b = a.b + a + b$
for all a, b ∈ R, where + and . denote the usual addition and multiplication of real numbers.

On solving E 7 you must have realised that a given set can be an underlying set of many different rings.

Now, let us look at the Cartesian product of rings.

**Example 8** : Let (A, +, .) and (B, ⊞, ⊡) be two rings. Show that their Cartesian product A X B is a ring with respect to ⊕ and * defined by
(a, b) ⊕ (a', b') = (a + a', b ⊞ b'), and
(a, b) * (a', b') = (a . a', b ⊡ b')

for all (a, b), (a', b') in A X B.

**Solution** : We have defmed the addition and multiplication in A X B componentwise. The zero element of A X B is (0, 0). The additive inverse of (a, b) is (− a, ⊟ b), where ⊟ b denotes the inverse of b with respect to ⊞.

Since the multiplications in A and B are associative, * is associative in A X B. Again, using the fact that R6 holds for A and B, we can show that R6 holds for A X B. Thus, (A X B, ⊕, *) is a ring.

If you have understood this example, you will be able to do the next exercise.

E 8) Write down the addition and multiplication tables for $Z_2 \times Z_3$.

Before going further we would like to make a remark about notational conventions. In the case of groups, we decided to use the notation G for $(G, *)$ for convenience. Here too, in future, we shall use the notation R for (R, +, .) for convenience. Thus, we shall assume that + and . are known. We shall also denote the product of two ring elements a and b by ab instead of a . b.

So now let us begin studying various properties of rings.

## 9.3 ELEMENTARY PROPERTIES

In this section we will prove some simple but important properties of rings which 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 results obtained for groups in the earlier units are applicable to the abelian group (R, +). In particular,

i) the zero element, 0, and the additive inverse of any element is unique.

ii) the cancellation law holds for addition;
i.e., ∀ a, b, c ∈ R, a + c = b + c ⟹ a = b.

As we have mentioned earlier, we will write a − b for a + (− b) and ab for a . b, where a, b ∈ R.

So let us state some properties which follow from the axiom R6, mainly,

**Theorem 1** : Let R be a ring. Then, for any a, b, c ∈ R,

i) a0 = 0 = 0a,

ii) a(− b) = (− a)b = − (ab),

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

iv) $a(b - c) = ab - ac$, and

v) $(b - c)a = ba - ca$.

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

$\Rightarrow a(0 + 0) = a0$

$\Rightarrow a0 + a0 = a0$, applying the distributive law.

$= a0 + 0$, since 0 is the additive identity.

$\Rightarrow a0 = 0$, by the cancellation law for $(R, +)$.

Using the other distributive law, we can similarly show that $0a = 0$.
Thus, $a0 = 0 = 0a$ for all $a \in R$.

ii) From the definition of additive inverse, we know that $b + (-b) = 0$.
Now, $0 = a0$, 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 you know that the additive inverse of an element is unique.

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

In the same manner, using the fact that $a + (-a) = 0$, we get $-(ab) = (-a)b$.
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.
$= a(-(-b))$, from (ii) above.
$= ab$, since b is the additive inverse of $(-b)$.

iv) For $a, b, c \in R$,
$a(b - c) = a(b + (-c))$
$= ab + a(-c)$, by distributivity.
$= ab + (-(ac))$, from (ii) above.
$= ab - ac$.

We can similarly prove (v).

Try this exercise now.

---

**E 9)** Show that { 0 } is a ring with respect to the usual addition and multiplication. (This is called the **trivial ring.)**

Also show that if any singleton is a ring, the singleton must be { 0 }.

E 10) 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.

---

Now let us 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).**

If k is an integer ($k \geq 2$) such that the sum of k elements in a ring R is defined, we define the sum of $(k + 1)$ elements $a_1, a_2, ..., a_{k+1}$ in R, taken in that order, as
$a_1 + ... + a_{k+1} = (a_1 + ..... + a_k) + a_{k+1}$.

In the same way if k is a positive integer such that the product of k elements in R is defined, we define the product of $(k + 1)$ elements $a_1, a_2, ..., a_{k+1}$ (taken in that order) as
$a_1.a_2. .... .a_{k+1} = (a_1.a_2. ... .a_k).a_{k+1}$.

As we did for groups, we can obtain laws of indices in the case of rings also with respect to both + and . . In fact, we have the following results for any ring R.

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

(ii) If m and n are arbitrary integers and $a, b \in R$, then
$(n + m)a = na + ma$,

$(nm)a = n(ma) = m(na)$,
$n(a + b) = na + nb$,
$m(ab) = (ma)b = a(mb)$, and
$(ma)(nb) = mn(ab) = (mna)b$.

(iii) If $a_1, a_2, \ldots, a_m, b_1, \ldots, b_n \in R$ then
$(a_1 + \ldots + a_m)(b_1 + \ldots + b_n)$
$= a_1b_1 + \ldots + a_1b_n + a_2b_1 + \ldots + a_2b_n + \ldots + a_mb_1 + \ldots + a_mb_n$.

Try this simple exercise now.

---

E 11) If R is a ring and a, b ∈ R such that ab = ba, then use induction on n ∈ N to derive the binomial expansion.
$(a + b)^n = a^n + {}^nC_1a^{n-1}b + \ldots + {}^nC_ka^{n-k}b^k + \ldots + {}^nC_{n-1}ab^{n-1} + b^n$,
where ${}^nC_k = \frac{n!}{k!\,(n-k)!}$.

---

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

## 9.4 TWO TYPES OF WINGS

The definition of a ring guarantees that the binary operation multiplication is associative and, along with +, satisfies 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. Let us introduce you to two of them now.

Definition : We say that a ring (R, +, .) is commutative if . is commutative, i.e., if ab = ba for all a, b ∈ R.

For example, Z, **Q** and R are commutative rings.

Definition : We say that a ring (R, +, .) is a **ring** with identity (or 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 ∈ R.

Can you think of such a ring? Aren't Z, **Q** and R examples of a ring with identity'?

Try this quickie before we go to our next definition.

---

E 12) Prove that if a ring R has an identity element with respect to multiplication, then it is unique. (We denote this unique identity element in a ring with identity by the symbol 1.)

---

Now let us combine the previous two definitions.

Definition : We say that a ring (R, +, .) is a commutative ring with unity, if it is a commutative ring and has the multiplicative identity element 1.

Thus, the rings Z, **Q,** R and C are all commutative rings with unity. The integer 1 is the multiplicative identity in all these rings.

We can also find commutative rings which are not rings with identity. For example, 2**Z**, the ring of all even integers is commutative. But it has no multiplicative identity.

Similarly, we can find rings with identity which are not commutative. For example, $\mathbf{M}_2(\mathbf{R})$ has the unit element $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$.

But it is not commutative. For instance,

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

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

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

Thus. $AB \neq BA$.

Try this exercise now.

---

E 13) Which of the rings in Example 1, 2, 3, 4, 6, 7 are commutative and which have unity? Give the identity, whenever it exists.

---

Now, can the trivial ring be a ring with identity? Since $0 . 0 = 0$, 0 is also the multiplicative identity for this ring. So $(\{0\}, +, .)$ 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 $R \neq \{0\}$, $\exists\, a \in R$, $a \neq 0$. Now suppose $0 = 1$. Then $a = a . 1 = a . 0 = 0$ (by Theorem 1). That is, $a = 0$, a contradiction. Thus, our supposition is wrong. That is, $0 \neq 1$.

Now let us go back to Example 8. When will $A \times B$ be commutative? $A \times B$ is commutative if and only if both the rings A and B are commutative. Let us see why. For convenience we will denote the operations in all three rings A, B and $A \times B$ by + and . . Let (a, b) and $(a', b') \in A \times B$.

Then $(a, b) . (a', b') = (a', b'). (a, b)$

$\Longleftrightarrow (a.a', b.b') = (a'. a, b'. b)$

$\Longleftrightarrow a.a' = a'.a$ and $b.b' = b'.b$.

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

We can similarly show that $A \times B$ is with unity iff A and B are with unity. If A and B have identities $e_1$ and $e_2$ respectively, then the identity of $A \times B$ is $(e_1, e_2)$.

Now for some exercises about commutative rings with identity.

---

E 14) Show that the ring in E 7 is a commutative ring with identity.

E 15) Show that the set of matrices $\left\{ \begin{bmatrix} x & x \\ x & x \end{bmatrix} \middle|\, x \in \mathbf{R} \right\}$ is a commutative ring with unity.

E 16) Let R be a 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.

---

Now we will give 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). It plays an important role in geometry, number theory and the study of mechanics.

Example 9 : Let $H = \{a + bi + cj + dk \mid a, b, c, d \in \mathbf{R}\}$, where i, j, k are symbols that satisfy $i^2 = -1 = j^2 = k^2$, $ij = k = -ji$, $jk = i = -kj$, $ki = j = -ik$.

We define addition and multiplication in **H** by

$(a + bi + cj + dk) + (a_1 + b_1i + c_1j + d_1k)$

$= (a + a_1) + (b + b_1)i + (c + c_1)j + (d + d_1)k$, and

$(a + bi + cj + dk)(a_1 + b_1i + c_1j + d_1k) = (aa_1 - bb_1 - cc_1 - dd_1)$

$+ (ab_1 + ba_1 + cd_1 - dc_1)i + (ac_1 - bd_1 + ca_1 + db_1)j + (ad_1 + bc_1 - cb_1 + da_1)k$

(This multiplication may seem complicated. But it is not so. It is simply performed as for polynomials, keeping the relationships between i, j and k in mind.)

Show that H is a ring.

**Solution** : Note that $\{\pm 1, \pm i, \pm j, \pm k\}$ is the group $Q_8$ (Example 4, Unit 4).

Now, you can verify that (H, +) is an abelian group in which the additive identity is $0 = 0 + 0i + 0j + 0k$, multiplication in H is associative, the distributive laws hold and $1 = 1 + 0i + 0j + 0k$ is the unity in H.

Do you agree that H is not a commutative ring? You will if you remember that $ij \neq ji$, for example.

So far, in this unit we have discussed various types of rings. We have seen examples of commutative and non-commutative rings. Though non-commutative rings are very importa for the sake of simplicity we shall only deal with commutative rings henceforth. Thus, from now on, for us **a ring will always mean a commutative ring.** We would like you to remember that both + and . are commutative in a commutative ring.

Now, let us summarise what we have done in this unit.

## 9.5 SUMMARY

In this unit we discussed the following points.

1) Definition and examples of a ring.

2) Some properties of a ring like
$a . 0 = 0 = 0 . a$,
$a(-b) = -(ab) = (-a)b$,
$(-a)(-b) = ab$,
$a(b - c) = ab - ac$,
$(b - c)a = ba - ca$
$\forall$ a, b, c in a ring R.

3) The laws of indices for addition and multiplication, and the generalised distributive law.

4) Commutative rings, rings with unity and commutative rings with unity.

Henceforth, we will always assume that a ring means a commutative ring, unless otherwise mentioned.

## 9.6 SOLUTIONS/ANSWERS

E 1) **Addition in $Z_6^*$**

| + | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ | $\bar{4}$ | $\bar{5}$ |
|---|---|---|---|---|---|
| $\bar{1}$ | $\bar{2}$ | $\bar{3}$ | $\bar{4}$ | $\bar{5}$ | $\bar{0}$ |
| $\bar{2}$ | $\bar{3}$ | $\bar{4}$ | $\bar{5}$ | $\bar{0}$ | $\bar{1}$ |
| $\bar{3}$ | $\bar{4}$ | $\bar{5}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ |
| $\bar{4}$ | $\bar{5}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ |
| $\bar{5}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ | $\bar{4}$ |

**Multiplication in $Z_6^*$**

| . | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ | $\bar{4}$ | $\bar{5}$ |
|---|---|---|---|---|---|
| $\bar{1}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ | $\bar{4}$ | $\bar{5}$ |
| $\bar{2}$ | $\bar{2}$ | $\bar{4}$ | $\bar{0}$ | $\bar{2}$ | $\bar{4}$ |
| $\bar{3}$ | $\bar{3}$ | $\bar{0}$ | $\bar{3}$ | $\bar{0}$ | $\bar{3}$ |
| $\bar{4}$ | $\bar{4}$ | $\bar{2}$ | $\bar{0}$ | $\bar{4}$ | $\bar{2}$ |
| $\bar{5}$ | $\bar{5}$ | $\bar{4}$ | $\bar{3}$ | $\bar{2}$ | $\bar{1}$ |

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

E 2) We define addition and multiplication in $Q + \sqrt{2}\mathbf{Q}$ by
$(a + \sqrt{2}b) + (c + \sqrt{2}d) = (a + c) + \sqrt{2}(b + d)$, and
$(a + \sqrt{2}b) . (c + \sqrt{2}d) = (ac + 2bd) + \sqrt{2}(ad + bc) \; \forall$ a, b, c, d $\in \mathbf{Q}$.
Since + is associative and commutative in R, the same holds for + in $\mathbf{Q} + \sqrt{2}\mathbf{Q}$. $0 = 0 + \sqrt{2} . 0$ is the additive identity and $(-a) + \sqrt{2}(-b)$ is the additive inverse of $a + \sqrt{2}b$.
Since multiplication in R is associative, R5 holds also. Since multiplication distributes over addition in R, it does so in $Q + \sqrt{2}\mathbf{Q}$ as well. Thus, $(Q + \sqrt{2}\mathbf{Q}, +, .)$ is a ring.

E 3) + and . are well defined binary operations on R. R1, R2, R5 and R6 hold since the same properties are true for $\mathbf{M}_2(\mathbf{R})$ (Example 5).

The zero element is $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$. The additive inverse of $\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$ is $\begin{bmatrix} -a & 0 \\ 0 & -b \end{bmatrix}$

Thus, R is a ring.

E 4) + and . are binary operations on R. You can check that (R, +, .) satisfies R1-R6.

E 5) U and $\cap$ are well defined binary operations on $\wp$ (X). Let us check which of the axioms R1-R6 is not satisfied by ($\wp$ (X), U, $\cap$). Since U is abelian, R1 is satisfied.
Since $\cup$ is associative, R2 is satisfied.
Also, for any $A \subseteq X$, $A \cup \phi = A$. Thus, $\phi$ is the identity with respect to U.
Thus, R3 is satisfied.
Now, for any $A \subseteq X$, $A \neq \phi$, there is no $B \subseteq X$ such that $A \cup B = \phi$.
Thus, R4 is not satisfied. Hence, ($\wp$ (X), U, $\cap$) is not a ring.

E 6) Since R satisfies R1, R2, R5 and R6, so does Map (X, R). The zero element is $0 : X \to R : 0(x) = 0$. The additive inverse of $f : X \to R$ is $(-f) : X \to R$.
Thus, (Map (X, R), +, .) is a ring.

E 7) Firstly, $\oplus$ and $\odot$ are well defined binary operations on .

R. Next, let us check if (R, $\oplus$, $\odot$) satisfies R1-R6 $\forall$ a, b, c $\in$ 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 : $a \oplus (-1) = a - 1 + 1 = a \; \forall \; a \in R$. 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** : $a \odot (b \oplus c) = a \odot (b + c + 1) = a(b + c + 1) + a + (b + c + 1)$

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

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

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

E 8) $\mathbf{Z}_2 = \{ \bar{0}, \bar{1} \}$, $\mathbf{Z}_3 = \{ \bar{0}, \bar{1}, \bar{2} \}$

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

Thus, the tables are

| + | $(\bar{0}, \bar{0})$ | $(\bar{0}, \bar{1})$ | $(\bar{0}, \bar{2})$ | $(\bar{1}, \bar{0})$ | $(\bar{1}, \bar{1})$ | $(\bar{1}, \bar{2})$ |
|---|---|---|---|---|---|---|
| $(\bar{0}, \bar{0})$ | $(\bar{0}, \bar{0})$ | $(\bar{0}, \bar{1})$ | $(\bar{0}, \bar{2})$ | $(\bar{1}, \bar{0})$ | $(\bar{1}, \bar{1})$ | $(\bar{1}, \bar{2})$ |
| $(\bar{0}, \bar{1})$ | $(\bar{0}, \bar{1})$ | $(\bar{0}, \bar{2})$ | $(\bar{0}, \bar{0})$ | $(\bar{1}, \bar{1})$ | $(\bar{1}, \bar{2})$ | $(\bar{1}, \bar{0})$ |
| $(\bar{0}, \bar{2})$ | $(\bar{0}, \bar{2})$ | $(\bar{0}, \bar{0})$ | $(\bar{0}, \bar{1})$ | $(\bar{1}, \bar{2})$ | $(\bar{1}, \bar{0})$ | $(\bar{1}, \bar{1})$ |
| $(\bar{1}, \bar{0})$ | $(\bar{1}, \bar{0})$ | $(\bar{1}, \bar{1})$ | $(\bar{1}, \bar{2})$ | $(\bar{0}, \bar{0})$ | $(\bar{0}, \bar{1})$ | $(\bar{0}, \bar{2})$ |
| $(\bar{1}, \bar{1})$ | $(\bar{1}, \bar{1})$ | [illegible] | $(\bar{1}, \bar{0})$ | $(\bar{0}, \bar{1})$ | $(\bar{0}, \bar{2})$ | $(0, 0)$ |
| $(\bar{1}, \bar{2})$ | $(\bar{1}, \bar{2})$ | $(\bar{1}, \bar{0})$ | $(\bar{1}, \bar{1})$ | $(\bar{0}, \bar{2})$ | $(\bar{0}, \bar{0})$ | $(\bar{0}, \bar{1})$ |

| $\cdot$ | $(\bar{0}, \bar{0})$ | $(\bar{0}, \bar{1})$ | $(\bar{0}, \bar{2})$ | $(\bar{1}, \bar{0})$ | $(\bar{1}, \bar{1})$ | $(\bar{1}, \bar{2})$ |
|---|---|---|---|---|---|---|
| $(\bar{0}, \bar{0})$ | $(\bar{0}, \bar{0})$ | $(\bar{0}, \bar{0})$ | $(\bar{0}, \bar{0})$ | $(\bar{0}, \bar{0})$ | $(\bar{0}, \bar{0})$ | $(\bar{0}, \bar{0})$ |
| $(\bar{0}, \bar{1})$ | $(\bar{0}, \bar{0})$ | $(\bar{0}, \bar{1})$ | $(\bar{0}, \bar{2})$ | $(\bar{0}, \bar{0})$ | $(\bar{0}, \bar{1})$ | $(\bar{0}, \bar{2})$ |
| $(\bar{0}, \bar{2})$ | $(\bar{0}, \bar{0})$ | $(\bar{0}, \bar{2})$ | $(\bar{0}, \bar{1})$ | $(\bar{0}, \bar{0})$ | $(\bar{0}, \bar{2})$ | $(\bar{0}, \bar{1})$ |
| $(\bar{1}, \bar{0})$ | $(\bar{0}, \bar{0})$ | $(\bar{0}, \bar{0})$ | $(\bar{0}, \bar{0})$ | $(\bar{1}, \bar{0})$ | $(\bar{1}, \bar{0})$ | $(\bar{1}, \bar{0})$ |
| $(\bar{1}, \bar{1})$ | $(\bar{0}, \bar{0})$ | $(\bar{0}, \bar{1})$ | $(\bar{0}, \bar{2})$ | $(\bar{1}, \bar{0})$ | $(\bar{1}, \bar{1})$ | $(\bar{1}, \bar{2})$ |
| $(\bar{1}, \bar{2})$ | $(\bar{0}, \bar{0})$ | $(\bar{0}, \bar{2})$ | $(\bar{0}, \bar{1})$ | $(\bar{1}, \bar{0})$ | $(\bar{1}, \bar{2})$ | $(\bar{1}, \bar{1})$ |

E 9) Note that + and . are binary operations on {0}. The properties R1-R6 are trivially satisfied.

Now, suppose a singleton {a} is a ring. Then this must contain the additive identity 0. Thus, {a} = {0}.

E 10) We know that $a + 0 = a \ \forall \ a \in R$. Since $a + 0 = a . 0$, we find that $a . 0 = a \ \forall \ a \in R$. But, by Theorem 1 we know that $a . 0 = 0$. Thus, $a = 0 \ \forall \ a \in R$. That is, R = {0}.

E 11) Since $(a + b)^1 = a^1 + b^1$, the statement is true for n = 1. Assume that the equality is true for n = m, i.e.,

$$(a + b)^m = a^m + {}^mC_1 a^{m-1}b + \ldots + {}^mC_{m-1} ab^{m-1} + b^m.$$

Now, $(a + b)^{m+1} = (a + b)(a + b)^m = (a + b)\left(\sum_0^m {}^mC_k a^{m-k} b^k\right)$

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

$= (a^{m+1} + {}^mC_1 a^{m+1-1} b + {}^mC_2 a^{m+1-2} b^2 + \ldots + {}^mC_m ab^m)$

$+ ({}^mC_0 a^m b + {}^mC_1 a^{m-1} b^2 + \ldots + {}^mC_{m-1} ab^m + b^{m+1})$

$= a^{m+1} + ({}^mC_1 + {}^mC_0) a^{m+1-1} b + \ldots + ({}^mC_k + {}^mC_{k-1}) a^{m+1-k} b^k + \ldots + b^{m+1}$

$= a^{m+1} + {}^{m+1}C_1 a^{m+1-1} b + \ldots + {}^{m+1}C_k a^{m+1-k} b^k + \ldots + {}^{m+1}C_m ab^m + b^{m+1}$

(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.

E 12) Let e and e′ be two multiplicative identity elements of R. Then
$e = e . e'$, since e′ is a multiplicative identity.
$= e'$, since e is a multiplicative identity.
Thus, e = e′, i.e., the multiplicative identity of R is unique.

E 13) For n = 1, n**Z** = **Z** is a commutative ring with identity 1.
$\forall \ n > 1$, n**Z** is commutative, but without identity.
$\mathbf{Z}_n$ is commutative with identity $\bar{1}$.
**Z** + i**Z** is commutative with identity 1 + i0.
$\wp$ (X) is commutative with identity X, since $A \cap X = A \ \forall \ A \subseteq X$.
C[0, 1] is commutative with identity $1 : [0, 1] \to \mathbf{R} : 1(x) = 1$.
End A is not commutative. It has identity $I_A : A \to A : I_A(x) = x$.

E 14) Since $a \odot b = b \odot a \ \forall \ a, b \in \mathbf{R}$, $\odot$ is commutative. Also, $a \odot 0 = a \ \forall \ a \in \mathbf{R}$. Thus, 0 is the multiplicative identity.

E 15) You must first check that the set 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 $\begin{bmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{bmatrix}$.

E 16) For any $a \in R$, $a^2 = a$.
In particular, $(2a)^2 = 2a \implies 4a^2 = 2a \implies 4a = 2a \implies 2a = 0$
$\implies a = -a$.

Now, for any $a, b \in R$, $a + b \in R$.
$\therefore (a + b)^2 = a + b \implies a^2 + ab + ba + b^2 = a + b$
$\implies a + ab + ba + b = a + b$, since $a^2 = a$ an $b^2 = b$
$\implies ab = -ba$
$\implies ab = ba$, since $-ba = ba$.
Thus, R is commutative.