

< **14 May** 9:45 AM

E content for students of patliputra university

B. Sc. (Honrs) Part 3 Paper 6

Subject Mathematics

Title/Heading of topic : Ring, Division ring

By Dr. Hari kant singh

Associate professor in mathematics

Definition and Examples of Rings

DEFINITION 14.1. A **ring** is a nonempty set R equipped with two operations \oplus and \otimes (more typically denoted as addition and multiplication) that satisfy the following conditions. For all $a, b, c \in R$:

- (1) If $a \in R$ and $b \in R$, then $a \oplus b \in R$.
- (2) $a \oplus (b \oplus c) = (a \oplus b) \oplus c$
- (3) $a \oplus b = b \oplus a$
- (4) There is an element 0_R in R such that

$$a \oplus 0_R = a \quad , \quad \forall a \in R \quad .$$

- (5) For each $a \in R$, the equation

$$a \oplus x = 0_R$$

has a solution in R .

- (6) If $a \in R$, and $b \in R$, then $ab \in R$.
- (7) $a \otimes (b \otimes c) = (a \otimes b) \otimes c$.
- (8) $a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c)$

DEFINITION 14.2. A **commutative ring** is a ring R such that

$$(14.1) \quad a \otimes b = b \otimes a \quad , \quad \forall a, b \in R \quad .$$

DEFINITION 14.3. A **ring with identity** is a ring R that contains an element 1_R such that

$$(14.2) \quad a \otimes 1_R = 1_R \otimes a = a \quad , \quad \forall a \in R \quad .$$

Let us continue with our discussion of examples of rings.

Example 1. \mathbb{Z} , \mathbb{Q} , \mathbb{R} , and \mathbb{C} are all commutative rings with identity.

Example 2. Let I denote an interval on the real line and let R denote the set of continuous functions $f : I \rightarrow \mathbb{R}$. R can be given the structure of a commutative ring with identity by setting

$$\begin{aligned} [f \oplus g](x) &= f(x) + g(x) \\ [f \otimes g](x) &= f(x)g(x) \\ 0_R &\equiv \text{function with constant value } 0 \\ 1_R &\equiv \text{function with constant value } 1 \end{aligned}$$

and then verifying that properties (1)-(10) hold.

Example 3.

Let R denote the set of continuous functions $f : \mathbb{R} \rightarrow \mathbb{R}$ such that

$$\int_0^{\infty} f(x) dx < \infty.$$

We can define $f \oplus g$, fg , 0_R just as in the previous example; however, we cannot define a multiplicative identity element in this case. This is because

$$\int_0^{\infty} 1dx = \lim_{x \rightarrow \infty} (x - 0) = \infty$$

so the function 1_R of the previous example does not belong to this set. Thus, the set of continuous functions that are integrable on $[0, \infty)$ form a commutative ring (without identity).

Example 4. Let \mathbb{E} denote the set of even integers. \mathbb{E} is a commutative ring, however, it lacks a multiplicative identity element.

Example 5. The set O of odd integers is not a ring because it is not closed under addition.

Subrings

As the preceding example shows, a subset of a ring need not be a ring

DEFINITION 14.4. Let S be a subset of the set of elements of a ring R . If under the notions of additions and multiplication inherited from the ring R , S is a ring (i.e. S satisfies conditions 1-8 in the definition of a ring), then we say S is a **subring** of R .

THEOREM 14.5. Let S be a subset of a ring R . Then S is a subring if

- (i) S is closed under addition.
- (ii) S is closed under multiplication.
- (iii) If $s \in S$, then $-s \in R$, the additive inverse of s as an element of R , is also in S .

Proof.

Since axioms 2, 3, 7, 8 hold for all elements of the original ring R they will also hold for any subset $S \subseteq R$. Therefore, to verify that a given subset S is a subring of a ring R , one must show that

- (1) S is closed under addition
 - This is implied by condition (i) on S
- (4) S is closed under multiplication;
 - This is implied by (ii) on S .
- (5) $0_R \in S$ and (6) When $a \in S$, the equation $a + x = 0_R$ has a solution in S .
 - If (iii) is true, then the additive inverse $-s \in R$ also belongs to S if $s \in S$. But then $s + (-s) = 0_R \in S$, because by (i) S is closed under addition. But then $0_R + s = s$ for every $s \in S$, and so 0_R is the additive identity for S (i.e. $0_S = 0_R$). So if (i) and (iii) are true, then S has an additive identity and for S then for every $s \in S$ we have a solution of $s + x = 0_S$ is S .

Example 6. Let $M_2(\mathbb{Z})$, $M_2(\mathbb{Q})$, $M_2(\mathbb{R})$ and $M_2(\mathbb{C})$ denote the sets of 2×2 matrices with entries, respectively, in the integers \mathbb{Z} , the rational numbers \mathbb{Q} , the real numbers \mathbb{R} , and the complex numbers \mathbb{C} . Addition and multiplication can be defined by

$$\begin{aligned} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \oplus \begin{pmatrix} e & f \\ g & h \end{pmatrix} &= \begin{pmatrix} a+b & b+f \\ c+g & d+h \end{pmatrix} \\ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \otimes \begin{pmatrix} e & f \\ g & h \end{pmatrix} &= \begin{pmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{pmatrix} \end{aligned}$$

with a, b, c, d, e, f, g, h in, respectively \mathbb{Z} , \mathbb{Q} , \mathbb{R} , and \mathbb{C} . The matrices

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

are then, respectively, additive identity elements and multiplicative identity elements of R . Note however that

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 1 & 0 \end{pmatrix} \neq \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

so multiplication in R is not commutative in general. Thus, each of these sets is a non-commutative ring with identity.

We have seen that some rings like \mathbb{Z} or \mathbb{Z}_p with p prime have the property that

$$a \otimes b = 0_R \quad \Rightarrow \quad a = 0_R \text{ or } b = 0_R \quad ;$$

but that this is not a property we can expect in general. This property is important enough to merit a special title.

DEFINITION 14.6. An **integral domain** is a commutative ring R with identity $1_R \neq 0_R$ such that

$$(14.3) \quad a \otimes b = 0_R \quad \Rightarrow \quad a = 0_R \text{ or } b = 0_R \quad .$$

Recall that the ring \mathbb{Z}_p when p is prime has the property that if $a \neq [0]$, then the equation

$$ax = [1]$$

always has a solution in \mathbb{Z}_p . This not true for the ring \mathbb{Z} ; because for example, the solution of

$$2x = 1$$

is $\frac{1}{2} \notin \mathbb{Z}$. However, the ring \mathbb{Q} of rational numbers does have this property.

DEFINITION 14.7. A **division ring** is a ring R with identity $1_R \neq 0_R$ such that for each $a \neq 0_R$ in R the equations $a \otimes x = 1_R$ and $x \otimes a = 1_R$ have solutions in R .

Note that we do not require a division ring to be commutative.

DEFINITION 14.8. A **field** is a division ring with commutative multiplication.

For the most part we will be concentrating on fields rather than non-commutative division rings.

Example: \mathbb{Q} , \mathbb{R} , \mathbb{Z}_p with p prime.

Example:

In the ring $M_2(\mathbb{C})$, let

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

The set \mathbb{H} of **real quaterions** consists of all matrices of the form

$$a1 + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} = \begin{pmatrix} a + ib & c + di \\ -c + di & a - bi \end{pmatrix}$$

where $a, b, c, d \in \mathbb{R}$. It is easy to verify that \mathbb{H} is closed under the usual addition of matrices. Also

\times	1	i	j	k
1	1	i	j	k
i	i	-1	k	-j
j	j	-k	-1	i
k	k	j	-i	-1

Note that multiplication is not commutative in this ring; e.g., $\mathbf{ij} = \mathbf{k} = -\mathbf{ji}$. It is possible to show nevertheless that \mathbb{H} is not only a ring with identity but a division ring.

Recall that the Cartesian product $A \times B$ of two sets A and B is the set of all ordered pairs (a, b) with $a \in A$ and $b \in B$.

THEOREM 14.9. *Let R and S be rings. Define addition and multiplication on $R \times S$ by*

$$\begin{aligned}(r, s) + (r, s) &= (r + r, s + s) \quad , \\ (r, s)(r, s) &= (rr, ss) \quad .\end{aligned}$$

Then $R \times S$ is a ring. If R and S are both commutative, then so is $R \times S$. If R and S each has an identity, then so does $R \times S$.

Proof. (homework problem)