Definition 1.1.26 A non-trivial ring R with unity is called a division ring (~~skew field~~) (or skew field) if every non-zero element of R is a unit.

Note that in a division ring, the set of all non-zero elements of R forms a group under multiplication.

Definition 1.1.27 A commutative division ring is called a field.

Examples 1.1.28 : 1. The ring $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are division rings which are field.

Note that there are division rings which are not fields. We have the following example:

2. Let $R = \left\{ \begin{bmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{bmatrix} \in M_2(\mathbb{C}) : \bar{\alpha}, \bar{\beta} \text{ denote the conjugate of } \alpha, \beta \right\}$

Define addition + and multiplication . in R by usual matrix addition and matrix multiplication

Let $A = \begin{bmatrix} a+ib & c+id \\ -(c-id) & a-ib \end{bmatrix}$, $B = \begin{bmatrix} r+it & u+iv \\ -(u-iv) & r-it \end{bmatrix} \in R$

Then $A+B$ and $AB \in R$ (check it). Observe that $0 = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \in R$ is the zero element and for any $A \in R$, $-A \in R$ such that $A + (-A) = 0$. Further, the distributive laws hold (check it). Hence R is a ring with unity $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in R$. Now $\begin{bmatrix} i & 1 \\ -1 & -i \end{bmatrix}, \begin{bmatrix} 1 & i \\ i & 1 \end{bmatrix} \in R$

and $\begin{bmatrix} i & 1 \\ -1 & -i \end{bmatrix}\begin{bmatrix} 1 & i \\ i & 1 \end{bmatrix} = \begin{bmatrix} 2i & 0 \\ 0 & -2i \end{bmatrix}$ and $\begin{bmatrix} 1 & i \\ i & 1 \end{bmatrix}\begin{bmatrix} i & 1 \\ -1 & -i \end{bmatrix} = \begin{bmatrix} 0 & 2 \\ -2 & 0 \end{bmatrix}$

So, ~~R is a non-commutative~~ R is a non-trivial non-commutative ring with unity. Let $\begin{bmatrix} a+ib & c+id \\ -(c-id) & a-ib \end{bmatrix}$ be a non-zero element of R. Then either $a+ib \neq 0$ or $c+id \neq 0$, i.e., either

$a^2+b^2 \neq 0$ or $c^2+d^2 \neq 0$ Hence $a^2+b^2+c^2+d^2 \neq 0$. Let $k = a^2+b^2+c^2+d^2$.

Observe that $\frac{1}{k}\begin{bmatrix} a-ib & c-id \\ -(c+id) & a+ib \end{bmatrix} \in R$ is the inverse of

$\begin{bmatrix} a+ib & c+id \\ -(c-id) & a-ib \end{bmatrix} \in R$. Hence each non-zero element of R has an inverse in R. So, R is a division ring. But as R is non-commutative, R is not a field.

Theorem 1.1.29 A division ring contains no divisor of zero.

Proof : Let R be a division ring and let a be a non-zero element of R. Let $a.b = 0$ where $b \in R$. Since each non-zero element in R is a unit, a^{-1} exists in R. and $a.a^{-1} = a^{-1}.a = 1$, 1 being the unity in R. So,

$a.b = 0 \Rightarrow a^{-1}.(a.b) = a^{-1}.0 \Rightarrow (a^{-1}.a).b = 0 \Rightarrow 1.b = 0 \Rightarrow b = 0$

This proves that a is not a left divisor of zero.
By similar arguments it can be shown that a is not right divisor of zero. Consequently, a is not a divisor of zero.
So, R contains no divisor of zero.

Theorem 1.1.30 Any field is an integral domain. Let R be a field and $a, b \in R$ such that $a \neq 0$ and $ab = 0$. In R, a is a unit, hence a^{-1} exists in R. Then $0 = a^{-1}.0 = a^{-1}(ab)$ $= 1.b = b$. Thus we find that R is a non-trivial commutative ring with unity and without divisor of zero. So, R is an integral domain.
Now, the converse is not true, in general. Clearly, the ring $(\mathbb{Z}, +, \cdot)$ is an integral domain which is not a field (2, has no inverse in $\mathbb{Z}$). But we show that any finite integral domain is field.

Theorem 1.1.31 Any finite integral domain is a field.

Proof: Let R be a finite integral domain. Suppose $R = \{a_1, a_2, \ldots, a_n\}$. Let $a \in R$ and $a \neq 0$ and consider the set $S = \{aa_1, aa_2, \ldots, aa_n\}$. Then $S \subseteq R$ since R is closed under multiplication. If $aa_i = aa_j$, for $0 < i < n$, $0 < j < n$ So, $a_i = a_j$ by Theorem 1.1.25 as $a \neq 0$ which implies that elements of S are distinct. Then $S = R$, as $S \subseteq R$ and $o(S) = n = o(R)$. Now since R contains 1, we have $1 = aa_j$ for some j $(1 \leq j \leq n)$, which implies a is a unit and since this happens for every non-zero element a of R, we have, R is a field.

Corollary 1.1.32 For any positive integer n, $\mathbb{Z}_n$ is a field if and only if n is a prime integer.

Proof: If $\mathbb{Z}_n$ is a field, then by Theorem 1.1.30, $\mathbb{Z}_n$ is an integral domain and hence from Theorem 1.1.24, n is a prime integer.

Conversely, suppose n is prime. Then $\mathbb{Z}_n$ is a finite integral domain by Theorem 1.1.24. So, by Theorem 1.1.31, $\mathbb{Z}_n$ is a field.

Definition 1.1.33 Characteristic of a ring: The characteristic of a ring R, denoted by $\text{char}R$, is defined as the least positive integer n (if it exists) such that $na = 0$ for all $a \in R$.

where $na = a + a + \ldots + a$ (n times)

If no such positive integer n exists, R is said to be of characteristic Zero.

Note 1.1.34 $\text{Char}R = 1$ if and only if R is the trivial ring.

Theorem 1.1.35 Let R be a ring with unity 1. If n be the least positive integer for which $n1 = 0$ then $\text{char } R = n$. If there does not exist a positive integer n for which $n1 = 0$ holds, then $\text{char } R = 0$

Proof: Let $a \in R$. Then let n be the least positive integer for which $n1 = 0$. Then $na = a + a + \cdots + a$ (n times)

$$= a(1 + 1 + \cdots + 1) \text{ (n times)}$$
$$= a(n1)$$
$$= a \cdot 0$$
$$= 0$$

Thus $na = 0$ for all $a \in R$ and since $1 \in R$ and for no positive integer $k < n$, $k1 = 0$, n is the least positive integer for which $na = 0$ holds for all $a \in R$.

This proves that $\text{char } R = n$

If for no positive integer n, $n1 = 0$ holds, then there does not exist a positive integer for which $na = 0$ holds for all $a \in R$. So, $\text{char } R = 0$

Examples 1.1.36 :

1. Let $R = (\mathbb{Z}, +, \cdot)$. Then $\text{char } R = 0$
2. Let $R = (\mathbb{Z}_6, +, \cdot)$ Then $\text{char } R = 6$
3. Let $R = (\mathbb{Z}_n, +, \cdot)$ Then $\text{char } R = n$

Theorem 1.1.37 The characteristic of an integral domain is either zero or a prime number.

Proof: Let the characteristic of an integral domain R be a positive integer m. $m \neq 1$ as R is a non-trivial ring. If possible, let m be a composite number. Then $m = pq$ where p, q are