Integral Domain

Definition: Zero Divisor

Let R be a ring and $r, s \in \mathbb{R}^*$ such that $r, s \neq 0$ and $rs = 0$. r is called a *left zero divisor* of s and s is called a *right zero divisor* of r.

Example

1). $\mathbb{Z} \times \mathbb{Z}$

$$(0, a)(b, 0) = (0, 0)$$

2). $\mathbb{Z}_6$

$$2 \cdot 3 = 0$$

3). $M_2(Z)$

$$\begin{bmatrix} 1 & -2 \\ -2 & 4 \end{bmatrix} \begin{bmatrix} 6 & 2 \\ 3 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

Definition: Integral Domain

Let R be a commutative ring with $1 \neq 0$. To say that R is an *integral domain* means that R has no zero divisors.

Theorem

Let R be a commutative ring with $1 \neq 0$. R is an integral domain iff the cancellation laws hold.

Proof

$\implies$ Assume R is an integral domain

Assume $rs = rt$ for $r, s, t \in R$ and $r \neq 0$
$rs - rt = 0$
$r(s - t) = 0$
But $r \neq 0$ by assumption, so $s - t = 0$ and $s = t$

Therefore, the left cancellation law holds.

Similarly, $sr = tr$
$sr - tr = 0$
$(s - t)r = 0$
and thus $s = t$

Therefore the right cancellation law holds.

$\Longleftarrow$ Assume that the cancellation laws hold

Assume $r, s \in R$ such that $r \neq 0$ and $rs = 0$
$r0 = 0$
$rs = r0$
So by left cancellation, $s = 0$

Therefore R contains no left zero divisors.

Similarly, assume $t \in R$ such that $tr = 0$
$0r = 0$
$tr = 0r$
So by right cancellation, $t = 0$

Therefore R contains no right zero divisors.

Therefore R is an integral domain.

Example

1). $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$

2). $\mathbb{Z}[x]$

3). $\mathbb{Z}[x, y]$

4). $\mathbb{Z}[i]$

5). $\mathbb{Z}[\omega]$

Note that $M_n(R)$ is not an integral domain due to lack of multiplicative commutativity.

Definition: Field

Let F be an integral domain. To say that F is a field means:

$$F^\times = F^*$$

In other words, every non-zero element in F is a unit.

Theorem

Let F be a finite integral domain. F is a field.

Proof

By definition, F is a commutative ring with unity $1 \neq 0$

Assume $a \in F, a \neq 0$
Let $L_a : F \to F$ be defined by $L_a(x) = ax$

Assume $L_a(x) = L_a(y)$
$ax = ay$
But F is an integral domain, so the cancellation laws hold
$x = y$
$\therefore L_a$ is one-to-one.

But F is finite, so L_a is also onto
$\therefore L_a$ is a bijection on F.

$1 \in F$
$\exists\, x \in F, L_a(x) = 1$
$ax = 1$
But F is commutative so $xa = 1$
So x is a multiplicative inverse for a
Thus every non-zero element of F has a multiplicative inverse

$\therefore F$ is a field.