Outline of Presentation

- INTEGRAL DOMAIN & FIELD
- EXAMPLES
- SUBRINGS
- IDEALS
- PRIME IDEAL & MAXIMAL IDEAL

Definition: A ring R is said to be a **ring with zero divisor** if

$$\exists \ 0 \neq a, b \ \in R \text{ such that } a.b = 0.$$

Definition: A ring R is said to be **ring without zero divisor** if

$a.b = 0$ *then either* $a = 0$ *or* $b = 0, \ \forall \ a, b \ \in R.$

Examples: (i) The ring of Integers is an example of ring without zero divisor.

(ii)A ring of 2x2 matrices with entries as integers is a ring without zero divisor.

Definition: A ring R is said to be an **Integral Domain** if

(i) R is commutative
(ii) R is ring with unity
(iii) R is without zero divisor.

Examples:

Z, Q are examples of Integral domain.

Definition: A ring R is said to be a **Field** if

(i) R is commutative
(ii) R is ring with unity
(iii) Ebach non-zero element of R possesses multiplicative inverse.

Examples: R(the ring of real numbers), Q (the ring of rational numbers) and C (the set of complex numbers) are examples of field.

Example: The set $G = \{\, a + ib \,:\, a, b \in Z\}$ of **Gaussian integers** forms a commutative ring with unity(1+i0) under addition and multiplication of complex numbers.

Is it a field?

Solu: G is not field. If a +ib be any non-zero element of G then its multiplicative inverse is $\frac{1}{a+ib} = \frac{1}{a+ib} \times \frac{a-ib}{a-ib} = \frac{a-ib}{a^2+b^2} = \frac{a}{a^2+b^2} + i\,\frac{(-b)}{a^2+b^2} \notin G$ since $\frac{a}{a^2+\,b^2}, \frac{-b}{a^2+\,b^2}$ are not integers. Hence, G is not a field.

Theorem: Prove that every field is an Integral domain. Does the converse true?

Proof: Let F be any field. By definition of field, F is commutative ring with unity. Therefore, in order to show F is an integral domain, it is enough that F has no zero divisors.

Suppose $a, b \in F \text{ such that } a \neq 0,\ a.b = 0$

Again, $a \neq 0 \Rightarrow a^{-1} \text{ exists}$.

Therefore, $a.b = 0$

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

Hence, $a \neq 0,\ a.b = 0 \Rightarrow b = 0$.

On the other hand, $\text{suppose } b \neq 0,\ a.b = 0$. Now $b \neq 0 \Rightarrow b^{-1} \text{ exists}$.

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

Thus, $a.b = 0 \Rightarrow \text{either } a = 0, \text{or } b = 0$.

This shows that F is without zero divisor and hence, F is an Integral domain.

Converse is not true. The ring of integers is an integral domain but not a field since integers does not have multiplicative inverse.

Theorem: Prove that a finite integral domain is a field.

Proof: Let F be a finite integral domain. This implies that F is a finite commutative ring without zero divisor. Suppose F has n-elements, a_1, a_2, a_3, a_4, ……. a_n.

In order to show that F is a field, it is enough to show that for every element

$0 \neq a \in F, \exists\ b \in F \text{ such that } a.b = 1.$

Suppose $0 \neq a \in F;\quad aa_1\ , aa_2\ , aa_3\ \ldots\ldots\ldots aa_n \in F.$

Also, $aa_1\ , aa_2\ , aa_3\ \ldots\ldots\ldots aa_n$ are all different elements of F. Therefore, one of the elements will be equal to a. Thus,

$$\exists\ c \in F \text{ such that } ac = a = ca$$

We have to show that c is the multiplicative identity of F.

Let $y \in F. \ Then, for\ x \ \in \ F, \ ax = y = xa.$

Now, cy = c(ax) = (ca)x = ax = y.

Hence, cy = y = yc for all y in F.

This shows that c is the unit element of F, denoted by 1. Now $1 \ \in F,$
$so \ \ one\ of\ element \ \ aa_1 \ \ , aa_2 \ \ , aa_3 \ \ \dots \dots \dots aa_n \ \ \in F$ will be equal to 1.

Thus, there exists $b \ \ \in F$ such that ab = 1 = ba, which shows that b is the multiplicative in verse of non-zero element of $a \ \in F.$ Hence, F is a field.

Definition: Let (R, +, .) be ring and S be a non-empty subset S of ring R. Then S is said to be **Subring** if S under same operation of R becomes a ring, i.e., (S, +, .) is a ring.

If R is any ring then {0} and R itself are always subring of R. These are known as Improper (trivial) subrings of R. Other subrings if any, of R are called Proper (non-trivial) subrings of R.

State and prove Necessary and Sufficient Conditions for a non-empty subset of a Ring to be a Subring

Statement: Let S be a non-empty subset of a ring R. Then S is a subring if and only if

$$\text{(i) } if\ a, b\ \in S\ then\ a - b\ \in S$$

$$(ii) if\ a, b\ \in S\ then\ ab\ \in S.$$

Proof: Suppose (S, +, .) is a subring of ring (R, +, .). Since S is a group under addition, $b\ \in S\ \Rightarrow\ -b\ \in S$. Again, S is closed under addition,

$$a \in S, b \in S\ \Rightarrow a \in S, -b \in S\ \ \Rightarrow a + (-b) \in S \Rightarrow a - b \in S.$$

Also, S is closed under multiplication, thus $if\ a, b\ \in S\ then\ ab\ \in S$.

Hence, the conditions are necessary.

Conversely, suppose S is non-empty subset of R and the conditions (i) and (ii) are satisfied. From (i), we have $a \in S, a \in S \Rightarrow a - a \in S \Rightarrow 0 \in S$.

Now, since $0 \in S, a \in S \Rightarrow 0 - a \in S \Rightarrow -a \in S,$ using (i).

If $a, b \in S$ then $-b \in S$. Using (i), we have $a - (-b) \in S \Rightarrow a + b \in S$.

Given S is subset of R. Therefore, associative and commutative property must hold in S since they hold in R. Thus, S is an Abelian group under addition. From (ii) S is closed under multiplication. Associativity of multiplication and distributivity of multiplication over addition must hold in S since they hold in R. Hence, S is a subring of R.

Theorem: The intersection of two subrings is a subring.

Proof: Let S and T be two subrings of a ring R. We have to show that $S \cap T$ is also a subring. It is trivial that $S \cap T$ is not empty subset of R,

since $0 \in S, 0 \in T, \ and\ S \subset R, T \subset R$. In order to show that $S \cap T$ is a subring it is enough to show that (i) $a - b \in S \cap T$ $(ii)\ a.b \in S \cap T\ \forall a, b \in S \cap T$.

We have $a \epsilon S \cap T$ $\Rightarrow$ a $\in$ S, a $\in$ T and b $\in S \cap T$ $\Rightarrow$ b $\in$ S, b $\in$ T.

Now, S and T are subrings, therefore $a \in S, b \in S \Rightarrow a - b \in S,\ a.b \in S$

Also $a \in T, b \in T \Rightarrow a - b \in T,\ \ a.b \in T$.

Thus, $a - b \in S, a - b \in T \Rightarrow a - b \in S \cap T$.

Also, $a.b \in S,\ a.b \in T \Rightarrow a.b \in S \cap T$. Hence, $S \cap T$ is a subring of R.

Theorem: An arbitrary intersection of subrings is a subring.

Proof: proof follows the same steps as in previous theorem.

Example: Let M be the ring of all 2x2 matrices with entries as integers. Then the set S of matrices $\begin{bmatrix} a & b \\ 0 & c \end{bmatrix}$ is a subring of ring M of 2x2 matrices.

Solution: Clearly, S is a subset of M.

Let $A, B \in S \Rightarrow A = \begin{bmatrix} a_1 & b_1 \\ 0 & c_1 \end{bmatrix}, B = \begin{bmatrix} a_2 & b_2 \\ 0 & 2 \end{bmatrix}$.

Then $A - B = \begin{bmatrix} a_1 - a_2 & b_1 - b_2 \\ 0 & c_1 - c_2 \end{bmatrix} \in S$.

Also, $A.B = \begin{bmatrix} a_1 a_2 & a_1 b_2 + b_1 c_2 \\ 0 & c_1 c_2 \end{bmatrix} \in S.$

Hence, S is a subring of M

Ex: Give an example to show that union of two subrings is not a subring

Solu: Consider the ring of integers (Z, +, .). Suppose S is a subring such that

S = { ….., -4, -2, 0, 2, 4…..} and T is a subring such that T = { ….-6, -3, 0, 3, 6,…}. Now $S \cup T = \{ ... -6, -4, -3, -2, 0, 2, 3, 4, 6, ... \}$.

As $2, 3 \in S \cup T$ but $2 + 3 \notin S \cup T$. Thus, $S \cup T$ is not closed under addition. Hence, $S \cup T$ is not a subring.

Definition: A non-empty subset I of ring (R, +, .) is said to be an **Ideal** of R if

(i) $For\ a, b \ \in I, \ \Rightarrow a - b \ \in \ I$
(ii) For $a \ \in I, \ r \ \in R, \ \Rightarrow a.r \ \in I$
(iii) For $a \ \in I, \ r \ \in R, \ \Rightarrow r.a \ \in I.$

Definition: An ideal P of ring R is said to be **Prime ideal** if $a.b \ \in P \ \Rightarrow either\ a \in P\ or\ b \ \in P.$

Definition: An ideal M of ring R is said to be **Maximal Ideal** if $M \neq R,$ and if for any ideal I of R such that

$M \subseteq I \ \subseteq R,$ we have I = M or I = R.

Examples:1. Let R = Z, the ring of integers and P = pZ, where p is prime. Then P is prime as well as maximal ideal.

2. Example of ring in which a prime ideal is not a maximal ideal.

Let R = ZxZ = {(a,b) / a, b $\in Z$}. Then (R, +, .) is ring.

Let I = {(a,0): a $\in Z$ }.Then I is prime ideal as

$(a_1, b_1)(a_2,b_2) \in I \Rightarrow (a_1 a_2, b_1 b_2) \in I, \Rightarrow b_1 b_2 = 0$

$\Rightarrow either \ \ b_1 = 0 \ \ or \ b_2 = 0$, since Z is an integral domain.

$\Rightarrow either \ (a_1, b_1) \in I, or \ (\ a_2, b_2) \ \in I.$

Hence, I is a prime ideal of R but not maximal ideal since there exists

J = {(a,2b)/ a,b $\in Z$} such that $I \subseteq J \ \subseteq R$.