Lecture 18 (Ring and Field)

Definition: A set R with two binary operations, addition (denoted by $a+b$) and multiplication (denoted by ab), is a ring, denoted by $(R,+,.)$, if the following conditions are satisfied.

1. $(R,+)$ is a commutative group.
2. Associative Property under multiplication: $a.(b.c) = (a.b).c, \quad \forall\ a,b,c \in R.$
3. Distributive Property: $a.(b+c) = a.b + a.c$ and $(b+c).a = b.a + c.a, \quad \forall\ a,b,c \in R.$

We say that a ring $(R,+,.)$ is commutative if $a.b = b.a$ for all $a,b \in R$.

Definition: A unity (or multiplicative identity) in a ring is a nonzero element that is an identity under multiplication. A nonzero element of a commutative ring with unity need not have a multiplicative inverse.

Theorem: (Rules of Multiplication)- Let a,b, and c belong to a ring R. Then

- $a.0 = 0.a = 0$,
- $a.(-b) = (-a).b = -(a.b)$,
- $(-a).(-b) = a.b$,
- $a.(b-c) = a.b - a.c$ and $(b-c).a = b.a - c.a$.

Furthermore, if R has a unity element 1, then

- $(-1).a = -a$.
- $(-1).(-1) = 1$.

Examples of Rings:

- The sets $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$ with respect to usual addition and usual multiplication are rings.
- The set $\mathbb{Z}_n = \{0,1,\ldots,n-1\}$ for $n \geq 1$ under addition and multiplication modulo n is a commutative ring with unity 1.
- The set $\mathbb{Z}[x]$ of all polynomials in the variable x with integer coefficients under ordinary addition and multiplication is a commutative ring with unity $f(x) = 1$.
- The set $2\mathbb{Z}$ of even integers under ordinary addition and multiplication is a commutative ring without unity.

- The set $M_2(\mathbb{Z})$ of 2×2 matrices with integer entries is a noncommutative ring with unity.

Subring: A subset S of a ring R is a subring of R if S is itself a ring with the operations of R.

(Subring Test) A nonempty subset S of a ring R is a subring if S is closed under subtraction and multiplication that is, if $a - b$ and $a.b$ are in S whenever a and b are in S.

Examples:

- $\{0\}$ and R are subrings of any ring R. $\{0\}$ is called the trivial subring of R.
- For each positive integer n, the set $n\mathbb{Z} = \{0, \pm n, \pm 2n, \pm 3n, \dots\}$ is a subring of the integers $\mathbb{Z}$.
- The set of Gaussian integers $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$ is a subring of the complex numbers $\mathbb{C}$.

Definition: A set F, containing at least two elements, with two binary operations, addition (denoted by $a + b$) and multiplication (denoted by $a.b$), is a field, denoted by $(F, +, .)$, if the following conditions are satisfied.

1. $(F, +)$ is a commutative group,
2. $(F \setminus \{0\}, .)$ is a commutative group, where 0 is additive identity of $(F, +)$,
3. Distributive Property $a.(b + c) = a.b + a.c$ and $(b + c).a = b.a + c.a$, $\forall\ a, b, c \in F$.

Examples of Fields:

- The sets $\mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$ with respect to usual addition and usual multiplication are fields.
- The set $\mathbb{Z}_p = \{0, 1, \dots, p-1\}$ for $p \geq 2$ under addition and multiplication modulo p is a field, where p is a prime number.
- The set $\mathbb{Z}$ of integers is not a field.