Lecture 19 (Ring and Field)

Definition: A ring R is a set with two binary operations, addition (denoted by $a+b$) and multiplication (denoted by ab), such that for all a, b, c in R :

1. $a+b=b+a$.
2. $(a+b)+c=a+(b+c)$.
3. There is an additive identity 0. That is, there is an element 0 in R such that $a+0=a$ for all a in R.
4. There is an element $-a$ in R such that $a+(-a)=0$.
5. Associative Property: $a(bc)=(ab)c$.
6. Distributive Property: $a(b+c)=ab+ac$ and $(b+c)a=ba+ca$.

The above can be summarized as follows: a ring is an Abelian group under addition, also having an associative multiplication that is left and right distributive over addition.
Definition: 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

- $a0=0a=0$.
- $a(-b)=(-a)b=-(ab)$.
- $(-a)(-b)=ab$.
- $a(b-c)=ab-ac$ and $(b-c)a=ba-ca$.
  Furthermore, if R has a unity element 1, then
- $(-1)a=-a$.
- $(-1)(-1)=1$.

Examples:

- 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.

Theorem: (**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 ab 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 field F, containing at least two elements, is a set with two binary operations, addition (denoted by $a + b$) and multiplication (denoted by ab), such that for all a, b, c in F :

1. $a + b = b + a$.
2. $(a + b) + c = a + (b + c)$.
3. There is an additive identity 0. That is, there is an element 0 in R such that $a + 0 = a$ for all a in R.
4. There is an element $-a$ in R such that $a + (-a) = 0$.
5. (Associativity of multiplication) $a(bc) = (ab)c$.
6. (Distributivity of multiplication) $a(b + c) = ab + ac$ and $(b + c)a = ba + ca$.
7. (Commutativity of multiplication) $ab = ba$.
8. (Existence of a multiplicative identity) There is an element $1 \in F$, such that $1 \neq 0$ and $a.1 = a$.
9. (Existence of a multiplicative inverses) If $x \neq 0$, then there is an element $x^{-1} \in F$ such that $xx^{-1} = 1$.

Examples:

- 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.