**Definition 12.1** ***Ring.***
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.** $a(bc) = (ab)c$.

**6.** $a(b + c) = ab + ac$ and $(b + c)a = ba + ca$.

**Remark.**
Note that multiplication need not be commutative. When it is, we say that the ring is *commutative*. Also, a ring need not have an identity under multiplication. A *unity* (or *identity*) in a ring is a nonzero element that is an identity under multiplication. A nonzero element of a com- mutative ring with unity need not have a multiplicative inverse. When it does, we say that it is a unit of the ring. Thus, $a$ is a unit if $a^{-1}$ exists.
The following terminology and notation are convenient. If $a$ and $b$ belong to a commutative ring $R$ and $a$ is nonzero, we say that $a$ *divides* $b$ (or that $a$ is a *factor* of $b$) and write $a|b$, if there exists an element $c$ in $R$ such that $b = ac$. If $a$ does not divide $b$, we write $a \nmid b$.

**Definition 12.2** ***Subring.***
A subset $S$ of a ring $R$ is a *subring of* $R$ if $S$ is itself a ring with the operations of $R$.

**Definition 13.1** ***Zero Divisors.***
A *zero-divisor* is a nonzero element $a$ of a commutative ring $R$ such that there is a nonzero element $b \in R$ with $ab = 0$.

**Definition 13.2** ***Integral Domain.***
An *integral domain* is a commutative ring with unity and no zero-divisors.

**Definition 13.3** ***Field.***
A *field* is a commutative ring with unity in which every nonzero element is a unit.

**Definition 13.4** ***Characteristic of a Ring.***
The *characteristic* of a ring $R$ is the least positive integer $n$ such that $nx = 0$ for all $x$ in $R$. If no such integer exists, we say that $R$ has characteristic 0. The characteristic of $R$ is denoted by char $R$.

**Definition 14.1** ***Ideal.***
A subring $A$ of a ring $R$ is called a (two-sided) *ideal* of $R$ if for every $r \in R$ and every $a \in A$ both $ra$ and $ar$ are in $A$.

**Remark.**
A *proper* ideal is an ideal $I$ of some ring $R$ such that it is a proper subset of $R$; that is, $I \subset R$.

**Definition 14.2** ***Prime Ideal, Maximal Ideal.***
A *prime ideal* $A$ of a commutative ring $R$ is a proper ideal of $R$ such that $a, b \in R$ and $ab \in A$ imply $a \in A$ or $b \in A$. A *maximal* ideal of a commutative ring $R$ is a *proper* ideal of $R$ such that, whenever $B$ is an ideal of $R$ and $A \subseteq B \subseteq R$, then $B = A$ or $B = R$.

**Definition 15.1** ***Ring Homomorphism, Ring Isomorphism.***
A *ring homomorphism* $\phi$ from a ring $R$ to a ring $S$ is a mapping from $R$ to $S$ that preserves the two ring operations; that is, for all $a, b$ in $R$,

$$\phi(a + b) = \phi(a) + \phi(b) \quad \text{and} \quad \phi(ab) = \phi(a)\phi(b)$$

A ring homomorphism that is both one-to-one and onto is called a *ring isomorphism*.

**Definition 16.1** ***Ring of Polynomials over* R.**
Let $R$ be a commutative ring. The set of formal symbols

$$R[x] = \{a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \mid a_i \in R, n \in \mathbb{Z}^+\}$$

is called the *ring of polynomials over $R$ in the indeterminate $x$.*
Two elements

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

and

$$b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0$$

of $R[x]$ are considered equal if and only if $a_i = b_i$ for all nonnegative integers $i$. (Define $a_i = 0$ when $i > n$ and $b_i = 0$ when $i > m$.)

**Definition 16.2** ***Addition and Multiplication in* R[x].**
Let $R$ be a commutative ring and let

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

and

$$g(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0$$

belong to $R[x]$. Then

$$f(x) + g(x) = (a_s + b_s)x^s + (a_{s-1} + b_{s-1})x^{s-1} + \cdots + (a_1 + b_1)x + a_0 + b_0$$

where $s$ is the maximum of $m$ and $n$, $a_i = 0$ for $i > n$, and $b_i = 0$ for $i > m$. Also,

$$f(x)g(x) = c_{m+n}x^{m+n} + c_{m+n-1}x^{m+n-1} + \cdots + c_1 x + c_0$$

where

$$c_k = a_k b_0 + a_{k-1}b_1 + \cdots + a_1 b_{k-1} + a_0 b_k$$

for $k = 0, \ldots, m+n$.

**Definition 16.3** ***Principal Ideal Domain (PID).***
A *principal ideal domain* is an integral domain $R$ in which every ideal has the form $\langle a \rangle = \{ra \mid r \in R\}$ for some $a$ in $R$.

**Definition 17.1** ***Irreducible Polynomial, Reducible Polynomial.***
Let $D$ be an integral domain. A polynomial $f(x)$ from $D[x]$ that is neither the zero polynomial nor a unit in $D[x]$ is said to be *irreducible over $D$*, whenever $f(x)$ is expressed as a product $f(x) = g(x)h(x)$, with $g(x)$ and $h(x)$ from $D[x]$, then $g(x)$ or $h(x)$ is a unit in $D[x]$. A nonzero, nonunit element of $D[x]$ that is not irreducible over $D$ is called *reducible over $D$*.

**Definition 17.2** ***Content of a Polynomial, Primitive Polynomial.***
The *content* of a nonzero polynomial $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$, where the $a$'a are integers, is the greatest common divisor of the integers $a_n, a_{n-1}, \ldots, a_0$. A *primitive polynomial* is an element of $\mathbb{Z}[x]$ with content 1.