Notes on Ring Theory & Linear Algebra - I (Core Course - VI)
Prepared by Subhasundar Bandyopadhyay (SB)

Books followed : 1. Higher Algebra (Abstract and Linear) - S. K. Mapa
2. Topics in Abstract Algebra - M. K. Sen, Shamik Ghosh & Parthasarathi Mukhopadhyay
3. Fundamentals of Abstract Algebra. D. S. Malik, John M. Mordeson and M. K. Sen
4. Contemporary Abstract Algebra - Joseph Gallian
5. A first Course in Abstract Algebra - J. B. Fraleigh

Unit-1 : Ring theory :

1.1 Definition of Ring : A ring $R$ is an algebraic structure $(R, +, \cdot)$ consisting of a non-empty set $R$ together with two binary operations $+$ and $\cdot$ (called addition and multiplication) such that the following conditions are satisfied :

1. $(R, +)$ is an abelian group,
2. $(R, \cdot)$ is a semigroup and
3. for any three elements $a, b, c \in R$,
   $a\cdot(b+c) = a\cdot b + a\cdot c$ (called left distributive law)
   $(b+c)\cdot a = b\cdot a + c\cdot a$ (called right distributive law)

We denote the identity element of the group $(R, +)$ by the symbol $0$ and the (additive) inverse of $a$ by $-a$ for all $a \in R$. If $R = \{0\}$, then $R$ is called the trivial ring.

So, we now write the definition of a ring in the following way :

A ring is an ordered triple $(R, +, \cdot)$ such that $R$ is a non-empty set where $+$ and $\cdot$ are two binary operations on $R$ (i.e., for each pair $(a, b)$ of elements $a, b \in R$, $\exists$ unique elements $a+b$ and $a\cdot b$ in $R$) satisfying the following axioms for all $a, b, c \in R$ :

(i) $a+b = b+a$ (commutative law for addition) ;
(ii) $a+(b+c) = (a+b)+c$ (associative law for addition) ;
(iii) $\exists$ an element $0 \in R$ such that $a+0 = a$ for all $a \in R$ (existence of additive identity)
(iv) for each $a \in R$, $\exists$ an element $-a \in R$ such that $a+(-a) = 0$ (existence of additive inverse)
(v) $a\cdot(b\cdot c) = (a\cdot b)\cdot c$ for all $a, b, c \in R$
(vi) $\left.\begin{array}{ll} a\cdot(b+c) = a\cdot b + a\cdot c & \text{(left distributive law)} \\ (b+c)\cdot a = b\cdot a + c\cdot a & \text{(right distributive law)} \end{array}\right\}$ (distributive laws)

Note 1.1.1. The ring $(R, +, \cdot)$ is sometimes denoted by $R$ when no confusion regarding the underlying binary operations arises.

1.1.2. Definition: $R$ is said to be a commutative ring if the multiplication is commutative (i.e., if $a \cdot b = b \cdot a$ for all $a, b \in R$) in the ring $R$. In a commutative ring $R$, the left and right distributive law is the same, called the distributive law.
$R$ is said to be a ring with unity if $\exists$ an element $1 \in R$ such that $a \cdot 1 = 1 \cdot a = a$ for all $a \in R$. The element 1, if exists, is unique. It is called the unity in $R$.

Note 1.1.3. $a \cdot b$ is generally written as $ab$.

1.1.4 Examples of Ring

1. $(\mathbb{Z}, +)$ is a commutative group and $(\mathbb{Z}, \cdot)$ is commutative monoid, 1 being the identity element. The distributive law holds. So, $(\mathbb{Z}, +, \cdot)$ is a commutative ring with unity.
$(\mathbb{Q}, +, \cdot)$ is a ~~commutative~~ commutative ring with unity.
$(\mathbb{C}, +, \cdot)$ is a commutative ring with unity.
$(\mathbb{R}, +, \cdot)$ is a commutative ring with unity.
[$\mathbb{Z}$ is the set of all integers, $\mathbb{Q}$ is the set of all rational numbers, $\mathbb{R}$ is the set of all real numbers and $\mathbb{C}$ is the set of all complex numbers. The binary operations $+$ and $\cdot$ are addition and multiplication in the respective sets]

2. Ring of integers modulo $n$: For a fixed $n \in \mathbb{N}$ (the set of all natural numbers), let $\mathbb{Z}_n$ be ~~the class~~ the set of all classes of residues of integers modulo $n$. Then $\mathbb{Z}_n = \{\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{n-1}\}$.
$(\mathbb{Z}_n, +)$ is a commutative group, where $+$ denotes addition (modulo $n$).
$(\mathbb{Z}_n, \cdot)$ is a commutative monoid where $\cdot$ denotes multiplication (modulo $n$).
The distributive law holds.

3. $(2\mathbb{Z}, +)$ is a commutative group and $(2\mathbb{Z}, \cdot)$ is a commutative semigroup. The distributive law holds

Note: Let $n \in \mathbb{N}$. Then $(n\mathbb{Z}, +, \cdot)$ is a commutive ring. If $n > 1$, then it is a commutative ring without unity.

4. Ring of Gaussian integers: Let us consider the subset of $\mathbb{C}$ given by $\mathbb{Z}[i] = \{a+ib \in \mathbb{C} : a, b \in \mathbb{Z},\ i = \sqrt{-1}\}$ i.e., $\mathbb{Z}[i]$ is the set of all complex numbers of the form $a+ib$, where $a$ and $b$ are integers. $\mathbb{Z}[i]$ forms a ring under addition and multiplication of complex numbers. This is a commutative ring with unity. This ring is called the ring of Gaussian integers.

5. Let $(G, +)$ be an abelian group, written additively. Define $a \cdot b = 0$ for all $a, b \in G$, where $0$ is the identity in $G$. Then $(G, +, \cdot)$ becomes a ring, called a null ring or zero ring.

6. Let $(G, +)$ be an abelian group and $R$ be the set of all endomorphisms of $G$ (An endomorphism of a group $G$ is a homomorphism from $G$ to $G$). Let $f, g \in R$ and we define $f+g$ and $f \circ g$ as follows: $(f+g)(x) = f(x) + g(x)$, $x \in G$ and $(f \circ g)(x) = f(g(x))$, $x \in G$.

Then $f+g$ and $f \circ g$ are in $R$ as for $x, y \in G$

$$
\begin{aligned}
(f+g)(x+y) &= f(x+y) + g(x+y) = f(x) + f(y) + g(x) + g(y) \\
&= f(x) + g(x) + f(y) + g(y) \quad (\text{As } G \text{ is abelian}) \\
&= (f+g)(x) + (f+g)(y)
\end{aligned}
$$

and

$$
\begin{aligned}
(f \circ g)(x+y) &= f(g(x+y)) = f(g(x) + g(y)) \\
&= f(g(x)) + f(g(y)) \\
&= (f \circ g)(x) + (f \circ g)(y)
\end{aligned}
$$

We can check that $(R, +, \circ)$ is a ring (called the ring of endomorphisms of $G$).

The additive identity of $R$ is the null mapping $\theta$ defined as: $\theta(x) = 0_G$ for all $x \in G$ where $0_G$ is the additive identity in $G$. Additive inverse of $f \in R$ is $-f$ defined by $(-f)(x) = -f(x)$ for all $x \in G$.

7. Let $R_1$ and $R_2$ be two rings. Let $R = R_1 \times R_2$. Define on $R$
$(a, b) + (c, d) = (a+c, b+d)$ and $(a, b) \cdot (c, d) = (ac, bd)$

Then $(R, +, \cdot)$ is a ring where $(0_{R_1}, 0_{R_2})$ is the additive identity element ($0_{R_1}$ is the additive identity of $R_1$ and $0_{R_2}$ is the additive identity of $R_2$) and $-(a, b) = (-a, -b)$ for all $a \in R_1$, $b \in R_2$. This ring $R$ is called the direct product of the rings $R_1$ and $R_2$.

8. Let $\mathbb{R}$ be the set of all real numbers. Denote the set of all polynomials (in the indeterminate $x$) with real coefficients by $\mathbb{R}[x]$. It is easy to verify that $(\mathbb{R}[x], +, \cdot)$ is a commutative ring with unity with the usual addition and multiplication of polynomials.

One may generalise the above concept for a commutative ring $R$ with unity. Let $R[x]$ be the set of all polynomials, in the indeterminate $x$, with coefficients in $R$. Define for any
$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$, $g(x) = b_0 + b_1 x + b_2 x^2 + \cdots + b_m x^m \in R[x]$

$$f(x) + g(x) = (a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2 + \cdots + (a_p + b_p)x^p$$
$$f(x)g(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_{m+n} x^{m+n},$$

where $p = \max\{m, n\}$ (considering $a_r = 0$ for all $r > n$ and $b_s = 0$ for all $s > m$)

and $c_k = \sum\limits_{\substack{i,j=0 \\ i+j=k}}^{k} a_i b_j$ for each $k = 0, 1, 2, \ldots, m+n$

i.e., $c_k = a_0 b_k + a_1 b_{k-1} + a_2 b_{k-2} + \cdots + a_k b_0$, $k = 0, 1, \ldots, m+n$

i.e., $c_0 = a_0 b_0$, $c_1 = a_0 b_1 + a_1 b_0$, $c_2 = a_0 b_2 + a_1 b_1 + a_2 b_0$, etc.

Then $(R[x], +, \cdot)$ forms a ring with the above addition and multiplication of polynomials. This ring is called polynomial ring over $R$.

9. Let $M_n(\mathbb{R})$ be the set of all $n \times n$ matrices. Then $(M_n(\mathbb{R}), +, \cdot)$ is a ring where $+$ is the matrix addition and $\cdot$ is the matrix multiplication.