

Rings and Modules

Nachiketa Kulkarni

Contents

1	Introduction to Rings	1
1.1	Definition of a Ring	1
1.1.1	Examples	1
1.2	Properties of Rings	2
1.3	Homomorphisms and Isomorphisms	2
1.3.1	Properties of Ring Homomorphisms	3
1.3.2	Ideals	3

Chapter 1

Introduction to Rings

1.1 Definition of a Ring

A ring R is a set with two binary operations, $+$ and \times , satisfying the following conditions:

- $(R, +)$ is an abelian group.
- \times is associative.
- \times distributes over $+$.

A Ring is said to be commutative if $a \times b = b \times a$ for all $a, b \in R$.

A Ring is said to have a multiplicative identity if there exists an element $1 \in R$ such that $1 \times a = a \times 1 = a$ for all $a \in R$.

Subrings: A subset S of a ring R is called a subring if:

- S is closed under addition and multiplication.
- S contains the additive identity 0 of R .
- For every $a \in S$, $-a \in S$.

1.1.1 Examples

- **Trivial Ring:** Take any abelian group $(G, +)$ and define multiplication as $a \times b = 0$ for all $a, b \in G$, where 0 is the identity of the group.
- **Integers:** The set of integers \mathbb{Z} with usual addition and multiplication forms a ring. Also, the quotient group $\mathbb{Z}/n\mathbb{Z}$ is a ring for any integer n .
- **Hamiltonian Quaternions:** The set of quaternions $\mathbb{H} = 1, i, j, k$, where $i^2 = j^2 = k^2 = -1$.
- **Polynomial Rings:** Fix a commutative ring R . The set of polynomials with coefficients in R , denoted $R[x]$, forms a ring with addition and multiplication defined as usual.

1.2 Properties of Rings

Proposition: If R is a ring, then the following hold:

1. $0a = a0 = 0$ for all $a \in R$.
2. $(-a)b = a(-b) = -(ab)$ for all $a, b \in R$.
3. If the ring has a multiplicative identity 1 , then it is unique.
4. $(-1)a = -a$ for all $a \in R$.

More Definitions: Consider a ring R :

- A non-zero element $a \in R$ is called a **zero divisor** if there exists a non-zero $b \in R$ such that either $ab = 0$ or $ba = 0$.
- Assume R has a multiplicative identity 1 . An element $a \in R$ is called a **unit** if there exists an element $b \in R$ such that $ab = ba = 1$. The set of all units in R is denoted by R^\times .
- A Ring R with identity is called an **integral domain** if it has no zero divisors and $1 \neq 0$.

Proposition: If R is an integral domain, then the following hold:

1. R^\times is a group under multiplication.
2. R is a field if multiplication is commutative and every non-zero element is a unit, i.e., $R^\times = R - \{0\}$.
3. A zero divisor cannot be a unit and vice versa.

Proof: If a is a zero divisor, then there exists a non-zero b such that $ab = 0$. Now, assume a is a unit, then there exists c such that $ac = 1$. But:

$$b = (ca)b = c(ab) = c0 = 0$$

1.3 Homomorphisms and Isomorphisms

Let R and S be rings. A **ring homomorphism** is a function $\phi : R \rightarrow S$ such that:

1. The map ϕ preserves addition: $\phi(a + b) = \phi(a) + \phi(b)$ for all $a, b \in R$.
2. The map ϕ preserves multiplication: $\phi(ab) = \phi(a)\phi(b)$ for all $a, b \in R$.

The kernel of a ring homomorphism ϕ , $\ker(\phi)$, is the set of elements in R that map to 0 in S . The Image of a ring homomorphism ϕ , $\text{Im}(\phi)$, is the set of elements in S that are images of elements in R . A bijective ring homomorphism is called a **ring isomorphism**, denoted by $R \cong S$.

1.3.1 Properties of Ring Homomorphisms

Let R and S be rings and $\phi : R \rightarrow S$ be a ring homomorphism. Image of ϕ is denoted by $\text{Im}(\phi)$ and kernel of ϕ is denoted by \ker .

Proposition: $\text{Im}(\phi)$ is a subring of S .

Proof: $\text{Im}(\phi)$ is a subring of S because:

- **Closure under addition:** If $x, y \in \text{Im}(\phi)$, then there exist $a, b \in R$ such that $\phi(a) = x$ and $\phi(b) = y$. Now, $\phi(a + b) = \phi(a) + \phi(b) = x + y$, hence $x + y \in \text{Im}(\phi)$.
- **Closure under multiplication:** If $x, y \in \text{Im}(\phi)$, then there exist $a, b \in R$ such that $\phi(a) = x$ and $\phi(b) = y$. Now, $\phi(ab) = \phi(a)\phi(b) = xy$, hence $xy \in \text{Im}(\phi)$.
- **Associativity of Addition and Multiplication** Inherited from the ring.
- **Additive Identity** $\phi(0) = 0$

Hence, $\text{Im}(\phi)$ is a subring of S .

Proposition: $\ker(\phi)$ is a subring of R . Also, if $\alpha \in R$, then $\{r\alpha, \alpha r\} \in \ker(\phi), \forall r \in R$.

Proof: Part 1 of the proof is same as above. For the second part, let $\phi(\alpha) = 0$ and $\phi(r) = a$.

$$0 = 0a = \phi(\alpha)\phi(r) = \phi(\alpha r) \qquad 0 = a0 = \phi(r)\phi(\alpha) = \phi(r\alpha)$$

1.3.2 Ideals

Definition: Let R be a ring, I be a subgroup of R . Let $r \in R$:

1. $rI = \{ra \mid a \in R\}$ and $Ir = \{ar \mid a \in R\}$
2. A subgroup I is called a left Ideal of R if:
 - I is a subring of R .
 - I is closed under left multiplication by elements from R , i.e., $rI \subseteq I$

The right Ideal is similarly defined.

3. If I is a botha left Ideal and right Ideal, then it is called an Ideal (two sided) of R .