1 Ring

Recall that a group is a set equipped with a binary operation. However, often times, a lot of sets are naturally endowed with two binary operations: addition and multiplication. In this case, we want to account for both of them at the same time instead of having two groups with the same sets but different operations. To that, we introduce the ring.

1.1 The Ring: Definition

Definition 1.1: 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. Commutative: a + b = b + a
- 2. **Associative:** (a + b) + c = a + (b + c)
- 3. Additive Identity: There is an additive identity $0 \in R$ such that a + 0 = 0 + a = a for all $a \in R$.
- 4. Additive Inverse: There is an element $-a \in R$ such that a + (-a) = (-a) + a = 0.
- 5. Associative: a(bc) = (ab)c.
- 6. Distributive Property: a(b+c) = ab + ac and (b+c)a = ba + ca.

We sometimes write this ring out as $(R, +, \cdot)$.

Remarks:

- A ring is an abelian group under addition, but also has an associative multiplication that is *left and* right distributive over addition.
- Multiplication does not have to be commutative. If it is commutative, we say that the ring is commutative.
- A ring does not need to 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 <u>commutative ring</u> with unity need not have a multiplicative inverse. When it does, we say that it is a <u>unit</u> of the ring. In other words, a is a unit if a^{-1} exists.
- If a and b belong to a commutative ring R and a is nonzero, then we say that a divides b (or that a is a factor of b) and write a|b if there exists $c \in R$ such that b = ac. If a does not divide b, we write $a \nmid b$.
- If we need to deal with something like:

$$\underbrace{a+a+\cdots+a}_{n \text{ times}}$$

Then, we will use $n \cdot a$ to mean this.

1.2 Basic Applications of the Ring

Here, we introduce several examples of rings.

1.2.1 Example 1: Integer Rings

$$\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$$

The set of integers under ordinary addition and multiplication is a commutative ring with unity 1. The *units* of \mathbb{Z} are 1 and -1.

1.2.2 Example 2: Integers Mod N

$$\mathbb{Z}/n\mathbb{Z} = \{0, 1, \dots, n-1\}$$

The set of integers modulo n under addition and multiplication is also a commutative ring with unity 1. The set of *units* is U(n). Here, we define U(n) to be the set of integers less than n and relatively prime to n under multiplication modulo n.

This can also be written as \mathbb{Z}_n .

1.2.3 Example 3: Polynomial Rings

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. Here, we define:

$$\mathbb{Z}[x] = \{a_0 + a_1x + a_2x^2 + \dots + a_nx^n \mid a_i \in \mathbb{Z}\}\$$

So, for example, $x^2 + 4x + 5 \in \mathbb{Z}[x]$.

1.2.4 Example 4: Matrix Rings

The set $M_2(\mathbb{Z})$ of 2×2 matrices with integer entries is a noncommutative ring with unity $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$.

1.2.5 Example 5: Even Integer Rings

The set $2\mathbb{Z}$ of even integers under ordinary addition and multiplication is a commutative ring without unity.

1.2.6 Example 6: Direct Sum

If R_1, R_2, \ldots, R_n are rings, then we can create a new ring:

$$R_1 \oplus R_2 \oplus \cdots \oplus R_3 = \{(a_1, a_2, \dots, a_n) \mid a_i \in R_i\}$$

From this, we can perform componentwise addition and multiplication; that is:

$$(a_1, a_2, \dots, a_n) + (b_1, b_2, \dots, b_n) = (a_1 + b_1, a_2 + b_2, \dots, a_n + b_n)$$
$$(a_1, a_2, \dots, a_n)(b_1, b_2, \dots, b_n) = (a_1b_1, a_2b_2, \dots, a_nb_n)$$

1.3 More on Rings

Definition 1.2: Commutative Ring

A ring R is **commutative** if ab = ba for all $a, b \in R$.

Definition 1.3: Unity

A ring R has **unity** if $1 \in R$ is a multiplicative identity:

$$1a = a1 = a$$

Definition 1.4: Unit

An element $a \in R$ is called a **unit** if it has a multiplicative inverse. In other words, a is a unit if there exists an $a^{-1} \in R$ such that:

$$a^{-1}a = aa^{-1} = 1$$

Remarks:

- $U(R) = \{ \text{Units in } R \}$
- $U(n) = \{\text{Units in } \mathbb{Z}/n\mathbb{Z}\}$

Definition 1.5: Division

For $a, b \in R$, we say that a **divides** b and write a|b if b = ac for some $c \in R$.