Rings

Definition of a Ring

A set $S$ is an associative ring if there are two operators $+$ and $\cdot$ such that:

1. $S$ is an abelian group under $+$.
2. $S$ is closed under $\cdot$.
3. For any $a, b, c \in S$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$. In other words, multiplication in $S$ is associative.
4. For any $a, b, c \in S$, $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(b + c) \cdot a = b \cdot a + c \cdot a$. In other words, multiplication distributes over addition in $S$.

Notes:

- When we say ring, we shall mean an associative ring.
- To avoid confusion, we use $0$ to represent the additive identity and $-a$ to represent the additive inverse of $a$.
- There is no requirement that a ring $R$ have a multiplicative identity. If it has one, we call the ring a ring with unit element and represent the multiplicative identity as $1$. Moreover, there is no requirement that every element have a multiplicative inverse.
- A ring is called a commutative ring if multiplication is commutative in the ring.

Examples of Rings

Theorem: The real numbers form a commutative ring with unit element over standard addition and multiplication.

Proof. We show that the above properties hold.

- We have already shown that the real numbers form an abelian group under addition.
- The product of any two real numbers is a real number.
- Multiplication over real numbers is associative.
- Multiplication distributes over addition for real numbers.
- Multiplication is commutative in $\mathbb{R}$.
- $1$ is a multiplicative identity in $\mathbb{R}$, as $1 \cdot a = a \cdot 1 = a$ for any $a \in \mathbb{R}$.

Theorem: The even integers form a commutative ring with no unit element over standard addition and multiplication.
Proof. We show that the above properties hold. They can be proven more rigorously than presented here.

- To show that the even integers form an abelian group under addition, we’ll show that it’s a subgroup of the integers.
  - The even integers are closed under addition.
  - If \( a \) is an even integer, so is \(-a\), its additive inverse.

Therefore, the even integers form a subgroup of the integers and are thus a group themselves. Addition of any integers is commutative, so the even integers are an abelian group under addition.

- The product of even integers is also an even integer.
- Multiplication over (even) integers is associative.
- Multiplication distributes over addition for (even) integers.
- Multiplication is commutative over (even) integers.
- There is no even integer \( e \) such that for any even integer \( a \), \( a \cdot e = e \cdot a = a \).

It is also true that the integers and complex numbers form commutative rings with unit element over standard addition and multiplication.

**Properties of Rings**

**Theorem:** If \( R \) is a ring, then \( a \cdot 0 = 0 \cdot a = 0 \) for any \( a \in R \).

*Proof.* First, we show that \( a \cdot 0 = 0 \). Since 0 is the additive identity in \( R \), \( 0 = 0 + 0 \). Therefore, \( a \cdot 0 = a \cdot (0 + 0) \). By the distributive property, this means that \( a \cdot 0 = a \cdot 0 + a \cdot 0 \). We can add the additive inverse of \( a \cdot 0 \) to each side, giving \( 0 = a \cdot 0 \).

Similarly, \( 0 \cdot a = 0 \) because \( a \cdot a = (0 + 0) \cdot a = 0 \cdot a + 0 \cdot a \) and so \( 0 \cdot a = 0 \).

**Theorem:** If \( R \) is a ring, then \((-a) \cdot b = a \cdot (-b) = -(a \cdot b)\) for any \( a, b \in R \).

*Proof.* We have that \((-a) \cdot b = 0(a \cdot b)\) if \((-a) \cdot b + a \cdot b = 0\), since we showed earlier that the additive inverse of a group is unique. But by the distributive property of rings, we have that \((-a) \cdot b + a \cdot b = (-a + a) \cdot b = 0 \cdot b = 0\).

We use the same approach to show that \( a \cdot (-b) = -(a \cdot b) \).

**Theorem:** If \( R \) is a ring, then \((-a) \cdot (-b) = a \cdot b \) for any \( a, b \in R \).

*Proof.* The above theorem shows that \((-a) \cdot (-b) = -(a \cdot (-b)) = -(a \cdot b))\). We showed earlier that if \( G \) is a group, then \((g^{-1})^{-1} = g\) for any \( g \in G \). Since \( R \) is a group under addition and \(-(-(a \cdot b))\) is just the inverse of the inverse of \((a \cdot b)\), \((-a) \cdot (-b) = a \cdot b \).
Theorem: If \( R \) is a ring with unit element 1, then \((-1) \cdot a = -a\) for any \( a \in R \).

*Proof.* \((-1) \cdot a = -a\) if \((-1) \cdot a + a = 0\). Because 1 is the unit element, \( a = 1 \cdot a \) and so \((-1) \cdot a + a = (-1) \cdot a + 1 \cdot a = (-1 + 1) \cdot a = 0 \cdot a = 0\).

\[ \square \]

Theorem: If \( R \) is a ring with unit element 1, then \((-1) \cdot (-1) = 1\).

*Proof.* This follows from the previous theorem for \( a = -1 \).

\[ \square \]

Fields

Definition of a Field

A set \( S \) is a field if:

1. \( S \) forms a commutative ring.
2. The set \( S \setminus \{0\} \) forms a group under multiplication.

Examples of Fields

It follows directly from what has been shown so far that \( \mathbb{R} \) and \( \mathbb{C} \) are fields and that the integers and even integers are not fields.

Practice Problems

1. Is each of the following a ring? A field?
   - The rational numbers
   - The irrational numbers
   - The odd integers
   - The set \( \{0, 1, 2, 3, 4\} \) under addition and multiplication mod 5.
   - The set \( \{0, 1, 2, 3, 4, 5\} \) under addition and multiplication mod 6.
   - The set \( \{a + b\sqrt{2} \mid a, b \in \mathbb{R}\} \)

2. Show that, if \( R \) is a ring and \( a, b \in R \), then \((a + b) \cdot (a + b) = a \cdot a + a \cdot b + b \cdot a + b \cdot b\).