Modern Algebra

Rings and Subrings

Orville D. Hombrebueno
odhombrebueno@nvsu.edu.ph

Saint Mary's University

March 30, 2019

The most general algebraic structure with two binary operations is called a *ring*.

Definition

A **ring** $\langle R, +, \cdot\rangle$ is a *set* R together with two binary operations $+$ and $\cdot$, which we call *addition* and *multiplication* defined on R such that the following axioms are satisfied $\forall\ a,\ b,\ c \in R$:

1. $\langle R, +\rangle$ is an abelian group.
   a. $a + b \in R$. (Closure)
   b. $a + (b + c) = (a + b) + c$. (Associative)
   c. $\exists\ 0 \in R$ s.t. $a + 0 = 0 + a = a$. (Identity)
   d. $\forall\ a \in R$, $\exists\ -a \in R$ s.t. $a + -a = -a + a = 0$. (Inverse)
   e. $a + b = b + a$. (Commutative)
2. R is closed under $\cdot$, $a \cdot b \in R$.
3. Multiplication is associative, $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.
4. $\forall\ a,\ b,\ c \in R$, the **left distributive law**, $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ and the **right distributive law** $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$ hold. ■

Examples

For example, $\langle \mathbb{Z}, +, \cdot\rangle$, $\langle \mathbb{Q}, +, \cdot\rangle$, $\langle \mathbb{R}, +, \cdot\rangle$, and $\langle \mathbb{C}, +, \cdot\rangle$ are rings.

Let R be any ring and let $M_n(R)$ be the collection of all $n \times n$ matrices having elements of R as entries. $M_n(R)$ is a ring. In particular, we have the rings $M_n(\mathbb{Z})$, $M_n(\mathbb{Q})$, $M_n(\mathbb{R})$, and $M_n(\mathbb{C})$. Note that multiplication is not a commutative operation in any of these rings for $n \geq 2$.

Let F be the set of all functions $f : \mathbb{R} \longrightarrow \mathbb{R}$. F is a ring.

Recall that in group theory, $n\mathbb{Z}$ is the cyclic subgroup of $\mathbb{Z}$ under addition consisting of all integer multiples of the integer n. $n\mathbb{Z}$ is a ring.

$\mathbb{Z}_n$ is a ring.

If $R_1,\ R_2, \cdots, R_n$ are rings, we can form the set $R_1 \times R_2 \times \cdots \times R_n$ of all ordered n-tuples $(r_1,\ r_2, \cdots, r_n)$, where $r_i \in R_i$. The set of all these n-tuples forms a ring under addition and multiplication by components. The ring $R_1 \times R_2 \times \cdots \times R_n$ is the **direct product** of the rings R_i.

Remarks

- A ring that is commutative under multiplication is called a *commutative ring*.
- R is a ring with *unity* if $\forall\ a \in R$, $\exists\ 1 \in R$ s.t. $1 \cdot a = a \cdot 1 = a$.
- R is a ring with a *unit* if $\forall\ a \in R$, $\exists\ a^{-1} \in R$ s.t. $a \cdot a^{-1} = a^{-1} \cdot a = 1$.

Properties of a Ring

Suppose R is a ring, $\forall\ a,\ b \in R$ the following holds:

1. $0 \cdot a = 0$,
2. $0 \neq 1$ (unless $R = \{0\}$),
3. $a \cdot (-b) = -(a \cdot b)$,
4. $(-a) \cdot (-b) = a \cdot b$,
5. $(-1) \cdot a = -a$. ■

Definition

Suppose R is a ring. A set S is a **subring** of R if:

1. $S \subseteq R$,
2. S is a ring under the operations of R. ■

Subring Test

$S \leq R$ if the following holds for S:

1. Closure$(+)$.
2. Closure$(\cdot)$.
3. $0 \in S$.
4. $\forall a \in S, \exists\ -a \in S$.

Example

Subring Proof:

$S = \{\cdots, -6, -3, 0, 3, 6, \cdots\} \leq \mathbb{Z}$

$S = \{3 \cdot m \mid m \in \mathbb{Z}\}$

1. Closure$(+)$.

Let a, b in