Math 521A

3.1 – Definition and Examples of Rings

Definition

A ring a set $R \neq \emptyset$ (empty set) equipped with two operations $+$ and $\cdot$ that satisfy the following properties:

1. $a + b \in R, \forall\ a, b \in R.$
2. $a + (b + c) = (a + b) + c, \forall\ a, b, c \in R.$
3. $a + b = b + a, \forall a, b \in R.$
4. $\exists\ 0_R \in R$ such that $a + 0_R = 0_R + a = a, \forall\ a \in R.$
5. $\forall\ a \in R, \exists\ b \in R$ such that $a + b = b + a = 0_R.$
6. $a \cdot b \in R, \forall\ a, b \in R.$
7. $a \cdot (b \cdot c) = (a \cdot b) \cdot c, \forall\ a, b, c \in R.$
8. $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(a + b) \cdot c = a \cdot c + b \cdot c, \forall\ a, b, c \in R.$

$\exists$ means "there exists" and $\forall$ means "for all."
Frequently, we write ab instead of $a \cdot b$.

Definition

A ring is said to be commutative if $a \cdot b = b \cdot a$, for all $a, b \in R$. A ring is said to be a ring with identity if $\exists\ 1_R \in R$ such that $a \cdot 1_R = 1_R \cdot a$, for all $a \in R$.

Example

$\mathbb{Z}, \mathbb{Z}_n, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ are commutative rings with identity. The set

$$M_n(\mathbb{R}) = \{\text{all } n \times n \text{ matrices with entries in } \mathbb{R}\}$$

is ring with identity that is not commutative for any $n \geq 2$. Note that $\mathbb{N}$ (natural numbers) is not a ring.

Example

All continuous functions from $\mathbb{R}$ to $\mathbb{R}$ form a ring under the usual addition and multiplication of functions. The set of even integers with the usual addition and multiplication is a ring. However, the set of odd integers is not a ring.

Definition

An integral domain is a commutative ring with identity $1_R \neq 0_R$ such that

$$a \cdot b = 0_R \Longrightarrow a = 0_R \text{ or } b = 0_R.$$

The condition $1_R \neq 0_R$ is necessary to exclude $R = \{0_R\}$.

Example

$\mathbb{Z}$ is an integral domain. $\mathbb{Z}_n$ is an integral domain if and only if n is prime. $M_n(\mathbb{R}), n \geq 2$ is not an integral domain. The set of even integers is not an integral domain.

Definition

A field is a commutative ring with identity $1_R \neq 0_R$ such that for each $a \neq 0_R$, the equation $a \cdot x = 1_R$ has a solution in R.

Remark: Every field is an integral domain, but not conversely.

Example

$\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are fields. $\mathbb{Z}_n$ is a field if and only if n is prime. Under the usual addition and multiplication, $\mathbb{Z}$ is not a field.

Example

$$\left\{ \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \mid a, b \in \mathbb{R} \right\}$$

is a field under the usual addition and multiplication for matrices.

Other examples of rings:

Example

Let $i = \sqrt{-1}$. Then

$$\{a + bi \mid a, b \in \mathbb{Z}\}$$

is a ring under the usual addition and multiplication for complex numbers.

Example

The set

$$\{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$$

is a ring under the usual addition and multiplication for real numbers.

Example

In $\mathbb{Z}$, define

$$a \oplus b = a + b - 1 \text{ and } a \odot b = a + b - ab.$$

Under these new operations of addition and multiplication, $\mathbb{Z}$ is an integral domain.

Example

The set

$$S = \left\{ \begin{bmatrix} a & 0 \\ a & 0 \end{bmatrix} \mid a \in \mathbb{Z} \right\}$$

is a commutative ring under the usual addition and multiplication for matrices.

Example

Let S be a set and let $\mathscr{P}$ be the set of all subsets of S. Define:

$$M + N = (M - N) \cup (N - M) = (M \cup N) - (M \cap N)$$

and

$$M \cdot N = M \cap N.$$

Under these operations of addition and multiplication, $\mathscr{P}$ is a ring.

New Rings from Old Rings:

Recall that given two sets R and S, their Cartesian product is defined as

$$R \times S := \{(r, s) \mid r \in R \text{ and } s \in S\}.$$

Theorem

Let R and S be rings. Define $+$ and $\cdot$ on $R \times S$ by:

$$\begin{cases} (r,s) + (r',s') & = & (r + r', s + s') \\ (r,s) \cdot (r',s') & = & (r \cdot r', s \cdot s'). \end{cases}$$

where $r + r'$ and $r \cdot r'$ take place in R whereas $s + s'$ and $s \cdot s'$ take place in S. Then $R \times S$ is a ring.

Example

$\mathbb{Z} \times \mathbb{Z}$, $\mathbb{Z}_2 \times \mathbb{Z}$, $\mathbb{Z}_2 \times \mathbb{Z}_2$, $\mathbb{Z}_2 \times \mathbb{Z}_3$, $\mathbb{Z} \times \mathbb{Q}$ are all rings.

Definition

Let R be a ring and let $S \subset R$. If S is a ring under the addition and multiplication in R, then we say that S is a subring of R.

Example

$R = \mathbb{Z}_3,\ S = \{0, 1\}$ (not a subring)
$R = \mathbb{Z}_{10},\ S = \{0, 2, 4, 6, 8\}$.

A criterion for deciding whether a given subset S of R is a subring of R will be presented in the next section.