

# L1: Definitions and Examples of Rings

## Definition 1.1: Rings and Fields

A **ring**  $R$  is a set with two binary operations  $+$ ,  $\cdot$  (addition and multiplication), i.e

$$+ : R \times R \rightarrow R$$

$$\cdot : R \times R \rightarrow R$$

such that:

(i)  $(R, +)$  is an **abelian group**, i.e

- (Additive Identity) There exists a unique  $0_R \in R$ , such that  $\forall a \in R$

$$a + 0_R = 0_R + a = a$$

- (Additive Inverse)  $\forall a \in R$  there exists a unique  $(-a) \in R$  such that

$$a + (-a) = (-a) + a = 0_R$$

- (Associativity) For all  $a, b, c \in R$ ,  $(a + b) + c = a + (b + c)$

- (Commutativity) For all  $a, b \in R$ ,  $a + b = b + a$

(ii)  $\cdot$  is **associative**, i.e  $\forall a, b, c \in R$

$$(a \cdot b) \cdot c = a \cdot (b \cdot c)$$

(iii)  $\cdot$  is **distributive** over  $+$ , i.e  $\forall a, b, c \in R$

$$a \cdot (b + c) = a \cdot b + a \cdot c$$

Now we see variations and the extension of a ring, the field:

- We say  $R$  has an **identity element**,  $1_R$ , if there exists a  $1_R \in R$  such that  $\forall a \in R$

$$a \cdot 1_R = 1_R \cdot a = a$$

- We say  $R$  is **commutative** if  $\forall a, b \in R$

$$a \cdot b = b \cdot a$$

- If  $R$  is a commutative ring with  $1_R \neq 0_R$ , then we say  $R$  is a **field** if every non-zero element has a multiplicative inverse, i.e  $\forall a \neq 0 \in R, \exists a^{-1} \in R$  such that

$$a \cdot (a^{-1}) = (a^{-1}) \cdot a = 1_R$$

For the rest of the notes, I will omit the  $R$  subscript from the additive and multiplicative identity, unless necessary. Anyways, now we can look at some examples of rings:

**Example 1.1.**  $(\mathbb{Z}, +, \cdot)$ , The integers with the usual addition and multiplication is a ring.

**Example 1.2.**  $(\mathbb{R}, +, \cdot)$ ,  $(\mathbb{C}, +, \cdot)$ ,  $(\mathbb{Q}, +, \cdot)$  are fields.

**Example 1.3.**  $(\mathbb{N}, +, \cdot)$  is **not** a ring, since there are no additive inverses.

**Example 1.4.**  $(\mathbb{R}^3, +, \cdot)$  is **not** a ring. It has addition  $\mathbf{v}, \mathbf{w} \in \mathbb{R}^3 \Rightarrow \mathbf{v} + \mathbf{w} \in \mathbb{R}^3$ , but no proper multiplication operator. You can check that the cross product,  $\times$ , not distributive.

**Definition 1.2: Unit**

We say  $a \in R$  is a **unit** if there exists a  $b \in R$  such that  $a \cdot b = b \cdot a = 1$ .  
Basically, a unit is an element whose multiplicative inverse is also in the ring.

**Example 1.5.** In  $\mathbb{R}$ , every element except 0 is a unit.

**Example 1.6.** In  $\mathbb{Z}$ , the only units are  $\{1, -1\}$ .

Now let us look at examples of rings other than the standard number types  $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ :

**Example 1.7.** The integers modulo  $n$  are also a ring. This set is written as  $\mathbb{Z}/n\mathbb{Z}$ . To understand this, first define the set of multiples of an integer  $n$  as

$$n\mathbb{Z} := \{n \cdot a \mid a \in \mathbb{Z}\}$$

Then,

$$\mathbb{Z}/n\mathbb{Z} := \mathbb{Z}/\sim$$

where  $\sim$  is the equivalence relation for  $x, y \in \mathbb{Z}$

$$x \sim y \iff x - y \in n\mathbb{Z}$$

which basically means two integers are equivalent if their difference is a multiple of  $n$ . Think about it like this, if  $x$  and  $y$  are multiples of  $n$  plus the same remainder, i.e

$$x = nk + r \quad y = nl + r$$

for some  $k, l \in \mathbb{Z}$  then their difference is exactly a multiple of  $n$ ,

$$x - y = nk + r - (nl + r) = n(k - l) = nm$$

for  $m \in \mathbb{Z}$ . They are equivalent in the sense of producing the same remainder when  $n$  is divided by them. This can be written in modulo arithmetic as

$$x \equiv y \pmod{n}$$

So,  $\mathbb{Z}/n\mathbb{Z}$  will contain equivalence classes of remainders when dividing any integer by  $n$ , and each of these classes contain all integers that produce such remainder

$$\mathbb{Z}/n\mathbb{Z} := \{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{n-1}\}$$

The numbers with bars indicate the equivalence classes generated when taking the integers modulo  $n$ . For example  $\mathbb{Z}/3\mathbb{Z}$  are the integers modulo 3

$$\mathbb{Z}/3\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}\}$$

where

$$\bar{0} = \{0, 3, 6, 9, \dots\}$$

$$\bar{1} = \{1, 4, 7, 10, \dots\}$$

$$\bar{2} = \{2, 5, 8, 11, \dots\}$$

Now, if  $\bar{a}, \bar{b} \in \mathbb{Z}/n\mathbb{Z}$  and  $a \in \bar{a}, b \in \bar{b}$  then we define

$$\bar{a} + \bar{b} = \overline{a + b}, \quad \bar{a} \cdot \bar{b} = \overline{a \cdot b}$$

This set with the two operations is a ring. (Exercise to show these operations are well defined).

**Example 1.8.** We can also have a rings of functions. Let  $R$  be a ring and  $X$  a set, define the set  $\mathfrak{F}$

$$\mathcal{F} := \{f : X \rightarrow R\}$$

which is the set of functions which take elements of the set  $X$  to elements of the ring  $R$ . Then

$$\begin{aligned} (f + g) : X &\rightarrow R & (f \cdot g) : X &\rightarrow R \\ x &\mapsto f(x) + g(x) & x &\mapsto f(x) \cdot g(x) \end{aligned}$$

are operations which with  $\mathfrak{F}$ , form a ring.

**Example 1.9.** Define the set of continuous functions on the closed interval  $[0, 1]$

$$C[0, 1] := \{f : [0, 1] \rightarrow \mathbb{R} | f \text{ continuous}\}$$

We know from calculus that if  $f, g \in C[0, 1]$ , then  $f + g$  and  $f \cdot g$  are also in  $C[0, 1]$ . Hence,  $C[0, 1]$  is a ring.

**Example 1.10.** Sets of matrices can also be rings. Define

$$M_n(\mathbb{R}) := \{n \times n \text{ matrices with real coefficients}\}$$

Then for matrices  $A, B$ :

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix}, B = \begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1n} \\ b_{21} & b_{22} & \cdots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n1} & b_{n2} & \cdots & b_{nn} \end{pmatrix}$$

we have

$$\begin{aligned} A + B &:= \begin{pmatrix} a_{11} + b_{11} & a_{12} + b_{12} & \cdots & a_{1n} + b_{1n} \\ a_{21} + b_{21} & a_{22} + b_{22} & \cdots & a_{2n} + b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} + b_{n1} & a_{n2} + b_{n2} & \cdots & a_{nn} + b_{nn} \end{pmatrix} \\ A \cdot B &:= (a_{ik} \cdot b_{ki}) \end{aligned}$$

In the product, the notation indicates that each element is the dot product of a row vector in  $A$  and a column vector in  $B$  (the variable  $i$  indicates the  $i$ th row and  $i$ th column, while the  $k$  varies to multiply the  $k$ th element of each vector). This is the usual matrix multiplication we are all aware of.

Also, the additive and multiplicative identity are

$$0 = \begin{pmatrix} 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}, 1 = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}$$