

## Chapter 7 - Rings

# 7.1

Def:

① A ring  $R$  is a set together with binary operations  $+$  and  $\cdot$  (called addition and multiplication) satisfying the following axioms:

(i)  $R$  is an abelian group under  $+$

- $a+b \in R$  for all  $a, b \in R$ .
- $a+(b+c) = (a+b)+c$  for all  $a, b, c \in R$ .
- There exists an additive identity called  $0$ , such that  $0+a = a+0$  for all  $a \in R$ .
- For each  $a \in R$ , there exists  $-a \in R$  where  $a+(-a) = (-a)+a = 0$ .
- $a+b = b+a$  for all  $a, b \in R$ .

$-a$  is called the additive inverse of  $a$ .

(ii)  $R$  is closed under  $\cdot$ . That is,  $a \cdot b \in R$  for all  $a, b \in R$ .

(iii)  $\cdot$  is associative, that is  $a \cdot (b \cdot c) = (a \cdot b) \cdot c$  for all  $a, b, c \in R$ .

(iv) The distributive laws hold

That is,  $(a+b) \cdot c = a \cdot c + b \cdot c$   
 $a \cdot (b+c) = a \cdot b + a \cdot c$   
for all  $a, b, c \in R$ .

Notes: • We  
1  
• We



$a \cdot b \in R$  for all  $a, b \in R$ .

$c$

hold

$$a \cdot c + b \cdot c$$

$$a \cdot b + a \cdot c$$

② A ring  $R$  is called commutative if  $a \cdot b = b \cdot a$  for all  $a, b \in R$ .

③ A ring  $R$  is said to have an identity (or "contain a 1" or "contains unity") if there is an element  $1 \in R$  where  $a \cdot 1 = 1 \cdot a = a$  for all  $a \in R$ .

Notes:

- We will show later that  $1$  is unique if it exists.
- $1$  is sometimes called the multiplicative identity.
- We will just write  $ab$  instead of  $a \cdot b$ .

$-a$  is called the additive inverse of  $a$ .



Ex:  $\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \dots\}$

is a commutative ring with identity.

Ex:  $2\mathbb{Z} = \{0, \pm 2, \pm 4, \dots\}$

is a commutative ring.  
(without identity)

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

is a commutative ring with identity.

Def: A ring  $R$  with identity  $1$ , where  $1 \neq 0$ , is called a division ring (or skew field)

if every nonzero element  $a \in R$  has a multiplicative inverse, that is if for every  $a \in R$  there exists  $b \in R$  where  $ab = ba = 1$ .

We will show later that if such a  $b$  exists then its unique. So we will denote such a  $b$  by  $a^{-1}$ .



Def: A field is a commutative division ring.

Ex:  $\mathbb{Z}_p$  is a field if  $p$  is prime.

Ex:  $\mathbb{Q}, \mathbb{R}, \mathbb{C}$  are fields.

Ex:  $\mathbb{Z}$  is not a field nor a division ring. 2 has no mult. inverse for example.

Ex:  $M_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{R} \right\}$

is a non-commutative ring with identity  $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ . It's not a division ring.

Ex: The quaternions are a non-commutative division ring.

} For fun.



Prop: Let  $R$  be a ring.

Then:

①  $0a = a0 = 0$  for all  $a \in R$

②  $(-a)b = a(-b) = -(ab)$  for all  $a, b \in R$ .

③  $(-a)(-b) = ab$  for all  $a, b \in R$

④ If  $R$  has an identity  $1$ , then the identity is unique. Also, the multiplicative inverses are unique.

⑤  $-a = (-1)a$  for all  $a \in R$ .



Proof:

① Let  $a \in R$ . Then,  $a0 = a(0+0) = a0 + a0$ .

So,  $-a0 + a0 = -a0 + a0 + a0$ .

Thus,  $0 = a0$ .

Similarly,  $0a = 0$ .

② Let  $a, b \in R$ .

Then  $(-a)b + ab = (-a+a)b = 0b = 0$ .

So,  $(-a)b = -(ab)$ .

Similarly,  $a(-b) = -(ab)$ .

③ Let  
Then

$(-a)(-$

④ Sup  
identr

1, =

$1_2$   
ide

Suppose  
 $a_1 = b_1 a_2$   
 $b_2 =$



$$) = a0 + a0.$$

$$)b = 0.$$

③ Let  $a, b \in R$ .

Then

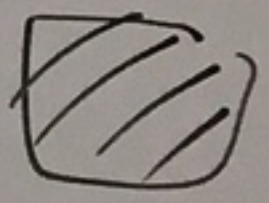
$$(-a)(-b) \stackrel{\textcircled{2}}{=} -(a)(-b) \stackrel{\textcircled{2}}{=} -(-a)(b) \stackrel{5401}{=} ab$$

④ Suppose  $1_1$  and  $1_2$  are both identities for  $R$ . Then,

$$1_1 = 1_1, 1_2 = 1_2$$

$1_2$  is identity

$1_1$  is an identity

⑤ Follows from 2. 

Suppose  $a \in R$  and  $b_1, b_2 \in R$  with  $ab_1 = b_1a = 1$  and  $ab_2 = b_2a = 1$ . Then

$$b_2 = b_2 \cdot \underline{1} = b_2 \underline{a b_1} = \underline{b_2 a} b_1 = \underline{1} b_1 = b_1.$$