

# الفصل الأول

# "Ring Theory"

## Contents

### Chapter One - Rings

Rings (Definition - Example and general properties of rings).

Direct sum of rings and some remarks.

Integral domain - Division ring - Field - Boolean rings - Center of a ring.

### Chapter Two - Subrings

Subrings (Definition - Characterization of subring - Examples).

Some operations on subrings - Subfields (Definition and examples).

### Chapter Three - Ideals

Ideals (Definitions and examples) - operations on ideals (addition of ideal, multiplication of ideals, intersection of ideal, union of ideal).

Finitely generated ideal - Principle ideal ring - Finitely generated ring - rings as direct sum of ideals.

### Chapter Four - Factor ring

Factor ring (definition and examples) - some relationships between a ring  $R$  and its factor ring.

## chapter five - Ring homomorphism

Ring homomorphism (definition and examples).  
- Kernel and image of ring homomorphism - some basic properties of ring homomorphism - Fundamental theorems of ring homomorphism - Embedding of ring and theorem of embedding.

## chapter six - Certain special types of ideals

Certain special types of ideals : maximal ideals, prime ideal, semiprime ideal, Primary ideal and radical of ideals (definitions and example and basic properties)

## chapter seven - (polynomial rings)

polynomial ring (definition and examples, some relationships between a ring  $R$  and polynomial ring over  $R$ ) - degree of polynomial with some theorems related with this concept - Division Algorithm - factor theorem - remainder theorem - irreducible polynomial - polynomial ring over field ( $F[x]$ , where  $F$  is a field) - the quotient of polynomial ring over field.

## Chapter eight - Extension of fields

---

Extension of fields (definitions) - some example  
to calculate extension field of certain field.

## Chapter nine - Modules

---

Modules - Submodules - Factor modules - homomorphism  
of Modules.

## References : المصادر

---

1. Introduction to abstract and linear algebra by  
David . M. Burton .

2- مقدمة في الجبر المجرد : تأليف  
د. ليلى سلمان محمود و  
د. محمد عبدالرزاق

3- ملزمة نظرية الحلقات : تأليف  
د. عادل عثمان دغوم و  
د. ياسر الهاشمي



## Definition

(Chapter one)

let  $R$  be a non-empty set and let  $+$ ,  $\cdot$  be two binary operations on  $R$ . Then  $(R, +, \cdot)$  is a ring if:

1.  $(R, +)$  is an abelian group, that is:

a.  $+$  is closed on  $R$

b.  $+$  is associative

c.  $\forall a \in R, \exists$  an element  $0 \in R$  s.t.  $a + 0 = a$ ,  
 $0$  is called the zero element.

d.  $\forall a \in R, \exists -a \in R$  s.t.  $a + (-a) = 0$ ,  $-a$  is called the additive inverse of  $a$ .

e.  $+$  is commutative.

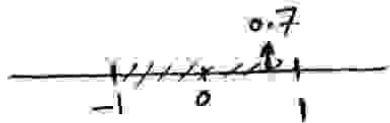
2.  $(a \cdot b) \cdot c = a \cdot (b \cdot c) \quad \forall a, b, c \in R$

3.  $a(b+c) = a \cdot b + a \cdot c \quad , \quad (b+c) \cdot a = b \cdot a + c \cdot a$   
 $\forall a, b, c \in R$ .

## Examples

1.  $(\mathbb{R}, +, \cdot)$ ,  $(\mathbb{Q}, +, \cdot)$ ,  $(\mathbb{Z}, +, \cdot)$ ,  $(\mathbb{C}, +, \cdot)$  are rings

2.  $((-1, 1), +, \cdot)$  is not ring, for example

$0.7 \in (-1, 1)$   , but  $0.7 + 0.7 = 1.4 \notin (-1, 1)$

3.  $(\mathbb{Z}_e, +, \cdot)$  be a ring, where  $\mathbb{Z}_e = \{x : x = 2k \text{ for some } k \in \mathbb{Z}\}$

4. let  $n$  be a fixed positive integer and  $n \neq 1$ .

## Definition

(chapter one)

let  $R$  be a non-empty set and let  $+, \cdot$  be two binary operations on  $R$ . Then  $(R, +, \cdot)$  is a ring if:

1.  $(R, +)$  is an abelian group, that is:

a.  $+$  is closed on  $R$

b.  $+$  is associative

c.  $\forall a \in R, \exists$  an element  $0 \in R$  s.t.  $a + 0 = a$ ,  $0$  is called the zero element.

d.  $\forall a \in R, \exists -a \in R$  s.t.  $a + (-a) = 0$ ,  $-a$  is called the additive inverse of  $a$ .

e.  $+$  is commutative.

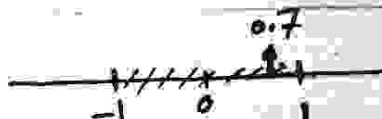
2.  $(a \cdot b) \cdot c = a \cdot (b \cdot c) \quad \forall a, b, c \in R$

3.  $a(b+c) = a \cdot b + a \cdot c \quad , \quad (b+c) \cdot a = b \cdot a + c \cdot a$   
 $\forall a, b, c \in R$ .

## Examples

1.  $(\mathbb{R}, +, \cdot), (\mathbb{Q}, +, \cdot), (\mathbb{Z}, +, \cdot), (\mathbb{C}, +, \cdot)$  are rings

2.  $((-1, 1), +, \cdot)$  is not ring, for example

$0.7 \in (-1, 1)$   , but  $0.7 + 0.7 = 1.4 \notin (-1, 1)$

3.  $(\mathbb{Z}_n, +, \cdot)$  be a ring, where  $\mathbb{Z}_n = \{x : x = 2k \text{ for some } k \in \mathbb{Z}\}$

4. let  $n$  be a fixed positive integer and  $n \neq 1$ .

Let  $A = \{x : x = nk \text{ for some } k \in \mathbb{Z}\}$ . Then  $(A, +, \cdot)$  is a ring. Show that (H.W.)

Definition:

Let  $R$  be a ring.  $R$  is said to be commutative ring, if  $a \cdot b = b \cdot a \quad \forall a, b \in R$ .

Definition:

Let  $R$  be a ring. Then  $\exists 1 \in R$  such that  $a \cdot 1 = 1 \cdot a = a \quad \forall a \in R$ .  $R$  is called a ring with identity (or unitary ring). Also, let  $a \in R$ . Then  $a$  is called invertible element, if  $\exists a^{-1} \in R$  st  $a \cdot a^{-1} = a^{-1} \cdot a = 1$ .

Examples:

1.  $(\mathbb{Z}, +, \cdot)$ ,  $(\mathbb{Q}, +, \cdot)$ ,  $(\mathbb{R}, +, \cdot)$ ,  $(\mathbb{C}, +, \cdot)$  are a commutative ring with identity.

2. Let  $R = M_n(\mathbb{R}) = \left\{ \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{bmatrix} : a_{ij} \in \mathbb{R} \right\}$   
 $\forall i, j = 1, \dots, n$

be the set of all matrices  $n \times n$  with usual addition and multiplicative for matrices. Then  $(R, +, \cdot)$  is a non-commutative ring with identity.

Since, let  $A = (a_{ij})_{n \times n}$  and  $B = (b_{ij})_{n \times n}$ . Then

1.  $A + B = (a_{ij} + b_{ij})_{n \times n} \in M_n(\mathbb{R})$  is comm. gp.

2.  $A \cdot B = \left( \sum_{k=1}^n a_{ik} b_{kj} \right)$ , Then • associative and

• distributive over +

$$I_n = \begin{pmatrix} 1 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix}_{n \times n} \in M_n(\mathbb{R})$$

Class

$$A \cdot I_n = I_n \cdot A = A$$

$$\forall A \in M_{n \times n}$$

$\therefore (M_{n \times n}, +, \cdot)$  is a ring with unity, but  $(M_{n \times n}, +, \cdot)$  is not Comm. in general.

3.  $(\mathbb{Z}, +, \cdot)$  is Comm. ring without identity

4. let  $X$  be a non-empty set. Then  $(P(X), \Delta, \cap)$  is a ring, where  $A \Delta B = (A \cup B) - (A \cap B)$   
 $= (A - B) \cup (B - A)$ .

This ring is Comm. with identity  $X$ . For example:

let  $X = \{1, 2\}$ . Then  $P(X) = \{\emptyset, \{1\}, \{2\}, X\}$

$\Delta$  is closed on  $P(X)$  and  $\cap$  is Comm. and associa.

$\emptyset$  = identity with respect to  $\Delta$  and every element in  $P(X)$  has inverse, also  $\Delta$  is associative, then  $(P(X), \Delta)$  is Comm. gp.

Now,  $\cap$  is asso. and  $\cap$  distributed over  $\Delta$ .

Therefore  $(P(X), \Delta, \cap)$  is a Comm. ring with identity

$X$ . { since,  $X \cap \{1\} = \{1\}$ ,  $X \cap \{2\} = \{2\}$ ,  $X \cap \emptyset = \emptyset$  and  $X \cap X = X$  }

5. let  $\mathbb{Z}[\sqrt{3}] = \{a + b\sqrt{3} : a, b \in \mathbb{Z}\}$ . Define  $+$  on  $\mathbb{Z}[\sqrt{3}]$  by

$$(a + b\sqrt{3}) + (c + d\sqrt{3}) = (a + c) + (b + d)\sqrt{3}$$

$$(a + b\sqrt{3}) \cdot (c + d\sqrt{3}) = (ac + 3bd) + (bc + ad)\sqrt{3}$$

Class

$$A \cdot I_n = I_n \cdot A = A$$

$$\forall A \in M_{n \times n}$$

$\therefore (M_{n \times n}, +, \cdot)$  is a ring with unity, but  $(M_{n \times n}, +, \cdot)$  is not Comm. in general.

3.  $(\mathbb{Z}, +, \cdot)$  is Comm. ring without identity

4. let  $X$  be a non-empty set. Then  $(P(X), \Delta, \cap)$  is a ring, where  $A \Delta B = (A \cup B) - (A \cap B)$   
 $= (A - B) \cup (B - A)$ .

This ring is Comm. with identity  $X$ . For example:

let  $X = \{1, 2\}$ . Then  $P(X) = \{\emptyset, \{1\}, \{2\}, X\}$   
 $\Delta$  is closed on  $P(X)$  and  $\cap$  is Comm. and associa.

$\emptyset$  = identity with respect to  $\Delta$  and every element in  $P(X)$  has inverse, also  $\cap$  is associative, then  $(P(X), \Delta)$  is Comm. gp.

Now,  $\cap$  is asso. and  $\cap$  distributed over  $\Delta$ .

Therefore  $(P(X), \Delta, \cap)$  is a Comm. ring with identity

$X$ . {since,  $X \cap \{1\} = \{1\}$ ,  $X \cap \{2\} = \{2\}$ ,  $X \cap \emptyset = \emptyset$   
 and  $X \cap X = X$ }

5. let  $\mathbb{Z}[\sqrt{3}] = \{a + b\sqrt{3} : a, b \in \mathbb{Z}\}$ . Define  $+$  on  $\mathbb{Z}[\sqrt{3}]$  by

$$(a + b\sqrt{3}) + (c + d\sqrt{3}) = (a + c) + (b + d)\sqrt{3}$$

$$(a + b\sqrt{3}) \cdot (c + d\sqrt{3}) = (ac + 3bd) + (bc + ad)\sqrt{3}$$

Then  $(\mathbb{Z}[\sqrt{3}], +, \cdot)$  be a Comm. ring with identity  $1 = 1 + 0\sqrt{3}$

6. let  $x \oplus y = x + y \quad \forall x, y \in \mathbb{Z}$  and  
 $x \odot y = 0 \quad \forall x, y \in \mathbb{Z}$

defined on  $\mathbb{Z}$ . Then  $(\mathbb{Z}, \oplus, \odot)$  is Comm. ring without unity.

Since,  $(\mathbb{Z}, \oplus)$  is Comm. gp.

① Now, To prove well-defined, if  $x = x_1$  and  $y = y_1$ , implies  $x \odot y = 0$  and  $x_1 \odot y_1 = 0$

Therefore  $x \odot y = x_1 \odot y_1$  and hence  $\odot$  well-defined

②.  $\forall x, y \in \mathbb{Z}, x \odot y = 0 \in \mathbb{Z}$   
 $\therefore \odot$  is closed on  $\mathbb{Z}$

③.  $x \odot y = y \odot x = 0$  which implies  $\odot$  is Comm.

④.  $\forall x, y, z \in \mathbb{Z}, x \odot (y \oplus z) = (x \odot y) \oplus (x \odot z) = 0 \oplus 0 = 0$   
 Thus  $\odot$  distributive over  $\oplus$ .

Thus  $(\mathbb{Z}, \oplus, \odot)$  is Comm. ring and  $\nexists b \in \mathbb{Z}$  s.t.  $a \odot b = a \quad \forall a \in \mathbb{Z}$  and  $a \neq 0$ . Hence the ring has no unity.

7. let  $C[0, 1] = \{f: [0, 1] \rightarrow \mathbb{R}\}$  which are continuous s.t.  $(f+g)_{(x)} = f(x) + g(x)$  and

$$(f \cdot g)_{(x)} = f(x) \cdot g(x)$$

Class

Then  $(\mathbb{C}[0,1], +, \cdot)$  is a Comm. ring with unity  $I(x)$  [identity function].

8. let  $\mathbb{Z}_n = \{\bar{0}, \bar{1}, \bar{2}, \dots, \bar{n-1}\}$ . Then  $(\mathbb{Z}_n, +_n, \cdot_n)$  is Comm. ring with identity 1.

special case:  $(\mathbb{Z}_4, +_4, \cdot_4)$  is Comm. ring with identity 1.

### Properties of Rings

let  $(R, +, \cdot)$  be a ring. Then for all  $a, b, c \in R$ .

1.  $a \cdot 0 = 0 = 0 \cdot a$
2.  $(-a) \cdot b = -(a \cdot b) = a \cdot (-b)$
3.  $-(-a) = a$
4.  $(-a) \cdot (-b) = a \cdot b$
5.  $-(a+b) = -a - b$
6.  $a \cdot (b+c) = a \cdot b + a \cdot c$
7.  $(a+b) \cdot c = a \cdot c + b \cdot c$
8. If  $R$  has unity 1, then
  - (i)  $(-1)a = -a$
  - (ii)  $(-1)(-1) = 1$

### Proofs

1. To prove  $a \cdot 0 = 0$ 

$$a \cdot 0 = a \cdot (0+0) = a \cdot 0 + a \cdot 0$$

$$a \cdot 0 - a \cdot 0 = a \cdot 0$$

$$0 = a \cdot 0$$

$$\begin{aligned} 4. \quad (-a)(-b) &= -(a(-b)) \quad \text{by (2)} \\ &= -(-ab) \quad \text{by (2)} \\ &= ab \quad \text{by (3)} \end{aligned}$$

$$\begin{aligned} 8. \quad (-1)a &= -(1.a) \quad \text{by (2)} \\ &= -a \end{aligned}$$

## Direct Sum of Rings and Some Remarks

الجمع المباشر للحلقات مع بعض الملاحظات

Definition:

Let  $(R, +, \cdot)$  and  $(R', +', \cdot')$  be any two rings.  
Let  $X = R \times R' = \{(a, b) : a \in R \wedge b \in R'\}$

Define  $\oplus, \otimes$  on  $X$  by:

$$(a, b) \oplus (c, d) = (a + c, b + d)$$

$$(a, b) \otimes (c, d) = (a \cdot c, b \cdot d)$$

Then  $(X, \oplus, \otimes)$  is a ring.

This ring is called the direct sum of  $R$  with  $R'$ .

From above example, we have the following remarks:

Remarks:

1. If  $(R, +, \cdot)$ ,  $(R', +', \cdot')$  are Comm. ring, then the ring of direct sum of  $R, R'$  is Comm. ring

2. If the ring  $(R, +, \cdot)$  has unity 1 and the ring  $(R', +', \cdot')$  has unity  $1'$ , then the ring  $R \times R'$  has

Class

unity  $(1, 1)$

3. If rings  $(R, +, \cdot)$  and  $(R', +', \cdot')$  have unities  $1, 1'$  and  $a \in R \wedge b \in R'$  such that  $a$  is an invertible in  $R \times R'$  and  $(a^{-1}, b^{-1}) = (a, b)^{-1}$ .

Example:

$$\text{let } \mathbb{Z}_2 \times \mathbb{Z}_3 = \{(\bar{0}, \bar{0}), (\bar{0}, \bar{1}), (\bar{0}, \bar{2}), (\bar{1}, \bar{0}), (\bar{1}, \bar{1}), (\bar{1}, \bar{2})\}$$

$$\text{and } (\bar{a}, \bar{b}) \oplus (\bar{c}, \bar{d}) = (\bar{a} + \bar{c}, \bar{b} + \bar{d})$$

$$(\bar{a}, \bar{b}) \otimes (\bar{c}, \bar{d}) = (\bar{a} \cdot_2 \bar{c}, \bar{b} \cdot_3 \bar{d})$$

Then  $(\mathbb{Z}_2 \times \mathbb{Z}_3, \oplus, \otimes)$  is a ring.

$\oplus$	$(\bar{0}, \bar{0})$	$(\bar{0}, \bar{1})$	$(\bar{0}, \bar{2})$	$(\bar{1}, \bar{0})$	$(\bar{1}, \bar{1})$	$(\bar{1}, \bar{2})$
$(\bar{0}, \bar{0})$	$(\bar{0}, \bar{0})$	$(\bar{0}, \bar{1})$	$(\bar{0}, \bar{2})$	$(\bar{1}, \bar{0})$	$(\bar{1}, \bar{1})$	$(\bar{1}, \bar{2})$
$(\bar{0}, \bar{1})$	$(\bar{0}, \bar{1})$	$(\bar{0}, \bar{2})$	$(\bar{0}, \bar{0})$	$(\bar{1}, \bar{1})$	$(\bar{1}, \bar{2})$	$(\bar{1}, \bar{0})$
$(\bar{0}, \bar{2})$	$(\bar{0}, \bar{2})$	$(\bar{0}, \bar{0})$	$(\bar{0}, \bar{1})$	$(\bar{1}, \bar{2})$	$(\bar{1}, \bar{0})$	$(\bar{1}, \bar{1})$
$(\bar{1}, \bar{0})$	$(\bar{1}, \bar{0})$	$(\bar{1}, \bar{1})$	$(\bar{1}, \bar{2})$	$(\bar{0}, \bar{0})$	$(\bar{0}, \bar{1})$	$(\bar{0}, \bar{2})$
$(\bar{1}, \bar{1})$	$(\bar{1}, \bar{1})$	$(\bar{1}, \bar{2})$	$(\bar{1}, \bar{0})$	$(\bar{0}, \bar{1})$	$(\bar{0}, \bar{2})$	$(\bar{0}, \bar{0})$
$(\bar{1}, \bar{2})$	$(\bar{1}, \bar{2})$	$(\bar{1}, \bar{0})$	$(\bar{1}, \bar{1})$	$(\bar{0}, \bar{2})$	$(\bar{0}, \bar{0})$	$(\bar{0}, \bar{1})$

النقائص الخمسة

$$-(\bar{0}, \bar{0}) = (\bar{0}, \bar{0})$$

$$-(\bar{0}, \bar{1}) = (\bar{0}, \bar{2})$$

$$-(\bar{1}, \bar{1}) = (\bar{1}, \bar{2})$$

$$-(\bar{0}, \bar{2}) = (\bar{0}, \bar{1})$$

$$-(\bar{1}, \bar{2}) = (\bar{1}, \bar{1})$$

$$-(\bar{1}, \bar{0}) = (\bar{1}, \bar{1})$$

Definition :- let  $(R, +, \cdot)$  be a ring and

$a, b \in R$ ,  $a \neq 0$ ,  $b \neq 0$ . If  $a \cdot b = 0$ , then  $a$  is called left zero divisor and  $b$  is called right zero divisor.

In Comm. ring, every left zero divisor is right zero divisor and conversely.

Examples :

1. In  $(\mathbb{Z}_3, +_3, \cdot_3)$ ,  $\bar{0}, \bar{1}, \bar{2}$  are not zero divisors.
2. In  $(\mathbb{Z}_4, +_4, \cdot_4)$ ,  $\bar{0}, \bar{1}, \bar{3}$  are not zero divisors, but  $\bar{2}$  is zero divisor, (since  $\bar{2} \cdot_4 \bar{2} = \bar{0}$ ).
3. In  $(\mathbb{Z}_6, +_6, \cdot_6)$ ,  $\bar{0}, \bar{1}, \bar{5}$  are not zero divisors. But  $\bar{2}, \bar{3}, \bar{4}$  are zero divisors.

Remark :- let  $(R, +, \cdot)$  be a Comm. ring with

unity 1. If  $a \in R$ ,  $a \neq 0$ ,  $a$  is an invertible element, then  $a$  is not zero divisor.

That is,  $a$  is invertible element  $\Rightarrow a$  is not zero divisor

Proof :- If  $a \in R$ ,  $a \neq 0$  and  $a$  is an invertible element.

$$\therefore \exists a^{-1} \in R \text{ s.t. } a^{-1} \cdot a = a \cdot a^{-1} = 1$$

Suppose  $a$  is a zero divisor.

Then  $\exists b \in R, b \neq 0$  s.t.  $a \cdot b = 0$

$$\bar{a} \cdot (a \cdot b) = \bar{a} \cdot 0 \Rightarrow (\bar{a} \cdot a) \cdot b = 0$$

$$\Rightarrow 1 \cdot b = 0 \Rightarrow b = 0 \text{ C! (since } b \neq 0 \text{).}$$

Thus  $a$  is not zero divisor.

والعلاقة العكسية  $a$  ان  
 $a$  is zero divisor  $\Rightarrow a$  is not invertible.

Now, we have the following example:

Example :

Consider the direct sum of  $(R, +, \cdot)$  with  $(R, +, \cdot)$

$$(a, 0) \oplus (0, b) = (0, 0) \quad \forall a \neq 0, \forall b \neq 0$$

Then all element of the form  $(a, 0), (0, b)$  where  $a \neq 0, b \neq 0$  are zero divisors.

Theorem :

let  $R$  be a comm. ring. Then  
 $R$  has no zero divisor  $\Leftrightarrow \forall a \in R, a \neq 0$ ,  
 $a \cdot b = a \cdot c$  which implies  $b = c$ .

proof:  $\Rightarrow$  If  $R$  has no zero divisor

let  $a \cdot b = a \cdot c$  and  $a \neq 0$

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

$$a \cdot b - a \cdot c = 0 \Rightarrow a(b - c) = 0$$

The Cancellation  
 law holds with  
 respect to  
 multiplication  
 operation

Q.E.D.

but  $a \neq 0$  and  $R$  has no zero divisor.

Then  $b - c = 0$  and hence  $b = c$ .

← Suppose  $R$  has zero divisor, so

$\exists a \neq 0, b \neq 0$  s.t.  $a \cdot b = 0$

let  $a \cdot 0 = 0$  (by properties of ring)

Then  $a \cdot b = a \cdot 0$  and hence  $b = 0$  C!

Therefore  $R$  has no zero divisor.

Theorem: let  $R$  be a comm. ring with unity 1

and  $R$  has no zero divisor. Then the equation  $a^2 = a$  has only two solutions  $a = 0$  or  $a = 1$ .

"Integral domain" (A.1.1)

Definition: let  $(R, +, \cdot)$  be a comm. ring with

unity 1. Then  $R$  is called an integral domain

↔  $R$  has no zero divisor.

Example: ① All rings  $(\mathbb{Z}, +, \cdot)$ ,  $(\mathbb{Q}, +, \cdot)$ ,  $(\mathbb{R}, +, \cdot)$ ,

$(\mathbb{C}, +, \cdot)$  have no zero divisors. Thus all these rings are integral domains.

②  $(\mathbb{Z}_3, +_3, \cdot_3)$ ,  $(\mathbb{Z}_5, +_5, \cdot_5)$  are integral domains

③  $(\mathbb{Z}_4, +_4, \cdot_4)$ ,  $(\mathbb{Z}_6, +_6, \cdot_6)$  are not integral domains

Class

Theorem:  $(\mathbb{Z}_n, +_n, \cdot_n)$  is an integral domain  $\Leftrightarrow$   $n$  is prime number.

Proof:  $\Rightarrow$  If  $(\mathbb{Z}_n, +_n, \cdot_n)$  is an integral domain

To prove  $n$  is a prime number  
suppose  $n$  is not prime number

$$\therefore \exists m, k \in \mathbb{Z}_+ \text{ s.t. } n = m \cdot k \quad 1 < m < n \quad 1 < k < n$$

$$\Rightarrow \bar{0} = \bar{m} \cdot \bar{k} \text{ and } \bar{m}, \bar{k} \text{ are no zero element.}$$

Then  $\bar{m}, \bar{k}$  are zero divisors in  $\mathbb{Z}_n$ .  
which is contradiction since  $\mathbb{Z}_n$  is an integral domain.  
Thus  $n$  is prime number.

$\Leftarrow$   $(\mathbb{Z}_n, +_n, \cdot_n)$  is Comm. ring with unity 1

To prove  $(\mathbb{Z}_n, +_n, \cdot_n)$  is an integral domain,  
we must prove that  $\mathbb{Z}_n$  has no zero divisor

suppose  $\mathbb{Z}_n$  has zero divisor

$$\exists \bar{m}, \bar{k} \in \mathbb{Z}_n \text{ s.t. } \bar{m} \neq \bar{0} \text{ and } \bar{k} \neq \bar{0}, \bar{m} \cdot \bar{k} = \bar{0}$$

$$\Rightarrow \bar{m} \cdot \bar{k} = \bar{n} \cdot \bar{r} \text{ for some } r \in \mathbb{Z}_+$$

$$\Rightarrow n \mid mk. \text{ Then } n \mid m \text{ or } n \mid k \text{ (since } n \text{ is prime)}$$

$$\text{If } n \mid m \Rightarrow m = \text{multiply of } n \Rightarrow \bar{m} = \bar{0} \text{ C!}$$

$$\text{If } n \mid k \Rightarrow k = \text{multiply of } n \Rightarrow \bar{k} = \bar{0} \text{ C!}$$

Thus  $\mathbb{Z}_n$  has no zero divisor.

Definition:

let  $(R, +, \cdot)$  be a Comm. ring with unity 1.  
Then  $(R, +, \cdot)$  is called field  $\Leftrightarrow \forall a \in R, a \neq 0, a$

Class

is an invertible.

Example:

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

2.  $(\mathbb{Z}, +, \cdot)$ ,  $(\mathbb{Z}_6, +, \cdot)$  is not a field.

3. direct sum of  $(\mathbb{R}, +, \cdot)$  with  $(\mathbb{R}, +, \cdot)$  is not a field.

Since all elements of the form  $(a, 0)$  and  $(0, b)$   $a \neq 0$ ,  $b \neq 0$  are not invertible elements.

problems:

1. let  $S = \mathbb{R} \times \mathbb{R}$ , Define  $\oplus$ ,  $\boxplus$

$$(a, b) \oplus (c, d) = (a+c, b+d)$$

$$(a, b) \boxplus (c, d) = (ac-bd, ad+bc)$$

Show that  $(S, \oplus, \boxplus)$  is field.

2. IS  $(\mathbb{Z}[\sqrt{3}], +, \cdot)$  field?

$$\text{let } x = 1+3\sqrt{3} \in \mathbb{Z}[\sqrt{3}]$$

$$\frac{1}{x} = \frac{1}{1+3\sqrt{3}} = \frac{1-3\sqrt{3}}{(1+3\sqrt{3})(1-3\sqrt{3})} = \frac{1-3\sqrt{3}}{-26} = \frac{-1}{26} + \frac{3}{26}\sqrt{3}$$

$$\notin \mathbb{Z}[\sqrt{3}]$$

$\therefore \mathbb{Z}[\sqrt{3}]$  is not field.

Theorem: Every field is an integral domain. But the Converse is not true in general for example

$(\mathbb{Z}, +, \cdot)$  is an integral domain but it is not field. Class

### Theorem

Every finite integral domain is a field.

### Proof :-

Let  $(R, +, \cdot)$  be a finite integral domain and let  $R = \{a_1, a_2, \dots, a_n\}$  a partition since,  $R$  is comm. ring with unity 1.

Let  $a_k$  be a non-zero element of  $R$ ;

$$S = \{a_k \cdot a_1, a_k \cdot a_2, \dots, a_k \cdot a_k, \dots, a_k \cdot a_n\} \subseteq R$$

Now, if  $a_k \cdot a_t = a_k \cdot a_s$ ,  $t \neq s$

$\Rightarrow a_t = a_s$  (Since  $R$  is an integral domain)

Then  $S$  has exactly  $n$  elements and hence

$S \subseteq R$ , also  $R$  has  $n$  elements. Then

$$S = R$$

$1 \in R \Rightarrow 1 \in S$ . Thus  $1 \in S \Rightarrow 1 = a_k \cdot a_r$

For some  $r$ ,  $1 \leq r \leq n$

$\Rightarrow a_k$  is an invertible element,  $a_k^{-1} = a_r$

Therefore  $R$  is field.

□

□

### Definition

A division ring is a ring with identity in which every non-zero element has invertible.

✓

### Remark

Every field is a division ring, but the converse is not true, in general. For example:

Let  $R = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a, b, c, d \in \mathbb{R} \right\}$  with usual addition and multiplication operations on matrices.

Then  $(R, +, \cdot)$  is a ring with identity  $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ .

Since, for example:

$$\begin{bmatrix} 0 & 2 \\ 1 & 3 \end{bmatrix} \cdot \begin{bmatrix} 1 & 3 \\ 2 & 1 \end{bmatrix} \neq \begin{bmatrix} 1 & 3 \\ 2 & 1 \end{bmatrix} \cdot \begin{bmatrix} 0 & 2 \\ 1 & 3 \end{bmatrix}$$

That is  $(R, +, \cdot)$  is not Comm. ring, but

every element in  $R$  has inverse

Therefore,  $R$  is division ring but not field.

### Definition

Let  $(F, +, \cdot)$  &  $(K, +, \cdot)$  be two fields s.t.  $F \subseteq K$ . Then  $F$  is called a subfield of  $K$ .

### Remark

Let  $(F, +, \cdot)$  be a field and let  $\emptyset \neq S \subseteq F$ . Then  $(S, +, \cdot)$  is a subfield of  $F \iff$

1.  $a \cdot b \in S \quad \forall a, b \in S$
2.  $a \cdot b^{-1} \in S \quad \forall a, b \in S$

### Example

$$\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$$

Then  $(\mathbb{Q}[\sqrt{2}], +, \cdot)$  is a subfield of  $\mathbb{R}$ .

let  $a+b\sqrt{2}, c+d\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$ . Then

$$1. (a+b\sqrt{2}) - (c+d\sqrt{2}) = (a-c) + (b-d)\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$$

$$2. (a+b\sqrt{2}) \cdot (c+d\sqrt{2})^{-1} = (a+b\sqrt{2}) \cdot \frac{1}{c+d\sqrt{2}}$$

$$= \frac{a+b\sqrt{2}}{c+d\sqrt{2}} = \frac{a+b\sqrt{2}}{c+d\sqrt{2}} \cdot \frac{c-d\sqrt{2}}{c-d\sqrt{2}}$$

$$= \frac{ac + ad\sqrt{2} + cb\sqrt{2} - 2bd}{c^2 - 2d^2} = \frac{(ac-2bd) + (ad+cb)\sqrt{2}}{c^2 - 2d^2}$$

$$= \underbrace{\frac{ac-2bd}{c^2-2d^2}}_{\in \mathbb{Q}} + \underbrace{\frac{ad+cb}{c^2-2d^2}}_{\in \mathbb{Q}} \sqrt{2} \in \mathbb{Q}[\sqrt{2}].$$

Remark :

let  $F$  be a field and let  $\{S_\alpha\}$  be any collection of subfield of  $F$ . Then  $\bigcap S_\alpha$  is a subfield of  $F$ .

Proof :

Since,  $0 \in S_\alpha \quad \forall \alpha \Rightarrow \bigcap S_\alpha \neq \emptyset$

let  $a, b \in \bigcap S_\alpha$

$\Rightarrow a, b \in S_\alpha \quad \forall \alpha$

But  $S_\alpha$  is a subfield of  $F \quad \forall \alpha$

$\therefore a-b \in S_\alpha, ab^{-1} \in S_\alpha \quad \forall \alpha$

-10-

$$a-b \in NS_{\alpha} \quad , \quad ab^{-1} \in NS_{\alpha}$$

$NS_{\alpha}$  is a subfield of  $F$ .



المرحلة الثالثة/قسم الرياضيات

المادة الحلقات

# الفصل الثاني

## Chapter Two

## Chapter two - Subrings

الكلمات المجزأة

### Definition

Let  $R$  be a ring, let  $\emptyset \neq S \subseteq R$ . Then  $S$  is called a subring of  $R \iff (S, +, \cdot)$  is a ring.

### Examples

1.  $(\mathbb{Z}, +, \cdot)$  is a subring of  $(\mathbb{R}, +, \cdot)$
2.  $(\mathbb{Z}, +, \cdot)$  is a subring of  $(\mathbb{Q}, +, \cdot)$
3.  $(\mathbb{Z}, +, \cdot)$  is a subring of  $(\mathbb{Z}, +, \cdot)$
4.  $(\mathbb{Z}[\sqrt{3}], +, \cdot)$  is a subring of  $(\mathbb{R}, +, \cdot)$
5.  $(A, +, \cdot)$  is a subring of  $(\mathbb{Z}, +, \cdot)$ , where  $A = \{nK, K \in \mathbb{Z}\}$ ,  $n$  is a fixed positive integer.

### Theorem

Let  $(R, +, \cdot)$  be a ring and let  $\emptyset \neq S \subseteq R$ . Then  $(S, +, \cdot)$  is a subring of  $(R, +, \cdot)$  iff

1.  $a - b \in S \quad \forall a, b \in S$
2.  $a \cdot b \in S \quad \forall a, b \in S$

### Proof :

$\implies$  It is clear that if  $(S, +, \cdot)$  is a subring of  $(R, +, \cdot)$ , then the two conditions hold

(Since,  $(S, +, \cdot)$  is subring of  $R \iff (S, +, \cdot)$  is a ring)

$\Leftarrow$  To prove  $S$  is a ring of  $R$ , we must prove that  $R$  holds all ring's conditions.

(11)

Since  $S \neq \emptyset$ , then  $\exists x \in S$

$$\underset{\substack{\downarrow \\ \text{zero ele.}}}{0} = x - x \in S \Rightarrow 0 \in S \quad \text{by Condition (1)}$$

$$\forall a \in S, 0 - a \in S \quad \text{by Condition (1)}$$

$$\Rightarrow -a \in S$$

$$\text{Now, } \forall a, b \in S, a + b = a - (-b) \in S$$

$+$  on  $S$  is Comm. (since  $S \subseteq R$  and  $+$  is Comm. on  $R$ )

$+$  on  $S$  is associative (since  $S \subseteq R$  and  $+$  asso. on  $R$ )

$\cdot$  is closed on  $S$  (is given Condition (2))

$\cdot$  is asso. on  $S$  ( $S \subseteq R$  and  $\cdot$  asso. on  $R$ )

$\cdot$  distr. over  $+$  on  $S$  ( $S \subseteq R$ ,  $\cdot$  distr. over  $+$  on  $R$ )

Thus  $(S, +, \cdot)$  is a ring.

Example

Consider  $(\mathbb{Z}_6, +_6, \cdot_6)$  ring.

Then all subrings of  $(\mathbb{Z}_6, +_6, \cdot_6)$  are:

1.  $(\mathbb{Z}_6, +_6, \cdot_6)$  is a subring of  $(\mathbb{Z}_6, +_6, \cdot_6)$

(2)  $(\{\bar{0}\}, +_6, \cdot_6)$  is a subring of  $(\mathbb{Z}_6, +_6, \cdot_6)$

(3)  $A = \{\bar{0}, \bar{2}, \bar{4}\}$

$+_6$	$\bar{0}$	$\bar{2}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{2}$	$\bar{4}$
$\bar{2}$	$\bar{2}$	$\bar{4}$	$\bar{0}$
$\bar{4}$	$\bar{4}$	$\bar{0}$	$\bar{2}$

$\cdot_6$	$\bar{0}$	$\bar{2}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{2}$	$\bar{0}$	$\bar{4}$	$\bar{2}$
$\bar{4}$	$\bar{0}$	$\bar{2}$	$\bar{4}$

$+_6$  closed on A

$\cdot_6$  closed on A

$+_6$  is Comm., associative on A

$\cdot_6$  associative on A

$$-\bar{2} = \bar{4} \in A$$

$$-\bar{4} = \bar{2} \in A$$

$\cdot_6$  dis. over  $+_6$  on A

Then A is a subring of  $\mathbb{Z}_6$

(4)  $B = \{\bar{0}, \bar{3}\}$ . To prove  $(B, +_6, \cdot_6)$  of  $(\mathbb{Z}_6, +_6, \cdot_6)$

$+_6$	$\bar{0}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{3}$
$\bar{3}$	$\bar{3}$	$\bar{0}$

$+_6$  closed on B

$+_6$  Comm.

$$\bar{0} \in B, -\bar{3} = \bar{3} \in B$$

$\cdot_6$  closed on B,

$\cdot_6$  associative

$\cdot_6$  dis. over  $+_6$  on B

Then B is a subring of  $\mathbb{Z}_6$ .

### Remark

Let  $(R, +, \cdot)$  be a ring. Then  $R$  has at least two subring  $\{0\}, R$ .

### Examples:

Consider the direct sum of  $(\mathbb{Z}, +, \cdot)$  with  $(\mathbb{Z}, +, \cdot)$

1. let  $A = \{(a, 0) : a \in \mathbb{Z}\}$ . Is  $A$  a subring of direct sum.

#### Solution

let  $(a_1, 0), (a_2, 0) \in A$

$$1. (a_1, 0) - (a_2, 0) = (a_1 - a_2, 0) \in A$$

$\underbrace{a_1 - a_2}_{\in \mathbb{Z}}$

$$2. (a_1, 0) \cdot (a_2, 0) = (a_1 a_2, 0) \in A$$

$\underbrace{a_1 a_2}_{\in \mathbb{Z}}$

$\therefore A$  is a subring of direct sum  $(\mathbb{Z} \times \mathbb{Z}, +, \cdot)$

2. let  $A = \{(a, 1) : a \in \mathbb{Z}\}$ . Is  $A$  a subring of direct sum.

#### Solution:

let  $(a_1, 1), (a_2, 1) \in A$

$$1. (a_1, 1) - (a_2, 1) = (a_1 - a_2, 0) \notin A$$

Therefore  $A$  is not subring of  $(\mathbb{Z}, +, \cdot)$

## Examples

Find all subrings of  $(\mathbb{Z}_{24}, +, \cdot)$  and  $(\mathbb{Z}_{30}, +, \cdot)$

①  $(\mathbb{Z}_{24}, +, \cdot)$

1.  $\mathbb{Z}_{24}$       2.  $\{0\}$       3.  $\{0, \bar{2}, \bar{4}, \bar{6}, \dots, \bar{22}\}$

4.  $\{0, \bar{4}, \bar{8}, \dots, \bar{20}\}$       5.  $\{0, \bar{3}, \bar{6}, \dots, \bar{21}\}$

6.  $\{0, \bar{6}, \bar{12}, \dots, \bar{18}\}$       7.  $\{0, \bar{8}, \bar{16}\}$       8.  $\{0, \bar{12}\}$

$(\mathbb{Z}_{30}, +, \cdot)$  H.W.

## Example :

Consider the ring  $(\mathbb{Z}[\sqrt{3}], +, \cdot)$ .

let  $A = \{a + b\sqrt{3} : a, b \in \mathbb{Z}\}$ . Is  $A$  a subring of  $\mathbb{Z}[\sqrt{3}]$ ? H.W.

## Solution

$$0 = 0 + 0\sqrt{3} \in A, \text{ so } A \neq \emptyset$$

$$\text{let } a_1 + b_1\sqrt{3} \text{ and } a_2 + b_2\sqrt{3} \in \mathbb{Z}[\sqrt{3}]$$

$$\text{Now, } (a_1 + b_1\sqrt{3}) - (a_2 + b_2\sqrt{3}) = \underbrace{(a_1 - a_2)}_{\in \mathbb{Z}} + \underbrace{(b_1 - b_2)}_{\in \mathbb{Z}}\sqrt{3} \in A$$

$$(a_1 + b_1\sqrt{3}) \cdot (a_2 + b_2\sqrt{3}) = a_1a_2 + a_1b_2\sqrt{3} + b_1a_2\sqrt{3} + 3b_1b_2$$

$$= (a_1a_2 + 3b_1b_2) + (a_1b_2 + b_1a_2)\sqrt{3} \in A$$

Therefore  $A$  is a subring of  $\mathbb{Z}[\sqrt{3}]$ .

## Remarks

Let  $R$  be a ring and  $S$  be a subring of  $R$ .

1. If  $R$  is Comm., then  $S$  is Comm.
2. If  $S$  is Comm., then it is not necessary that  $R$  is Comm. For example:  
 $(M_2(\mathbb{R}), +, \cdot)$  is not Comm. ring

Let  $A = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}, a, b \in \mathbb{R} \right\}$ . Then  $A$  is Comm. subring of  $(M_2(\mathbb{R}), +, \cdot)$ .

3. If  $R$  has unity, then it is not necessary that  $S$  has unity. For example:  $(\mathbb{Z}, +, \cdot)$  has unity 1, but the subring  $(2\mathbb{Z}, +, \cdot)$  of  $(\mathbb{Z}, +, \cdot)$  has no unity.

4. It may be that  $R, S$  have the same unity. For example:  $(\mathbb{R}, +, \cdot)$  has unity 1 and  $(\mathbb{Z}, +, \cdot)$  is a subring of  $(\mathbb{R}, +, \cdot)$  has unity 1.

5. It may be that  $R, S$  have distinct unities. For example: The ring  $(\mathbb{Z}_6, +, \cdot)$  has unity  $\bar{1}$ , but the subring  $(\{\bar{0}, \bar{2}, \bar{4}\}, +, \cdot)$  of  $(\mathbb{Z}_6, +, \cdot)$  has unity  $\bar{4}$  (since  $\bar{4} \cdot \bar{0} = \bar{0}$ ,  $\bar{4} \cdot \bar{2} = \bar{2}$ ,  $\bar{4} \cdot \bar{4} = \bar{4}$ ).

6. It may be that  $S$  has unity, but  $R$  has no unity.

7. If  $R$  is an integral domain, is  $S$  an integral domain? ☒
8. If  $S$  is an integral domain, is  $R$  an integral domain? ☐

⑧.  $\mathbb{Z}_6$  is not integral domain since  $\bar{2} \cdot \bar{3} = \bar{0}$

but  $S = \{\bar{0}, \bar{2}, \bar{4}\}$  has no zero divisor  $\Rightarrow$  integral domain

### Theorem

Let  $(R, +, \cdot)$  be a ring and let  $(A, +, \cdot), (B, +, \cdot)$  be two subrings of  $(R, +, \cdot)$ . Then  $(A \cap B, +, \cdot)$  is a subring.

### Proof

$0 \in A$  and  $0 \in B$  (since  $A, B$  are subrings of  $R$ )

$\Rightarrow 0 \in A \cap B$ , implies that  $A \cap B \neq \emptyset$ .

Let  $a, b \in A \cap B$ , implies  $a, b \in A$  and  $a, b \in B$ .

Thus  $a \in A$  and  $b \in A \Rightarrow a \cdot b \in A$  and  $a \cdot b \in A$  (since  $A$  is subring of  $R$ )  $\rightarrow$  ①

or  $a, b \in B \Rightarrow a \cdot b \in B$  and  $a \cdot b \in B$  (since  $B$  is a subring of  $R$ )  $\rightarrow$  ②

From ① and ②, we get  $a \cdot b \in A \cap B$  and  $a \cdot b \in A \cap B$ .  
Thus  $A \cap B$  is a subring of  $(R, +, \cdot)$ .

● As a generalization of above theorem, we have

The intersection of any family  $\{A_i\}$ ,  $\lambda$  is any index set of subring of a ring  $(R, +, \cdot)$  is a subring of  $(R, +, \cdot)$ .

### Remark

The union of two subrings of a ring  $(R, +, \cdot)$  need not be subring of  $R$ .

For example, Consider the ring  $(\mathbb{Z}, +, \cdot)$  and the subrings  $A = \{0, \pm 2, \pm 4, \dots\}$ ,  $B = \{0, \pm 3, \pm 6, \pm 9, \dots\}$   
 $A \cup B = \{0, \pm 2, \pm 3, \pm 4, \pm 6, \dots\}$

(14)

Since  $2 \in A \cup B$ ,  $3 \in A \cup B$  but  $3-2-1 \notin A \cup B$ .  
Thus  $A \cup B$  is not subring.

### Definition

Let  $(R, +, \cdot)$  be a ring, the set  $\{x : x \in R \wedge x \cdot y = y \cdot x \quad \forall y \in R\}$  is called the center of  $R$  and denoted by  $\text{Cent}(R)$ .

### Remarks :

(1) If  $R$  is Comm. ring, then  $\text{Cent}(R) = R$ .

(2)  $\text{Cent}(R)$  is a subring of  $(R, +, \cdot)$ .

### Proof

Let  $x_1, x_2 \in \text{Cent}(R)$

$$\begin{aligned} 1. & x_1 \cdot y = y \cdot x_1 & \forall y \in R & \rightarrow \textcircled{1} \\ 2. & x_2 \cdot y = y \cdot x_2 & \forall y \in R & \rightarrow \textcircled{2} \end{aligned}$$

Now,  $\forall y \in R$  by  $\textcircled{1}$  and  $\textcircled{2}$  we get  
 $(x_1 - x_2) \cdot y = x_1 \cdot y - x_2 \cdot y = y \cdot x_1 - y \cdot x_2 = y \cdot (x_1 - x_2)$

$$\Rightarrow x_1 - x_2 \in \text{Cent}(R)$$

Similarly  $x_1, x_2 \in \text{Cent}(R)$

$$(x_1 \cdot x_2) \cdot y = x_1 \cdot (x_2 \cdot y) = x_1 \cdot (y \cdot x_2) = (x_1 \cdot y) \cdot x_2$$

$$= (y \cdot x_1) \cdot x_2 = y \cdot (x_1 \cdot x_2)$$

$$\Rightarrow x_1 \cdot x_2 \in \text{Cent}(R)$$

$\therefore \text{Cent}(R)$  is a subring of  $(R, +, \cdot)$

### Definition :

Let  $(R, +, \cdot)$  be a ring and let  $a \in R, n \in \mathbb{Z}$ .

Then :

1.  $na = a + a + \dots + a$  (n-times)
2.  $(-n)a = (-a) + (-a) + \dots + (-a)$  (n-times)
3.  $a^n = a \cdot a \cdot \dots \cdot a$  (n-times)
4. If  $R$  has unity and  $a$  has multiplicative inverse  $a^{-1}$ , then  $a^{-n} = a^{-1} \cdot a^{-1} \cdot \dots \cdot a^{-1}$

### Example :

Consider the ring  $(\mathbb{Z}_8, +, \cdot)$

Find  $(2) \cdot \bar{3}$ ,  $(-2) \cdot \bar{3}$ ,  $7^{-2}$

### Solution :

$$1. (2) \bar{3} = \bar{3} + \bar{3} = \bar{6}$$

$$2. (-2) \cdot \bar{3} = (-\bar{3}) + (-\bar{3}) = \bar{5} + \bar{5} = \bar{2}$$

$$3. 7^{-2} = (\bar{7}^{-1})^2 = (\bar{7})^2 = \bar{7} \cdot \bar{7} = \bar{1}$$

### Theorem :

Let  $(R, +, \cdot)$  be a ring. Then for  $a, b \in R$  and arbitrary integers  $m$  and  $n$ , the following hold

1.  $(n+m)a = na + ma$
2.  $(nm)a = n(ma)$
3.  $n(a+b) = na + nb$
4.  $n(a \cdot b) = (na) \cdot b = a \cdot (nb)$
5.  $(na) \cdot (mb) = (nm) \cdot (a \cdot b)$

### Proof :- ①

Case (i)  $n \in \mathbb{Z}_+, m \in \mathbb{Z}_+$

Class

(15)

$$na + ma = (\underbrace{a + a + \dots + a}_{n \text{ times}}) + (\underbrace{a + a + \dots + a}_{m \text{ times}})$$

$$= \underbrace{a + a + a + \dots + a}_{(n+m) \text{ times}}$$

$$= (n+m)a$$

Case (ii):  $n \in \mathbb{Z}, m=0$

$$na + ma = na + 0 \cdot a = na = (n+0)a = (n+m)a$$

Case (iii):  $n \in \mathbb{Z}_-, m \in \mathbb{Z}_- \quad \underline{\underline{\text{H.W.}}}$

Case (IV):  $n \in \mathbb{Z}_+, m \in \mathbb{Z}_- \quad \underline{\underline{\text{H.W.}}}$

Definition: <sup>u.w.p</sup>

Let  $(R, +, \cdot)$  be a ring, if there exists a positive  $n$  s.t.  $na = 0 \quad \forall a \in R$ , then the least positive integer with this property is called characteristic of  $R$  (simply  $\text{ch}(R)$ ).

if no such positive integer exists, implies  $\text{ch}(R) = 0$ .

Examples:

1. Consider  $(\mathbb{Z}, +, \cdot)$

$$\forall a \in \mathbb{Z}, \text{ only } na = \overset{\text{u.l.b}}{0}, \text{ then } n = \overset{\text{u.l.b}}{0}$$

$$\therefore \text{ch}(\mathbb{Z}) = 0$$

2. Each ring  $(\mathbb{Q}, +, \cdot), (\mathbb{R}, +, \cdot), (\mathbb{C}, +, \cdot)$

has chara. Zero.

3. Consider  $(M_2(\mathbb{R}), +, \cdot)$

Class

let  $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{R})$

$$\forall n \in \mathbb{Z}_+, nA = \begin{pmatrix} na & nb \\ nc & nd \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

if  $A \neq O_{2 \times 2}$ , then  $\text{ch}(M_2(\mathbb{R})) = 0$

(4) Consider  $(\mathbb{Z}_3, +_3, \cdot_3)$

$$(3) \bar{1} = \bar{1} +_3 \bar{1} +_3 \bar{1} = \bar{0}$$

$$(3) \bar{2} = \bar{2} +_3 \bar{2} +_3 \bar{2} = \bar{0}$$

$$\therefore \text{ch}(\mathbb{Z}_3) = 3$$

(4) let  $X \neq \emptyset$ , Consider  $(P(X), \Delta, \cap)$

Zero element of this ring is  $\emptyset$

let  $A \in P(X)$

$$(1) A = A \Delta A = \emptyset$$

since  $A \Delta A = (A/A) \cup (A/A) = \emptyset \cup \emptyset = \emptyset = \text{Zero element}$

$$\therefore \text{ch}(P(X), \Delta, \cap) = 2$$

⊗ problem: Prove or disprove

Let  $R$  be a ring and let  $S$  be a subring of  $R$ .

Then:

$$1. \text{ch}(R) = \text{ch}(S)$$

$$2. \text{ch}(R) \neq \text{ch}(S)$$

$$\text{ch}(\mathbb{Z}_6) = 6$$

$$\text{but } A = \{\bar{0}, \bar{2}, \bar{4}\}$$

The identity element of  $A$  is  $\bar{4}$

$$\text{Then } \text{ch}(A) = 3$$

$$\text{Since, } \underset{6}{\bar{4}} + \underset{6}{\bar{4}} + \underset{6}{\bar{4}} = \bar{0}$$

(16)

### Theorem:

Let  $(R, +, \cdot)$  be a ring with unity 1. Then  $\text{ch}(R) = n, n \in \mathbb{Z}_+$   $\iff$   $n$  is the least positive integer s.t.  $n1 = 0 \rightarrow$  Zero element

### Proof:

$\implies$  If  $\text{ch}(R) = n, n \in \mathbb{Z}_+$

①  $\leftarrow n$  is the least positive integer s.t.  $na = 0 \forall a \in R$

$1 \in R \implies n1 = 0$  by ①

Suppose  $\exists m \in \mathbb{Z}_+$  and  $m < n$  and  $m1 = 0$  المرشح ان

$\forall a \in R, ma = m(1 \cdot a) = (m \cdot 1) \cdot a = 0 \cdot a = a$  أكثر عدد صحيح موجب

Since,  $ma = a \forall a \in R$  and  $m < n$  which Contradict the state ① ناقض الفرضية

Thus  $n$  is the least positive s.t.  $n1 = 0$

$\longleftarrow$  let  $a \in R, na = n(1 \cdot a) = (n \cdot 1) a = 0 \cdot a = 0$

$\therefore \text{ch}(R) \leq n$ , we must prove that  $n$  is the least positive integer

suppose  $\text{ch}(R) = m$  and  $m < n$  فإن  $\text{ch}(R) = n$  يتبع

$\implies m \cdot 1 = 0$  Cl. Therefore  $\text{ch}(R) = n$ .

### Corollary:

$\text{ch}(\mathbb{Z}_n, +_n, \cdot_n) = n, n > 1$

تطبق هنا على القسمة

where  $n1 = \underbrace{1 + 1 + 1 + \dots + 1}_n = 0$

### Theorem

let  $(R, +, \cdot)$  be an integral domain. Then  $\text{ch}(R)$  is either Zero or prime number.

### Proof

Suppose  $\text{ch}(R) = n$ ,  $(n \in \mathbb{Z}_+)$  and  $n$  is not prime. Thus  $n = mk$  for some  $m, k \in \mathbb{Z}_+$   
 $1 < m < n$ ,  $1 < k < n$

$\text{ch}(R) = n$  (since  $n$  is the least positive integer)  $\Rightarrow$   $n \cdot 1 = 0$   
 s.t.  $n \cdot 1 = 0$

$n \cdot 1 = 0 = \text{Zero element}$

$$(m \cdot k) (1 \cdot 1) = 0 \Rightarrow (m \cdot 1) (k \cdot 1) = 0$$

$\Rightarrow m \cdot 1 = 0$  or  $k \cdot 1 = 0$  (since  $R$  is an integral domain. i.e.  $R$  has no zero divisor)

Case ①  $m \cdot 1 = 0$ , but  $m < n \Rightarrow \text{C! with } \otimes$

Case ② if  $k \cdot 1 = 0$  C! with  $\otimes$  (since  $k < n$ )

$\therefore$  our assumption is false  $\Rightarrow \text{ch}(R) = 0$  or prime number.

كلية التربية للعلوم الصرفة / ابن الهيثم

قسم الرياضيات / المرحلة الثالثة

المادة / حلقات

# الفصل الثالث

## chapter three

## Chapter Three

## \*(IDEAL)\*

المثاليات  
ideals

Definition :-

let  $(R, +, \cdot)$  be a ring and  $S$  a subring of  $R$ .

1.  $S$  is called a right ideal of  $R \iff a \cdot r \in S$
2.  $S$  is called a left ideal of  $R \iff r \cdot a \in S$

$$\forall a \in S, \forall r \in R$$

3.  $S$  is called left and right ideal of  $R$  (or two sided ideal)  $\iff a \cdot r \in S$  and  $r \cdot a \in S$   
 $\forall a \in S, r \in R$ .

Remark :

gn commutative every left ideal is right ideal and conversely.

Example :

The subring  $(\mathbb{Z}_e, +, \cdot)$  is an ideal of  $(\mathbb{Z}, +, \cdot)$ .

Since, if  $a = 2n \in \mathbb{Z}_e$  and  $r \in \mathbb{Z}$ , then  
 $r \cdot a = a \cdot r = (2n) \cdot r = 2(nr) \in \mathbb{Z}_e$

Theorem :-

let  $(R, +, \cdot)$  be a ring, and let  $\emptyset \neq S \subseteq R$ . Then  $S$  is an ideal of  $R \iff$

$$1. a - b \in S \quad \forall a, b \in S$$

$$2. a \cdot r \in S \text{ and } r \cdot a \in S \quad \forall a \in S, r \in R$$

Class

Examples :

1. Consider  $(\mathbb{R}, +, \cdot)$ ,  $\emptyset \neq \mathbb{Z} \subseteq \mathbb{R}$

$$5 \in \mathbb{Z}, \frac{1}{3} \in \mathbb{R}, \text{ but } 5 \cdot \frac{1}{3} = \frac{5}{3} \notin \mathbb{Z}$$

$\therefore \mathbb{Z}$  is not an ideal of  $\mathbb{R}$ .

هذا المثال يوضح انه  
ليس كل subring  
يكون ideal

ideal  $\Rightarrow$  subring  
4

2.  $\emptyset \neq \mathbb{Q} \subseteq \mathbb{R}$ ,  $\frac{1}{2} \in \mathbb{Q}$ ,  $\sqrt{3} \in \mathbb{R}$ , but

$$\frac{\sqrt{3}}{2} \notin \mathbb{Q}. \text{ Then } \mathbb{Q} \text{ is not ideal in } \mathbb{R}.$$

3. Find all ideals of  $(\mathbb{Z}_6, +, \cdot)$

- a.  $(1) = \mathbb{Z}_6$       b.  $\{0\}$       c.  $\{0, 2, 4\}$       d.  $\{0, 3\}$

تقريب :  
جميع الكائنات الجزئية من الحلقة  $(\mathbb{Z}_n, +, \cdot)$  هي مثاليات  
اي بمعنى ليس كل subring هو ideal ففي  $(\mathbb{Z}_n, +, \cdot)$

Remark : let  $(R, +, \cdot)$  be a ring and  $R \neq \{0\}$ .  
Then  $R$  has at least two subrings which are  
 $\{0\}$ ,  $R$ .

Example :

Consider the ring  $(M_2(\mathbb{Z}), +, \cdot)$ .

let

$$1. S_1 = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} : a, b \in \mathbb{Z} \right\}$$

$$S_2 = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} : a, b \in \mathbb{Z} \right\}$$

$$S_3 = \left\{ \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} : a, b \in \mathbb{Z} \right\}$$

Class

- ① Is  $S_1$  left (right) ideal of  $M_2(\mathbb{Z})$ ?
- ② Is  $S_2$  left (right) ideal of  $M_2(\mathbb{Z})$ ?
- ③ Is  $S_3$  left (right) ideal of  $M_2(\mathbb{Z})$ ?

Solution :

①  $\emptyset \neq S_1 \subseteq M_2(\mathbb{Z})$

let

$$\begin{pmatrix} a_1 & 0 \\ 0 & b_1 \end{pmatrix}, \begin{pmatrix} a_2 & 0 \\ 0 & b_2 \end{pmatrix} \in S_1 \quad a_1, a_2, b_1, b_2 \in \mathbb{Z}$$

$$\begin{pmatrix} a_1 & 0 \\ 0 & b_1 \end{pmatrix} - \begin{pmatrix} a_2 & 0 \\ 0 & b_2 \end{pmatrix} = \begin{pmatrix} a_1 - a_2 & 0 \\ 0 & b_1 - b_2 \end{pmatrix} \in S_1$$

let  $\begin{pmatrix} x & y \\ z & w \end{pmatrix} \in M_2(\mathbb{Z})$

$$\begin{pmatrix} x & y \\ z & w \end{pmatrix} \cdot \begin{pmatrix} a_1 & 0 \\ 0 & b_1 \end{pmatrix} = \begin{pmatrix} xa_1 & yb_1 \\ za_1 & wb_1 \end{pmatrix} \notin S_1$$

$\therefore S_1$  is not left ideal.

To prove (right)

$$\begin{pmatrix} a_1 & 0 \\ 0 & b_1 \end{pmatrix} \begin{pmatrix} x & y \\ z & w \end{pmatrix} = \begin{pmatrix} a_1x & a_1y \\ b_1z & b_1w \end{pmatrix} \notin S_1$$

$\therefore S_1$  is not right ideal.

Example :

let  $R = (\mathbb{Z} \times \mathbb{Z}, \oplus, \odot)$

let :

$$S_1 = \{(a, 0) ; a \in \mathbb{Z}\}$$

$$S_2 = \{(a, b) ; a \in \mathbb{Z}, b \in \mathbb{Z}\}$$

$$S_3 = \{(a, b) ; a \in \mathbb{Z}, b \in \mathbb{Z}_e\}$$

$$S_4 = \{(a, b) ; a \in \mathbb{Z}_e \wedge b \in \mathbb{Z}_e\}$$

IS  $S_1, S_2, S_3, S_4$  an ideal of  $R$  ?

Solution : ③

$$\emptyset \neq S_2 \subseteq R$$

$$\text{let } (a_1, b_1), (a_2, b_2) \in S_2 \quad \text{s.t. } a_1, a_2 \in \mathbb{Z} \\ b_1, b_2 \in \mathbb{Z}_e$$

$$(a_1, b_1) - (a_2, b_2) = (a_1 - a_2, b_1 - b_2) \in S_2$$

$$\text{Since } a_1, a_2 \in \mathbb{Z} \Rightarrow a_1 - a_2 \in \mathbb{Z} \\ b_1, b_2 \in \mathbb{Z}_e \Rightarrow b_1 - b_2 \in \mathbb{Z}_e$$

$$\text{let } (x, y) \in R = \mathbb{Z} \times \mathbb{Z}$$

$$(x, y) \odot (a_1, b_1) = (xa_1, yb_1) \in S_2$$

$$\text{Since } x \in \mathbb{Z}, a_1 \in \mathbb{Z} \Rightarrow xa_1 \in \mathbb{Z}$$

$$y \in \mathbb{Z}, b_1 \in \mathbb{Z}_e \Rightarrow yb_1 \in \mathbb{Z}_e \quad \text{and } \odot \text{ is Comm.}$$

We have  $S_2$  is an ideal of  $R = \mathbb{Z} \times \mathbb{Z}$

Remarks :

1. let  $(R, +, \cdot)$  be a ring with unity 1,  $I$  be an

Class

(19)

ideal of  $R$ . If  $1 \in I$ , then  $I = R$

Proof:

$I \subseteq R$  (by def. of ideal)

$\forall r \in R \Rightarrow r = r \cdot 1$  ( $1$  is the identity of  $R$ )

but  $r \in R, 1 \in I \Rightarrow r \cdot 1 \in I$  ( $I$  is an ideal)

$\therefore r \in I$

$\therefore R \subseteq I$ . Thus  $R = I$

~~~~~

② Let  $R$  be a ring with unity  $1$  and  $I$  is an ideal of  $R$ ,  $a \in R$ . If  $a$  is an invertible element and  $a \in I$ , then  $I = R$ .

Proof:

let  $a \in I$  and  $a$  is an invertible element.

Then  $\exists a^{-1} \in R$  s.t.  $aa^{-1} = 1$

Therefore  $1 = \underset{a \in I}{a} \cdot \underset{a^{-1} \in R}{a^{-1}} \in I$  ( $I$  is an ideal of  $R$ )

$\therefore 1 \in I$

(by previous remark)

~~~~~

③ Any Field  $(F, +, \cdot)$  has only two ideals namely  $F$  and  $\{0\}$ .

Proof: let  $I$  be an ideal of  $R$  s.t.  $I \neq \{0\}$

$\therefore \exists a \in I \wedge a \neq 0$

$\therefore a$  is an invertible element (since  $F$  is field)

Thus  $I = F$  by previous remark.

~~~~~

Class

Theorem:

let  $(R, +, \cdot)$  be a ring and let  $I, J$  be two ideals of  $R$ . Then  $(IJ, +, \cdot)$  is an ideal of  $R$ .

Proof:  $\emptyset \neq IJ \subseteq R$  (since  $0 \in I, 0 \in J \Rightarrow 0 \in IJ$ )

let  $a, b \in IJ, r \in R$ .

$a, b \in IJ \Rightarrow a \in I \wedge a \in J, b \in I \wedge b \in J$

$\therefore a - b \in I \wedge a - b \in J$

$r \cdot a \in I \wedge r \cdot a \in J$  (since  $I$  is an ideal of  $R$ )

$r \cdot a \in J \wedge r \cdot a \in J$  (since  $J$  is an ideal of  $R$ )

Thus  $a - b \in IJ$  and  $r \cdot a \in IJ, r \cdot a \in IJ$

$\therefore IJ$  is an ideal of  $R$ .

Remark:

The union of two ideals of ring  $R$  is not necessary an ideal of  $R$ , for example:

$(\mathbb{Z}_6, +, \cdot), (\bar{2})$  and  $(\bar{3})$  are ideals of  $\mathbb{Z}_6$

But  $(\bar{2}) \cup (\bar{3}) = \{\bar{0}, \bar{2}, \bar{3}, \bar{4}\}$ .

since  $4 - 3 = 1 \notin (\bar{2}) \cup (\bar{3})$

Definition:

let  $R$  be a Comm. ring with unity and  $a \in R$ . let  $I = \{r \cdot a : r \in R\}$ . Then  $I$  is an ideal of  $R$  and this ideal is called a principle ideal generated by  $a$  and denoted by  $(a)$ ,  $\text{id}(a)$ ,  $\langle a \rangle$ .

(20)

proof:  $I \neq \emptyset$  Since,  $0 = 0 \cdot a \in I$

let  $x_1, x_2 \in I$ ;  $c \in R$

$$x_1 = r_1 a, \quad x_2 = r_2 a \quad \text{for some } r_1, r_2 \in R$$

$$x_1 - x_2 = r_1 a - r_2 a = (r_1 - r_2) a \in I$$

$$c x_1 = c \cdot (r_1 a) = (c r_1) \cdot a \in I$$

$\therefore I$  is an ideal of  $R$ .

Example:

① Consider the ring  $(\mathbb{Z}, +, \cdot)$

$$\text{id}(2) = \{x \cdot 2 : x \in \mathbb{Z}\} = \{0, \pm 2, \pm 4, \dots\}$$

$$\text{id}(-2) = \{x \cdot (-2) : x \in \mathbb{Z}\} = \{0, \pm 2, \pm 4, \dots\}$$

$$\text{id}(a) = \text{id}(-a) \quad \text{بصورة عامة}$$

↑  
النظير المجمع لـ  $a$

$$\text{id}(1) = \mathbb{Z}, \quad \text{id}(0) = \{0\}$$

② Consider the ring  $(\mathbb{Z}_6, +, \cdot)$

$$\text{id}(\bar{1}) = \{\bar{x} \cdot \bar{1} : \bar{x} \in \mathbb{Z}_6\} = \mathbb{Z}_6$$

$$\text{id}(\bar{0}) = \{\bar{0}\}$$

$$\text{id}(\bar{2}) = \{\bar{x} \cdot \bar{2} : \bar{x} \in \mathbb{Z}_6\}$$

$$= \{\bar{0} \cdot \bar{2}, \bar{1} \cdot \bar{2}, \bar{2} \cdot \bar{2}, \bar{3} \cdot \bar{2}, \bar{4} \cdot \bar{2}, \bar{5} \cdot \bar{2}\}$$

$$= \{\bar{0}, \bar{2}, \bar{4}, \bar{0}, \bar{2}, \bar{4}\} = \{\bar{0}, \bar{2}, \bar{4}\}$$

Class

$$\text{id}(\bar{3}) = \{\bar{0}, \bar{3}\}$$

$$\text{id}(\bar{4}) = \{\bar{0}, \bar{4}, \bar{2}\}$$

$$\text{id}(\bar{4}) = \text{id}(\bar{2})$$

(لأنه واحد نظير الآخر)

$$\text{id}(\bar{5}) = \{\bar{0}, \bar{5}, \bar{4}, \bar{3}, \bar{2}, \bar{1}\} = \mathbb{Z}_6$$

لأنه

$$\bar{5} \cdot \bar{5} = \bar{1} \in \text{id}(\bar{5})$$

$$\therefore \text{id}(\bar{5}) = \mathbb{Z}_6$$

Theorem :-

let  $R$  be a comm. ring with unity 1.

Then:-

$$1. \text{id}(1) = R \text{ and } \text{id}(0) = \{0\}$$

$$2. a \in \text{id}(a)$$

$$3. \text{id}(a) = \text{id}(-a)$$

$$4. \text{id}(a) = R \text{ if } a \text{ is an invertible.}$$

problems :-

$$1. \text{ Find all P.I. in } (\mathbb{Z}_5, +_5, \cdot_5)$$

$$2. \text{ Find all P.I. in } (\mathbb{Z}_{12}, +_{12}, \cdot_{12})$$

Definition : let  $R$  be a comm. ring with unity 1, and let  $a, b \in R$

$I = \{r_1 a + r_2 b : r_1, r_2 \in R\}$ . Then  $I$  is an ideal of  $R$  and this ideal is called the ideal generated by  $a$  and  $b$ , denoted by  $\text{id}(a, b)$ ,  $\langle a, b \rangle$ ,  $(a, b)$ .

Class

(21)

let  $R$  be a Comm. ring with unity 1

let  $a_1, a_2, a_3, \dots, a_n \in R$

تقسيم  
مكرر

let  $I = \left\{ \sum_{i=1}^n x_i a_i : x_i \in R \right\}$ . Then  $I$  is an ideal of  $R$ .

Example :

Consider the ring  $(\mathbb{Z}, +, \cdot)$ .

Find  $\text{id}(2, 3)$ ,  $\text{id}(2, 4, 6)$ ,  $\text{id}(3, 5)$

$$\text{id}(3, 5) = \{x_1 \cdot 3 + x_2 \cdot 5 : x_1, x_2 \in \mathbb{Z}\}$$

$$1 = 2 \cdot 3 + (-1) \cdot 5 \in \text{id}(3, 5) = \mathbb{Z} = \text{id}(1)$$

$$\therefore \text{id}(n, m) = \text{id}(d)$$

حيث  $d = \text{القاسم المشترك}$

وهذه في حالة  $\mathbb{Z}$  فقط

وذلك حسب خواصه الانقليدية والتوزيع

$$\left\{ \begin{array}{l} \text{let } a, b \in \mathbb{Z}, d = \gcd(a, b) \\ \Rightarrow d = r_1 a + r_2 b \quad \text{for some } r_1, r_2 \in \mathbb{Z} \end{array} \right\}$$

Example :

let  $R$  be the direct sum of  $(\mathbb{Z}, +, \cdot)$  with  $(\mathbb{Z}, +, \cdot)$ . Then Find :

$$1. \text{id}(1, 0) = \{(r, k) \odot (1, 0) : (r, k) \in R\}$$

$$= \{(x, 0) : x \in \mathbb{Z}\}$$

$$2. \text{id}((1, 1), (1, 1)) = R$$

Class

$$3. \text{id}((1,0), (0,1)) = \{(x_1, k_1), (x_2, k_2)\} @ ((1,0), (0,1))$$

$$\text{و } (x_1, k_1), (x_2, k_2) \in R \}$$

$$= \{(x_1, 0), (0, k_2) \mid x_1, k_2 \in \mathbb{Z}\} \\ \mathbb{Z} \times \{0\} \cup \{0\} \times \mathbb{Z}$$

Definition :-

let  $R$  be a comm. ring with unity 1.  
 $R$  is called a principle ideal ring (P.I.R.) iff every ideal of  $R$  is a p.I.

Example :-  $(\mathbb{Z}_8, +_8, \cdot_8)$  is a p.I.R.

Theorem :-  $(\mathbb{Z}, +, \cdot)$  is a P.I.R.

Proof :- let  $I$  be any ideal of  $\mathbb{Z}$

if  $I = \{0\}$ , then  $I = \text{id}(0)$  is a p.I.

if  $I \neq \{0\}$ , then  $\exists m \in I \wedge m \neq 0$

Since  $m \in I \Rightarrow -m \in I$

So,  $I$  contains positive integers

لذلك هي مجموعة كل الأعداد الطبيعية الموجبة الموجودة في  $I$

$\therefore S \subseteq \mathbb{Z}_+$ . But  $\mathbb{Z}_+$  is a w.o.s

مجموعة ترتيبية

$\therefore S$  has a least element say  $n$ .

$\therefore n$  is the least positive integer of  $I$ .

Class

we claim that  $I = \text{id}(n)$

let  $x \in \text{id}(n)$

$$x = r \cdot n \text{ where } r \in \mathbb{Z}$$

but  $n \in I \Rightarrow x = rn \in I$

$$\therefore \text{id}(n) \subseteq I \rightarrow \textcircled{1}$$

Now, let  $x \in I$

$$\therefore x, n \in \mathbb{Z} \Rightarrow \exists q, r \in \mathbb{Z} \text{ s.t.}$$

$$x = qn + r \quad 0 \leq r < n \quad (\text{قسم الممتدة})$$

$$\text{if } 0 < r < n, \quad r = x - \underbrace{qn}_{\in I} \in I$$

$\therefore x$  is a positive integer in  $I$  and  $r < n$  C!

$I$  كونه مجموعة جزئية من  $\mathbb{Z}$  و  $n \in I$

Thus  $r=0$  and so  $x = qn \in \text{id}(n)$

$$\therefore I \subseteq \text{id}(n) \rightarrow \textcircled{2}$$

From  $\textcircled{1}$  and  $\textcircled{2}$ , we get  $I = \text{id}(n)$ .

Theorem :-

Every field is a P.I.R.

Proof :- let  $(F, +, \cdot)$  be any field and  $F$  has only two ideals which are  $F, \{0\}$ . But  $F = \text{id}(1)$ ,  $\{0\} = \text{id}(0)$

$\therefore F$  is P.I.R

Class

# Some operations on ideals

Definition :

Let  $(R, +, \cdot)$  be a ring and  $I, J$  be two ideals of  $R$ .

Define  $I + J = \{x + y : x \in I \wedge y \in J\}$ . Then  $I + J$  is said to be the sum of  $I$  and  $J$ .

Remark :  $I + J$  is an ideal of a ring  $(R, +, \cdot)$ , where  $I, J$  are ideals of  $R$ .

Proof :-

Since  $I + J \subseteq R$  (by Def. of ideal)

and  $I + J \neq \emptyset$ , since  $0 = \underset{\in I}{0} + \underset{\in J}{0} \in I + J$

Now, let  $x_1 + y_1$  and  $x_2 + y_2 \in I + J$

s.t.  $x_1, x_2 \in I$  and  $y_1, y_2 \in J$

$$(x_1 + y_1) - (x_2 + y_2) = (x_1 - x_2) + (y_1 - y_2) \in I + J$$

Since,  $x_1, x_2 \in I \Rightarrow (x_1 - x_2) \in I$  (since,  $I, J$  are ideals of  $R$ )  
 $y_1, y_2 \in J \Rightarrow (y_1 - y_2) \in J$

let  $r \in R$ ,  $r \cdot (x_1 + y_1) = rx_1 + ry_1$

$x_1 \in I \rightarrow rx_1 \in I$  (since  $I \wedge J$  are ideals of  $R$ )  
 $y_1 \in I \rightarrow ry_1 \in I$

Similarly :  $(x_1 + y_1)r \in I + J$ .

Thus  $I + J$  is an ideal of  $R$ .

Class

(23)

Remark :

let  $(R, +, \cdot)$  be a comm. ring and  $a, b \in R$ .  
Then  $\text{id}(a, b) = \text{id}(a) + \text{id}(b)$

Examples :

1. In  $(\mathbb{Z}, +, \cdot)$

$$\circledast \text{id}(3) + \text{id}(4) = \text{id}(3, 4) = \text{id}(1) = \mathbb{Z}$$

$$\circledast \text{id}(2) + \text{id}(4) = \text{id}(2, 4) = \text{id}(2) = \mathbb{Z}_2$$

2. Consider  $(\mathbb{Z}_{12}, +_{12}, \cdot_{12})$  ring.

let  $I = \text{id}(\bar{2})$  ,  $J = \text{id}(\bar{3})$  ,  $K = \text{id}(\bar{4})$  ,

$L = \text{id}(\bar{6})$

$$\circledast K + L = \text{id}(\bar{4}) + \text{id}(\bar{6}) = \{\bar{0}, \bar{4}, \bar{8}\} + \{\bar{0}, \bar{6}\}$$

$$= \{ \underset{12}{\bar{0} + \bar{0}}, \underset{12}{\bar{0} + \bar{6}}, \underset{12}{\bar{4} + \bar{0}}, \underset{12}{\bar{4} + \bar{6}}, \underset{12}{\bar{8} + \bar{0}}, \underset{12}{\bar{8} + \bar{6}} \}$$

$$= \{\bar{0}, \bar{6}, \bar{4}, \bar{10}, \bar{8}, \bar{2}\} = \text{id}(\bar{2})$$

$$\circledast L + L = \text{id}(\bar{6}) + \text{id}(\bar{6}) = \{\bar{0}, \bar{6}\} + \{\bar{0}, \bar{6}\}$$

$$= \{\bar{0}, \bar{6}\}$$

عند جمع المثالي مع نفسه  
فإن الناتج المثالي نفسه

Now, Find  $J + L$  ,  $J + K$  ,  $I + L$  (H.W)

Class

Remark :

Let  $R$  be a ring,  $I$  be an ideal of  $R$ .  
Then  $I + I = I$ .

Proof :

It's clearly  $I \subseteq I + I$ .

To prove  $I + I \overset{?}{\subseteq} I$

For all  $x + y \in I + I$ ,  $x \in I \wedge y \in I$

$\therefore x + y \in I$  ( $I$  is an ideal of  $R$ ).

Thus  $I + I \subseteq I$  and hence  $I + I = I$ .

Definition :

Let  $(R, +, \cdot)$  be a ring,  $I, J$  be two ideals of  $R$ .

Let  $I \cdot J = \left\{ \sum_{\text{finite sum}} a_i b_i : a_i \in I, b_i \in J \right\}$ . Then

$I \cdot J$  is called the product of  $I$  and  $J$ .

Remark :

$IJ \subseteq I$  and  $IJ \subseteq J$

Proof :

T.P.  $IJ \overset{?}{\subseteq} I$

Let  $x \in IJ \Rightarrow x = \sum_{\text{finite sum}} a_i b_i$ ,  $a_i \in I, b_i \in J$   
 $\forall i$

$x = a_1 b_1 + a_2 b_2 + \dots + a_n b_n$  for some  $n \in \mathbb{Z}_+$

but  $a_i \in I \quad \forall i = 1, 2, \dots, n \Rightarrow a_i b_i \in I \quad \forall i$

Class

$\therefore x \in I$  (since  $+$  is closed on  $I$ )  $\Rightarrow IJ \subseteq I$

Similarly,  $IJ \subseteq J$ .

Example:

Consider  $(\mathbb{Z}_6, +, \cdot)$ . let  $I = \{\bar{0}, \bar{2}, \bar{4}\}$   
 $J = \{\bar{0}, \bar{3}\}$

Thus  $a_i \cdot b_i = 0 \quad \forall a_i \in I, b_i \in J$

$$\therefore I \cdot J = \{\bar{0}\}$$

Remark:

It is not necessary that  $I \cdot I = I$ .  
 For example:

Consider  $(\mathbb{Z}, +, \cdot)$   
 let  $I = \text{id}(2)$ ,  $J = \text{id}(3)$

$$I \cdot J = \left\{ \sum_{\text{finite sum}} a_i b_i : a_i \in \text{id}(2), b_i \in \text{id}(3) \right\}$$

$$\therefore \begin{aligned} a_i &= 2m_i & m_i &\in \mathbb{Z} \\ b_i &= 3n_i & n_i &\in \mathbb{Z} \end{aligned}$$

$$a_i \cdot b_i = (2m_i) \cdot (3n_i) = 6(m_i n_i) = 6c_i \quad \text{where } c_i = m_i n_i$$

$$\therefore \sum_{\text{finite sum}} a_i b_i = \text{multiple of } 6$$

$$\therefore IJ = \text{id}(6)$$

$$I \cdot I = \text{id}(4) \subsetneq I$$

كلية التربية للعلوم الصرفة/ابن الهيثم

قسم الرياضيات/المرحلة الثالثة

المادة /الحلقات

## الفصل الرابع والخامس

## Chapter Four And Five

# Chapter Four (Factor Rings) الحلقات الكسورية

عرب

## Quotient Rings

Let  $(R, +, \cdot)$  be a ring,  $(I, +, \cdot)$  be an ideal of  $R$ .

let  $(R, +)$  is a Comm. group.

$(I, +)$  is a subgroup of  $(R, +)$

$I \triangleleft R$ , since every subgp. of Comm. gp is normal.

$$R/I = \{a + I : a \in R\}$$

Define  $\oplus$  on  $R/I$  by :

$$(a + I) \oplus (b + I) = (a + b) + I \quad \forall a + I, b + I \in R/I$$

and define  $\odot$  on  $R/I$  by :

$$(a + I) \odot (b + I) = a \cdot b + I \quad \forall a + I, b + I \in R/I$$

Then  $(R/I, \oplus, \odot)$  is a ring.

Since  $\oplus, \odot$  are closed on  $R/I$  (by Def. of  $\oplus$  and  $\odot$ )

To prove  $\oplus$  is well-define

$$\begin{aligned} \text{let } a + I = a_1 + I &\text{ means } a + (-a_1) \in I \Rightarrow a - a_1 \in I \\ b + I = b_1 + I &\text{ means } b + (-b_1) \in I \Rightarrow b - b_1 \in I \end{aligned}$$

We must  $(a + I) \oplus (b + I) = (a_1 + I) \oplus (b_1 + I)$   
that is,  $(a + b) - (a_1 + b_1) \in I$

Now,  $(a+b) - (a_1+b_1) = a+b-a_1-b_1$

$$= \underbrace{(a-a_1)}_{\in I} + \underbrace{(b-b_1)}_{\in I} \in I$$

Thus  $\oplus$  is well-defined.

To prove  $\odot$  is well-defined

let  $a+I = a_1+I$  and  $b+I = b_1+I$

$$\Downarrow \quad \Downarrow$$

$$\Rightarrow a-a_1 \in I \quad \text{and} \quad b-b_1 \in I$$

We want to prove that  $(a+I) \odot (b+I) = (a_1+I) \odot (b_1+I)$   
That is,  $(a \cdot b) - (a_1 \cdot b_1) \in I$

$$\begin{aligned} a \cdot b - a_1 \cdot b_1 &= ab - ab + ab - a_1 b_1 \\ &= (a-a_1)b + a_1(b-b_1) \in I \end{aligned}$$

Since  $a-a_1 \in I \Rightarrow (a-a_1) \cdot b \in I$  ( $I$  is an ideal)  
 $b-b_1 \in I \Rightarrow a_1(b-b_1) \in I$

Thus  $\odot$  is well-defined

It is clear that  $(R/I, \oplus)$  is Comm. grp.

and  $\odot$  is associative, also  $\odot$  distributive over  $\oplus$

Therefore  $(R/I, \oplus, \odot)$  is a ring. This ring is called the quotient ring of  $R$  by  $I$ .

Remarks :

Let  $(R, +, \cdot)$  be a ring and  $I$  be an ideal of  $R$ . Then :

1. If  $R$  is Comm. ring, then  $R/I$  is Comm. ring

2.  $R/I$  is Comm.  $\iff a \cdot b - b \cdot a \in I \quad \forall a, b \in R$ .

3. If  $R$  has unity  $1$ , then  $R/I$  has unity  $1 + I$

(b) Find all maximal ideals of  $\mathbb{Z}_{10}$

Proofs : (b)  $\mathbb{Z}_{10} = \mathbb{Z}_{2} \times \mathbb{Z}_{5}$

1.  $\forall (a+I), (b+I) \in R/I$  is Comm. ring

$$\begin{aligned} (a+I) \odot (b+I) &= a \cdot b + I \quad (\text{by definition of } \odot) \\ &= b \cdot a + I \quad (\cdot \text{ Comm. operation}) \\ &= (b+I) \odot (a+I) \quad (\text{by def. of } \odot) \end{aligned}$$

$$2. R/I \text{ is Comm.} \xLeftrightarrow[\text{Def.}]{\text{by}} (a+I) \odot (b+I) = (b+I) \odot (a+I)$$

$$\iff ab + I = ba + I$$

$$\iff ab - ba \in I$$

3. It is clear from definition of identity of  $R$  and  $R/I$

Example :

Consider  $(\mathbb{Z}_4, +, \cdot)$  be a ring.

let  $I = \{\bar{0}, \bar{2}\}$

$$\mathbb{Z}_4 \setminus I = \{a+I : a \in \mathbb{Z}_4\}$$

$$\bar{0} + I = I$$

Class

(26)

$$\bar{1} + I = \{\bar{1}, \bar{3}\}$$

$$\bar{2} + I = I \quad \text{and} \quad \bar{3} + I = \bar{1} + (\bar{2} + I) = \bar{1} + I$$

$$\therefore \mathbb{Z}_4 \setminus I = \{\bar{0} + I, \bar{1} + I\}$$

| $\oplus$      | $\bar{0} + I$ | $\bar{1} + I$ |
|---------------|---------------|---------------|
| $\bar{0} + I$ | $\bar{0} + I$ | $\bar{1} + I$ |
| $\bar{1} + I$ | $\bar{1} + I$ | $\bar{0} + I$ |

↗ 1x18 CAPP

| $\odot$       | $\bar{0} + I$ | $\bar{1} + I$ |
|---------------|---------------|---------------|
| $\bar{0} + I$ | $\bar{0} + I$ | $\bar{0} + I$ |
| $\bar{1} + I$ | $\bar{0} + I$ | $\bar{1} + I$ |

↗ 1x18 CAPP

Notice

1.  $\mathbb{Z}_4$  has Zero divisor  $\bar{2}$ , but  $\mathbb{Z}_4 \setminus I$  has no Zero divisor.

2.  $\mathbb{Z}_4$  is not integral domain (not field), but  $\mathbb{Z}_4 \setminus I$  is a field (and so it is integral domain)

$$3. \text{ch}(\mathbb{Z}_4) = 4$$

$$4. \text{ch}(\mathbb{Z}_4 \setminus I) = 2 \quad (\text{since } (\bar{1} + I) \oplus (\bar{1} + I) = \bar{2} + I = \bar{0} + I)$$

Examples

$$1. \mathbb{Z}_n \setminus \{\bar{0}\} = \{\bar{0}\} \quad \forall n > 1$$

$$2. \mathbb{Z}_n \setminus \mathbb{Z}_n = \mathbb{Z}_n \quad \forall n > 1$$

3. Consider the ring  $(\mathbb{Z}, +, \cdot)$ ,  $I = \text{id}(4)$ .

$$\mathbb{Z} \setminus \text{id}(4) = \{a + \text{id}(4) : a \in \mathbb{Z}\}$$



$$0+I = I = \{0, 4, 8, \dots\}$$

$$1+I = \{\dots, -7, -3, 1, 5, 9, \dots\}$$

$$2+I = \{\dots, -6, -2, 2, 6, 10, \dots\}$$

$$3+I = \{\dots, -5, -1, 3, 7, 11, \dots\}$$

$$\Rightarrow \dots -8+I = -4+I = 0+I = 4+I = 8+I = \dots$$

$$5+I = 1+(4+I) = 1+I$$

$$6+I = (2+(4+I)) = 2+I$$

$$7+I = 3+(4+I) = 3+I$$

وهذا الشيء

$$-1+I = 3+(-4+I) = 3+I$$

$$-2+I = 2+(-4+I) = 2+I$$

وهذا الشيء

$$\therefore \forall a \in \mathbb{Z} \Rightarrow \exists k, r \in \mathbb{Z} \text{ s.t. } a = 4k + r$$

where  $0 \leq r < 4$

$$\therefore a+I = 4k+r+I = r+(4k+I) = r+I$$

$$\therefore \mathbb{Z} \setminus I = \{0+I, 1+I, 2+I, 3+I\} = \mathbb{Z}_4$$

$$\text{Therefore } (\mathbb{Z} \setminus I, \oplus, \odot) = (\mathbb{Z}_4, +_4, \cdot_4)$$

Notice that  $(\mathbb{Z}, +, \cdot)$  is an integral domain and  $\text{ch}(\mathbb{Z}) = 0$ , but  $(\mathbb{Z}_4, +_4, \cdot_4)$  is not integral

Class

27

domain,  $\text{ch}(\mathbb{Z}_4) = 4$ .

قسم لهذا المثال

Consider the ring  $(\mathbb{Z}, +, \cdot)$  and let  $I = \text{id}(n)$  where  $n$  is a fixed positive integer. Then

$$(\mathbb{Z} \setminus I, \oplus, \otimes) = (\mathbb{Z}_n, +_n, \cdot_n)$$

Problem: H.W

let  $(\mathbb{Z}_6, +, \cdot)$  be a ring and let  
 $I = \{\bar{0}, \bar{2}, \bar{4}\}$ ,  $J = \{\bar{0}, \bar{3}\}$ .

Then find all element of

1.  $\mathbb{Z}_6 \setminus I$

2.  $\mathbb{Z}_6 \setminus J$

3.  $\mathbb{Z}_6 \setminus I + J$

4.  $\mathbb{Z}_6 \setminus I \cdot J$

## Chapter Five - Ring homomorphism - المثلثات الكلي

Definition : let  $(R, +, \cdot)$  and  $(R', +', \cdot')$  be two ring.  
Mapping  $f: R \rightarrow R'$  is called ring homomorphism

$$\iff \begin{aligned} 1. & f(a+b) = f(a) + f(b) \quad \forall a, b \in R \\ 2. & f(a \cdot b) = f(a) \cdot f(b) \end{aligned}$$

Examples :

1. let  $(R, +, \cdot)$  and  $(R', +', \cdot')$  be two rings.  
 QP  $f: R \rightarrow R'$  s.t.  $f(x) = \bar{0} \quad \forall x \in R$  where  
 $\bar{0}$  = Zero element of  $R'$ .

Solution  $f(a+b) = \bar{0}$   
 $f(a) + f(b) = \bar{0} + \bar{0} = \bar{0}$   
 $f(a \cdot b) = \bar{0}, \quad f(a) \cdot f(b) = \bar{0} \cdot \bar{0} = \bar{0}$

2. let  $f: \mathbb{R} \rightarrow \mathbb{R}$  be a ring homo. s.t.  $f(x) = x$

3. let  $f: (\mathbb{Z}, +, \cdot) \rightarrow (\mathbb{Z}, +, \cdot)$  s.t.  $f(x) = 3x \quad \forall x \in \mathbb{Z}$   
 Qs  $f$  homo. ?

Solution :  $\forall a, b \in \mathbb{Z}$

$$f(a+b) = 3(a+b) = 3a + 3b = f(a) + f(b)$$

$$f(a \cdot b) = 3ab, \text{ but } f(a) \cdot f(b) = 3a \cdot 3b = 9ab$$

$\therefore f$  is not homo.

④ let  $f: (\mathbb{Z}[\sqrt{3}], +, \cdot) \rightarrow (\mathbb{Z}[\sqrt{2}], +, \cdot)$  s.t.

$$f(a + b\sqrt{3}) = a + b\sqrt{2} \quad \forall a, b \in \mathbb{Z}$$

Solution:

let  $a + b\sqrt{3}, c + d\sqrt{3} \in \mathbb{Z}[\sqrt{3}]$

$$f[(a + b\sqrt{3}) + (c + d\sqrt{3})] = f[(a + c) + (b + d)\sqrt{3}]$$

$$= (a + c) + (b + d)\sqrt{2} = (a + b\sqrt{2}) + (c + d\sqrt{2})$$

$$= f(a + b\sqrt{3}) + f(c + d\sqrt{3})$$

$$f[(a + b\sqrt{3})(c + d\sqrt{3})] = f[(ac + 3bd) + (bc + ad)\sqrt{3}]$$

$$= (ac + 3bd) + (bc + ad)\sqrt{2}$$

$$\text{But } f(a + b\sqrt{3}) \cdot f(c + d\sqrt{3}) = (a + b\sqrt{2}) \cdot (c + d\sqrt{2})$$

$$= (ac + 2bd) + (bc + ad)\sqrt{2}$$

$$\text{Since } f[(a + b\sqrt{3})(c + d\sqrt{3})] \neq f(a + b\sqrt{3}) \cdot f(c + d\sqrt{3})$$

$\therefore f$  is not homo.

Problems: ① which of the following mappings from  $(\mathbb{Z}, +, \cdot)$  into  $(\mathbb{Z}, +, \cdot)$  is homo.

- a.  $f(x) = x^2$
- b.  $f(x) = 2x + 1$
- c.  $f(x) = 2^x$
- d.  $f(x) = 1$



- ② let  $f: (\mathbb{C}, +, \cdot) \rightarrow (\mathbb{C}, +, \cdot)$  s.t.  
 $f(a+ib) = a-ib$  (where  $i^2 = -1$ ). Is  $f$  homo.

Theorem :

let  $f: (R, +, \cdot) \rightarrow (R', +, \cdot)$  be any homo. Then

- ①  $f(0) = \bar{0}$  where  $0$  = zero element of  $R$   
 $\bar{0}$  = zero element of  $R'$
- ②  $f(-a) = -f(a) \quad \forall a \in R$
- ③  $f(a-b) = f(a) - f(b) \quad \forall a, b \in R$
- ④ if  $S$  is a subring of  $R$ , then  $f(S)$  is a subring of  $R'$
- ⑤ if  $S'$  is a subring of  $R'$ , then  $f^{-1}(S')$  is a subring of  $R$ .
- ⑥ if  $I$  is an ideal of  $R$ ,  $f$  is onto, then  $f(I)$  is an ideal of  $R'$ .
- ⑦ if  $J$  is an ideal of  $R'$ , then  $f^{-1}(J)$  is an ideal of  $R$ .
- ⑧ if  $R$  has unity  $1$ , then  $f(1)$  is unity of  $f(R)$ .
- ⑨ if  $R$  has unity  $1$ ,  $f$  is onto, then  $f(1)$  is unity of  $R'$ .

Proofs : ①  $f(0) = f(0+0) = f(0) + f(0)$   
 $\therefore f(0) + 0 = f(0) + f(0)$   
 $\therefore f(0) = 0$

(29)

$$(2) \quad f(0) = 0 \Rightarrow f(a + (-a)) = 0$$

$$f(a) + f(-a) = 0 \xrightarrow[\text{لطرفين}]{\text{نضيف}}$$

$$f(-a) = -f(a)$$

$$(3) \quad f(a - b) = f(a + (-b)) = f(a) + f(-b)$$

$$= f(a) + (-f(b)) = f(a) - f(b)$$

(5)  $S$  is subring of  $R$ . Then  $0 \in S$

but  $f(0) = 0$  by (1)

$$f(0) \in S \Rightarrow 0 \in f(S)$$

$$\therefore f(S) \neq \emptyset \quad \text{Also } f(S) \subseteq R \quad \text{by def.}$$

$$\text{let } a, b \in f(S) \Rightarrow f(a) \in S \wedge f(b) \in S$$

$$f(a) - f(b) = f(a - b) \quad \text{by (3)}$$

$$\therefore f(a - b) \in S \Rightarrow a - b \in f(S)$$

$$\text{Also, } f(a) \cdot f(b) = f(a \cdot b) \in S$$

$$\Rightarrow a \cdot b \in f(S)$$

$$\therefore f(S) \text{ is a subring of } R.$$

(6)

$$0 = f(0) \in f(I) \quad \therefore f(I) \neq \emptyset$$

$$\text{Also, } f(I) \subseteq R \quad \text{by def.}$$

Class

let  $y_1, y_2 \in f(I)$  means  $\exists x_1, x_2 \in I$  s.t.

$$y_1 = f(x_1) \text{ and } y_2 = f(x_2)$$

$$\therefore y_1 - y_2 = f(x_1) - f(x_2) = f(x_1 - x_2)$$

but  $x_1 - x_2 \in I$ , since  $x_1, x_2 \in I$  and  $I$  is an ideal of  $R$ .

$$\therefore y_1 - y_2 = f(\underbrace{x_1 - x_2}_{\in I}) \in f(I)$$

Now,  $f: R \rightarrow R'$  onto,  $c \in R'$

$$\therefore \exists x \in R \text{ s.t. } c = f(x)$$

$$\therefore c \cdot y = f(x) \cdot f(x_1) = f(x \cdot x_1) \in f(I)$$

$\therefore f(I)$  is an ideal of  $R'$

Definition:

let  $f: (R, +, \cdot) \rightarrow (R', +, \cdot)$  be a ring homo. The set  $\{x: x \in R, f(x) = \bar{0}\}$  where  $\bar{0}$  is the zero element of  $R'$  is called the kernel of  $f$  and denoted by  $\text{Ker}(f)$ . Since  $\text{Ker } f = f^{-1}\{\bar{0}\}$

Remark:

$\text{Ker } f$  is an ideal of  $R$ .

Since  $\text{Ker } f = f^{-1}\{\bar{0}\}$  and  $\{\bar{0}\}$  is an ideal of  $R'$  then by Theorem of properties of homo number ⑦  $\text{Ker } f$  is an ideal of  $R$ .

30

Theorem: let  $f: (R, +, \cdot) \rightarrow (R', +, \cdot)$  be a ring homo. Then  $\text{Ker} f = \{0\} \iff f$  is (1-1).

Proof :-  $\implies$ ) Suppose that  $\text{Ker} f = \{0\}$

Now, let  $x, y \in R$  and  $f(x) = f(y) \implies f(x) - f(y) = 0$

$f(x-y) = 0$  (since  $f$  is homo.)  $\implies x-y \in \text{Ker} f = \{0\}$

$\therefore x-y = 0 \implies x = y$ . Therefore  $f$  is (1-1).

$\impliedby$ ) Suppose  $f$  is (1-1).

let  $x \in \text{Ker} f \implies f(x) = 0 \implies f(x) = f(0)$

$\implies x = 0 \implies \text{Ker} f = \{0\}$

Example :-

let  $f: R \rightarrow R$  be homo. and  $f(x, y) = (x, 0)$   
 $\forall (x, y) \in R$ , where  $R = (\mathbb{Z}, +, \cdot) \times (\mathbb{Z}, +, \cdot)$   
direct sum

Then find  $\text{Ker} f$ .  $f(x, y) = (x, 0)$

$\text{Ker} f = \{(x, y) : f(x, y) = (0, 0)\} = \{(x, y) : (x, 0) = (0, 0)\}$

$= \{(x, y) : x = 0\} = \{(0, y) : y \in \mathbb{Z}\}$

Definition :

let  $f: R \rightarrow R$  be a ring homo.

①  $f$  is called monomorphism  $\iff f$  is (1-1)

②  $f$  is called epimorphism  $\iff f$  is onto

Class

③  $f$  is called isomorphism  $\iff f$  is (1-1) and onto.

Definition: let  $(R, +, \cdot)$ ,  $(R', +', \cdot')$  be two rings

$R$  is called isomorphic to  $R'$  ( $R \cong R'$ )  $\iff \exists f: R \rightarrow R'$  s.t.  $f$  is an isomorphism.

Examples:

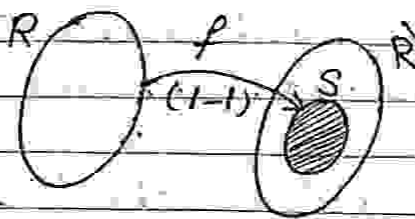
①  $(\mathbb{Z}_4, +_4, \cdot_4)$  is not isom. to  $(\mathbb{Z}_2, +_2, \cdot_2)$

Since  $\nexists f: \mathbb{Z}_4 \rightarrow \mathbb{Z}_2$  s.t.  $f$  is (1-1)

② if  $R$  has  $n$  element,  $R'$  has  $m$  element s.t.  $m \neq n$ , then  $R \not\cong R'$ .

Definition: (تعريف التضمين في الحلقات)

let  $(R, +, \cdot)$  and  $(R', +', \cdot')$  be two rings,  $R$  is said to be embedded in  $R'$  iff  $\exists (S, +', \cdot')$  subring of  $(R', +', \cdot')$  s.t.  $R \cong S$ .



Examples:

① Let  $R = \mathbb{Z} \times \mathbb{Z}$  be a ring. Then show that  $(\mathbb{Z}, +, \cdot)$  can be embedded in  $R$ .

Solution:

let  $S = \{(a, 0) : a \in \mathbb{Z}\}$ . Then  $S$  is

Class

a subring of  $R$ .

Define  $f: \mathbb{Z} \rightarrow S$  by  $f(a) = (a, 0)$   
 $\therefore f$  is an isomorphism

$\therefore \mathbb{Z}$  can be embedded in  $R$ .

(2)  $(\mathbb{Z}_2, +_2, \cdot_2)$  cannot be embedded in  $(\mathbb{Z}_3, +_3, \cdot_3)$

لأن  $\mathbb{Z}_2$  لا يوجد له Subring كـ  $\mathbb{Z}_3$  لأن  $\mathbb{Z}_3$  ليس  $\mathbb{Z}_2$  وحق  
 شرط أن تكون الـ  $\mathbb{Z}_2$  Isomorphism

Theorem:

let  $(R, +, \cdot)$  be a ring. Then there exists a ring  $R'$  with unity such that  $R$  is embedded in  $R'$ .

Proof:-

let  $R' = \{(a, n) : a \in R \wedge n \in \mathbb{Z}\} = R \times \mathbb{Z}$

Define  $+', \cdot'$  on  $R'$  by:

$$(a, n) + (b, m) = (a + b, n + m) \in R'$$

$$(a, n) \cdot (b, m) = (\underbrace{a \cdot b + nb + ma}_{\in R}, \underbrace{mn}_{\in \mathbb{Z}}) \in R'$$

$\therefore (R', +', \cdot')$  is a ring (check).

The unity of  $R'$  is  $(0, 1)$ , since

$$(a, n) + (0, 1) = (a + 0, n + 1) = (a, n + 1) \neq (a, n)$$

let  $S = \{(a, 0) : a \in R\} \subseteq R'$ . Then  $S$  is a subring of  $R'$  (check).

Define  $f: (R, +, \cdot) \rightarrow (S, +', \cdot')$  s.t.  $f(a) = (a, 0)$

$f$  is an isomorphism (check). which completes the proof.

### Definition:

let  $(R, +, \cdot)$  be a ring,  $I$  is an ideal of  $R$ , the map,  $f: (R, +, \cdot) \rightarrow (R/I, +, \cdot)$  s.t.  $f(x) = x + I$  is called the natural mapping (denoted by  $\text{nat}_I$ )  $\forall x \in R$ .  
 $\text{nat}_I$  is ring homo, onto.

Theorem: let  $f: (R, +, \cdot) \rightarrow (R', +, \cdot)$  be a ring homo, onto. If  $R$  is principle ideal ring, then  $R'$  is a P.I.R.

Proof:

let  $f: (R, +, \cdot) \rightarrow (R', +, \cdot)$  be a ring homo. onto, and let  $I'$  be any ideal of  $R'$ .

To prove that  $R'$  is a P.I.R, we must prove that  $I'$  is a principle ideal of  $R'$ .

$\because I'$  is an ideal of  $R' \Rightarrow f^{-1}(I')$  is an ideal of  $R$

let  $f^{-1}(I') = I$ . But  $R$  is P.I.R. then  $I$  is a P.I. means  $\exists a \in R$  s.t.  $I = \text{id}(a)$ .

we claim that  $I' = \text{id}(f(a))$

let  $y \in \text{id}(f(a)) \Rightarrow y = x' \cdot f(a)$  for some  $x' \in R'$

but  $f$  is onto,  $x' \in R'$ , so  $\exists x \in R$  s.t.  $x' = f(x)$

$\therefore y = f(x) \cdot f(a) = f(xa) \in f(I)$

$\therefore y \in f(I) \Rightarrow y \in I' \Rightarrow \text{id}(f(a)) \subseteq I'$

Now, To prove  $I' \subseteq \text{id}(f(a))$

let  $y \in I' \Rightarrow y \in f(I)$  since  $f^{-1}(I') = I$ ,  $f$  is onto

and  $I'$  ideal of  $R' \Rightarrow y = x' \cdot f(a) = f(xa)$

$\therefore y \in \text{id}(f(a))$ .

# The Fundamental theorems of ring homo.

(المبرهنات الأساسية للمشاكل الكلاسيكية)

Theorem(1): First Fund. theorem (المبرهن الأول)

Let  $f: R \rightarrow R'$  is an  $R$ -homo., then  $R/\text{Ker} f \cong \text{Im} f$

Proof: Define  $g: R/\text{Ker} f \rightarrow \text{Im} f$  s.t

$$g(x + \text{Ker} f) = f(x) \quad \forall x \in R$$

T.P.  $g$  is well-define?

Let  $x_1 + \text{Ker} f = x_2 + \text{Ker} f$  where  $x_1 + \text{Ker} f$  and  $x_2 + \text{Ker} f \in R/\text{Ker} f$

$$\Rightarrow x_1 - x_2 \in \text{Ker} f \Rightarrow f(x_1 - x_2) = 0$$

$$f(x_1) - f(x_2) = 0 \Rightarrow f(x_1) = f(x_2) \Rightarrow g(x_1 + \text{Ker} f) = g(x_2 + \text{Ker} f)$$

=  $g$  is well-define

T.P.  $g$  is homo.?

Let  $x_1 + \text{Ker} f, x_2 + \text{Ker} f \in R/\text{Ker} f$

$$\textcircled{1} g[(x_1 + \text{Ker} f) \oplus (x_2 + \text{Ker} f)] = g[(x_1 + x_2) + \text{Ker} f]$$

$$= f(x_1) \oplus f(x_2) = g(x_1 + \text{Ker} f) \oplus g(x_2 + \text{Ker} f)$$

$$\textcircled{2} x_1 + \text{Ker} f, x_2 + \text{Ker} f \in R/\text{Ker} f$$

$$g[(x_1 + \text{Ker} f) \otimes (x_2 + \text{Ker} f)] = g(x_1 x_2 + \text{Ker} f) = f(x_1 x_2)$$

$$= f(x_1) \otimes f(x_2) = g(x_1 + \text{Ker} f) \otimes g(x_2 + \text{Ker} f)$$

class

$f$  is homo.

T.P.  $g$  is (1-1) ?

عكس برهان well define من اجل ان اعد

$$\text{let } g(x_1 + \ker f) = g(x_2 + \ker f)$$

$$\Rightarrow f(x_1) = f(x_2) \Rightarrow f(x_1) - f(x_2) = 0 \Rightarrow f(x_1 - x_2) = 0$$

$$\Rightarrow x_1 - x_2 \in \ker f \Rightarrow x_1 + \ker f = x_2 + \ker f$$

T.P.  $g$  is onto ?

let  $y$  be any element of  $\text{Im } f$

$$\exists x \in R \text{ s.t. } f(x) = y$$

$$\Rightarrow g(x + \ker f) = y \quad \therefore g \text{ is onto.}$$

Corollary :- If  $f: R \rightarrow R'$  is an epimorphism,  
then  $R/\ker f \cong R'$

Theorem (2) : Second Fun. Theorem (القول الثاني)

If  $K$  and  $L$  are two ideals of a ring  $R$ , then

$$K/L \cong K+L/L$$

Proof : Define  $f: K \rightarrow (K+L)/L$  s.t.  
 $f(x) = x+L \quad \forall x \in K$

$$\forall x \in K \Rightarrow x+0 \in K+L \Rightarrow x+L \in K+L/L$$

T.P.  $f$  is well define

$$\text{if } x_1 = x_2 \Rightarrow x_1 + L = x_2 + L \Rightarrow f(x_1) = f(x_2)$$

$\therefore f$  is well define.

T.P.  $f$  is homo?

let  $x_1, x_2 \in K$

$$f(x_1 + x_2) = (x_1 + x_2) + L = (x_1 + L) + (x_2 + L) = f(x_1) + f(x_2)$$

$$f(x_1 x_2) = x_1 x_2 + L = (x_1 + L) \odot (x_2 + L) = f(x_1) \cdot f(x_2)$$

T.P.  $f$  is onto?

let  $(x+y) + L \in (K+L)/L$  where  $x \in K$  &  $y \in L$

$$(x+y) + L = (x+L) + (y+L) = (x+L) + L = x+L = f(x)$$

By Theorem (1)  $K/\ker f \cong (K+L)/L$

T.P.  $\ker f = L \cap K$

$$\ker f = \{x \in K : f(x) = 0\} = \{x \in K : x+L = L\}$$

$$= \{x \in K \wedge x \in L\} = K \cap L$$

Therefore  $K/L \cap K \cong K+L/L$

Theorem (3) Third theorem (Third Isomorphism)

Let  $K$  and  $L$  two ideals of a ring  $R$  and  $K \subseteq L$ , then  $R/K / L/K \cong R/L$ .

Proof: Define  $f: R/K \rightarrow R/L$  st.  $f(x+K) = x+L$   
 $\forall x \in R$ .

T.P.  $f$  is well-define?

$$\forall x+K \in R/K \Rightarrow x+L \in R/L \Rightarrow f(x+K) \in R/L$$

$$\text{q.p. } x_1 + K = x_2 + K \Rightarrow x_1 - x_2 \in K \Rightarrow x_1 - x_2 \in L$$

$$\Rightarrow x_1 + L = x_2 + L \Rightarrow f(x_1 + K) = f(x_2 + K)$$

(34)

T.p.  $f$  is homo?

$$\forall x_1 + K, x_2 + K \in R/K$$

$$\textcircled{1} f[(x_1 + K) \oplus (x_2 + K)] = f[(x_1 + x_2) + K]$$

$$= (x_1 + x_2) + L = (x_1 + L) + (x_2 + L) = f(x_1 + K) + f(x_2 + K)$$

$$\textcircled{2} f[(x_1 + K) \odot (x_2 + K)] = f[(x_1 x_2) + K]$$

$$= x_1 x_2 + L = (x_1 + L) \odot (x_2 + L) = f(x_1 + K) \odot f(x_2 + K)$$

T.p.  $f$  is onto?

$$\text{Im } f = \{f(x + K) : x \in R\} = \{x + L : x \in R\} = R/L$$

∴  $f$  is onto.

$$\text{By theorem (1)} \Rightarrow R/K / \ker f \cong R/L$$

T.p.  $\ker f = L/K$ 

$$\ker f = \{x + K \in R/K : f(x + K) = L\}$$

$$= \{(x + K) \in R/K : x + L = L\}$$

$$= \{x + K \in R/K : x \in L\} = L/K$$

$$\therefore R/K / L/K \cong R/L$$

كلية التربية للعلوم الصرفة/ابن الهيثم

قسم الرياضيات/المرحلة الثالثة

المادة/حلقات

# الفصل السادس

## Chapter Six

# Chapter Six

# 6

## Certain special types of ideals

انواع خاصة من المثاليات

In this chapter we study a special types of ideals : maximal ideal, prime ideal, semiprime ideal and primary ideals many properties and characterizations of these concepts are given, also some results are discussed about these concepts and also we study the concept of Boolean rings.

### Maximal ideals المثاليات العظمى

Definition :

An ideal  $M$  of a ring  $R$  is called maximal ideal if the following conditions hold:

- ①  $M \neq R$
- ② If  $\exists$  ideal  $J$  in  $R$  s.t.  $M \subsetneq J$ , then  $J = R$ .

Class

Example: Consider the ring  $(\mathbb{Z}_{12}, +_{12}, \cdot_{12})$ .

$\mathbb{Z}_{12}$  is not max. ideal

$\{0\}$  is not max. ideal, since  $\exists$  ideal  $J = \{\bar{0}, \bar{6}\}$  s.t.

$$\{0\} \subsetneq \{\bar{0}, \bar{6}\} \subsetneq \mathbb{Z}_{12}$$

$M_1 = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}, \bar{10}\}$  is max. ideal

$M_1$  لا يوجد مثالي في  $\mathbb{Z}_{12}$  يحتويه

$M_2 = \{\bar{0}, \bar{3}, \bar{6}, \bar{9}\}$  is max. ideal

$M_3 = \{\bar{0}, \bar{4}, \bar{8}\}$  is not max. ideal.

Since  $\exists M_1$  s.t.  $M_3 \subsetneq M_1 \subsetneq \mathbb{Z}_{12}$

$M_4 = \{\bar{0}, \bar{6}\}$  is not max. ideal, since  $\exists M_1, M_2$  ideals of  $\mathbb{Z}_{12}$

s.t.  $M_4 \subsetneq M_1 \subsetneq \mathbb{Z}_{12}$  and  $M_4 \subsetneq M_2 \subsetneq \mathbb{Z}_{12}$ .

problems:

① Find all maximal ideals of  $(\mathbb{Z}_8, +_8, \cdot_8)$ .

② Find all maximal ideals of  $(\mathbb{Z}_{15}, +_{15}, \cdot_{15})$ .

Theorem 8: In the ring  $\mathbb{Z}$ , the  $\text{id}(n)$ ,  $(n \in \mathbb{Z}, n \neq 1)$  is maximal ideal  $\iff n$  is prime number.

proof:  $\implies$  let  $I = \text{id}(n)$  is max. ideal.

(36)

To prove,  $n$  is prime number.

Suppose  $n$  is not prime number. Then  $\exists m, k \in \mathbb{Z}_+$

s.t.  $1 < m < n$ ,  $1 < k < n$  and  $n = mk$

$\therefore \text{id}(n) \subsetneq \text{id}(m) \subsetneq \mathbb{Z}$  and  $\text{id}(n) \subsetneq \text{id}(k) \subsetneq \mathbb{Z}$

which is contradiction with definition of max ideal

$\iff$  If  $n$  is prime number, to prove  $I = \text{id}(n)$  is max. ideal

suppose  $I = \text{id}(n)$  is not max. Then  $\exists$  ideal  $J$  of  $\mathbb{Z}$  s.t.

$I \subsetneq J \subsetneq \mathbb{Z}$ . But  $\mathbb{Z}$  is p.i.r. Then  $\exists m \in \mathbb{Z}_+$ ,  $m \neq 1$

s.t.  $J = \text{id}(m) \Rightarrow \text{id}(n) \subsetneq \text{id}(m) \subsetneq \mathbb{Z}$

Since  $n \in \text{id}(n)$ , since  $n = 1 \cdot n \Rightarrow n \in \text{id}(m)$

$\therefore n = mk$  for some  $k \in \mathbb{Z}_+$  and  $k \neq 1$ .

Hence  $n$  is not prime number.  $\square$

$\therefore I = \text{id}(n)$  is max. ideal.

problems: let  $R = \text{d.s of } (\mathbb{Z}_+, +, \cdot)$  with itself

let  $I_1 = \{(2n, 0) : n \in \mathbb{Z}\}$ . Is  $I_1$  max. ideal of  $R$

$I_2 = \{(2n, 3m) : n, m \in \mathbb{Z}\}$ . Is  $I_2$  max. ideal of  $R$ .

Remark : let  $(F, +, \cdot)$  be a field. Then  $\{0\}$  is the only max. ideal of  $F$ .

Definition :

let  $(R, +, \cdot)$  be a comm. ring,  $R$  is called local ring  $\iff R$  has unique max. ideal

Example :  $(\mathbb{Z}_4, +, \cdot)$  is local ring, since  $\mathbb{Z}_4$  has only one max. ideal which is  $\{\bar{0}, \bar{2}\}$ .

②  $\mathbb{Z}_8, \mathbb{Z}_{32}$  are local rings.

Theorem : let  $R$  be a comm. ring with unity 1. let  $M$  be a proper ideal of  $R$ . Then  $M$  is max. ideal  $\iff (M, a) = R \quad \forall a \in R, a \notin M$ .

Where  $(M, a) = \{m + ra : m \in M, r \in R\}$

proof :  $\implies$  ) If  $M$  is max ideal, To prove  $(M, a) = R$

$M \subsetneq (M, a) = M + id(a) \implies a = 0 + 1 \cdot a \in (M, a)$ . But

$a \notin M$ . Thus  $(M, a) = R$  (contradiction to  $M$  is max)

$\impliedby$  ) If  $(M, a) = R, \forall a \notin M$ . To prove  $M$  is max ideal

suppose  $M$  is not max. ideal  $\implies \exists$  ideal  $J$  of  $R$  s.t.

$M \subsetneq J \subsetneq R$ .

(37)

$\therefore \exists a \in J$  and  $a \notin M$ . But  $(M, a) = R$

$\therefore \forall x \in (M, a) \Rightarrow x = \underbrace{m}_J + \underbrace{ra}_J, m \in M \subseteq J$

$\therefore x \in J \Rightarrow (M, a) \subseteq J$  and  $J \subseteq (M, a)$

$\therefore (M, a) = J \Rightarrow R \subseteq J$

$\therefore R = J$  Contradiction! Thus  $M$  is max. ideal

Theorem 8

Let  $R$  be a comm. ring with unity.  $I$  be a proper ideal of  $R$ , then  $\exists$  a max. ideal of  $R$  s.t.  $I \subseteq J$

Proof:

البرهان يعتمد على مفهومة زورن (Zorn's lemma) والتي تنص:

ليكن  $X$  مجموعة غير خالية وليكن  $F$  مجموعة غير خالية من مجموعات جزئية من  $X$  إذا كان لكل  $J$  سلسلة  $\{C_i\}$  من عناصر  $F$  فإن  $\bigcup C_i \in F$  وأن  $F$  تملك عنصراً "أكبراً".

let  $I$  be a proper ideal of  $R$ .

See the collection  $F = \{J : J \supseteq I, J \text{ is a proper ideal of } R\}$

$F \neq \emptyset$  (because  $I$  is proper ideal and  $I \in F$ )

let  $\{C_i\}$  be a chain of  $F$   
سلسلة

let  $x, y \in \bigcup_{i \in \Lambda} C_i$ ,  $r \in R$

$\Rightarrow \exists j \in \Lambda$  s.t.  $x \in C_j$  and  $\exists k \in \Lambda$  s.t.  $y \in C_k$

$\Rightarrow \{C_i\}$  is a chain  $\Rightarrow C_j \subseteq C_k$  or  $C_k \subseteq C_j$

suppose  $C_k \subseteq C_j \Rightarrow x, y \in C_k \Rightarrow x-y \in C_k$

It's clear that  $I \subseteq \bigcup_{i \in \Lambda} C_i$   $\forall I \subseteq C_i$   
من الواضح ان

$\bigcup_{i \in \Lambda} C_i \neq R$  (because  $1 \notin C_i \forall i$ ,  $C_i$  is a proper ideal)

$\Rightarrow \bigcup_{i \in \Lambda} C_i \in F$ . Then by Zorn's lemma  $F$  has maximal element, we say  $M$ .

To prove that  $M$  is maximal ideal of  $R$ .

let  $K$  be an ideal of  $R$  s.t.  $M \subsetneq K$

$K \neq F$  لان خلاف ذلك لكان  $M$  على حداق من  $K$  وهذا مستحيل

$K = R$ . Then  $M$  is maximal ideal.

نتيجة  
Corollary

كتاب في الجبر

let  $R$  be a comm. ring with unity,  $a \in R$ . Then  $a$  is an invertible  $\Leftrightarrow a$  belongs to no max. ideal of  $R$ .

مع الفرضية

Proof :-  $\Rightarrow$  suppose that  $a$  is an invertible.

$(a)$  is the smallest ideal of  $R$  containing  $a$ .

But  $(a) = R \Rightarrow a$  is not belong to any max. ideal.

$\Leftarrow$  suppose that  $M$  is max. ideal and  $a \notin M$ .

see the id  $(a)$ . if  $R = (a)$ , then  $a$  is an invertible element.

either, if  $R \neq (a)$ , then by above theorem,  $\exists$  max. ideal  $M$  containing  $(a)$ .

$M$  and  $(a) \subseteq M \Rightarrow a \in M$ !  $(a \notin M \text{ contradiction})$

$\therefore$  it must be  $R = (a)$ .

هذا هو المطلوب

Corollary

let  $R$  be a comm. ring with unity. Then  $R$  has at least one max. ideal.

Proof :- since  $R$  is comm ring with 1,  $R$  has at least one proper ideal say  $I$ .

$\therefore \exists$  max ideal  $J$  of  $R$  s.t.  $I \subsetneq J \subsetneq R$  (by above theorem).

Theorem :-

let  $R$  be a comm. ring with unity 1. if  $R$  is local ring, then the only idempotent elements of  $R$  are 0 and 1.

هذا هو المطلوب

Def: Let  $R$  be a comm. ring with unity  $1$  - 39 -

$a \neq 0 \in R$  is called idempotent element if  $a^2 = a$ .  
also note

Proof :- Suppose that  $a$  is an idempotent element in  $R$  and  $a \neq 0, a \neq 1$

$$\because a^2 = a \Rightarrow a^2 - a = 0 \Rightarrow a(a-1) = 0$$

But  $a \neq 0$  and  $a-1 \neq 0$   $\therefore$   $a$  and  $a-1$  are zero divisors

This means  $a$  and  $a-1$  are zero divisors  
يعني  $a$  و  $a-1$  هما قاسم للصفر

$\therefore a$  and  $a-1$  have no invertible elements

$\therefore a$  and  $a-1$  belong to maximal ideal in  $R$

But  $R$  has only one max. ideal  $M$

$$\therefore a, a-1 \in M \Rightarrow 1 = a - (a-1) \in M$$

$$\therefore M = R \text{ ! } (R \text{ is not a local ring})$$

Example

Theorem 5 - Let  $R$  be a comm. ring with unity  $1$ .

and let  $I$  be a proper ideal of  $R$ . Then  $I$  is maximal

ideal  $\iff R/I$  is a field.

Proof :-  $\implies$

$R/I$  is a field

let  $a+I \in R/I$  and  $a+I \neq I \implies a \notin I$

But  $I$  is max. ideal  $\implies R = (I, a)$

$$\therefore 1 = x + ra \quad \text{where } r \in R, x \in I$$

$$\therefore 1 - ra = x \in I \Rightarrow (1 - ra) + I = I$$

$$\Rightarrow ra + I = 1 + I \Rightarrow (r + I)(a + I) = 1 + I$$

$$\therefore a + I \text{ has invertible element } (r + I)$$

⬅) let  $J$  be a proper ideal of  $R$  s.t.  $I \subsetneq J$ .

$$\therefore \exists w \in J, w \notin I \Rightarrow w + I \neq I$$

$$\therefore w + I \text{ has invertible element in the field } R/I$$

$$\therefore \exists b + I \in R/I \text{ s.t. } (w + I)(b + I) = 1 + I$$

$$\Leftrightarrow 1 - wb \in I$$

$$\text{we say } 1 - wb = c \text{ s.t. } c \in I$$

$$\therefore 1 = \underbrace{c}_{\substack{\in I \\ I \subseteq J}} - \underbrace{wb}_{\substack{\in I \\ \in J}} \Rightarrow 1 \in J \Rightarrow J = R$$

Remark 8

The theorem is not true in rings without unity, for example \*

The ring  $(\mathbb{Z}_8, +, \cdot)$  has no unity.

let  $M = \{0, 4, 8, \dots\}$  is max. ideal of  $\mathbb{Z}_8$ . But

$\mathbb{Z}_8/M = \{0 + m, 2 + m\}$  is not field.

Definition : Let  $R$  be a comm. ring,  $I$  be an ideal of  $R$ .  $I$  is called prime ideal iff  $\forall a, b \in R$ ,  $ab \in I \Rightarrow$  either  $a \in I$  or  $b \in I$ .

Example : In the ring  $(\mathbb{Z}, +, \cdot)$

let  $\text{id}(2) = \{0, \pm 2, \pm 4, \pm 6, \dots\}$

let  $a, b \in \mathbb{Z}$  s.t.  $ab \in \text{id}(2)$

is  $ab = 2c$  for some  $c \in \mathbb{Z}$

$\Rightarrow 2 \mid ab$ . But 2 is prime number  $\Rightarrow$  either  $2 \mid a$

or  $2 \mid b \Rightarrow a$  is multiply of 2 or  $b$  is multiply of 2

$\Rightarrow a \in \text{id}(2)$  or  $b \in \text{id}(2)$

$\therefore \text{id}(2)$  is prime ideal.

proof : In the ring  $(\mathbb{Z}, +, \cdot)$ , if  $P$  is a prime number, then  $\text{id}(P)$  is a prime ideal.

Theorem :

Let  $R$  be a comm. ring with unity 1. Then  $R$  is an integral domain  $\Leftrightarrow \{0\}$  is a prime ideal.

Proof  $\Rightarrow$  Suppose  $R$  is an integral domain.

To prove  $\{0\}$  is prime ideal.

let  $a, b \in R$  s.t.  $ab \in \{0\} \Rightarrow ab = 0$

So,  $a=0$  or  $b=0$  (since  $R$  has no zero divisor)

$\Rightarrow a \in \{0\}$  or  $b \in \{0\}$ . Thus  $\{0\}$  is prime ideal.

$\leftarrow$ ) let  $a, b \in R$ ,  $ab=0$

$\Rightarrow ab \in \{0\}$ . But  $\{0\}$  is prime ideal

$\Rightarrow a \in \{0\}$  or  $b \in \{0\} \Rightarrow a=0$  or  $b=0$

$\therefore R$  has no zero divisor  $\Rightarrow R$  is an integral domain.

Problem: (H.W)

في كلتا

In  $(\mathbb{Z}_n, +, \cdot)$ : A non trivial ideal  $I \neq \mathbb{Z}$ ,  $I \neq \{0\}$

is prime ideal  $\iff n$  is prime number.

Example:  $(\mathbb{Z}_6, +, \cdot)$

let  $I = \{\bar{0}, \bar{3}\}$ ,  $J = \{\bar{0}, \bar{2}, \bar{4}\}$ ,  $K = \{\bar{0}\}$

$I, J$  are prime ideal. But  $K$  is not prime ideal.

since  $a, b \in \mathbb{Z}_6$   
 $2, 3 \in \mathbb{Z}_6$

$$2 \cdot 3 = 0 \in \mathbb{Z}_6$$

Example:

In the ring  $(\mathbb{Z}_5, +, \cdot)$ .  $2 \in \mathbb{Z}_5 \wedge 3 \in \mathbb{Z}_5$

since  $\mathbb{Z}_5$  is field  $\Rightarrow \mathbb{Z}_5$  is an integral domain

$\therefore \{0\}$  is the only proper prime ideal

في الساحة المثالي الأولي الوحيد هو  $\{0\}$

Theorem : let  $R$  be a commutative ring with unity  $1$ . Then every maximal ideal of  $R$  is prime ideal.

Proof : let  $M$  be a max ideal of  $R$

To prove  $M$  is prime ideal.

let  $a, b \in R$  s.t.  $ab \in M$  and  $a \notin M$   
we must prove that  $b \in M$ . But  $M$  is max. ideal,  $a \notin M$

$\Rightarrow (M, a) = R \Rightarrow 1 \in (M, a) \Rightarrow 1 = m + ra$  for some

$m \in M, r \in R \Rightarrow b = mb + rab \in M$

$\therefore b \in M$ . Thus  $M$  is prime ideal.

عكس البرهان اعلاه غير صحيح والمثال التالي يوضح ذلك

$\{0\}$  in  $(\mathbb{Z}, +, \cdot)$  is prime ideal. But  $\{0\}$  is not max. ideal

Problem 5 - (H.W)

let  $R = \text{d.s. of } (\mathbb{Z}, +, \cdot)$  with  $(\mathbb{Z}, +, \cdot)$   
and let  $I = \{(a, a) : a \in \mathbb{Z}\}$ . Show that  $I$  is a prime ideal, but  $I$  is not maximal ideal.

Remark :

The theorem is not true in rings without unity

Example :  $I = \{0, \pm 4, \pm 8, \pm 12, \dots\}$  is max. in  $\mathbb{Z}_6$

But  $I$  is not prime ideal (Since  $4 = 2 \cdot 2 \in I$ , but  $2 \notin I$ )

Theorem 8 Let  $R$  be a comm. ring with unity  $1$ .  
 Let  $I$  be an ideal of  $R$ . Then  $I$  is a prime ideal  $\iff (R/I, +, \cdot)$  is an integral domain.

Proof  $\implies$   $R$  is comm. ring with unity  $1 \implies R/I$  is comm. ring with unity  $1 + I$ .

If  $(a + I)(b + I) = I \xrightarrow{\text{Zero element of } R/I}$

$\implies ab + I = I \implies ab \in I$ , but  $I$  is a prime ideal

of  $R \implies$  either  $a \in I$  or  $b \in I$ .

If  $a \in I$ , then  $a + I = I$  and if  $b \in I$ , then  $b + I = I$

$\implies R/I$  has no zero divisor and so  $R/I$  is an integral domain. satisfies

$\longleftarrow$  To prove  $I$  is prime ideal

let  $a, b \in R$  s.t.  $ab \in I \implies ab + I = I$

$(a + I)(b + I) = I$

either  $a + I = I$  or  $b + I = I$  (since  $R/I$  has no zero divisor)

$\implies a \in I$  or  $b \in I$

$\implies I$  is prime ideal.

Theorem 8 - let  $R$  be a P.I.D. Then a nontrivial ideal  $I$  of  $R$  is maximal ideal  $\iff$  it is prime ideal.

Proof :  $\leftarrow$

let  $I$  be a prime ideal of  $R$  and  $I \neq \{0\}$ .

let  $J$  be an ideal of  $R$  s.t.  $I \subsetneq J$ .

$\because R$  is P.I.D., that means  $\exists a, b \in R$  s.t.

$$I = (a), \quad J = (b)$$

$$\Rightarrow a \in (a) \subsetneq (b)$$

$$\textcircled{1} \quad a = tb \quad \text{for some } t \in R \Rightarrow tb \in I$$

But  $I$  is prime ideal  $\Rightarrow$  either  $t \in I$  or  $b \in I$

$$\text{if } b \in I \Rightarrow (b) \subseteq I = (a) \Rightarrow I = J \text{ !}$$

$$\text{Then } t \in I \Rightarrow t \in I = (a)$$

$$\textcircled{2} \quad t = sa, \quad s \in R$$

From  $\textcircled{1}$  and  $\textcircled{2}$ , we get  $a = sba$

$\because R$  is an integral domain,  $a \neq 0$

$$\therefore sb = 1 \Rightarrow 1 \in J \Rightarrow R = J$$

$\therefore I$  is maximal ideal of  $R$ .

(42)

Theorem :- let  $R$  be a comm. ring with unity  $1$  s.t.  $b^2 = b$

for all  $b \in R$ . Then a non-trivial ideal  $I$  is maximal ideal  
 $\iff I$  is prime ideal

proof :-  $\leftarrow$  let  $I$  be a prime ideal of  $R$  s.t.

$I \neq \{0\}$  and let  $J$  be an ideal of  $R$  s.t.  $I \subsetneq J$ .

Then  $\exists b \in J, b \notin I$

since  $b^2 = b$  (by hypothesis)

$\therefore b^2 - b = 0 \implies b(b-1) = 0 \in I$

$\therefore I$  is prime ideal,  $b \notin I$

$\therefore (b-1) \in I \implies b-1 \in J$

But  $b \in J \implies b, (b-1) \in J$  (by def. of ideal)

$\therefore 1 \in J \implies J = R$

$\therefore I$  is maximal ideal.

Definition :

الجزء القوي : nil radical

let  $(R, +, \cdot)$  be a ring and  $I$  be an ideal of  $R$ , the set  $\{x \in R : x^n \in I \text{ for some } n \in \mathbb{Z}_+\}$  is called nil radical and denoted by  $\sqrt{I}$ .

Example : ①  $(12)$  is an ideal in  $\mathbb{Z}$

$$\sqrt{(12)} = \sqrt{2^2 \cdot 3} = (6)$$

②  $(4)$  is an ideal in  $\mathbb{Z}$

$$\sqrt{(4)} = (2)$$

Remarks :

$$\textcircled{1} I \subseteq \sqrt{I}$$

② let  $n \in \mathbb{Z}_+$  and  $(n)$  is an ideal s.t.  $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$

$$\text{Then } \sqrt{(n)} = \sqrt{(p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k})} = (p_1 p_2 \dots p_k)$$

③  $x \in \sqrt{I} \iff x + I$  is nilpotent element in  $R/I$

و هو يكافئ العنصر

$$x^n + I = 0 \Rightarrow x^n \in I$$

That is,  $x \in \sqrt{I} \Rightarrow x^n \in I$  for some  $n \in \mathbb{Z}_+$

Proposition :-

$\sqrt{I}$  is an ideal of  $R$ .

Proof :-

let  $x, y \in \sqrt{I}$ . Then  $\exists n, m \in \mathbb{Z}_+$  s.t.  $x^n \in I$  and  $y^m \in I$

Class

Definition :

- 43 -

nil radical. الجذر النيلي

let  $(R, +, \cdot)$  be a ring and  $I$  be an ideal of  $R$ , the set  $\{x \in R : x^n \in I \text{ for some } n \in \mathbb{Z}_+\}$  is called nil radical and denoted by  $\sqrt{I}$ .

Example : ①  $(12)$  is an ideal in  $\mathbb{Z}$

$$\sqrt{(12)} = \sqrt{2^2 \cdot 3} = (6)$$

②  $(4)$  is an ideal in  $\mathbb{Z}$

$$\sqrt{(4)} = (2)$$

Remarks :

①  $I \subseteq \sqrt{I}$

② let  $n \in \mathbb{Z}_+$  and  $(n)$  is an ideal s.t.  $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$

$$\text{Then } \sqrt{(n)} = \sqrt{(p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k})} = (p_1 p_2 \dots p_k)$$

③  $x \in \sqrt{I} \iff x + I$  is nilpotent element in  $R/I$   
أي  $x + I$  هو العنصر النيلي

$$x^n + I = 0 \Rightarrow x^n \in I$$

That is,  $x \in \sqrt{I} \Rightarrow x^n \in I$  for some  $n \in \mathbb{Z}_+$

Proposition :-

$\sqrt{I}$  is an ideal of  $R$ .

Proof :-

let  $x, y \in \sqrt{I}$ . Then  $\exists n, m \in \mathbb{Z}_+$  s.t.  
 $x^n \in I$  and  $y^m \in I$

Class

$$(x-y) = \overset{n+m}{x} + \overset{n+m}{(n+m)x} + \overset{n+m-1}{y} + \dots + \overset{n}{(-)^{n-m}}xy + \dots + \overset{m+n}{y}$$

$\in I \quad \in I \quad \in I \quad \in I$

$$\therefore (x-y) \in \sqrt{I}$$

let  $x \in R, x \in \sqrt{I} \Rightarrow x^n \in I$

$$(xx^n) = \overset{n}{x} \overset{n}{x} \Rightarrow rx \in \sqrt{I}$$

$\in I$

$\therefore \sqrt{I}$  is an ideal of  $R$ .

Remark :-

$$\sqrt{\sqrt{I}} = \sqrt{I}$$

Proof :- It is clear that  $\sqrt{I} \subseteq \sqrt{\sqrt{I}}$  by def.  $\rightarrow ①$

Now, To prove  $\sqrt{\sqrt{I}} \subseteq \sqrt{I}$

let  $w \in \sqrt{\sqrt{I}}$ . Then  $\exists n \in \mathbb{Z}_+$  s.t.

$$w^n \in \sqrt{I} \Rightarrow (w^n)^m \in I, m \in \mathbb{Z}_+$$

$$\Rightarrow \overset{nm}{w} \in I \Rightarrow w \in \sqrt{I}$$

$$\& \sqrt{\sqrt{I}} \subseteq \sqrt{I} \rightarrow ②$$

From ① and ②, we get  $\sqrt{\sqrt{I}} = \sqrt{I}$ .

Definition :

let  $(R, +, \cdot)$  be a ring and  $I$  be an ideal of  $R$ . Then  $I$  is called semiprime if  $I = \sqrt{I}$ .

بداية

Example :

let  $6\mathbb{Z}$  be an ideal of  $\mathbb{Z}$ .  
 Then  $6\mathbb{Z}$  is a semiprime ideal of  $\mathbb{Z}$ .  
 Since  $\sqrt{6\mathbb{Z}} = 6\mathbb{Z} = (6)$

Remark : - Every prime ideal is semiprime.

But the Converse is not true in general for  
 example :  $6\mathbb{Z}$  is semiprime ideal in  $\mathbb{Z}$ , but  
 it is not prime in  $\mathbb{Z}$ .

Theorem : -

let  $I$  be an ideal of  $R$ . Then  
 $I$  is semiprime  $\iff R/I$  has not contain nilpotent  
 elements only zero element.

Proof : -  $\implies$ ) let  $a+I$  be nilpotent element in

$$R/I \implies (a+I)^n = I, n \in \mathbb{Z}_+$$

$$\therefore a^n + I = I \implies a^n \in I \implies a \in \sqrt{I} = I \quad (\text{since } I \text{ is semiprime ideal})$$

$$\therefore a + I = I$$

$$\iff \text{it is clear that } I \subseteq \sqrt{I}$$

Now, let  $x \in \sqrt{I} \implies x^n \in I$  for some  $n \in \mathbb{Z}_+$

$$\iff x^n + I = I$$

$$\therefore (x+I)^n = x^n + I = I$$

$\therefore x+I$  is nilpotent element in  $R/I$

$$\stackrel{\text{Theorem}}{\implies} \sqrt{I} = I \quad \because x+I = I \implies x \in I$$

## Definition

Let  $(R, +, \cdot)$  be a ring,  $I$  be an ideal of  $R$ . Then  $I$  is called primary ideal if the following holds

$\forall a, b \in R, a \notin I, \text{ then } b^n \in I \text{ for some } n \in \mathbb{Z}_+$

## Example :

$4\mathbb{Z}$  is primary ideal in  $\mathbb{Z}$  ( $2 \cdot 2 = 4 \in 4\mathbb{Z} \Rightarrow 2 \in \sqrt{4\mathbb{Z}}$  but  $2 \notin 4\mathbb{Z}$ )

## Remark

$$a, b \in R \Rightarrow a \in I \text{ or } b \in I \Rightarrow I \text{ is prime}$$

Every prime ideal is primary ideal but the converse is not true. For example  $\text{id}(4)$  in  $\mathbb{Z}$  is primary ideal but not prime.

Theorem: Let  $R$  be a ring and  $I$  be a non-trivial ideal of  $R$ . Then  $I$  is primary ideal if and only if all

Zero divisors in  $\frac{R}{I}$  are nilpotent elements.

proof :  $\Rightarrow$ ) let  $I$  be a primary ideal,  $a+I$  be zero

divisor in  $R/I$  that means  $a+I \neq I$  and  $\exists b+I \neq I$

$$\text{s.t. } (a+I)(b+I) = I \Rightarrow ab+I = I \Rightarrow ab \in I$$

But  $b \notin I$  and  $I$  is primary ideal. Then  $\exists$  positive integer

$n$  s.t.  $a^n \in I \Leftrightarrow a^n+I = I$ . Therefore  $a+I$  is nilpotent element.

$\Leftarrow$ ) let  $ab \in I$  and  $a \notin I \Rightarrow a+I \neq I$

now,  $ab \in I \Rightarrow ab+I = I \Rightarrow (a+I)(b+I) = I$

if  $b+I = I \Rightarrow b \in I$ . This completes the proof

if  $b+I \neq I \Rightarrow b+I$  is zero divisor. Then  $b+I$  is

nilpotent, that is  $\exists$  positive integer number  $n \in \mathbb{Z}_+$

s.t.  $(b+I)^n = 0+I = I \Rightarrow b^n \in I \Rightarrow b^n+I = I$

Thus  $I$  is primary ideal.

## Boolean Rings

الحلقات البوليانية

### Definition :

let  $(R, +, \cdot)$  be a ring with unity. Then  $R$  is called Boolean ring if  $a^2 = a$  for all  $a \in R$ .

### Examples :

(1)  $(\mathbb{Z}_2, +_2, \cdot_2)$  is Boolean ring

Since  $(1)^2 = 1$  ,  $(0)^2 = 0$

(2)  $(\mathbb{Z}_3, +_3, \cdot_3)$  is not Boolean ring

since  $(2)^2 = 1$

Remark : Every Boolean ring is Comm. ring and  $ch(R)=2$

Theorem :

Let  $(R, +, \cdot)$  be a Boolean ring and  $I$  be a proper ideal of  $R$ . The following statements are equivalent

- (1)  $I$  is max. ideal
- (2)  $I$  is prime ideal
- (3)  $\forall 0 \neq a \in R$  either  $a \in I$  or  $1-a \in I$ .

Proof (1)  $\Rightarrow$  (2) is proved.

(2)  $\Rightarrow$  (3) let  $a \in R, a \neq 0$

$\therefore a(1-a) = a - a^2 = a - a = 0 \Rightarrow 0 \in I \Rightarrow$  either  $a \in I$  or  $(1-a) \in I$  because  $I$  is prime ideal

(3)  $\Rightarrow$  (1)

let  $M$  be an ideal of  $R$  st.  $I \subsetneq M$ , then  $\exists x \in M, x \notin I$ , Therefore by (3)  $1-x \in I \subset M$

$\therefore x, 1-x \in M, M$  is an ideal of  $R \Rightarrow 1 \in M \Rightarrow M=R$   $\square$ !

$\therefore I$  is max. ideal

Theorem :

$(R, +, \cdot)$  is a Boolean <sup>field</sup> if and only if  $R \cong \mathbb{Z}_2$

Proof :  $\Rightarrow$ ) let  $a \in R, a \neq 0$

$$a = a \cdot 1 = a(a \bar{a}) = (a \cdot a) \bar{a} = a^2 \bar{a} = a \cdot \bar{a} = 1$$

$$\therefore R = \{0, 1\} \Rightarrow R \cong \mathbb{Z}_2$$

$\Leftarrow$ ) It is clear

Received of the T.C. a certain sum of money

the sum of

Rs. 1,000/-

for

the sum of

Rs. 1,000/-

for

د. حاتم + د. نسيه

# الفصل السابع

## Chapter Seven

# حلقة الحدوديات

## Chapter Seven

### "Polynomial Ring"

7

Def: Let  $R$  be any ring

Let  $S = \{ f(x) : f(x) = a_0 + a_1x + \dots + a_nx^n, a_0, a_1, \dots, a_n \in R \}$

or  $\{ f(x) : f(x) = \sum_{i=0}^n a_i x^i, a_i \in R, \forall i \leq n \}$

Any  $f(x) \in S$  is called polynomial over  $R$ . Define  $+$  as by:-

Let  $f(x), g(x) \in S$ ;  $f(x) = \sum_{i=0}^n a_i x^i, a_i \in R, a_i = 0 \forall i > n$

$g(x) = \sum_{i=0}^m b_i x^i, b_i \in R, b_i = 0 \forall i > m$

1)  $f(x) + g(x) = \left( \sum_{i=0}^t c_i x^i \right) \in S$  where  $c_i = a_i + b_i$

$\forall i = 0, 1, \dots, t, c_i = 0 \forall i > \max\{n, m\}$

2)  $f(x) \cdot g(x) = \sum_{k=0}^t c_k x^k, c_k = 0 \forall k > n+m$  where

$$c_0 = a_0 b_0$$

$$c_1 = a_0 b_1 + a_1 b_0$$

$$c_2 = a_0 b_2 + a_1 b_1 + a_2 b_0$$

$$c_3 = a_0 b_3 + a_1 b_2 + a_2 b_1 + a_3 b_0$$

$$c_t = a_0 b_t + a_1 b_{t-1} + a_2 b_{t-2} + \dots + a_t b_0$$

or  $c_s = \sum_{i+j=s} a_i b_j \quad i, j \geq 0$

(47)

Notice that  $+$ ,  $\cdot$  are closed on  $S$ .

Ex:- Let  $f(x), g(x)$  be two polynomials over  $Z_4$  where  $f(x) = 3 + x$ ,  $g(x) = 1 - x + x^2$

$$f(x) = 3 + x, \quad a_0 = 3, \quad a_1 = 1, \quad a_2 = a_3 = \dots = a_n = 0$$

$$g(x) = 1 - x + x^2, \quad b_0 = 1, \quad b_1 = -1 = 3 \pmod{4}, \quad b_2 = 1$$

$$b_3 = b_4 = \dots = b_n = 0$$

$$\begin{aligned} f(x) + g(x) &= (a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2 \\ &= \left(1 + 3\right) + \left(1 + 3\right)x + (0 + 1)x^2 \\ &= x^2 \end{aligned}$$

$$f(x) \cdot g(x) = \sum_{k=0}^{\infty} c_k x^k, \quad \text{where } c_0 = a_0 b_0 = 3 \cdot 1 = 3$$

$$c_1 = a_0 b_1 + a_1 b_0 = 3 \cdot 3 + 1 \cdot 1 = 2 \Rightarrow c_1 x = 2x$$

$$c_2 = a_0 b_2 + a_1 b_1 + a_2 b_0 = 3 \cdot 1 + 1 \cdot 3 + 0 \cdot 1 = 2$$

$$c_3 = a_0 b_3 + a_1 b_2 + a_2 b_1 + a_3 b_0 = 3 \cdot 0 + 1 \cdot 1 + 0 \cdot 3 + 0 \cdot 0 = 1$$

$$c_4 = a_0 b_4 + a_1 b_3 + a_2 b_2 + a_3 b_1 + a_4 b_0 = 0$$

Similarly,

$$\text{Since, } c_5 = c_6 = 0$$

$$\therefore f(x) \cdot g(x) = 3 + 2x + 2x^2 + x^3 \text{ which is poly. over } Z_4$$

Note:-

If  $R$  is a ring, then  $S = \{f(x) : f(x) \text{ is a poly over } R\}$  is denoted by  $R[x]$ .

Show that  $(R[x], +, \cdot)$  is a ring.

①  $+$  and  $\cdot$  are closed on  $R[x]$ .

② If  $f(x) = \sum_{i=1}^n a_i x^i$ ,  $g(x) = \sum_{i=1}^m b_i x^i$

$$f(x) + g(x) = \sum_{i=0}^t (a_i + b_i) x^i, \quad t \leq \max(n, m)$$

$$\sum_{i=0}^t (b_i + a_i) x^i = \sum_{i=0}^m b_i x^i + \sum_{i=0}^n a_i x^i = g(x) + f(x)$$

$+$  is comm.

③  $+$  is asso. on  $R[x]$ .

④ let  $h(x) = 0$ ;  $h(x) \in R[x]$

and  $h(x) + f(x) = f(x)$ , then  $h(x)$  = additive identity of  $R[x]$ .

⑤ If  $f(x) = \sum_{i=0}^n a_i x^i$ , let  $(-f)(x) = \sum_{i=0}^n (-a_i) x^i$

⑥  $f(x) + [(-f)(x)] = 0 = h(x)$

$\therefore -f(x)$  is the additive inverse of  $f(x)$

• asso. on  $R[x]$ .

• dist. over  $+$  on  $R[x]$ .

$\therefore R[x]$  is a ring.

## Remark

- ① If  $R$  is comm. ring, then  $R[x]$  is comm. ring.
- ② If  $R$  has unity 1, then  $R[x]$  has unity ( $0(x)=1$ )

## Definition:

Let  $f(x) = \sum_{i=0}^n a_i x^i \in R[x]$ ,  $f(x) \neq \text{Zero poly}$

$a_n$  is called the leading coefficient

- If  $a_n \neq 0$ , then  $f(x)$  has degree  $n$

- If  $f(x) = a$  ( $a \in R$ ),  $f(x)$  is called constant poly. of degree zero where  $a \neq 0$

- If  $f(x) = 0$ , we shall assign no degree for  $f(x)$ .

## Theorem "1.1.1"

Let  $R$  be an integral domain,  $f(x), g(x)$  non zero polys in  $R[x]$  then:

- ①  $\deg(f(x)g(x)) = \deg f(x) + \deg g(x) = n + m$
- ② either  $f(x) + g(x) = 0$  or  $\deg(f(x) + g(x)) \leq \max(\deg f(x), \deg g(x))$

proof

① let  $f(x) = a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n$  is non-zero poly.

$a_n \neq 0$ , i.e. deg  $f(x) = n$  is finite

Let  $g(x) = b_0 + b_1x + \dots + b_mx^m$  is a non-zero poly.

$b_m \neq 0$ , i.e. deg  $g(x) = m$  is finite

Notice  $a_i = 0 \quad \forall i > n$

$b_i = 0 \quad \forall i > m$

$$f(x) \cdot g(x) = \sum_{k=0}^{\infty} C_k x^k, \text{ where } C_0 = a_0 b_0, C_1 = a_0 b_1 + a_1 b_0$$

$$C_{m+n} = \underbrace{a_0 b_{m+n}}_{=0} + \underbrace{a_1 b_{m+n-1}}_{=0} + \dots + \underbrace{a_n b_m}_{=0''} + \underbrace{a_{n+1} b_{m-1}}_{=0''} + \dots + \underbrace{a_{n+m} b_0}_{=0''}$$

$$C_{m+n} = a_n b_m \neq 0 \quad \left( \begin{array}{l} \text{Since } a_n, b_m \in R, a_n \neq 0, b_m \neq 0 \text{ and } R \\ \text{has no zero divisor} \end{array} \right)$$

$$C_{n+m+1} = \underbrace{a_0 b_{n+m+1}}_{=0} + \underbrace{a_1 b_{n+m}}_{=0} + \dots + \underbrace{a_n b_{m+1}}_{=0} + \underbrace{a_{n+1} b_m}_{=0} + \dots + \underbrace{a_{n+m+1} b_0}_{=0}$$

$$\text{Since } C_{n+m+s} = 0 \quad \forall s \geq 1$$

$$\therefore \deg(f(x) \cdot g(x)) = n+m = \deg f(x) + \deg g(x)$$

Corollary 2.11

If  $R$  is an integral domain, then  $R[x]$  is an integral domain

Proof

$R$  is an integral domain  $\Rightarrow R$  is comm. ring with unity and  $R$  has no zero divisor.

Since  $R$  is comm. ring with unity  $\Rightarrow R[X]$  is comm. ring with unity.

Let  $f(x), g(x) \in R[X]$ ,  $f(x) \neq 0$ ,  $g(x) \neq 0$

① Let  $f(x) = a_0 \neq 0$ ,  $g(x) = b_0 \neq 0$

Then  $f(x)g(x) = a_0b_0 \neq 0$  since  $R$  has no zero divisor.

② Let  $f(x), g(x)$  are non-zero poly. of degrees  $n, m$  respectively then  $f(x)g(x)$  is poly of degree  $(n+m)$

and  $f(x)g(x) \neq 0$ . Thus  $R[X]$  has no zero divisor.

$\therefore R[X]$  is an integral domain.

Theorem

The Division Algorithm

~~is a well defined algorithm~~

Let  $R$  be a comm. ring with unity and  $f(x), g(x)$  are non-zero poly's in  $R[X]$  such that the leading coefficient of  $g(x)$  is an invertible element in  $R$ . Then there exists a unique poly's  $q(x), r(x)$  in  $R[X]$  such that

$f(x) = q(x)g(x) + r(x)$  where  $r(x) = 0$  or  $\deg r(x) < \deg g(x)$

ooo ————— ooo

### Example

let  $f(x) = x^3 + 2x + 1$  and  $g(x) = 4x + 1 \in \mathbb{Z}_5[x]$

Divide  $f(x)$  by  $g(x)$ .

$$\begin{array}{r}
 4x + 1 \overline{) x^3 + 2x + 1} \\
 \underline{-(x^3 + 4x^2)} \phantom{+ 1} \\
 3x^2 + 2x + 1 \\
 \underline{-(3x^2 + 3x)} \phantom{+ 1} \\
 x + 1 \\
 \underline{-(x + 1)} \\
 0
 \end{array}$$

$\therefore f(x) = g(x)(4x^2 - x + 2) + (-1)$   
 $\quad \quad \quad \text{divisor} \quad \quad \text{quotient} \quad \quad \text{remainder}$

### Corollary (Remainder theorem)

let  $R$  be a comm ring with unity.  $f, p \in R[x]$   
 $a \in R$ . Then  $\exists! q(x) \in R[x]$  s.t.  $f(x) = (x-a)q(x) + f(a)$

proof:

$f(x), (x-a) \in R[x]$ , then by Div. Alg,  $\exists! q(x), r(x)$

$\in R[x]$  s.t.  $f(x) = (x-a)q(x) + r(x)$  where  $r(x) = 0$  or

$\deg(r(x)) < \deg(x-a) = 1$

$\therefore r(x) = 0$  or  $\deg r(x) < 1$ , then  $r(x)$  is Constant poly.

$\therefore r(x) = c$  for some  $c \in R$

$$f(x) = (x-a)q(x) + c$$

دفعه  $x$  الى  $a$

$$\therefore f(a) = (a-a)q(a) + c = c \Rightarrow f(a) = c$$

Thus  $f(x) = (x-a)q(x) + f(a)$

### Example

$$f(x) = 2x^4 + 5x^2 + 1 \in \mathbb{Z}_6[x]$$

$a = 4 \in \mathbb{Z}_6$  is

$$\therefore 2x^4 + 5x^2 + 1 = (x-4)q(x) + f(4)$$

$$f(4) = 2 \cdot 4^4 + 5 \cdot 4^2 + 1 = 5$$

$$\begin{array}{r} 2x^3 + 2x^2 + x + 4 \\ x-4 \overline{) 2x^4 + 5x^2 + 1} \\ \underline{+ 2x^4} \quad \underline{+ 2x^3} \phantom{+ 1} \\ 2x^3 + 5x^2 + 1 \\ \underline{+ 2x^3} \quad \underline{+ 2x^2} \phantom{+ 1} \\ x^2 + 1 \\ \underline{+ x^2} \quad \underline{+ 4x} \phantom{+ 1} \\ 4x + 1 \\ \underline{+ 4x} \quad \underline{+ 4} \\ 1 \end{array}$$

$$\begin{array}{r} 2x^3 + 5x^2 + 1 \\ \underline{+ 2x^3} \quad \underline{+ 2x^2} \\ x^2 + 1 \\ \underline{+ x^2} \quad \underline{+ 4x} \\ 4x + 1 \\ \underline{+ 4x} \quad \underline{+ 4} \\ 1 \end{array}$$

$$\begin{array}{r} x^2 + 1 \\ \underline{+ x^2} \quad \underline{+ 4x} \\ 4x + 1 \\ \underline{+ 4x} \quad \underline{+ 4} \\ 1 \end{array}$$

$$\begin{array}{r} 4x + 1 \\ \underline{+ 4x} \quad \underline{+ 4} \\ 1 \end{array}$$

اذن الباقي هو 5

5 وهو يعقل 5 في  $\mathbb{Z}_6$

### Definition

If  $f(x) \in R[x]$ , then

①  $a \in R \wedge f(a) = 0$ , then  $a$  is called a root of  $f(x)$ .

②  $\forall f, g(x) \in R[x]$

$f(x)$  divide  $g(x)$  ( $f(x) | g(x)$ ) means  $\exists k(x) \in R[x]$  st.  
 $g(x) = k(x)f(x)$ .

### Theorem Factorization theorem

The poly  $f(x) \in R[x]$  is division by  $(x-a)$  (where  $a \in R$ )  
 $\iff a$  is a root of  $f(x)$ .

Proof  $(x-a) | f(x) \iff f(x) = (x-a)k(x)$  for some  $k(x) \in R[x]$   
 $\iff f(a) = 0 \implies a$  is a root of  $f(x)$ .

Example let  $f(x) = x^3 + x^2 + 1 \in \mathbb{Z}_3[x]$

1 is a root of  $f(x)$ , since  $f(1) = 1^3 + 1^2 + 1 = 0$

$$\begin{array}{r} x^2 + 2x + 2 \\ x-1 \overline{) x^3 + x^2 + 1} \\ \underline{-(x^3 + x^2)} \phantom{+ 1} \\ 0 \phantom{+ 1} \end{array}$$

$$\begin{array}{r} 2x^2 + 1 \\ 2x-1 \overline{) 2x^2 + 2x} \\ \underline{-(2x^2 + 2x)} \\ 0 \end{array}$$

$$\therefore f(x) = (x-1)(x^2 + 2x + 2)$$

$$\begin{array}{r} 2x + 1 \\ 2x-1 \overline{) 2x + 2} \\ \underline{-(2x - 2)} \\ 4 \end{array}$$



Example : let  $f(x) = x^3 + 4x^2 + 4x + 1 \in \mathbb{Z}_5[x]$

0 is not root of  $f(x)$ , since  $f(0) = 1 \neq 0$

1 is root of  $f(x)$ , since  $f(1) = 0$

2 is not root of  $f(x)$

لدينا في السطر الثالثه فوجدنا  
بوجود لها ثلاثة جذور

3 = = = = =

4 is root of  $f(x)$

$\therefore 1, 4$  are two root of  $f(x)$   
أي أن 1 و 4 هما جذور  $f(x)$

$$\begin{array}{r} x^2 + 4 \\ x-1 \overline{) x^3 + 4x^2 + 4x + 1} \\ \underline{x^3 + x^2} \phantom{+ 4x + 1} \\ 3x^2 + 4x + 1 \\ \underline{3x^2 + 3x} \phantom{+ 1} \\ x + 1 \\ \underline{x + 4} \\ 0 \end{array}$$

$$\therefore f(x) = (x-1)(x-4)(?)$$

$$\therefore f(x) = (x-1)(x^2 + 4)$$

$K(x)$

1 is root of  $K(x)$

4 = = = = =

$$x^2 + 4 = K(x) = (x-1)(x-4) \Rightarrow f(x) = (x-1)(x-1)(x-4)$$

$K(x)$

Theorem :

If  $F$  is a field then  $F[x]$  is a P.I.D.

proof

$F$  is field  $\rightarrow F$  is an integral domain

$$\Rightarrow F[x] = = =$$

let  $I$  be any ideal in  $F[x]$ . To prove  $I$  is P.I.  
 If  $I = \{0\} \Rightarrow I$  is P.I.

$I \neq \{0\}$ , we choose a poly.  $p(x)$  in  $I$ ,  $p(x) \neq 0$  with lowest deg. we claim that  $I = \text{id}(p(x))$ . To prove that  $\text{id}(p(x)) \subseteq I$ . For any  $f(x) \in \text{id}(p(x))$

$$\therefore f(x) = k(x) \underbrace{p(x)}_{\in I} \in I \Rightarrow \text{id}(p(x)) \subseteq I$$

for any  $g(x) \in I$ . To prove  $I \subseteq \text{id}(p(x))$

then by division Alg.  $\exists s(x), r(x) \in F[x] \ni g(x) = s(x)p(x) + r(x)$

where  $r(x) = 0$  or  $\deg r(x) < \deg p(x)$

$$\therefore r(x) = \underbrace{g(x)}_{\in I} - \underbrace{s(x)p(x)}_{\in I} \Rightarrow r(x) \in I$$

So, if  $\deg r(x) < \deg p(x)$ , we get  $r(x) = 0$

$$\Rightarrow g(x) = s(x)p(x) \in \text{id}(p(x))$$

$$\therefore I \subseteq \text{id}(p(x)). \text{ Therefore } I = \text{id}(p(x))$$

Corollary:  $R[x], Q[x], Z[x], C[x]$  are PID.

Corollary: let  $F$  be any field. Then any non-trivial ideal in  $F[x]$  is prime  $\iff$  it is max.

proof  $F$  is field  $\Rightarrow F[x]$  is PID, so a non-trivial ideal in PID is prime  $\iff$  it is max

Example show that  $\mathbb{Z}[x]$  is not PID.

let  $I = \{a_1x + a_2x^2 + \dots + a_nx^n, a_i \in \mathbb{Z}\}$

$I$  is not max (problem)

$\mathbb{Z}[x]$  is not PID.

Definition

let  $f(x)$  be a non-zero and non-constant poly  $R[x]$ ,  $f(x)$  is called reducible, if  $\exists g(x), h(x)$  (non-constant poly's) s.t.  $f(x) = h(x)g(x)$ .

$f(x)$  is called irreducible if it is not reducible.

Example

① let  $f(x) = x^2 + 4 \in \mathbb{R}[x]$   
it is irreducible

② let  $f(x) = x^2 + 4 \in \mathbb{Z}_5[x] = (x+1)(x+4)$

$f(x)$  is reducible

Remark: let  $F$  be any field,  $f(x) \in F[x]$ ,  $\deg f(x) = 1$   
if  $f(x) = ax + b$ , then  $f(x)$  has root  $(-ba^{-1})$

Remark: let  $f(x) \in F[x]$ ,  $\deg f(x) \geq 1$ . if

$f(x)$  has a root  $\Rightarrow f(x)$  is reducible

proof: if  $a$  is a root of  $f(x)$

if  $a$  is a root of  $f(x)$  then  $f(x) = (x-a)q(x)$   
2nd part

(53)

$$(x-a) \mid f(x) \Rightarrow \exists g(x) \in F[x] \text{ s.t. } f(x) = g(x)(x-a)$$

and  $\deg g(x) \geq 1 \Rightarrow f(x)$  is reducible

Remark

$f(x)$  has a root, then  $f(x)$  is reducible

$f(x)$  is irreducible  $\Rightarrow f(x)$  has <sup>لا يوجد</sup> no root

Example :  $f(x) = x^2 + 1 \in \mathbb{R}[x]$

$f(x)$  is irreducible  $\Rightarrow f(x)$  has no roots

Remark : if  $f(x)$  is reducible poly., then it is not

necessary that  $f(x)$  has root. <sup>لا يعني ان يكون له جذور</sup>

Example : let  $f(x) = x^4 + 5x^2 + 4 \in \mathbb{R}[x]$  <sup>ولكن لا يتحقق</sup>

$f(x)$  is reducible, since  $f(x) = (x^2+1)(x^2+4)$ . <sup>فيمكن ان نقسم</sup>

But  $f(x)$  has no root in  $\mathbb{R}$  because  $\forall x \in \mathbb{R}, f(x) \geq 4$

i.e.  $\nexists x \in \mathbb{R}$  s.t.  $f(x) = 0$

Remark : let  $F$  be any field,  $f(x) \in F[x]$ ,  $\deg f(x) = 2$

or 3. Then  $f(x)$  has root  $\Leftrightarrow f(x)$  is reducible.

Proof

$\Rightarrow$  <sup>مماثل</sup>

$\Leftarrow$ ) If  $\deg f(x) = 3$ ,  $f(x)$  is reducible

$\Rightarrow \exists g(x), h(x)$  of poly's s.t.  $f(x) = g(x)h(x)$

$$3 = \deg f(x) = \deg g(x) + \deg h(x)$$

$\Rightarrow \deg g(x) = 1, \deg h(x) = 2$  or  $\deg g(x) = 2, \deg h(x) = 1$

Case ①  $\deg g(x) = 1$  and  $\deg h(x) = 2$

$$g(x) = ax + b, a \neq 0$$

$\Rightarrow g(x)$  has a root,  $c = -b/a$  that is  $g(c) = 0$

$$\text{Hence } f(c) = g(c)h(c) = 0 \cdot h(c) = 0$$

$\Rightarrow c$  is a root of  $f(x)$

شبهاً في

Similarly Case ②  $\deg f(x) = 2 \Rightarrow \deg g(x) = 1,$

$$\deg h(x) = 1$$

أو

Theorem: Let  $F$  be a field. Then the following are equivalent:

①  $f(x)$  is irreducible poly. in  $F[x]$

②  $\text{id}(f(x))$  is max. (prime) ideal in  $F[x]$

③  $F[x]/\text{id}(f(x))$  is a field.

proof ①  $\Rightarrow$  ②

$F$  is a field  $\Rightarrow F[x]$  is a PID

Then any non trivial ideal in  $F[x]$  is max  $\iff$  it is Prime.  
To prove that  $I = \text{id}(f(x))$  is max.

Suppose  $\exists$  ideal  $J$  in  $F[x]$  s.t.  $I \subsetneq J \subsetneq F[x]$ .

Since  $F[x]$  is PID,  $\therefore \exists g(x) \in F[x]$  s.t.

$$\text{id}(g(x)) = J$$

$\therefore \text{id}(f(x)) \subsetneq \text{id}(g(x)) \subsetneq F[x]$ , since  $f(x) \in \text{id}(f(x))$

$$\therefore f(x) \in \text{id}(g(x)) \implies f(x) = h(x)g(x) \quad \begin{matrix} \xrightarrow{\text{if } x \in \text{id}(f(x))} \\ x = f(x) \end{matrix}$$

q.p.  $h(x) = c \neq 0$  (Constant)

$$\therefore f(x) = cg(x) \implies g(x) = c^{-1}f(x) \in \text{id}(f(x))$$

$$\implies J = \text{id}(g(x)) \subseteq \text{id}(f(x)) \quad \text{C!}$$

Thus  $h(x)$  is a poly of deg  $> 1$

$$\therefore f(x) = h(x)g(x) \quad \text{C! وهذا يناقض الفرض عليه وإلا!}$$

$$\textcircled{2} \implies \textcircled{3} \quad \text{id}(f(x)) \text{ is max ideal} \implies F[x]/\text{id}(f(x)) \text{ is field}$$

$$\textcircled{3} \implies \textcircled{1} \quad \text{C! Multiples}$$

$F[x]/\text{id}(f(x))$  field  $\implies f(x)$  is irreducible in  $F[x]$

Suppose  $f(x)$  is reducible

$$\exists g(x), h(x) \in F[x] \text{ of positive degree s.t. } f(x) = g(x)h(x) \quad \text{C!}$$

$$\text{id}(f(x)) \subsetneq \text{id}(g(x)) \subsetneq F[x] \implies \text{id}(f(x)) \text{ is not max}$$

$$\therefore F[x]/\text{id}(f(x)) \text{ is not field C!}$$

# الفصل الثامن

# والتاسع

# Chapter Eight and Nine

# Chapter eight

- 55 -

"8"

مقدمة النظرية

## Introduction to Galois theory

گالواس

في البداية سوف نذكر تعريف الحقل

Definition :

let  $F \neq \emptyset$ . Then  $(F, +, \cdot)$  is called field if every element  $a \in F$ ,  $a$  is an invertible element.

Examples :  $(\mathbb{I}, +, \cdot)$ ,  $(\mathbb{R}, +, \cdot)$  و  $(\mathbb{Q}, +, \cdot)$

$(\mathbb{Q}[\sqrt{2}], +, \cdot)$ , where  $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$

Definition :

let  $(F, +, \cdot)$ ,  $(K, +, \cdot)$  be two fields s.t.  $F \subseteq K$ . Then  $F$  is called a subfield of  $K$ .

Remark :

let  $(F, +, \cdot)$  be a field and let  $\emptyset \neq S \subseteq F$ . Then  $(S, +, \cdot)$  is a subfield of  $F \iff$

- (1)  $a - b \in S$
  - (2)  $a \cdot b^{-1} \in S$
- }  $\forall a, b \in S$

Example :

$\mathbb{Q}[\sqrt{2}]$  is a subfield of  $\mathbb{R}$

let  $a + b\sqrt{2}$ ,  $c + d\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$

$(a + b\sqrt{2}) - (c + d\sqrt{2}) = (a - c) + (b - d)\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$

$(a + b\sqrt{2}) \cdot (c + d\sqrt{2})^{-1} \in \mathbb{Q}[\sqrt{2}]$

Definition: let  $F$  be a subfield of (the field)  $K$ . Then

$K$  is called an extension of  $F$ .  
توسيع

Definition:

let  $f(x) \in F[x]$ . Define

$$S(F, f) = \{K : K \text{ is an extension of } F \text{ and contains all roots of } f(x)\}.$$

And

$$R_L(F, f) = \bigcap \{K : K \in S(F, f)\}$$

Examples:

(1) let  $f(x) = x^2 - 2 \in \mathbb{Q}[x]$

$\pm\sqrt{2}$  are roots of  $f(x)$

$$\therefore R_L(\mathbb{Q}, f) = \mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$$

(2) let  $f(x) = x^2 + 1 \in \mathbb{Q}[x]$

$\pm i$  are roots of  $f(x)$

$$\therefore R_L(\mathbb{Q}, f) = \mathbb{Q}[i] = \{a + ib : a, b \in \mathbb{Q}\}$$

Definition: let  $K$  be an extension of a field  $F$ .  $K$  is called a normal extension of  $F$ , if  $\exists$

$$f(x) \in F[x] \text{ s.t. } R_L(F, f) = K.$$

Ex 8-

$\mathbb{Q}[\sqrt{2}]$  is a normal extension of  $\mathbb{Q}$

since  $\exists f(x) = x^2 - 2 \in \mathbb{Q}[x] \ni R_L(\mathbb{Q}, f) = \mathbb{Q}[\sqrt{2}]$

Definition : poly. القابلة للحل بواسطة الجذور  
 نسبة الامور من  $\mathbb{Q}$  الى  $\mathbb{Q}$

let  $f(x) \in F[x]$ ,  $K = R_L(F, f)$

$f(x)$  is called solvable by radical if  $\exists$  a finite sequence  
 قابلة للحل بواسطة الجذور

$$F = L_0 \subseteq L_1 \subseteq L_2 \subseteq \dots \subseteq L_n = K$$

اصغر  
مقل جزئي شوي  
على الشكل

where  $L_i = R_L(L_{i-1}, f_i)$ ,  $f_i(x) = x^{n_i} - a_i$

Example : let  $f(x) = ax + b \in F[x]$ ,  $a \neq 0$

$$x = -\frac{b}{a} \text{ جذر الدالة}$$

$$L_0 = R_L(F, f) = \mathbb{Q}$$

$$F = L_0 = R_L(F, f) = \mathbb{Q}$$

$f(x)$  is solvable by radical

Example : - let  $f(x) = ax^2 + bx + c \in \mathbb{Q}[x]$

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

$$\mathbb{Q} = L_0 \subseteq L_1 = R_L(\mathbb{Q}, f_1) \text{ where } f_1 = x^2 - a_1 = x^2 - b$$

Definition : let  $f(x) \in F[x]$ ,  $K = R_t(F, P)$ . Then  
 $gp(G(K/F), 0)$  is called Galois gp.  
 زمرة غالوا

## Theorem Fundamental theorem of Galois

المبرهن الاساسي لجالوا

let  $F$  be any field,  $K$  be the normal Extension of  $F$ .

let  $S = \{E : E \text{ is subfield of } K, F \subseteq E\}$ ,

$\bar{S} = \{H : H \text{ subgp of } G(K/F) \text{ and } H \supseteq G(K/E)\}$

let  $\gamma : S \rightarrow \bar{S}$  define by  $\gamma(E) = G(K/E)$ . Then

- (1)  $\gamma$  is (1-1) and onto
- (2)  $E \subseteq E' \Rightarrow \gamma(E') \subseteq \gamma(E)$
- (3)  $E$  is normal Extension of  $F \iff \gamma(E)$  is normal subgp of  $G(K/F)$

(4) if  $E, E'$  are normal extension of  $F$ , then  $E \subseteq E'$

$$\Rightarrow \gamma(E') \setminus \gamma(E) = G(E/E')$$

لا يوجد تقاطع بين المجموعتين

# Modules: - (الموديول) Chapter nine

Def: - Let  $R$  be a ring with identity. An abelian group  $(M, +)$  is called a Left  $R$ -module (or Left  $R$ -module over  $R$ ) if there exists a mapping  $\alpha: R \times M \rightarrow M$  such that  $\alpha(r, m) = rm \ \forall r \in R$  and  $\forall m \in M$  satisfying the following conditions:

$$\textcircled{1} \quad \alpha(r, m_1 + m_2) = \alpha(r, m_1) + \alpha(r, m_2) \text{ OR } r(m_1 + m_2) = rm_1 + rm_2 \quad \forall r \in R \quad \forall m_1, m_2 \in M.$$

$$\textcircled{2} \quad \alpha(r_1 + r_2, m) = \alpha(r_1, m) + \alpha(r_2, m) \text{ OR } (r_1 + r_2)m = r_1m + r_2m \quad \forall r_1, r_2 \in R, \quad \forall m \in M.$$

$$\textcircled{3} \quad \alpha(r_1 r_2, m) = \alpha(r_1, \alpha(r_2, m)) \text{ OR } (r_1 r_2)m = r_1(r_2 m) \quad \forall r_1, r_2 \in R, \quad \forall m \in M.$$

$\textcircled{4}$  if in addition  $1 \cdot m = m \ \forall m \in M$ , then  $M$  is called a unital  $R$ -module.

Examples:  $\textcircled{1}$  Every abelian group with  $+$  is a  $\mathbb{Z}$ -module

$\textcircled{2}$   $\mathbb{Z}_n$  is a  $\mathbb{Z}$ -module  $\forall n \in \mathbb{N}$

$\textcircled{3}$   $\mathbb{Q}$  is a  $\mathbb{Z}$ -module

$\textcircled{4}$  Let  $R$  be a ring then every left ideal  $I$  of  $R$  is a left  $R$ -module.

$\textcircled{5}$   $n\mathbb{Z}$  is a  $\mathbb{Z}$ -module  $\forall n \in \mathbb{N}$

$\textcircled{6}$  Every ring  $R$  can be considered as an  $R$ -module (a module over itself)

Submodules :-

Def :- A non-empty subset  $N$  of an  $R$ -module  $M$  is called a submodule of  $M$  if and only if :-

- ①  $(N, +)$  is a subgroup of  $(M, +)$  and
- ②  $rN \subseteq N \quad \forall r \in R$ .

Remark :- Let  $M$  be an  $R$ -module and  $\emptyset \neq N \subseteq M$ . Then  $N$  is a submodule of  $M$  if and only if :-

- ①  $x + y \in N \quad \forall x, y \in N$
- ②  $rx \in N \quad \forall r \in R, \forall x \in N$

Example 5 :-

(1) If  $M$  is an  $R$ -module, then  $\{0\}$  and  $M$  are submodules of  $M$ .

If there is any submodule  $N$  of  $M$  which is different from  $\{0\}$  and  $M$ , then  $N$  is called a proper submodule.

Def :- An  $R$ -module  $M$  is called simple if  $M$  has no proper submodules.

For any prime number  $p$ ,  $\mathbb{Z}_p$  is a simple  $\mathbb{Z}$ -module.

(2) If  $R$  is any ring, then  $R$  is an  $R$ -module and the submodules of  $R$  are just the ideals of  $R$ .

For example :-  $n\mathbb{Z}$  is a submodule of  $\mathbb{Z} \quad \forall n = 0, 1, 2, \dots$

(3)  $\mathbb{Z}$  is a  $\mathbb{Z}$ -module of  $\mathbb{Q}$  over  $\mathbb{Z}$ .

Remark :- (1) If  $N$  and  $K$  are two submodules of an  $R$ -module  $M$ , then  $N \cap K$  is also a submodule.

(b) If  $\{N_i\}_{i \in I}$  is any collection of submodules of an  $R$ -module  $M$ , then  $\bigcap_{i \in I} N_i$  is also a submodule of  $M$ .

المركب (الجزئي) المتولد

Def:

Let  $M$  be an  $R$ -module and let  $x \in M$ , then the submodule of  $M$  generated by  $x$  denoted by  $(x)$ , it is defined to be the intersection of all submodules of  $M$  which contains  $x$ , that is

$$(x) = \bigcap \{N; N \text{ is a submodule of } M \text{ and } x \in N\}$$

The set  $X = (x)$  is called a generating set of  $(x)$ .

Equivalently:  $(x)$  is the smallest submodule of  $M$  containing  $x$ .

If  $X = \{x\}$ , then the submodule of  $M$  generated by  $x$  denoted by  $(x)$ , it is defined to be the set  $\{rx \mid r \in R\} = Rx$ .  $M$  is called a cyclic  $R$ -module if  $M = Rx = (x)$  for some  $x \in M$ .

Examples:

①  $\mathbb{Z}$  as  $\mathbb{Z}$ -module is cyclic since  $\mathbb{Z} = (1)$

②  $E$  is a cyclic submodule of  $\mathbb{Z}$  since  $E = (2)$

In general  $n\mathbb{Z} = (n)$  is cyclic submodule of  $\mathbb{Z}$   $\forall n \in \mathbb{Z}$ .

③  $\mathbb{Z}_n$  is a cyclic  $\mathbb{Z}$ -module since  $\mathbb{Z}_n = (1) \forall n \in \mathbb{Z}$ .

Note: - An  $R$ -module  $M$  is called finitely generated (f.g) if there exists a finite subset  $X$  of  $M$  such that  $M = (x)$  that is,  $M = \sum_{i=1}^n Rx_i = Rx_1 + Rx_2 + \dots + Rx_n$  where  $\{x_1, x_2, \dots, x_n\} \subseteq M$ .

## Homomorphisms on Modules :-

Def :- Let  $M$  and  $N$  be two  $R$ -modules a mapping  $f: M \rightarrow N$  is called an  $R$  homomorphism if :-

- (1)  $f(m_1 + m_2) = f(m_1) + f(m_2) \quad \forall m_1, m_2 \in M$
- (2)  $f(rm) = r f(m) \quad \forall r \in R, \forall m \in M.$

Example :- (1) Let  $M$  and  $N$  be any  $R$ -modules. Let  $f: M \rightarrow N$  be such that  $f(m) = 0_N \quad \forall m \in M$ , then  $f$  is an  $R$ -module,  $f$  is called the trivial homo. from  $M$  into  $N$ .

Sol :- (1)  $\forall m_1, m_2 \in M$  s.t.  $f(m) = 0_N \quad \forall m \in M$   
 $f(m_1 + m_2) = 0_N$  (Def. of  $f$ )  
 $= 0_N + 0_N$   
 $= f(m_1) + f(m_2).$

(2)  $\forall m \in M, r \in R, f(rm) = 0_N = r 0_N$  (since  $M$  is module)  
 $= r f(m).$

(2) Let  $M$  be any  $R$ -module, the identity map.  
 $I_M: M \rightarrow M$  is an  $R$ -homomorphism.  $I_M$  is called the identity homomorphism on  $M$ .

Sol (How)

(3) f  $f(m) = c \quad \forall m \in M$ , then  $f$  is not homo.

since  $f(m_1 + m_2) \neq f(m_1) + f(m_2)$

$c + c \neq c + c$

(4) If  $N$  a submodule of an  $R$ -module  $M$ , the inclusion map  $i_N: N \rightarrow N$  is an  $R$ -homo.

$i_N$  is called the inclusion homo. on  $N$ .

Sol ①  $i_N(m_1 + m_2) = m_1 + m_2 = i_N(m_1) + i_N(m_2) \quad \forall m_1, m_2 \in M$

②  $i_N(rm) = rm = r i_N(m) \quad \forall r \in R, \forall m \in M$

Def:- Let  $N$  be a submodule of an  $R$ -module  $M$  and  
 Let  $M/N = \{x+N, x \in M\}$  where  $x+N = \{x+a : a \in N\}$   
 is the coset of  $N$  determined by  $x$ .

$M/N$  is an  $R$ -module w.r.t  $(+)$  &  $(\cdot)$  defined by:-

(1)  $(x+N) + (y+N) = (x+y) + N \quad \forall x, y \in M$

(2)  $r(x+N) = rx + N \quad \forall r \in R, \forall x \in M$

Show that  $M/N$  is an  $R$ -module  $M/N$  is called the quotient module of  $M$  determined by  $N$ .

Example:- If  $N$  is a submodule of an  $R$ -module  $M$ , the  
 natural map  $\pi: M \rightarrow M/N$  such that  
 $\pi(m) = m + N \quad \forall m \in M$ ,  $\pi$  is an  $R$ -homo. It is called  
 the natural homo.

Sol:- (1)  $\pi(m_1 + m_2) = (m_1 + m_2) + N = (m_1 + N) + (m_2 + N) = \pi(m_1) + \pi(m_2)$   
 $\forall m_1, m_2 \in M$

(2)  $\pi(rm) = rm + N = r(m + N) = r\pi(m)$   
 $\forall r \in R, \forall m \in M$

Def:- Let  $f: M \rightarrow N$  be an  $R$ -homo.

(1) Kernel of  $f$  denoted by  $\text{Ker} f$ , it is the set  
 $\text{Ker} f = \{x \in M : f(x) = 0\} \subseteq M$

(2) The image of  $f$  denoted by  $\text{Im} f$ , it is the set  
 $\text{Im} f = \{f(x) : x \in M\} \subseteq N$

Remark:- (1)  $\text{Ker} f$  is a submodule of  $M$ .

Let  $f: M \rightarrow N$  be an  $R$ -homo. then

- ①  $f(0) = 0$ , ②  $f(x) = f(x)$  ③  $f(x-y) = f(x) - f(y)$   
 $\forall x, y \in M$ .

Def:- Let  $f: M \rightarrow N$  be an  $R$ -homo.

- (1)  $f$  is called a monomorphism if and only if  $f$  is 1-1.  
 (2)  $f$  is called an epimorphism if and only if  $f$  is onto.  
 (3)  $f$  is called an isomorphism if and only if  $f$  is 1-1 and onto.

## ("The Fundamental theorems of Homomorphism")

Theorem (1):- If  $f: M \rightarrow N$  is an  $R$ -homo, then

$$M/\text{Ker } f \cong \text{Im } f$$

proof:- Define  $g: M/\text{Ker } f \rightarrow \text{Im } f$  such that  
 $g(x + \text{Ker } f) = f(x) \quad \forall x \in M$ .

T.P.  $g$  is well-defined?

Let  $x_1 + \text{Ker } f = x_2 + \text{Ker } f$  in  $M/\text{Ker } f$ .

$$\Rightarrow x_1 - x_2 \in \text{Ker } f$$

$$\Rightarrow f(x_1 - x_2) = 0 \quad (\text{define of Ker } f).$$

$$\Rightarrow f(x_1) - f(x_2) = 0 \quad (\text{define of homo}).$$

$$\Rightarrow f(x_1) = f(x_2)$$

$$\Rightarrow g \text{ is well-defined.}$$

T.P.  $g$  is homo?

Let  $m_1 + \text{Ker } f, m_2 + \text{Ker } f \in M/\text{Ker } f$

$$\begin{aligned} \textcircled{1} \quad g[(m_1 + \text{Ker } f) \oplus (m_2 + \text{Ker } f)] &= g[(m_1 + m_2) + \text{Ker } f] = f(m_1 + m_2) \\ &= f(m_1) \oplus f(m_2) \\ &= g(m_1 + \text{Ker } f) \oplus g(m_2 + \text{Ker } f) \end{aligned}$$

②  $\forall r \in R, m + \text{Ker } f \in M/\text{Ker } f$

$$g[r(m + \text{Ker } f)] = g(rm + \text{Ker } f) = f(rm) = r f(m) \quad (\text{fishaw})$$

$$g(m + \ker f)$$

Thus  $g$  is homo.

T.P  $g$  is 1-1?

Let  $m_1 + \ker f, m_2 + \ker f \in M/\ker f$  such that:

$$g(m_1 + \ker f) = g(m_2 + \ker f)$$

$$f(m_1) = f(m_2)$$

$$f(m_1) - f(m_2) = 0$$

$$f(m_1 - m_2) = 0 \quad \text{since } f \text{ is homo.}$$

$$m_1 - m_2 \in \ker f \Rightarrow m_1 + \ker f = m_2 + \ker f.$$

$\therefore g$  is 1-1

T.P  $g$  is on to?

Let  $y$  be any element of  $N$

$$\because f \text{ is on to} \Rightarrow \exists x \in M \text{ s.t. } f(x) = y$$

$$\Rightarrow g(x + \ker f) = y$$

$\therefore g$  is on to.

Corollary: - If  $f: M \rightarrow N$  is an epimorphism, then  $M/\ker f \cong N$

Theorem (2): - If  $K$  and  $L$  are two submodules of an  $R$ -module  $M$ . Then  $K/L \cap K \cong K+L/L$

proof: - Define  $f: K \rightarrow (K+L)/L$  s.t.  $f(x) = x+L \quad \forall x \in K$

$$\forall x \in K \Rightarrow x+0 \in K+L \Rightarrow x+L \in (K+L)/L$$

$$\text{If } x_1 = x_2 \Rightarrow x_1+L = x_2+L \Rightarrow f(x_1) = f(x_2)$$

$\therefore f$  is well-defined.

T.P  $f$  is homo?

(i) Let  $x_1, x_2 \in K$

$$f(x_1 + x_2) = (x_1 + x_2) + L = (x_1 + L) + (x_2 + L) = f(x_1) + f(x_2)$$

2) Let  $x \in R \wedge z \in K$ ,  $f(rx) = rx + L = r(x + L) = r f(x)$   
 $\therefore f$  is homo.

T.P  $f$  is onto?

Let  $(x+L) + L \in (K+L)/L$  where  $x \in K \wedge y \in L$   
 $(x+y)+L = (x+L) + (y+L) = (x+L) + L = x+L = f(x)$

$\therefore f$  is onto.

By Theorem (1)  $\Rightarrow K/\text{Ker } f \simeq (K+L)/L$

T.P  $\text{Ker } f = L \cap K$ ?

$$\begin{aligned} \text{Ker } f &= \{x \in K : f(x) = 0\} \\ &= \{x \in K : x+L = L\} \\ &= \{x \in K \wedge x \in L\} = K \cap L \end{aligned}$$

Therefore  $K/L \cap K \simeq K+L/L$ .

Theorem (3) :- If  $K$  and  $L$  are two submodules of an  $R$ -module  $M$  and  $K \subseteq L$ , then :-

(1)  $L/K$  is a submodule of  $M/K$ .

(2)  $M/K / L/K \simeq M/L$

Proof :- ① T.P  $L/K \subseteq M/K$ ?

$$\text{Let } L/K = \{a+K, a \in L\}$$

$$M/K = \{m+K, m \in M\}$$

$$0+K \in L/K, 0 \in L \Rightarrow L/K \neq \emptyset$$

$$\forall a+K \in L/K \Rightarrow a+K \in M/K \text{ (since } L \subseteq M)$$

$$\therefore L/K \subseteq M/K$$

$$\forall a_1+K, a_2+K \in L/K$$

$$(a_1+K) + (a_2+K) = (a_1+a_2)+K \in L/K \text{ (since } a_1+a_2 \in L)$$

$$\forall r \in R, \forall a+K \in L/K \text{ T.P } r(a+K) \in L/K?$$

$$r(a+K) = ra+K \in L/K \text{ (since } L \subseteq M)$$

$$\therefore r(m+K) \in L/K$$

$\therefore L/K$  is a submodule of  $M/K$ .

(2) Define  $f: M/K \rightarrow M/L$  s.t.  $f(m+K) = m+L$   
 $\forall m \in M$ .

T.P.  $f$  is well defined?

$$\forall m+K \in M/K \Rightarrow m+L \in M/L \Rightarrow f(m+K) \in M/L$$

$$\forall m_1+K = m_2+K \Rightarrow m_1-m_2 \in K \Rightarrow m_1-m_2 \in L$$

$$\Rightarrow m_1+L = m_2+L$$

$$\Rightarrow f(m_1+K) = f(m_2+K)$$

T.P.  $f$  is homo?

$$\textcircled{1} \forall m_1+K, m_2+K \in M/K \Rightarrow f[(m_1+K) \oplus (m_2+K)] = f[(m_1+m_2)+K]$$

$$= (m_1+m_2)+L = (m_1+L) + (m_2+L)$$

$$= f(m_1+K) + f(m_2+K)$$

$$\textcircled{2} f[r(m+K)] = f[rm+K] \text{ (since } M \text{ is an } R\text{-module)}$$

$$= rm+L = r(m+L) = rf(m+K)$$

$\therefore f$  is homo.

T.P.  $f$  is onto?

$$\text{Im } f = \{ f(m+K) : m \in M \}$$

$$= \{ m+L : m \in M \} = M/L$$

$\therefore f$  is onto.

$$\text{By Theorem 4} \Rightarrow M/\text{Ker } f \simeq M/L$$

$$\text{T.P. } \text{Ker } f = L/K$$

$$\text{Ker } f = \{ (m+K) \in M/K : f(m+K) = L \}$$

$$= \{ (m+K) \in M/K : m+L = L \}$$

$$= \{ m+K \in M/K : m \in L \} = L/K$$

$$\therefore M/K / L/K \simeq M/L$$

الحسن فضل

الكرديبولات

- Study on Group, Ring, Module, Vector Space
- Study on Commutative Algebra (Prof. Dr. V. S. Varadarajan, 1998)
- Foundations of Module and Ring Theory by R. S. Varadarajan (1998)
- Commutative Theory of Ideals (Prof. Dr. V. S. Varadarajan)
- Algebraic Modules (Prof. Dr. V. S. Varadarajan)

## Theory of Modules

Def: Let  $R$  be a ring with identity. An abelian group  $(M, +)$  is called a left  $R$ -module (or left  $R$ -module over  $R$ ) if there exists a mapping

$$R \times M \rightarrow M \text{ s.t. } \alpha(r, m) = rm \quad \forall r \in R \text{ and } m \in M,$$

satisfying the following conditions:

- ①  $\alpha(r_1 + r_2, m) = \alpha(r_1, m) + \alpha(r_2, m)$  OR  $(r_1 + r_2)m = r_1m + r_2m \quad \forall r_1, r_2 \in R \text{ and } m \in M$
- ②  $\alpha(r_1, m_1 + m_2) = \alpha(r_1, m_1) + \alpha(r_1, m_2)$  OR  $(r_1 + r_2)m = r_1m + r_2m \quad \forall r_1, r_2 \in R \text{ and } m \in M$

(2)

$$(3) \quad \alpha(r_1 r_2, m) = r_1 \alpha(r_2, m) \text{ or } (r_1 r_2) m = r_1 (r_2 m) \quad \forall r_1, r_2 \in R, \forall m \in M.$$

(4) If in addition  $1 \cdot m = m \quad \forall m \in M$ . Then  $M$  is called a unital  $R$ -module.

Note:-

One can be define right  $R$ -module similarly. That is An additive abelian group  $M$  is called a right  $R$ -module, if there exists a mapping  $M \times R \rightarrow M$  with  $(m, r) \rightarrow mr \quad \forall m \in M, \forall r \in R$  satisfying :-

$$\left. \begin{array}{l} (1) \quad m(r_1 + r_2) = mr_1 + mr_2 \\ (2) \quad (m_1 + m_2)r = m_1 r + m_2 r \\ (3) \quad m(r_1 r_2) = (mr_1)r_2 \\ (4) \quad m \cdot 1 = m \end{array} \right\} \begin{array}{l} \forall r, r_1, r_2 \in R \wedge \\ \forall m, m_1, m_2 \in M. \end{array}$$

Remark :- If  $R$  is a comm. ring, then every left  $R$ -module can be made into a right  $R$ -module.

Def:- Let  $R$  be a ring with identity and let  $M$  be a left  $R$ -module.  $M$  is called a unital (or, a unitary) left  $R$ -module, if  $1 \cdot m = m \quad \forall m \in M$ .  
(i.e.  $(1, m) \rightarrow m \quad \forall m \in M$ )

Examples:-

(1) Every additive abelian group is a  $\mathbb{Z}$ -module.

Solution:- Let  $(M, +)$  be an abelian gp.

Define a mapping  $\phi: \mathbb{Z} \times M \rightarrow M$  s.t

$\phi(n, a) = na$  where

$$na = \begin{cases} a + a + \dots + a & (n\text{-times}) \text{ if } n > 0 \\ (-a) + (-a) + \dots + (-a) & (n\text{-times}) \text{ if } n < 0 \end{cases}$$

(3)

Now, we satisfying the conditions: .

$$(i) \phi(n, a_1 + a_2) = n(a_1 + a_2)$$

$$= \begin{cases} (a_1 + a_2) + \dots + (a_1 + a_2) & (n\text{-times}) \\ & \text{if } n > 0 \\ -(a_1 + a_2) + \dots + -(a_1 + a_2) & (n\text{-times}) \\ & \text{if } n < 0 \end{cases}$$

$$= \begin{cases} \underbrace{a_1 + a_1 + \dots + a_1}_{n\text{-times}} + \underbrace{a_2 + a_2 + \dots + a_2}_{n\text{-times}} \\ \underbrace{(-a_1) + (-a_1) + \dots + (-a_1)}_{n\text{-times}} + \underbrace{(-a_2) + \dots + (-a_2)}_{n\text{-times}} \end{cases}$$

$$= na_1 + na_2$$

$$= \phi(n, a_1) + \phi(n, a_2)$$

وہذا ثابت ہے کہ یہ شرطیں پوری ہوتی ہیں۔

(2) Every ring  $R$  is an  $R$ -module.

(since every ring is an abelian gp  $(R, +)$  is abelian gp and itself ring. Thus is an  $R$ -module).

(3) Every <sup>left</sup> ideal of  $R$  is an  $R$ -module.

Sol: Since  $(I, +)$  is abelian gp and

$$ra \in I, \forall r \in R, \forall a \in I$$

یہ ہر ایلیمینٹ کے لیے درست ہے اور اس لیے  $I$  ایک لیفٹ آئیڈیل ہے۔

$$(i) (r, a_1 + a_2) = r(a_1 + a_2) = \underbrace{ra_1}_{\in I} + \underbrace{ra_2}_{\in I} = \alpha(r, a_1) + \alpha(r, a_2)$$

$$\forall r \in R, \forall a_1, a_2 \in I$$

$$(ii) (r_1 + r_2, a) = (r_1 + r_2)a = r_1a + r_2a = \alpha(r_1, a) + \alpha(r_2, a)$$



(5)

For example: - Take  $R = \mathbb{Z}$ ,  $I = n\mathbb{Z} \Rightarrow R/I = \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$  is a  $\mathbb{Z}$ -module.

(6) Let  $R$  be a ring. Then  $M_{m \times n}(R)$  is an abelian gp with respect to addition of matrices.

Define:  $\alpha: M_{m \times n}(R) \times M_{m \times n}(R) \rightarrow M_{m \times n}(R)$  s.t

$\alpha(A, B) = AB$  (multiplication of matrices).  $\forall A, B \in M_{m \times n}(R)$

Then  $M_{m \times n}(R)$  is a left  $M_{m \times n}(R)$ -module.

Similarly,  $M_{m \times n}(R)$  is a right  $M_{m \times n}(R)$ -module.

$\therefore$   $\rho, m=1$   $\Rightarrow$   $\alpha$  is a map  $M_{m \times n}(R) \times M_{m \times n}(R) \rightarrow M_{m \times n}(R)$

$M_{1 \times n}(R)$  = The set of all  $1 \times n$  matrices (or set of all  $n$ -tuples) of a ring  $R$ , namely,

$R^n = \{(a_1, \dots, a_n) : a_i \in R, i=1, \dots, n\}$  and

$R \times R^n \rightarrow R^n$  such that  $r(a_1, \dots, a_n) = (ra_1, \dots, ra_n)$   
 $\forall r \in R, \forall (a_1, \dots, a_n) \in R^n$ .

$R^n$  is an  $R$ -module.

(7) Let  $R$  and  $S$  be two rings and let  $f: R \rightarrow S$  be any ring homo.

Let  $M$  be an  $S$ -module. Then  $M$  is also an  $R$ -module.

Pf Since  $M$  is an  $S$ -module, then  $(M, +)$  is an abelian gp. and  $\exists$  a map  $\alpha: S \times M \rightarrow M$  s.t  $\alpha(s, m) \rightarrow sm$   $\forall s \in S \forall m \in M$  satisfying 1, 2, 3, 4 in the def.

Define  $\beta: R \times M \rightarrow M$  s.t  $\beta(r, m) = r \cdot m$

$\vee \beta(r, m) = f(r)m, \forall m \in M$

⑥

Sol:

(i) Let  $r \in R, m_1, m_2 \in M$ .

$$(r, m_1 + m_2) = f(r) \cdot (m_1 + m_2) = f(r)m_1 + f(r)m_2 \\ = (r, m_1) + (r, m_2)$$

$f(r) \in S, r \in R, m_1, m_2 \in M$ .

(ii) Let  $r_1, r_2 \in R, m \in M$

$$(r_1 + r_2, m) = f(r_1 + r_2) \cdot m = [f(r_1) + f(r_2)]m \quad (\text{homo def}) \\ = f(r_1)m + f(r_2)m \\ = (r_1, m) + (r_2, m)$$

(iii) check

④ Since  $R$  is a ring with unity  $\Rightarrow \exists 1$  is an identity element

But  $f$  is homo  $\Rightarrow f(1) = \hat{1}$  the identity element of  $S$ .

Now,  $\forall m \in M \Rightarrow (1, m) = f(1) \cdot m = \hat{1} \cdot m = m$ .

Thus  $M$  is an  $R$ -module.

⑧ Let  $M$  be an additive abelian group and let  $\text{End}(M)$  = The set of all group homomorphisms on  $M$ .

i.e  $\text{End}(M) = \{f \mid f: M \rightarrow M, f \text{ is a group homo.}\}$

Define:  $+$  and  $\circ$  on  $\text{End}(M)$  as follows:-

$$(f+g)(m) = f(m) + g(m) \quad \forall f, g \in \text{End}(M), \forall m \in M.$$

$$(f \circ g)(m) = f(g(m)) \quad \forall f, g \in \text{End}(M), \forall m \in M.$$

Then:- (1)  $(\text{End}(M), +, \circ)$  is a ring with identity

(2)  $M$  is an  $\text{End}(M)$ -module.?

7

Pf: (1) T.P.  $(\text{End}(M), +)$  is an abelian gp?

(i) Let  $f, g \in \text{End}(M)$

$$= f(m) + g(m) = f + g(m) \quad \forall f, g \in \text{End}(M) \\ \forall m \in M.$$

Thus  $+$  is closed.

(ii) Let  $f, g, h \in \text{End}(M)$ :

$$\begin{aligned} ((f+g)+h)(m) &= (f+g)^{(m)} + h(m) \\ &= (f(m) + g(m)) + h(m) \\ &= f(m) + (g(m) + h(m)) \\ &= (f + (g+h))(m) \end{aligned}$$

Therefore  $+$  is ass.

كذلك لا فرق واجب

$\therefore (\text{End}(M), +)$  is an abelian gp.

(2) Define:  $\phi: \text{End}(M) \times M \rightarrow M$  s.t

$$\phi(f, m) = f(m) \quad \forall f \in \text{End}(M), \forall m \in M.$$

Pf: (i) Let  $f \in \text{End}(M), \wedge m_1, m_2 \in M$

$$\begin{aligned} (f, m_1 + m_2) &= f(m_1 + m_2) = f(m_1) + f(m_2) \\ &= (f, m_1) + (f, m_2) \quad (\text{since } f \text{ is homo.}) \end{aligned}$$

$$\begin{aligned} \text{(ii)} \quad (f+g, m) &= (f+g)(m), \quad \forall f, g \in \text{End}(M), \forall m \in M \\ &= f(m) + g(m) \\ &= (f, m) + (g, m) \end{aligned}$$

(iii) Let  $f, g \in \text{End}(M), m \in M$ .

$$\begin{aligned} (f \circ g, m) &= (f \circ g)(m) = f(g(m)) = (f, g(m)) \\ &= (f, g, m) \end{aligned}$$

(8)

(VI)

Since  $(I, m) = I(m) = m$  where  $I$  is the identity map.

Thus

$M$  is  $\text{End}(M)$ -module.

Def:- Let  $R$  and  $S$  be two rings and let  $M$  be an additive abelian gp.  $M$  is called an  $R$ - $S$ -bimodule if  $M$  is a left  $R$ -module and a right  $S$ -module, and  $r(ms) = (rm)s$  for all  $r \in R$ ,  $s \in S$ ,  $m \in M$ .

Ex:-  $M(R)$  is an  $M_{m \times n}(R) - M_{n \times m}(R)$ -bimodule.

row = column اگر صفیں برابر ہوں

Def:-

Let  $M$  be an  $R$ -module. The left annihilator of  $M$  over  $R$  denoted by  $\text{ann}_R(M)$  (or  $\text{ann } M$ ), and, it is defined by:

$$\text{ann}_R(M) = \{r \in R : rm = 0, \forall m \in M\}$$

Note:- If  $\text{ann}_R(M) = 0$ , then  $M$  is called a faithful  $R$ -module.

Remark:- Let  $M$  be an  $R$ -module. Then:-

$$1 - r \cdot 0_M = 0_M \quad \forall r \in R$$

$$2 - 0_R \cdot m = 0_M \quad \forall m \in M$$

$$3 - (-r)m = -(rm) = r(-m) \quad \forall r \in R, \forall m \in M$$

(9)

Pf:- (1)  $0_R \cdot m = (0 + 0)_R \cdot m = 0 \cdot m + 0 \cdot m$  (المعنى)  
 بالتعريف،  $0 \cdot m + (- (0 \cdot m)) = 0 \cdot m + 0 \cdot m + (- (0 \cdot m))$   
 $0 = 0 \cdot m$

(2)  $r \cdot 0_M = r \cdot (0 + 0)_M = r \cdot 0 + r \cdot 0$

$r \cdot 0 + (- (r \cdot 0)) = r \cdot 0 + (r \cdot 0 + (- (r \cdot 0)))$

(3)  $(-r)m + rm = (-r + r)m$

$= 0 \cdot m$

$= 0$  by (1)

Thus  $-(rm)$  is the inverse of  $(r)m$

i.e.  $-(rm) = -(r)m$

Remark:- If  $M$  is a  $R$ -module, then

(1)  $\text{ann } M$  is a left ideal of  $R$ .

(2)  $M_R$  is a faithful  $R/\text{ann } M$ -module.

Pf Exercise.

Remark:- Let  $M$  be an  $R$ -module and  $I$  be an ideal of  $R$ . If  $I \subseteq \text{ann } M$ , then  $M$  is an  $R/I$ -module.

Pf:- Define  $\phi: R/I \times M \rightarrow M$  s.t.:

$\phi(r+I, m) = rm \quad \forall r+I \in R/I, \forall m \in M$

$\phi$  is an mapping?

Let  $(r+I, m_1) = (b+I, m_2)$  in  $R/I \times M$ .

$\Rightarrow r+I = b+I \wedge m_1 = m_2$  هذا من تعريف المساواة

$r+b \in I$

(10)

$$\Rightarrow b-a \in \text{ann } M \Rightarrow (a-b)m = 0 \quad \forall m \in M$$

$$\Rightarrow am - bm = 0$$

$$am = bm$$

$$\phi(a+I, m) = \phi(b+I, m)$$

$\therefore \phi$  is well-defined.

برهان شرط لا غریبی واجب

Ex:  $\mathbb{Z}_6$  is a  $\mathbb{Z}_3$ -module. since

$$\text{ann } \mathbb{Z}_6 = 6\mathbb{Z} \subseteq 3\mathbb{Z} = I$$

$\therefore \mathbb{Z}_6$  is a  $\mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}_3$ -module.

## Submodules

~~~~~

Def: Let  $M$  be an  $R$ -module. A non-empty subset  $N$  of  $M$  is called a submodule of  $M$  (or an  $R$ -submodule of  $M$ ) if and only if:

$$(1) \quad a-b \in N \quad \forall a, b \in N$$

$$(2) \quad \forall a \in N \quad \forall \alpha \in N, \forall r \in R.$$

شرط من خوار لیفتی است:

(شرط اول: یعنی  $(N, +)$  زیره جزئی من زیره  $(M, +)$ )

(شرط ثانی: یعنی  $\alpha$  اکتال  $R \times M \rightarrow M$  تم اقتضا می کند  $R \times N$

فان  $(f: R \times N \rightarrow N)$ .

ایان پودول الجزئی من پودول  $M$  هوقه پودول علی نفسی کلمه.

Remark: Let  $M$  be an  $R$ -module and  $\phi \neq \emptyset \subseteq M$ .

Then  $N$  is a submodule of  $M$  if and only if

$$ra + sb \in N \quad \forall a, b \in N, \forall r, s \in R$$