جبر الحلقات

Ring Theory

المرحله الثالثه

الهيئه التدريسيه

ا.م.د. حاتم يحيى خلف

م.د. غالب احمد حمود

2019-2020

الفصل الاول

« Ring Theorey »

Concents

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 polynomail - 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.

Refernces : المصادر

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

2- مقدمة في الجبر المجرد : تأليف د. لبنى سلمان محمود و د. محمد عبد الرزاق

3- ملزمة نظرية الحلقات : تأليف د. عادل عثمان نعوم و د. باسل 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:

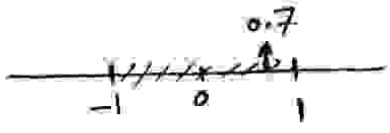
1. $(R, +)$ is an abelain group, that is
   a. $+$ is closed on R
   b. $+$ is associative
   c. $\forall a \in R$, $\exists$ an element $0 \in R$ s.t. $a + 0 = a$, 0 is called the zero element.
   d. $\forall a \in R$, $\exists -a \in R$ s.t. $a + (-a) = 0$, $-a$ is called the additive inverse of a.
   e. $+$ is Commutative.

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

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

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:

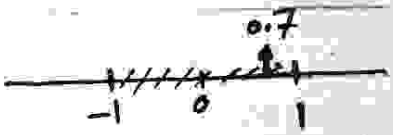
1. $(R, +)$ is an abelain group, that is
   a. $+$ is closed on R
   b. $+$ is associative
   c. $\forall a \in R$, $\exists$ an element $0 \in R$ s.t. $a + 0 = a$, 0 is called the zero element.
   d. $\forall a \in R$, $\exists -a \in R$ s.t. $a + (-a) = 0$, $-a$ is called the additive inverse of a.
   e. $+$ is commutative.

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

Examples

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

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 $a.b=b.a \quad \forall a,b\in R$.

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

Examples:

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

2. let $R=M_{n\times n}(\mathbb{R})=\left\{\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ \vdots & & & \\ a_{n1} & a_{n2} & \cdots & a_{nn}\end{bmatrix} ; a_{ij}\in\mathbb{R} \ \forall i,j=1,\ldots,n\right\}$ be the set of all metrices nxn 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. $A+B=(a_{ij}+b_{ij})_{n\times n}\in M_{n\times n}(\mathbb{R})$ is Comm. gp.

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

$$I_n=\begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 0 & \cdots & 1\end{pmatrix}_{n\times n}\in M_{n\times n}(\mathbb{R})$$

Class

$A \cdot I_n = I_n \cdot A = A \qquad \forall A \in M_{n\times n}$

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

3. $(Ze, +, \cdot)$ 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 $P(X) = \{\emptyset, \{1\}, \{2\}, X\}$
Δ is closed on $P(X)$ and $\cap$ is Comm. and associa.

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

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

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 $Z[\sqrt{3}] = \{a + b\sqrt{3} : a, b \in Z\}$. Define $+, \cdot$ on $Z[\sqrt{3}]$ 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

$A \cdot I_n = I_n \cdot A = A \qquad \forall A \in M_{n\times n}$

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

3. $(2\mathbb{Z}_e, +, \cdot)$ is Comm. ring without identity

4. let X be a non-empty set. Then $(\mathcal{P}(X), \Delta, \cap)$ 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 $\mathcal{P}(X) = \{\emptyset, \{1\}, \{2\}, X\}$
Δ is closed on $\mathcal{P}(X)$ and $\cap$ is Comm. and associa.

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

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

Therefore $(\mathcal{P}(X), \Delta, \cap)$ 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 $+, \cdot$ 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 $C[0,1] = \{f : [0,1] \longrightarrow \mathbb{R}\}$ which are Countinuas s.t. $(f+g)_{(x)} = f(x) + g(x)$ and

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

Thus

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

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

Special Case: $(Z_4, +_4, \cdot_4)$ is Comm. ring with identity 1.

o ——— o

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. $a \cdot (b-c) = a \cdot b - b \cdot c$
7. $(a \cdot b) \cdot c = a \cdot c - b \cdot c$
8. If R has unity 1, then
   (i) $(-1)a = -a$
   (ii) $(-1)(-1) = 1$

Proofs

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

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

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

$0 = a \cdot 0$.

4. $(-a)(-b) = -(a(-b))$ by (2)
$= -(-(ab))$ by (2)
$= ab$ by (3)

8. $(-1)a = -(1.a)$ by (2)
$= -a$

Direct Sum of Rings and Some Remarks

الجمع المباشر للحلقات مع بعض الخواص

Definition:

let $(R,+,.)$ and $(R',+',.')$ be any two rings.
let $X = R \times R' = \{(a,b) : a \in R \wedge b \in R'\}$
Define $\oplus, \odot$ on X by:

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

$(a,b) \odot (c,d) = (a.c, b.'d)$.

Then $(X, \oplus, \odot)$ 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 $(R,+,.)$, $(R',+',.')$ are Comm. ring, then the ring of direct sum of R, R' is Comm. ring

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

unity $(1, \hat{1})$

3. If rings $(R, +, \cdot)$, $(R', \hat{+}, \hat{\cdot})$ have unities $1, \hat{1}$ 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:

let $Z_2 \times Z_3 = \{(\bar{0}, \bar{0}), (\bar{0}, \bar{1}), (\bar{0}, \bar{2}), (\bar{1}, \bar{0}), (\bar{1}, \bar{1}), (\bar{1}, \bar{2})\}$

and $(\bar{a}, \bar{b}) \oplus (\bar{c}, \bar{d}) = (\bar{a} +_2 \bar{c}, \bar{b} +_3 \bar{d})$

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

Then $(Z_2 \times Z_3, \oplus, \odot)$ is a ring.

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

النظائر الجمعية

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

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

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

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

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 $(Z_3, +_3, \cdot_3)$, $\bar{0}, \bar{1}, \bar{2}$ are not zero divisors
2. In $(Z_4, +_4, \cdot_4)$, $\bar{0}, \bar{1}, \bar{3}$ are not zero divisors, but $\bar{2}$ is zero divisor, (since $\bar{2} \cdot_4 \bar{2} = \bar{0}$).
3. In $(Z_6, +_6, \cdot_6)$, $\bar{0}, \bar{1}, \bar{5}$ 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.
$\therefore \exists\ a^{-1} \in R$ s.t. $a^{-1} \cdot a = a \cdot a^{-1} = 1$

Class

Suppose a is a zero divisor.

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

$\bar{a}^{-1}.(a.b) = \bar{a}^{-1}.0 \Longrightarrow (\bar{a}^{-1}.a).b = 0$

$\Rightarrow 1.b = 0 \Rightarrow b = 0$ C! (since $b \neq 0$).

Thus a is not zero divisor.

والعلاقة اعلاه مكافئة الى

a is zero divisor $\Longrightarrow$ a is not invertible.

Now, we have the following example:

Example :-

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

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

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 $\Longleftrightarrow \forall a \in R,\ a \neq 0$, $a.b = a.c$ which implies $b = c$.

The Cancellation law holds with respect to multiplication operation

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

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

$a.b + (-ac) = ac + (-ac)$

$a.b - ac = 0 \Longrightarrow a(b-c) = 0$

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 solution $a = 0$ or $a = 1$.

"Integral domain" (حلم)

Definition:- let $(R, +, \cdot)$ be a comm. ring with unity 1. Then R is called an integral domain $\Leftrightarrow$ 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
$\therefore \exists\ m, k \in \mathbb{Z}^+$ s.t. $n = m \cdot k$ $\quad 1 < m < n$, $1 < k < n$
$\Rightarrow \bar{0} = \bar{m} \cdot_n \bar{k}$ and $\bar{m}, \bar{k}$ 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
$\exists\ \bar{m}, \bar{k} \in \mathbb{Z}_n$ s.t. $\bar{m} \neq \bar{0}$ and $\bar{k} \neq \bar{0}$, $\bar{m} \cdot \bar{k} = 0$

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

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

If $n \mid m \Rightarrow m$ = multiply of $n \Rightarrow \bar{m} = \bar{0}$ C!
If $n \mid k \Rightarrow k$ = multiply of $n \Rightarrow \bar{k} = \bar{0}$ 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. $(\mathbb{Z},+,\cdot)$, $(2\mathbb{Z},+,\cdot)$ 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 $\oplus$, $\odot$

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

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

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

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

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

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

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

Theorem:- Every field is an integral domain. But the Converse is not true ingeneral 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 $R = \{a_1, a_2, \ldots, a_n\}$ since, R is comm. ring with unity 1

let a_k be a non-zero element of R ;

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

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 , $1 \leq r < n$

$\Rightarrow a_k$ 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, ingeneral. 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:

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

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

Example

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

Class

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

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

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

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

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

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

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

Remark :

Let F be a fied and let $\{S_\alpha\}$ be any Collection of subfield of F. Then $\cap S_\alpha$ is a subfield of F.

Proof :

Since, $0 \in S_\alpha \ \forall \alpha \Longrightarrow \cap S_\alpha \neq \emptyset$

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

$\Longrightarrow a, b \in S_\alpha \ \forall \alpha$

But S_α is a subfield of $F \ \forall \alpha$

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

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

$\therefore \bigcap S_\alpha$ is a subfield of F.

المرحله الثالثه/قسم الرياضيات

الماده الحلقات

الفصل الثاني

Chapter Two

Chapter two - Subrings

الكلمات الجديدة

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. $(2\mathbb{Z},+,\cdot)$ 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 :

$\Rightarrow$) It is clear that if $(S,+,\cdot)$ is a subring of $(R,+,\cdot)$, the 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.

Class

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

$0 = x - x \in S \Rightarrow 0 \in S$ by Condition ①

(0 ↙ zero ele.)

$\forall a \in S$, $0 - a \in S$ by Condition ①

$\Rightarrow -a \in S$

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

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

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

Example

Consider $(Z_6, +_6, \cdot_6)$ ring.

Then all subrings of $(Z_6, +_6, \cdot_6)$ are:

1. $(Z_6, +_6, \cdot_6)$ is a subring of $(Z_6, +_6, \cdot_6)$

Class

(2) $(\{\bar{0}\}, +_6, \cdot_6)$ is a subring of $(Z_6, +_6, \cdot_6)$

(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

$+_6$ is Comm., associative on A

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

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

$\cdot_6$ closed on A

$\cdot_6$ associative on A

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

Then A is a subring of Z_6

(4) $B = \{\bar{0}, \bar{3}\}$. To prove $(B, +_6, \cdot_6)$ of $(Z_6, +_6, \cdot_6)$

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

$+_6$ 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 Z_6.

Class

Remark

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

Examples:

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

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

Solution

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

1. $(a_1,0)-(a_2,0) = (\underbrace{a_1-a_2}_{\in Z}, 0) \in A$

2. $(a_1,0)\cdot(a_2,0) = (\underbrace{a_1 a_2}_{\in Z},0) \in A$

$\therefore$ A is a subring of direct sum $(Z\times Z, \oplus, \odot)$

2. let $A=\{(a,1) : a \in Z\}$. Is 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 $(Z,+,\cdot)$

Class

Examples

Find all subrings of $(Z_{24}, +_{24}, \cdot_{24})$ and $(Z_{30}, +_{30}, \cdot_{30})$

① $(Z_{24}, +_{24}, \cdot_{24})$

1. Z_{24} 2. $\{\bar{0}\}$ 3. $\{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \ldots, \bar{22}\}$

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

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

$(Z_{30}, +_{30}, \cdot_{30})$ (H.W.)

Example:

Consider the ring $(Z[\sqrt{3}], +, \cdot)$.
let $A = \{a + b\sqrt{3} : a, b \in Z_e\}$. Is A subring of $Z[\sqrt{3}]$? (H.W.)

Solution

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

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

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

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

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

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

Class

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 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 a unites. For example: The ring $(\mathbb{Z}_6, +_6, \cdot_6)$ has unity $\bar{1}$, but the subring $(\{\bar{0}, \bar{2}, \bar{4}\}, +_6, \cdot_6)$ of $(\mathbb{Z}_6, +_6, \cdot_6)$ has unity $\bar{4}$ (since $\bar{4} \cdot_6 \bar{0} = \bar{0}$, $\bar{4} \cdot_6 \bar{2} = \bar{2}$, $\bar{4} \cdot_6 \bar{4} = \bar{4}$).

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

H.W. 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 $\bar{2} \cdot_6 \bar{3} = \bar{0}$ but $S = \{0, 2, 4\}$ has no zero divisor $\Rightarrow$ integ...

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 $b\in A \Rightarrow a-b\in A$ and $a.b\in A$ (since A is subring of R) ——→ ①

or $a,b\in B \Rightarrow a-b\in B$ and $a.b\in B$ (since B is a subring of R) ——→ ②

From ① and ②, we get $a-b\in A\cap B$ and $a.b\in A\cap B$

Thus $A\cap B$ is a subring of $(R,+,\cdot)$

● As a generalization of above theorem, we have

The intersection of any family $\{A_i\}_{i\in\Lambda}$, Λ 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 $A=\{0,\mp2,\mp4,\cdots\}$, $B=\{0,\mp3,\mp6,\mp9\cdots\}$

$A\cup B=\{0,\mp2,\mp3,\mp4,\mp6,\cdots\}$

Class

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 $Cent(R)$

Remarks :

(1) If R is Comm. ring, then $Cent(R) = R$.

(2) $Cent(R)$ is a subring of $(R,+,\cdot)$

Proof :

let $x_1, x_2 \in Cent(R)$

1. $x_1 \cdot y = y \cdot x_1 \quad \forall y \in R \longrightarrow (1)$
2. $x_2 \cdot y = y \cdot x_2 \quad \forall y \in R \longrightarrow (2)$

Now, $\forall y \in R$ by (1) and (2) we get

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

$\therefore x_1 - x_2 \in Cent(R)$

Similarly $x_1, x_2 \in Cent(R)$

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

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

$\therefore x_1 x_2 \in Cent(R)$

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

Definition :

Let $(R,+,\cdot)$ be a ring and let $a \in R$, $n \in Z_+$.

Then :

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

Example :

Consider the ring $(Z_8, +_8, \cdot_8)$

Fined $(2).\bar{3}$, $(-2).\bar{3}$, 7^{-2}

solution :

1. $(2)\bar{3} = \bar{3} +_8 \bar{3} = \bar{6}$

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

3. $\bar{7}^{-2} = (\bar{7}^{-1})^2 = (\bar{7})^2 = \bar{7} \cdot_8 \bar{7} = \bar{1}$

Theorem :

Let $(R,+,\cdot)$ be a ring. Then for $a, b \in R$ and arbitary 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. $n(a.b) = (na).b = a.(nb)$
5. $(na).(mb) = (nm)(a.b)$

Proof :- (1)

Case (i) $n \in Z_+, m \in Z_+$

Class

$na + ma = (a + a + \cdots + a) + (a + a + \cdots + a)$
(n times) (m times)

$= a + a + a + \cdots + a + \cdots + a$
($n+m$) times

$= (n+m)a$

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

$na + ma = na + 0.a = na = (n+0)a = (n+m)a$

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

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

Definition :

Let $(R, +, \cdot)$ be a ring, if there exists a positive n s.t. $na = 0$ $\forall a \in R$, then the least positive integer with this property is called characteristic of R (simply $ch(R)$).
If no such positive integer exists, implies $ch(R) = 0$

Examples :

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

$\forall a \in \mathbb{Z}$, only $na = \bar{0}$ ثابت, then $n = \bar{0}$ ثابت
$\therefore ch(\mathbb{Z}) = 0$

2. Each ring $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{Z}_e, +, \cdot)$ 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 $ch(M_2(\mathbb{R})) = 0$

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

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

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

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

(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 $A \Delta A = (A/A) \cup (A/A) = \emptyset \cup \emptyset = \emptyset$ = Zero element

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

⊛ problem: Prove or disprove
let R be a ring and let S be a subring of R.
Then:
1. $ch(R) = ch(S)$
2. $ch(R) \neq ch(S)$

$ch(\mathbb{Z}_6) = 6$
but $A = \{\bar{0}, \bar{2}, \bar{4}\}$
The identity element of A is $\bar{4}$.
Then $ch(A) = 3$
Since, $\bar{4} +_6 \bar{4} +_6 \bar{4} = \bar{0}$

Class

Theorem:

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

Proof:-

$\Rightarrow$) If $ch(R) = n$, $n \in \mathbb{Z}^+$

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

$1 \in R \Rightarrow n1 = 0$ by ①

suppose $\exists m \in \mathbb{Z}^+$ and $m < n$ and $m1 = 0$ البرهنة ان اصغر عدد صحيح موجب

$\forall a \in R$, $ma = m(1 \cdot a) = (m.1) \cdot a = 0 \cdot a = a$

Since, $ma = 0$ $\forall a \in R$ and $m < n$ which Contradict the state ① يناقض العبارة

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

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

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

حتى نثبت $ch(R) = n$

suppose $ch(R) = m$ and $m < n$

$\Rightarrow m.1 = 0$ Cl . Therefore $ch(R) = n$.

Corollary:-

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

تطبيق مباشر على النظرية اعلاه

where $n\bar{1} = \bar{1} +_n \bar{1} +_n \bar{1} +_n \cdots +_n \bar{1} = \bar{0}$

Class

Theorem :-

Let $(R, +, .)$ be an integral domain. Then $Ch(R)$ is either Zero or prime number.

Proof :-

Suppose $Ch(R) = n$, $(n \in Z_+)$ and n is not prime. Thus $n = mk$ for some $m, k \in Z_+$

$1 < m < n$, $1 < k < n$

$Ch(R) = n$ (since n is the least positive integer) s.t. $n1 = 0$ ⊛

$n1 = 0$ = Zero element

$(m.k)(1.1) = 0 \Longrightarrow (m.1)(k.1) = 0$

$\Longrightarrow m1 = 0$ or $k1 = 0$ (since R is an integral domain. i.e R has no Zero divisor)

Case ① $m1 = 0$, but $m < n \Longrightarrow$ C! with ⊛

Case ② $k1 = 0$ C! with ⊛ (since $k < n$)

∴ our assumption is false $\Longrightarrow Ch(R) = 0$ or prime number.

كلية التربيه للعلوم الصرفه /ابن الهيثم
قسم الرياضيات/المرحله الثالثه
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 $R \iff a.r \in S$
2. S is called a left ideal of $R \iff r.a \in S$

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

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

Remark :

In Comm. ring every left ideal is right ideal and Conversely.

Example :

The subring $(2\mathbb{Z},+,\cdot)$ is an ideal of $(\mathbb{Z},+,\cdot)$.

Since : If $a = 2n \in 2\mathbb{Z}$ and $r \in \mathbb{Z}$, then

$r.a = a.r = (2n).r = 2(n.r) \in 2\mathbb{Z}$

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. $a.r \in S$ and $r.a \in S \quad \forall a \in S, r \in R$

Class

Examples :

هذا المثال يوضح انه ليس كل subring يكون ideal

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

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

ideal $\Rightarrow$ subring
$\not\Leftarrow$

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

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

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

3. Find all ideals of $(Z_6, +_6, \cdot_6)$

a. $(\bar{1}) = Z_6$ b. $\{\bar{0}\}$ c. $\{\bar{0}, \bar{2}, \bar{4}\}$ d. $\{\bar{0}, \bar{3}\}$

تعميم :

جميع الحلقات الجزئية من الحلقة $(Z_n, +_n, \cdot_n)$ هي مثاليات اي بمعنى ليس كل subring هو ideal في $(Z_n, +_n, \cdot_n)$.

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 $(M_2(Z), +, \cdot)$.

let

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

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

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

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

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

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

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)

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

$\therefore S_1$ 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

$\emptyset \neq S_2 \subseteq R$

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

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

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

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

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

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

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

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

Remarks :

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

Class

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 $a a^{-1} = 1$

Therefore $1 = \underset{\in I}{a} \cdot \underset{\in R}{a^{-1}} \in I$ (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.

Theorem:

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

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

let $a, b \in I \cap J$, $r \in R$.

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

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

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

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

Thus $a - b \in I \cap J$ and $r.a \in I \cap J$, $a.r \in I \cap J$

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

Remark:

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

$(Z_6, +_6, \cdot_6)$, $(\bar{2})$ and $(\bar{3})$ are ideals of 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 $I = \{r.a : r \in R\}$. Then I is an ideal of R and this ideal is called a principl ideal generated by a and denoted by (a), $id(a)$, $\langle a \rangle$.

Class

proof: $I \neq \emptyset$ since $0 = 0.a \in I$

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

$x_1 = r_1 a$, $x_2 = r_2 a$ for some $r_1, r_2 \in R$

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

$cx_1 = c.(r_1 a) = (cr_1).a \in I$

$\therefore$ I is an ideal of R .

Example :

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

$id(2) = \{r.2 : r \in \mathbb{Z}\} = \{0, \pm 2, \pm 4, \dots\}$

$id(-2) = \{r.(-2) : r \in \mathbb{Z}\} = \{0, \pm 2, \pm 4, \dots\}$

$id(a) = id(-a)$ بصورة عامة.

↑ النظير الجمعي لـ a

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

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

$id(\bar{1}) = \{\bar{r} ._6 \bar{1} ; \bar{r} \in \mathbb{Z}_6\} = \mathbb{Z}_6$

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

$id(\bar{2}) = \{\bar{r} ._6 \bar{2} : \bar{r} \in \mathbb{Z}_6\}$

$= \{\bar{0} ._6 \bar{2}, \bar{1} ._6 \bar{2}, \bar{2} ._6 \bar{2}, \bar{3} ._6 \bar{2}, \bar{4} ._6 \bar{2}, \bar{5} ._6 \bar{2}\}$

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

Class

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

$id(\bar{4}) = \{\bar{0}, \bar{4}, \bar{2}\}$ $id(\bar{4}) = id(\bar{2})$ نلاحظ (لأنه واحد نظير الآخر)

$id(\bar{5}) = \{\bar{0}, \bar{5}, \bar{4}, \bar{3}, \bar{2}, \bar{1}\} = Z_6$

لأنه

$$\bar{5} \cdot_6 \bar{5} = \bar{1} \in id(\bar{5})$$

$\therefore id(\bar{5}) = Z_6$

Theorem :-

Let R be a Comm. ring with unity 1.

Then :-

1. $id(1) = R$ and $id(0) = \{0\}$
2. $a \in id(a)$
3. $id(a) = id(-a)$
4. $id(a) = R$ if a is an invertible.

problems :-

1. Find all P.I. in $(Z_5, +_5, \cdot_5)$
2. Find all P.I. in $(Z_{12}, +_{12}, \cdot_{12})$

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 $id(a,b)$, $\langle a,b \rangle$, (a,b).

Class

تعميم

let R be a Comm. ring with unity 1
let $a_1, a_2, a_3, \dots, a_n \in R$

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

Example :

Consider the ring $(\mathbb{Z}, +, \cdot)$.
Find $id(2,3)$, $id(2,4,6)$, $id(3,5)$

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

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

$\therefore id(n,m) = id(d)$

حيث d = القاسم المشترك
وهذه في حالة $\mathbb{Z}$ فقط
وذلك حسب خوارزمية الاقليدية والتي تنص

let $a, b \in \mathbb{Z}$, $d = gcd(a,b)$
$\Rightarrow d = r_1 a + r_2 b$ for some $r_1, r_2 \in \mathbb{Z}$

Example :

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

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

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

2. $id((1,1),(1,1)) = R$

Class

3. id $((1,0),(0,1)) = \{((r_1,k_1),(r_2,k_2)) \odot ((1,0),(0,1))$

$; (r_1,k_1),(r_2,k_2) \in R \}$

$= \{(r_1,0),(0,k_2) \; ; \; r_1,k_2 \in Z\}$.

$Z \times \{0\} \cup \{0\} \times Z$

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 :- $(Z_8, +_8, \cdot_8)$ is a P.I.R.

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

Proof :- let I be any ideal of Z

If $I = \{0\}$, then $I = id(0)$ 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 Contians positive integers

لتكن S هي مجموعة كل الأعداد الصحيحة الموجبة الموجودة في I

$\therefore S \subseteq Z_+$. But Z_+ is a w.o.s

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

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

we claim that $I = id(n)$

let $x \in id(n)$

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

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

$\therefore id(n) \subseteq I \longrightarrow ①$

Now, let $x \in I$

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

$x = qn + r \quad 0 \leq r < n$ (حسب خوارزمية القسمة)

if $0 < r < n$, $\quad r = x - qn \in I$

$\in I \quad \in I$

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

كون n اصغر عدد صحيح موجب في I

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

$\therefore I \subseteq id(n) \longrightarrow ②$

From ① and ②, we get $I = id(n)$.

Theorem :-

Every field is a P.I.R.

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

$\therefore F$ is P.I.R

Class

Some operations on ideals بعض العمليات على المثاليات

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

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

$x_1\in I \longrightarrow rx_1\in I$
$y_1\in I \longrightarrow ry_1\in I$ (Since $I \wedge J$ are ideals of R.)

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

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

Class

Remark :

let $(R,+,\cdot)$ be a Comm. ring and $a,b \in R$.
Then $id(a,b) = id(a) + id(b)$

Examples :

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

* $id(3) + id(4) = id(3,4) = id(1) = \mathbb{Z}$
* $id(2) + id(4) = id(2,4) = id(2) = 2\mathbb{Z}$

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

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

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

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

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

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

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

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

عند جمع المثالي مع نفسه يكون 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 :
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 $I \cdot J = \{ \sum_{\text{finite sum}} a_i b_i : a_i \in I, b_i \in J \}$. 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 $x \in IJ \Rightarrow x = \sum_{\text{finite sum}} a_i b_i$, $a_i \in I$, $b_i \in J$ $\forall i$

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

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

Class

$\therefore xr \in I$ (since $\cdot$ is closed on I) $\Rightarrow IJ \subseteq I$

Similarly, $IJ \subseteq J$.

Example:

Consider $(\mathbb{Z}_6, +_6, \cdot_6)$. 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 $I = id(2)$, $J = id(3)$

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

$\therefore a_i = 2m_i \quad m_i \in \mathbb{Z}$
$b_i = 3n_i \quad n_i \in \mathbb{Z}$

$a_i \cdot b_i = (2m_i) \cdot (3n_i) = 6(m_i n_i) = 6c_i$ where $c_i = m_i n_i$

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

$\therefore IJ = id(6)$
$I \cdot I = id(4) \subsetneq I$

Class

كلية التربيه للعلوم الصرفه/ابن الهيثم
قسم الرياضيات/المرحله الثالثه
الماده /الحلقات

الفصل الرابع والخامس

Chapter Four And Five

Chapter Four Factor Rings الحلقات الكسرية
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 $R\setminus I$ by:

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

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

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

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

let $a+I = a_1+I$ means $a+(-a_1) \in I \Rightarrow a-a_1 \in I$
$b+I = b_1+I$ means $b+(-b_1) \in I \Rightarrow b-b_1 \in I$

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

Class

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 $b+I = b_1+I$

$\Rightarrow a-a_1 \in I$ and $b-b_1 \in I$

we want to prove that $(a+I)\odot(b+I) = (a_1+I)\odot(b_1+I)$

That is, $(a.b)-(a_1.b_1) \in I$

$a.b - a_1b_1 = ab - a_1b + a_1b - a_1b_1$

$= (a-a_1)b + a_1(b-b_1) \in I$

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 $(R\setminus I, \oplus)$ is Comm. gp.

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

Therefore $(R\setminus I, \oplus, \odot)$ 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. $R\backslash I$ is Comm. $\iff a.b - ba \in I \quad \forall a,b \in R$.

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

Proofs :

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

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

2. $R\backslash I$ is Comm. $\overset{\text{by Def.}}{\iff} (a+I)\odot(b+I) = (b+I)\odot(a+I)$

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

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

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

Example :

Consider $(\mathbb{Z}_4, +_4, \cdot_4)$ be a ring.

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

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

$\bar{0}+I = I$

Class

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

$\bar{2}+I=I$ and $\bar{3}+I=\bar{1}+(\underbrace{\bar{2}+I}_{I})=\bar{1}+I$

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

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

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

Notice

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

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

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

4. $Ch(\mathbb{Z}_4\backslash I)=2$ (since $(\bar{1}+I)\oplus(\bar{1}+I)=\bar{2}+I=\bar{0}+I$).

Examples

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

2. $\mathbb{Z}_n\backslash\mathbb{Z}_n=\overline{\mathbb{Z}}_n$ $\forall n>1$

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

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

Class

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

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

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

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

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

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

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

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

وهكذا البقية !

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

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

وهكذا البقية !

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

where $0 \leq r < 4$

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

$\therefore Z \setminus I = \{0+I, 1+I, 2+I, 3+I\} = Z_4$

Therefore $(Z \setminus I, \oplus, \odot) = (Z_4, +_4, \cdot_4)$

Notice that $(Z, +, \cdot)$ is an integral domain and $ch(Z) = 0$, but $(Z_4, +_4, \cdot_4)$ is not integral

Class

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

تقسيم لهذا المثال

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

$$(\mathbb{Z}\backslash I, \oplus, \odot) = (\mathbb{Z}_n, +_n, \cdot_n)$$

Problem: (H.W) let $(\mathbb{Z}_6, +_6, \cdot_6)$ be a ring and let $I = \{\bar{0}, \bar{2}, \bar{4}\}$, $J = \{\bar{0}, \bar{3}\}$.

Then find all element of

1. $\mathbb{Z}_6 \backslash I$
2. $\mathbb{Z}_6 \backslash J$
3. $\mathbb{Z}_6 \backslash I + J$
4. $\mathbb{Z}_6 \backslash I \cdot J$

Class

Chapter Five – Ring homomorphism – التشاكل الحلقي

Definition : let $(R,+,\cdot)$ and $(R',\dot{+},\dot{\cdot})$ be two ring. A mapping $f:R \longrightarrow R'$ is called ring homomorphism

$\Longleftrightarrow$ 1. $f(a+b) = f(a) \dot{+} f(b)$ $\quad \forall a,b \in R$

2. $f(a.b) = f(a) \dot{\cdot} f(b)$

Examples :

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

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

$f(a) \dot{+} f(b) = \grave{0} \dot{+} \grave{0} = \bar{0}$

$f(a.b) = \bar{0}$, $f(a) \dot{\cdot} f(b) = \grave{0} \dot{\cdot} \grave{0} = \grave{0}$

2. let $f:R \longrightarrow R$ be a ring homo. s.t. $f(x) = x$

3. let $f:(Z,+,\cdot) \longrightarrow (Z,+,\cdot)$ s.t. $f(x) = 3x$ $\forall x \in Z$ Is f homo. ?

Solution : $\forall a,b \in Z$

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

$f(a.b) = 3ab$, but $f(a).f(b) = 3a.3b = 9ab$

$\therefore f$ is not homo.

Class

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

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

Solution:

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

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

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

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

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

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

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

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

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

$\therefore f$ is not homo.

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

a. $f(x) = x^2$

b. $f(x) = 2x+1$

c. $f(x) = 2^x$

d. $f(x) = 1$

Class

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

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

① $f(0) = \bar{0}$ where 0 = Zero element of R
$\bar{0}$ = Zero element of R'

② $f(-a) = -' f(a)$ $\forall a \in R$

③ $f(a-b) = f(a) -' f(b)$ $\forall a, b \in R$

④ qf S is a subring of R, then $f(S)$ is a subring of R'

⑤ qf S' is a subring of R', then $f^{-1}(S')$ is a subring of R.

⑥ qf I is an ideal of R, f is onto, then $f(I)$ is an ideal of R'.

⑦ qf J is an ideal of R', then $f^{-1}(J)$ is an ideal of R.

⑧ qf R has unity 1, then $f(1)$ is unity of $f(R)$.

⑨ qf R has unity 1, f is onto, then $f(1)$ is unity of R'

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

Class

② $f(0)=\grave{0} \Rightarrow f(a+(-a))=\grave{0}$

$f(a)\grave{+}f(-a)=\grave{0}$ نضيف للطرفين $-f(a)$ $\Rightarrow f(a)\grave{-}f(a)\grave{+}f(-a)=\grave{0}\grave{-}f(a)$

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

③ $f(a-b)=f(a+(-b))=f(a)\grave{+}f(-b)$

$=f(a)\grave{+}(-f(b))=f(a)\grave{-}f(b)$

⑤ S' is subring of R'. Then $\grave{0}\in S'$

but $f(0)=\grave{0}$ by (1)

$f(0)\in S' \Rightarrow \therefore 0\in f^{-1}(S')$

$\therefore f^{-1}(S')\neq\emptyset$ Also $f^{-1}(S')\subseteq R$ by def.

let $a,b\in f^{-1}(S') \rightarrow f(a)\in S' \wedge f(b)\in S'$

$f(a)\grave{-}f(b)=f(a-b)$ by ③

$\therefore f(a-b)\in S' \Rightarrow a-b\in f^{-1}(S')$.

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

$\Rightarrow a\cdot b\in f^{-1}(S')$

$\therefore f^{-1}(S')$ is a subring of R.

⑥

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

Also, $f(I)\subseteq R'$ by def.

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

$y_1 = f(x_1)$ 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, $\because f: R \to R'$ onto, $c \in R'$

$\therefore \exists\, r \in R$ s.t. $c = f(r)$

$\therefore c \cdot y_1 = f(r) \cdot f(x_1) = f(r \cdot x_1) \in f(I)$

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

Definition:

let $f: (R, +, \cdot) \to (R', +', \cdot')$ 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 kernal of f and denoted by $\ker(f)$. Since $\ker f = f^{-1}\{\bar{0}\}$

Remark:

$\ker f$ is an ideal of R.

Since $\ker f = f^{-1}\{\dot{0}\}$ and $\{\dot{0}\}$ is an ideal of R' Then by Theorem of properties of homo number (7) $\ker f$ is an ideal of R.

Class

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

Proof :- $\Rightarrow$) Suppose that $\ker f=\{0\}$

Now, let $x,y\in R$ and $f(x)=f(y)\Rightarrow f(x)-f(y)=\bar{0}$

$f(x-y)=\grave{0}$ (since f is homo.) $\Rightarrow x-y\in \ker f=\{0\}$

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

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

let $x\in\ker f\Rightarrow f(x)=0\Rightarrow f(x)=f(0)$

$\Rightarrow x=0\Rightarrow \ker f=\{0\}$

Example :-

let $f:R\to R$ 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 $\ker f$. $f(x,y)=(x,0)$

$\ker f=\{(x,y):f(x,y)=(\grave{0},\grave{0})\}=\{(x,y):(x,0)=(\grave{0},\grave{0})\}$

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

Definition :-

let $f:R\to R$ 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 $\Leftrightarrow$ f is (1-1) and onto.

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

R is Called isomorphic to R $(R \cong R') \Leftrightarrow$
$\exists f: R \to R'$ s.t. f is an isomorphism.

Examples:

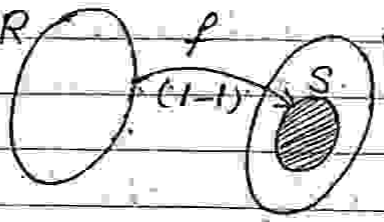
① $(Z_4,+_4,\cdot_4)$ is not isom. to $(Z_2,+_2,\cdot_2)$

Since $\nexists f: Z_4 \to Z_2$ s.t. f is (1-1)

② If R has n element, $\bar{R}$ has m element s.t. $m \neq n$, then $R \neq R'$.

Definition: (تعريف خلاصة مقورة في خلاصة)

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



Examples:

① Let $R = Z \times Z$ be a ring. Then show that $(Z,+,\cdot)$ Can be embeded in R.

Solution:

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

a subring of R.

Define $f: Z \to S$ by $f(a) = (a,0)$
∴ f is an isomorphism

∴ Z can be embeded in R.

② $(Z_2, +_2, \cdot_2)$ Cannot be embeded in $(Z_3, +_3, \cdot_3)$

لان Z_3 لا توجد لديها subring تركيب على عناصرين وتحقق شروط ان تكون الدالة بينهما isomorphism

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

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

Define $+', \cdot'$ on R' by:
$(a,n) +' (b,m) = (a+b, n+m) \in R'$
$(a,n) \cdot' (b,m) = (\underbrace{a \cdot b + nb + ma}_{\in R}, \underbrace{mn}_{\in Z}) \in R'$
∴ $(R', +', \cdot')$ is a ring (check).
The unity of R' is $(0,1)$, since
$(a,n) \cdot' (0,1) = (a \cdot 0 + n \cdot 0 + 1 \cdot a, n) = (a,n) \quad \forall (a,n) \in R'$.

let $S = \{(a,0) : a \in R\} \subseteq R'$. Then S is a subring of R' (check).
Define $f: (R,+,\cdot) \to (S,+',\cdot')$ s.t. $f(a) = (a,0)$
∴ f is an isomo. (check). which Completes the proof.

Class

Definition:-
Let $(R,+,\cdot)$ be a ring, I is an ideal of R, the map, $f: (R,+,\cdot) \longrightarrow (R/I,+,\cdot)$ s.t. $f(x) = x+I$ is called the natural mapping (denoted by nat_I) $\forall x \in R$.
nat_I is ring homo, onto.

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

Proof:
Let $f:(R,+,\cdot) \longrightarrow (R',+',\cdot')$ 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 $R' \Longrightarrow f^{-1}(I')$ 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. $I = id(a)$.
we claim that $I' = id(f(a))$
let $y \in id(f(a)) \Longrightarrow y = r' \cdot' f(a)$ for some $r' \in R'$
but f is onto, $r' \in R'$, so $\exists\, r \in R$ s.t. $r' = f(r)$
$\therefore y = f(r) \cdot' f(a) = f(ra) \in f(I)$
$\therefore y \in f(I) \Longrightarrow y \in I' \Longrightarrow \therefore id(f(a)) \subseteq I'$

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

let $y \in I' \Longrightarrow y \in f(I)$ since $f(I) = I'$, f is onto and I' ideal of $R' \Longrightarrow y = r' \cdot f(a) = f(ra)$
$\therefore y \in id(f(a))$.

Class

The fundamental theorems of ring homo.

(البرهنات الاساسية للتشاكل الحلقي)

Theorem(1): First fund. theorem (البرهنة الاولى)

If $f: R \longrightarrow R'$ is an R-homo., then $R/\ker f \cong \operatorname{Im} f$

Proof:- Define $g: R/\ker f \longrightarrow \operatorname{Im} f$ s.t

$$g(x+\ker f) = f(x) \quad \forall x \in R$$

T.P. g is well-define ?

let $x_1+\ker f = x_2+\ker f$ where $x_1+\ker f$ and $x_2+\ker f \in R/\ker f$

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

$f(x_1)-f(x_2)=0 \Rightarrow f(x_1)=f(x_2) \Rightarrow g(x_1+\ker f)+g(x_2+\ker f)$

$\therefore$ g is well-define

T.P. g is homo. ?

let $x_1+\ker f, x_2+\ker f \in R/\ker f$

① $g[(x_1+\ker f)\oplus(x_2+\ker f)] = g[(x_1+x_2)+\ker f]$

$= f(x_1)\oplus f(x_2) = g(x_1+\ker f)\oplus g(x_2+\ker f)$

② $x_2+\ker f, x_1+\ker f \in R/\ker f$

$g[(x_1+\ker f)\odot(x_2+\ker f)] = g(x_1x_2+\ker f) = f(x_1x_2)$

$= f(x_1)\odot f(x_2) = g(x_1+\ker f)\odot g(x_2+\ker f)$

Class ✓

∴ f is homo.

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

عكس برهان well define من الاسفل الى اعلى

اذا يصبح

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

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

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

T.P. g is onto ?

let y be any element of Imf

$\therefore \exists x \in R$ s.t. $f(x)=y$

$\Rightarrow g(x+\ker f) = y$ ∴ g is onto.

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

Theorem (2) : Second Fun. Theorem (النظرية الثانية)

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

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

Proof : Define $f: K \longrightarrow (K+L)/L$ 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

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

∴ f is well-define.

T.P f is homo ?

let $x_1, x_2 \in K$

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

$f(x_1x_2) = x_1x_2+L = (x_1+L)\odot(x_2+L) = f(x_1)\cdot f(x_2)$

T.P f is onto ?

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

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

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 (المبرهنة الثالثة)

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

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

T.P f is well-define ?

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

If $x_1+K = x_2+K \Rightarrow x_1-x_2 \in K \Rightarrow x_1-x_2 \in L$

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

Class

T.P. f is homo ?

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

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

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

② $f[(x_1+K)\odot(x_2+K)] = f[(x_1x_2)+K]$

$= x_1x_2+L = (x_1+L)\odot(x_2+L) = f(x_1+K)\odot f(x_2+K)$.

T.P. f is onto ?

$\text{Im}f = \{f(x+K) : x\in R\} = \{x+L : x\in R\} = R/L$

$\therefore f$ is onto.

By theorem (1) $\Longrightarrow R/K/\ker f \cong R/L$.

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

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

$= \{(x+K)\in R/K : x+L = L\}$

$= \{x+K \in R/K : x\in L\} = L/K$

$\therefore R/K / L/K \cong R/L$.

Class

الفصل السادس

Chapter Six

Chapter Six 6

Certian 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 $(Z_{12}, +_{12}, \cdot_{12})$.

Z_{12} is not max. ideal لأنها الحلقة نفسها لا يمكن ان تكون مثالي اعظمي

$[\bar{0}]$ is not max. ideal, since $\exists$ ideal $J = \{\bar{0}, \bar{6}\}$ s.t.

$\{0\} \subsetneq \{\bar{0}, \bar{6}\} \subsetneq Z_{12}$

$M_1 = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}, \bar{10}\}$ is max. ideal
لانه لا يوجد مثالي في Z_{12} يحوي المثالي M_1

$M_2 = \{\bar{0}, \bar{3}, \bar{6}, \bar{9}\}$ is max. ideal

$M_3 = \{\bar{0}, \bar{4}, \bar{8}\}$ is not max. ideal.

since $\exists M_1$ s.t. $M_3 \subsetneq M_1 \subsetneq Z_{12}$

$M_4 = \{\bar{0}, \bar{6}\}$ is not max ideal, since $\exists M_1, M_2$ ideals of Z_{12} s.t. $M_4 \subsetneq M_1 \subsetneq Z_{12}$ and $M_4 \subsetneq M_2 \subsetneq Z_{12}$.

problems:-

① Find all maximal ideals of $(Z_8, +_8, \cdot_8)$.

② Find all maximal ideals of $(Z_{15}, +_{15}, \cdot_{15})$.

Theorem:- In the ring Z, the id (n), $(n \in Z, n > 1)$ is maximal ideal $\iff$ n is prime number.

proof:- $\Rightarrow$) let $I = id(n)$ is max. ideal.

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 $n = mk$
$\therefore id(n) \subsetneq id(m) \subsetneq \mathbb{Z}$ and $id(n) \subsetneq id(k) \subsetneq \mathbb{Z}$
which is Contradiction with definition of max ideal
تناقض مع تعريف المثالي الأعظمي

$\Longleftarrow$ If n is prime number, to prove $I = id(n)$ is max. idea
Suppose $I = id(n)$ 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. $J = id(m) \Rightarrow id(n) \subsetneq id(m) \subsetneq \mathbb{Z}$
Since $n \in id(n)$, since $n = 1.n \Rightarrow n \in id(m)$
$\therefore n = mk$ for some $k \in \mathbb{Z}_+$ and $k \neq 1$.
Hence n is not prime number C!
$\therefore I = id(n)$ is max. ideal.

problems:- let R = 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 (حلقة موضعية) $\iff$ R has unique max. ideal

Example :- ① $(\mathbb{Z}_4,+_4,\cdot_4)$ 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 $\iff (M,a)=R$ $\forall a\in R$, $a\notin M$.

where $(M,a)=\{m+ra : m\in M, r\in R\}$

proof :- $\Rightarrow$) If M is max. ideal, To prove $(M,a)=R$

$M \subsetneq (M,a) = M+id(a) \Rightarrow a = 0+1\cdot a \in (M,a)$. But $a\notin M$. Thus $(M,a)=R$ (لان M هو اكبر مثالي)

$\Leftarrow$) If $(M,a)=R$, $\forall a\notin M$. To prove M is max ideal suppose M is not max. ideal $\Rightarrow \exists$ ideal J of R s.t. $M \subsetneq J \subsetneq R$.

$\therefore \exists a \in J$ and $a \notin M$. But $(M,a) = R$

$\therefore \forall x \in (M,a) \Rightarrow x = \underset{J}{m} + \underset{J}{ra}$, $m \in M \subsetneq J$

$\therefore x \in J \Rightarrow \therefore (M,a) \subseteq J$ and $J \subseteq (M,a)$

$\therefore (M,a) = J \Rightarrow R \subseteq J$

$\therefore R = J$ C! . Thus (عندئذ) M is max. ideal

Theorem :-

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 :-

(Zorn's lemma) البرهان يعتمد على مبرهنة زورن

ونصها كالتالي :-

لتكن X مجموعة غير خالية ولتكن $\mathcal{F}$ مجموعة غير خالية من مجموعات جزئية من X إذا كان لكل سلسلة $\{C_i\}$ من عناصر $\mathcal{F}$ فإن $\bigcup C_i \in \mathcal{F}$ وإن $\mathcal{F}$ تحتوي عنصراً أعظمياً .

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 $x, y \in \bigcup_{i \in \Lambda} C_i$, $r \in R$

$\therefore \exists\, j \in \Lambda$ s.t. $x \in C_j$ and $\exists\, k \in \Lambda$ s.t. $y \in C_k$

$\because \{C_i\}$ is a chain $\Rightarrow C_j \subseteq C_k$ or $C_k \subseteq C_j$

suppose $C_k \subseteq C_j \Rightarrow x, y \in C_k \Rightarrow x - y \in \bigcup C_i$

It's clear that $I \subseteq \bigcup C_i \quad \forall I \subseteq C_i$
من الواضحات

$\therefore \bigcup C_i \neq R$ (because $1 \notin C_i \ \forall i$, C_i is a proper ideal

$\Rightarrow \bigcup C_i \in F$. 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 $M \subsetneq K$

$\therefore K \notin F$ لأن خلاف ذلك يدخل في تناقض مركون M عنصراً "أكبر"

$\therefore K = R$. Then M is maximal ideal.

نتيجة — كتابع لهذه النظرية

Corollary

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.

حلقة لها نظير جزري

Proof :- ⟹) suppose that a is an invertible.

- (a) is the smallest ideal of R Contian a

But (a) = R ⟹ a is not belong to any max. ideal.

⟸) suppose that M is max. ideal and a ∉ M.

see the id (a). If R = (a), then a is an invertible elem
عنصر قابل للعكس

either, if R ≠ (a), then by above theorem, ∃ max. ideal
اما اذا بواسطة النظرية اعلاه

M and (a) ⊆ M ⟹ a ∈ M C! (a ∉ M بتناقض)

∴ it must to be R = (a)
اذن يجب ان تكون

نتيجة
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

∴ ∃ max ideal J of R s.t I ⊊ J ⊊ R (by above theora
من النظرية اعلاه

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.
العناصر المتطابقة

Def: Let R be a comm. ring with unity 1, $a \neq 0 \in R$ is called idempotent element if $a^2 = a$.

عنصر مخادد

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 $a-1 \neq 0$ بالفرض

This mean a and $a-1$ are Zero divisors

عناصر قاسمة 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

$\therefore a, a-1 \in M \Rightarrow 1 = a-(a-1) \in M$

$\therefore M = R$ C! (R لا يمكن أن يكون M مثالي)

مبرهنة

Theorem :- let R be a Comm. ring with unity 1. and let Π be a proper ideal of R. Then Π is maximal ideal $\Leftrightarrow$ R/Π is a field.

Proof :- $\Rightarrow$)

لنأخذ العنصر في R/I

let $a+I \in R/I$ and $a+I \neq I \Rightarrow a \notin I$

But I is max. ideal $\Rightarrow R = (I, a)$

$\therefore 1 = x + ra$ where $r \in R, x \in I$

$\therefore 1 - ra = x \in I \Longrightarrow (1-ra) + I = I$

$\Longrightarrow ra + I = 1 + I \Longrightarrow (r+I)(a+I) = 1+I$

$\therefore a+I$ has invertible element $(r+I)$

$\Longleftarrow$ let J be a proper ideal of R s.t. $I \subsetneq J$

$\therefore \exists\ w \in J, w \notin I \Longrightarrow w + I \neq I$

$\therefore w+I$ has invertible element in the field R/I

$\therefore \exists\ b+I \in R/I$ s.t. $(w+I).(b+I) = 1+I$

$\Longleftrightarrow 1 - wb \in I$.

we say $1 - wb = c$ s.t. $c \in I$

$\therefore 1 = \underbrace{c}_{\in I} - \underbrace{wb}_{\in J} \Longrightarrow 1 \in J \Longrightarrow J = R$.

$I \subsetneq J$ b/c

Remark :-

The theorem is not true in rings without unity, for example :

The ring $(2\mathbb{Z}_e, +, \cdot)$ has no unity.

let $M = \{0, \mp 4, \mp 8, \dots\}$ is max. ideal of $2\mathbb{Z}_e$. But

$2\mathbb{Z}_e / M = \{0+m, 2+m\}$ is not field.

Definition :- Let R be a Comm. ring, I be an ideal of R. I is called prime ideal iff $\forall a,b \in R$, $ab \in R \Rightarrow$ either $a \in I$ or $b \in I$

Example :- In the ring $(\mathbb{Z}, +, \cdot)$

let $id(2) = \{0, \pm 2, \pm 4, \pm 6, \dots\}$

let $a, b \in \mathbb{Z}$ s.t $ab \in id(2)$

$\Rightarrow ab = 2c$ for some $c \in \mathbb{Z}$

$\Rightarrow 2/ab$. But 2 is prime number $\Rightarrow$ either $2/a$ or $2/b \Rightarrow$ a is multiply of 2 or b is multiply of 2

$\Rightarrow a \in id(2)$ or $b \in id(2)$

$\Rightarrow id(2)$ is prime ideal.

Prop :- In the ring $(\mathbb{Z}, +, \cdot)$ if P is a prime number, then $id(P)$ 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 $ab \in R$ 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 $a,b \in R$, $ab=0$

$\therefore ab \in \{0\}$. But $\{0\}$ is prime ideal

$\therefore a \in \{0\}$ 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)

In $(\mathbb{Z}, +, \cdot)$: a non trivial ideal I of $\mathbb{Z}$, $I = \langle n \rangle$ is prime ideal $\Leftrightarrow n$ is prime number.

Example: $(\mathbb{Z}_6, +_6, \cdot_6)$

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 $a,b \in \mathbb{Z}_6$

$2,3 \in \mathbb{Z}_6$

$2.3 = 0 \in \mathbb{Z}_6$

$2 \in \mathbb{Z}_6 \wedge 3 \in \mathbb{Z}_6$

Example: In the ring $(\mathbb{Z}_5, +_5, \cdot_5)$

since $\mathbb{Z}_5$ is field $\Rightarrow \mathbb{Z}_5$ is an integral domain

$\therefore \{\bar{0}\}$ is the only proper prime ideal

في الساعة المثالي الأولي الوحيد هو $\{0\}$

Theorem :- let R be a comm. 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 المبرهنة اعلاه غير صحيح والمثال التالي يوضح ذلك

$\{0\}$ in $(\mathbb{Z},+,\cdot)$ is prime ideal. But $\{0\}$ is not max. ideal

Problem :- (H.W)

let R = 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 $\mathbb{Z}_e$

But I is not prime ideal (since $4 = 2 \cdot 2 \in I$, but $2 \notin I$)

Theorem: Let R be a Comm. ring with unity 1. Let I be an ideal of R. Then I is a prime ideal $\iff$ $(R/I, \oplus, \odot)$ is an integral domain.

Proof: $\Rightarrow$) R is Comm. ring with unity $1 \Rightarrow R/I$ is Comm. ring with unity $1 + I$.

If $(a + I) \odot (b + I) = I$ ← Zero element of R/I

$\therefore ab + I = I \Rightarrow ab \in I$, but I is a prime ideal of $R \Rightarrow$ either $a \in I$ or $b \in I$.

If $a \in I$, then $a + I = I$ and if $b \in I$, then $b + I = I$

$\therefore R/I$ has no zero divisor and so R/I is an integral domain.

$\Leftarrow$) To prove I is prime ideal

let $a, b \in R$ s.t $ab \in I \Rightarrow ab + I = I$

$(a + I) \odot (b + I) = I$

Either $a + I = I$ or $b + I = I$ (since R/I has no zero divisor)

$\therefore a \in I$ or $b \in I$

$\therefore$ I is prime ideal.

Theorem :- let R be a P.I.D. Then a nontrivial ideal I of R is maximal ideal $\iff$ it is prime ideal.

مثالية رئيسية

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.

$I = (a)$, $J = (b)$.

$\Rightarrow a \in (a) \subsetneq (b)$

① $a = tb$ for some $t \in R \Rightarrow tb \in I$.

But I is prime ideal $\Rightarrow$ either $t \in I$ or $b \in I$

if $b \in I \Rightarrow (b) \subseteq I = (a) \Rightarrow I = J$ C!

Then $t \in I \Rightarrow t \in I = (a)$

② $t = sa$, $s \in R$

From ① and 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.

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)

$\therefore b^2-b=0 \Rightarrow b(b-1)=0 \in I$

$\because I$ is prime ideal, $b\notin I$

$\therefore (b-1)\in I \Rightarrow b-1\in J$.

But $b\in J \Rightarrow b-(b-1)\in J$ (by def. of ideal)

$\therefore 1\in J \Rightarrow J=R$

$\therefore I$ is maximal ideal.

Definition : nil radical : الجذر العدمي

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 dented 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. $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$

Then $\sqrt{(n)} = \sqrt{(p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k})} = (p_1 p_2 \cdots p_k)$

③ $x \in \sqrt{I} \iff x + I$ is nilpotent element in R/I

وهذا بكافي التعريف

$$x^n + I = 0 \Rightarrow x^n \in I$$

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 : nil radical . الجذر العدمي

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 dented 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. $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$

Then $\sqrt{(n)} = \sqrt{(p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k})} = (p_1 p_2 \cdots p_k)$

③ $x \in \sqrt{I} \iff x + I$ is nilpotent element in R/I

وهذا بكافئ التعريف

$$x^n + I = 0 \Rightarrow x^n \in I$$

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

$$(x-y)^{n+m} = \underset{\in I}{x^{n+m}} + (n+m)\underset{\in I}{x^{n+m-1}}y + \cdots + (\cdot)\underset{\in I}{x^n y^m} + \cdots + \underset{\in I}{y^{m+n}}$$

$\therefore (x-y) \in \sqrt{I}$.

let $x \in R$, $x \in \sqrt{I} \Rightarrow x^n \in I$

$(rx)^n = r^n x^n \Rightarrow rx \in \sqrt{I}$
$\in I$

$\therefore \sqrt{I}$ 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 $\exists\, n \in Z_+$ s.t.

$w^n \in \sqrt{I} \Rightarrow (w^n)^m \in I$, $m \in Z_+$

$\Rightarrow w^{nm} \in I \Rightarrow w \in \sqrt{I}$

$\therefore \sqrt{\sqrt{I}} \subseteq \sqrt{I} \rightarrow$ 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 $I = \sqrt{I}$

Class

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 ingeneral 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:- $\Rightarrow$) let $a+I$ be nilpotent element in R\I $\Rightarrow (a+I)^n = I$, $n \in \mathbb{Z}^+$

$\therefore a^n + I = I \Rightarrow a^n \in I \Rightarrow a \in \sqrt{I} = I$ (since I is semiprime ideal)

$\therefore a + I = I$

$\Leftarrow$) It is clear that $I \subseteq \sqrt{I}$

Now, let $x \in \sqrt{I} \Rightarrow x^n \in I$ 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
$\therefore \sqrt{I} = I$. $\because x+I = I \Rightarrow x \in I$

Definition

let $(R,+,\cdot)$ be a ring, I be an ideal of R. Then I is called primary ideal if the following holds

$\forall\ ab \in I$, $a \notin I$, then $b^n \in I$ for some $n \in \mathbb{Z}^+$

Example:

$4\mathbb{Z}$ is primary ideal in $\mathbb{Z}$ $(2\cdot 2 = 4 \in 4\mathbb{Z} \Rightarrow 2^2 \in 4\mathbb{Z}$ but $2 \notin 4\mathbb{Z})$

Remark

Every prime ideal is primary ideal but the Converse is not true. For example $id(4)$ 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 $\exists\ b+I \neq I$ 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 حلقات بوليان

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

(2) $(\mathbb{Z}_3, +_3, \cdot_3)$ is not Boolean ring

Since $(\bar{2})^2 = \bar{1}$

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 $R \Rightarrow 1\in M \Rightarrow M=R$ C!
$\therefore I$ is max. ideal

Theorem :
$(R,+,\cdot)$ is a Boolean field if and only if $R\simeq \mathbb{Z}_2$

Proof : $\Rightarrow$) let $a\in R$, $a\neq 0$
$a = a\cdot 1 = a(a\bar{a}^{-1}) = (a\cdot a)\bar{a}^{-1} = a^2\cdot\bar{a}^{-1} = a\cdot\bar{a}^{-1} = 1$
$\therefore R=\{0,1\} \Rightarrow R\simeq \mathbb{Z}_2$

$\Leftarrow$) gt is clear

جامعة بغداد/كلية التربيه للعلوم الصرفه/ابن الهيثم
قسم الرياضيات/المرحله الثالثه
الماده الحلقات

د. هاتم + د. بشيه

الفصل السابع

Chapter Seven

Chapter Seven

حلقة الكثيرات

"Polynomail Ring"

7

Def:- Let R be any ring

Let $S = \{ f(x) : f(x) = a_0 + a_1x_1 + \cdots + a_nx^n, a_0, a_1, \ldots, a_n \in R \}$

or $\{ f(x) : f(x) = \sum_{i=0}^{n} a_i x^i, a_i = 0, \forall i > n \}$

Any $f(x) \in S$ is called Polynomail over R. Define $+, \cdot$ 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 $c_i = a_i + b_i$

$\forall i = 0, 1, \ldots, t$, $c_i = 0$ $\forall i > \max\{n, m\}$

2) $f(x) \cdot g(x) = \sum_{K=0}^{t} c_K x^K$ $c_K = 0$ $\forall K > n+m$ where

$c_0 = a_0 b_0$

$c_1 = a_0 b_1 + a_1 b_0$

$c_2 = a_0 b_2 + a_1 b_1 + a_2 b_0$

$c_3 = a_0 b_3 + a_1 b_2 + a_2 b_1 + a_3 b_0$

$\vdots$

$c_t = a_0 b_t + a_1 b_{t-1} + a_2 b_{t-2} + \cdots + a_t b_0$

or $\left\{ c_s = \sum_{i+j=s} a_i b_j \quad i, j \geq 0 \right\}$

Notice that $+_n, \cdot_n$ are closed on S.

Ex:- Let $f(x), g(x)$ be two polynomailes over Z_4 where $f(x) = 3 + x$, $g(x) = 1 - x + x^2$

$f(x) = 3 + x$, $a_0 = 3$, $a_1 = 1$, $a_2 = a_3 = \cdots = a_n = 0$

$g(x) = 1 - x + x^2$, $b_0 = 1$, $b_1 = -1 = 3 \pmod 4$, $b_2 = 1$

$b_3 = b_4 = \cdots = b_n = 0$

$$f(x) + g(x) = (a_0 +_n b_0) + (a_1 +_n b_1)x + (a_2 +_n b_2)x^2$$
$$= (1 +_4 3) + (1 +_4 3)\cdot x + (0 +_4 1)x^2$$
$$= x^2$$

$$f(x) \cdot g(x) = \sum_{k=0}^{t} c_k x^k \quad , \text{ where } c_0 = a_0 b_0 = 3 \cdot_4 1 = 3$$

$$c_1 = a_0 b_1 + a_1 b_0 = 3 \cdot_4 3 + 1 \cdot_4 1 = 2 \Rightarrow c_1 x = 2x$$

$$c_2 = a_0 b_2 + a_1 b_1 + a_2 b_0 = 3 \cdot_4 1 + 1 \cdot_4 3 + 0 \cdot_4 1 = 2$$

$$c_3 = a_0 b_3 + a_1 b_1 + a_2 b_1 + a_3 b_0 = 3 \cdot_4 0 + 1 \cdot_4 1 + 0 \cdot_4 3 + 0 \cdot_4 b_0 = 1$$

$$c_4 = a_0 \underbrace{b_4}_{0} + a_1 \underbrace{b_3}_{0} + \underbrace{a_2 b_2}_{0} + \underbrace{a_3 b_1}_{0} + \underbrace{a_n b_0}_{0} = 0$$

Since, $c_5 = c_6 = 0$

$\Rightarrow f(x) \cdot g(x) = 3 + 2x + 2x^2 + x^3$ 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 $+, \cdot$ are closed on $R[x]$.

② If $f(x) = \sum_{i=1}^{n} a_i x^i$, $g(x) = \sum_{i=1}^{m} b_i x^i$

$f(x) + g(x) = \sum_{i=0}^{t} (a_i + b_i) x^i$, $t \leq \max(n, m)$

$\sum_{i=0}^{t} (b_i + a_i) x^i = \sum_{i=0}^{m} b_i x^i + \sum_{i=0}^{n} a_i x^i = g(x) + f(x)$

$\therefore +$ 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 ($\theta(x)=1$)

Definition :

let $f(x)=\sum_{i=0}^{n} a_i x^i \in R[x]$, $f(x) \neq$ 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

let R be an integral domain, $f(x), g(x)$ non Zero poly's 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 $f(x)=a_0+a_1x+a_2x^2+\cdots+a_nx^n$ is non Zero poly.

$a_n \neq 0$, i.e $\deg f(x) = n$ حيث

let $g(x) = b_0 + b_1 x + \cdots + b_m x^m$ is a non-zero poly.

$b_m \neq 0$, i.e $\deg g(x) = m$ حيث

Notic $a_i = 0 \quad \forall i > n$

$b_i = 0 \quad \forall i > m$

$f(x) \cdot g(x) = \sum_{k=0}^{t} C_k x^k$, where $C_0 = a_0 b_0$, $C_1 = a_0 b_1 + a_1 b_0$

$C_{m+n} = \underbrace{a_0 b_{m+n}}_{=0} + \underbrace{a_1 b_{m+n-1}}_{0=} + \cdots + a_n b_m + \underbrace{a_{n+1} b_{m-1}}_{0''} + \cdots + \underbrace{a_{n+m} b_0}_{0''}$

$C_{m+n} = a_n b_m \neq 0$ (Since $a_n, b_m \in R$, $a_n \neq 0$, $b_m \neq 0$ and R has no zero divisor)

$C_{n+m+1} = a_0 b_{n+m+1} + a_1 b_{n+m} + \cdots + a_n b_{m+1} + a_{n+1} b_m + \cdots + a_{n+m+1} b_0$

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 نتيجة

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.

If $f(x), g(x) \in R[x]$, $f(x) \neq 0$, $g(x) \neq 0$

① If $f(x) = a_0 \neq 0$, $g(x) = b_0 \neq 0$

Then $f(x)g(x) = a_0 b_0 \neq 0$ since R has no zero divisor.

② If $f(x), g(x)$ 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**

نظرية القسمة

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 coficient 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 $f(x)=x^3+2x+1$, $g(x)=4x+1 \in Z_5[x]$

Divide $f(x)$ by $g(x)$.

$$\begin{array}{r|l} x^3+2x+1 & 4x+1 \\ -x^3-4x^2 & 4x^2-x+2 \\ \hline -4x^2+2x+1 & \\ +4x^2+x & \\ \hline 3x+1 & \\ +3x+2 & \\ \hline -1 & \end{array}$$

$\therefore f(x)=g(x)(4x^2-x+2)+(-1)$

Corollary (Remainder thm.)

let R be a comm ring with unity. $\forall f(x) \in R[x]$ $a \in R$. 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 $c \in R$

$\therefore f(x) = (x-a)\,q(x) + c$

نعوض بدل كل x بـ a

$\therefore f(a) = (a-a)\,q(a) + c = c \Rightarrow f(a) = c$

إذن Thus $f(x) = (x-a)\,q(x) + f(a)$

Example

$f(x) = 2x^4 + 5x^2 + 1 \in Z_6[x]$

إذن $a = 4 \in Z_6$

$\therefore 2x^4 + 5x^2 + 1 = (x-4)\,q(x) + f(4)$

$f(4) = 2\cdot 4^4 + 5\cdot 4^2 + 1 = 5$

$$
\begin{array}{r|l}
 & 2x^3 + 2x^2 + x + 4 \\
\hline
x-4 & 2x^4 + 5x^2 + 1 \\
\mp 2x^4 \quad \pm 2x^3 & \\
\hline
 & 2x^3 + 5x^2 + 1 \\
 & \mp 2x^3 \quad \pm 2x^2 \\
\hline
 & x^2 + 1 \\
 & \mp x^2 \quad \pm 4x \\
\hline
 & 4x + 1 \\
 & \mp 4x \quad \pm 4
\end{array}
$$

إذن الباقي فعلاً هو 5

5 وهو يقابل 5 في 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 If $g(x) \in R[x]$

$f(x)$ divide $g(x)$ ($f(x) / g(x)$) means $\exists\, k(x) \in R[x]$ s.t.

$g(x) = k(x) f(x)$.

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 $k(x) \in R[x]$

$x = a$ نعوض

$\iff f(a) = 0 \implies a$ is a root of $f(x)$.

Example let $f(x) = x^3 + x^2 + 1 \in Z_3[x]$

1 is a root of $f(x)$, since $f(1) = 1^3 + 1^2 + 1 = 0$ (in Z_3)

$$
\begin{array}{r|l}
x - 1 & x^3 + x^2 + 1 \\
\hline
 & x^2 + 2x + 2 \\
 & \mp x^3 \pm x^2 \\
\hline
 & 2x^2 + 1 \\
 & \mp 2x^2 \pm 2x \\
\hline
 & 2x + 1 \\
 & \mp 2x \pm 2 \\
\hline
 & 0
\end{array}
$$

$\therefore f(x) = (x-1)(x^2 + 2x + 2)$.

Examples

① $f(x)=x^2+1 \in \mathbb{R}[x]$ has no root.

② $f(x)=x^2-4 \in \mathbb{Z}[x]$ has two distinct roots

③ $f(x)=x^3-x^2+x-1 \in \mathbb{Z}[x]$ has only one root which is 1

④ $f(x)=x^2+4 \in \mathbb{Z}_5[x]$ has two roots which are 1, 4

Theorem :- let $(R,+,\cdot)$ be an integral domain and $f(x) \in R[x]$ be a non-zero of deg n. Then $f(x)$ at most n distinct roots

proof The proof is by induction

if $f(x)=ax+b$, a is an invertible element, then $-ba^{-1}$ is a root of $f(x)$, since $a(-ba^{-1})+b=0$

Suppose any poly. of deg $(n-1)$

if a is a root of $f(x)$, then $f(x)=(x-a)g(x)$

Hence $\deg(g(x))=n-1$

$n=\deg f(x) = \deg(x-1) + \deg g(x)$

$\therefore \deg g(x)=n-1$. But $g(x)$ has at most $(n-1)$ distinct roots say $a_1,\dots,a_{n-1}$. Thus $f(x)=(x-a)\underbrace{(x-a_1)\cdots(x-a_{n-1})}_{g(x)}$

$\therefore f(x)$ has at most n distinct roots.

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 $f(x)$ — لانه من الدرجه الثالثه فممكن يوجد لها ثلاثه جذور

3 " " " " "

4 is root of $f(x)$

$\therefore 1, 4$ are two root of $f(x)$
لذلك هنا نشوف الجذور المتكررة

$\therefore f(x) = (x-1)(x-4)(\,?\,)$

$\therefore f(x) = (x-1)\underbrace{(x^2+4)}_{K(x)}$

Long division (x^3+4x^2+4x+1 divided by $x-1$):

Quotient: $x^2 + 4$

$x - 1 \,)\, x^3 + 4x^2 + 4x + 1$

$\mp x^3 \pm x^2$

$4x + 1$

$\mp 4x \pm 4$

0

1 is root of $K(x)$

4 " " " "

$x^2 + 4 = K(x) = (x-1)(x-4) \Longrightarrow \therefore f(x) = (x-1)\underbrace{(x-1)(x-4)}_{K(x)}$

Theorem:

If F is a field then $F[x]$ is a P.I.D.

proof

F is field $\rightarrow$ F is an integral domain

$\Longrightarrow F[x]$ " "

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 $I=id(p(x))$. To prove that $id(p(x)) \subseteq I$. For any $f(x) \in id(p(x))$

$\therefore f(x)=k(x)\underbrace{p(x)}_{\in I} \in I \Rightarrow id(p(x)) \subseteq I$

for any $g(x) \in I$. To prove $I \subseteq id(p(x))$

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 $r(x)=0$

$\Rightarrow g(x)=s(x)p(x) \in id(p(x))$

$\therefore I \subseteq id(p(x))$. Therefore $I=id(p(x))$

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 $\Leftrightarrow$ it is max.

Proof: F is field $\Rightarrow F[x]$ is PID, so a non-trivial ideal in PID is prime $\Leftrightarrow$ it is max

Example show that $\mathbb{Z}[x]$ is not PID.

let $I = \{a_1 x + a_2 x^2 + \dots + a_n x^n, a_i \in \mathbb{Z}\}$

I is not max (problem)

$\therefore \mathbb{Z}[x]$ 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 $f(x) = x^2 + 4 \in \mathbb{R}[x]$

f is irreducible لأنه

② let $f(x) = x^2 + 4 \in \mathbb{Z}_5[x] = (x+1)(x+4)$

$f(x)$ is reducible لأنه

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 $f(x)$

لأن $f(x)$ يقسم على $(x-a)$ root لأنه

$x-a \mid f(x)$

$\therefore (x-a) / f(x) \Rightarrow \exists\, g(x) \in F[x]$ 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 irrducible $\Rightarrow f(x)$ has no root مناقشة الكل

Example :- $f(x) = x^2 + 1 \in \mathbb{R}[x]$

$f(x)$ is irrducible $\Rightarrow f(x)$ has no roots

Remark : If $f(x)$ is reducible poly., then it is not necessary that $f(x)$ has roots.

معروفاً بعض الدوال ذات الدرجة الأكثر من 3 يكون لها تحليل أولي ولكنها لا تحتمل تحليلة أخرى تقف

Example :- let $f(x) = x^4 + 5x^2 + 4 \in \mathbb{R}[x]$

$f(x)$ is reducible, since $f(x) = (x^2+1)(x^2+4)$.

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 → متحقق دائماً

$\Leftarrow$) If $\deg f(x) = 3$, $f(x)$ is reducible

$\therefore \exists\ g(x), h(x)$ of poly's s.t. $f(x) = g(x)h(x)$

$3 = \deg f(x) = \deg g(x) + \deg h(x)$

$\therefore \deg g(x) = 1,\ \deg h(x) = 2$ or $\deg g(x) = 2,\ \deg h(x) = 1$

Case ① $\deg g(x) = 1$ and $\deg h(x) = 2$

$g(x) = ax + b,\ a \neq 0$

$\therefore g(x)$ has a root, $c = -ba^{-1}$ that is $g(c) = 0$

Hence $f(c) = g(c)h(c) = 0 \cdot h(c) = 0$

$\therefore c$ is a root of $f(x)$

Similarly Case ② : $\deg f(x) = 2 \Longrightarrow \deg g(x) = 1$, $\deg h(x) = 1$

Theorem: Let F be a field. Then the following are equivalent:

① $f(x)$ is irreducible poly. in $F[x]$

② $\mathrm{id}(f(x))$ is max. (prime) ideal in $F[x]$

③ $F[x]/\mathrm{id}(f(x))$ is a field.

Proof ① $\Longrightarrow$ 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 $I = id(f(x))$ is max.

suppose $\exists$ ideal J in F[x] s.t. $I \subsetneq J \subsetneq F[x]$

since F[x] is P.I.D, $\therefore \exists\ g(x) \in F[x]$ s.t.

$id(g(x)) = I$

$\therefore id(f(x)) \subsetneq id(g(x)) \subsetneq F[x]$, since $f(x) \in id(f(x))$

$\therefore f(x) \in id(g(x)) \Longrightarrow f(x) = h(x)g(x)$ (نفرض $x \in id(x) \iff x = 0$)

if $h(x) = c \neq 0$ (Constant) ثابت

$\therefore f(x) = cg(x) \Longrightarrow g(x) = c^{-1} f(x) \in id(f(x))$

$\Longrightarrow J = id(g(x)) \subseteq id(f(x))$ C!

Thus h(x) is a poly of deg ≥ 1

$\therefore f(x) = h(x)g(x)$ C! وهذا يناقض الفرض عبارة واحد

② $\Longrightarrow$ ③ id(f(x)) is max ideal $\Longrightarrow$ F[x]/id(f(x)) is fie

③ $\Longrightarrow$ ① نفرض العكس

F[x]/id(f(x)) field $\Longrightarrow$ f(x) is irreducible in F[x]

suppose f(x) is reducible

$\exists\ g(x), h(x) \in F[x]$ of positive degree s.t. $f(x) = g(x)h(x)$

$id(f(x)) \subsetneq id(g(x)) \subseteq F[x] \Longrightarrow id(f(x))$ is not max

$\therefore$ F[x]/id(f(x)) is not field C!

جامعة بغداد/كلية التربيه للعلوم الصرفه/ابن الهيثم
قسم الرياضيات/المرحله الثالثه
الماده/حلقات

الفصل الثامن والتاسع

Chapter Eight and Nine

Chapter eight

"8"

مقدمة لنظرية جالوا
Introduction to Galois theory

في البداية سوف نتذكر تعريف الحقل

Definition :

let $F \neq \emptyset$. Then $(F, +, .)$ is called field if every element $a \in F$, a is an invertible element.

Examples : $(\mathbb{Z}, +, .)$, $(\mathbb{R}, +, .)$, $(\mathbb{Q}, +, .)$

$(\mathbb{Q}[\sqrt{2}], +, .)$, where $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \; ; \; a, b \in \mathbb{Q}\}$

Definition :

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

Remark :

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

$$\left.\begin{array}{l} (1)\ a - b \in S \\ (2)\ a \cdot b^{-1} \in S \end{array}\right\} \forall a, b \in S$$

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
$S(F,f) = \{K : K$ is an extension of F and contains all roots of $f(x)\}$.
And
$R_t(F,f) = \cap\{K : K \in S(F,f)\}$

Examples :

(1) let $f(x) = x^2 - 2 \in Q[X]$

$\mp\sqrt{2}$ are roots of $f(x)$

$\therefore R_t(Q,f) = Q[\sqrt{2}] = \{a+b\sqrt{2} : a,b \in Q\}$

(2) let $f(x) = x^2 + 1 \in Q[X]$
$\mp i$ are roots of $f(x)$

$\therefore R_t = (Q,f) = Q[i] = \{a+ib : a,b \in Q\}$

Definition : let K be an extension of a field F. K is called a normal extension of F, if $\exists$ $f(x) \in F[X]$ s.t. $R_t(F,f) = K$.

Ex :-

$\underbrace{Q[\sqrt{2}]}_{K}$ is a normal extension of $\underbrace{Q}_{F}$

since $\exists\ f(x) = x^2 - 2 \in Q[X] \ni R_t(Q, f) = Q[\sqrt{2}]$

Definition : تعريف .poly القابلة للحل بواسطة الجذور الذهاب من رتبة الأعداد ص ب ن + 8

let $f(x) \in F[X]$, $K = R_t(F, f)$

$f(x)$ is Called solvable by radical if $\exists$ a finite sequence

قابلة للحل بواسطة الجذور

$F = L_0 \subseteq L_1 \subseteq L_2 \subseteq \cdots \subseteq L_n = K$ ← أصغر حقل جزئي يحتوي على الحل

where $L_i = R_t(L_{i-1}, f_i)$, $f_i(x) = x^{n_i} - a_i$

Example : let $f(x) = ax + b \in F[X]$, $a \neq 0$

$x = \frac{-b}{a}$ جذر الدالة

$\therefore L_0 = R_t(F, f) = Q$

$\therefore F = L_0 = R_t(F, f) = Q$

$\therefore f(x)$ is solvable by radical

Example :- let $f(x) = ax^2 + bx + c \in Q[X]$

نستخرج جذور $f(x)$ بالدستور

$x = \frac{-b \mp \sqrt{b^2 - 4ac}}{2a}$

$Q = L_0 \subseteq L_1 = R_t(Q, f_1)$ where $f_1 = x^{n_1} - a_1$

$= x^2 - b$

Definition : let $f(x) \in F[x]$, $K = R_t(F, f)$. Then $gp(G(K/F), o)$ is called Galoies gp.
زمرة گالوا

Theorem Fundamental theorem of Galois
المبرهنة الاساسية لگالوا

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 $\gamma : S \to \bar{S}$ define by $\gamma(E) = G(K/E)$. Then

(1) γ 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 $E \subseteq E'$

$\Rightarrow \gamma(E') \setminus \gamma(E) = G(E/E')$

هذه هي نص النظرية

"9"

Modules:- الموديولات Chapter nine

Def:- Let R be a ring with identity. An abelain group $(M,+)$ is called a Left R-module (or Left R-module over R) if there exists a mapping $\alpha: R \times M \to M$ such that $\alpha(r,m) = rm$ $\forall r \in R$ and $\forall m \in M$ satisfying the following conditions:-

① $\alpha(r, m_1 + m_2) = \alpha(r, m_1) + \alpha(r, m_2)$ or $r(m_1 + m_2) = rm_1 + rm_2$ $\forall r \in R$ $\forall m_1, m_2 \in M$.

② $\alpha(r_1 + r_2, m) = \alpha(r_1, m) + \alpha(r_2, m)$ or $(r_1 + r_2)m = r_1 m + r_2 m$ $\forall r_1, r_2 \in R$, $\forall m \in M$.

③ $\alpha(r_1 r_2, m) = \alpha(r_1), \alpha(r_2, m)$ or $(r_1 r_2)m = r_1(r_2 m)$ $\forall r_1, r_2 \in R$, $\forall m \in M$.

④ if in addition $1m = m$ $\forall m \in M$, then M is called a unital R-module.

Examples: ① Every abelain group with $+$ is a $\mathbb{Z}$ module

② $\mathbb{Z}_n$ is a $\mathbb{Z}$-module $\forall n \in \mathbb{N}$

③ $\mathbb{Q}$ is a $\mathbb{Z}$-module

④ Let R be a ring then every left ideal I of R is a left R-module.

⑤ $n\mathbb{Z}$ is a $\mathbb{Z}$-module $\forall n \in \mathbb{N}$

⑥ Every ring R can be considered as an R-module (a module over itself).

المودولات الجزئية

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. $rx \in N \quad \forall r \in R, \forall x \in N$

Examples :-

(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 prim number p, Z_p is a simple 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 : nZ is a submodule of $Z \quad \forall n = 0, 1, 2, \ldots$

(3) $\dot{Z}$ is a Z-module of Q over Z

Remark :- (1) If N and K are two submodules of an R-module M, then $N \cap K$ is also a submodule

~~If $\{N_i\}_{i\in I}$ is any collection of submodules of an R-modules M, then $\bigcap_{i\in I} N_i$ is also a submodule of M~~

البرهان الجزئي بالتمارين

Def :-

Let M be an R-module and Let $x \subseteq M$, 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

$(x) = \bigcap \{ N : N \text{ is a submodule of } M \text{ and } N \supseteq x \}$

The set $X = (x)$ is called a generating set of (x)

Equivalentely :- (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 Z as Z-module is cyclic since $Z = (1)$

② E is cyclic submodule of Z since $E = (2)$

In general $nZ = (n)$ is cyclic submodule of Z $\forall n \in Z_+$

③ Z_n is a cyclic Z-module since $Z_n = (\bar{1})$ $\forall n Z_+$

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 $f : M \to N$ is called an R-homomorphism if :-

(1) $f(m_1 + m_2) = f(m_1) + f(m_2)$ $\forall m_1, m_2 \in M$

(2) $f(rm) = r f(m)$ $\forall r \in R$, $\forall m \in M$.

Example :- (1) Let M and N be any R-modules. Let $f : M \to N$ be such that $f(m) = 0_N$ $\forall m \in M$, then f is as an R-module, f is called the trivail homo. from M into N.

Sol :- (1) $\forall m_1, m_2 \in M$ s.t $f(m) = 0_N$ $\forall m \in M$

$f(m_1 + m_2) = 0_N$ (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 $I_M : M \to M$ is an R-homomorphism. I_M is called the identity homomorphism on M.

Sol (H.W)

(3) If $f(m) = c$ $\forall m \in M$, then f is not homo.

since $f(m_1 + m_2) \neq f(m_1) + f(m_2)$

$c \neq c + c$

(4) If N a submodule of an R-module M, the inclusion map $i_N : N \to N$ is an R-homo.

i_N is called the inclusion homo. on N.

Sol ① $i_N(m_1+m_2) = m_1+m_2 = i_N(m_1)+i_N(m_2)$ $\forall m_1, m_2 \in M$

② $i_N(rm) = rm = r\,i_N(m)$ $\forall r \in R$, $\forall m \in M$.

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) $(x+N)+(y+N) = (x+y)+N$ $\forall x, y \in M$

(2) $r(x+N) = rx+N$ $\forall r \in R$, $\forall x \in M$.

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 $\Pi : M \to M/N$ such that $\Pi(m) = m+N$ $\forall m \in M$, Π is an R-homo. it is called the natural homo.

Sol:- (1) $\Pi(m_1+m_2) = (m_1+m_2)+N = (m_1+N)+(m_2+N)$ $\forall m_1, m_2 \in M$ $= \Pi(m_1)+\Pi(m_2)$

(2) $\Pi(rm) = rm+N = r(m+N) = r\Pi(m)$ $\forall r \in R$, $\forall m \in M$.

Def:- Let $f : M \to N$ be an R-homo.

(1) Kernal of f denoted by $\ker f$, it is the set $\ker f = \{x \in M : f(x) = 0\} \subseteq M$

(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:

Let $f : M \to N$ 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 $f: M \to N$ 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 $f: M \to N$ is an R-homo, then

$$M/\ker f \cong \operatorname{Im} f$$

proof:- Define $g: M/\ker f \to \operatorname{Im} f$ such that

$$g(x+\ker f) = f(x) \quad \forall x \in M.$$

T.P g is well-defined?

Let $x_1+\ker f = x_2+\ker f$ in $M/\ker f$.

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

$\Rightarrow f(x_1-x_2)=0$ (define of kerf).

$\Rightarrow f(x_1)-f(x_2)=0$ (define of homo).

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

$\Rightarrow$ g is well-defined.

T.P g is homo?

Let $m_1+\ker f, m_2+\ker f \in M/\ker f$

① $g[(m_1+\ker f)\oplus(m_2+\ker f)] = g[(m_1+m_2)+\ker f] = f(m_1 \oplus m_2)$

$= f(m_1)\oplus f(m_2)$

$= g(m_1+\ker f)\oplus g(m_2+\ker f)$

② $\forall r \in R, m+\ker f \in M/\ker f$

$g[r(m+\ker f)] = g(rm+\ker f) = f(rm) = r f(m)$ (f is homo)

~~$= r\,g(m+\ker f)$, 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:

$g(m_1+\ker f) = g(m_2+\ker f)$

$f(m_1) = f(m_2)$

$f(m_1) - f(m_2) = 0$

$f(m_1 - m_2) = 0$ since f 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 onto ?

Let y be any element of Im f

$\because$ f is onto $\Rightarrow \exists x \in M$ s.t $f(x)=y$

$\Rightarrow g(x+\ker f)=y$

$\therefore$ g is onto.

Corollary :- If $f: M \to N$ is an epimorphism, then $M/\ker f \simeq N$

Theorem (2) :- If K and L are two submodules of an R-module M. Then $K/L \cap K \simeq K+L/L$

proof :- Define $f: K \to (K+L)/L$ s.t $f(x) = x+L \ \forall x \in K$

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

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?

(1) 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 $r \in R \wedge x \in K$, $f(rx) = rx+L = r(x+L) = rf(x)$

$\therefore$ f is homo.

T.P f is onto?

Let $(x+y)+L \in (K+L)/L$ where $x \in K \wedge y \in L$

$(x+y)+L = (x+L)+(y+L) = (x+L)+L = x+L$ ($y+L \in L$)

$= f(x)$

$\therefore$ f is onto.

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

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

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

$= \{x \in K : x+L = L\}$

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

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 $L/K \leq M/K$?

Let $L/K = \{a+K, a \in L\}$

$M/K = \{m+K, m \in M\}$

$0+K \in L/K$, $0 \in L \Rightarrow L/K \neq \phi$

$\forall\ a+K \in L/K \Rightarrow a+K \in M/K$ (since $L \leq M$)

$\therefore L/K \leq M/K$

$\forall\ a_1+K, a_2+K \in L/K$

$(a_1+K)+(a_2+K) = (a_1+a_2)+K \in L/K$ (since $a_1+a_2 \in L$)

$\forall\ r \in R, \forall\ a+K \in L/K$ T.P $r(a+K) \in L/K$?

$r(a+K) = ra+K \in L/K$ (since $L \leq M$)

$\therefore r(a+K) \in L/K$

$\therefore L/K$ is a submodule of M/K.

(2) Define $f: M/K \to M/L$ s.t $\therefore f(m+K) = m+L$ $\forall m \in M$.

T.P f is well defined?

$\forall m+K \in M/K \Rightarrow m+L \in M/L \Rightarrow f(m+K) \in M/L$

If $m_1+K = m_2+K \Rightarrow m_1-m_2 \in K \Rightarrow m_1-m_2 \in L$

$\Rightarrow m_1+L = m_2+L$

$\Rightarrow f(m_1+K) = f(m_2+K)$

T.P f is homo?

① $\forall m_1+K, m_2+K \in M/K \Rightarrow f[(m_1+K) \oplus (m_2+K)] = f[(m_1+m_2)+K]$

$= (m_1+m_2)+L = (m_1+L)+(m_2+L)$

$= f(m_1+K) + f(m_2+K)$

② $f[r(m+K)] = f[rm+K]$ (since M is an R-module)

$= rm+L = r(m+L) = rf(m+K)$

$\therefore f$ is homo.

T.P f is onto?

$Imf = \{f(m+K) : m \in M\}$

$= \{m+L : m \in M\} = M/L$.

$\therefore f$ is onto.

By Theorem 1 $\Rightarrow M/Kerf \simeq M/L$

T.P $Kerf = L/K$

$Kerf = \{(m+K) \in M/K : f(m+K) = L\}$

$= \{(m+K) \in M/K : m+L = L\}$

$= \{m+K \in M/K : m \in L\} = L/K$

$\therefore M/K / L/K \simeq M/L$

ملحمہ فصل

اکویولات

Theory of Modules

Def: Let R be a ring (not necessarily commutative with identity). An abelian group $(M,+)$ is called a left R-module (or left R-space over R) if there exists a mapping

$$R \times M \longrightarrow M \quad \text{s.t.} : \quad \lambda(r,m) = rm \quad \forall r \in R \text{ and } m \in M.$$

satisfying the following conditions :

1. $\lambda(r, m_1+m_2) = \lambda(r, m_1) + \lambda(r, m_2)$ OR
   $r(m_1+m_2) = rm_1 + rm_2 \quad \forall r \in R \text{ and } \forall\, m_1, m_2 \in M$

2. $\lambda(r_1+r_2, m) = \lambda(r_1, m) + \lambda(r_2, m)$ OR
   $(r_1+r_2)m = r_1m + r_2m \quad \forall\, r_1, r_2 \in R,\ m \in M$

(3) $\alpha(r_1 r_2, m) = r_1 \alpha(r_2 m)$ or $\underline{r}$
$(r_1 r_2)m = r_1(r_2 m) \quad \forall r_1, r_2 \in R, \forall m \in M.$

(4) If in addition $1.m = m \ \forall m \in M$. 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 $M \times R \to M$ with $(m, r) \to mr \ \forall m \in M, \forall r \in R$ satisfying :-

$$\left.\begin{array}{ll} (1) & m(r_1 + r_2) = mr_1 + mr_2 \\ (2) & (m_1 + m_2)r = m_1 r + m_2 r \\ (3) & m(r_1 r_2) = (mr_1) r_2 \\ (4) & m.1 = m \end{array}\right\} \forall r, r_1, r_2 \in R \wedge \forall m, m_1, m_2 \in M.$$

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 $1.m = m \ \forall m \in M$. (i.e $(1, m) \to m \ \forall m \in M$)

Examples :-
(1) Every additive abelian group is a Z-module.

Solution :- Let $(M, +)$ be an abelian gp.
Define a mapping $\phi : Z \times M \to M$ s.t
$\phi(n, a) = na$ where

$$na = \begin{cases} a + a + \cdots + a \ (n\text{-times}) & \text{if } n > 0 \\ (-a) + (-a) + \cdots + (-a) \ (n\text{-times}) & \text{if } n < 0 \end{cases}$$

Now, we satisfying the conditions:-

(i) $\phi(n, a_1+a_2) = n(a_1+a_2)$

$$= \begin{cases} (a_1+a_2)+\cdots+(a_1+a_2) & (n\text{-times}) \\ & \text{if } n>0 \\ (-(a_1+a_2))+\cdots+(-(a_1+a_2)) & (n\text{-times}) \\ & \text{if } n<0 \end{cases}$$

$$= \begin{cases} \underbrace{a_1+a_1+\cdots+a_1}_{n\text{-times}} + \underbrace{a_2+a_2+\cdots+a_2}_{n\text{-times}} \\ \underbrace{(-a_1)+(-a_1)+\cdots+(-a_1)}_{n\text{-times}} + \underbrace{(-a_2)+\cdots+(-a_2)}_{n\text{-times}} \end{cases}$$

$$= na_1 + na_2$$
$$= \phi(n, a_1) + \phi(n, a_2)$$

وهكذا تطبق بقية الشروط بنفس الطريقة .

(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 left ideal of R is an R-module.

Sol:- Since $(I,+)$ is abelian gp and
$ra \in I$, $\forall r \in R \wedge \forall a \in I$
اي نقصد هنا ان عملية الضرب معرفه بالاضافه لعملية الجمع وهي مغلقه .

(i) $(r, a_1+a_2) = \underbrace{r(a_1+a_2)}_{\in I} = \underbrace{ra_1}_{\in I} + \underbrace{ra_2}_{\in I}$ من خاصية التوزيع
$= \alpha(r, a_1) + \alpha(r, a_2)$
$\forall r \in R, \forall a_1, a_2 \in I$

(ii) $(r_1+r_2, a) = (r_1+r_2)a = r_1a + r_2a$
$= \alpha(r_1, a) + \alpha(r_2, a)$

(iii) $(r_1 r_2)a = r_1(r_2 a)$ $\in I$ $\in I$ من شرط الحلقة تجميعية.
$= r_1 a(r_2, a)$.

(iv) $1 \cdot a = a \in I$

(4) nZ is a Z-module $\forall n \in N$.

For examples:-

$nZ = id(n)$
$2Z = id(2)$ is a Z-module.
$3Z = id(3)$ " " " "
⋮ ⋮

(5) Let R be a ring and I be a left ideal in R and $R\backslash I = \{a+I, a \in R\}$. Then $(R\backslash I, \oplus)$ is abelian gp where $(a+I) \oplus (b+I) = (a+b) + I$ $\forall a, b \in R$.
Define: $\alpha : R \times R\backslash I \longrightarrow R\backslash I$ s.t
$\alpha(r, a+I) = ra + I$ $\forall r \in R$ and $\forall a+I \in R\backslash I$.
Then $R\backslash I$ is an R-module.

sol:- (i) $\alpha(r, (a+I) \oplus (b+I)) = r(a+b) + I$
$= ra + rb + I$
$= (ra + I) \oplus (rb + I)$
$= \alpha(r, a+I) \oplus \alpha(r, b+I)$
where $I + I = I$

(ii) $\alpha(r_1 + r_2, a+I) = (r_1 + r_2)a + I$
$= r_1 a + I \oplus r_2 a + I$
$= (r_1, a+I) \oplus (r_2, a+I)$
$= \alpha(r_1, a+I) \oplus \alpha(r_2, a+I)$
وبنفس الطريقة نثبت الشرط الثالث والرابع.

For example:- Take $R=\mathbb{Z}$, $I=n\mathbb{Z} \Rightarrow R\setminus I = \mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}_n$ 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: $\alpha : M_{m\times n}(R) \times M_{m\times n}(R) \longrightarrow M_{m\times n}(R)$ 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.

∴ حالة خاصة من هذا المثال نحصل عليها عندما يكون $m=1$

$M_{1\times n}(R)$ = 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

$R \times R^n \longrightarrow R^n$ such that $r(a_1,\dots,a_n) = (ra_1,\dots,ra_n)$

$\forall r \in R, \forall (a_1,\dots,a_n) \in R$.

R^n is an R-module.

(7) Let R and S be two rings and Let $f: R \to S$ 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 $\alpha: S\times M \to M$ s.t $\alpha(s,m) \to sm$ $\forall s \in S \wedge \forall m \in M$ satisfying 1,2,3,4 in the def.

Define $\beta: R\times M \to M$ s.t $\beta(r,m) = \grave{r}m$

or $\beta(r,m) = f(r)m$, $\forall m \in M$

- 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 $r_1, r_2 \in R \wedge m \in M$

$(r_1 + r_2, m) = f(r_1 + r_2) \cdot m = [f(r_1) + f(r_2)]m$ (homo ملاحظة)

$= f(r_1)m + f(r_2)m$

$= (r_1, m) + (r_2, m)$.

(iii) check

(iv) Since R is a ring with unity $\Rightarrow \exists 1$ is an identity element

- But f is homo $\Rightarrow f(1) = 1'$ the identity element of S.

Now, $\forall m \in M \Rightarrow (1, m) = f(1) \cdot m = 1' \cdot m = m$.

Thus M is an R-module.

(8) Let M be an additive abelain group and Let

End(M) = The set of all group homomorphisms on M.

i.e $End(M) = \{f / f: M \to M, f \text{ is a group. homo.}\}$

Define: + and o on End(M) as follows:-

$(f+g)(m) = f(m) + g(m) \quad \forall f, g \in End(M), \forall m \in M.$

$(f \circ g)(m) = f(g(m)) \quad \forall f, g \in End(M), \forall m \in M.$

Then:- (1) $(End(M), +, o)$ is a ring with identit

(2) M is an End(M) − module.?

Pf: (1) T.P (End(M), +) is abelain gp ?

(i) Let $f, g \in End(M)$

$= f(m) + g(m) = f+g(m)$ $\forall f, g \in End(M)$ $\forall m \in M$.

Thus + is closed.

(ii) Let $f, g, h \in End(M)$:

$((f+g)+h)(m) = (f+g)(m) + h(m)$

$= (f(m) + g(m)) + h(m)$

$= f(m) + (g(m) + h(m))$

$= (f + (g+h))(m)$

Therefore + is ass.

بخواص بزغرك واجب

$\therefore (End(M), +)$ is abelian gp.

(2) Define: $\phi : End(M) \times M \to M$ s.t

$\phi(f, m) = f(m)$ $\forall f \in End(M), \forall m \in M$.

Pf:- (i) Let $f \in End(M)$, $m_1, m_2 \in M$

$(f, m_1 + m_2) = f(m_1 + m_2) = f(m_1) + f(m_2)$

$= (f, m_1) + (f, m_2)$ (since f is homo.

(ii) $(f+g)(m) = (f+g)(m)$, $\forall f, g \in End(M), \forall m \in M$

$= f(m) + g(m)$

$= (f, m) + (g, m)$

(iii) Let $f, g \in End(M)$, $m \in M$.

$(fog, m) = (fog)(m) = f(g(m)) = (f, g(m))$

$= (f, (g, m))$

(VI) since $(I, m) = I(m) = m$ where I is the identity map.

Thus

M is $End(M)$ - 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 $r \in R \wedge \forall s \in S \wedge \forall m \in M$

Ex :- $M_{mxn}(R)$ is an $M_{mxm}(R) - M_{nxn}(R)$ - bimodule.

row = column

Def :-

Let M be an R-module. The left annihilator of M over R denoted by $ann_R(M)$ (or $ann M$), and, it is defined by:

$$ann_R(M) = \{r \in R : rm = 0, \forall m \in M\}$$

Note :- If $ann_R(M) = 0$, 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- $(-r)m = -(rm) = r(-m) \quad \forall r \in R, \forall m \in M$

Pf:- (1) $0_R \cdot m = (0+_R 0)\cdot m = 0\cdot m + 0\cdot m$ (التوزيع)

بتعديل بجمع، $0\cdot m + (-(0\cdot m)) = 0\cdot m + 0\cdot m + (-(0\cdot m))$

$0 = 0\cdot m$

(2) $r\cdot 0_M = r\cdot(0+_M 0) = r\cdot 0 + r\cdot 0$

$r\cdot 0 + (-(r\cdot 0)) = r\cdot 0 + (r\cdot 0 + (-(r\cdot 0)))$

(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) $\operatorname{ann}_R M$ is a left ideal of R.

(2) M is a faithful $R/\operatorname{ann}_R M$-module.

Pf: Exercise.

Remark:- Let M be an R-module and I be an ideal of R. If $I \subseteq \operatorname{ann}_R M$, then M is an R/I-module.

Pf: Define $\phi : R/I \times M \to M$ s.t.:

$\phi(r+I, m) = rm$. $\forall\, r+I \in R/I,\ \forall\, m \in M$

ϕ is an mapping?

Let $(r+I, m_1) = (b+I, m_2)$ in $R/I \times M$.

$\Rightarrow r+I = b+I \ \wedge\ m_1 = m_2$ (من تعريف المساواة)

$r+b \in I$

$\Rightarrow b-a \in \operatorname{ann} M \Rightarrow (a-b)m = 0 \quad \forall m \in M$

$\Rightarrow am - bm = 0$

$am = bm$

$\phi(a+I, m) = \phi(b+I, m)$

$\therefore \phi$ is well-defined.

برهان بشرط الأخرى واجب.

Ex:- Z_6 is a Z_3-module. since

$$\operatorname{ann} Z_6 = 6Z \subseteq 3Z = I$$

$\therefore Z_6$ is a $Z/6Z \cong Z_3$-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) $a-b \in N \quad \forall a, b \in N$

(2) $ra \in N \quad \forall a \in N, \forall r \in R$.

نلاحظ من خلال التعريف أن:

(شرط الأول: يعني أن $(N,+)$ زمرة جزئية من الزمرة $(M,+)$)

(شرط الثاني: يعني أن، كل تأثير $f: R \times M \to M$ تم اقتصارها على $R \times N$ تأثيرا $f: R \times N \to N$).

أي أن المودول الجزئي من المودول M هو بنفسه مودول على نفس الحلقة.

Remark:- Let M be an R-module and $\phi \neq N \subseteq M$.

Then N is a submodule of M if and only if $ra + sb \in N \quad \forall a, b \in N, \forall r, s \in R$