[illegible]
[illegible]

[illegible]

[illegible]
[illegible]
[illegible]
[illegible]
[illegible]
[illegible]

جامعة بغداد/كلية التربيه للعلوم الصرفه/ابن الهيثم

قسم الرياضيات/المرحله الثالثه

الماده الحلقات

د. حاتم + د. بثينه

الفصل السابع

Chapter Seven

Scanned by CamScanner

حلقة الحدوديات

Chapter Seven

7

"Polynomail Ring"

Def:- Let R be any ring

Let $S = \{ f(x) ; f(x) = a_0 + a_1x_1 + \dots + a_nx^n , a_0, a_1, \dots, a_n \in R$

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

Any $f(x) \in S$ is called Polynomail over R. Define $+, \cdot$ as by:-

Let $f(x), g(x) \in S$; $f(x) = \sum_{i=0}^{n} a_ix^i , a_i \in R , a_i = 0 \ \forall i > n$

$g(x) = \sum_{i=0}^{m} b_ix^i , b_i \in R , b_i = 0 \ \forall i > m$

الجمع $f(x) + g(x) = \left(\sum_{i=0}^{t} c_ix^i \right) \in S$ where $c_i = a_i + b_i$

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

الضرب $f(x) \cdot g(x) = \sum_{k=0}^{t} C_kx^k$ $C_k = 0 \ \forall k > n+m$ where

$C_0 = a_0b_0$

$C_1 = a_0b_1 + a_1b_0$

$C_2 = a_0b_2 + a_1b_1 + a_2b_0$

$C_3 = a_0b_3 + a_1b_2 + a_2b_1 + a_3b_0$

$\vdots$

$C_t = a_0b_t + a_1b_{t-1} + a_2b_{t-2} + \dots + a_tb_0$

or $\boxed{C_s = \sum_{i+j=s} a_ib_j \quad i, j \geq 0}$ الصيغة العامة

~~Notice that $+ , \cdot$ are closed on S.~~

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

$f(x) = 3 + x$, $a_0 = 3$, $a_1 = 1$, $a_2 = a_3 = \cdots = a_n =$
$g(x) = 1 - x + x^2$, $b_0 = 1$, $b_1 = -1 = 3 \pmod 4$, $b_2 = 1$
نغيرها
$b_3 = b_4 = \cdots = b_n = 0$

$$f(x) + g(x) = (a_0 \overset{n}{+} b_0) \overset{n}{+} (a_1 \overset{n}{+} b_1) x \overset{n}{+} (a_2 \overset{n}{+} b_2) x^2$$
$$= (1 \underset{4}{+} 3) + (1 \underset{4}{+} 3) \cdot x + (0 + 1) x^2$$
$$= x^2$$

$$f(x) \cdot g(x) = \sum_{k=0}^{t} c_k X^k \quad , \text{ where } C_0 = a_0 b_0 = 3 \underset{4}{\cdot} 1 = 3$$

$$C_1 = a_0 b_1 + a_1 b_0 = 3 \underset{4}{\cdot} 3 + 1 \underset{4}{\cdot} 1 = 2 \Rightarrow C_1 X = 2X$$

$$C_2 = a_0 b_2 + a_1 b_1 + a_2 b_0 = 3 \underset{4}{\cdot} 1 + 1 \underset{4}{\cdot} 3 + 0 \underset{4}{\cdot} 1 = 2$$

$$C_3 = a_0 b_3 + a_1 b_1 + a_2 b_1 + a_3 b_0 = 3 \underset{4}{\cdot} 0 + 1 \underset{4}{\cdot} 1 + 0 \underset{4}{\cdot} 3 + 0 \underset{4}{\cdot} b_0 = 1$$

$$C_4 = a_0 \underbrace{b_4}_{0} + a_1 \underbrace{b_3}_{0} + \underbrace{a_2}_{0} b_2 + \underbrace{a_3}_{0} b_1 + \underbrace{a_n}_{0} b_0 = 0$$

[illegible]
Since, $C_5 = C_6 = 0 \cdots$

$\therefore f(x) \cdot g(x) = 3 + 2X + 2X^2 + X^3$ 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 $R[X]$.
نرمز لها

Show that $(R[x], +, \cdot)$ is a ring.

① $+, \cdot$ are closed on $R[x]$.

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

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

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

$\therefore$ + is Comm

تجميعية

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 $f(x) + [(-f)(x)] = \underset{\text{محايد جمعي}}{0} = h(x)$

$\therefore -f(x)$ is the additive inverse of $f(x)$

- asso. on $R[x]$.

, dist. over + on $R[x]$.

$\therefore R[x]$ is a ring.

٤/8

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 Cofficient

- 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 $f(x)$.

أهمية

Theorem "1 مهم جدا

let R be an integral domain, $f(x), g(x)$ non zero poly's in $R[X]$ then:

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

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 $\deg f(x) = n$ لانها ليست صفرية

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

$b_m \neq 0$, i.e $\deg g(x) = m$ لانها ليست صفرية

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 $C_0 = a_0 b_0$, $C_1 = a_0 b_1 + a_1 b_0$

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

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

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

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 $f(x)g(x) = a_0b_0 \neq 0$ since R has no zero divisor.

② If $f(x), g(x)$ are non-zero poly. of degrees n, m respectively then $f(x) \cdot g(x)$ 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 $\boxed{\text{The Division Algorithm}}$

نظرية خوارزمية 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

$$f(x) = q(x)g(x) + r(x) \quad \text{where } r(x) = 0 \text{ or } \deg r(x) < \deg g(x)$$

ooo———ooo

Example

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

Divide $f(x)$ by $g(x)$.
قسم

$2 \cdot 4 = 8$
5 [illegible]
3 [illegible]

$$
\begin{array}{rl}
 & 4x^2 - x + 2 \\
4x+1 \,\big) & \cancel{x^3} + 2x + 1 \\
 & \mp \cancel{x^3} \mp 4x^2 \\ \hline
 & -\cancel{4x^2} + 2x + 1 \\
 & \pm \cancel{4x^2} \pm x \\ \hline
 & 3\cancel{x} + 1 \\
 & \mp 3x \mp 2 \\ \hline
 & -1
\end{array}
$$

$\therefore f(x) = g(x)\underbrace{(4x^2 - x + 2)}_{q(x)\ \text{الناتج}} + \underbrace{(-1)}_{r(x)\ \text{الباقي}}$

Corollary (Remainder thm.)
نظرية الباقي

let R be a comm ring with unity. If $f(x) \in R[x]$, $a \in R$. Then $\exists!$ (يوجد وحيد) $q(x) \in R[x]$ 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

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

عندئذ Thus $f(x) = (x-a)\,q(x) + f(a)$

Example

$f(x) = 2x^4 + 5x^2 + 1 \in \mathbb{Z}_6[x]$

نأخذ $a = 4 \in \mathbb{Z}_6$

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

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

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

اذن الباقي فعلاً هو 5

5 وهو يمثل 5 في $\mathbb{Z}_6$

Definition

If $f(x) \in R[x]$, then

① $a \in R \wedge f(a) = 0$, then a is called a root of $f(x)$.

② 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 $a \in R$) $\Longleftrightarrow$ a is a root of $f(x)$.

Proof $(x-a)/f(x) \Longleftrightarrow f(x) = (x-a)K(x)$ for some $K(x) \in R[x]$

نعوض مكان كل $x = a$

$\Longleftrightarrow f(a) = 0 \Longrightarrow a$ 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 $f(1) = 1^3 +_3 1^2 +_3 1 = 0$

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

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

Examples

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

جذور مختلفة

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

نعوض عن 1 و 4 فتكون الناتج صفر

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 dictinct roots

مختلفة

proof نبرهن بالاستقراء الرياضي 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 $a(-ba^{-1}) + b = 0$

بشرط معامل x من الدرجة الاولى يكون inv.

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

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

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

$n = \deg f(x) = \underbrace{\deg(x-1)}_{1} + \deg g(x)$

خطأ الدكتور

$\therefore \deg g(x) = n-1$. But $g(x)$ has at most $(n-1)$ distinct roots say $a_1, \ldots, a_{n-1}$. 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 $f(x)$ — لدوال من الدرجة الثالثة فعندنا يوجد لها ثلاثة جذور

3 " " " " "

4 is root of $f(x)$

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

$$\begin{array}{r|l} & x^2 + 4 \\ \hline x-1 & \cancel{x^3} + \cancel{4x^2} + 4x + 1 \\ & \cancel{\mp x^3} \pm \cancel{x^2} \\ \hline & \cancel{4x} + \cancel{1} \\ & +\cancel{4x} \mp 4 \\ \hline & 0 \end{array}$$

$\therefore f(x) = (x-1)(x-4)(\;؟\;)$

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

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 $I=\{0\} \Longrightarrow I$ 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 $f(x) \in id(p(x))$

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

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 $\deg r(x) < \deg p(x)$

$\therefore r(x) = \underbrace{g(x)}_{\in I} - \underbrace{s(x)p(x)}_{\in I} \Longrightarrow r(x) \in I$

So, if $\deg r(x) < \deg p(x)$, we get $r(x)=0$

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

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

Corollary: $R[x]$, $Q[x]$, ~~$Z[x]$~~, $\mathbb{C}[x]$ are PID.

Corollary: let F be any field. Then any non-trivial ideal in $F[x]$ is prime $\Longleftrightarrow$ it is max.

proof F is field $\Longrightarrow F[x]$ is PID, so a non-trivial ideal in PID is prime $\Longleftrightarrow$ it is max

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

let $I = \{a_1x + a_2x^2 + \cdots a_nx^n, a_i \in \mathbb{Z}\}$

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 $f(x) = x^2+4 \in \mathbb{R}[x]$
It is irreducible لا تتحلل

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

$f(x)$ is reducible تتحلل

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 $f(x) \in F[x]$, $\deg f(x) > 1$. If

$f(x)$ has a root $\Longrightarrow$ $f(x)$ is reducible

proof: If a is a root of $f(x)$

ملحوظة: مضمونة root انه يقسم f(x) بدون باقي

$x-a \,\big)\overline{f(x)}$

$\therefore (x-a) / f(x) \Longrightarrow \exists\, g(x) \in F[x]$ s.t. $f(x) = g(x)(x-a)$

and $\deg g(x) \geq 1 \Longrightarrow f(x)$ is reducible

a. Remark

$f(x)$ has a root, then $f(x)$ is reducible

$f(x)$ is irrducible $\Longrightarrow f(x)$ has no root مكافئة لها

Example :- $f(x) = x^2+1 \in \mathbb{R}[x]$
$f(x)$ is irreducible $\Longrightarrow f(x)$ has no roots

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

ملحوظة بعض الدوال ذات الدرجة الأكثر من 3 يكون لها تحليل أولي ولكنها لا تتحلل 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 R because $\forall x \in R$, $f(x) \geq 4$

i.e $\nexists\, x \in R$ 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 $\Longleftrightarrow f(x)$ 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 $\deg h(x) = 2$

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

هذا يعني

$\therefore g(x)$ 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 $f(x)$

بنفس الطريقة

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

مهم

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

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

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

③ $F[x]/id(f(x))$ is a field.

proof ① $\Longrightarrow$ ②

F is a field $\Longrightarrow F[x]$ is a PID

Then any non trivial ideal in $F[x]$ is max $\Longleftrightarrow$ it is Prime

To prove that $I = id(f(x))$ is max.

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

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

$id(g(x)) = I$

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

$\therefore f(x) \in id(g(x)) \Longrightarrow f(x) = h(x)g(x)$ $\xrightarrow{\text{نفرض}}$ $\left(\begin{array}{l} x \in id(a) \\ x = ra \end{array}\right)$

If $h(x) = c \neq 0$ (Constant) ثابتة

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

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

Thus $h(x)$ is a poly of deg > 1

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

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

③ $\Longrightarrow$ ① 6 نفرض عكسها

$F[x]/id(f(x))$ 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. $f(x) = g(x)h(x)$

$id(f(x)) \subsetneqq id(g(x)) \subseteq F[x] \Longrightarrow id(f(x))$ 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 الى مبرهنة
Introduction to Galois theory گالواسن

في البداية سوف نستذكر تعريف الحقل

Definition :

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

Examples : $(\mathbb{C},+,\cdot)$, $(\mathbb{R},+,\cdot)$, $(Q,+,\cdot)$

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

Definition :

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

Remark :

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

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

Example :

$Q[\sqrt{2}]$ is a subfield of $\mathbb{R}$

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

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

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

Definition: let F be a subfield of (the field) K. Then K is called an extension of F.
توسيع

Definition:

let $f(x)\in F[X]$. Define
$S(F,f)=\{K : K \text{ is an extension of } F \text{ and contains all roots of } f(x)\}$.
And
$R_t(F,f)=\bigcap\{K : K\in S(F,f)\}$

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 $\overset{F}{Q}$

since $\exists\ f(x) = x^2 - 2 \in Q[X] \ni R_t(Q, f) = Q[\sqrt{2}]$

Definition : تعريف الـ poly. القابلة للحل بواسطة الجذور الذي هنا مهم

[illegible]

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 الجذر

$F = L_0 \subseteq L_1 \subseteq L_2 \subseteq \_\_\_ \subseteq L_n = K \leftarrow$ اصغر حقل جزئي يحوي 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

$\therefore \quad L_0 = R_t(F, f) = Q$

$\therefore F = L_0 = R_t(F, f) = Q$

$\therefore f(x)$ 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 كالواس

Theorem Fundamental theorem of Galois

المبرهنة الاساسية لكالواس

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) $E \subseteq E' \Longrightarrow \gamma(E') \subseteq \gamma(E)$

(3) E is normal Extension of $F \Longleftrightarrow \gamma(E)$ is normal subgp of $G(K/F)$

(4) If E, E' are normal extension of F, then $E \subseteq E'$

$\Longrightarrow \gamma(E') \backslash \gamma(E) = G(E/E')$

ملاحظة/ حفظ نص النظرية مهم

"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
$(r_1+r_2)m = r_1m + r_2m$ $\forall r_1, r_2 \in R$, $\forall m \in M$.

③ $\alpha(r_1r_2, m) = \alpha(r_1), \alpha(r_2,m)$ or $(r_1r_2)m = r_1(r_2m)$
$\forall r_1, r_2 \in R$, $\forall m \in M$.

④ if in addition $1.m = m$ $\forall m\in M$, then M is called a unital R-module.

Examples: ① Every abelain group with $+$ is a $\mathbb{Z}$-moddle

② $\mathbb{Z}_n$ is a $\mathbb{Z}$-moddle $\forall n\in \mathbb{N}$
③ $\mathbb{Q}$ is a $\mathbb{Z}$-moddle
④ Let R be a ring then every left ideal I of R is a left R-module.
⑤ $n\mathbb{Z}$ is a $\mathbb{Z}$-moddle $\forall n\in\mathbb{N}$
⑥ Every ring R can be considered as an R-module (a module over itself)

المودیولات الجزئیه

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 بسيط 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 $Z \quad \forall n=0,1,2,\dots$

(3) 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

(b) 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

الموديل الجزئي المتولد بمجموعه

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 a 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 amapping $f: M \to N$ is called an R-homomorphism if :-

(1) $f(m_1+m_2) = f(m_1) + f(m_2) \quad \forall m_1, m_2 \in M$

(2) $f(rm) = r f(m) \quad \forall r \in R, \forall m \in M.$

Example: (1) Let M and N be any R-modules. Let $f: M \to N$ 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 $f(m) = c \quad \forall m \in M$, 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 (دالة الاحتواء) $i_N : N \to N$ 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.

$M\backslash N$ 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 $M\backslash N$ is an R module $M\backslash N$ 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 $\operatorname{Im} f$, it is the set $\operatorname{Im} f = \{f(x) : x \in M\} \subseteq N$.

Remark: (مهم اشكال)

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

$$M/\ker f \simeq \operatorname{Im} f$$

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

$= r\,g(m+Ker f)$, 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 Imf

$\therefore$ 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 $x\in K \wedge y\in L$

$(x+y)+L = (x+L)+\underset{\in L}{(y+L)} = (x+L)+L = x+L$
$= f(x)$

$\therefore$ f is onto.

By Theorem (1) $\Rightarrow K/Kerf \simeq (K+L)/L$

T.P $Kerf = L\cap K$?

$Kerf = \{x\in K : f(x) = 0\}$
$= \{x\in K : x+L = L\}$
$= \{x\in K \wedge x\in L\} = K\cap L$

Therefore $K/L\cap K \simeq K+L/L$.

<u>Theorem(3)</u> :- 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) $M/K / L/K \simeq M/L$

<u>proof</u>:- ① T.P $L/K \leq M/K$?

Let $L/K = \{a+K, a\in L\}$
$M/K = \{m+K, m\in M\}$

$0+K \in L/K , 0\in L \Rightarrow L/K\neq\emptyset$

$\forall a+K\in L/K \Rightarrow a+K \in M/K$ (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: $f(m+K) = m+L$ $\forall m \in M$.

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 $Kerf = L/K$

$Kerf = \{(m+K) \in M/K : f(m+K) = L\}$

$= \{(m+K) \in M/K : m+L = L\}$

$= \{m+K \in M/K : m \in L\} = L/K$

$\therefore M/K / L/K \simeq M/L$

ملحق فصل
الموديولات

[illegible]

[illegible]:

- [illegible] Rings, [illegible] (19[illegible])
- [illegible] Commutative Ring theory (by H. [illegible] (19[illegible])
- Foundations of Module and Ring theory by R. Wisbauer (1991)
- [illegible] theory of Modules by H. [illegible]
- Injective Modules by D.W. Sharpe.

Theory of Modules

Def:- Let R be a ring with identity. An abelian group $(M,+)$ is called a left R-module (or a left module over R) if there exists a mapping

$\alpha : R \times M \longrightarrow M$ s.t.: $\alpha(r,m) = rm \ \forall r \in R$ and $m \in M$,

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 $(r_1+r_2)m = r_1m + r_2m \ \forall r_1, r_2 \in R$ & $m \in M$

③ $\alpha(r_1r_2, m) = r_1\alpha(r_2 m)$ or
$(r_1r_2)m = r_1(r_2m)$ $\forall r_1, r_2 \in R \wedge \forall m \in M.$

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 $(m, r) \to mr$ $\forall m \in M \wedge \forall r \in R$ satisfying :-

$$\left.\begin{array}{ll} (1) & m(r_1+r_2) = mr_1 + mr_2 \\ (2) & (m_1+m_2)r = m_1r + m_2r \\ (3) & m(r_1r_2) = (mr_1)r_2 \\ (4) & m.1 = m \end{array}\right\} \begin{array}{l} \forall r, r_1, r_2 \in R \wedge \\ \forall m, m_1, m_2 \in M. \end{array}$$

Remark :- If R is a comm. ring, then every left R-module can be made into a right R-module

Def :- Let R be a ring with identity and let M be a left R-module. M is called a unital (or a unitary) left R-module, if $1.m = m$ $\forall m \in M$. (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

$$na = \begin{cases} a + a + \dots + a \text{ (n-times)} & \text{if } n > 0 \\ (-a) + (-a) + \dots + (-a) \text{ (n-times)} & \text{if } n < 0 \end{cases}$$

Now, we satisfying the conditions :-

(i) $\phi(n, a_1+a_2) = n(a_1+a_2)$

$$= \begin{cases} (a_1+a_2)+\cdots\cdots(a_1+a_2) \quad (n\text{-times}) \\ \qquad\qquad \text{if } n>0 \\ (-(a_1+a_2))+\cdots+(-(a_1+a_2)) \quad (n\text{-times}) \\ \qquad\qquad \text{if } n<0 \end{cases}$$

$$= \begin{cases} \underbrace{a_1+a_1+\cdots+a_1}_{n\text{-times}}+\underbrace{a_2+a_2+\cdots+a_2}_{n\text{-times}} \\ \underbrace{(-a_1)+(-a_1)+\cdots+(-a_1)}_{n\text{-times}}+\underbrace{(-a_2)+\cdots+(-a_2)}_{n\text{-times}} \end{cases}$$

$$= na_1 + na_2$$
$$= \phi(n, a_1) + \phi(n, a_2)$$

وهكذا تحقق بقية الشرط 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 $\overset{\text{Left}}{\uparrow}$ 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 متحققه .

(i) $(r, a_1+a_2) = \overbrace{r(a_1+a_2)}^{\in I} = \overbrace{ra_1}^{\in I} + \overbrace{ra_2}^{\in I}$ 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) $(r_1 r_2)a \doteq r_1\overbrace{(\overbrace{r_2 a}^{\in I})}^{\in I}$ من شروط الحلقة تجميعية.

$= r_1\, \alpha(r_2, a).$

(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.

$3Z = id(3)$ " " " "

$\vdots \qquad \vdots$

(5) Let R be a ring and I be a left ideal in R and $R\setminus I = \{a+I, a \in R\}$. Then $(R\setminus I, \oplus)$ is abelian gp where $(a+I) \oplus (b+I) = (a+b)+I$ $\forall a,b \in R$.
Define: $\alpha : R \times R\setminus I \longrightarrow R\setminus I$ s.t
$\alpha(r, a+I) = ra+I$ $\forall r \in R$ and $\forall a+I \in R\setminus I$.
Then $R\setminus I$ 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 الاسلوب يتم برهان الشروط الاخرى.

For example:- Take $R=\mathbb{Z}$, $I=n\mathbb{Z} \Rightarrow R\backslash I = \mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}_n$ 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 $m=1$ وهي :

$M_{1\times n}(R)$ = The set of all $1\times n$ matrices (or set of all n-triples) of a ring R, namely,

$R^n = \{(a_1,\dots,a_n) : a_i \in R,\ i=1,\dots,n\}$ and

$R\times R^n \to R^n$ 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

<u>Pf</u> 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 $\beta: R\times M \longrightarrow M$ 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 خواص)
$= f(r_1)m + f(r_2)m$
$= (r_1, m) + (r_2, m)$.

(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 $\circ$ 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) $(End(M), +, \circ)$ is a ring with identity

(2) M is an $End(M)$-module?

pf: (1) T.P (End(M), +) is abelain gp ?

(i) Let $f, g \in End(M)$

$= f(m) + g(m) = f+g(m) \quad \forall f, g \in End(M)$
$\forall m \in M.$

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.

الخواص الأخرى واجب

$\therefore$ (End(M), +) is abelian gp.

(2) Define: $\phi : End(M) \times M \Rightarrow M$ s.t
$\phi(f, m) = f(m) \quad \forall f \in End(M), \forall m \in M.$

pf:- (i) Let $f \in End(M)$, $\wedge$ $m_1, m_2 \in M$

$(f, m_1+m_2) = f(m_1+m_2) = f(m_1) + f(m_2)$
$= (f, m_1) + (f, m_2)$ (since f is homo.

(ii) $(f+g)(m) = (f+g)(m), \quad \forall f, g \in End(M), \forall m \in M$
$= f(m) + g(m)$
$= (f, m) + (g, m)$

(iii) Let $f, g \in End(M)$, $m \in M$:
$(f \circ g, m) = (f \circ g)(m) = f(\underline{g(m)}) = (f, g(m))$
$= (f, (g, m))$

(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 abelain 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 :- $M_{m \times n}(R)$ is an $M_{m \times m}(R) - M_{n \times n}(R)$ - bimodule.

row = cluom اكو هنا تعبير كلي عليه مساواة

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- $r \cdot O_M = O_M \quad \forall r \in R$

2- $O_R \cdot m = O_M \quad \forall m \in M$

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)

بالجمع، $0 \cdot m + (-(0 \cdot m)) = 0 \cdot m + \cancel{0 \cdot m + (-(0 \cdot m))}$

$0 = 0 \cdot m$

(2) $r \cdot 0_M = r \cdot (0 +_M 0) = \varphi \cdot 0 + r \cdot 0$

$r \cdot 0 + (-(r \cdot 0)) = r \cdot 0 + (r \cdot 0 + (-(\varphi \cdot 0))$

(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 $R/\operatorname{ann}M$-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:

$\phi(r + I, m) = rm \quad \forall r + I \in R/I, \forall m \in M$

ϕ is an mapping?

Let $(r + I, m_1) = (b + I, m_2)$ in $R/I \times M$.

$\Rightarrow r + I = b + I \wedge m_1 = m_2$ هذا 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 الشرط الاخر واجب.

Ex:- Z_6 is a Z_3-module. since

$\operatorname{ann} Z_6 = 6Z \subseteq 3Z = I$

$\therefore Z_6$ is a $Z/3Z \cong Z_3$-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 انه :

(الشرط الاول: يعني ان $(N,+)$ زمرة جزئية من الزمرة $((M,+))$

(الشرط الثاني: يعني ان الدالة $f: R\times M \to M$ تم اقتصارها على $R\times N$

تماما $(f: R\times N \to N)$.

اي ان الموديول الجزئي من الموديول M هو نفسه موديول 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 $ra + sb \in N \quad \forall\, a,b \in N, \forall\, r,s \in R$