University of Mosul
College of Education
For Pure Sciences

محاضرات في مادة جبر الحلقات RINGS THEORY

كلية التربية للعلوم الصرفة/قسم الرياضيات

المرحلة الثالثة

Prof.Dr. Nada Yassen Kasm Yahya

Dr.Luma Ahmed Khaleel

Mrs. Shaymaa mohammed

أ . د . ندى ياسين قاسم يحيى

م . د . لمى احمد خليل

م . م . شيماء محمد يونس

المحاضرة الأولى

The Module Left R-Module

The Module

Definition :. Left R - Module

let $(R, +, \cdot)$ be a ring with identity and $(M, +)$ be an abelian group. then $(M, +)$ is called a left R - Module. If $\exists$ a mapping

$f : R \times M \longrightarrow M$ s.t

$f((r, m)) = rm \quad \forall (r, m) \in R \times M$ and

f Satisfy the following Condition :.

$\forall r, r_1, r_2 \in R$ and $\forall m, m_1, m_2 \in M$, then

1- $f((r_1 + r_2, m)) = (r_1 + r_2) \cdot m = r_1 \cdot m + r_2 \cdot m$

2- $f((r, m_1 + m_2)) = r \cdot (m_1 + m_2) = r\, m_1 + r\, m_2$

3- $f((r_1 r_2, m)) = (r_1 \cdot r_2) \cdot m = r_1 (r_2 \cdot m)$

4- if 1 is the identity element of a ring R, then

$1 \cdot m = m \quad \forall \ m \in M$

Definition: Right R - Module

M is called right R - Module if

① $(M, +)$ is an abelian group.

② $(R, +, \cdot)$ be a ring with identity.

Then, $\exists$ a mapping $f : M \times R \to M$ s.t. $f(m, r) = m \cdot r$

$\forall (m, r) \in M \times R$ and f Satisfy the following condition

1- $f((m, r_1 + r_2)) = m \cdot (r_1 + r_2) = mr_1 + mr_2$, $m \in M, r_1, r_2 \in R$

2- $f((m_1 + m_2), r) = (m_1 + m_2) r = m_1 r + m_2 r$, $m_1, m_2 \in M$

3- $f((m, r_1 r_2)) = m(r_1 r_2) = (m r_1) r_2$ $\quad r \in R$

4- if 1 is the identity element of R, then $m \cdot 1 = m$

Example:.. مثال

Show that R is Q - Module. حلية

Solution:. { الكلمة المرتبطة بـ Module هي التي تمثل الكلمة } حل

Since ① $(R,+)$ is an abelian group.

② $(Q,+,.)$ be a ring with identity.

Then ∃ a mapping $f: Q \times R \longrightarrow R$ s.t

$$f((r,m)) = r.m$$

∀ $(r,m) \in Q \times R$ and f satisfy the following condition.

∀ $r, r_1, r_2 \in Q$ and $M, M_1, M_2 \in R$.

① $f((r_1+r_2, M)) = (r_1+r_2)M = r_1M + r_2M$

② $f((r, M_1+M_2)) = r\cdot(M_1+M_2) = rM_1 + rM_2$

③ $f((r_1r_2, M)) = (r_1r_2).M = r_1(r_2M)$

④ $1 \in Q$, $1.M = M$ ∀ $M \in R$.

∴ $(R,+)$ is Q - Module.

Ex: Show that :-

$\mathbb{R}$ is R - Module.

$\mathbb{C}$ is R - Module.

الحل يكون بنفس الطريقة

Example 2 :- Show that $\mathbb{Q}$ is $\mathbb{Z}$-Module.

Solution :-

Since (1) $(\mathbb{Q}, +)$ is an abelian group.

(2) $(\mathbb{Z}, +, \cdot)$ is ring with identity,

$\therefore f : \mathbb{Z} \times \mathbb{Q} \longrightarrow \mathbb{Q}$ s.t.

$f((r, m)) = r \cdot m \quad , \forall (r, m) \in \mathbb{Z} \times \mathbb{Q}$

$= (m + m + \cdots + m)$

r-time.

$\forall r, r_1, r_2 \in \mathbb{Z}$ and $m, m_1, m_2 \in \mathbb{Q}$

(1) $f((r_1 + r_2), m) = (r_1 + r_2) \cdot m$

$= (m + \cdots + m)$

$(r_1 + r_2)$ − time.

$= (m + \cdots + m) + (m + \cdots + m)$.

r_1-times $\qquad$ r_2 −time.

$= r_1 m + r_2 m$

(2) $f((r, m_1 + m_2)) = r \cdot (m_1 + m_2)$

$= ((m_1 + m_2) + \cdots + (m_1 + m_2))$

r- times

$= (m_1 + \cdots + m_1) + (m_2 + \cdots + m_2)$

r-times $\qquad$ r times

$= r m_1 + r m_2$

③ $f((r_1r_2, m)) = (r_1r_2)m = (m + \dots + m)$ — (1)
(r_1r_2 - times)

$r_1 \cdot (r_2 m) = ((r_2 m) + \dots + (r_2 m))$
(r_1 - times)

$= ((m + \dots + m) + \dots + (m + \dots + m))$
(r_2 - time, r_2 - times)

$\leftarrow$ r_1 - times $\rightarrow$

$= (m + \dots + m)$ — (2)
(r_1r_2 - time)

$\therefore f((r_1r_2), m) = (r_1r_2)m = r_1(r_2m)$

بنفس الطريقة كل الأمثلة
show that :-
$\mathbb{R}$ is $\mathbb{Z}$-module
$\mathbb{Z}_n$ is $\mathbb{Z}$-Module
$\mathbb{C}$ is $\mathbb{Z}$-module

④ $1 \in \mathbb{Z}$, $1 \cdot m = m$, $\forall m \in \mathbb{Q}$
$\therefore (\mathbb{Q}, +)$ is $\mathbb{Z}$ - Module.

Definition: Sub module

Let M be any R-Module and $\emptyset \neq N \subseteq M$, then $(N, +)$ is called Sub module of a module $(M, +)$ over a ring $(R, +, \cdot)$ iff:-

① $a + b \in N$, $\forall a, b \in N$.
② $r \cdot a \in N$, $\forall r \in R$ and $a \in N$.

Example:-

$(\mathbb{Q}, +)$ is sub module of $\mathbb{R}$ as $\mathbb{Z}$-module since $\emptyset \neq \mathbb{Q} \subseteq \mathbb{R}$ and.

① $a + b \in \mathbb{Q}$, $\forall a, b \in \mathbb{Q}$
② $r \cdot a \in \mathbb{Q}$, $\forall r \in \mathbb{Z}$ and $\forall a \in \mathbb{Q}$

Definition :-

let M be any R- module, then the trivial submdule of a module M which are $(M,+)$, $(\{0\},+)$.

Example :-

Find all submodules of the module $(Z_6, +)$ over a ring of $(Z,+,\cdot)$

Solution :-

the submodul of Z_6 over a ring Z are

$(Z_6,+),(\{0\},+),(\{0,2,4\},+)$, $(\{0,3\},+)$.

Example :-

Find all sub module of $(Z_{14},+)$ over aring of $(Z,+$

Solution :

The submodul of Z_{14} over aring Z are.

$(Z_{14},+)$, $(\{0\},+)$, $(\{0,2,4,6,8,10,12\},+)$.

$(\{0,7\},+)$.

Definition : Cyclic_Module

let $(M,+)$ be any R-module, then M is called cyclic module if $\exists\ x \in M$ s.t

$$(x) = R.x = \{r.x : \forall r \in R\} = M$$

x is called generators of Module M.

Examples:-

① let $(Z,+)$ be a Z-modul, then Z is a cyclic module since $\exists\ 1 \in Z$ s.t $(1) = Z.1 = Z$.

$\therefore$ 1 is generators of module Z.

② let $(Ze,+)$ be a Z-module, then Ze is cyclic module since $\exists\ 2 \in Ze$ s.t $(2) = Z.2 = \{2.r : \forall r \in Z\}$

$= Ze$

$\therefore$ 2 is generators of module Ze.

③ let Z_6 be Z-module. Find the generators of Z_6

$$(X) = R.X = \{r.x , \forall r \in R\}.$$

$(1) = \{1.r : r \in Z_6\} = \{0,1,2,3,4,5,0,..\} = Z_6.$

$(2) = \{2.r : r \in Z_6\} = \{0,2,4\} \neq Z_6$

$(3) = \{3.r : r \in Z_6\} = \{0,3\} \neq Z_6$

$(4) = \{4.r : r \in Z_6\} = \{0,4,2\} \neq Z_6$

$(5) = \{5.r : r \in Z_6\} = \{0,5,4,3,2,1\} = Z_6$

$\therefore$ 1,5 are generators of module Z_6.

المحاضرة الثانية

Remainder Theorem

Remainder Theorem

Let $(R,+,\cdot)$ be a commutative ring with identity, If $f(x) \in R[x]$ and $a \in R$. Then there exist unqiue polynomial $q(x) \in R[x]$, such that

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

Examples:

1- Let $f(x) = x^3 + 4x^2 + 2x + 2 \in Z[x]$, and $a = -1 \in Z$
Find $q(x)$.

Sol:-

By using Remainder Theorem.

$g(x) = x - a$
$= x - (-1) = x + 1$

$\therefore q(x) = x^2 + 3x - 1$

$r(x) = 3$

$f(a) = f(-1)$
$= (-1)^3 + 4(-1)^2 + 2(-1) + 2$
$= 3$

$$\begin{array}{r|l} & x^2 + 3x - 1 \quad q(x) \\ x+1 & x^3 + 4x^2 + 2x + 2 \\ \text{بالطرح} & -x^3 \mp 2x \\ \hline & 3x^2 + 2x \\ \text{بالطرح} & \mp 3x^2 \mp 3x \\ \hline & -x + 2 \\ \text{بالطرح} & \mp x \mp 1 \\ \hline & 3 \quad r(x) = f(a) \end{array}$$

∴ للتأكد من صحة الحل يجب ان يكون باقي القسمة هو صورة العنصر $f(a)$.

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

find $q(x)$.

Sol:-

By using Reminder theorem

$g(x) = x - a$

$= x - 4$

$\therefore q(x) = 2x^3 + 2x^2 + x + 4$

$r(x) = 5$

$f(a) = f(x) = 2x^4 + 5x^2 + 1$

$= f(4) = 2_6(4)^4 + 5_6(4)^2 + 1$

$= 2 \cdot 4 + 5 \cdot 4 + 1$

$= 2 + 2 + 1 = 5$

$$x - 4 \;\big|\; 2x^4 + 5x^2 + 1 \quad (2x^3 + 2x^2 + x + 4)$$

$-2x^4 \pm 2x^3 \pmod 6$

$2x^3 + 5x^2 + 1$

$-2x^3 \pm 2x^2 \pmod 6$

$x^2 + 1$

$-x^2 \pm 4x \pmod 6$

$5 \quad r(x) = f(a) = f(4)$

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

$f(x) = (x - 4)(2x^3 + 2x^2 + x + 4) + 5$

3- Let $f(x) = x^2 - 5x + 8$, $a = 2 \in Z$

Find $q(x)$.

Sol:-

By using Remainder Theorem

$g(x) = x - a$

$= x - 2$

$\therefore q(x) = x - 3$

$r(x) = 2$

$\therefore f(a) = f(x) = x^2 - 5x + 8$

$= f(2) = (2)^2 - 5(2) + 8$

$= 2$

$$\begin{array}{r|l} & x - 3 \\ \hline x - 2 & x^2 - 5x + 8 \\ & -x^2 \pm 2x \\ \hline & -3x + 8 \\ & \pm 3x \mp 6 \\ \hline & 2 \end{array}$$

$\therefore r(x) = f(a) = f(2)$

4- let $f(x) = x^3 - 5x^2 + 3x + 8 \in Z[x]$, $a = 1 \in Z$

Find $q(x)$

Sol:-

By using Remainder Th.

$g(x) = x - a = x - 1$

$\therefore q(x) = x^2 - 4x - 1$

$r(x) = 7$

$$\begin{array}{r|l} & x^2 - 4x - 1 \\ \hline x - 1 & x^3 - 5x^2 + 3x + 8 \\ & -x^3 \pm x^2 \\ \hline & -4x^2 + 3x \\ & +4x^2 \mp 4x \\ \hline & -x + 8 \\ & +x \mp 1 \\ \hline & 7 \end{array}$$

$7 = r(x)$

المحاضرة الثالثة

Division Algorithm and some theorems of polynomial rings

Division Algorithm

Theorem :-

let $f(x)$ be any polynomial and $g(x)$ be a non Zero polynomial in the polynomial domain $(F[x], +, \cdot)$ over a field F. Then there exists two unique polynomials $q(x)$ and $r(x)$ in $F[x]$, such that

$f(x) = q(x) \cdot g(x) + r(x)$, where $r(x) = 0$ or

$\deg(r(x)) \leq \deg(g(x))$.

Example :-

let $f(x) = x^4 - 3x^3 + 2x^2 + 4x - 1$ and
$g(x) = x^2 - 2x + 3$ be two polynomials in a ring $(\mathbb{Q}[x], +, \cdot)$. Find $q(x)$ and $r(x)$.

Sol :-

$$
\begin{array}{r|l}
x^2 - 2x + 3 & x^4 - 3x^3 + 2x^2 + 4x - 1 \\
 & \mp x^4 \pm 2x^3 \mp 3x^2 \\
\hline
 & -x^3 - x^2 + 4x - 1 \\
 & \pm x^3 \mp 2x^2 \pm 3x \\
\hline
 & -3x^2 + 7x - 1 \\
 & \mp 3x^2 \mp 6x \pm 9 \\
\hline
 & x + 8
\end{array}
\qquad
\begin{array}{l}
q(x) \\
\hline
x^2 - x - 3 \\
\text{الخارج} \\
\text{الخارج} \\
\text{الخارج} \\
r(x)
\end{array}
$$

$q(x) = x^2 - x - 3$

$r(x) = x + 8$

$f(x) = q(x) \cdot g(x) + r(x)$

$= (x^2 - x - 3) \cdot (x^2 - 2x + 3) + (x + 8)$.

Example:-

let $f(x) = x^4 + x^3 + x + 2$, $g(x) = x^2 + 2x + 1$

such that $f(x), g(x) \in Z_5$. find $q(x)$, $r(x)$

Sol:-

$f(x) = g(x) \cdot q(x) + r(x)$.

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

$\therefore f(x) = g(x) \cdot q(x) + r(x)$

$2 + x + x^3 + x^4 = ((1 + 2x + x^2) \cdot (1 - x + x^2)) + 1$

or

$x^4 + x^3 + x + 2 = [(x^2 + 2x + 1) \cdot (x^2 - x + 1)] + 1$

Polynomial Rings:

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.

Example:

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

Sol.

0 is not root of $f(x)$, since $f(0) = 1 \neq 0$
1 is root of $f(x)$, since $f(1) = 10 = 0$
2 is not root of $f(x)$.
3 " " " "
4 is root of $f(x)$.

$\therefore$ 1, 4 are two root of $f(x)$

Theorem:

Let $(R, +, \cdot)$ be an integral domain. Then $(R[x], +, \cdot)$ is an integral domain. is called polynomial domain

Theorem: (*)

If R is an integral domain and $f(x), g(x) \in R[x]$ with $f(x) \neq 0, g(x) \neq 0$, then

$$\deg(f(x) \cdot g(x)) = \deg f(x) + \deg g(x).$$

Remark:

If R is not an integral domain. then Theorem (*) is not true ingeneral.

Example:

If $f(x) = 2x^2$ and $g(x) = 2x^2 + 1 \in Z_4[x]$

then $f(x) \cdot g(x) = 2x^2$

$\therefore \deg(f(x) \cdot g(x)) = 2 \neq 4 = \deg(f(x)) + \deg(g(x))$

Theorem:

If $(R, +, \cdot)$ is an integral domain, then the ring $(R[x], +, \cdot)$ is not field.

Corollary

A non zero polynomial $f(x) \in R[x]$ has more roots then the degree of $f(x)$, if R is not field.

Example:-

Let $f(x) = 3x$ be poly. in the $Z_6[x]$

Sol:-

$Z_6 = \{0, 1, 2, 3, 4, 5\}$.

$f(0) = 3 \cdot 0 = 0 \Rightarrow 0$ is the roots of $f(x)$ in $Z_6[x]$.
$f(1) = 3 \cdot 1 = 3 \Rightarrow 3$ is not " " " " " "
$f(2) = 3 \cdot 2 = 0 \Rightarrow 2$ is the " " " " " "
$f(3) = 3 \cdot 3 = 3 \Rightarrow 3$: not : " " " " "
$f(4) = 3 \cdot 4 = 0 \Rightarrow 4$ = the " " " " " "
$f(5) = 3 \cdot 5 = 3 \Rightarrow 5$: not " " " " " "

Then, the roots of $f(x)$ which are $0, 2, 4$.

the number of roots of $f(x)$ is 3 and

the $\deg(f(x)) = 1$

$\therefore$ the number of roots of $f(x) = 3 > \deg(f(x)) = 1$

Corollary :-

A none Zero polynomial $f(x) \in R[X]$ of degree n can have at most n roots, if R is a field.

Example :-

let $f(x) = X^3 + X^2 + 1$ be a polynomial in the poly. domain $Z_3[X]$ over a field Z_3.

Sol :-

$Z_3 = \{0, 1, 2\}$, now we find the roots of $f(x)$.

$f(0) = 0^3 + 0^2 + 1 = 1 \neq 0 \Rightarrow 0$ is not root of $f(x)$

$f(1) = 1^3 + 1^2 + 1 = 0 \Rightarrow 1$ is root of $f(x)$ in $Z_3[X]$

$f(2) = 2^3 + 2^2 + 1 = 1 \neq 0 \Rightarrow 2$ is not root of $f(x)$ in $Z_3[X]$

$\therefore$ The roots of $f(x)$ is 1

And, the $\deg(f(x)) = 3$

$\therefore$ The number of roots of $f(x) = 1 < \deg(f(x)) = 3$.

المحاضرة الرابعة

Boolean Ring

Boolean Ring

حلقة بولين

Definition:-

A Boolean ring $(R,+,.)$ is a ring with identity and every element in a ring R is an idempotent element. That is $a^2=a$, $\forall\ a\in R$.

Examples:-

1- A ring $(Z_2,+,.)$ is a Boolean ring.

$\because (Z_2,+,.)$ is a ring with identity and for all $a\in$ Ring $Z_2=\{0,1\}$ is an idempotent element.

i.e $0^2=0$, $1^2=1$

2- A ring $(P(X),\Delta,\cap)$, where $P(X)=\{A: A\subseteq X\}$ is a Boolean ring.

$\because (P(X),\Delta,\cap)$ is a ring with identity, $\forall A\in P(X)$

$\therefore A^2=A\cap A=A$.

3- A ring $(Z_3,+,.)$ is not Boolean ring.

$\because \exists\ 2\in Z_3$, $2^2=2.2\neq 2$

4- A ring $(Z_6,+,.)$ is not Boolean ring

since $0^2=0$ ←

$1^2=1$ ←

$2^2=4\neq 2$ not Bool. ring.

Lemma(*) :-

Let R be a Boolean Ring. Then $\forall x \in R, -x = x$

Proof:-

From the definition of a Boolean Ring

$$x^2 = x \quad , \quad -x \in R$$

① — Thus $(-x)^2 = -x$ (since Boolean ring)

② — But $(-x)^2 = x^2 = x$ (Σ = =)

By (1), (2), we have

$$-x = x$$

Theorem:-

Every Boolean ring $(R, +, \cdot)$ is a commutative ring with the characteristic 2.

Proof:-

i- T.P Boolean ring R is a Comm. ring.

Let $a, b \in R$, and R is a ring $\Rightarrow a+b \in R$.

$a+b = (a+b)^2$ (since R is a Boolean ring)

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

$a+b = a^2 + a\cdot b + b\cdot a + b^2$

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

$0 = a\cdot b + b\cdot a$

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

$\because b \in R$, R is a ring $\Rightarrow -b \in R$

$\therefore$ R is Boolean ring

then $-b = (-b)^2 = b^2 = b$ (by lemma *)

$\Rightarrow a\cdot b = -b\,a = b\cdot a$.

Therefore R is a Commutative ring.

ii- T.P $ch(R) = 2$, that is $2a = 0 \; \forall \; a \in R$.

let $a \in R$, and since R is a ring

$\Rightarrow a + a \in R$.

$a + a = (a+a)^2 = a^2 + 2a^2 + a^2$

$a + a = a + 2a + a$ (R is Boolean ring)

$0 = 2a$.

$\therefore 2a = 0, \; \forall \; a \in R$, Thus $ch(R) = 2$.

Theorem:-

A Boolean ring R is a field iff $R \simeq Z_2 = \{0,1\}$

Proof:-

↳ let R is a field.

T.P $R = \{0,1\}$

Let $a \in R$ such that $a \neq 0$.

Now since R is Boolean ring

$\therefore a^2 = a \Rightarrow a \cdot a = a$

since $a^{-1} \in R$ (Field).

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

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

$\therefore a = 1 \Rightarrow R$ has only two element are 0, 1

$\therefore R = \{0,1\} \Rightarrow R \simeq Z_2$

↵ Suppose $R \simeq Z_2 = \{0,1\}$.

T.P R is a field. ① comm. ② identity 1 ③ $0 \neq a \in R$ s.t $a^{-1} \in R$

since R is Boolean ring., then By Def Boolean ring and by Theorem (Boolean ring is a comm.)

$\Rightarrow$ R is Commatative ring with identity

Since $R = \{0,1\}$, then $1 \cdot 1 = 1 \Rightarrow (1)^{-1} = 1$

$\therefore$ R has inverse under multiplication.

Therefor Boolean ring R is a field.

Theorem:-

In a Boolean Ring every prime ideal is Maximal ideal.

Proof:-

If P is prime ideal of R,

T.P. P is Max. ideal of R.

let J be an ideal in R such that

$P \subset J \subseteq R$.

since $P \subset J$, then $\exists\ a \in J$, $a \notin P$.

$a \in R$, since R is Boolean ring.

$\therefore a^2 = a \Rightarrow a^2 - a = 0$

$\Rightarrow a(a-1) = 0 \in P$.

$\therefore$ either $a \in P$ or $a-1 \in P \subset J$

$\therefore a-1 \in J$ and $a \in J$

$\therefore a-(a-1) = a-a+1 = 1 \in J = R$ C!

Therefor P is Maximal ideal of R.

Theorem:-

If $(R, +, \cdot)$ is a Boolean ring, then any ideal of R is idempotent.

Proof:-

Let R is Boolean ring than $x^2 = x \; \forall \; x \in R$

let I be an ideal of R

T.P $I^2 = I$

$$I^2 = \{ x_1 \cdot y_1 + x_2 \cdot y_2 + \cdots + x_n y_n : x_i, y_i \in I \; n \geq 1 \}.$$

It is clear that $I^2 \subseteq I$

we prove that $I \subseteq I^2$

let $x \in I$ —①

$x^2 \in I^2$.

Sin $x^2 = x$, $\forall \; x \in R$ then

$x \in I$ —② ②

∴ By ① and ② we have $I \subseteq I^2$

Therefor $I^2 = I$.

المحاضرة الخامسة

Polynomial of Rings

Polynomial Ring

Definition :-

let $(R, +, \cdot)$ be any ring a function

$f(x) = \sum_{i=0}^{\infty} a_i x^i = a_0x^0 + a_1x^1 + a_2x^2 + \dots + a_nx^n + \dots$, where

$a_0, a_1, a_2, \dots, a_n \in R$ and the powers $0, 1, 2, \dots, n, \dots$ are non negative integers, then $f(x)$ is called a Polynomial over a ring R.

Example :-

1- $f(x) = 3 + 7x^1 - 20x^4$ is a polynomial over a ring $\mathbb{Z}$

2- $f(x) = \frac{1}{2} + 17x^2 - 28x^5$ is a polynomial over a ring $\mathbb{Q}$ but is not over a ring $\mathbb{Z}$, since $\frac{1}{2} \notin \mathbb{Z}$

Definition : Polynomial of Degree n

Let $f(x)$ be a polynomial over a ring R, then if $\exists$ a non negative integer n such that, $a_n \neq 0$ and $a_i = 0, \forall i > n$

i.e If $f(x) = a_0x^0 + a_1x^1 + a_2x^2 + \dots + a_nx^n$, then $f(x)$ is called a polynomial of degree and is denoted by $\deg f(x) = n$].

Example:-

1- $f(x) = 4 + 17x' - 2x^3$ is Poly. over a ring $\mathbb{Z}$ of degree 3.

2- $g(x) = \frac{1}{3} + 7x^2 - 8x^7$ is Poly. over a ring $\mathbb{Q}$ of degree 7

3- $h(x) = \sqrt{3}\,x$ is a Poly. over a ring R of degree 1.

Definition: Leading Term and Leading Coefficient

Let $f(x) = a_0x^0 + a_1x' + a_2x^2 + \dots + a_nx^n$ be Polynomial of degree n over a ring R. Then the term a_nx^n is Called leading term and a_n is called Leading Coefficient.

Example:-

Find the leading term and the leading Coefficeient of the following Poly.

1- $f(x) = 4 + x - 2x^3 + 4x^6$

The leading term of $f(x)$ is $4x^6$. and leading cofficeient is 4

2- $f(x) = \frac{5}{4} + 8x^3 - 8x^5 - \sqrt{5}\,x^8$

The leading term of $f(x)$ is $-\sqrt{5}\,x^8$ and leading Coeffcient is $-\sqrt{5}$

Definition: The sum of Polynomails

let $f(x) = a_0x^0 + a_1x^1 + a_2x^2 + \cdots + a_mx^m$, $a_m \neq 0$ and

$g(x) = b_0x^0 + b_1x^1 + b_2x^2 + \cdots + b_nx^n$, $b_n \neq 0$

be two polynomials of degree m and n respectively over a ring R. Then The sum of $f(x)$ and $g(x)$ is also polynomial over R and is defined by

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

$$= (a_0+b_0)x^0 + (a_1+b_1)x^1 + \cdots + (a_m+b_n)x^{\max(m,n)}$$

where, $\deg(f(x)+g(x)) = \begin{cases} \max(m,n) & \text{if } m \neq n \\ m & \text{if } m = n \text{ and } a_m+b_n \neq 0 \\ < m & \text{if } m = n \text{ and } a_m+b_n = 0 \end{cases}$

Examples:-

2) مثال

1- Let $f(x) = 3 + x + 4x^2$ and $g(x) = 4 + 5x + 7x^2$ be two poly. over a ring Z_9. Find $f(x) + g(x)$.

Sol:-

$$f(x)+g(x) = \begin{array}{r} 3 + x + 4x^2 \\ 4 + 5x + 7x^2 \\ \hline 7 + 6x + 2x^2 \end{array} \quad +9$$

3) مثال

2- Let $f(x) = 1 + 8x - 3x^2$ and $g(x) = 2 + x + 3x^2$ be two poly. over a ring $\mathbb{Q}$. Find $f(x) + g(x)$.

$$f(x)+g(x) = 1 + 8x - 3x^2 + 2 + x + 3x^2$$

$$= 3 + 9x$$

4) مثال

3- let $f(x) = 2 + 3x + 5x^2$ and $g(x) = 3 - 5x + 4x^2 - 9x^3$ be two poly. over a ring Z. find $f(x) + g(x)$.

طريقة القانون

$$\deg.(f(x)+g(x)) = \text{Max}(\deg.f(x), \deg.g(x))$$

$$= \text{Max}(2, 3) = 3$$

$$f(x)+g(x) = (a_0+b_0)x^0 + (a_1+b_1)x^1 + (a_2+b_2)x^2 + (a_3+b_3)x^3$$

$$= 5x^0 - 2x + 9x^2 - 9x^3$$

Definition :-

The Polynomial

$R[X] = f(X) = a_0x^0 + a_1x^1 + a_2x^2 + \cdots + a_nx^n$

is called Zero polynomial, where $a_0, a_1, a_2 \cdots, a_n = 0$

Theorem :-

let $(R, +, \cdot)$ be ring. Then $(R[X], +, \cdot)$ is a ring and called polynomial ring

Theorem :-

1- If $(R, +, \cdot)$ be commutative ring. Then $(R[X], +, \cdot)$ is commutative ring.

2- If $(R, +, \cdot)$ be a ring with identity. Then $(R[X], +, \cdot)$ is a ring with identity.

3- let $(R, +, \cdot)$ be an integral domain. Then $(R[X], +, \cdot)$ is integral domain.

Root of Polynomial

جذر متعدد الحدود

Definition:

Let $(R,+,\cdot)$ be a comm. ring with identity and $f(x)$ be a non-zero polynomial of a ring $(R[x],+,\cdot)$, let $a \in R$. Then, a is called root of poly. $f(x)$ iff $f(a)=0$

Examples:

Determine whether the following poly. has roots.

1. $f(x)=x^2-4 \in Z[x]$

$x^2-4=0 \Rightarrow x^2=4 \Rightarrow x=\mp 2 \in Z[x]$

$\therefore x=\mp 2$ are roots of the poly $f(x)=x^2-4 \in Z[x]$

2. $f(x)=x^2+4 \in Z[x]$

$x^2+4=0 \Rightarrow x^2=-4 \Rightarrow x=\mp\sqrt{-4}=\mp 2i \notin Z[x]$

$\therefore f(x)=x^2+4$ has no roots in $Z[x]$

3. $f(x)=x^2+4 \in \mathbb{C}[x]$

$x^2+4=0 \Rightarrow x^2=-4 \Rightarrow x=\mp 2i \in \mathbb{C}[x]$

$\therefore x=\mp 2i$ are roots of the poly. $f(x)=x^2+4 \in \mathbb{C}[x]$

3. $f(x) = x^2 + 4 \in Z_5[x]$

$\because Z_5 = \{0, 1, 2, 3, 4\}$

$\Rightarrow f(0) = (0)^2 + 4 = 4 \neq 0$

$f(1) = (1)^2 + 4 = 0$

$f(2) = (2)^2 + 4 = 3 \neq 0$

$f(3) = (3)^2 + 4 = 3 \neq 0$

$f(4) = (4)^2 + 4 = 0$

$\therefore$ The root of poly. $f(x) = x^2 + 4$ are 1, 4

4- $f(x) = x^2 - 1 \in Z_8[x]$?

5 - $f(x) = x^2 + 3x + 2 \in Z_6[x]$?