Example: Consider the ring $(Z_{12}, +_{12}, \cdot_{12})$.

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

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

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

$M_1 = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}, \bar{10}\}$ is max. ideal
لان 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. $M_3 \subsetneqq M_1 \subsetneqq Z_{12}$

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

s.t. $M_4 \subsetneqq M_1 \subsetneqq Z_{12}$ and $M_4 \subsetneqq M_2 \subsetneqq Z_{12}$.

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 $\Longleftrightarrow$ 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 $n = mk$

$\therefore\ id(n) \subsetneqq id(m) \subsetneqq \mathbb{Z}$ and $id(n) \subsetneqq id(k) \subsetneqq \mathbb{Z}$

which is Contradiction with definition of max ideal
هذا تناقض مع تعريف المثالي الاعظم

$\Leftarrow$) 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.
$I \subsetneqq J \subsetneqq \mathbb{Z}$. But $\mathbb{Z}$ is P.I.R. Then $\exists\, m \in \mathbb{Z}_+$, $m \neq 1$
s.t. $J = id(m) \Rightarrow id(n) \subsetneqq id(m) \subsetneqq \mathbb{Z}$
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
(مع نفسه)

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 :-

حلقة موضعية

let $(R,+,\cdot)$ be a comm. ring, R is called local ring $\Leftrightarrow$ R has uniqe max. ideal

Example : ① $(Z_4,+_4,\cdot_4)$ is local ring, since Z_4 has only one max. ideal which is $\{\bar{0},\bar{2}\}$.

② Z_8, 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 $\Leftrightarrow$ $(M,a)=R$ $\forall a\in R$, $a\notin M$.

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 $(M,a)=R$ (لأن M أعظمي)

$\Leftarrow$) 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 $(M, a) = R$

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

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

البرهان يعتمد على مبرهنة زورن (Zorn's lemma) والتي تنص:

لتكن X مجموعة غير خالية ولتكن F مجموعة غير خالية من مجموعات جزئية من X. اذا كان لكل سلسلة $\{C_i\}$ من عناصر F فان $\cup C_i \in F$ فان F تمتلك عنصراً اعظماً.

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 (سلسلة) of F

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. $M \subsetneq K$

$\therefore K \notin F$ لان خلاف ذلك سوف نحصل على تناقض مع كون M عنصراً اعظماً

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

نتيجة كنتائج لمبرهنة المقترحة

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.

حفظ له نظر جزئي

Proof :- $\Rightarrow$) suppose that a is an invertible.

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

But $(a)=R \Rightarrow$ a is not belong to any max. ideal.

$\Leftarrow$) suppose that M is max. ideal and $a \notin M$.

see the id (a). If $R=(a)$, then a is an invertible elem
تأمل او لاحظ

either, if $R \neq (a)$, then by above theorem, $\exists$ max. ideal
اما اذا بواسطة النظرية اعلاه

M and $(a) \subseteq M \Rightarrow a \in M$ C! ($a \notin M$ بالفرض)

∴ 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

∴ $\exists$ max. ideal J of R s.t $I \subsetneq J \subsetneq R$ (by above theorem
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 المتحايدة

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

عنصر متحايد

Proof: suppose that a is an idempotent element in R and $a \neq 0$, $a \neq 1$

$\therefore a^2 = a \Longrightarrow a^2 - a = 0 \Longrightarrow a(a-1) = 0$

But $a \neq 0$ and $a - 1 \neq 0$ بالفرض

هذا يعني

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

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

$\therefore M = R$ C! (R [illegible] M لان)

مهم جداً

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

Proof: $\Longrightarrow$)

هنا شكل العنصر في R/I

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

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

$\therefore 1 = x + ra$ 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. $c \in I$

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

Remark :-

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

The ring $(Z_e, +, \cdot)$ has no unity.

let $M = \{0, \mp 4, \mp 8, \ldots\}$ is max. ideal of Z_e. But $Z_e / M = \{0 + m, 2 + m\}$ is not field.

Definition : let R be a comm. ring, I be an ideal of R. I is called prime ideal iff $\forall a,b \in R$, $a.b \in R \Rightarrow$ either $a \in I$ or $b \in I$ يتحقق اولي

Example : In the ring $(Z,+,.)$

let $id(2) = \{0, \mp 2, \mp 4, \mp 6, \ldots\}$

let $a,b \in Z$ s.t $a.b \in id(2)$

$\therefore ab = 2.c$ for some $c \in Z$

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

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

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

تعميم : In the ring $(Z,+,.)$. 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 $a,b \in R$ s.t $ab \in \{0\} \Rightarrow ab = 0$

So, $a=0$ or $b=0$ (since R has no zero divisor)

$\Longrightarrow a \in \{0\}$ or $b \in \{0\}$. Thus $\{0\}$ is prime ideal.

$\Longleftarrow$) let $a,b \in R$, $ab=0$

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

$\therefore a \in \{0\}$ or $b \in \{0\} \Longrightarrow a=0$ or $b=0$

$\therefore$ R has no zero divisor $\Longrightarrow$ R is an integral domain.

Problem: (H.W)

غير كافية

In $(Z, +, \cdot)$: A non trivial ideal I of Z, I = $\langle n \rangle$

is prime ideal $\Longleftrightarrow$ n is prime number.

Example: $(Z_6, +_6, \cdot_6)$

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 $a,b \in Z_6$

$2,3 \in Z_6$

$2 \cdot 3 = 0 \in Z_6$

$2 \notin Z_6 \wedge 3 \notin Z_6$

Example:

In the ring $(Z_5, +_5, \cdot_5)$

since Z_5 is field $\Longrightarrow Z_5$ is an integral domain

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

في الحلقة المثالي الأولي الوحيد هو $\{\bar{0}\}$

Theorem: let R be a comm. ring with unity 1. Then every maximal ideal of R is prime ideal.

<u>Proof</u>: 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 $(Z, +, \cdot)$ is prime ideal. But $\{0\}$ is not max. ideal

<u>Problem</u>: (H.W)

let R = d.s. of $(Z, +, \cdot)$ with $(Z, +, \cdot)$
and let $I = \{(a, 0) : a \in Z\}$. Show that I is a prime ideal, but I is not maximal ideal.

<u>Remark</u>:

The theorem is not true in rings without unity

<u>Example</u>: $I = \{0, \mp 4, \mp 8, \mp 12, \ldots\}$ is max in Z_e

But I is not prime ideal (since $4 = 2.2 \in I$, but $2 \notin I$)

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

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
ماهو مثاليات رئيسية
I of R is maximal ideal $\Longleftrightarrow$ It is prime ideal.

Proof :- $\Leftarrow$)

let I be a prime ideal of R and $I \neq \{0\}$.

let J be an ideal of R s.t. $I \subsetneq J$.

$\because R$ is P.I.D., that means $\exists\ a, b \in R$ s.t.
هذا يعني

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

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

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

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

If $b \in I \Longrightarrow (b) \subseteq I = (a) \Longrightarrow I = J$ C!

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

② $t = sa$, $s \in R$

From ① and ②, we get $a = sba$
يحصل

$\because R$ is an integral domain, $a \neq 0$

$\therefore sb = 1 \Longrightarrow 1 \in J \Longrightarrow R = J$

$\therefore I$ 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-trivail ideal I is maximal ideal $\Leftrightarrow$ 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)

حسب الفرض

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

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

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

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

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

$\therefore I$ is maximal ideal.

Definition : nil radical : الجذر المعدوم

let $(R,+,\cdot)$ be a ring and I be an ideal of R, the set $\{x \in R : x^n \in I \text{ for some } n \in Z_+\}$ is Called nil radical and dented by $\sqrt{I}$.

Example : ① (12) is an ideal in Z

$$\sqrt{(12)} = \sqrt{2^2 \cdot 3} = (6)$$

② (4) is an ideal in Z

$$\sqrt{(4)} = (2)$$

Remarks :

① $I \subseteq \sqrt{I}$

② let $n \in Z_+$ and (n) is an ideal s.t. $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}$

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

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

وهنا نكافئ التعريف

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

That is, $x \in \sqrt{I} \Rightarrow x^n \in I$ for some $n \in Z_+$

Proposition :-

$\sqrt{I}$ is an ideal of R.

Proof :-

let $x, y \in \sqrt{I}$. Then $\exists\, n, m \in Z_+$ s.t. $x^n \in I$ and $y^m \in I$

Class

Definition : nil radical : الجذر المعدوم

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. $n = P_1^{\alpha_1} \cdot P_2^{\alpha_2} \cdots P_k^{\alpha_k}$

Then $\sqrt{(n)} = \sqrt{(P_1^{\alpha_1} \cdot P_2^{\alpha_2} \cdots P_k^{\alpha_k})} = (P_1 P_2 \cdots P_k)$

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

وهنا تكافئ التعريف

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

That is, $x \in \sqrt{I} \Longrightarrow x^n \in I$ 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 $y^m \in I$

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

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

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

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

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

شبه اولي

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 $\Leftrightarrow$ $R\backslash I$ has not Contain nilpotent elements only Zero element.

Proof :- $\Rightarrow$) let $a+I$ be nilpotent element in

$R\backslash I \Rightarrow (a+I)^n = I$, $n \in \mathbb{Z}_+$

$\therefore a^n + I = I \Rightarrow a^n \in I \Rightarrow a \in \sqrt{I} = I$ (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 $n \in \mathbb{Z}_+$

$\Leftrightarrow x^n + I = I$

$\therefore (x+I)^n = x^n + I = I$

$\therefore x+I$ 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

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

Example:

$4\mathbb{Z}$ is primary ideal in $\mathbb{Z}$ $(2.2 = 4 \in 4\mathbb{Z} \Rightarrow 2^2 \in 4\mathbb{Z}$ but $2 \notin 4\mathbb{Z}$

$a.b \in I \Rightarrow a^n \in I$ or $b^n \in I \Rightarrow I$ is primary

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.

عناصر عديمة القوة

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 بولين

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

$\Leftarrow$) It is clear

[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

Chapter Seven 7

حلقة الحدوديات

"Polynomail Ring"

Def: Let R be any ring

Let $S = \{ f(x) : f(x) = a_0 + a_1 x_1 + \dots + a_n x^n , a_0, a_1, \dots, a_n \in R$

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

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

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

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

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

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

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

$c_0 = a_0 b_0$

$c_1 = a_0 b_1 + a_1 b_0$

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

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

$\vdots$

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

or $\boxed{c_s = \sum_{i+j=s} a_i b_j \quad i, j \geq 0}$ الصيغة العامة

~~Notice that +, · are closed on S.~~

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

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

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

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

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

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

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

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

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

وهكذا
Since, $C_5 = C_6 = 0 \ldots$

$\therefore f(x) \cdot g(x) = 3 + 2x + 2x^2 + x^3$ 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 $f(x) = \sum_{i=1}^{n} a_i x^i$, $g(x) = \sum_{i=1}^{m} b_i x^i$

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

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

$\therefore$ + 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 $f(x) + [(-f)(x)] = 0 = h(x)$

عنصر محايد

$\therefore -f(x)$ 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 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 $f(x)$.

Theorem "مهم جداً" أعرفه

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 $f(x)=a_0+a_1x+a_2x^2+\dots+a_nx^n$ is non Zero poly.

$a_n \neq 0$, i.e $\deg f(x) = n$ لأنها ليست صفرية

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

$b_m \neq 0$, i.e $\deg g(x) = m$ لأنها 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 $C_0 = a_0 b_0$, $C_1 = a_0 b_1 + a_1 b_0$

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

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

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

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.