

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

$\mathbb{Z}_{12}$ is not max. ideal

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

$$\{0\} \subsetneq \{\bar{0}, \bar{6}\} \subsetneq \mathbb{Z}_{12}$$

$M_1 = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}, \bar{10}\}$ is max. ideal

M_1 لا يوجد مثالي في $\mathbb{Z}_{12}$ يحتويه

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

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

Since $\exists M_1$ s.t. $M_3 \subsetneq M_1 \subsetneq \mathbb{Z}_{12}$

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

s.t. $M_4 \subsetneq M_1 \subsetneq \mathbb{Z}_{12}$ and $M_4 \subsetneq M_2 \subsetneq \mathbb{Z}_{12}$.

problems:

① Find all maximal ideals of $(\mathbb{Z}_8, +_8, \cdot_8)$.

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

Theorem 8: In the ring $\mathbb{Z}$, the $\text{id}(n)$, $(n \in \mathbb{Z}, n \neq 1)$ is maximal ideal $\iff n$ is prime number.

proof: $\implies$ let $I = \text{id}(n)$ is max. ideal.

(36)

To prove, n is prime number.

Suppose n is not prime number. Then $\exists m, k \in \mathbb{Z}_+$

s.t. $1 < m < n$, $1 < k < n$ and $n = mk$

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

which is contradiction with definition of max ideal

$\iff$ If n is prime number, to prove $I = \text{id}(n)$ is max. ideal

suppose $I = \text{id}(n)$ is not max. Then $\exists$ ideal J of $\mathbb{Z}$ s.t.

$I \subsetneq J \subsetneq \mathbb{Z}$. But $\mathbb{Z}$ is p.i.r. Then $\exists m \in \mathbb{Z}_+$, $m \neq 1$

s.t. $J = \text{id}(m) \Rightarrow \text{id}(n) \subsetneq \text{id}(m) \subsetneq \mathbb{Z}$

Since $n \in \text{id}(n)$, since $n = 1 \cdot n \Rightarrow n \in \text{id}(m)$

$\therefore n = mk$ for some $k \in \mathbb{Z}_+$ and $k \neq 1$.

Hence n is not prime number. $\square$

$\therefore I = \text{id}(n)$ is max. ideal.

problems: let $R = \text{d.s of } (\mathbb{Z}_+, +, \cdot)$ with itself

let $I_1 = \{(2n, 0) : n \in \mathbb{Z}\}$. Is I_1 max. ideal of R

$I_2 = \{(2n, 3m) : n, m \in \mathbb{Z}\}$. Is I_2 max. ideal of R .

Remark : let $(F, +, \cdot)$ be a field. Then $\{0\}$ is the only max. ideal of F .

Definition :

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

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

② $\mathbb{Z}_8, \mathbb{Z}_{32}$ are local rings.

Theorem : let R be a comm. ring with unity 1. let M be a proper ideal of R . Then M is max. ideal $\iff (M, a) = R \quad \forall a \in R, a \notin M$.

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

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

$M \subsetneq (M, a) = M + id(a) \implies a = 0 + 1 \cdot a \in (M, a)$. But $a \notin M$. Thus $(M, a) = R$ (selection of 1)

$\impliedby$) If $(M, a) = R, \forall a \notin M$. To prove M is max ideal

suppose M is not max. ideal $\implies \exists$ ideal J of R s.t.

$M \subsetneq J \subsetneq R$.

(37)

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

$\therefore \forall x \in (M, a) \Rightarrow x = \underbrace{m}_J + \underbrace{ra}_J, m \in M \not\subseteq J$

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

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

$\therefore R = J$ Contradiction! Thus M is max. ideal

Theorem 8

Let R be a comm. ring with unity. I be a proper ideal of R , then $\exists$ a max. ideal of R s.t. $I \subseteq J$

Proof:

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

ليكن X مجموعة غير خالية وليكن F مجموعة غير خالية من مجموعات جزئية من X إذا كان لكل $\{C_i\}$ من F عناصر F فإن $F \ni U C_i$ وان F تملك عنصراً "أكبراً".

let I be a proper ideal of R .

See the collection $F = \{J : J \supseteq I, J \text{ is a proper ideal of } R\}$

$F \neq \emptyset$ (because I is proper ideal and $I \in F$)

let $\{C_i\}$ be a chain of F
سلسلة

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

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

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

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

It's clear that $I \subseteq \bigcup_{i \in \Lambda} C_i$ $\forall I \subseteq C_i$
من الواضح ان

$\bigcup_{i \in \Lambda} C_i \neq R$ (because $1 \notin C_i \forall i$, C_i is a proper ideal)

$\Rightarrow \bigcup_{i \in \Lambda} C_i \in F$. Then by Zorn's lemma F has maximal element, we say M .

To prove that M is maximal ideal of R .

let K be an ideal of R s.t. $M \subsetneq K$

$K \neq F$ لأن M هو أقصى

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

نتيجة
Corollary

كل $a \in R$ ليس في أي مثالي أقصى

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 .

معرف المثالي

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

(a) is the smallest ideal of R containing a .

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

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

see the id (a) . if $R = (a)$, then a is an invertible element.

either, if $R \neq (a)$, then by above theorem, $\exists$ max. ideal M containing (a) .

M and $(a) \subseteq M \Rightarrow a \in M$! $(a \notin M \text{ contradiction})$

$\therefore$ it must be $R = (a)$.

هذا هو المطلوب

Corollary

let R be a comm. ring with unity. Then R has at least one max. ideal.

Proof :- since R is comm ring with 1, R has at least one proper ideal say I .

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

Theorem :-

let R be a comm. ring with unity 1. if R is local ring, then the only idempotent elements of R are 0 and 1.

هذا هو المطلوب

Def: Let R be a comm. ring with unity 1 - 39 -

$a \neq 0 \in R$ is called idempotent element if $a^2 = a$.
also note

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

$$\because a^2 = a \Rightarrow a^2 - a = 0 \Rightarrow a(a-1) = 0$$

But $a \neq 0$ and $a-1 \neq 0$ *أيضا*

= *أيضا*

This means a and $a-1$ are Zero divisors
أيضا

$\therefore a$ and $a-1$ have no invertible elements

$\therefore a$ and $a-1$ belong to maximal ideal in R

But R has only one max. ideal M

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

$$\therefore M = R \text{ ! } (R \text{ is not a field})$$

Theorem

Let R be a Comm. ring with unity 1 .

and let I be a proper ideal of R . Then I is maximal

ideal $\iff R/I$ is a field.

Proof :- $\implies$

R/I is a field

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

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

$$\therefore 1 = x + ra \quad \text{where } r \in R, x \in I$$

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

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

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

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

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

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

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

$$\Leftrightarrow 1 - wb \in I$$

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

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

Remark 8

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

The ring $(\mathbb{Z}_8, +, \cdot)$ has no unity.

let $M = \{0, 4, 8, \dots\}$ is max. ideal of $\mathbb{Z}_8$. But

$\mathbb{Z}_8/M = \{0 + m, 2 + m\}$ is not field.

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

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

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

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

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

$\Rightarrow 2 \mid ab$. But 2 is prime number $\Rightarrow$ either $2 \mid a$

or $2 \mid b \Rightarrow a$ is multiply of 2 or b is multiply of 2

$\Rightarrow a \in \text{id}(2)$ or $b \in \text{id}(2)$

$\therefore \text{id}(2)$ is prime ideal.

proof : In the ring $(\mathbb{Z}, +, \cdot)$, if P is a prime number, then $\text{id}(P)$ is a prime ideal.

Theorem :

Let R be a comm. ring with unity 1. Then R is an integral domain $\Leftrightarrow \{0\}$ is a prime ideal.

Proof $\Rightarrow$ Suppose R is an integral domain.

To prove $\{0\}$ is prime ideal.

let $a, b \in R$ s.t. $ab \in \{0\} \Rightarrow ab = 0$

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

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

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

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

$\Rightarrow a \in \{0\}$ or $b \in \{0\} \Rightarrow a=0$ or $b=0$

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

Problem: (H.W)

في كلتا

In $(\mathbb{Z}_n, +, \cdot)$: A non trivial ideal $I \neq \mathbb{Z}_n$, $I \neq \{0\}$

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

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

let $I = \{\bar{0}, \bar{3}\}$, $J = \{\bar{0}, \bar{2}, \bar{4}\}$, $K = \{\bar{0}\}$

I, J are prime ideal. But K is not prime ideal.

since $a, b \in \mathbb{Z}_6$
 $2, 3 \in \mathbb{Z}_6$

$$2 \cdot 3 = 0 \in \mathbb{Z}_6$$

Example:

In the ring $(\mathbb{Z}_5, +, \cdot)$. $2 \in \mathbb{Z}_5 \wedge 3 \in \mathbb{Z}_5$

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

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

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

Theorem : let R be a comm's 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, $a \notin M$

$$\Rightarrow (M, a) = R \Rightarrow 1 \in (M, a) \Rightarrow 1 = m + ra \text{ for some}$$

$$m \in M, r \in R \Rightarrow b = mb + rab \in M$$

$\therefore b \in M$. Thus M is prime ideal.

عكس البرهان اعلاه غير صحيح والمثال التالي يوضح ذلك

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

Problem 5 - (H.W)

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

Remark :

The theorem is not true in rings without unity

Example : $I = \{0, \pm 4, \pm 8, \pm 12, \dots\}$ is max. in $\mathbb{Z}_6$

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

Theorem 8 let R be a comm. ring with unity 1 .
 If I be an ideal of R . Then I is a prime ideal $\iff (R/I, +, \cdot)$ is an integral domain.

Proof $\implies$ R is comm. ring with unity $1 \implies R/I$ is comm. ring with unity $1+I$.

If $(a+I)(b+I) = I \xrightarrow{\text{Zero element of } R/I}$

$\implies ab+I = I \implies ab \in I$, but I is a prime ideal

of $R \implies$ either $a \in I$ or $b \in I$.

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

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

$\longleftarrow$ To prove I is prime ideal

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

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

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

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

$\therefore I$ is prime ideal.

Theorem 8 - let R be a P.I.D. Then a nontrivial ideal I of R is maximal ideal $\iff$ it is prime ideal.

Proof : $\leftarrow$

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

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

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

$$I = (a), \quad J = (b)$$

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

$$\textcircled{1} \quad a = tb \quad \text{for some } t \in R \Rightarrow tb \in I$$

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

$$\text{if } b \in I \Rightarrow (b) \subseteq I = (a) \Rightarrow I = J \text{ !}$$

$$\text{Then } t \in I \Rightarrow t \in I = (a)$$

$$\textcircled{2} \quad t = sa, \quad s \in R$$

From $\textcircled{1}$ and $\textcircled{2}$, we get $a = sba$

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

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

$\therefore I$ is maximal ideal of R .

(42)

Theorem :- let R be a comm. ring with unity 1 s.t. $b^2 = b$

for all $b \in R$. Then a non-trivial ideal I is maximal ideal
 $\iff I$ is prime ideal

proof :- $\leftarrow$ let I be a prime ideal of R s.t.

$I \neq \{0\}$ and let J be an ideal of R s.t. $I \subsetneq J$.

Then $\exists b \in J, b \notin I$

since $b^2 = b$ (by hypothesis)

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

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

$\therefore (b-1) \in I \implies b-1 \in J$

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

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

$\therefore I$ is maximal ideal.

Definition :

الجزء القوي : nil radical

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

Example : ① (12) is an ideal in $\mathbb{Z}$

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

② (4) is an ideal in $\mathbb{Z}$

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

Remarks :

$$\textcircled{1} I \subseteq \sqrt{I}$$

② let $n \in \mathbb{Z}_+$ and (n) is an ideal s.t. $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$

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

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

و هو يكافئ العنصر

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

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

Proposition :-

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

Proof :-

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

Definition :

- 43 -

nil radical. الجذر النيلي

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

Example : ① (12) is an ideal in $\mathbb{Z}$

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

② (4) is an ideal in $\mathbb{Z}$

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

Remarks :

① $I \subseteq \sqrt{I}$

② let $n \in \mathbb{Z}_+$ and (n) is an ideal s.t. $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$

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

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

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

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

Proposition :-

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

Proof :-

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

Class

$$(x-y) = \overset{n+m}{x} + \overset{n+m}{(n+m)x} + \overset{n+m-1}{y} + \dots + \overset{n}{(-)^{n-m}}xy + \dots + \overset{m+n}{y}$$

$\in I \quad \in I \quad \in I \quad \in I$

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

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

$$(xx^n) = \overset{n}{x} \overset{n}{x} \Rightarrow \overset{n}{xx} \in I$$

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

Remark :-

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

Proof :- It is clear that $\sqrt{I} \subseteq \sqrt{\sqrt{I}}$ by def. $\rightarrow$ ①

Now, To prove $\sqrt{\sqrt{I}} \subseteq \sqrt{I}$

let $w \in \sqrt{\sqrt{I}}$. Then $\exists n \in \mathbb{Z}_+$ s.t.

$$\overset{n}{w} \in \sqrt{I} \Rightarrow (\overset{n}{w})^m \in I, m \in \mathbb{Z}_+$$

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

$$\& \sqrt{\sqrt{I}} \subseteq \sqrt{I} \rightarrow \textcircled{2}$$

From ① and ②, we get $\sqrt{\sqrt{I}} = \sqrt{I}$.

Definition :

let $(R, +, \cdot)$ be a ring and I be an ideal of R . Then I is called semiprime if $I = \sqrt{I}$.

بداية

Example :

let $6\mathbb{Z}$ be an ideal of $\mathbb{Z}$.
Then $6\mathbb{Z}$ is a semiprime ideal of $\mathbb{Z}$.
Since $\sqrt{6\mathbb{Z}} = 6\mathbb{Z} = (6)$

Remark : - Every prime ideal is semiprime.

But the Converse is not true in general for
example : $6\mathbb{Z}$ is semiprime ideal in $\mathbb{Z}$, but
it is not prime in $\mathbb{Z}$.

Theorem : -

let I be an ideal of R . Then

I is semiprime $\iff R/I$ has not contain nilpotent elements only zero element.

Proof : $\implies$ let $a+I$ be nilpotent element in

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

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

$$\therefore a + I = I$$

$$\iff \text{it is clear that } I \subseteq \sqrt{I}$$

Now, let $x \in \sqrt{I} \implies x^n \in I$ for some $n \in \mathbb{Z}_+$

$$\iff x^n + I = I$$

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

$\therefore x+I$ is nilpotent element in R/I

$$\stackrel{\text{Theorem}}{\implies} \sqrt{I} = I \quad \because x+I = I \implies x \in I$$

Definition

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

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

Example :

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

Remark

$$a, b \in R \Rightarrow a \in I \text{ or } b \in I \Rightarrow I \text{ is prime}$$

Every prime ideal is primary ideal but the converse is not true. For example $\text{id}(4)$ in $\mathbb{Z}$ is primary ideal but not prime.

Theorem: Let R be a ring and I be a non-trivial ideal of R . Then I is primary ideal if and only if all

Zero divisors in $\frac{R}{I}$ are nilpotent elements.

proof: $\Rightarrow$) let I be a primary ideal, $a+I$ be zero

divisor in R/I that means $a+I \neq I$ and $\exists b+I \neq I$

$$\text{s.t. } (a+I)(b+I) = I \Rightarrow ab+I = I \Rightarrow ab \in I$$

But $b \notin I$ and I is primary ideal. Then $\exists$ positive integer

n s.t. $a^n \in I \Leftrightarrow a^n+I = I$. Therefore $a+I$ is nilpotent element.

$\Leftarrow$) let $ab \in I$ and $a \notin I \Rightarrow a+I \neq I$

now, $ab \in I \Rightarrow ab+I = I \Rightarrow (a+I)(b+I) = I$

if $b+I = I \Rightarrow b \in I$. This completes the proof

if $b+I \neq I \Rightarrow b+I$ is zero divisor. Then $b+I$ is

nilpotent, that is $\exists$ positive integer number $n \in \mathbb{Z}_+$

s.t. $(b+I)^n = 0+I = I \Rightarrow b^n \in I \Rightarrow b^n+I = I$

Thus I is primary ideal.

Boolean Rings

الحلقات 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 $(1)^2 = 1$, $(0)^2 = 0$

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

since $(2)^2 = 1$

Remark : Every Boolean ring is Comm. ring and $ch(R)=2$

Theorem :

Let $(R, +, \cdot)$ be a Boolean ring and I be a proper ideal of R . The following statements are equivalent

- (1) I is max. ideal
- (2) I is prime ideal
- (3) $\forall 0 \neq a \in R$ either $a \in I$ or $1-a \in I$.

Proof (1) $\Rightarrow$ (2) is proved.

(2) $\Rightarrow$ (3) let $a \in R, a \neq 0$

$\therefore a(1-a) = a - a^2 = a - a = 0 \Rightarrow 0 \in I \Rightarrow$ either $a \in I$ or $(1-a) \in I$ because I is prime ideal

(3) $\Rightarrow$ (1)

let M be an ideal of R st. $I \subsetneq M$, then $\exists x \in M, x \notin I$, Therefore by (3) $1-x \in I \subset M$

$\therefore x, 1-x \in M, M$ is an ideal of $R \Rightarrow 1 \in M \Rightarrow M=R$ $\square$

$\therefore I$ is max. ideal

Theorem :

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

Proof : $\Rightarrow$) let $a \in R, a \neq 0$

$$a = a \cdot 1 = a(a \bar{a}) = (a \cdot a) \bar{a} = a^2 \cdot \bar{a} = a \cdot \bar{a} = 1$$

$$\therefore R = \{0, 1\} \Rightarrow R \cong \mathbb{Z}_2$$

$\Leftarrow$) It is clear



I have been thinking about you a lot lately.

I have been thinking of you very much lately, and I hope you are well. I am well and hope this letter finds you the same. I am sure you are. I am sure you are. I am sure you are.

1. Yellow
 2. Orange
 3. Red
 4. Green
 5. Blue
 6. Purple
 7. Pink
 8. White
 9. Black
 10. Grey
 11. Brown
 12. Gold
 13. Silver
 14. Maroon
 15. Teal
 16. Light Blue
 17. Light Green
 18. Light Purple
 19. Light Pink
 20. Light Yellow
 21. Light Orange
 22. Light Red
 23. Light Green
 24. Light Blue
 25. Light Purple
 26. Light Pink
 27. Light Yellow
 28. Light Orange
 29. Light Red
 30. Light Green
 31. Light Blue
 32. Light Purple
 33. Light Pink
 34. Light Yellow
 35. Light Orange
 36. Light Red
 37. Light Green
 38. Light Blue
 39. Light Purple
 40. Light Pink
 41. Light Yellow
 42. Light Orange
 43. Light Red
 44. Light Green
 45. Light Blue
 46. Light Purple
 47. Light Pink
 48. Light Yellow
 49. Light Orange
 50. Light Red
 51. Light Green
 52. Light Blue
 53. Light Purple
 54. Light Pink
 55. Light Yellow
 56. Light Orange
 57. Light Red
 58. Light Green
 59. Light Blue
 60. Light Purple
 61. Light Pink
 62. Light Yellow
 63. Light Orange
 64. Light Red
 65. Light Green
 66. Light Blue
 67. Light Purple
 68. Light Pink
 69. Light Yellow
 70. Light Orange
 71. Light Red
 72. Light Green
 73. Light Blue
 74. Light Purple
 75. Light Pink
 76. Light Yellow
 77. Light Orange
 78. Light Red
 79. Light Green
 80. Light Blue
 81. Light Purple
 82. Light Pink
 83. Light Yellow
 84. Light Orange
 85. Light Red
 86. Light Green
 87. Light Blue
 88. Light Purple
 89. Light Pink
 90. Light Yellow
 91. Light Orange
 92. Light Red
 93. Light Green
 94. Light Blue
 95. Light Purple
 96. Light Pink
 97. Light Yellow
 98. Light Orange
 99. Light Red
 100. Light Green
 101. Light Blue
 102. Light Purple
 103. Light Pink
 104. Light Yellow
 105. Light Orange
 106. Light Red
 107. Light Green
 108. Light Blue
 109. Light Purple
 110. Light Pink
 111. Light Yellow
 112. Light Orange
 113. Light Red
 114. Light Green
 115. Light Blue
 116. Light Purple
 117. Light Pink
 118. Light Yellow
 119. Light Orange
 120. Light Red
 121. Light Green
 122. Light Blue
 123. Light Purple
 124. Light Pink
 125. Light Yellow
 126. Light Orange
 127. Light Red
 128. Light Green
 129. Light Blue
 130. Light Purple
 131. Light Pink
 132. Light Yellow
 133. Light Orange
 134. Light Red
 135. Light Green
 136. Light Blue
 137. Light Purple
 138. Light Pink
 139. Light Yellow
 140. Light Orange
 141. Light Red
 142. Light Green
 143. Light Blue
 144. Light Purple
 145. Light Pink
 146. Light Yellow
 147. Light Orange
 148. Light Red
 149. Light Green
 150. Light Blue
 151. Light Purple
 152. Light Pink
 153. Light Yellow
 154. Light Orange
 155. Light Red
 156. Light Green
 157. Light Blue
 158. Light Purple
 159. Light Pink
 160. Light Yellow
 161. Light Orange
 162. Light Red
 163. Light Green
 164. Light Blue
 165. Light Purple
 166. Light Pink
 167. Light Yellow
 168. Light Orange
 169. Light Red
 170. Light Green
 171. Light Blue
 172. Light Purple
 173. Light Pink
 174. Light Yellow
 175. Light Orange
 176. Light Red
 177. Light Green
 178. Light Blue
 179. Light Purple
 180. Light Pink
 181. Light Yellow
 182. Light Orange
 183. Light Red
 184. Light Green
 185. Light Blue
 186. Light Purple
 187. Light Pink
 188. Light Yellow
 189. Light Orange
 190. Light Red
 191. Light Green
 192. Light Blue
 193. Light Purple
 194. Light Pink
 195. Light Yellow
 196. Light Orange
 197. Light Red
 198. Light Green
 199. Light Blue
 200. Light Purple
 201. Light Pink
 202. Light Yellow
 203. Light Orange
 204. Light Red
 205. Light Green
 206. Light Blue
 207. Light Purple
 208. Light Pink
 209. Light Yellow
 210. Light Orange
 211. Light Red
 212. Light Green
 213. Light Blue
 214. Light Purple
 215. Light Pink
 216. Light Yellow
 217. Light Orange
 218. Light Red
 219. Light Green
 220. Light Blue
 221. Light Purple
 222. Light Pink
 223. Light Yellow
 224. Light Orange
 225. Light Red
 226. Light Green
 227. Light Blue
 228. Light Purple
 229. Light Pink
 230. Light Yellow
 231. Light Orange
 232. Light Red
 233. Light Green
 234. Light Blue
 235. Light Purple
 236. Light Pink
 237. Light Yellow
 238. Light Orange
 239. Light Red
 240. Light Green
 241. Light Blue
 242. Light Purple
 243. Light Pink
 244. Light Yellow
 245. Light Orange
 246. Light Red
 247. Light Green
 248. Light Blue

د. حاتم + د. نسيه

الفصل السابع

Chapter Seven

ملقة الحدوديات

Chapter Seven

"Polynomial Ring"

7

Def: Let R be any ringLet $S = \{ f(x) : f(x) = a_0 + a_1x + \dots + a_nx^n, a_0, a_1, \dots, a_n \in R \}$ or $\{ f(x) : f(x) = \sum_{i=0}^n a_i x^i, a_i \in R, \forall i \leq n \}$ Any $f(x) \in S$ is called polynomial over R . Define $+$ as by:-Let $f(x), g(x) \in S$; $f(x) = \sum_{i=0}^n a_i x^i, a_i \in R, a_i = 0 \forall i > n$ $g(x) = \sum_{i=0}^m b_i x^i, b_i \in R, b_i = 0 \forall i > m$ 1) $f(x) + g(x) = \left(\sum_{i=0}^t c_i x^i \right) \in S$ where $c_i = a_i + b_i$ $\forall i = 0, 1, \dots, t, c_i = 0 \forall i > \max\{n, m\}$ 2) $f(x) \cdot g(x) = \sum_{k=0}^t c_k x^k, c_k = 0 \forall k > n+m$ where

$$c_0 = a_0 b_0$$

$$c_1 = a_0 b_1 + a_1 b_0$$

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

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

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

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

(47)

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

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

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

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

$$b_3 = b_4 = \dots = b_n = 0$$

$$\begin{aligned} f(x) + g(x) &= (a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2 \\ &= (1 + 3) + (1 + 3)x + (0 + 1)x^2 \\ &= x^2 \end{aligned}$$

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

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

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

$$c_3 = a_0 b_3 + a_1 b_2 + a_2 b_1 + a_3 b_0 = 3 \cdot 0 + 1 \cdot 1 + 0 \cdot 3 + 0 \cdot 0 = 1$$

$$c_4 = a_0 b_4 + a_1 b_3 + a_2 b_2 + a_3 b_1 + a_4 b_0 = 0$$

Similarly,

$$\text{Since, } c_5 = c_6 = 0$$

$$\therefore f(x) \cdot g(x) = 3 + 2x + 2x^2 + x^3 \text{ which is poly. over } Z_4$$

Note:-

If R is a ring, then $S = \{f(x) : f(x) \text{ is a poly over } R\}$ is denoted by $R[x]$.

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

① $+$ and $\cdot$ are closed on $R[x]$.

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

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

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

$+$ is comm.

③ $+$ is asso. on $R[x]$.

④ let $h(x) = 0$; $h(x) \in R[x]$

and $h(x) + f(x) = f(x)$, then $h(x)$ = additive identity of $R[x]$.

⑤ If $f(x) = \sum_{i=0}^n a_i x^i$, let $(-f)(x) = \sum_{i=0}^n (-a_i) x^i$

⑥ $f(x) + [(-f)(x)] = 0 = h(x)$

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

• asso. on $R[x]$.

• dist. over $+$ on $R[x]$.

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

Remark

- ① If R is comm. ring, then $R[x]$ is comm. ring.
- ② If R has unity 1, then $R[x]$ has unity ($0(x)=1$)

Definition:

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

a_n is called the leading coefficient

- If $a_n \neq 0$, then $f(x)$ has degree n

- If $f(x) = a$ ($a \in R$), $f(x)$ is called constant poly.

of degree zero where $a \neq 0$

- If $f(x) = 0$, we shall assign no degree for $f(x)$.

Theorem "1.1.1"

Let R be an integral domain, $f(x), g(x)$ non zero polys in $R[x]$ then:

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

② either $f(x) + g(x) = 0$ or $\deg(f(x) + g(x)) \leq \max(\deg f(x), \deg g(x))$

proof

① let $f(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n$ is non-zero poly.

$a_n \neq 0$, i.e. $\deg f(x) = n$ is a polynomial

Let $g(x) = b_0 + b_1x + \dots + b_mx^m$ is a non-zero poly.

$b_m \neq 0$, i.e. $\deg g(x) = m$ is a polynomial

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

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

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

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

$$C_{m+n} = a_n b_m \neq 0 \quad \left(\begin{array}{l} \text{Since } a_n, b_m \in R, a_n \neq 0, b_m \neq 0 \text{ and } R \\ \text{has no zero divisor} \end{array} \right)$$

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

$$\text{Since } C_{n+m+s} = 0 \quad \forall s \geq 1$$

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

Corollary 2.11

If R is an integral domain, then $R[x]$ is an integral domain

Proof

R is an integral domain $\Rightarrow R$ is comm. ring with unity and R has no zero divisor.