Ring Theory

1- Definition of rings and some examples
2- Subrings and ideals
3- Ring homomorphism
4- Maximal ideals and their properties
5- Prime ideals and their properties
6- Semiprime ideals and their properties
7- Primary ideals and their properties
8- Jacobsin radical and Nilradical

Def: (a binary operation)

abinary operation of a set A is a funaction * defined by :

(a.b)=a*b , for all a,b belong to R

العملية الثنائية هي دالة معرفة حسب التعريف اعلاه (لكل عنصرين موجودين في المجموعة حاصل العملية على العنصرين يكون بالمجموعة ايضا)

Def: (ring)

let R be anon empty set and +,. Be to binary operation on R then (R,+,.) said to be ring if :

1- (R,+)is abelian group

2- (R,.)is semi group

3-For all a,b,c belong to R

a.(b+c)=a.b+a.c

(a+b).c=a.c+b.c

لتكن R مجموعة غير خالية و +. عمليتين ثنائيتين يسمى الزوج الثلاثي حلقة اذا الحلقة : حققت الشروط اعلاه

Def: (commutative ring)

(R,+,.) is said to be commutative ring if a.b=b.a for all a,b belong to R

تكون الحلقة ابدالية اذا حققت a.b=b.a

Def:

(R,+,.) is said to be commutative ring with identity if thier exist 1 such that a.1=1.a=a

تكون الحلقة ابدالية مع وجود العنصر المحايد اذا وجد عنصر محايد حاصل ضربه مع العنصر يكون الناتج العنصر نفسه

Def: (invertable)

(R,+,.)be a ring with identity 1 an element $a\neq0$ belong to R is said to be invertable if fined a^{-1} belong to R s.t. $a.a^{-1}=a^{-1}.a=1$

يسمى العنصر قابل للانعكاس اذا وجد له معكوس بحيث ان حاصل ضربه العنصر في معكوسه يساوي العنصر المحايد(1)

Ex: $z_3=[\bar{0},\bar{1},\bar{2}]$

The invertable element $\bar{1}$ and$\bar{2}$

Ex : (Q,+,.) ,(R,+,.),(Z,+,.) are comm. Ring with identity

Ex : (Q,+,.)has an invertabile element ?

Q an invertabile element

$\frac{a}{b} \in R \;\; \exists \frac{b}{a}$

b≠0 s.t $\frac{a}{b} \quad \frac{b}{a} = 1$

ex : (Z,+,.) has an invertabile element ?

no, because a∈ Z but a^{-1} doesn't belong to Z

ex: (z,+,.) has not invertiable element because a∈z but a^{-1} don't belong to z

Def :((divisior))

a ring (R,+,.) is said to have divisors of zero if ∃ non zero element a,b ∈R ∋a.b =0

a,b ≠0

يمكن ان تحوي الحلقة قواسم صفرية اذا كان عنصرين لا يساوون صفر حاصل ضربهم يساوي صفر

Ex : $(z_6,+_6,._6)$

$Z_6= [\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}]$

$$\bar{2}.\bar{3} = \bar{0}$$

$$\overline{\bar{2}, \bar{3}, \bar{4}}$$

Are zero divisior

REMARK : there is a ring contain an identity and others doesn't contain an identity

بعض الحلقات ممكن ان تحوي على عنصر محايد و بعضها لا تحوي

REMARK : : there are a rings commutative and others not commutative

بعض الحلقات تكون ابدالية و بعضها غير ابدالية

Ex : (z,+,.) has identity 1

(2z,+,.) has no identity

Q : if we have zero divisiors in the ring does you can use the concellation law? Why?

اذا عندي قواسم صفرية اكدر احقق قانون الحذف ؟؟؟؟

We cant use the concellation law if we have zero divisiors in the ring for example in Z_6

$\overline{2}.\overline{3} = 0$ and $\overline{3}.\overline{4} = 0$

$$\overline{2}.\overline{3} = \overline{3}.\overline{4} then\ \overline{2} = \overline{4}\ \ C!$$

لا يمكن استخدام قانون الحذف عندما يكون هناك قواسم صفرية يكون تنااقض

Def : (integral domain)

a commutative ring with identity (R,+,.) is said to be integral domain if does not have zero divisors , for all a $\in$ R ,for all b$\in$ R s.t a.b$\neq$ 0

تسمى الحلقة الابدالية التي تمتلك عنصر محايد ساحى تامة اذا كانت لا تمتلك قواسم صفرية

Def : (field)

A commutative ring with identity (R,+,.) is said to be a field if every non zero element has an inverse in R

تسمى الحلقة الابدالية التي تمتلك عنصر محايد بالحقل اذا كان لكل عنصر غير صفري يوجد له نضير

Ex : (Q, +,.) is a field

Since for all $0\neq \frac{m}{n} \in Q \ni \frac{n}{m} \in Q \; s.t \;\; \frac{m}{n}.\frac{n}{m} = 1$

Ex : (z,+,.) a field ?

No since not every non zero element has inverse

Theorem : every field is integral domain

كل حقل هو ساحة تامة

(عكس المبرهنة اعلاه لا يتحقق الا بشرط)

Theorem : every finite I.D. is a field

Proof : let (R,+,.) be I.D.

Suppose a1,a2,a3,…,an are members of the set R

Let 0≠a ∈R be a fixed elements a,a1,…,an

If a.ai=a.aj

So ai=aj (since R is I.D.)

Thus every element is at the form a.ai=1 a-1=ai

every non zero element has inverse in R

(R,+,.) is field

Theorem : let R be a ring then

1- a.0=0.a , for all a belong to R

2- (-a).(b)=(a). (_b)= - (a.b) for all a,b belong to R

3- (-a).(-b)=a.b

a-b ≡a+(-b)

def :

let (R,+,.) be a ring if there exist appositive integer (n) such that n.a=0

then the positive integer with this property is called characteristic of the ring if no such positive integer exist we say (R,+,.)

has characteristic zero

Def (subring)

Let (R,+,.) be a ring and let $\emptyset \neq s$ subset of R then (S,+,.) is called a

Subring of R if (s,+,.) is ring itself

حلقة جزبية اذا كانت حلقة s تكون ال Rمجموعة غير خالية و جزبية من الحلقة sلتكن ال ايضا

Theorem : (s,+,.) is a subring of (R,+,.) iff the following are satisfies :

1_ $\forall\, a,b \in s\,, a-b \in s$

2_ $\forall a,b \in s\,, a.b \in s$

Ex : (Q,+,.) , (z,+,.) are subring of (Q,+,.)

Remark : let (R,+,.) be a ring and let (s,+,.) be a subring of R then :

1- If (R,+,.) has an identity element then (s,+,.) not necessary has an identity

اذا كانت الحلقة تحوي عنصر محايد ليس بالصرورة ان الحلقة الجزبية تمتلك عنصر محايد

Ex : (z,+,.) has identity but subring (2z,+,.) has not identity

2- There are a rings has an identity which is deferent of the identity of the subring

العنصر المحايد للحلقة ليس بالضرورة ان يساوي العنصر المحايد للحلقة الجزئية

Ex : the identity element of (Z_6 , $+_6$,$._6$) is 1 but the identity of ($\{\bar{0},\bar{2},\bar{4}\}$,$+_6$,$._6$) is 4 and $1 \neq 4$

Def (ideal)

Let R be a ring and $\emptyset \neq I \subseteq R$ we called I an ideal if :

1- a-b $\in I\,, \forall a,b \in I$

2- ar$\in I \;\wedge ra \epsilon I\,, \forall a \in I\,, \forall r \in R$

تسمى الحلقة مثالية اذا حققت الشروط اعلاه

REMARK : 1- every ideal is a subring but the converse is not true for example (z,+,.) ⊆ (Q,+,.)

كل حلقة مثالية هي حلقة جزئية لكن العكس غير صحيح

2- let R be a ring then {0} , R are trivial ideal

هو مجموعة الصفر و الحلقة نفسها R الحل التافه للحلقة

3- every ring of the form nz is an ideal of Z

كل حلقة من نوع nz تكون مثالية للحلقة z

4- {0} , Q are the only ideals in (Q,+,.)

هو مجموعة الصفر و البحلقة نفسها (لها مثالي تافه فقط) Q المثالي الوحيد للحلقة

5- let (R,+,.) be a ring with identity and let I be an ideal in R if 1∈I then I=R

Proof : $1 \in I$, $\forall r \in R$ $\;1.r \in I \Rightarrow R \subseteq I \Rightarrow I=R$

6- let (R,+,.) be a ring and let I be an ideal in R if I contain an invertable element then R=I

a∈ I has inverse say b ⇒ 1=a.b belong to I then I=R

7- if R is a field then the trivial ideals are the only undines

اذا كالنت ال R حقل فان المثالي لها يكون المثالي التافه فقط

Ex : in (Q,+,.) {0} are the only ideal in Q

Def : let (R_1 ,+,.) ,(R_2 ,+,.) are two rings we define :

R_1XR_2 ={(a,b),a ∈R_1 and b∈R_2}

Define +,. As follows

(a,b)+(c,d)=(a+c,b+d)

(a,b).(c,d)=(a.c,b.d)

Then $R_1 \times R_2$ is called the direct product of R_1 AND R_2

Remark : the direct product of two integral domain is not nessary integral domain

Ex : Z×Z ={(a,b),a,b ∈ z } every element of the (a,0) , $0 \neq a \in z$ is zero divisor (a,0),(0,a)=(0,0)

Def : let R be aring and let a ∈ R a is called idempotent element if $a^2=a$

اذا حقق الشرط اعلاه idempotent تسمى العنصر الذي ينتمي للحلقة ب

Def : an element a∈R is called nilpotent if $a^n=0$ where n is positive integer

Theorem : let R be a ring such that every element in R is idempotent then R is commutative

اذا كانت الحلقة ابدالية idempotent يكون R كل عنصر في الحلقة

Remark : the convers is not true for example (z,+,.) is commutative but not every element in z is an idempotent it is only 0,1 are idempotent elements

Theorem : every non zero nilpotent element is zero divisor

كلnilpotent غير صفري هي قواسم صفرية

Remark : the nilpotent element in the integral domain is =0

Proof : suppose $0 \neq a$ is nilpotent element in integral domain

A is zero divisor c!

a=0 (since R is I.D)

Theorem : let R be a ring with identity and let a be nilpotent in R then 1+a has inverse

Def : let $(R_1,+,.),(R_2,+,.)$ are two rings then the function $f:R_1 \rightarrow R_2$ is called ring homomorphism if the following satisfies :

1- f(a+b)=f(a)+f(b) ,$\forall a,b \in R$

2- f(a.b)=f(a).f(b) ,$\forall a, b \in R$

Ex : f: $z \rightarrow z$ defined bt f(n)=2n

Let n,m belong to Z

1- f(n+m)=2(n+m)=2n+2m=f(n)+f(m)

2- f(n.m) =2nm$\neq$2n.2m

F is not ring homo

Theorem : there is no ring homo. From $Z+_0Z$ except the identity function f:Z $\rightarrow$Z defined by f(n)=n ,$\forall n \in Z$

Proof :1- f(n+m)=n+m=f(n)+f(m)

2- f(n.m)=n.m=f(n).f(m)

THEOREM: let (R,+,.) be a ring with identity then (R,+,.) has char $n>0$ iff n is the least positive integer for which $n.1=0$

هي اصغر n اذا و فقط اذا n>0 حيث nحلقة تحوي نظير فان مميز الحلقة هو Rاذا كانت رقم موجب صحيح حيث n.1=0

Proof;

$\Rightarrow$ if $char(R)=n>0 \Rightarrow n.1=0$

$\Leftarrow$now suppose that $m.1=0$ where $0<m<n$

$m.a=m.(1.a)$

$=(m.1).a$

$=0.a=0 \quad , \forall a \in R$

n is the least integer for which $n.1=0$

THEOREM : let (R, +,.) be an integral domain ,then $char(R)=0$ or prime number

Proof ;

Suppose that char (R) $=n>0$ and we assume that n is not prime

$n= n_1.n_2$ ($n_i<n>0$,where $i=1,2$)

$0=n._1=n_1.n_2.1$

$=n_1.n_2.1^2$

$=(n_1.1).(n_2.1)$

R is integral domain $\Rightarrow$ either $n_1.1=0$ or $n_2.1=0$ C!

Def : a ring homo. f=$R \to \acute{R}$ is said one to one iff is one to one and onto iff is onto and iff is one to one and onto then we say that f is an isomorphism and this case we write $R \cong R$

Def : let . f=R→R´ be ring homo then the kernel of f is the set

Ker f ={x∈ $R\ s.t\ f(x) = \acute{0}\} \neq \emptyset$

Theorem : (ker f ,+,.) is an ideal of R

Proof: 1- let $a, b \in kerf$

⇒ f(a)=0 and f(b)=0

f(a-b)=f(a)-f(b)=0-0=0

a-b∈ $kerf$

theorem : 1- let f=R→R´ be ring homo then f is one to one iff kernal f =0

2- let f=R→R´ be ring homo then:

a- $F(0_R)=0_R$

b- F(-r)=-f(r)

c- If ś is a subring of Ŕ then $f^{-1}(\acute{S})$SUBRING OF R and $f^{-1}(\acute{s}) = \{x \in \acute{R}, f(x) \in \acute{s}\}$

3- if I is an ideal in R then $f^{-1}(1)$ is an ideal in R

4- if I is an ideal in R and F is onto then f(I) is an ideal in Ŕ

DEF : let R be a ring and let I_1 and I_2 are two ideal in R then

$I_1 + I_2 = \{a+b, \text{ where } a \in I_1 \text{ and } b \in I_2\}$

$I_1 . I_2 = \{ a_i b_i , a_i \in I_1 , b_i \in I_2 , \forall i\}$

Theorem : $I_1 + I_2$ and $I_1 . I_2$ are ideal in R

Def : let $I_1, I_2, \ldots, I_n$ are ideal in a ring R if :

1- $R = I_1 + I_2 + \ldots + I_n$

2- $I_1 \cap (I_1 + I_2 + \ldots + I_{J-1} + I_{Jn} + \ldots + I_n) = \{0\}$

Then we say that R is a direct sum of $I_1, I_2, \ldots, I_n$ and denoted by

$R = I_1 \oplus I_2 \oplus \ldots \oplus I_n$

Theorem : $R = I + J$ iff every element in R written by x+y where $X \in I \wedge Y \in J$ and written in one way

Def (maximal ideal)

An ideal (I,+,.) of the ring (R,+,.) is a maximal ideal provided $I \neq R$ and if $I \subset J \subset R$ where J is an ideal in R then J =R

مثالي اعظم اذا كانت هي اكبر مثالي في الحلقة . اذا وجد مثالي اكبر منها فانه Iتكون ال يساوي الحلقة نفسها

Ex : $(Z_6 , +_6 , ._6)$

$I_1 = \{\bar{0}, \bar{3}\}$, $I_2 = \{\bar{0}, \bar{2}, \bar{4}\}$

I_1 and I_2 are maximal ideal

Ex : $(Z_4 , +_4 , ._4)$

$I = \{ \bar{0}, \bar{2} \}$is the maximal in z_4

Ex : in (Z,+,.)

<n> is maximal ideal in z $\Leftrightarrow$ n is prime , where = {rn ,r Z}

remark : there is no proper ideal in Q , R, Ø

in general if F is a field then {0} and F the uniqnes ideal in F

(في الحقل المثالي الوحيد هو المثالي التافه (الصفر و الحلقة نفسها

ex : Z_5 is a field ⇒ there is no proper ideal in Z_5

Z ⊆ Q but not an ideal

Remark : 1- if R_1 and R_2 are two rings with identity then R1 X R2 has an identity

اذا كانت الحلقات تحوي عنصر محايد فان الجداء المباشر لهم يحوي على عنصر محايد ايضا

2- if R1 and R2 are two commutative rings then R1 X R2 is also commutative ring

اذا كانت الحلقات ابدالية فان الجداء المباشر لهم يكون ابدالي ايضا

Ex : Q×Q is not a field

(a,0),(0,b) in Q×Q but (a,0),(0,b) =(0,0)

So QXQ contain zero divisor

Ex : 2Z ×Z is an ideal in Z×Z ? H.W

Q; in the following rings what are the nilpotent and idempotent elements ?

1- $(Z_8,+_8,._8)$

2- $(Z_6,+_6,._6)$

Def : (Boolen ring)

A Boolen ring (R,+,.) is a ring with identity every element of which is idempotent , $a^2=a$, for all a belong to R

اذا كان كل عنصر بالحلقة هو عنصر متحايد booleanتسمى الحلقة

Ex : 1- Z_2, $0^2=0$, $1^2=1$

2- p(x) , $A^2=A \cap A = A$, $\forall A \subseteq X$

Remark : (-a)(-b)=(ab)

Remark : the set of all nilpotent elements form an ideal ((H.W))

Q: every zero divisor is nilpotent ?

No , in Z_6 we have $\overline{2}.\overline{3}$ but for any number power n 2^n or $3^n \neq 0$

Remark : 1- in z the nilpotent element are only {0} since z is integral domain

2- Z_8 is not integral domain

Zornes lemma : let x non empty set and F non empty set be the set of all subset of x , where for every chain $\{c \propto\}_{\alpha\in\cap}$ of sets from $F \cup_{\propto\in\cap} \subset\propto F$ then F has a maximal element

Theorem : let R be a commutative ring with identity and let I be a proper ideal in R then there exist a maximal ideal M such that $I \subseteq M$

لتكن R حلقة ابدالية تحوي عنصر محايد و لتكن I (proper ideal) فان وجد للحلقة m جزئية من المثالي الاعظم I يكون مثالي اعظم للحلقة بحيث

Claim : M is the maximal ideal which is contain I suppose that I$\subseteq M \subset N \subset R$ where N is an ideal in R .

N$\notin F$ (since M is the maximal element of F)

N=R

$\therefore$ M is a maximal ideal such that $I \subset M$

Def : (local ring)

A commutative ring with identity is called local ring if it has a unique maximal ideal

تسمى الحلقة حلقة موضعية اذا كان المثالي الاعظم للحلقة وحيد

Ex : Z_4 is a local ring since {0,2} is the unique maximal in Z_4

Cor : every field is a local ring H.W

كل حقل هو حلقة موضعية

Lemma : in the local ring the idempotent elements is only 0 and 1

في الحلقة الموضعية العناصر المتحايدة هي فقط 1 , 0

Proof :$\Longrightarrow$ let 0$\neq a$ *and* $1 \neq a$ be an idempotent element

$a^2=a$

$a^2-a=0$

a(a-1)=0

$\because 0 \neq a$ *and* a *and* $a-1$ *is zero divisor*

$\because$ a and (a-1) has no inverse (since the zero divisor has no inverse)

$\Longrightarrow$ a and a-1 must belong to some maximal ideal say M

$\because a \text{ and } a-1 \in M$

1= a and a-1 ∈ M C!

∴either a=0 or a=1

Ex : In $Z_2=\{\overline{0},\overline{1}\}$ every element is an idempotent

Z_2 is a local ring

Theorem : let I be a proper ideal in R then I is a maximal iff $\forall a \in R, a \notin$ I where <I,a>=R

Proof : :⟹ let I ⊊ R be a maximal and a ∈ R with a∉ I

I⊂ <I,a>⊆ R

But I is maximal

<I,a>=R

⇐ let I ⊊R and <I,a>=R

Where a ∉ I

We want to proof that I is maximal

Suppose that there exist an ideal kin R

I ⊊ K ⊆ R

Thus by assumption <I,a>=R

1∈ R ,1=m+ra , where m belong to I ,r belong to R

So 1∈ R , k=R

∴I is maximal

تذكير على زمرة القسمة $\frac{R}{I}$

صيغة العنصر a+I

العنصر المحايد1+I

Zero للحلقة (I)

THEOREM : Let R be commutative ring with identity let I be a proper ideal in R . then I is maximal ideal iff $\frac{R}{I}$ is a field

Proof : $\Longrightarrow$ let (a+I) $\in \frac{R}{I}$ *where I is proper maximal*

$\therefore I \text{ } is \text{ } maximal$

$\therefore$ <I ,a> =R

$\therefore 1\epsilon < I, a > \Longrightarrow 1 = m + ra \qquad r \in R\ , m \in I$

$\therefore m = (1 - ra) \in I$

$\because ra + I = 1 + I$

(r+I)(a+I)=1+I

a+I has an inverse in $\frac{R}{I}$

$\therefore \frac{R}{I}$ is a field

$\Longleftarrow$ we have to show that I is maximal suppose that $I \subsetneq J \ \subseteq R$

$\because I \subsetneq J \ \Longrightarrow \exists x \in J \text{ } and \text{ } x \notin I$

$I \neq x + I \in \frac{R}{I}$

$\therefore \frac{R}{I} \text{ } is \text{ } a \text{ } field \ \Longrightarrow \exists y \in I$

$\ni (x+I)(y+I) = 1+I$

Xy+I=1+I

(1-xy)∈ $I \subset J$

$\therefore xy \in J$

$\Longrightarrow 1 - xy + xy \in J$ $\quad\quad\because 1 \in J$

J=R so I is maximal

Def : (prime ideal)

Let R be a commutative ring with identity . let p be a proper ideal in R ,P is called a prime ideal if whenever a.b∈p then either a∈p or b∈p , for all a,b ∈R

Ex :1- (0) is prime ideal in Z

a.b=0 , but z is I.D (has no zero divisor)

⟹ either a=0 or b=0

$\Longrightarrow a \in (0) or\ b \in (0)$

So (0) is prime ideal

2- (n) is prime ideal in Z ⇔ n is prime integers

Proof ⟹

$\Longleftarrow (a.b) \in (n)$

$\because n\ is\ prime\ integer$ ⟹ nI ab ⟹ n I a or n I b

$\Longrightarrow a \in (n) or\ b \in (n)$

3- 2Z is prime in Z

Lemma : a commutative ring with identity is an integral domain iff (0) is prime ideal

Proof : $\Longrightarrow let\ a, b\ \in R\ such\ that\ a.b \in (0)$

a.b=0

$\because R\ is\ I.D$

$\therefore either\ a = 0\ or\ b = 0\ \Longrightarrow either\ a \in (0) or\ b \in (0)$

(0) Is prime ideal

$\Longleftarrow$ let (0) be a prime ideal

a.b=0

$\because (0) is\ prime\ ideal\ \Longrightarrow either\ a \in (0) or\ b\ \in (0)$

i.e a=0 or b=0

$\therefore R\ is\ I.D$

Ex : in (Z_6, $+_6$, $._6$)

$\overline{2}.\overline{3} = 0$

But $\overline{2} \neq 0$, $\overline{3} \neq 0$

$\overline{2} \notin (0)$, $\overline{3} \notin (0)$

(0)Is not prime ideal in Z_6

Theorem : let R be a commutative ring with identity and I be a proper ideal in R then I is prime ideal iff $\frac{R}{I}$ is I.D

Proof :$\Longrightarrow let\ (a + I), (b + I) \in \frac{R}{I}$

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

$\Leftrightarrow (a.b + I) = I$

$\Leftrightarrow a.b \in I$

But I is prime ideal

Either $a \in I\ or\ b \in I$

$\therefore \frac{R}{I}\ is\ I.D$

$\Longleftarrow let\ a.b\ \in I\ \ \Leftrightarrow (a.b) + I = I$

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

$\because \frac{R}{I}\ is\ I.D$

$\because \frac{R}{I}\ HAS\ NO\ ZERO\ DIVISOR$

Either a+I =I or b+I=I

I is prime ideal

Cor : every maximal ideal is prime

Proof : let I be a maximal ideal then by last theorem $\frac{R}{I}$ Is a field

$\Longrightarrow \frac{R}{I}$ is I.D.

By last theorem I is prime

The converse is not true as the following ex. Show:

Ex " since (0) is prime in Z but not max

Lemma :let R be (P.I.D) let 0≠I is an ideal in R then I is maximal iff I is prime .

Proof : ⟹by theorem every maximal is prime

⟸ let I be a prime ideal in R

Suppose that I ⊂ $J \subseteq R$

$\because R\ is\ P.I.D \implies \exists a \neq 0\ and\ b \neq 0 , \in R\ s.t$

I=<a> , J=<b> $\therefore < a > \subset < b > \subseteq R$

$\because a \in < a > \implies a \in < b >$

$\therefore a = rb \quad , r \in R$

$\therefore rb \in < a > = I , b \notin < a >$

<b>⊂ <a>

<b>= <a> C!

And since <a> =I is prime

R belong to <a>

r=t

t belong to R

a=t.a.b=at.b

Def: let R be commutative ring with identity and let I be an ideal in R define $\sqrt{I} = \{r \in R, r^n \in I \; for \; some \; n \; \in N\} \neq 0$

The set is called nil radical of I

Ex in $Z_4=\{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$, $\{\bar{0}\}$,$\{\bar{0}, \bar{2}\}$

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

Remark :$\sqrt{I}$ is an ideal in R

let $a, b \in \sqrt{I} \implies \exists \; m, n \; \in N \; \ni \; a^n \; \in I \; and \; b^n \; \in I$

$\therefore \; (a-b)^{n+m} \; \in I \implies a - b \in \sqrt{I}$

Let $a \in \sqrt{I} \; , r \in R \; \longrightarrow \; ra \in \sqrt{I} \; \implies \exists n \in N \; \ni a^n \in I$

REMARK : for any ideal I , J in R we have :

1- $\sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$

2- $I \; \subseteq \sqrt{I}$

3- $\sqrt{\sqrt{I}} = \; \sqrt{I}$

4- $\sqrt{I} + \sqrt{J} \subseteq \sqrt{I + J}$

PROOF : H. W

Remark : in Z (P.I.D) every ideal in Z is of the form <n> where n∈ Z

1) Let n= $p_1 p_2, \ldots, p_n$

Where $p_1 p_2, \ldots, p_n$ is distinct prime num

Then $\sqrt{< p1p2 , \dots , pn >} = < p1p2 , \dots , pn >$

2) If n= $P_1^{x1} p_2^{x2} ,\dots,p_m^{xm}$

Where p_1p_2 , … , p_n are prime and

X1,x2,…,xm ∈ Z^+

Then $\sqrt{< n >} = \sqrt{< p_1^{x1}, p_2^{x2}, \dots , p_m^{xm}}$

= $<p_1 \, p_2 ,\dots, p_m>$

$\sqrt{< 2^3, 3^4 >} \quad , < 2,3 > =< 6 >$

Ex :in Z

$\sqrt{< 8 >} = \sqrt{2^3} = < 2 >$

$\sqrt{< 6 >} = \sqrt{< 2.3 >} = < 2.3 > = < 6 >$

$\sqrt{< 50 >} = \sqrt{< 5^2 . 2 >} =< 5.2 > = < 10 >$

Def :(semi prime)

let R be commutative ring with identity and I be a proper ideal in R we say I semi prime if $I = \sqrt{I}$

في الحلقة يسمى proper ideal هو I حلقة ابداليه و تحوي على عنصر محايد و Rلتكن الI شبه اولي اذا كان $I = \sqrt{I}$

Ex : $\sqrt{< 6 >} =< 6 >$

<6> is semi prime

Lemma : every prime ideal is semi prime

كل مثالي اولي هو مثالي شبه اولي

Proof : let I be a prime ideal in R we known that $I \subseteq \sqrt{I}$ So it enough to proof $\sqrt{I} \subseteq I$

Let w $\in$ $\sqrt{I} \implies w^n \in I$ $\quad$ $for\ some\ n \in I$

We chose n the smallest no. satisfy this

Claim : n=1

If n>1

$I \ni w^n = w^{n-1}.w \quad C!$

If $w^{n-1} = w.w^{n-2} \quad C!$

For example w^2=w.w

n=1

W belong to I

$\sqrt{I} \subseteq I \quad , \quad I = \sqrt{I}$

I is semi prime

The converse is not true $\quad$ (Semi prime $\nrightarrow$ not prime)

In z

6z is semi prime but not prime

2$\notin$ <6>

$3 \notin <6>$

But $2,3 \in <6>$

Remark : in Z (P.I.D) every ideal in Z is of the form $<n>$ where $n \in Z$

3) Let $n= p_1p_2 , \dots , p_n$

Where $p_1p_2 , \dots , p_n$ is distinct prime number

Then $\sqrt{< p1p2 , \dots ,pn >} = < p1p2 , \dots ,pn >$

4) If $n= P_1{\propto^1}\ p_2{\propto^2} ,\dots,p_m{\propto^m}$

Where $p_1p_2 , \dots , p_n$ are prime and

$\propto 1,\propto 2,\dots,\propto m \in Z^+$

Then $\sqrt{< n >} = \sqrt{< p_1^{\propto 1} p_2^{\propto 2}, \dots , p_m^{\propto m}}$

$= <p_1\ p_2 ,\dots, p_m>$

$\sqrt{< 2^3\ 3^4 >}$ $\quad , < 2\ 3 > =< 6 >$

Ex :in Z

$\sqrt{< 8 >}= \sqrt{2^3} = < 2 >$

$\sqrt{< 6 >}= \sqrt{< 2.3 >}= < 2.3 >= < 6 >$

$\sqrt{< 50 >}= \sqrt{< 5^2 . 2 >}=< 5.2 > = < 10 >$

Lemma :let R be (P.I.D) let $0\neq I$ is an ideal in R then I is maximal iff I is prime .

Proof : $\Longrightarrow$by theorem every maximal is prime

$\Longleftarrow$ let I be a prime ideal in R

Suppose that $I \subset J \subseteq R$

$\because R \text{ is } P.I.D \Longrightarrow \exists a \neq 0 \text{ and } b \neq 0 , \in R \text{ s.t}$

I=<a> , J=<b> $\therefore < a > \subset < b > \subseteq R$

$\because a \in < a > \Longrightarrow a \in < b >$

$\therefore a = rb \quad , r \in R$

$\therefore rb \in < a > = I , b \notin < a >$

<b>⊂ <a>

<b>= <a> C!

And since <a> =I is prime

R belong to <a>

r=t

t belong to R

a=t.a.b=at.b

Def: nil radical

let R be commutative ring with identity and let I be an ideal in R define $\sqrt{I} = \{r \in R, r^n \in I \text{ for some } n \in N\} \neq 0$

The set is called nil radical of I

Ex: in $Z_4=\{\bar{0},\bar{1},\bar{2},\bar{3}\}$, $\{\bar{0}\}$,$\{\bar{0},\bar{2}\}$ $\sqrt{\bar{0}}=\{\bar{0},\bar{2}\}$

Remark :$\sqrt{I}$ is an ideal in R

Proof : let $a,b\in\sqrt{I}\ \Longrightarrow \exists\ m,n\ \in N\ \ni\ a^n\ \in I\ and\ b^m\ \in I$

$\therefore\ (a-b)^{n+m}\ \in I\ \Longrightarrow a-b\in\sqrt{I}$

Let $a\in\sqrt{I}\ ,r\in R\ \longrightarrow\ ra\in\sqrt{I}\ \Longrightarrow\exists n\in N\ \ni a^n\in I$

REMARK : for any ideal I , J in R we have :

5- $\sqrt{I\cap J}=\sqrt{I}\cap\sqrt{J}=\ \sqrt{I-J}\ ,where\ I.J=\sum a_i.b_i\ \ ,a_i\in I\ ,b_i\in J$

6- $I\ \subseteq\sqrt{I}$

7- $\sqrt{\sqrt{I}}=\ \sqrt{I}$

8- $\sqrt{I}+\sqrt{J}\subseteq\sqrt{I+J}$

Proof : 1- $let\ X\ \in\sqrt{I\cap J}\ \Longrightarrow\exists n\in Z\ \ni x^n\in I\cap J$

$\Longrightarrow x^n\in I\ \wedge x^n\in J\ \Longrightarrow x\quad\in\sqrt{I}\wedge x\quad\in\sqrt{J}$

$\therefore\ \sqrt{I\cap J}\subseteq\sqrt{I}\cap\sqrt{J}$ 1

$let\ y\ \in\sqrt{I}\ \cap\sqrt{J}\ \Longrightarrow y\in\sqrt{I}\ \wedge\quad y\in\sqrt{J}$

$\exists n,m\in Z\ \ni y^n\in\sqrt{I}\wedge y^n\ \in\sqrt{J}$

$y^{n+m}=y^n.y^m\in I\cap J\Longrightarrow y\ \in\sqrt{I\cap J}$.....2

From 1 and 2

$\sqrt{I\cap J}=\sqrt{I}\cap\sqrt{J}$

$let\ t\ \in \sqrt{I-J} \Longrightarrow t^k \in I\ \wedge t^k \in J \Longrightarrow t \in \sqrt{I} \cap \sqrt{J} \Longrightarrow t \in \sqrt{I \cap J}$

$$\therefore \sqrt{I-J} \subseteq \sqrt{I \cap J}$$

Let w $\in \sqrt{I \cap J} \Longrightarrow w^n \in I\ \wedge w^m \in J\ for\ some\ m \Longrightarrow w \in \sqrt{I-J} \Longrightarrow$

$\sqrt{I \cap J} \subseteq \sqrt{I-J} \quad \therefore \sqrt{I \cap J} = \sqrt{I-J}$

2 – let $t \in I$, $\grave{t} \in I \Longrightarrow t \in \sqrt{I}$

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

3- from 2 $\Longrightarrow \sqrt{I} \subseteq \sqrt{\sqrt{I}}$ …….1

$let\ w\ \in \sqrt{\sqrt{I}} \Longrightarrow w^n \in \sqrt{I}, for\ some\ n\ \in Z$

$(w^n)^m \in I, for\ some\ m\ \in Z$

$w^{n.m} \in I \quad \therefore w \in \sqrt{I}$ … . .2

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

4 – let $w \in \sqrt{I} + \sqrt{J}$

W=a+b, where $a \in \sqrt{I}\ \wedge b \in \sqrt{J}$

$w^{n+m} = w^n . w^m = (a+b)^n . (a+b)^m = (a+b)^{n+m}$

$\therefore w^{n+m} \in I + J\ , w \in \sqrt{I+J}$

Remark : let R be a Boolean ring and I is maximal iff I is prime

مثالي اولي I مثالي اعظم اذا و فقط اذا Iفي حلقة بولين تكون ال

Proof: $\Longrightarrow clear$

$\Longleftarrow let\ R\ be\ a\ boolean\ ring\ and\ I\ be\ a\ prime\ ideal\ I \neq R$

$let\ I \subset J \subseteq R$

$\exists a \in J\ and\ a \notin J$

$R\ is\ boolean\ ring$

$a(a-1) \in I$

$a \notin I$ `$and\ I\ is\ prime \Longrightarrow a-1 \in J$

a,a-1$\in J$

a-(a-1)$\in J \quad \Longrightarrow 1 \in J$

J=R

I is maximal

Theorem : (quotient ring)

if (I,+,.) is an ideal of (R,+,.) then ($\frac{R}{I}$,+,.) is a ring , known as the quotient ring of R by I

proof : let (I ,+,.)be an ideal of the ring (R,+,.)

$(I\ ,+)\Delta(R,+)$

$a + I = \{a + i$ i ∈ I$\}$ $the\ coset\ of\ I\ in\ R\ where\ a\ \in R$

a+I=b+I$\Leftrightarrow a - b \in I$

$\frac{R}{I}$= the collection of distinct cossets of I in R

$$= \{r + a\ r \in R\}$$

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

($\frac{R}{I}$,+) is abelian group

(a+I).(b+I) =(a.b+I)

(I,+,.) is an ideal

a.b-a1.b1=a(b-b1)+(a-a1).b1

a.b+I=a1.b1+I

Lemma : let R be commutative ring with identity and let I be a proper ideal in R then I semi prime iff 0 is the uniqness nilpotent element in $\frac{R}{I}$

Proof :

$\Longrightarrow let\ I\ be\ a\ semi\ prime\ ideal$

$let\ a + I \in \frac{R}{I}\ \ni a + I\ is\ nilpotent\ element$

$\exists n \in Z\ \ni\ (a + I)^n = I \Leftrightarrow a^n + I = I \Leftrightarrow a^n \in I\ \Leftrightarrow a \in \sqrt{I}$

$but\ I\ is\ semi\ prime\ \sqrt{I} = I$

a$\in I\ \Leftrightarrow a + I = I$

$\Leftarrow it\ is\ enough\ to\ prove\ that\ \sqrt{I} \subseteq I$

$let\ w\ \in \sqrt{I}\ \Longrightarrow \exists n \in Z\ \ni w^n \in I$

$w^n + I = I \Leftrightarrow (w+I)^n = I$

$(w+I)\quad = I$

$w \in I$

$\sqrt{I}\ \subseteq I$

$\sqrt{I} = I\ , I\ is\ semiprime$

Lemma : every prime ideal is semi prime

Proof : let I be a prime ideal in R we known that $I \subseteq \sqrt{I}$

So it enough to proof $\sqrt{I}\ \subseteq I$

Let w $\in$ $\sqrt{I}$ $\Longrightarrow$ $w^n \in I$ $\qquad for\ some\ n\ \in I$

We chose n the smallest no. satisfy this

Claim : n=1

If n>1

$I\ \ni w^n =\ w^{n-1}.w \qquad C!$

If $w^{n-1} = w.w^{n-2} \qquad C!$

For example w^2=w.w

n=1

W belong to I

$\sqrt{I} \subseteq I$, $I = \sqrt{I}$

I is semi prime

The converse is not true

Semi prime $\nrightarrow$ not prime

Theorem : if (I,+,.) is an ideal of (R,+,.) then ($\frac{R}{I}$,+,.) is a ring , known as the quotient ring of R by I

PROOF : H.M

Lemma : let R be commutative ring with identity and let I be a proper ideal in R then I semi prime iff 0 is the uniqness nilpotent element in $\frac{R}{I}$

Def : let R be commutative ring with identity and let I be an ideal in R ∋

1- $I \neq R$

2- If $\exists\ a, b \in R \ni a.b \in I$

Then $a \notin I$ then $b^n \in I$, for n belong to Z^+

If I satisfy 1 and 2 then I is called primary ideal

Remark : every prime ideal is primary .

Proof : let X,Y belong to R . there exist x.y belong to R

I is prime then $y = y^1$ belong to I n=1

Then I is primary

Lemma : let R be a commutative ring with identity and let I be a primary ideal in R then $\sqrt{I}$ is prime ideal in R and $\sqrt{I}$ is the smallest prime ideal contain I

Proof : let a,b $\in \sqrt{I}$

And suppose that $a \notin \sqrt{I}$

$\Leftrightarrow (a.b)^m$ belong to I for some $m \in Z^+$

$\Leftrightarrow a^m . b^m$ belong to I

$\because a^n \notin I \quad , \forall n \in Z$

$a^m \notin I$

and since I is primary

$\exists\ kZ \ni$

$(b^m)^k = b^{m.k} \in I$

$\therefore\ b \in \sqrt{I}$

$\sqrt{I}$ *is prime ideal*

Def : (primary ideal)المثالي الابتدائي

let R be commutative ring with identity and let I be an ideal in R ∋

3- I≠R

4- If $\exists\ a, b \in R \ni a.b \in I$

Then $a \notin I$ then $b^n \in I$, for n belong to Z^+

If I satisfy 1 and 2 then I is called primary ideal

Remark : every prime ideal is primary .

كل مثالي اولي هو مثالي ابتدائي

Proof : let X,Y belong to I . ∋ x.y belong to I , $x \notin I$

I is prime⟹ $y = y^1$ belong to I n=1

Then I is primary

Ex : $2,4 \notin 8Z \quad but\ 2.4 = 8 \in 8Z$

$\therefore 8Z\ is\ not\ prime$

Lemma : (مهمة)

Let R be a commutative ring with identity and let I be a primary ideal in R then $\sqrt{I}$ is prime ideal in R and $\sqrt{I}$ is the smallest prime ideal contain I

Proof :let a.b ∈ $\sqrt{I}$ and suppose that $a \notin \sqrt{I}$

$\Leftrightarrow (a.b)^m\ \in I\ for\ some\ m \in Z \quad \Leftrightarrow a^m b^m \in I$

$\because a^n \notin I \ \Longrightarrow a^m \notin I$ and since I is primary $(b^m)^k$=$b^{m.k} \in I$

$\therefore b \in \sqrt{I} \qquad \therefore \sqrt{I}\ is\ prime\ ideal$

Theorem: Let R be a commutative ring with identity and let I be a proper ideal in R then I is primary iff every zero divisor in $\frac{R}{I}$ is nilpotent

Proof : $\Longrightarrow let\ I\ ba\ a\ proper\ ideal\ which\ is\ primary\ and\ let\ x + I \in \frac{R}{I}$

$\therefore \exists y + I \in \frac{R}{I} \ni (y+I)(x+I) = I$

$\Leftrightarrow x.y \in I \quad but\ y \notin I \quad and\ I\ is\ primary\ \ni x^n \in I$

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

X+I is nilpotent

$\Longleftarrow let\ x.y \in I\ \ and\ y \notin I$

$(x+I)(y+I)=I \quad if\ x+I=I\ then\ I\ is\ primary$

$if\ x+I\neq I\ then\ x+I\ is\ nilpotent$

$x^n+I=I \quad \Leftrightarrow x^n\in I$

I is primary

Def : (Jacobson radical) ☹

Let R be a commutative ring with identity then set $J(R)=\cap\{M: Mis\ maximal\ ideal\ in\ R\}$ is called the Jacobson radical of R

Remark : 1- $J(R)\neq \emptyset$

2 - $J(R)$ is an ideal

EX : 1 – (Z_4,+,.) j(Z_4)={0,2}

2 - – (Z_6,+,.) j(z)={0} {0,2,4} {0,3} Z_6

REMARK: 1- $J(R)$ Is proper ideal always

2 -- $J(R)\neq R$ since if - $J(R)=R$

1∈R that mean 1∈ $J(R)$ C!

3 - J(Z) =∩ P

=2∩ 3 ∩ 5 ∩ … = {0}

Lemma : let R be a commutative ring with identity 1 and let I be an ideal in R then I ⊆ J(R) iff every element in 1+I has an inverse

Proof : ⟹ suppose that the statement is true

$\exists\ w \in 1 + I\ has\ no\ inverse$

$\Longrightarrow w = 1 + a$, where a$\in I$

$\therefore \exists\ maximal\ ideal\ M\ in\ R\ \ \ni w \in M$

$\therefore a \in I \subseteq J(R) \subseteq M \quad\quad \because a \in M$

Thus a,w belong to M i.e a, 1+a belong to M

$\Longrightarrow 1 \in M \quad C!$

Each element in 1+I has an inverse

$\Longleftarrow suppose\ I\ \nsubseteq J(R)$

$\because \exists x\ \in I\ and\ x \notin J(R)$

∃ maximal ideal M in R ∋ $x \notin M$

So (M,x)=R

1 belong to R   m∈ 1+I

m has an inverse   1=m.m^{-1} belong to M   C!

$\therefore I\ \subseteq J(R)$

Cor : $a \in J(R) \Longleftrightarrow$ the element 1+RA has an inverse $\forall\ r\ \in R$

Proof : take I=(a) , by last theorem $a \in (a) \subseteq J(a)$

$\Leftrightarrow$ every element in 1+(a) has an inverse

Lemma : the uniqness idempotent in J(R) is (0)

Proof : let a belong to R

$a=a^2$

$a=a^2=0$

a(a-1)=0

a-(1+(-1)a)=0

1+(-1)a has an inverse in R

$\therefore \exists\ b\epsilon R\ s.t\ \ (1+(-1)a).b=1$

0.b=a.1

0=a

Remark : the ideal I is called nil ideal if each element in I is nilpotent

Lemma : every nil ideal contains in J(R)

Lemma : $J\left(\frac{R}{J(R)}\right)=0$

Def : let R be a commutative ring with identity 1 the set

L(R) $=\cap \{P: P \text{ is prime ideal in } R\}$ is called prime radical for the ring R

Remark: : 1- $L(R) \neq \emptyset$

2 - $L(R) \subseteq J(R)$

Theorem : : let R be a commutative ring with identity 1 and let I be a proper ideal in R then $\sqrt{I} =\cap \{P: P \text{ is prime ideal contain } I\}$

Remark : $\sqrt{(0)} =\cap \{I, I \text{ is prime which contain } 0\}$ *the set of all nilpotent element*

Def : let $(R_1,+,.)$,$(R_2,+,.)$ are two rings then the function $f:R_1\to R_2$ is called ring homomorphism if the following satisfies :

1- f(a+b)=f(a)+f(b) ,$\forall$a,b$\in$R

5- f(a.b)=f(a).f(b) ,$\forall a, b \in R$

Theorem : let F : $R \to \acute{R}$ be epimorphism then :

1- If M is maximal in R contain kerf then f(M) is maximal in $\acute{R}$

2- *If* $\acute{M}$ *is maximal in* $\acute{R}$ *then* $f^{-1}(M)$ *is maximal in* R

3- *There is an isomorphism between the maximal ideal in* $\acute{R}$ *and the maximal ideals in* R which is contain kerf

Proof :