Poset : A poset is a reflexive, antisymmetric and transitive relation.

A poset is a set equipped with a partial order.

Or

We take a set S, and the partial order on S is a binary relation $\leq$ with the following properties

⇒ reflexivity : $x \leq x$ always

⇒ transitivity : If $x \leq y \leq z$, then $x \leq z$

⇒ Antisymmetry : If ~~$x \leq y \leq x$~~ $x \leq y \leq x$ then $x = y$.

Theorem:- Every non-zero ring has a maximal ideal.

proof:- let R be a non-zero ring and

put $\sum = \{ I \mid I \trianglelefteq R, I \neq R \}$.

Then $\sum$ is a poset with respect to $\subseteq$.

$\sum$ is non-empty since it contains the zero ideal.

let $C \subseteq \sum$ be a chain. If C is empty then we will set $K = \{0\}$

If C is non-empty then we will set

Let $K = \bigcup_{I \in C} \{ x \in R \mid x \in I \text{ for some } I \in C \}$

$\Rightarrow K \trianglelefteq R$

$\Rightarrow K \neq R$ because of we set

$K = R$ then one of the ideals of the chain would contain 1 and thus all of R

Now here we are getting contradiction since $\sum = \{I \mid I \triangle R, I \neq R\}$

does not contain R.

This implies $K \in \sum$ and K is an upper bound for C.

By Zorn's lemma, $\sum$ has a maximal element M which is precisely a maximal ideal of R.

Zorn lemma :- If $(S, \leq)$ is a partially ordered set such that every chain C in S has an upper bound in S then for every element x in S there is a maximal element y in S with $x \leq y$.

Local Ring :-

⇒ A local ring is a ring with exactly one maximal ideal.

Suppose A a ring A with exactly one maximal ideal m, then $K = \frac{A}{m}$ is called the ~~residue~~ residue field of A.

Example ① All fields are local rings since $\{0\}$ is the only maximal ideal in these rings.

② A similarly in skew field (division rings)

skew field are generally known as non-commutative ring in which every has a two sided inverse.

Example ~~Example~~ Example : Quaternion ring.

The ring $\frac{\mathbb{Z}}{p^n\mathbb{Z}}$ is a local ring for $n \geq 1$.

Here (p) is the only maximal ideal of $\mathbb{Z}/p^n\mathbb{Z}$

Proof:- let $I = (p)$ a non-zero prime ideal

$$\Rightarrow I^n = \langle p^n \rangle$$

If $I^n \subseteq J$ with J a prime ideal,

there exist a maximal ideal $J \subseteq K$

Hence $I^n \subseteq K$

Since K is a ~~maximal~~ maximal ideal

$\Rightarrow$ K is also prime ideal ~~such that~~ with

$p \in K$

Therefore ~~I~~ $K = I = (p)$

So the ~~only~~ only maximal (and prime) ideal

in $\frac{\mathbb{Z}}{p^n\mathbb{Z}}$ is (p)

let A be a ring and $m \neq (1)$ an ideal of A such that $x \in A - m$ is a unit in A. Then A is a local ring and m is maximal ideal.

Proof: Suppose A is a local ring with unique maximal ideal m. let $x \notin m$. Consd. i.e $x \in A - m$. consider the ideal (x). If ideal (x) is proper then it lies in some maximal ideal.

Since A is a local ring and we know that in local ring there is exactly one - maximal ideal so ideal (x) is lies in m, which is Contradiction.

Thus ~~Thus $(x) = A$ so~~ Thus $(x) = A$ so $1 = rx$ for some r where x is unit

Thus $(x) = A$, then $1 \in (x)$

$1 \in (x)$ so we can write

$1 = ax$ for some $a \in A$

this implies x is ~~unit~~ a unit.

Defination of unit :-

A a unit of ring R

is any element $u \in R$ that has

multiplicative inverse in R

i/e there exist an element $v \in R$ such that

$vu = uv = 1$ where 1 is the

multiplicative identity.

So every ideal $\neq (1)$ consist of non-units.

i.e contained in m.

Hence

Hence m is the only maximal ideal of A.

Q. If R is local ring with maximal ideal M, then every element of R-M is a unit

proof:- Suppose $x \in R-M$. If x is not a unit, then $(x) \neq R$

Now by using zorn lemma we can construct a maximal ideal M' containing (x) i.e $x \in M'$

Since R is a local ring $\Rightarrow$ so R has only one maximal ideal

$\Rightarrow M = M'$

But this leads to a contradiction

because $x \in M$

Therefore

Therefore every element of R-M is a unit.

Theorem :- let A be a ring and m a maximal ideal of A, such that every element of $1+m$ (i.e every $1+x$, where $x \in m$) is a unit in A. Then A is a local ring.

proof :- Given ring A. Take any $x \in A - m$

Then the ideal $(x) + m$ generated by x and m.

i.e $(x) + M = (1) = A$

Also, we can say the ideal generated by x and m is $A = (1)$

Here $(1) = (m, x)$

$= a$ (say).

Then there exist $y \in A$ and $t \in m$

such that $xy + t = 1. \in A$

~~Since $xy = 1 - t$~~

$\Rightarrow xy = 1 - t$

Since $m \in M$ implies $-m \in M$

i.e $t \in m$ implies $-t \in m$

Therefore $1 - t \in 1 + m$.

Since we have assume $1 + m$ as a unit in A

So xy is a unit.

$\Rightarrow xy = 1$ for some $y \in A$

$\Rightarrow x$ is unit.

Since $x \in A - m$

i.e $x \notin m$

unit $\notin m$

So m contain all the non-unit element of A

Now using the theorem a ring R with 1 is local if and only if the set of non-unit elements of R is an ~~ideal~~ ideal of R

$\Rightarrow$ A is a local Ring.

Semi-local ring:- A ring with only a finite number of maximals ideals is called semi-local.

Example:- $Z_{(p)} = \left\{ \frac{a}{b} \in \mathbb{Q} \text{ such that } p \nmid a, p \nmid b \right\}$

$Z_{(p)} = \left\{ \frac{a}{b} ; a, b \in \mathbb{Z}, p \nmid b \right\}$

$Z_{(p)}$ is semi-local ring because

$Z_{(p)}$ has unique maximal ideal

$$m = \left\{ \frac{a}{b} \in \mathbb{Q} \text{ s.t } p \mid a, p \nmid b \right\}$$

$$\frac{Z_{(p)}}{\langle m \rangle} \cong \mathbb{Z}/p$$

Irreducible element :-

Let R be a commutative ring with unity.

~~Ans~~ A non-zero, non-unit element $p \in R$ is called an irreducible element.

If $p = ab$ implies that either a or b is a unit $a, b \in R$.

Example $f(x) = x + 1$ or $f(x) = x \cdot = 1 \cdot x$

$= (1) \cdot (x+1)$ over $\mathbb{F}[x]$

Prime element :-

Let R be a commutative ring with unity. A non-zero, non-unit element $p \in R$ is called a prime element, if

$p \mid ab$ $(a, b \in R)$ implies that either $p \mid a$ or $p \mid b$

Example : 2 is prime element in $\mathbb{Z}$ but not in $\mathbb{Z}[i]$

$\Rightarrow 2 = (1+i)(1-i)$

but $(1+i) \nmid 2$ or $1-i \nmid 2$

$A = K[x_1, x_2, \ldots, x_n]$ K is a field.

let $f \in A$ be an irreducible polynomial.

Then by unique factorization, the ideal (f) is prime.

Proof:- An ideal I is prime if $xy \in I \Rightarrow x \in I$ or $y \in I$.

Now take two polynomials g, h and say $gh \in (f)$, $\Rightarrow f \mid h$ or $f \mid g$

$gh \in (f) \Rightarrow gh = kf$ where k is some polynomial.

$\Rightarrow$ fo

$\Rightarrow$ It is given that f is an irreducible polynomial so f is a irreducible element

$\Rightarrow$ Since irreducible polynomial are the irreducible element.

example of

Now by using the theorem :- If F be a field and $x_1, \ldots, x_n$ be indeterminates. Then the polynomial ring $F[x_1, \ldots, x_n]$ is U.F.D

From the theorem

$$A = K[x_1, x_2, \ldots, x_n] \text{ is U.F.D}$$

We know that in U.F.D, every irreducible element of R is prime.

Here f is irreducible element

so by unique factorization (UFD), the ideal (f) is prime

i.e we have $gh = kf$

$\Rightarrow f \mid g$ or $f \mid h$

take $f = 3$, $g = 3 \times 5$ / $h \neq$ /

$h = 3$, $g = k = 5$

$3 \times 5 = 5 \times 3 \Rightarrow g \cdot h = kf$

$3 \mid 3 \Rightarrow$

The ideal m of all polynomials in

$A = K[x_1, \ldots, x_n]$ with zero constant

term is maximal.

Here $m = \{ f \in K[x] \mid f(0) = 0 \}$

$\phi : K[x] \longrightarrow K$ defined by

$\phi(f) = f(0)$

$\phi(f(x)) = f(0)$

$$\frac{K[x]}{\langle m \rangle} \cong K$$

$f(0) = 0$ mean $f(x)$ contain x.

take $f = x$, then $x \in K$

$f(x) \in K[x]$

$\phi(f(x)) \longrightarrow f(0)$

$\phi(f(x)) \longrightarrow x$

$\Rightarrow$

Principal ideal :-

If ~~R~~ & be

let 'a' be any element of a commutative ring R. The smallest ideal of R which contain a is called the principal ideal generated by 'a'.

It is denoted by $\langle a \rangle$ or (a).

Theorem :- If R be a commutative ring and $a \in R$ then

$$(a) = \{ar + na : r \in R, n \in \mathbb{Z}\}.$$

or

$$(a) = \{ar : r \in R\} = aR$$

Since $ar + na = a(r+n)$

$= ar$

Since $r + n = r \in R$.

Example :- let $n \in \mathbb{Z}$. The principal ideal of $\mathbb{Z}$ generated by n is $(n) = n\mathbb{Z}$.

Theorem:- let R be a principal ideal domain. let P be a non-zero prime ideal in R. show that P is a maximal ideal in R.

proof:- A principal ideal domain in R is an integral domain in which every ideal P is the form

$$(a) = \{ar \mid r \in R\}.$$

i/e we can write $P = (a)$, an ideal generated by an element $a \in R$

Then $P = \langle a \rangle$ for some $a \neq 0$ in R

Suppose that P is not maximal. Then there is some proper ideal I such that P is properly contained in I.

i/e $P \subset I \subset R$ for some ideal

we can write $I = (b)$ for some $b \in R$

$P \subset I \subset R$

$\langle a \rangle \subset \langle b \rangle \subset R$

$\Rightarrow \quad a \in \langle b \rangle$

$\Rightarrow \quad a = bd$ for some $d \in R$ — (1)

$\therefore \quad bd \in P$

Since P is a prime ideal of the ~~prime~~ principal ideal domain R

Therefore either $b \in P$ or $d \in P$

But $b \notin P$ because if $b \in P$

then $I = (b) \subset P$

we have already assumed that $P \subset I$

$\therefore \quad P = I$ which is a contradiction because P is properly contained in I

So $b \in P$ is not possible

i.e $b \notin P$.

And $d \in P$ is possible.

$\Rightarrow d \in (a)$

$\Rightarrow d = ar$ for some $r \in R$ —(2)

From (1) and (2) we have

$a = bd = bar$

$a = bar$

$a - bar = 0$

$a(1 - br) = 0$

$1 - br = 0 \Rightarrow \boxed{br = 1}$

So b is a unit.

Now used the theorem :- let R be a ring. x is unit in R if and only if $(x) = R$

Theorem: Let R be a ring. x is a unit in R if and only if $(x) = R$

Proof: If x is a unit, then there is some $y \in R$ such that $xy = yx = 1$

Now for all $r \in R$, we can write

$$r = r \cdot 1 = r(yx) = (ry)x$$

since $r \in R$ and $y \in R$

so $(ry) \in R$

$$r = (ry)x = r \cdot 1 \in (x)$$

$$= r \in (x)$$

Therefore $(x) = R$.

Conversely, assume $(x) = R$, then $1 \in (x)$. In particular, $rx = 1$ for some $r \in R$

Therefore x is a unit

Thus by the given theorem we
Conclude that $(b) = \mathbb{R}$

i.e $\frac{\mathbb{R}}{I} = \frac{(b)}{I} = \mathbb{R}$

Hence, $P = (a)$ is maximal.

Theorem :- The Set $N = \{$ nilpotent elements of $A \}$ is an ideal and $\frac{A}{N}$ has no non-zero nilpotents.

proof :- Since $0 \in N$ so $N \neq \phi$

Let $x, y \in N$ and $x^m = 0$ and $y^n = 0$

Then $(x-y)^{n-m} = 0$ by binomial theorem

If $x^n = 0$, then $(rx)^n = 0$.

Thus N is an ideal.

Suppose $r + N \in \frac{A}{N}$ is nilpotent-

then $(r+N)^n = r^n + N = 0 + N$

for some positive integer n.

Hence $r^n \in N$ implies that $(r^n)^m = 0$

for some +ve integer m

Hence $r^{nm} = 0$ i.e $r \in N$

thus $\gamma + N = \delta + N$

so $\frac{A}{N}$ has no non-zero nilpotent elements

The ideal N is called nil of nilradical of A i.e $N = \{f \in R \mid f^m = 0 \text{ for some } m\}$

Theorem: The nilradical of A is the intersection of all the prime ideals of A.

proof: Suppose f is nilpotent and let P be a prime ideal

Also if $f \in N$ (nilradical of A), then $f^n = 0 \in P$ for some $n \in \mathbb{Z}^+$.

$\Rightarrow f^n = f \cdot f^{n-1} = 0 \in P$

Since P is prime ideal so $f \in P$ or $f^{n-1} \in P$.

$f^{n-1} \in P \Rightarrow f^m \in P$ for some $m \leq n-1$

then $f^m = f \cdot f^{m-1} \in P$

Thus $f \in P$ or $f^{m-1} \in P$

Now mathematical Induction on $m \geq 1$

We conclude that $f_1^m \in P$ for all $0 < m \leq n-1$.

in particular $f \in P$.

Therefore f is contained in any prime ideal

$$\Rightarrow N \subseteq \bigcap_{P \not\subseteq R} P$$

$$\Rightarrow \not\exists \; (f \in N \Rightarrow f \in \bigcap_{P \not\subseteq R} P$$

Jacobson radical :-

The Jacobson radical $J(R)$ of a ring R is the intersection of the maximal ideals of R.

Since all maximal ideals are prime, the nilradical is contained in the Jacobson radical.

Theorem :- Let $x \in R$. Then x lies in the Jacobson radical $J(R)$ of R if and only if $1 - xy$ is a unit for all $y \in R$.

proof :- Let x be in $J(R)$. Suppose $1 - xy$ is a non-unit for some $y \in R$. Then $1 - xy \in M$ for some maximal ideal M.

Since I the ideal generated by $1 - xy$ and $I \neq R$, as ring is commutative with identity, each proper ideal is contained in a maximal ideal.

So let $I \subseteq M \Rightarrow 1 - xy \in M$.

Here M is the ideal of R and

if also we have $x \in R$ which

is like x in the Jacobson radical

$J(R)$ of R. $\Rightarrow$ $x \in M$

So Thus, for all $x \in M$ and $y \in R$,

we have $xy \in M$.

Now $1 - xy \in M$ and $xy \in M$

we know that ideal is closed under

addition

$$(1 - xy) + xy \in M$$

$$1 \in M$$

$\Rightarrow$ 1 is in M, a contradiction because

$$1 \notin M$$

if $1 \in M \Rightarrow M = R$

By using this theorem:- Let R be a ring with identity, and I be an ideal of R

If $1 \in I$, then $I = R$.

proof: Since I is an ideal containing 1, if $r \in R$ then

$$r = r \cdot 1 \in I$$

It follow that $R \subseteq I$

and $I \subseteq R$ is trivial ~~as~~ i.e this inclusion is trivial.

Therefore $I = R$

Universal property of LCM :-

$\Rightarrow$ $x_1\mathbb{Z} \cap \dots \cap x_n\mathbb{Z}$

$= Lcm(x_1, \dots, x_n)\mathbb{Z}$

proof : $a \in x_1\mathbb{Z} \cap \dots \cap x_n\mathbb{Z}$

$\Rightarrow x_1, x_2, \dots, x_n \mid a$

$Lcm(x_1, \dots, x_n) \mid a$

$\Rightarrow$ ~~$a \in Ka \in$~~ $a \in K\mathbb{Z}$

where $K = Lcm(x_1, \dots x_n)$

Bezout's identity : let a and b be integers or polynomials with greatest common divisor d.

Then there exist integer or polynomial x and y such that $ax + by = d$.

$\therefore ax + by = gcd(a, b)$

$a = (m)$, $b = (n)$

$\Rightarrow$ $a + b$ $a \cap b$ is the ideal generated by $\text{Lcm}(a,b)$.

$(ab) = (mn)$

If $nz + mz = dz$, then d is a greatest common divisor of n and m.

proof let $nz \subseteq mz \iff m \mid n$.

$nz, mz \subset \gcd(m,n)z$

$\iff \gcd(m,n) \mid m,n$

$\gcd(m,n)z \iff$

If $mz, nz \subseteq rz$, then

$\gcd(m,n)z \iff r \mid m,n$

$r \mid \gcd(m,n)$

By using Bezout theorem

$r \mid m, n \Rightarrow r \mid an + bm$

$r \mid \gcd(m, n)$ for some $a, b \in \mathbb{Z}$

~~$(ab) \neq a \cap b$~~

$ab \neq a \cap b$

Take $a = b = 2\mathbb{Z}$

~~$ab \subseteq a \cap b$~~ $ab \subseteq a \cap b$

let R be a commutative ring with unity.

let a, b be ideals.

$ab \subseteq aR \subseteq a$

$ab \subseteq Rb \subseteq b$

Therefore $\boxed{ab \subseteq a \cap b}$.

Theorem :- Let A be a commutative ring with unity

Let $a, b \subseteq A$ be co-prime ideals.

Then product equal to their Intersection

$$ab = a \cap b.$$

Proof: $ab \subseteq aA \subseteq a$

$ab \subseteq bA \subseteq b$

~~$ab \subseteq a \cap B$~~ $ab \subseteq a \cap b$

Now we have to show ~~that~~ that

$$\boxed{a \cap b \subseteq ab} \quad \text{---(1)}$$

Let $c \in a \cap b$

$\gcd(a,b) = 1$, so by Bezout theorem,

there exist $x \in a$, $y \in b$ such

$$x + y = 1.$$

$c \in a \cap b$

$\Rightarrow c \in a, b$

and $x \in a, y \in b$.

$c = cx + cy$.

Therefore

we have $c \in$ ~~$a \cdot b$~~ ab

$c \in ab$

$\Rightarrow \boxed{a \cap b \subseteq ab.}$ — (ii)

From (1) and (2), we have

$$\boxed{ab = a \cap b}$$

Let A be a ring and $a_1, a_2, \ldots a_n$ ideals of A. Define a homomorphism

$$\phi : A \longrightarrow \prod_{i=1}^{n} (A/a_i)$$ by the rule $\phi(x) = (x + a_1, \ldots, x + a_n)$

① If a_i, a_j are coprime whenever $i \neq j$

then $\prod a_i = \bigcap a_i$

Sol^n: We will induct on n, the numbers of ideals when $n = 2$, the argument is ~~handleabove~~. easily verified. or when $n = 2$ the argument is handled above.

Suppose we have $a_1, a_2, \ldots a_n$ and the result is true for any set of $n-1$ ideals.

let us assumpt $b = \prod_{i=1}^{n-1} a_i = \bigcap_{i=1}^{n-1} a_i$

Since a_i, a_j are coprime so

$a_i + a_n = 1$ (by Bezout lemma)

for $1 \le i \le n-1$.

(By ~~Bezout lemma~~), ~~we have~~

Theorem :- Let (m) and (n) be ideal of the integer $\mathbb{Z}$

Let $d = (m) + (n)$

Then $d = \gcd(m,n)$

i/e $(d) = (m) + (n) = \{ x \in \mathbb{Z} : \exists\, a,b \in \mathbb{Z} : x = am + bn \}$

Now we have equation $x_i + y_i = 1$

where $x_i \in a_i$, $y_i \in a_n$)

$\Rightarrow x_i = 1 - y_i$

Therefore $\prod_{i=1}^{n-1} x_i = \prod_{i=1}^{n-1} (1 - y_i)$

Since $y_i \in a_n$

$$\Rightarrow y_i \equiv 0 \pmod{a_n}$$

So $\prod_{i=1}^{n-1} x_i = \prod_{i=1}^{n-1} (1 - y_i) \equiv 1 \pmod{a_n}$

Hence $an + b = (1)$ so they are co-prime.

Therefore $\prod_{i=1}^{n} a_i = \prod_{i=1}^{n-1} a_i \; a_n.$

$$= b \; a_n$$

$$= b \cap a_n.$$

$$\prod_{i=1}^{n} a_i = \bigcap_{i=1}^{n} a_n.$$

If a, b are two ideals in a ring A, their quotient is

$$(a : b) = \{ x \in A : xb \subseteq a \}.$$

which is an ideal. Example :- $A = \mathbb{Z}$

$(6\mathbb{Z} : 8\mathbb{Z}) = 3\mathbb{Z}$

(*) $(0 : b)$ is called the annihilator of b and is also denoted by $\mathrm{Ann}(b)$

$\mathrm{Ann}(b)$ is the set of all $x \in A$ such that $xb = 0$.

If b is a principal ideal (x), we shall write $(a : x)$ in place of $(a : (x))$

Note :- In a ring R, a non-zero element $a \in R$ is said to be a zero divisor if there exist a non-zero $b \in R$ such that

$$a \cdot b = 0$$

we know that $Ann(b)$ is the set of all $x \in A$ such that $x.b = 0$

The set of all zero-divisor in A is denoted by

$$D = \bigcup_{x \neq 0} Ann(x)$$

Let I be ideal of R

$$(0 : I) = \{ r \in R \mid rI = (0) \}$$ is called the Annihilator of I or $Ann(I)$

Example :- $R = \frac{\mathbb{Z}}{48\mathbb{Z}}$

$$(0 : 4\mathbb{Z}) = 12\mathbb{Z}$$

$$(0 : \bar{I}) = (\{0\} : I) = \{ x \in R \mid rI = \{0\} \}$$

Theorem :- Let $A = \mathbb{Z}$, $a = (m)$, $b = (n)$

where

$$m = 2^{x_2} 3^{x_3} 5^{x_5} \cdots$$

$$n = 2^{y_2} 3^{y_3} 5^{y_5} \cdots$$

$$(a:b) = \{ r \mid rb \subseteq a \}$$

$\Rightarrow$ Then $(a:b)$ is the set of all numbers which when multiplied with n give a multiple of m.

$$\boxed{(a:b) = (q)}$$ where

$$q = 2^{z_2} 3^{z_3} 5^{z_5} \cdots$$

and $z_k = \max(x_k - y_k, 0)$

or we can write

$$(a : b) = (q)$$

$$= \frac{m}{\gcd(m,n)}$$

Example :- Take $a = m\mathbb{Z}$

$b = n\mathbb{Z}$

$$(m\mathbb{Z}, n\mathbb{Z}) = \frac{m}{\gcd(m,n)}\mathbb{Z}$$

$$(6\mathbb{Z} : 8\mathbb{Z}) = \frac{6}{\gcd(6,8)}\mathbb{Z}$$

$$= 3\mathbb{Z}$$

(i) $a \subseteq (a:b)$

(ii) $(a:b)\,b \subseteq a$

(iii) $((a:b):c) = (a:bc)$

$= ((a:c):b)$

(iv) $(\cap_i a_i : b) = \cap_i (a_i : b)$

(v) $(a : \sum_i b_i) = \cap_i (a : b_i)$

If a is any ideal of A, then the radical of a is

$$r(a) = \{x \in A : x^n \in a \text{ for some } n > 0\}$$

Natural projection :-

If H is a normal subgroup of a group G, then the mapping

$$\varphi : G \longrightarrow \frac{G}{H} \quad \text{where } \varphi(x) = xH \text{ for all } x \in G$$

$$: x \longrightarrow xH.$$ is a onto homomorphism.

$$\varphi(xy) = xyH = xH \cdot yH$$
$$= \varphi(x)\varphi(y)$$

The identity element of the factor group $\frac{G}{H}$ is the coset $eH = H$

$$\ker(\varphi) = \{x \in G : \varphi(x) = H\}.$$

$$= \{x \in G : xH = H\}$$

$$= H$$

The mapping φ is called natural projection.

~~let I be~~

let I be an ideal of a ring R.

$\varphi : R \longrightarrow \frac{R}{I}$ is defined by

$$r \longmapsto r + I$$

Here $\ker(\varphi) = I$

Let R be a ring, and I be an ideal

$$rad(I) = \{ r \in R \mid r^k \in I \text{ for some } k \in \mathbb{N} \}$$

Let P be a prime ideal containing I.
If $r \in R$ is such that $r^k \in I$, then
$r^k \in P$, so $r \in P$ since P is prime.

Therefore $rad(I) \subseteq \bigcap_{I \subseteq P} P$

Note: The radical of an ideal I in a commutative ring R, denoted by $rad(I)$ or $\sqrt{I}$, is defined as

$$\sqrt{I} = \{ r \in R \mid r^n \in I \text{ for some } n \in \mathbb{Z}^+ \}$$

Theorem : $r(I)$ is an ideal of A for any ideal I in A.

proof :- let I be any ideal in the ring A, and let $\phi : A \longrightarrow A/I$ be natural map defined by

$$\phi(x) = x + I$$

let $n_{A/I}$ be the nilradical of A. Then

$\phi^{-1}(n_{A/I})$ is an ideal of A

where

$$\phi^{-1}(n_{A/I}) = \{ x \in A \mid \phi(x) \in n_{A/I} \}$$

$$= \{ x \in A \mid x + I \in n_{A/I} \}$$

$$= \{ x \in A \mid (x+I)^n = I \text{ for some } n > 0 \}$$

$$= \{ x \in A \mid x^n + I = I \text{ for some } n > 0 \}$$

$$= \{ x \in A \mid x^n \in I \text{ for some } n > 0 \}$$

$$= \gamma(I)$$

$$= \{ x \in A \mid x + I \text{ is nilpotent in } A/I \}$$

$$\phi^{-1}(n_{A/I}) = \gamma(I)$$

$$\Rightarrow \phi(\gamma(I)) = n_{A/I}$$

$\Rightarrow$ Also, ϕ is natural map

$$\phi(\gamma(I)) = \gamma(I) + I \subseteq n_{A/I}$$

$$\text{or } \gamma(I) \subseteq n_{A/I}$$

Here $n_{A/I}$ is nilradical of A

$\Downarrow$

Intersection of all the prime ideal of A.

Theorem :- $\gamma((x)) = (\bar{x})$ where

$x = p_1^{\alpha} \cdots p_n^{\alpha_n}$ and $\bar{x} = p_1 \cdots p_n$

Proof :- let $\alpha = \max(\alpha_1, \alpha_2, \ldots, \alpha_n)$.

Then we have

$$\bar{x}^{\alpha} = (p_1 \cdots p_n)^{\alpha}$$

$$= p_1^{\alpha} \cdots p_n^{\alpha}$$

$$= p_1^{\alpha - \alpha_1} \cdots p_n^{\alpha - \alpha_n} \; p_1^{\alpha_1} \cdots p_n^{\alpha_n}$$

$\because$

let $y = p_1^{\alpha - \alpha_1} \cdots p_n^{\alpha - \alpha_n}$.

Then $\bar{x}^{\alpha} = y \cdot p_1^{\alpha_1} \cdots p_n^{\alpha_n}$.

$$\bar{x}^{\alpha} = y \cdot x$$

$\Rightarrow \bar{x}^{\alpha} \in (x)$ — (1)

Assume that $y \in r((x))$

and $y \neq 0$.

$y \in r((x)) \Rightarrow y^n \in (x)$ for some $n \in \mathbb{N}$.

$\Rightarrow x$ divides y^n i.e $x \mid y^n$

Also, $P_i \mid x$ for any $i \in \{1, \ldots n\}$.

$P_i \mid y^n$

$P_i \mid y$.

Now for $i \neq j$ element P_i and P_j are

Coprime, so $\overline{x} \mid y$

$y \in (\overline{x})$ — (2)

From (1) and (2), we conclude that

$$r((x)) = (\overline{x})$$

Example :- Take $R = \mathbb{Z}$, $r = (12)$

Then $\gamma((12)) = (2.3) = (6)$

$$12 = 4.3 = 2^2.3$$

i.e $\gamma(12) = (6) = \{0, \pm 6, \pm 12, \pm 18 \cdots\}$

Note :-

Let $(r, +, \cdot)$ be an ideal of the ring $(R, +, \cdot)$. Then the radical of the ideal of ideal r denoted by $\sqrt{r}$

$$\sqrt{r} = \{r \in R : r^n \in I, \text{ for some } n \in \mathbb{N}\}$$

Prove that

$$r(I) = \bigcap_{i=1}^{r} P_i \mathbb{Z}$$

proof: let $A = \mathbb{Z}$ and $I = m\mathbb{Z}$ where $m \neq 2$.

write $m = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ for distinct primes $p_1, \cdots p_r$ and positive integer $\alpha_1, \cdots \alpha_r$

Observe that

Now, take $\beta = \max\{\alpha_1, \cdots, \alpha_r\}$

$$(p_1 \cdots p_r)^{\beta} \in I$$

By the definition of radical

$$p_1 \cdots p_r \in r(I)$$

$p_1 \ldots p_r \mathbb{Z} \subseteq \gamma(I)$ — (1)

Now take $y \in \gamma(I)$

By defination of radical

$y^k \in I$ for some $k \in \mathbb{N}$

$y^k \Rightarrow m \mid y^k$, p

$p_i \mid m \Rightarrow p_i \mid y^k$ for $i = 1, 2, \ldots n$

$p_i \mid y$

$y \in I$

$y \in \gamma(I) \Rightarrow y \in I$

$\gamma(I) \subseteq I$

$\gamma(I) \subseteq p_1 \ldots p_r \mathbb{Z}$ — (2)

From (1) and (2), we have

$$\gamma(I) = P_1 \dots P_r \mathbb{Z}$$

$$\gamma(I) = \bigcap_{i=1}^{\gamma} P_i \mathbb{Z}$$

By the theorem of ideal I, J are co-prime, then $\boxed{IJ = I \cap J.}$

For coprime $x_1, x_2 \dots x_n \in R$

we have $\boxed{(x_1 \dots x_n) = (x_1) \cap \dots \cap (x_n)}$

Note :- $\gamma(I) = \phi^{-1}(N_{A/I})$

$$= \phi^{-1}\left(\bigcap_{\text{prime ideal } P \supseteq I} P/I\right)$$

$$= \bigcap_{\text{prime ideal } I \subseteq P} \phi^{-1}(P/I)$$

$$= \bigcap_{\text{prime ideal } I \subseteq P} P$$

$$\boxed{\gamma(I) = \bigcap_{\text{prime ideal } I \subseteq P} P}$$

Also, any prime ideal of A/I has the form P/I where P is a prime ideal of A containing I.

Note: In the ring $\mathbb{Z}/4\mathbb{Z}$, the residue class $\bar{2}$ is a zero divisor since $\bar{2} \times \bar{2} = \bar{4} = 0$

Let R be a ring.

Theorem: The set of zero-divisors of R is equal to its radical $\bigcup_{x \neq 0} \sqrt{Ann\, x}$.

Proof: Let D be the set of zero-divisor of R

$$Ann(x) = (0 : x)$$

$$= \{ y \in A : yx \subseteq 0 \}$$

From the theorem if a is any ideal of R,

Then $\boxed{a \subseteq r(a)}$ — (1)

from (1), we have

$D \subseteq r(D)$. Suppose $y \in r(D)$.

Then $y^k \in D$ for some $k \geq 1$, hence

$y^k x = 0$ for some non-zero $x \in R$.

If $k = 1$, then $y \in D$ and if $k \neq 1$, then

$y(y^{k-1} x) = 0$ implies $y \in D$

where $y^{k-1} x \neq 0$