Certain Types of Ideals

Definition. Let R be ring and I be an ideal of R, then I is said to be ***maximal ideal*** of R if it satisfy the following conditions:

1. $I \neq R$ (I is a proper ideal of R, $I \subsetneq R$)
2. If J is an ideal of R such that $J \supsetneq I$, then $J = R$.

Example.

1. $3\mathbb{Z}$ is a maximal of $\mathbb{Z}$.
   Proof. let N be an ideal of $\mathbb{Z}$ such that $N \supsetneq 3\mathbb{Z}$. $\longrightarrow \exists\, m \in N$, $m \notin 3\mathbb{Z}$ with $\gcd(m, 3) = 1$. Let $s, t \in \mathbb{Z}$ such that $ms + 3t = 1$ $\longrightarrow 1 \in N \longrightarrow N = \mathbb{Z}$.
2. $4\mathbb{Z}$ is not maximal of $\mathbb{Z}$. ($4\mathbb{Z} \subsetneq 2\mathbb{Z} \subsetneq \mathbb{Z}$)

Question.

Find the maximal ideals of $\mathbb{Z}_6$ and $\mathbb{Z}_{12}$?

Theorem. let n be a positive integer, then: $<n>$ (the ideal generated by n) is maximal iff n is prime.

Proof. $\Longrightarrow$) suppose n is not prime and $<n>$ is maximal ideal of R.

$\longrightarrow n = p_1p_2$ (p_1 and p_2 are prime ideals of R).

$\longrightarrow <n> \subset <p_1> \subset \mathbb{Z} \longrightarrow <n>$ is not maximal ideal of $\mathbb{Z}$ C!

$\therefore$ n is prime number

$\Longleftarrow$) suppose that n is prime and there is an ideal $I \subsetneq \mathbb{Z}$ such that $<n> \subset I \longrightarrow \exists\, m \in I$ such that $m \notin <n> \longrightarrow \gcd(m, n) = 1$ (n prime)

$\exists\, s, t \in \mathbb{Z}$ such that $sm + tn = 1 \longrightarrow m \in I \longrightarrow 1 \in I \longrightarrow I = R$.

$\therefore <n>$ is maximal ideal of R

<u>Theorem</u>. Let I be a proper ideal of a ring R, then I is maximal iff <I, a> = R for all a ∈ R-I.

Proof. (I, a) = {i + ra |i ∈ I and r ∈ R}

⟹) Suppose that I is a maximal ideal and a ∈ R and a ∉ I. since I ⊊ <I, a> ⊆ R and by hypothesis I is a maximal ideal ⟶ <I, a >= R (by definition of maximal ideal)

⟸) Suppose that for all a∈ R and a ∉ I, <I, a> = R. Suppose that I ⊊ J ⊊ R ⟶ ∃ x ∈ J and x ∉ I ⟶ <I, x> = R (by hypotheses)

But <I, x> ⊊ R ⟶ R ⊆ J ⟶ J = R

∴ I is maximal ideal

<u>Remark</u>. the maximal ideal of a ring R is not necessary unique.

<u>Example</u>. The ideals <2>, <3>, <5>, … of the ring ℤ are maximal ideals.

<u>Zorn's lemma</u>. If (S, ≤) is a partially ordered set with the property that every chain in S has an upper bound in S, then S possesses at least one maximal element.

Theorem. In a commutative ring with identity, each proper ideal is contained in a maximal ideal.

Proof. Let I be any proper ideal of R with r is commutative ring with identity 1.

Define a family a family of ideals of R by

F= {J| I ⊆ J, J is a proper ideal of R}

F ≠ ϕ (I ∈ F)

Let $\{J_i\}_{i\in\Lambda}$ be an arbitrary chain of ideals in F and a, b ∈ $\bigcup_{i\in\Lambda} J_i$,
r ∈R. ∃ j and k indexes for which a ∈ J_i, b ∈ J_k.

⟶ we have a chain: either $J_i \subseteq J_k$ or $J_k \subseteq J_i$.

Suppose that $J_i \subseteq J_k$ ⟶ a, b ∈ J_k but J_k ideal

⟶ a-b ∈ $J_k \subseteq \bigcup_{i\in\Lambda} J_i$ …..(1)

and ar, ra ∈ $J_k \subseteq \bigcup_{i\in\Lambda} J_i$ …(2)

by (1) and (2) $\bigcup_{i\in\Lambda} J_i$ is an ideal of R

1 ∉ $\bigcup_{i\in\Lambda} J_i$ (if not ∃ k indexes such that 1 ∈ J_k C! since J_k is proper)
→ $\bigcup_{i\in\Lambda} J_i$ is proper ideal of R and I⊆ $\bigcup_{i\in\Lambda} J_i$ ∈ F.

By Zorn's lemma , F has maximal element M ⟶ M is proper ideal of R with I ⊆ M. now, to prove M is maximal ideal : suppose ∃ J ⊆R such that M ⊂ J ⊆ R. Since M is maximal element of F. then J ∉ F.

⟶ J is improper ⟶ J = R ⟶ M is maximal ideal.

<u>Remarks</u>.

1. Let R be finitely generated ring. Then every proper ideal of R contained in a maximal ideal.
2. An element in a commutative ring with identity is invertible iff it belongs to no maximal ideal of R.
3. Example : the maximal ideals of $\mathbb{Z}_6$ are $\{\bar{0}, \overline{2, 4}\}$ and $\{\bar{0}, \bar{3}\}$. So $\bar{5}$ is an invertible element in $\mathbb{Z}_6$.
4. The element $\bar{0}$ in $\mathbb{Z}_4$ is not invertible (why?)
5. The only maximal ideal in any field F is <0>
   Proof. Suppose that F field.
   ⟶ for all 0≠ a ∈ F has inverse ⟶ a ∉ I for a maximal ideal I

⟶ I proper ideal. But F is field, hence the only ideals of R are {0} and F ⟶ I = {0} is the only maximal ideal of R.

6. If R is a commutative ring with identity and has only one maximal ideal, then R is said to be ***local ring***.
7. If a ring R have exactly one maximal ideal I, then the idempotent elements in R only 0 and 1.
   Proof. Suppose that R has only one maximal ideal (say I) and a an idempotent element in I such that a ≠ 0, 1.
   ⟶ $a^2 = a$ ⟶ a^2-a = 0 ⟶ a(a-1) = 0. Since a ≠ 0, 1 ⟶ a-1 ≠ 0 then a and a-1 are zero divisors.
   ⟶ Neither a nor a-1 invertible element(by: every zero divisor is not invertible) ⟶ a and a-1 ∈ I(I maximal)
   ⟶ a – (a-1) = 1 ∈ I(I ideal)
   ⟶ I = R C! (I maximal) ⟶ a = 0 and 1
8. The converse of (6) is not true in general: the only idempotent in the ring (ℤ,+, .) is 0, 1 but (ℤ, +, .) has an infinitely maximal ideal.
9. The ring $\mathbb{Z}_4$ is local ring while $\mathbb{Z}_6$ and ℤ are not.
10. Let R be a commutative ring with identity and I be a proper ideal of R, then I is a maximal ideal iff the quotient ring $\frac{R}{I}$ is field.

<u>Definition</u>. Let R be a commutative ring with identity. The set

$$Rad(R) = \cap\{M |\ M \text{ is maximal ideal of } R\}$$

is called ***Jacobson radical*** of a ring R.

<u>Remarks</u>.

1. If Rad(R) = {0}, then R is said to be ring without radical.
2. Rad(R) ≠ ∅.
3. Rad(R) is an ideal.

4. Rad(R) is always exist (since any commutative ring with identity contains at least one maximal ideal).

Examples.

1. $\text{Rad}(\mathbb{Z}_4) = \{\bar{0}, \bar{2}\}$
2. $\text{Rad}(\mathbb{Z}_6) = \{\bar{0}\}$
3. $\text{Rad}(\mathbb{Z}_p) = \{\bar{0}\}$
4. $\text{Rad}(\mathbb{Z}) = \cap \{<p> | \text{ p is prime number}\}$
   $= \{\bar{0}\}$

Remarks.

1. Rad(R) is proper ideal of a ring R(if not: 1 ∈ R= Rad(R) ⟶ 1 ∈ maximal ideal C!)
2. Let R be a commutative ring with identity 1 and I be an ideal of R. Then I ⊆ Rad(R) if and only if each element in 1+I has invertible in R.
3. Let R is commutative ring with identity 1, then a ∈ Rad(R) if and only if the element 1-ra invertible for each r ∈ R.
4. In a commutative ring with identity 1, the only idempotent element in Rad(R) is 0.
   Proof. Let a ∈ Rad(R) with $a^2 = a \longrightarrow a^2 - a = a(a - 1) = 0$
   ⟶ 1- a invertible element ⟶ ∃ b ∈ R such that (1 - a)b = 1
   ⟶a= a(1-a)b = 0 . b ⟶ a = 0.
5. Every nil ideal of R is contained in Rad(R).

Definition. Let R be a ring and P be an ideal of R. Then P is said to be ***prime ideal*** of R if whenever a.b ∈ I, either a ∈ I or b ∈ I for a, b ∈ R.

Examples.

1. $5\mathbb{Z}$ is prime ideal of $\mathbb{Z}$.
2. $4\mathbb{Z}$ is not prime ideal of $\mathbb{Z}$(since $2.2 = 4 \in 4\mathbb{Z}$ while $2 \notin 4\mathbb{Z}$)
3. $6\mathbb{Z}$ is not prime ideal of $\mathbb{Z}$(why?)
4. In $\mathbb{Z}_6$, the prime ideals are $\{\bar{0}, \bar{3}\}$ and $\{\bar{0}, \bar{2}, \bar{4}\}$

H.W. Find the prime ideals in $\mathbb{Z}$ and $\mathbb{Z}_{12}$?

Q / Is the zero ideal prime in any ring?

The answer of Q depends on the type of the ring. For example:

1. In $\mathbb{Z}_6$, the <0> ideal is not prime. Since if $x = \bar{2}$ and $y = \bar{3}$ then x.y = 0 ∈ <0> while neither x nor y ∈ <0>
2. By the same way, in $\mathbb{Z}_4$, the <0> ideal is not prime.
3. In $\mathbb{Z}$, the <0> ideal is prime(since if a.b = 0, either a ∈ <0> or b∈ <0>)
4. In $\mathbb{Z}_p$(p is prime), the <0> ideal is prime(since $\mathbb{Z}_p$ has nonzero divisor)

The following theorem answers about the above question:

Theorem. The zero ideal (0) is a prime in a commutative ring with identity R if and only if R is an integral domain.

Proof. ⟹) Let a, b ∈ R such that a.b = 0 with $a \neq 0 \rightarrow a \notin (0)$.

But (0) is prime ideal and a.b. = 0 ∈ (0) → b ∈ (0) → b = 0

→ a is not zero divisor element → R has no nonzero divisor element.

Since R is commutative ring with identity1→ R is an integral domain.

⟸) Suppose that R is an integral domain and a, b ∈ R such that a, b ∈ (0) → a.b = 0. If a ∉ (0) → a ≠ 0. Since R is an integral domain, then b = 0 → b ∈ (0) → (0) is prime ideal.

Theorem. The prime ideals in ℤ are only (0) and (p)(p is prime number).

Proof. Since ℤ is an integral domain, then (0) is prime ideal in ℤ. Now, let p be a prime integers and n, m ∈ ℤ such that n.m ∈ (p)

→ n.m. = rp → p\ n.m → p\n or p\m

→ either n = r_1p → n ∈ (p)

Or m = r_2p → m ∈ (p)

∴ (p) is prime ideal

Example. The ring ℤ x ℤ = {(n,m)| n, m ∈ ℤ}. Let p = ℤ x {0} is an ideal in ℤ x ℤ. Then (p) is prime ideal in the ring ℤ x ℤ.

Proof. let (n_1, m_1), (n_2, m_2) ∈ ℤ x ℤ such that (n_1, m_1).(n_2, m_2) = (n_1.n_1, m_1.m_2) ∈ ℤ x {0} → m_1.m_2 = 0 → either m_1 = 0 or m_2 = 0(because (0) is prime ideal in ℤ) → either (n_1, m_1) ∈ ℤ x {0} or (n_2, m_2) ∈ ℤ x {0}→ ℤ x {0} is prime ideal.

Theorem. In a commutative ring with identity 1, every maximal ideal is a prime.

Proof. let M be a maximal ideal in a ring R and a.b ∈ R such that a.b∈ M with a ∉ M. Now, a ∈ R and a ∉ M with M is maximal ideal, then (M, a) = R → 1 ∈ (M, a) → 1 = m + ra → b = mb + rab ∈ M

→ b ∈ M → M is a prime ideal in R.

Remark. Maximal ideal $\rightarrow$ prime ideal

The converse of the previous theorem is not true in general. For example:

The ring $\mathbb{Z} \times \mathbb{Z} = \{(n,m) | n, m \in \mathbb{Z}\}$. Let $p = \mathbb{Z} \times \{0\}$ is an ideal in $\mathbb{Z} \times \mathbb{Z}$. Then (p) is prime ideal in the ring $\mathbb{Z} \times \mathbb{Z}$ (because , $\exists\ \mathbb{Z} \times 2\mathbb{Z} \subsetneq \mathbb{Z} \times \mathbb{Z}$ such that $\mathbb{Z} \times \{0\} \subsetneq \mathbb{Z} \times 2\mathbb{Z} \subseteq \mathbb{Z} \times \mathbb{Z}$).

Q/ fined another example about: prime ideal $\nrightarrow$ maximal ideal.

Theorem. Let R be a commutative ring with 1. Let P be a proper ideal of R. Then P is prime ideal if and only if $\frac{R}{P}$ is an integral domain.

Proof. $\Longrightarrow$) since R is commutative ring with identity 1. So, $\frac{R}{P}$ is commutative ring with identity 1+P. Suppose that $\frac{R}{P}$ is not integral domain. i.e $\frac{R}{P}$ has zero divisor. Let a+P and b+P $\in \frac{R}{P}$ such that

$(a+P) \neq P$ and $(b+P) \neq P$ with $(a+P)(b+P) = P$

$\rightarrow (a+P)(b+P) = ab + P = P \rightarrow ab \in P$ since P is prime ideal

$\rightarrow$ either $a \in P \rightarrow a+P = P$ C! or $b \in P \rightarrow b+P = P$ C!

$\frac{R}{P}$ has no zero divisors $\rightarrow \frac{R}{P}$ is an integral domain.

$\Longleftarrow$) Let a, b $\in$ R such that $a.b \in P$ and $a \notin P$. If $a.b \in P \rightarrow ab + P = P$.
$\rightarrow (a+P)(b+P) = P$ but $a \notin P \rightarrow a+P \neq P$ and $\frac{R}{P}$ is an integral domain
$\rightarrow b+P = P$ ($\frac{R}{P}$ has no zero divisor) $\rightarrow b \in P \rightarrow$ P is prime ideal.

Remark. From the theorem(every maximal ideal is prime but the converse is not true in general) the following theorem give the condition under which the converse is true.

Theorem. Let R be a principal ideal domain. A non trivial ideal P is prime if and only if P is maximal ideal.

Proof. ⇒) H.W.

⇐) Let $0 \neq M$ be a prime ideal of PID R. Suppose $\exists\, N \subseteq R$ is an ideal of R such that $M \subsetneq N$. Since N is PID → N = (a) and M = (b) for some a, b ∈ R.

Now, $b \in M \subsetneq N \rightarrow b \in N \rightarrow b = ta$ for some $t \in R$. Since M is prime ideal and $b = ta \in M$.

→ either $t \in M = (b) \rightarrow t = sb$ for some $s \in R$

→ $b = sba = bsa \rightarrow 1 = sa$ (by cancellation law)

= as (R is commutative ring)

→ a is invertible element. But $a \in N \rightarrow N = R \rightarrow 0 \neq M$ is maximal ideal ring.

Remark. if the ideal is trivial, then the previous theorem is not true in general.

Example. Let $R = \mathbb{Z}$ is PID. Then (0) is trivial ideal and prime in $\mathbb{Z}$, but (0) is not maximal ideal in $\mathbb{Z}$.

Theorem. Let R be a commutative ring with 1such that $a^2 = a$ for each $a \in R$. Then, a non trivial ideal I of R is prime if and only if I is maximal ideal of R.

Proof. ⇐) H.W.

$\Rightarrow$) Let P be a prime ideal of a commutative ring with 1. To prove P is maximal ideal, suppose $\exists\ P \subsetneq K \rightarrow \exists\ x \in K\text{-}P$. But R is Boolean ring (i.e. $a^2 = a$ for each $a \in R$) $\rightarrow x^2 = x \rightarrow x(x-1) = 0 \in P$ ($0 \in P$). But P is prime ideal and $x \notin P \rightarrow x-1 \in P \subsetneq K \rightarrow x-1 \in K$

$\rightarrow x- (x-1) = 1 \in K \rightarrow K = R \rightarrow$ P is maximal ideal.

Definition. A ring R is said to be regular if for each $a \in R$, $\exists\ b \in R$ such that $aba = a$.

Remark. If R is commutative ring, then R is regular if $a^2b = a$.

Example. The ring $\mathbb{Z}$ is not regular.

Q/ find another example.

Theorem. let R be a commutative regular ring, then every prime ideal of R is maximal ideal.

Proof. Let I be a prime ideal in R and $a \notin I$, $a \in R$. Since R is regular ring, $\exists\ b \in R$ such that $a^2b = a \rightarrow a^2b - a = a(ab - 1) = 0 \in I \rightarrow a(ab - 1) \in I$. But I is prime ideal and $a \notin I \rightarrow ab - 1 \in I$. Put $x = ab - 1 \in I$.

$1 = ab - x = -x + ab \in (I, a) \rightarrow 1 \in (I, a) \rightarrow (I, a) = R$.

$\rightarrow$ I is maximal ideal.

Definition. Let I be an ideal of a ring R. Then the nil radical of I(denoted by $\sqrt{I}$) is the set:

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

1. $\sqrt{I}$ is an ideal of R.(H.W. prove)
2. $I \subseteq \sqrt{I}$
3. $\sqrt{0} = \{r \in R \mid r^n = 0 \text{ for some } n \in \mathbb{Z}_+\}$

= the set of all nilpotent element.

4. $\sqrt{0}$ is said to be nil radical of R.

Remarks. If I and J are two ideals of a ring R, then:

1. $\sqrt{IJ} = \sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$
2. $\sqrt{I + J} = \sqrt{\sqrt{I} + \sqrt{J}} \supseteq \sqrt{I} + \sqrt{J}$
3. $\sqrt{\sqrt{I}} = \sqrt{I}$
4. If $I^k \subseteq J$ for some $k \in \mathbb{Z}$, then $\sqrt{I} \subseteq \sqrt{J}$.

Proof. Let $x \in \sqrt{I} \cap \sqrt{J} \rightarrow x \in \sqrt{I}$ & $x \in \sqrt{J} \rightarrow \exists\, n \in \mathbb{Z}_+$ such that $x^n \in I$ & $\exists\, m \in \mathbb{Z}_+$ such that $x^m \in J$.

$\rightarrow (x^n)^m = x^n \,.\, x^n \ldots x^n$ (m-times)

$\rightarrow (x^m)^n = x^m \,.\, x^m \ldots x^m$ (n-times)

$\rightarrow \exists\, nm \in \mathbb{Z}_+$ such that $x^{nm} = (x^n)^m = (x^m)^n \in I \cap J$.

$\rightarrow x \in \sqrt{I \cap J} \rightarrow \sqrt{I} \cap \sqrt{J} \subseteq \sqrt{I \cap J}$ …(1)

Let $y \in \sqrt{I \cap J} \rightarrow \exists\, n \in \mathbb{Z}_+$ such that $y^n \in I \cap J \rightarrow y^n \in I$ & $y^n \in J$

$\rightarrow y \in \sqrt{I} \cap \sqrt{J} \rightarrow \sqrt{I \cap J} \rightarrow \sqrt{I} \cap \sqrt{J}$ …(2)

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

H.W'S: prove the following

1. $\sqrt{IJ} = \sqrt{I} \cap \sqrt{J}$
2. (2), (3), (4)