Commutative Algebra

By Krishna Shinde
Department of Mathematics
Modern College of Arts, Science and Commerce(Autonomous)
Shivajinagar, Pune - 5

CHAPTER 1

Rings and Ideals

RINGS AND RING HOMOMORPHISMS:

DEFINITION. A ring A is a set with two binary operations (addition and multiplication) such that
(1) A is an abelian group with respect to addition(That is, A has zero element denoted by 0, and for every element $x \in A$ has an additive inverse $-x$).
(2) Multiplication is associative($(xy)\,z = x\,(yz)$) and distributive over addition ($x\,(y+z) = xy + xz = (y+z)\,x$) for all $x, y, z \in A$.
(3) $xy = yx$ for all $x, y \in A$.
(4) $\exists 1 \in A$ such that $1x = 1$ for all $x \in A$.
Note: Through out the course the word "ring" shall mean a commutative ring with an identity element.
Example:
(1) Z, R, C and Q are examples of rings. (2) $A = \{0\}$ is a ring with $1_A = 0$ called as zero-ring.
(3) If A is a ring, then $A\,[x] = \{a_0 + a_1 x + ... + a_n x^n / n \in N, a_i \in A\}$.
(4) Let S be any set, then $F\,(S) = \{f : S \to R\}$ is ring with respect to addition and multiplication defined below,
$(f+g)\,(s) = f\,(s) + g\,(s)$
$(f \cdot g)\,(s) = f\,(s) \cdot g\,(s)$.
DEFINITION. Let A be a ring, a subset B of ring A is subring if B itself ring under same operations on A.
Examples:
(1) $Z \subset Q \subset R \subset C$.
(2) Every ring A is subring of $A\,[x]$.
(3) $A_1\,[x] =$ Set of all polynomials $p\,(x) \in A\,[x]$ such that constant term of $p\,(x)$ is 0.
(4) $A_2\,[x] = \{a_0 + a_1 x^2 + ... + a_n x^{2n} / a_0, a_1, ..., a_n \in A\} = A\,[x^2]$.
DEFINITION. A mapping $f : A \to B$, from ring A to ring B is said to be ring homomorphism if
(1) $f\,(x+y) = f\,(x) + f\,(y)$ for all $x, y \in A$.
(2) $f\,(x \cdot y) = f\,(x) \cdot f\,(y)$, for all $x, y \in A$.
(3) $f\,(1_A) = 1_B$.
Examples: (1) If $f : A \to B$ and $g : B \to C$ are ring homomorphisms then $f \circ g : A \to C$

is ring homomorphism.
(2) If S is subring of a ring A which contains identity of A, then identity mapping from S to A is ring homomorphism.

IDEALS. QUOTIENT RINGS :

A subset I of a ring A is an ideal of A, if $(I,+)$ is additive subgroup of A and for every $a \in A$ and $x \in I$ the product $ax \in I$.

Example.
(1) $\{0\} \subseteq A$ and $A \subseteq A$.
(2) $nZ \subseteq Z$.
(3) Collection of polynomials with constant term 0 is ideal of ring $A[x]$.
(4) $I = \{f \in F(S)/f(x) = 0, \forall x \in S\}$ is ideal of $F(S)$.
(5) If $f : A \to B$ is ring homomorphism then $\ker f$ is ideal of A.
Define a relation on ring A by $a \sim b$ iff $a - b \in I$ where I is ideal of ring A.
Then clearly $\sim$ is equivalence relation on A and the collection of equivalence classes are denoted by A/I called quotient of A by I.
Define addition and multiplication on A/I as follows:
Addition: $(a + I) + (b + I) = (a + b) + I$
Multiplication: $(a + I)(b + I) = (ab) + I$
Then A/I is commutative ring with identity.

Proposition 1.1. *There is one-to-one order-preserving correspondence between the set of ideals of A containing I and the set of ideals of A/I.*

PROOF. There is natural mapping $\phi : A \to A/I$ defined by $\phi(a) = a + I$, which is surjective ring homomorphism(Check).
If $f : A \to B$ is ring homomorphism, then $\ker f$ is an ideal of A, and $\Im f$ is subring of B, then $A/\ker f \equiv \Im f$.

Question. If $f : A \to B$ is ring homomorphism and I is an ideal of A, then $f(I)$ is ideal of A ?
Answer. No.
Counter example. The identity mapping $f : \mathbb{Z} \to \mathbb{Q}$ is ring homomorphism and $n\mathbb{Z}$ is an ideal in $\mathbb{Z}$ but $f(n\mathbb{Z}) = n\mathbb{Z}$ is not ideal in $\mathbb{Q}$.

Example. If $f : A \to B$ is ring homomorphism and J is an ideal of B, then show that $f^{-1}(J)$ is an ideal in A.
Proof. Since J is an ideal in $B \Rightarrow 0 \in J$.
$\Rightarrow 0 \in f^{-1}(J)$ $\quad \because$ f is homomorphism $\Rightarrow f(0) = 0 \Rightarrow 0 = f^{-1}(0)$
$\Rightarrow f^{-1}(J) \neq \phi$.
Let $x, y \in f^{-1}(J) \Rightarrow a = f(x), b = f(y) \in J$.
$\Rightarrow a - b = f(x) - f(y) \in J$ $\quad \because J$ is an ideal in B, $a, b \in J \Rightarrow a - b \in J$
$\Rightarrow f(x - y) \in J$ $\quad \because f$ is homomorphism
$\Rightarrow x - y \in f^{-1}(J)$
$\Rightarrow f^{-1}(J)$ is additive abelian subgroup of A.
Let $x \in f^{-1}(J) \Rightarrow a = f(x) \in J$ and $b \in A \Rightarrow f(b) = r \in B$.
$\Rightarrow ra \in J$
$\Rightarrow f(b)f(x) \in J$
$\Rightarrow f(bx) \in J$
$\Rightarrow bx \in f^{-1}(J)$. $\therefore$, $f^{-1}(J)$ is an ideal in A.

ZERO-DIVISOR. NILPOTENT ELEMENT. UNITS
DEFINITION.
(1) A zero-divisor in a ring A is an element x which divides "0" i.e., for which there exists $y \neq 0$ in A such that $xy = 0$.
(2) A ring with no zero-divisor $\neq 0$ is called integral domain.
(3) An element $x \in A$ is nilpotent if $x^n = 0$ for some integer $n > 0$.
- A nilpotent element is a zero-divisor but not conversely.
Counter example. $2 \in \mathbb{Z}_6$ is zero-divisor but not nilpotent.
(4) A unit in A is an element x which divides 1, that is, an element x such that $xy = 1$ for some $y \in A$.
- The element y is uniquely determined by x, and written as x^{-1}.
The multiples ax of an element $x \in A$ forms a principal ideal, denoted by (x) or Ax.
x is unit iff $(x) = A = (1)$.
(5) A field is a ring A in which $1 \neq 0$ and every non-zero element is unit.
- Every field is integral domain but not conversely.
Examples.
(1) $F(S)$ is not integral domain.
Solution: Let $S = \{a, b\}$ define $f(a) = 1, f(b) = 0$ and $g(a) = 0, g(b) = 1$.
$\Rightarrow (f \cdot g)(a) = f(a)g(a) = 0$ also $(f \cdot g)(b) = f(b)g(b) = 0$.
$\Rightarrow f \cdot g \equiv 0$.
(2) If A is integral domain then $A[x]$ is integral domain.
Solution: On contrary assume that $A[x]$ is not integral domain.
$\exists f(x), g(x) \in A[x]$ such that $f(x) \cdot g(x) = 0$ for some non-zero $f(x) = a_0 + a_1x + a_2x^2 + ... + a_nx^n$ and $g(x) = b_0 + b_1x + b_2x^2 + ... + b_mx^m$.
$f(x) \cdot g(x) = 0 \Rightarrow (a_0 + a_1x + a_2x^2 + ... + a_nx^n)(b_0 + b_1x + b_2x^2 + ... + b_mx^m) = 0$
$\Rightarrow a_nb_m = 0$
$a_n = 0$ or $a_m = 0$ (Which is contradiction).
Therefore, $A[x]$ must be integral domain.
Proposition 1.2. *Let A be a ring $\neq 0$. Then following are equivalent:*
(i) *A is a field;*
(ii) *The only ideals in A are 0 and (1);*
(iii) *Every homomorphism of A into a non-zero ring B is injective.*
PROOF. (i) $\Rightarrow$ (ii)
Suppose A is a field.
Let I be an non-zero ideal in A.
$\Rightarrow \exists 0 \neq x \in I$ such that $(x) \subseteq I$ but every non-zero element of A is unit.
$\Rightarrow (x) = A = (1)$
$\Rightarrow I = (1)$
(ii) $\Rightarrow$(iii)
Suppose, the only ideals in A are 0 and (1).
Let $\phi : A \to B$ be a ring homomorphism.
Then kernel of ϕ is an proper ideal of A $\because$ If $\ker \phi = (1)$ then $\phi(1) = 0$ which is not true.
$\Rightarrow \ker \phi = 0$
$\Rightarrow \phi$ is injective.
(iii) $\Rightarrow$ (i)

Let x be an element of A which is not a unit.
Then $(x) \neq (1)$ hence, $B = A/(x)$ is non-zero ring.
Let $\phi : A \to B$ be the natural homomorphism of A onto B with $\ker\phi = (x)$.
but by our assumption $\ker\phi = 0 \Rightarrow (x) = 0 \Rightarrow x = 0$.
$\Rightarrow$ Non-unit in A is 0.
$\Rightarrow$ Every non-zero element in A is unit.
$\Rightarrow$ A is field.

PRIME IDEAL AND MAXIMAL IDEAL

An ideal P in A is prime if $P \neq (1)$ and if $ab \in P \Rightarrow a \in P$ or $b \in P$.

Example.

(1) 0 is prime ideal $\Leftrightarrow A$ is integral domain.
(2) P is prime ideal in A iff A/P is an integral domain.
PROOF. Suppose P is prime ideal in A.
Clearly A/P is commutative ring with identity.
Assume that $(a+P)(b+P) = 0+P$ for some $a+P, b+P \in A/P$.
$\Rightarrow (ab)+P = 0+P$
$\Rightarrow (ab-0) \in P$
$\Rightarrow ab \in P$
$\Rightarrow a \in P$ or $b \in P$ $\quad\because P$ is prime ideal
$\Rightarrow a+P = 0+P$ or $b+P = 0+P$.
$\Rightarrow A/P$ is an integral domain.
Conversely, Suppose A/P is integral domain.
$\Rightarrow 1+P \neq 0+P$ and A/P is commutative ring which has no zero-divisor.
$\Rightarrow P \neq A$
Assume that $ab \in P$ then $ab+P = 0+P$
$\Rightarrow (a+P)(b+P) = 0+P$
$\Rightarrow a+P = 0+P$ or $b+P = 0+P$
$\Rightarrow a \in P$ or $b \in P$
$\Rightarrow P$ is prime ideal.
An ideal M in A is maximal if $M \neq (1)$ and if there is no ideal I such that $M \subset I \subset (1)$.

Exercise

1. M is maximal ideal if and only if A/M is a field.
2. Show that every maximal ideal is prime ideal.
3. If $f : A \to B$ is a ring homomorphism and P is prime ideal in B, then $f^{-1}(P)$ is prime ideal in A.
4. Find an example of homomorphism in which inverse image of maximal ideal need not be a maximal ideal.

Question. Whether every ring $A \neq 0$ has maximal ideal ?

Theorem 1.3. Every ring $A \neq 0$ has at least one maximal ideal.

PROOF. Let $A \neq 0$ be a ring and $\sum$ be collection of all proper ideals in A.
That is, $\sum = \{I/I$ is proper ideal of $A\}$
Then $\sum \neq \phi$. $\quad\because (0) \in \sum$
Let $I_1 \subset I_2 \subset ...$ be chain in $\sum$.
$\cup_{n=1}^{\infty} I_n$ is an ideal in A $\quad\because I_1 \subset I_2 \subset ...$ is an increasing chain.
If $\cup_{n=1}^{\infty} I_n = A$ then $1_A \in \cup_{n=1}^{\infty} I_n$

$\Rightarrow 1_A \in I_n$ for some in $\rightarrow\leftarrow$. $\because I_n \subsetneq A$
$\Rightarrow \cup_{n=1}^{\infty} I_n \in \sum$ and it is upper bound of chain $I_1 \subset I_2 \subset ...$
$\Rightarrow$ Any increasing chain in $\sum$ has maximal element.
$\therefore$ by Zorn's lemma $\sum$ has maximal element say M.
Now if M is not maximal ideal in A then there exists an ideal J in A such that $M \subsetneq J \subsetneq A$.
$\Rightarrow J \in \sum$ which contradiction to maximality of $\sum$. $\because M$ is maximal element in $\sum$.
$\therefore M$ is maximal ideal in A. ■

Corollary 1.4. *If $I \neq (1)$ is an ideal of A, then there exists a maximal ideal of A containing I.*

PROOF. Let $\sum$ be collection of all ideals of A which contains I.
That is,
$\sum = \{J/J$ is an proper ideal of A and $I \subset J\}$.
Then by previous theorem there exists maximal ideal M which contains I. ■

Corollary 1.5 *Every non-unit of A is contained in a maximal ideal.*

PROOF. Suppose x be a non-unit element in A then $x \in (x) \subsetneq A$.
Also by proposition 1.4. every proper ideal is contained in a maximal ideal.
$\Rightarrow (x) \subset M$, where M is a maximal ideal in A. $\Rightarrow x \in M$. ■

DEFINITION.
1. A ring A with exactly one maximal ideal M is called as local ring.
- Example. $\mathbb{Z}_p \simeq \mathbb{Z}/p\mathbb{Z}$.
2. The field A/M is called as residue field.
- Example. $\mathbb{Z}_p \simeq \mathbb{Z}/p\mathbb{Z}$.
3. A ring with finitely many maximal ideals are called as semi-local rings.
- Example. $\mathbb{Z}_n \simeq \mathbb{Z}/n\mathbb{Z}$.

Corollary 1.6. i) *Let A be a ring and $M \neq (1)$ an ideal of A such that every $x \in A - M$ is a unit in A. Then A is local ring and M is maximal ideal.*
ii) *Let A be a ring and M is a maximal ideal of A, such that every element of $1 + M$ is a unit in A. Then A is a local ring.*

PROOF. i) Since every ideal $\neq (1)$ consist of non-units and also we know that every ideal in contained in some maximal ideal.
Here every $x \in A - M$ is unit hence M contains all non-units hence it is only maximal ideal in A.
$\Rightarrow A$ is a local ring.
ii) Suppose A is a ring and M is maximal ideal in A such that $1 + M$ is unit in A.
Let x be a non-unit in a ring A.
If $x \notin M$ then $(x) + M = (1)$.
$\Rightarrow \exists u \in M$ and $r \in (x)$ such that $u + rx = 1$.
$\Rightarrow 1 - u = rx$.
$\Rightarrow 1 - u$ is unit in A. $\because$ by hypothesis $1 + x$ is unit for every $x \in M$
$\Rightarrow rx$ is unit.
$\Rightarrow x$ is unit $\rightarrow\leftarrow$ to assumption that M is maximal ideal.
$\therefore x \in M$.
Every non-unit are contained in M.
$\Rightarrow M$ is the unique maximal ideal in A. ■

DEFINITION. A principal ideal domain is an integral domain in which every ideal is

principal.
Result. In principal ideal domain every non-zero prime ideal is maximal.
PROOF. Suppose $(x) \neq (0)$ is prime ideal in PID A and suppose $(x) \subset (y)$.
$\implies x \in (y)$.
$\implies x = yz$ for some $z \in A$.
$\implies yz = x \in (x) \implies yz \in (x)$.
But $y \notin (x) \implies z \in (x)$.
$\implies z = tx$ for some $t \in A$.
Then $x = yz = ytx \implies x = ytx$.
$\implies yt = 1$.
$\implies 1 \in (y)$.
$\implies (y) = (1)$.
$\implies (x)$ is maximal ideal in A.
$\implies$ Every non-zero prime ideal in PID is a maximal ideal. ■

NILRADICAL AND JACOBSON RADICAL

Proposition 1.7. *The set $\Re$ of all nilpotent elements in a ring A is an ideal, and $A/\Re$ has no nilpotent element $\neq 0$.*
PROOF. If $x \in \Re \implies x^n = 0$ for some $n > 0$.
$\implies (ax)^n = a^n x^n = a^n(0) = 0$.
$\implies ax \in \Re$.
Now let $x, y \in \Re$ then $x^n = 0$ and $y^m = 0$ for some $m, n > 0$.
Consider, $(x+y)^{n+m-1} = x^{n+m-1} +^{n+n-1} C_1 x^{n+m-2} y + ... + y^{n+m-1}$.
It is sum of integer multiple of products $x^r y^s$, where $r + s = m + n - 1$. We cannot have both $r < m$ and $s < n$ hence each of these product vanishes.
$\implies (x+y)^{n+m-1} = 0 \implies x + y \in \Re$.
$\implies \Re$ is ideal of ring A.
Also all nilpotent elements are in $\Re$ hence $A/\Re$ has no non-zero nilpotent element. ■
DEFINITION. The ideal $\Re$ is called nilradical of A.
Proposition 1.8. *The nilradical of A is intersection of all prime ideals of A.*
PROOF. Let $\Re'$ denote the intersection of all prime ideals of A.
If $f \in A$ is nilpotent element and P is prime ideal, then $f^n = 0 \in P$, for some $n > 0$.
$\implies f^n \in P$ and P is prime ideal $\implies f \in P$.
$\implies \Re \subseteq \Re'$. (1)
Suppose f is not nilpotent element.
Let $\sum$ be the set of ideals I such that $f^n \notin I$ for any $n > 0$.
Since $(0) \in \sum \implies \sum \neq \phi$.
Then by Zorn's lemma lemma $\sum$ has maximal element.
Let P be maximal element of $\sum$.
Now we shall show P is prime ideal.
Let $x, y \notin P$. $\implies P + (x), P + (y)$ contains P.
$\implies P + (x), P + (y) \notin \sum$. $\because P$ is maximal element in $\sum$.
$\implies f^m \in P + (x)$ and $f^n \in P + (y)$ for some $m, n > 0$.
$\implies f^{m+n} \in P + (xy)$ and hence $P + (xy) \notin \sum$.
$\implies xy \notin P$.
Hence P is prime ideal such that $f \notin P$.

Thus, If f is not nilpotent, then $f \notin P$ for some prime ideal of ring $A \implies f \notin \cap_{P \subset A} P = \Re'$.
$\implies f \notin \Re'$.
$\implies \Re' \subseteq \Re$. (2)
From (1) and (2) we get $\Re' = \Re$.
Therefore, the nilradical of A is intersection of all prime ideals of A. ■
DEFINITION. The Jacobson radical of ring A is defined to be the intersection of all maximal ideals of A.
Proposition 1.9. *If J is Jacobson radical of A, then $x \in J \iff 1 - xy$ is unit for all $y \in A$.*
PROOF. Suppose J is Jacobson radical of ring A.
Let $x \in J$. On contrary assume that $1 - xy$ is non-unit then, there exists maximal ideal M such that $1 - xy \in M$ for some maximal ideal M of ring A.
Since, $x \in J \implies x \in M$.
$\implies xy \in M, \quad \forall y \in A$.
$\implies 1 = xy + (1 - xy) \in M \to\leftarrow$. $\because M$ is proper ideal of ring A.
$\therefore 1 - xy$ must be unit.
Conversely, Suppose $1 - xy$ is unit for all $y \in A$.
If $x \notin J$, then there exists maximal ideal M such that $x \notin M$.
$\implies M + (x) = A$.
$\implies m + xy = 1$ for some $m \in M$ and $y \in A$.
$\implies m = 1 - xy$.
$\implies m$ is unit $\to\leftarrow$.
$\therefore x \in J$. ■
Example 1. Let A be a ring and let $A[x]$ be the ring of polynomials in an indeterminate x, with coefficients in A. Let $f = a_0 + a_1 x + ... + a_n x^n \in A[x]$. Prove that
(i) f is unit in $A[x]$ if and only if a_0 is unit in A and $a_, a_2, ..., a_n$, are nilpotent.
(ii) f is nilpotent if and only if $a_0, a_1, ..., a_n$ are nilpotent.
(iii) f is zero-divisor if and only if there exists $a \neq 0$ in A such that $af = 0$.
Solution. (i) Suppose f is unit in $A[x]$.
$\implies \exists g = b_0 + b_1 x + ... + b_m x^m \in A[x]$ such that $f \cdot g = 1$.
$\implies (a_0 + a_1 x + ... + a_n x^n)(b_0 + b_1 x + ... + b_m x^m) = 1$.
$\implies a_0 b_0 = 1 \implies a_0$ is unit in A.
Also, $a_n b_m = 0$ and $a_{n-1} b_m + a_n b_{m-1} = 0$. Multiplying both side by a_n we get.
$a_n a_{n-1} b_m + a_n^2 b_{m-1} = 0 \implies a_n^2 b_{m-1} = 0$.
Similarly multiplying both side of $a_{n-2} b_m + a_{n-1} b_{m-1} + a_n b_{m-2} = 0$ by a_n^2.
$\implies a_n^2 a_{n-2} b_m + a_n^2 a_{n-1} b_{m-1} + a_n^3 b_{m-2} = 0 \implies a_n^3 b_{m-2} = 0$
If the sum of powers of a_n and subscripts of b is $m + 1$, then the corresponding product is 0.
$\implies a_n^{m+1} b_0 = 0$.
Multiplying this it by a_0 we get.
$a_n^{m+1} b_0 a_0 = 0 \implies a_n^{m+1} = 0$. $\because a_0 b_0 = 1$
$\therefore a_n$ is nilpotent.
Inductively, $a_i = 0$ for all $1 \leq i \leq n$.
Conversely, Suppose a_0 is unit and $a_1, a_2, ..., a_n$ are nilpotent in $A[x]$.

Then $f = a_0 + a_1x + ... + a_nx^n$ is sum of nilpotent element and unit and hence it is unit.
(ii) Suppose $f = a_0 + a_1x + ... + a_nx^n$ is nilpotent in $A[x]$.
$\Longrightarrow 1 - f$ is unit in $A[x]$.
$\Longrightarrow 1 - a_0$ is unit in $A[x]$ and $a_i's, 1 \leq i \leq n$ are nilpotent in A.
Also, $f^m = 0 \Longrightarrow a_0^m = 0 \Longrightarrow a_0$ is nilpotent.
Conversely, Suppose $a_0, a_1, ..., a_n$ are nilpotent.
If $d \in \mathbb{N}$ such that $a_i^d = 0, 0 \leq i \leq n$, then $f^d = 0$.
$\Longrightarrow f$ is nilpotent.
(iii) Suppose f is zero-divisor.
$\Longrightarrow \exists 0 \neq g \in A[x]$ such that $fg = 0$ then g must be of degree 0.
Because if $g = b_0 + b_1x + ... + b_mx^m$ where $b_m \neq 0$ then $a_nb_m = 0 \Longrightarrow a_n = 0 \rightarrow\leftarrow$. $\because$ degree of f is n.
Therefore, g must of degree $0 \Longrightarrow \exists 0 \neq a \in A$ such that $\Longrightarrow af = 0$.
Conversely, Suppose $\exists 0 \neq a \in A$ such that $af = 0$.
$\Longrightarrow f$ is zero-divisor.

Example 2. In a ring $A[x]$, the Jaconson radical is equal to nilradical.

Solution. Suppose $\mathfrak{R}, \mathfrak{J}$ are nilradical and Jaconson radical of $A[x]$ respectively.
$f(x) \in \mathfrak{R}$
$\Longrightarrow (f(x))^n = 0 \in \mathfrak{J}$ for some $n > 0$.
$\Longrightarrow f(x) \in \mathfrak{J}$.
$\mathfrak{R} \subseteq \mathfrak{J}$.
$f(x) \in \mathfrak{J}$.
$1 - f(x)g(x)$ is unit for all $g(x) \in A[x]$.
Let $g(x) = x$ and $f(x) = a_0 + a_1x + ... + a_nx^n$.
$\Longrightarrow 1 - f(x)g(x) = 1 - a_0x + a_1x^2 + ... + a_nx^{n+1}$ is unit.
$\Longrightarrow a_0, a_1, ..., a_n$ are nilpotent.
$\Longrightarrow f(x)$ is nilpotent.
$f(x) \in \mathfrak{R}$
$\Longrightarrow \mathfrak{J} \subseteq \mathfrak{R}$. $\Longrightarrow \mathfrak{R} = \mathfrak{J}$.
$\therefore A[x]$ is Hilbert ring.

Example 3. A ring A is such that every ideal not contained in the nilradical contains a non-zero idempotent. Prove that A is Hilbert ring.

Proof. It is sufficient to show that every prime ideal in A is maximal ideal.
Let P be a prime ideal in A and let x be a non-zero element in $A - P$.
$\Longrightarrow (x)$ contains non-zero idempotent, say a_0x.
$\Longrightarrow a_0x(a_0x - 1) = 0 \in P$.
$\Longrightarrow a_0x(a_0x - 1)$ is zero-element in A/P.
But A/P is an integral domain and $a_0x \neq 0$.
$\Longrightarrow a_0x - 1 = 0$.
$\Longrightarrow a_0x = 1$ or x is unit.
$\Longrightarrow A/P$ is field.
$\Longrightarrow P$ is maximal ideal.
$\therefore A$ is Hilbert ring.

Example 4. If A is ring in which every element x satisfies $x^n = x$, for some $n > 1$. Show that every prime ideal in A is maximal.

Solution. Let P be prime ideal in ring A.
$\therefore A/P$ is integral domain.
Let $\bar{x}$ such that $\bar{x} \neq \bar{0}$.
But $x^n = x \implies \bar{x}^n = \bar{x}$.
$\implies \bar{x}(1 - \bar{x}^{n-1}) = 0 \in P$.
$\implies 1 - \bar{x}^{n-1} \in P$. $\because P$ is prime ideal and $\bar{x} \notin P$
$\implies (1 - \bar{x}) + P = 0 + P$.
$\implies 1 + P = x^{n-1} + P$.
$\implies \bar{1} = \bar{x}^{n-1}$.
$\implies \bar{x} \cdot \bar{x}^{n-2} = 1$.
$\implies \bar{x}$ is unit in A/P.
$\implies$ Every non-zero element is A/P is unit.
$\therefore A/P$ is field.
$\implies P$ is maximal ideal.
Example 5. Let $A \neq 0$ be a ring. Show that set of prime ideals in A has minimal element with respect to inclusion.
Proof. Let $\sum = \{P/P$ is prime ideal in $A\}$.
Since every non-zero ring has at least one maximal ideal hence $\sum \neq 0$.
Define relation on $\sum$ as $P_1 \leq P_2$ if and only if $P_2 \subseteq P_1$.
Then $(\sum, \leq)$ is poset.
Let $C : P_1 \leq P_2 \leq ...$ be any chain in P.
$\implies C : P_1 \supseteq P_2 \supseteq ....$
Let $P = \cap_{P_i \in C} P_i$.
$\implies P$ is ideal of A.
Now we shall show P is prime ideal of A.
Suppose $xy \in P$ and $x \notin P$.
$\implies xy \in P$.
$\implies xy \in P_i$ for all i.
Also, $x \notin P \implies x \notin P_i, \quad \forall i$.
$\implies y \in P_i, \quad \forall i$.
$\therefore y \in P$.
$\implies P$ is prime ideal.
$\implies P \in \sum$ and $P \subseteq P_i, \quad \forall i$.
$\therefore P$ is upper bound of chain C in $\sum$.
$\therefore$ By Zorn's lemma $\sum$ has maximal element, which is required minimal prime ideal.
Example 6. If $x \notin M$ for any maximal ideal of ring A, then $M + (x) = A$.
Solution. If $M + (x) \subset A$.
$\implies M \subset M + (x) \subset A \rightarrow\leftarrow$. $\because M$ is maximal ideal of A.
Example 7. Let A be ring and $\Re$ is it's nilradical. Show that following are equivalent.
(i) A has exactly one prime ideal;
(ii) Every element of A is either a unit or nilpotent;
(iii) $A/\Re$ is field.
Proof. (i) $\implies$ (ii)
Suppose A has exactly one prime ideal.
$\implies A$ has exactly one maximal ideal.

$\Longrightarrow A$ is local ring.
$\therefore$ Nil$(A) = P$.
Also, $x \notin P \Longrightarrow x$ is unit in A. $\because$ if x is not unit then $(x) \subseteq M$ for some maximal ideal M in A. But $M = P \Rightarrow x \in P \rightarrow\leftarrow$
$\therefore$ Every element of A is either unit or nilpotent.
(ii) $\Longrightarrow$ (iii)
Let $\Re$ is nilradical in A and every element of A outside of $\Re$ is unit.
$\Longrightarrow$ Every non-zero element of $A/\Re$ is unit.
$\Longrightarrow A/\Re$ is field.
(iii) $\Longrightarrow$ (i)
Suppose $A/\Re$ is field.
$\Longrightarrow \Re$ is maximal ideal in A.
But $\Re = \cap_{P-\text{prime}} P$.
$\Longrightarrow \Re \subseteq P, \quad \forall P$.
But $\Re$ is maximal and hence $\Re = P$.
$\therefore A$ has exactly one prime ideal.
Example 8. A ring A is Boolean if $x^2 = x$ for all $x \in A$. In a Boolean ring A, show that
(i) $2x = 0$ for all $x \in A$;
(ii) Every prime ideal P is maximal, and A/P is a field with two elements;
(iii) Every finitely generated ideal in A is principal.
Proof. (i) Let $x \in A$.
$\therefore (1+x)^2 = 1+x$
$\Longrightarrow (1+x)(1+x) = (1+x)$
$\Longrightarrow 1+x+x+x^2 = 1+x$
$\Longrightarrow 1+x+2x = 1+x$
$\Longrightarrow 2x = 0, \quad \forall x \in A$.
(ii) Let P be a prime ideal in A.
$\therefore A/P$ is integral domain.
Also, $x^2 = x, \quad \forall x \in A$ that is,
$x^2 + P = x + P$ in A/P.
Every element in A/P is idempotent.
But 0 and 1 are the only idempotents in integral domain.
Hence $A/P \cong Z_2$, but Z_2 is field.
$\Longrightarrow A/P$ is field.
$\therefore P$ is maximal ideal.
(iii) It is sufficient to show ideal generated by two elements is principal.
Let $I = (x, y)$ and $z = x + y + xy$.
Now consider,

$$\begin{aligned} zx &= (x+y+xy)x \\ &= x^2 + xy + x^2y \\ &= x + xy + xy \\ &= x + 2xy \\ &= x \end{aligned}$$

$\Longrightarrow zx = x$.
Similarly,

$$\begin{aligned} zy &= (x+y+xy)y \\ &= xy+y^2+xy^2 \\ &= xy+y+xy \\ &= y+2xy \\ &= y \end{aligned}$$

$\implies z$ is multiplication identity in I.
$\implies I=(z)$.
Therefore, every ideal in A is principal.
Example 8. A local ring contains no idempotent $\neq 0,1$.
Proof. Let A be a local ring.
$\implies A$ has unique maximal ideal, say M.
Suppose x be an idempotent in a ring A.
$\implies x^2=x$.
$\implies x(1-x)=0\in M$.
$\implies x=0,1$
Because if $x\notin\{0,1\}$ then $x,1-x\in M$.
$\implies 1=x+(1-x)\in M \rightarrow\leftarrow$.
$\therefore x\in\{0,1\}$.
OPERATIONS ON IDEAL
If I and J are ideals in a ring A, then the sum $I+J=\{x+y/x\in I, y\in J\}$ is smallest ideal containing I and J. More generally we may define the sum $\sum_{i\in\Delta} I_i = \left\{\sum_{\text{finite}} x_i/x_i\in I_i\right\}$ is smallest ideal containing all ideals I_i.
The ideal I and J are said to be co-prime ideals of A if $I+J=A$.
Result. If I and J are co-prime ideals, then $I\cap J=IJ$.
Proof. Since $IJ\subseteq I$ and $IJ\subseteq J\implies IJ\subseteq I\cap J$.
Also, I and J are co-prime $\implies I+J=A$.
$\implies x+y=1$ for some $x\in I$ and $y\in J$.
$\implies IJ=I\cap J$.
The intersection of any family $(I_i)_{i\in\Delta}$ of ideals is an ideal. Thus the ideals of A forms a complete lattice with respect to inclusion.
The product of two ideals I and J in A is the ideal $IJ=\left\{\sum_{\text{finite}} x_iy_i/x_i\in I, y_i\in J\right\}$.
Similarly we define the product of any finite family of ideals.
Example.
(1) If $A=Z, I=(m), J=(n)$ then $I+J$ is the ideal generated by g.c.d. of m and n.
$I\cap J$ is ideal generated by l.c.m. of m and n.
$IJ=I\cap J$ iff m,n are co-prime.
Let $A_1,A_2,...,A_n$ be rings then the direct product $A=\prod_{i=1}^{n} A_i$ is set of all sequences $(x_1,x_2,...,x_n)$ with $x_i\in A_i (1\le i\le n)$ is commutative ring with identity with respect to

component wise addition and multiplication.
The projections $p_i : A \to A_i$ by $p_i(x) = x_i$ are homomorphisms.

Let A be a ring and $I_1, I_2, ..., I_n$ ideals of A. Define a homomorphism $\phi : A \to \prod_{i=1}^{n}(A/I_i)$.
by $\phi(x) = (x + I_1, x + I_2, ..., x + I_n)$.

Proposition 1.10. (i) *If I_i and I_j are co-prime whenever $i \neq j$, then* $\prod_{i=1}^{n} I_i = \cap_{i=1}^{n} I_i$.
(ii) *ϕ is surjective $\iff I_i, I_j$ are co-prime $i \neq j$.*
(iii) *ϕ is injective $\iff \cap_{i=1}^{n} I_i = (0)$.*

Proof. (i) We will use mathematical induction to prove this part.
If I_1 and I_2 are two ideals then $I_1 \cap I_2 = I_1 I_2$ holds.
Therefore the result is true for $n = 2$.
Assume that the result is true for $n - 1$ ideals.
That is, $\prod_{i=1}^{n-1} I_i = \cap_{i=1}^{n-1} I_i$.
Now we shall prove the result is true for n ideals.
Suppose $B = \cap_{i=1}^{n-1} I_i$.
Now I_i and I_n are co-prime for all $i = 1, 2, ...n - 1$.
$\therefore I_i + I_n = (1)$.
$\therefore x_i + y_i = 1$, for some $x_i \in I_i$ and $y_i \in I_n$.
$\therefore x_i = 1 - y_i \in I_i$.
Let $x = x_1 x_2 ... x_n \in \prod_{i=1}^{n-1} I_i = B$.
$\therefore x = (1 - y_1)(1 - y_2)...(1 - y_{n-1})$.
$\therefore x = 1 - y$, for some $y \in I_n$.
$\therefore x + y = 1$ for some $x \in B$ and $y \in I_n$.
Therefore, B and I_n are co-prime ideals.
$\therefore B \cdot I_n = B \cap I_n$.
$\implies \prod_{i=1}^{n} I_i = \cap_{i=1}^{n} I_i$.
(ii) Suppose ϕ is surjective.
First we will prove that I_1 and I_i are co-prime ideals.
Since ϕ is surjective $\exists x \in A$ such that $\phi(x) = (1 + I_1, 0 + I_2, ..., 0 + I_n)$.
$\implies (x + I_1, x + I_2, ..., x + I_n) = (1 + I_1, 0 + I_2, ..., 0 + I_n)$.
$\implies x + I_1 = 1 + I_1$ and $x + I_i = 0 + I_i, \quad \forall i = 2, 3, ..., n$.
$\implies 1 - x \in I_1$ and $x \in I_i, \quad \forall i = 2, 3, ..., n$.
$\therefore x + (1 - x) \in I_1 + I_i$.
$\therefore 1 \in I_1 + I_i$.
$\implies I_1$ and I_i are co-prime.
Similarly, I_i and I_j are co-prime for $i \neq j$.
Conversely, suppose I_i and I_j are co-prime for $i \neq j$.
It is sufficient to show that there exist $v \in A$ such that $\phi(v) = (1 + I_1, 0 + I_2, ..., 0 + I_n)$.
Since, I_1 and I_j are co-prime for $j = 2, 3, ..., n$.

$\implies \exists u_i \in I_1$ and $v_j \in I_j$ such that $u_i + v_j = 1$.
Take, $v = v_2 \cdot v_3 \cdot ... \cdot v_n$.
$\implies v = (1-u_2)(1-u_3)...(1-u_n)$.
$\implies v = 1-u$, for some $u \in I_1$.

$$\begin{aligned} \therefore \phi(v) &= (v+I_1, v+I_2, ..., v+I_n) \\ &= ((1-u)+I_1, 0+I_2, ..., 0+I_n) \\ &= (1+I_1, 0+I_2, ..., 0+I_n) \end{aligned}$$

$\implies \phi(v) = (1+I_1, 0+I_2, ..., 0+I_n)$.
Similarly, For each $e_j \in \prod_{i=1}^{n}(A/I_i)$, $\exists$ some v_j in A such that $\phi(v_j) = e_j$ for $j = 2, 3, ..., n$.
Where $e_j = (0+I_1, 0+I_2, ..., 1+I_i, ..., 0+I_n)$.
$\therefore \phi$ is surjective.
(iii) Let $x \in \ker\phi$.
$\iff \phi(x) = 0$.
$\iff (x+I_1, x+I_2, ..., x+I_n) = (I_1, I_2, ..., I_n)$.
$\iff x+I_1 = 0+I_1, x+I_2 = 0+I_2, ..., x+I_n = 0+I_n$.
$\iff x+I_1 = I_1, x+I_2 = I_2, ..., x+I_n = I_n$.
$\iff x \in I_1, x \in I_2, ..., x \in I_n$.
$\iff x \in \cap_{i=1}^{n} I_i$.
$\implies \ker\phi = \cap_{i=1}^{n} I_i$.
We know that $\ker\phi = (0) \iff \phi$ is injective.
$\therefore \ker\phi = \cap_{i=1}^{n} I_i = (0)$. ■

Proposition 1. 11. (i) *Let $P_1, P_2, ..., P_n$ be prime ideals and let I be an ideal contained in $\cup_{i=1}^{n} P_i$. Then $I \subseteq P_i$ for some i.*
(ii) *Let $I_1, I_2, ..., I_n$ be ideals and let P be prime ideal containing $\cap_{i=1}^{n} I_i$. Then $P \supseteq I_i$ for some i. If $P = \cap_{i=1}^{n} I_i$, the $P = I_i$ for some i.*
PROOF. (i) We will prove this by induction.
Let P_1, P_2 are two prime ideals and I be an ideal such that $I \subseteq P_1 \cup P_2$.
Let $x \in I$ and suppose $I \nsubseteq P_1$.
$\exists y \in I$ such that $y \notin P_1$.
$\implies y \in P_2$.
$\implies x + y \in I \subseteq P_1 \cup P_2$.
Suppose $x + y \in P_1$.
If $x \in P_1 \implies y = (x+y) - x \in P_1 \rightarrow\leftarrow$.
$\therefore x \notin P_1 \implies x + y \notin P_1$.
$\implies x + y \in P_2$.
$\implies x = (x+y) - y \in P_2 \implies I \subseteq P_2$.
$\therefore$ The result is true for $n = 2$.
Now assume that the result is true for $n-1$ ideals.
That is, if $P_1, P_2, ..., P_{n-1}$ are prime ideals and $I \subseteq \cup_{i=1}^{n-1} P_i$, then $I \subseteq P_i$ for some $i = 1, 2, ..., n-1$.
Now suppose $P_1, P_2, ..., P_n$ are prime ideals and $I \subseteq \cup_{i=1}^{n} P_i$.
To show: $I \subseteq P_i$ for some $i = 1, 2, ..., n$.

We will prove the contrapositive statement.
That is, if $I \nsubseteq P_i \quad 1 \le i \le n \Longrightarrow I \nsubseteq \cup_{i=1}^{n} P_i$.
$\Longrightarrow$ For each i there exists $x_i \in I$ such that $x_i \notin P_j$ whenever $i \neq j$.
If for some i we have $x_i \notin P_i$ then we are through.
Suppose $x_i \in P_i$ for all $1 \le i \le n$.
Now consider the element, $y = \sum_{i=1}^{n} x_1 x_2 ... x_{i-1} x_{i+1} ... x_n$
Then we have $y \in I$ and $y \notin P_i$ for all $1 \le i \le n$.
$\Longrightarrow I \nsubseteq \cup_{i=1}^{n} P_i$.
(ii) Suppose $I_1, I_2, ..., I_n$ be ideals and P be prime ideal containing $\cap_{i=1}^{n} I_i$.
To show: $P \supseteq I_i$ for some i.
That is, to show : If $I_i \nsubseteq P$ for all i, then $\cap I_i \nsubseteq P$.
Suppose $I_i \nsubseteq I_i$ for all i.
$\Longrightarrow \exists x_i \in I_i, x_i \notin P (1 \le i \le n)$, and therefore $\prod x_i \in \prod I_i \subseteq \cap I_i$.
But P is prime ideal $\Longrightarrow \prod x_i \notin P$.
$\Longrightarrow \cap I_i \nsubseteq P$.
If $P = \cap I_i$, then $P = I_i$ for some i. ■

Definition. If I and J are ideals in a ring A then their ideal quotient is denoted by $(I : J)$ and defined as, $(I : J) = \{x \in A / xJ \subseteq I\}$.

Result 1. Show that $(I : J)$ is ideal in A.
PROOF. Let $x, y \in (I : J) \Longrightarrow xJ \subseteq I, yJ \subseteq I$.
Consider, $(x - y)J = xJ - yJ \subseteq I$.
$\Longrightarrow x - y \in (I : J)$.
Also, for $x \in (I : J)$ and $a \in A$.
$(ax)J = a(xJ) \subseteq I$.
$\Longrightarrow ax \in (I : J)$.
$\therefore (I : J)$ is an ideal in A. ■

Definition. If $I = (0)$ then $(0 : J) = \{x \in A / xJ = 0\}$.
$\Longrightarrow (0 : J) = \{x \in A / xy = 0, \quad \forall y \in J\}$.
The ideal $(0 : J)$ is called annihilator of J and is also denoted by $\mathrm{Ann}(J)$.

Result 2. If D denote set of all zero-divisors in a ring A then $D = \cup_{x \neq 0} \mathrm{Ann}(x)$.
PROOF. Let $x \in D$, then there exists $0 \neq y \in A$ such that $xy = 0$.
$\Longrightarrow x \in \mathrm{Ann}(y)$.
$\Longrightarrow x \in \cup_{x \neq 0} \mathrm{Ann}(x)$.
$\therefore D \subseteq \cup_{x \neq 0} \mathrm{Ann}(x)$. (1)
Suppose, $y \in \cup_{x \neq 0} \mathrm{Ann}(x)$.
$\Longrightarrow y \in \mathrm{Ann}(x)$ for some $0 \neq x \in A$.
$\Longrightarrow yx = 0$.
$\Longrightarrow y \in D$.
$\therefore \cup_{x \neq 0} \mathrm{Ann}(x) \subseteq D$. (2)
From (1) and (2) we get, $D = \cup_{x \neq 0} \mathrm{Ann}(x)$. ■

Definition. If I is any ideal of A, then radical of I is $r(I) = \{x \in A / x^n \in I \text{ for some } n > 0\}$.

Result 3. $r(I)$ is an ideal of a ring A.
PROOF. If $\phi : A \to A/I$ is standard homomorphism,

Consider,

$$\begin{aligned}\Re(A/I) &= \{\bar{x} \in A/I : \bar{x}^n = \bar{0}, \text{ for some } n > 0\} \\ &= \{\bar{x} \in A/I : x^n + I = I, \text{ for some } n > 0\} \\ &= \{\bar{x} \in A/I : x^n \in I, \text{ for some } n > 0\}\end{aligned}$$

$$\begin{aligned}\phi^{-1}(\Re(A/I)) &= \{x \in A : \phi(x) \in \Re(A/I)\} \\ &= \{x \in A : x + I \in \Re(A/I)\} \\ &= \{x \in A : (x+I)^n = I, \text{ for some } n > 0\} \\ &= \{x \in A : x^n + I = I, \text{ for some } n > 0\} \\ &= \{x \in A : x^n \in I, \text{ for some } n > 0\} \\ &= r(I)\end{aligned}$$

$\therefore r(I)$ is subspace of A.
Exercise 1.13 (i) $r(I) \supseteq I$
(ii) $r(r(I)) = r(I)$
(iii) $r(IJ) = r(I \cap J) = r(I) \cap r(J)$
(iv) If P is prime ideal, then $r(P) = P$(Exercise)
(v) $r(I + J) = r(r(I) + r(J))$(Exercise)
(vi) $r(I) = (1) \Leftrightarrow I = (1)$(Exercise)
Solution. (i) Let $x \in I$
$\Longrightarrow x^n \in I$
$\Longrightarrow x \in r(I)$
$I \subseteq r(I)$.
(ii) By part (i) $r(I) \subseteq r(r(I))$
Let $x \in r(r(I))$
$\Longrightarrow x^n \in r(I)$ for some $n > 0$
$\Longrightarrow (x^n)^m \in I$ for some $m > 0$
$\Longrightarrow x^{nm} \in I$
$\Longrightarrow x \in r(I)$
$\Longrightarrow r(r(I)) \subseteq r(I)$
$\therefore r(r(I)) = r(I)$.
(iii) Since $IJ \subseteq I \cap J \Longrightarrow r(IJ) \subseteq r(I \cap J)$.
Let $x \in r(I \cap J)$
$\Longrightarrow x^n \in I \cap J$
$\Longrightarrow x^n \in I$ and $x^n \in J$ for some $n > 0$.
$\Longrightarrow x^n \cdot x^n \in IJ$
$\Longrightarrow x^{2n} \in IJ$
$\Longrightarrow x \in r(IJ)$
$\therefore r(IJ) = r(I \cap J)$.
Also, $I \cap J \subseteq I$ and $I \cap J \subseteq J$
$\Longrightarrow r(I \cap J) \subseteq r(I)$ and $r(I \cap J) \subseteq r(J)$
$\Longrightarrow r(I \cap J) \subseteq r(I) \cap r(J)$
Let $x \in r(I) \cap r(J)$
$\Longrightarrow x \in r(I)$ and $x \in r(J)$
$\Longrightarrow x^n \in I$ and $x^m \in J$ for some $n, m > 0$.

$\implies x^{nm} \in I$ and $x^{mn} \in J$.
$\implies x^{mn} \in I \cap J$
$\implies x \in r(I \cap J)$
$\therefore r(I \cap J) = r(I) \cap r(J)$.
$\therefore r(IJ) = r(I \cap J) = r(I) \cap r(J)$. ■

Proposition 1.14. *The radical of an ideal I is the intersection of the prime ideals which contains I.*
PROOF. Exercise.

Note. We may define the radical $r(E)$ for any subset E of ring A. It is not ideal in general.

Example. If $A = Z, I = (m)$, let $p_i (1 \leq i \leq r)$ be the distinct prime divisors of m, then find $r(I)$.
Solution. We know that $r(I) = r((m))$.
$\implies r(I) = (p_1 \cdot p_2 \cdots p_r)$
$\implies r(I) = \cap_{i=1}^{r} p_r$.

Proposition. *Let I, J be ideals in a ring A such that $r(I), r(J)$ are coprime. Then I, J are coprime.*
PROOF. Let I and J are ideals of ring A and $r(I), r(J)$ are coprime ideals.
$\implies r(I) + r(J) = (1)$.
Consider, $r(I + J) = r(r(I) + r(J))$
$\implies r(I + J) = r(1) = (1)$
$\implies I + J = 1$. ■

EXTENSION and CONTRACTION

Let $f : A \to B$ be a ring homomorphism. If I is an ideal in A, then the set $f(I)$ is not necessarily an ideal in B. We define the Extension I^e of I to be the ideal $B(f(I))$ that is ideal generated by $f(I)$ in B. Then $I^e = \{\sum y_i f(x_i) / y_i \in B \text{ and } x_i \in I\}$.
If J is ideal in B, then $f^{-1}(J)$ is always an ideal in A, called the contraction J^c.
If I is prime ideal in A, then I^e need not be prime in B.
Counter Examples: 1. $f : Z \to Q, I \neq 0$, then $I^e = Q$, which is not prime ideal.
2. Consider the identity mapping $f : Z \to Z[i]$, then (2) is prime ideal in Z but $(2)^e$ is not prime ideal.
Because $(1 + i)(1 - i) = 2 \in (2)^e$ but none of $1 + i$ or $1 - i$ lies in $(2)^e$.
Therefore, I^e is not prime ideal.

Result 1. If $I_1 \subseteq I_2$ are ideals of ring A, then show that $I_1^e \subseteq I_2^e$.
PROOF. Let $y \in I_1^e$.
$\implies y = \sum b_i f(a_i)$ for some $a_i \in I_1$ and $b_i \in B$.
$\implies y = \sum b_i f(a_i)$ for some $a_i \in I_2$ and $b_i \in B$. $\quad \because a_i \in I_1 \subseteq I_2$
$\implies y \in I_2^e$.
$\therefore I_1^e \subseteq I_2^e$. ■

Result 2. If $J_1 \subseteq J_2$ are ideals of ring B then show that $J_2^c \subseteq J_1^c$.
PROOF. Exercise.

Proposition. *Let $f : A \to B$ be ring homomorphism and let I, J are ideals of A, B respectively then,*
(i) $I \subseteq I^{ec}, J^{ce} \subseteq J$.
(ii) $J^c = J^{cec}, I^e = I^{ece}$.

(iii) *If* C *is set of contraction ideals in* A *and if* E *is the set of extended ideals in* B*, then* $C = \{I/I^{ec} = I\}, E = \{J/J^{ce} = J\}$*, and* $I \mapsto I^e$ *is bijective map of* C *onto* E*, whose inverse is* $J \mapsto J^c$*.*

PROOF. (i) Let $x \in I$
$\Longrightarrow f(x) \in I^e$
$\Longrightarrow x = f^{-1}(f(x)) \in I^{ec}$
$\therefore I \subseteq I^{ec}$.
Suppose $y \in J^{ce}$
$\Longrightarrow f^{-1}(y) \in J^c$
$\Longrightarrow y = f(f^{-1}(y)) \in J$
$\therefore J^{ce} \subseteq J$.
(ii) By part (i) we have $I \subseteq I^{ec}$.
$\Longrightarrow I^e \subseteq (I^{ec})^e$. $\quad \because I_1 \subseteq I_2 \Rightarrow I_1^e \subseteq I_2^e$
$\Longrightarrow I^e \subseteq I^{ece}$.
Consider, $I^{ece} = (I^e)^{ce} \subseteq I^e$. $\quad \because J^{ce} \subseteq J$
$\Longrightarrow I^{ece} \subseteq I^e$.
$\therefore I^{ece} = I^e$.
Similarly we can show $J^c = J^{cec}$(Exercise).
(iii) We have $C = \{I/I^{ec} = I\}$ and $E = \{J/J^{ce} = J\}$.
Now define, $\phi : C \to E$ by $\phi(I) = I^e$.
Let I_1, I_2 be ideals in ring A.
Consider,

$$\begin{aligned} \phi(I_1) &= \phi(I_2) \\ \Longrightarrow I_1^e &= I_2^e \\ \Longrightarrow I_1^{ec} &= I_2^{ec} \\ \Longrightarrow I_1 &= I_2. \qquad \because I^{ec} = I, \quad \forall I \in C. \end{aligned}$$

$\Longrightarrow \phi$ is one-one mapping.
Also we have for each $J \in E$,

$$\begin{aligned} J &= J^{ce} \\ &= (J^c)^e \\ &= \phi(J^c) \end{aligned}$$

$\Longrightarrow \phi$ is onto.
Let $\psi : E \to C$ be mapping defined by $\psi(J) = J^c$.
Consider,

$$\begin{aligned} (\psi \circ \phi)(I) &= \psi(\phi(I)) \\ &= \psi(I^e) \\ &= (I^e)^c \\ &= I. \qquad \because I \in C \Longrightarrow I^{ec} = I. \end{aligned}$$

$\Longrightarrow (\psi \circ \phi)(I) = I, \quad \forall I \in E.$
$\Longrightarrow \phi = \psi^{-1}$. ■

Result. Let A be a ring and X be the set of all prime ideals of A. For each subset E of A, let $V(E)$ denote the set of all prime ideals in A containing E. Prove that

(i) If I is ideal generated by E then $V(E) = V(I) = V(r(I))$.
(ii) $V(0) = X, V(1) = \phi$.
(iii) If $(E_i)_{i\in\Delta}$ is any family of subsets of A, then $V(\cup_{i\in\Delta}E_i) = \cap_{i\in\Delta}V(E_i)$.
(iv) $V(I \cap J) = V(IJ) = V(I) \cup V(J)$ for any ideals I, J of A.
PROOF. We have given $X = \{P/P$ is prime ideal of ring $A\}$ and
$V(E) = \{P/E \subseteq P -$ is prime ideal of ring $A\}$.
(i) Let $I = (E) \Longrightarrow E \subseteq I$.
$\Longrightarrow V(I) \subseteq V(E)$.
Because, if $P \in V(I) \Longrightarrow I \subseteq P$.
$\Longrightarrow E \subseteq I \subseteq P \Longrightarrow E \subseteq P$.
$\Longrightarrow P \in V(E)$.
Now consider, $P \in V(E)$.
$\Longrightarrow E \subseteq P$.
$\Longrightarrow (E) \subseteq P$. $\because (E)$ is smallest ideal which contains E.
$\Longrightarrow (E) = I \subseteq P$.
$\Longrightarrow P \in V(I)$.
$\therefore V(E) = V(I)$.
(ii) We know that every prime ideal P in ring A contains 0.
$\Longrightarrow V(0) = X$.
Also, none of prime ideal contains 1 $\Longrightarrow V(1) = \phi$.
(iii) To show: $V(\cup_{i\in\Delta}E_i) = \cap_{i\in\Delta}V(E_i)$.
If $(E_i)_{i\in\Delta}$ be any family of subsets of A.
We know that each $i \in \Delta, E_i \subseteq \cup_{i\in\Delta}E_i$.
$\Longrightarrow V(\cup_{i\in\Delta}E_i) \subseteq V(E_i), \quad \forall i \in \Delta$.
$\Longrightarrow V(\cup_{i\in\Delta}E_i) \subseteq \cap_{i\in\Delta}V(E_i)$.
Let $P \in \cap_{i\in\Delta}V(E_i)$.
$\Longrightarrow P \in V(E_i) \quad \forall i \in \Delta$.
$\Longrightarrow E_i \subseteq P, \quad \forall i \in \Delta$.
$\Longrightarrow \cup E_i \subseteq P, \quad \forall i \in \Delta$.
$\Longrightarrow P \in V(\cup_{i\in\Delta}E_i)$.
$\Longrightarrow \cap_{i\in\Delta}V(E_i) \subseteq V(\cup_{i\in\Delta}E_i)$
$\therefore V(\cup_{i\in\Delta}E_i) = \cap_{i\in\Delta}V(E_i)$.
(iv) To show: $V(I \cap J) = V(IJ) = V(I) \cup V(J)$ for any ideals I, J of A.
Let I and J be ideals of ring A.
Since $IJ \subset I \cap I \Longrightarrow V(I \cap J) \subseteq V(IJ)$.
Let $P \in V(IJ)$.
$\Longrightarrow IJ \subseteq P$.
$\Longrightarrow I \subseteq P$ or $J \subseteq P$. $\because P$ is prime ideal.
But $I \cap J \subseteq I$ and J.
$\Longrightarrow I \cap J \subseteq P$.
$\Longrightarrow P \in V(I \cap J)$.
$\therefore V(I \cap J) = V(IJ)$.
We know that $I \cap J \subseteq I \Longrightarrow V(I) \subseteq V(I \cap J)$.
Similarly, $I \cap J \subseteq J \Longrightarrow V(J) \subseteq V(I \cap J)$.
$\Longrightarrow V(I) \cup V(J) \subseteq V(I \cap J)$.

Let $P \in V(I \cap J) \Longrightarrow I \cap J \subseteq P$.
Claim: $I \subseteq P$ or $J \subseteq P$.
On contrary assume that $I \nsubseteq P$ and $J \nsubseteq P$.
Let $x \in I$ and $y \in J$ such that $xy \notin P$.
But $xy \in IJ \subseteq I \cap J \subseteq P$.
$\rightarrow\leftarrow$.
$\therefore$ Either $I \subseteq P$ or $J \subseteq P$.
$\Longrightarrow P \in V(I)$ or $P \in V(J)$.
$\Longrightarrow P \in V(I) \cup V(J)$.
$\Longrightarrow V(I \cap J) \subseteq V(I) \cup V(J)$.
$\therefore V(I \cap J) = V(I) \cup V(J)$. ■
$\therefore V(E)$ satisfies axioms for the closed sets in topological space. The resulting topology is called as Zariski topology. The topological space X is called the prime spectrum of A.
Result. Let J_i be family of subsets of ring A, then $\cap_{i\in\Delta} V(J_i) = V(\sum_{i\in\Delta} J_i)$.

PROOF. We know that, $J_i \subseteq \sum_{i\in\Delta} J_i, \quad \forall i$.
$\Longrightarrow V(\sum_{i\in\Delta} J_i) \subseteq V(J_i) \quad \forall i$.
$$\Longrightarrow V(\sum_{i\in\Delta} J_i) \subseteq \cap_{i\in\Delta} V(J_i). \tag{1}$$
Let $P \in \cap_{i\in\Delta} V(J_i)$.

$\Longrightarrow P \in V(J_i), \quad \forall i \in \Delta$.

$\Longrightarrow J_i \subseteq P \quad \forall i \in \Delta$.

$\Longrightarrow \sum_{i\in\Delta} J_i \subseteq P$.
$\Longrightarrow P \in V(\sum_{i\in\Delta} J_i)$.
$$\Longrightarrow \cap_{i\in\Delta} V(J_i) \subseteq V(\sum_{i\in\Delta} J_i). \tag{2}$$
From (1) and (2) $\cap_{i\in\Delta} V(J_i) = V(\sum_{i\in\Delta} J_i)$. ■
Result. For each $f \in A, V(f) = \{P \in \text{ Spec}(A)/f \in P\}$.
Let $X_f = \text{ Spec}(A) - V(f)$.
That is, $X_f = \{P \in \text{ Spec}(A)/f \notin P\}$ is open set.
For each $f \in A, X_f$ denote the complement of $V(f)$ in $X = \text{ Spec}(A)$. The set X_f are open. Show that they form a basis of open set for the Zariski topology and that
(i) $X_f \cap X_g = X_{fg}$;
(ii) $X_f = \phi$ if and only if f is nilpotent;
(iii) $X_f = X$ if and only if f is unit;
(iv) $X_f = X_g$ if and only if $r((f)) = r((g))$;
(v) X is quasi-compact;

PROOF. (i) Let $P \in X_f \cap X_g$.
$\Longleftrightarrow P \in X_f$ and $P \in X_g$.
$\Longleftrightarrow f \notin P$ and $g \notin P$.
$\Longleftrightarrow fg \notin P$. $\because P$ is prime ideal.
$\Longleftrightarrow P \in X_{fg}$.
$\therefore X_f \cap X_g = X_{fg}$.
(ii) Suppose $X_f = \phi$.
$\Longleftrightarrow$ Every prime ideal contains f.
$\Longleftrightarrow f \in \cap_{P-\text{Prime}} P = \Re(A)$.
$\Longleftrightarrow f$ is nilpotent.
$\therefore X_f = \phi \Longleftrightarrow f$ is nilpotent.
(iii) $X_f = X$.
$\Longleftrightarrow$ None of prime ideal contains f.
$\Longleftrightarrow (f) = A$.
$\Longleftrightarrow f$ is unit in A.
(iv) Suppose $X_f = X_g$.
To show: $r((f)) = r((g))$.
$X_f = X_g$.
$\Longleftrightarrow X - X_f = X - X_g$.
$\Longleftrightarrow V(f) = V(g)$.
$\Longleftrightarrow$ Every prime ideal P which contains f that also contains g.
Consider,

$$\begin{aligned} r((f)) &= \cap_{P-\text{Prime ideal and } f \in P} P \\ &= \cap_{P \in V(f)} P \\ &= \cap_{P \in V(g)} P \\ &= \cap_{P-\text{Prime ideal and } g \in P} P \\ &= r((g)) \end{aligned}$$

$\Longleftrightarrow r((f)) = r((g))$.
(v) To show: X is quasi-compact.
Let $X = \cup_{\alpha \in \Delta} X_{f_\alpha}$.
For any $P \in X \Longrightarrow P \in X_{f_\alpha}$ for some $\alpha \in \Delta$.
$\Longrightarrow f_\alpha \notin P$ for some $\alpha \in \Delta$.
Let $I = (f_{\alpha_1}, f_{\alpha_2}, ...)$, then I is a non-zero ideal of A.
If $I \neq A$ then there exists a prime ideal P such that $I \subseteq P$.
$\therefore f_\alpha \in P, \quad \forall \alpha \in \Delta$.
$\Longrightarrow P \notin X_{f_\alpha}, \quad \forall \alpha \in \Delta$.
$\rightarrow\leftarrow$.
$\therefore I = A$.
$\Longrightarrow 1 \in I = (f_{\alpha_1}, f_{\alpha_2}, ...)$.
$\Longrightarrow 1 = a_1 f_{\alpha_1} + a_2 f_{\alpha_2} + ... + a_n f_{\alpha_n}$ for some $a_i \in A$.
$\Longrightarrow 1 = \sum_{i=1}^{n} a_i f_i \in \sum_{i=1}^{n} (f_{\alpha_i})$.

$\implies V(1) = V(\sum_{i=1}^{n}(f_{\alpha_i}))$.
$\implies \phi = \cap_{i=1}^{n} V(f_{\alpha_i})$.
$\implies X - \phi = X - \cap_{i=1}^{n} V(f_{\alpha_i})$.
$\implies X = \cup_{i=1}^{n}(X - V(f_{\alpha_i}))$.
$\implies X = \cup_{i=1}^{n} X_{f_{\alpha_i}}$.
$\therefore X$ is compact. ■

Example 1. A topological space X is said to irreducible if $X \neq \phi$ and if every pair of non-empty open sets in X intersects, or equivalently if every non-empty open set is dense in X(X is irreducible iff X cannot be union of two closed sets). Show that Spec(A) is irreducible if and only if the nilradical of A is prime a prime ideal.

PROOF. Suppose X is irreducible.
On contrary assume that $\Re(A)$ is not prime ideal.
$\therefore \exists x, y \notin \Re(A)$ but $xy \in \Re(A)$.
Let $K_x = V((x))$ and $K_y = V((y))$.
Then K_x and K_y are closed sets in X.
Let $P \in X = \text{Spec}(A)$.
We know that $\Re(A) \subseteq P$ and $xy \in \Re(A)$.
$\implies xy \in P$.
$\implies x \in P$ or $y \in P$.
$\implies (x) \subseteq P$ or $(y) \subseteq P$.
$\implies P \in K_x$ or $P \in K_y$. $\implies P \in K_x \cup K_y$.
$\therefore X = K_x \cup K_y$.
Now it is remains to prove K_x and K_y are proper subsets of A.
Since $x \notin \Re(A) = \cap P$.
$\therefore \exists$ prime ideal P such that $x \notin P$.
$\implies P \notin K_x$.
$\therefore K_x \neq X$.
Similarly, $K_y \neq X$.
$\implies K_x$ and K_y are proper closed sets of X whose union is X.
$\rightarrow\leftarrow$. $\because X$ is irreducible.
$\therefore \Re(A)$ is prime ideal.
Conversely, suppose $\Re(A)$ is prime ideal.
To show: X is irreducible.
We shall prove the contrapositive statement.
That is, if X is reducible, then $\Re(A)$ is not prime ideal.
Suppose X is reducible.
To show: $\Re(A)$ is not prime ideal.
Since X is reducible $\implies X = V(I) \cup V(J)$, where $V(I), V(J) \neq X$.
$\implies X = V(I \cap J)$.
Let $P \in X$.
$\implies P \in V(I \cap J)$.
$\implies I \cap J \subseteq P, \quad \forall P \in X$.
$\implies I \cap J \subseteq \cap P = \Re(A)$.

Since, $V(I), V(J) \neq X$.
$\implies I \cap J \subset \Re(A)$.
But $IJ \subseteq I \cap J \subset \Re(A)$.
That is, $\exists x \in I - \Re(A)$ and $y \in J - \Re(A)$ such that $xy \in IJ \subset \Re(A)$.
$\therefore \Re(A)$ is not prime ideal. ■

Example 2. Let X be topological space.
(i) If Y is irreducible subspace of X, then the closure $\bar{Y}$ of Y in X is irreducible.
(ii) Every irreducible subspace of X is contained in a maximal irreducible subspace.
PROOF. (i) Let Y is irreducible subspace of X.
On the contrary assume that $\bar{Y}$ is not irreducible.
$\implies \bar{Y} = S \cup T$ for some proper closed sets T and S of $\bar{Y}$.
But we know that, $Y = Y \cap \bar{Y}$.
$\implies Y = (Y \cap S) \cup (Y \cap T)$.
Since S and T are closed subsets of $\bar{Y}$ and $\bar{Y} \subseteq X$.
$\implies Y \cap S$ and $Y \cap T$ are closed in Y.
It is remains to show $Y \cap S$ and $Y \cap T$ are proper subsets of Y.
If $Y \cap S = Y \implies Y \subseteq S$.
$\implies \bar{Y} = S \to\leftarrow$. $\because S$ is proper subset of $\bar{Y}$.
$\therefore Y \cap S$ and $Y \cap T$ are proper closed subsets of Y such that $Y = (Y \cap S) \cup (Y \cap T)$.
$\implies Y$ is reducible $\to\leftarrow$.
$\therefore \bar{Y}$ must be irreducible in X.
(ii) Let Y be a irreducible subspace of X.
$\sum = \{Z/Z$ is irreducble and contains $Y\}$.
Then $\sum \neq \phi$. $\because Y \in \sum$.
Then $\sum$ is poset under set inclusion.
Let $C : Z_1 \subseteq Z_2 \subseteq ...$ be any chain in $\sum$.
Take, $Z = \cup Z_i$, where each $Z_i \in \sum$.
Claim: Z is irreducible.
On contrary assume that Z is not irreducible.
$\implies Z = S \cup T$ for some proper closed subsets S and T of Z.
Then,

$$\begin{aligned} Z_1 &= Z_1 \cap Z \\ &= Z_1 \cap (S \cup T) \\ &= (Z_1 \cap S) \cup (Z_1 \cap T) \end{aligned}$$

$\implies Z_1$ is union of two proper closed subsets of Z_1.
$\implies Z_1$ is not irreducible $\to\leftarrow$.
$\therefore Z$ must be irreducible.
Hence every chain in $\sum$ has upper bound in $\sum$.
Therefore, by Zorn's lemma $\sum$ has maximal element.
Such maximal irreducible subspace is called as irreducible component. ■

♣♣♣

CHAPTER 2
Modules

MODULES AND MODULE HOMOMORPHISMS

Definition. Let A be a ring. An A-module is an abelian group M on which A acts linearly; more precisely, it is pair (M, μ), where M is abelian group and $\mu : A \times M \to M$ is mapping defined by $\mu(a, x) = ax$ and satisfies following axioms:
(i) $\mu((a, x + y)) = a(x + y) = ax + ay$.
(ii) $\mu((a + b), x) = (a + b)x = ax + bx$.
(iii) $\mu(ab, x) = (ab)x = a(bx)$.
(iv) $1x = x$, for all $x, y \in M$ and $a, b \in A$.
Examples. (1) An ideal I of ring A is an A-module. In particular A itself is an $A-$module.
(2) If A is field F, then A-module = F-vector space.
(3) $A = \mathbb{Z}$, then $\mathbb{Z}-$module = abelian group.
(4) $A = F[x]$, where F is field; an A-module is a K-vector space with linear transformation.
Definition. Let M, N be A-modules. A mapping $f : M \to N$ is an A-module homomorphism (or A-linear) if
(i) $f(x + y) = f(x) + f(y)$.
(ii)$f(ax) = af(x)$. for all $x, y \in M$ and $a \in A$.
If A is field, an A-module homomorphism is the same thing as a linear transformation of vector spaces.
The composition of A-modules homomorphisms is again an A-module homomorphism.
The set of all A-module homomorphism from M to N can be turned into and $A-$module as follows: we define addition and multiplication by the rules
$(f + g)(x) = f(x) + g(x)$,
$(af)(x) = af(x)$, for all $a \in A$ and $x \in M$.
which is denoted by $\mathrm{Hom}_A(A, M)$ or just by $\mathrm{Hom}(A, M)$.

SUBMODULES AND QUOTIENT MODULES

A submodule M' of M is subgroup of M which is closed under multiplication by elements of A.
That is, M' is submodule of M is it satisfies following properties:
(1) For $x, y \in M' \Longrightarrow x - y \in M'$.
(2) $ax \in M'$ for all $a \in A$ and $x \in M'$.
Note. The submodule of A over an A-module are the ideals of A.
Let M' be a submodule of A-module M, then
$M/M' = \{m + M'/m \in M\}$ is module over A called as quotient module.
PROOF. Clearly M/M' is additive abelian group of A.
Let $a, b \in A$ and $\bar{x}, \bar{y} \in M/M'$.

$$\begin{aligned} a(\bar{x}+\bar{y}) &= a(x+M'+y+M') \\ &= a((x+y)+M') \\ &= a(x+y)+M' \\ &= (ax+ay)+M' \\ &= ax+M'+ay+M' \\ &= a(x+M')+a(y+M') \\ &= a\bar{x}+a\bar{y} \end{aligned}$$

$$\begin{aligned} (a+b)\bar{x} &= (a+b)(x+M') \\ &= (a+b)x+M' \\ &= (ax+bx)+M' \\ &= ax+M'+bx+M' \\ &= a(x+M')+b(x+M') \\ &= a\bar{x}+b\bar{y} \end{aligned}$$

$$\begin{aligned} a(b\bar{x}) &= a(b(x+M')) \\ &= a(bx+M') \\ &= (ab)x+M' \\ &= (ab)\bar{x} \end{aligned}$$

and $1 \cdot \bar{x} = \bar{x}$
$\therefore M/M'$ is module over A called quotient module. ■
Note. (1) There is a one-to-one order-preserving correspondence between submodules of M containing M' and submodules of M/M'.
(2) Submodule of M/M' is of the form M_1/M', where M_1 is submodule of M containing M'.
Let $f : M \to N$ be an module homomorphism then

$$\ker f = \{x \in M / f(x) = 0\}$$

and is a submoule of M.
The image set of f is the set

$$\mathrm{Im}(f) = f(M) = \{y \in N / f(x) = y, x \in M\}$$

is an submodule of N.
The cokernel of f is

$$\mathrm{Coker}(f) = N/\mathrm{Im}(f)$$

which is quotient module of N.
Result. Let $f : M \to N$ be a ring homomorphism and M' be submodule of A-module M such that $M' \subseteq \ker f$, then the mapping $\bar{f} : M/M' \to N$, defined by $\bar{f}(\bar{x}) = f(x)$ is homomorphism induced by f with $\ker \bar{f} = \ker f/M'$.
PROOF. To show: $\bar{f}$ is homomorphism.

Let $\bar{x} = x + M', \bar{y} = y + M' \in M/M'$ and $a \in A$.
Consider,

$$\begin{aligned}
\bar{f}(\bar{x} + a\bar{y}) &= \bar{f}((x + M') + a(y + M')) \\
&= \bar{f}((x + ay) + M') \\
&= \bar{f}(\overline{x + ay}) \\
&= f(x + ay) \\
&= f(x) + af(y) \qquad \because f \text{ is module homomorphism.} \\
&= \bar{f}(\bar{x}) + a\bar{f}(\bar{y})
\end{aligned}$$

$\therefore \bar{f}(\bar{x} + a\bar{y}) = \bar{f}(\bar{x}) + a\bar{f}(\bar{y})$.
$\Longrightarrow \bar{f}$ is module homomorphism.
Now consider,

$$\begin{aligned}
\ker \bar{f} &= \left\{\bar{x} \in M/M' : \bar{f}(\bar{x}) = 0\right\} \\
&= \{x + M' \in M/M' : f(x) = 0\} \\
&= \{x + M' \in M/M' : x \in \ker f\} \\
&= \ker f/M'
\end{aligned}$$

$\therefore \ker \bar{f} = \ker f/M'$. ■

OPERATIONS ON SUBMODULES
Let M be an A-module and let $(M_i)_{i\in\Delta}$ be a family of submodules of M. Their sum $\sum M_i$ is the set of all finite sums $\sum x_i$ where $x_i \in M_i$ for all $i \in \Delta$ and almost all the x_i are zero.
$\sum M_i$ is smallest submodule of M which contains all the M_i.
The intersection $\cap M_i$ is again submodule of M. Thus the submodule of M form a complete lattice with respect to inclusion.
Proposition. (i) If $L \supseteq M \supseteq N$ are A-modules, then
$(L/N)/(M/N) \cong L/M$.
(ii) If M_1, M_2 are submodules of M, then
$(M_1 + M_2)/M_1 \cong M_2/(M_1 \cap M_2)$.
PROOF. (i) Define the mapping $\theta : L/N \to L/M$ by $\theta(x + N) = x + M$.
Let $\bar{x} = x + N, \bar{y} = y + N \in L/N$ and $a \in A$.
Consider,

$$\begin{aligned}
\theta(\bar{x} + a\bar{y}) &= \theta((x + N) + a(y + N)) \\
&= \theta((x + ay) + N) \\
&= (x + ay) + M \\
&= (x + M) + (ay + M) \\
&= (x + M) + a(y + M) \\
&= \theta(x + N) + a\theta(y + N) \\
&= \theta(\bar{x}) + a\theta(\bar{y})
\end{aligned}$$

Therefore, θ is module homomorphism.
Also, for each $x + N \in L/N$ there exists $x + M \in L/M$ such that $\theta(x + N) = x + M$.
$\Longrightarrow \theta$ is onto.
Consider,

$$\begin{aligned}\ker\theta &= \{\bar{x}\in L/N : \theta(\bar{x})=\bar{0}\}\\ &= \{x+N\in L/N : \theta(x+N)=M\}\\ &= \{x+N\in L/N : x+M=M\}\\ &= \{x+N\in L/N : x\in M\}\\ &= M/N\end{aligned}$$

$\therefore \theta$ is module homomorphism L/N onto L/M with kernel M/N.
$\implies (L/N)/(M/N)\cong (L/M)$.
(ii) Define $g : M_2 \to (M_1+M_2)/M_1$ by $g(x)=x+M_1$.
Let $x, y\in M_2$ and $a\in A$.
Consider,

$$\begin{aligned}g(x+ay) &= (x+ay)+M_1\\ &= x+M_1+ay+M_1\\ &= (x+M_1)+a(y+M_1)\\ &= g(x)+ag(y)\end{aligned}$$

$\therefore g$ is module homomorphism.
Also, for each $x+M_1\in (M_1+M_2)/M_1$, there exists $x\in M_2$ such that $g(x)=x+M_1$.
$\therefore g$ is onto.
Now consider,

$$\begin{aligned}\ker g &= \{x\in M_2 : g(x)=\bar{0}\}\\ &= \{x\in M_2 : x+M_1=M_1\}\\ &= \{x\in M_2 : x\in M_1\}\\ &= M_1\cap M_2\end{aligned}$$

$\therefore g$ is module homomorphism from M_2 onto $(M_1+M_2)/M_1$ with kernel $M_1\cap M_2$.
$\therefore M_2/(M_1\cap M_2)\cong (M_1+M_2)/M_1$. ■
We cannot in general define product of two submodules, but we can define product IM, where I is an ideal and M an A-module.

$IM = \left\{\sum_{\text{finite}} a_i x_i : a_i\in I, x_i\in M\right\}$.
Let $x, y\in IM \implies x=\sum_{\text{finite}} a_i x_i, \quad y=\sum_{\text{finite}} b_i y_i$ for some $a_i, b_i\in I$ and $x_i, y_i\in M$.
Then, $x-y=\sum_{i=1}^{n} a_i x_i - \sum_{i=1}^{m} b_i y_i \in IM$.
Also, for $a\in A$ and $x\in IM$.

$$\begin{aligned}ax &= a(\sum_{i=1}^{n} a_i x_i)\\ &= \sum_{i=1}^{n}(aa_i)x_i\in IM\end{aligned}$$

$\therefore IM$ is submodule of M.
If N, P are submodules of M, then $(N : P) = \{x \in A : xP \subseteq N\}$ is ideal of A.
In particular $(0 : M) = \{x \in A : xM = 0\} = Ann(M)$ is ideal of A called as annihilator of M.
Any $A-$module M is said to be faithful if $Ann(M) = 0$.
Result. Suppose M be an $A-$module with $Ann(M) \neq 0$ and I be an ideal A such that $I \subseteq Ann(M)$ then M is faithful module over A/I.
Exercise. Prove that
(i) $Ann(M + N) = Ann(M) \cap Ann(N)$.
(ii) $(N : P) = Ann(\frac{N+P}{N})$.
PROOF. (i) We know that $M + N = \{x + y/x \in M, y \in N\}$.
$\therefore M \subseteq M + N$ and $N \subseteq M + N$.
$\implies Ann(M + N) \subseteq Ann(M)$ and $Ann(M + N) \subseteq Ann(N)$.
$\implies Ann(M + N) \subseteq Ann(M) \cap Ann(N)$.
Let $a \in Ann(M) \cap Ann(N)$.
$\implies a \in Ann(M)$ and $a \in Ann(N)$.
$\implies ax = 0, \quad \forall x \in M$ and $ay = 0, \quad \forall y \in N$.
Now consider, $a(x + y) = ax + ay = 0, \quad \forall x + y \in M + N$.
$\implies a \in Ann(M + N)$.
$\implies Ann(M) \cap Ann(N) \subseteq Ann(M + N)$.
$\therefore Ann(M + N) = Ann(M) \cap Ann(N)$.
(ii) Let $a \in (N : P) \implies aP \subseteq N$.
$\implies ax \in N, \quad \forall x \in P$ and let $y + N \in \frac{N+P}{N}$ for some $y \in P$.
Consider, $a(y + N) = ay + N = \bar{0}, \quad \forall y + N \in \frac{N+P}{N}$. $\quad \because ay \in N$.
$\implies a \in Ann(\frac{N+P}{N})$.
$\implies (N : P) \subseteq Ann(\frac{N+P}{N})$.
Let $b \in Ann(\frac{N+P}{N})$.
$\implies b(y + N) = \bar{0} = N$.
$\implies by + N = N$.
$\implies by \in N, \quad \forall y \in P$.
$\implies bP \subseteq N$.
$\implies b \in (N : P)$.
$\implies Ann(\frac{N+P}{N}) \subseteq (N : P)$.
$\therefore (N : P) = Ann(\frac{N+P}{N})$. ∎

DIRECT SUM AND PRODUCTS
If M and N are $A-$modules, their direct sum $M \oplus N = \{(x, y)/x \in M, y \in N\}$. This is an $A-$module with respect to addition and multiplication:
$(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2)$
$a(x, y) = (ax, ay)$.
More generally $\{M_i\}_{i\in\Delta}$ is collection of $A-$modules then the direct sum of $M_i's$ is given by $\oplus_{i\in\Delta} M_i = (x_1, x_2, ...)$ such that $x_i \in M_i$ and $x_i \neq 0$ for all but finitely many i.
If we drop the condition on number of $x_i's$ are non-zero we have direct product $\prod_{i=1}^{n} M_i$.
Therefore, direct sum and direct product are same if the index set Δ is finite, but not

otherwise, in general.

Suppose that the ring A is a direct product $\prod_{i=1}^{n} A_i$. Then the set I_i of all elements of A of the form $(0, 0, ..., 0, a_i, 0, ..., 0)$ with $a_i \in A_i$ is an ideal of A but not subring.
A ring A considered as an $A-$module then it's ideal are submodules of A. Hence A is direct sum of A modules I_i.
FINITELY GENERATED MODULES
A free $A-$module is one which is isomorphic to an $A-$module of the form $\oplus_{i\in\Delta} M_i$, where $M_i \cong A$ (as an $A-$module).
A finitely generated free $A-$module is isomorphic to $A \oplus A \oplus ... \oplus A$(n-times) which is denoted by A^n.
Proposition. *M is a finitely generated $A-$module if and only if M is isomorphic to a quotient of A^n for some integer $n > 0$.*
PROOF. Suppose M is finitely generated $A-$module.
$\therefore M =< x_1, x_2, ..., x_n >$.
Define, $\phi : A^n \to M$ by $\phi((a_1, a_2, ..., a_n)) = a_1x_1 + a_2x_2 + ... + a_nx_n$.
Now for any $a, b \in A^n \implies a = (a_1, a_2, ..., a_n), b = (b_1, b_2, ..., b_n)$ and $r \in A$.
Consider,

$$\begin{aligned}
\phi(a + rb) &= \phi((a_1, a_2, ..., a_n) + r(b_1, b_2, ..., b_n)) \\
&= \phi((a_1 + rb_1, a_2 + rb_2, ..., a_n + rb_n) \\
&= (a_1 + rb_1)x_1 + (a_2 + rb_2)x_2 + ... + (a_n + rb_n)x_n \\
&= a_1x_1 + rb_1x_1 + a_2x_2 + rb_2x_2 + ... + a_nx_n + rb_nx_n \\
&= (a_1x_1 + a_2x_2 + ... + a_nx_n) + r(b_1x_1 + b_2x_2 + ... + b_nx_n) \\
&= \phi((a_1, a_2, ..., a_n)) + r\phi((b_1, b_2, ..., b_n)) \\
&= \phi(a) + r\phi(b)
\end{aligned}$$

$\implies \phi$ is module homomorphism.
For each $x \in M \implies x = a_1x_1 + a_2x_2 + ... + a_nx_n$ then $(a_1, a_2, ..., a_n) \in A^n$ such that $\phi((a_1, a_2, ..., a_n)) = a_1x_1 + a_2x_2 + ... + a_nx_n = x$.
$\implies \phi$ is onto.
$\implies \phi$ is onto module homomorphism.
$\therefore A^n/\ker\phi \cong M$.
Conversely, suppose $M \cong A^n/I$ for some ideal I of A.
If $\bar{x} \in A^n/I$ then,

$$\begin{aligned}
\bar{x} &= (x_1, x_2, ...x_n) + I \\
&= (x_1(1, 0, ..., 0) + x_2(0, 1, 0, ..., 0) + ... + x_n(0, 0, ..., 1)) + I \\
&= (x_1e_1 + x_2e_2 + ... + x_ne_n) + I \\
&= x_1(e_1 + I) + x_2(e_2 + I) + ... + x_n(e_n + I) \\
&= x_1\bar{e_1} + x_2\bar{e_2} + ... + x_n\bar{e_n}
\end{aligned}$$

$\implies \{\bar{e_1}, \bar{e_2}, ..., \bar{e_n}\}$ generates A^n/I.
Let $\phi : A^n/I \to M$ be isomorphism and $\phi(\bar{e_1}) = x_1, \phi(\bar{e_2}) = x_2, ..., \phi(\bar{e_n}) = x_n$.
$\therefore \{\phi(\bar{e_1}), \phi(\bar{e_2}), ..., \phi(\bar{e_n})\} = \{x_1, x_2, ..., x_n\}$ is generating set of M.

Because for each $x \in M$.

$$\begin{aligned} x &= \phi(\bar{y}) \text{ for some } \bar{y} \in A^n/I \implies \bar{y} = a_1\bar{e_1} + a_2\bar{e_2} + ... + a_n\bar{e_n} \text{ for some } a_1, a_2, ...a_n \in A. \\ &= \phi(a_1\bar{e_1} + a_2\bar{e_2} + ... + a_n\bar{e_n}) \\ &= a_1\phi(\bar{e_1}) + a_2\phi(\bar{e_2}) + ... + a_n\phi(\bar{e_n}) \\ &= a_1x_1 + a_2x_2 + ... + a_nx_n \end{aligned}$$

$\therefore M =< x_1, x_2, ..., x_n >$. ■

Proposition. *Let M be finitely generated $A-$module, let I be an ideal of A, and let ϕ be an $A-$module endomorphism of M such that $\phi(M) \subseteq IM$. Then ϕ satisfies an equation of the form*
$\phi^n + a_1\phi^{n-1} + ... + a_n = 0$ *where* $a_i \in A$.
PROOF. Let M is finitely generated $A-$module.
Let $M =< x_1, x_2, ..., x_n >$.
Since $\phi(M) \subseteq IM$.
$\implies \phi(x_i) = \sum_{j=1}^{n} a_{ij}x_j, \quad \forall 1 \leq i \leq n, a_{ij} \in I$ for all i, j.
This is system of n equations in n unknowns can be written as:
$\sum_{j=1}^{n}(\delta_{ij}\phi - a_{ij})x_j = 0.$
Multiplying both side by adjoint of $\delta_{ij}\phi - a_{ij}$ we get.
adj$(\delta_{ij}\phi - a_{ij})(\delta_{ij}\phi - a_{ij})x_j = 0.$
$\implies \det(\delta_{ij}\phi - a_{ij}) = 0.$ $\because \{x_1, x_2, ..., x_n\}$ generates M.
Expanding this determinant we get:
$\phi^n + a_1\phi^{n-1} + ... + a_n = 0.$ ■

Proposition. (Nakayama's Lemma). *Let M be a finitely generated $A-$module and I be an ideal of A contained in Joconson radical $\mathcal{J}$ of A. Then $IM = M \implies M = 0$.*
PROOF. On contrary assume that $M \neq 0$.
Let $\{x_1, x_2, ..., x_n\}$ be minimal generating set of M.
We have given $IM = M$.
For $x_1 \in M$ and $a_{ij} \in A, 1 \leq i, j \leq n$.

$$\begin{aligned} x_1 &= a_{11}x_1 + a_{12}x_2 + ... + a_{1n}x_n \\ &. \\ &. \\ &. \\ x_n &= a_{n1}x_1 + a_{n2}x_2 + ... + a_{nn}x_n \end{aligned}$$

Since, $x_1 = a_{11}x_1 + a_{12}x_2 + ... + a_{1n}x_n$.
$\implies (1 - a_{11})x_1 - a_{12}x_2 - ... - a_{1n}x_n = 0.$
Also, $a_{1i} \in I \subseteq \mathcal{J}$.
$\implies 1 - a_{11}$ is unit in A.
$\implies x_1 = (1 - a_{11})^{-1}a_{12}x_2 + (1 - a_{11})^{-1}a_{13}x_3 + ... + (1 - a_{11})^{-1}a_{1n}x_n.$
$\implies \{x_2, x_3, ..., x_n\}$ generates M.
$\longrightarrow\!\longleftarrow$ to minimality of generating set M.
$\therefore M = 0.$ ■

Corollary. *Let M be a finitely generated $A-$module, N a submodule of $M, I \subseteq \mathcal{J}$ an ideal. Then $M = IM + N \Longrightarrow M = N$.*
PROOF. Since $N \subseteq M + N$, hence it is submodule of $M + N$.
$\Longrightarrow M + N$ is an $A-$module also M is finitely generated hence M/N is also finitely generated.
Now consider,

$$\begin{aligned} I(M/N) &= IM/N \\ &= (IM + N)/N \\ &= M/N \end{aligned}$$

$\Longrightarrow I(M/N) = M/N$, where $I \subseteq \mathcal{J}$.
Therefore by previous proposition(applying previous proposition on M/N).
$M/N \equiv 0$.
$\Longrightarrow M = N$. ■
Result. Let A be a local ring with maximal ideal I and M be a finitely generated $A-$module. Then show that M/IM is annihilated by I.
PROOF. Since I is maximal ideal and M is $A-$module.
$\Longrightarrow IM$ is submodule of M.
Also, M/IM is $A-$module.
If $x + IM \in M/IM$ and $a \in I$
Then, $a(x + IM) = ax + IM = IM$.
$\Longrightarrow a \in \text{ Ann}(M/IM)$.
$\Longrightarrow I \subseteq \text{ Ann}(M/IM)$.
$\therefore M = \text{ Ann}(M/IM)$. $\because I$ is maximal ideal in A.
$\Longrightarrow M/IM$ annihilates by I. ■
Note. Let A be local ring with maximal ideal I, then $F = A/I$ its residue field. Then M/IM forms vector space over field F.
Proposition. *Let A be local ring with maximal ideal I. If $\{x_1, x_2, ..., x_n\}$ be elements of M whose images in M/IM form a basis of vector space M/IM, then show that x_i generates M.*
PROOF. Let N be submodule of M generated by $\{x_1, x_2, ..., x_n\}$.
Suppose $f : N \to M$ defined by $f(x) = x, \quad \forall x \in N$ and $g : M \to M/IM$ defined by $g(y) = y + IM, \quad \forall y \in M$.
Then $g \circ f : N \to M/IM$ is onto mapping.
Because for any $\bar{y} = y + IM \in M/IM$.
$\Longrightarrow \bar{y} = (a_1 + I)x_1 + (a_2 + I)x_2 + ... + (a_n + I)x_n$, for some $a_1 + I, a_2 + I, ..., a_n + I \in A/I$.
Take $z = a_1x_1 + a_2x_2 + ... + a_nx_n \in N$.
Then,

$$\begin{aligned} (g \circ f)(z) &= g(f(z)) \\ &= g(z) \\ &= z + IM \\ &= (a_1x_1 + a_2x_2 + ... + a_nx_n) + IM \\ &= a_1x_1 + IM + a_2x_2 + IM + ... + a_nx_n + IM \\ &= a_1(x_1 + IM) + a_2(x_2 + IM) + ... + a_n(x_n + IM) \\ &= (a_1 + I)x_1 + (a_2 + I)x_2 + ... + (a_n + I)x_n \\ &= \bar{y} \end{aligned}$$

Now let $\phi : M \to M/IM$ be natural mapping defined by $\phi(m) = m + IM$,
then $\phi(N) = N/IM = (N + IM)/IM$. $\because IM/N = (N + IM)/N$ for any ideal I.
$\implies M/IM = (N + IM)/IM$.
$\implies \frac{M/IM}{(N+IM)/IM} = 0$.
$\implies M(N + IM) = 0$.
$\implies M = N + IM$.
$\therefore N + IM = M$.
$\therefore$ By previous corollary of Nakayama's lemma.
$\therefore N = M$. ■

EXACT SEQUENCES

Definition. A sequence of $A-$modules and $A-$homomorphisms

$$\cdots \to M_{i-1} \xrightarrow{f_i} M_i \xrightarrow{f_{i+1}} M_{i+1} \to \cdots$$

is said to be exact at M_i if $\mathrm{Im}(f_i) = \ker(f_{i+1})$.
A sequence is exact if it is exact at each M_i.

Example 1. $0 \to M' \xrightarrow{f} M$ is exact $\iff f$ is injective.

Example 2. $M \xrightarrow{g} M'' \to 0$ is exact $\iff g$ is surjective.

Example 3. $0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ is exact $\iff f$ is injective, g is surjective and g induces an isomorphism of $\mathrm{Coker}(f) = M/f(M')$ onto M''.

♣♣♣

CHAPTER 3

Integral Dependence and Valuations

Integral Dependence

Definition. Let B be a ring and A be a subring of B. An element x of B is said to be integral over A if x if x is a root of monic polynomial with coefficients in A, that is x satisfies an equation of the form.

$$x^n + a_1x^{n-1} + ... + a_n \quad = \quad 0$$

where, a_i are elements of A.

Example 1. Every element of ring A is integral over A.

Example 2. $A = \mathbb{Z}, B = \mathbb{Q}$. If a rational number $x = r/s$ is integral over $\mathbb{Z}$, where r, s have no common factor.

$\Longrightarrow x$ satisfies equation of the form $x^n + a_1x^{n-1} + ... + a_{n-1}x + a_n = 0$.

$\Longrightarrow (r/s)^n + a_1(r/s)^{n-1} + ... + a_{n-1}(r/s) + a_n = 0$.

Multiplying both side by s^n we get,

$r^n + a_1r^{n-1}s + ... + a_ns^n = 0$.

$\Longrightarrow r^n = -a_1r^{n-1}s - ... - a_ns^n$.

$\Longrightarrow r^n = (-a_1r^{n-1} - ... - a_ns^{n-1})s$.

$\Longrightarrow s$ divides r^n.

$\Longrightarrow s = \pm 1$.

$\Longrightarrow x \in \mathbb{Z}$.

$\Longrightarrow$ Element in $\mathbb{Q}$ is integral over $\mathbb{Z}$, if it is integer.

Example 3. $A = k[x^2], B = k[x]$ then $x \in B$ in integral over A.

Because it satisfies equation of the form $y^2 - x^2$.

Example 4. Let R be a ring and G be a finite subgroups of Automorphisms(Isomorphism from R to R) of R.

Let $A = R^G = \{a \in R : g(a) = a, \quad \forall g \in G\}$ and $a \in R$.

Let $P(y) = \prod_{g \in G}(y - g(a))$.

Every element of R is integral over R^G.

Proposition. *Let $A \subseteq B$ be rings, then the followings are equivalent:*

(i) $x \in B$ *is integral over* A*;*

(ii) $A[x]$ *is a finitely generated* $A-$*module;*

(iii) $A[x]$ *is contained in a subring* C *of* B *such that* C *is finitely generated* $A-$*module;*

(iv) *There exists a faithful* $A[x]-$*module* M *which is finitely generated as an* $A-$*module.*

PROOF. (i) $\Longrightarrow$ (ii).

Let $x \in B$ is integral over A.

$\Longrightarrow x$ satisfies equation of the form $x^n + a_1x^{n-1} + ... + a_n = 0$ for some $a_i \in A$.

$\Longrightarrow x^n = -a_1x^{n-1} - ... - a_n$.

$\Longrightarrow A[x]$ is generated by $\{1, x, ..., x^{n-1}\}$.

$\Longrightarrow A[x]$ is finitely generated.

(ii) $\Longrightarrow$ (iii)

Suppose $A[x]$ is finitely generated.

Take $C = A[x]$.
(iii) $\implies$ (iv)
Suppose, $A[x]$ is contained in a subring C of B such that C is finitely generated $A-$module.
Take $C = M$, then it is faithful $A[x]-$module.
Because for any $y \in A[x]$, $yC = 0 \implies y \cdot 1 = 0 \implies y = 0$.
(iv) $\implies$ (i)
Suppose, there exists a faithful $A[x]-$module M which is finitely generated as an $A-$module.
Consider the map $\phi : M \to M$ defined by $\phi(m) = xm$.
$\implies \phi(M) \subseteq M \implies xM \subseteq M$.
Suppose M is generated by $\{m_1, m_2, ..., m_n\}$ over A.
Then $\phi(m_1) = xm_1$.
$\implies \phi(m_1) = \sum_{j=1}^{n} a_{1j}m_j$.
$\implies \phi(m_1) - \sum_{j=1}^{n} a_{1j}m_j = 0$.
$\implies [\phi\delta_{1j} - a_{1j}][m_1, m_2, ..., m_n]^{\perp} = 0$.
$\therefore [\phi\delta_{ij} - a_{ij}][m_1, m_2, ..., m_n]^{\perp} = 0$.
Multiplying both side by adjoint of matrix of $[\phi\delta_{ij} - a_{ij}]$ we get,
$\det[\phi\delta_{ij} - a_{ij}](m_i) = 0, \quad \forall 1 \leq i \leq n$.
$\implies (\phi^n + a_1\phi^{n-1} + ... + a_n)(m_i) = 0, \quad \forall 1 \leq i \leq n$.
$\implies (x^n + a_1x^{n-1} + ... + a_n)m_i = 0, \quad \forall 1 \leq i \leq n$.
$\implies x^n + a_1x^{n-1} + ... + a_n \in Ann(M) = (0)$. $\because M$ is faithful $A-$module.
$\implies x^n + a_1x^{n-1} + ... + a_n = 0$.
$\implies x \in B$ is integral over A. ■
Note. If N is finitely generated $B-$module and B is finitely generated $A-$module, then N is finitely generated $A-$module.
Corollary. *Let $x_i (1 \leq i \leq n)$ be elements of B, each integral over A. Then the ring $A[x_1, x_2, ..., x_n]$ is a finitely-generated $A-$module.*
PROOF. We will prove this corollary by induction on n.
For $n = 1$, that is if $x_1 \in B$ is integral over A then $A[x_1]$ is finitely generated. $\because$ By previous preposition.
Assume that the result is true for $n - 1$ elements.
That is, If $x_1, x_2, ..., x_{n-1} \in B$ are integral over B, then $A_{n-1} = A[x_1, x_2, ..., x_{n-1}]$ is finitely generated $A-$module.
To prove: The result is true for n elements.
That is to prove, If $x_1, x_2, ..., x_n \in B$ are integral over B, then $A_n = A[x_1, x_2, ..., x_n]$ is finitely generated $A-$module.
Suppose, $x_1, x_2, ..., x_n \in B$ are integral over B.
Then $A_n = A_{n-1}[x_n]$ is finitely generated $A_{n-1}-$module.
$\therefore A_n$ is finitely generated $A-$module.
Because, If N is finitely generated $B-$module and B is finitely generated $A-$module, then N is finitely generated $A-$module. ■
Corollary. *The set C of elements of B which are integral over A is subring of B con-*

taining A.
PROOF. Exercise.
Definition. The ring C of elements of B which are integral over A is called the integral closure of A in B. If $C = A$ then A is said to be integrally closed in B.
Definition. Let $f : A \to B$ be a ring homomorphism. If $a \in A$ and $b \in B$, define a product $ab = f(a)b$ such that, with respect to this multiplication B forms $A-$module structure. The ring B which has both ring and $A-$module structure is called as an $A-$algebra.
Remark. Let $f : A \to B$ be a ring homomorphism, so that B is an $A-$algebra. Then f is said to be integral, and B is said to be an integral $A-$algebra, if B is integral over its subring $f(A)$.
Corollary. *If $A \subseteq B \subseteq C$ are rings and if B is integral over A, and C is integral over B, then C is integral over A(transitivity of integral dependence).*
PROOF. Let $x \in C$ in integral over B.
$\implies x^n + b_1x^{n-1} + ... + b_n = 0 \qquad (b_i \in B)$.
$\implies B' = [b_1, b_2, ..., b_n]$ is a finitely generated $A-$module, and $B'[x]$ is a finitely generated $B'-$module(since x is integral over B').
Hence $B'[x]$ is a finitely generated $A-$module and hence x is integral over A. ■
Corollary. *Let $A \subseteq B$ be rings and let C be the integral closure of A in B. Then C is integrally closed in B.*
PROOF. Let $x \in B$ be integral over C.
$\implies x$ is integral over A, hence $x \in C$. ■

♣♣♣