Commutative Algebra

Sumanth N R

August 30, 2023

Contents

Chapter 1

Rings and Ideals

1.1 Rings and Ring Homomorphisms

Throughout the book, we will be working with **commutative rings with identity**. We will define a ring as

Definition 1.1: Ring

A ring A is a set with two binary operations

$$+ : A \times A \longrightarrow A$$
$$\cdot : A \times A \longrightarrow A$$

such that

1. A is an abelian group under $+$ (identity denoted by 0 and inverse denoted by $-x$ forall x).
2. Multiplication $\cdot$ is associative and distributive over addition.
3. Multiplication $\cdot$ is commutative.
4. There exists an element 1 such that $1 \cdot x = x \cdot 1 = x$ for all $x \in A$.

Note:-

Throughout the book, the word **ring** will be used to indicate a commutative ring with identity unless specified otherwise.

Definition 1.1

A **ring homomorphism** is a function $f : A \longrightarrow B$ satisfying

$$f(x+y) = f(x) + f(y)$$
$$f(x \cdot y) = f(x) \cdot f(y)$$
$$f(1) = 1$$

1.2 Ideals and Quotient Rings

An ideal $\mathfrak{a}$ of a ring A is a subset of A which is closed under addition and multiplication with absorption property.

Definition 1.2 Ideal

An ideal $\mathfrak{a}$ of a ring A is a subset of A such that

$$A\mathfrak{a} \subseteq \mathfrak{a}$$

That is,

$$x \in A, y \in \mathfrak{a} \implies xy \in \mathfrak{a}$$

Consider $A/_{\mathfrak{a}}$ to be the set of all cosets of $\mathfrak{a}$ in A of the form $x + \mathfrak{a}$ for $x \in A$.
Let us define a ring homomorphism $\phi : A \to A/_{\mathfrak{a}}$ that maps each element $x \in A$ to its coset $x + \mathfrak{a}$. Clearly, ϕ is a surjective ring homomorphism.

Theorem 1.1 Correspondence Theorem

There is a one-to-one order preserving correspondence between ideals $\mathfrak{b}$ of a ring A which contain $\mathfrak{a}$ and the ideals $\overline{\mathfrak{b}}$ of the quotient ring $A/_{\mathfrak{a}}$.

Theorem 1.2 First Isomorphism Theorem

Let $f : A \to B$ be any ring homomorphism. The kernel of f, say $\mathfrak{a}$ is an ideal of A and the image of f, say C is a subring of B.
Then f induces a ring isomorphism $A/_{\mathfrak{a}} \cong C$.

We also use the notation $x \equiv y \pmod{\mathfrak{a}}$ and this means that $x - y \in \mathfrak{a}$.

1.3 Zero Divisors, Nilpotent Elements, Units

A **zero-divisor** in a ring A is an element x which *divides* 0.

Definition 1.3 Zero Divisor

An element $x \in A$ is called a **zero-divisor** if

$$\exists\, y \in A \quad \text{s.t.} \quad xy = 0$$

A ring with no zero-divisors is called an integral domain.

Definition 1.4 Integral Domain

A ring A is called an **integral domain** if

$$\forall\, x, y \in A \text{ s.t. } xy = 0 \implies x = 0 \text{ or } y = 0$$

Definition 1.5 Nilpotent Element

An element $x \in A$ is called **nilpotent** if

$$\exists\, n \in \mathbb{N} \quad \text{s.t.} \quad x^n = 0$$

Note:-

$x \in A$ is nilpotent $\implies$ x is a zero-divisor.
The converse is not true in general.

A unit in a ring A is an element x which *divides* 1.

Definition 1.6 Unit

An element $x \in A$ is called a **unit** if

$$\exists\, y \in A \quad \text{s.t.} \quad xy = 1$$

Theorem 1.3 Group of Units

The set of units of a ring A form a group under multiplication.

Definition 1.7 Principal Ideal

The multiples ax of an element x form a principal ideal, denoted by (x) or Ax.

Note that

$$x \text{ is a unit } \iff (x) = A = (1)$$

The zero ideal (0) is usually denoted by 0.

Definition 1.8 Field

A field is a ring A in which $1 \neq 0$ and every non-zero element is a unit.

Every field is an integral domain but the converse is not true in general.

Proposition 1.1

Let A be a ring with $1 \neq 0$. Then, the following are equivalent.

1. A is a field.
2. The only ideals are (0) and (1).
3. Every homomorphism from A into a non-zero ring B is injective.

Proof. $1 \implies 2$
Consider a non-zero ideal $\mathfrak{a}$ of A.
$\implies \mathfrak{a}$ contains a non-zero element x.
Since A is a field, x is a unit.
$\implies \exists\, y \in A$ s.t. $xy = 1$ and thus $1 \in \mathfrak{a}$.
$\implies \mathfrak{a} = A = (1)$

$2 \implies 3$
Consider a ring homomorphism $f : A \longrightarrow B$ with $B \neq 0$.
If $\operatorname{Ker}(f) \neq 0 \implies \operatorname{Ker}(f) = (1)$
But $\operatorname{Ker}(f) = (1) \implies \operatorname{Im}(f) = B = 0$
We have $\operatorname{Ker}(f) = 0$ and hence, we can conclude that f is injective.

$3 \implies 1$
Consider an element $x \in A$ which is not a unit.
Clearly, $(x) \neq (1)$. Thus, $B = {}^{A}\big/_{(x)}$ is a non-zero ring.
Consider the natural homomorphism from A to B given by $a \mapsto a + (x)$.
Clearly, the kernel is given by (x) and since $B \neq 0$ and the homomorphism is injective, we have $(x) = 0$.
$\implies x = 0$
Thus, 0 is the only non-unit of A which implies A is a field. □

1.4 Prime Ideals and Maximal Ideals

Definition 1.9 Prime Ideal

An ideal $\mathfrak{p}$ of A is called a **prime ideal** if $\mathfrak{p} \neq (1)$ and

$$\forall\, x, y \in A \text{ s.t. } xy \in \mathfrak{p} \implies x \in \mathfrak{p} \text{ or } y \in \mathfrak{p}$$

Definition 1.10 Maximal Ideal

An ideal $\mathfrak{m}$ of A is called a **maximal ideal** if $\mathfrak{m} \neq (1)$ and there is no ideal $\mathfrak{a}$ of A such that $\mathfrak{m} \subset \mathfrak{a} \subset (1)$ (Strict inclusion). Equivalently,

$$\mathfrak{m} \subseteq \mathfrak{a} \subseteq (1) \implies \mathfrak{m} = \mathfrak{a} \text{ or } \mathfrak{a} = (1)$$

Theorem 1.4

Suppose $\mathfrak{p}$ and $\mathfrak{m}$ be ideals of A. Then,

$$\begin{aligned} \mathfrak{p} \text{ is a prime ideal } &\iff A\big/\mathfrak{p} \text{ is an Integral Domain} \\ \mathfrak{m} \text{ is a maximal ideal } &\iff A\big/\mathfrak{m} \text{ is a Field} \end{aligned}$$

Proof. Trivial □

Corollary 1.1

Every maximal ideal is a prime ideal.

Lemma 1.1

The zero ideal is prime $\iff$ A is an integral domain.

Proof. (0) is a prime ideal
$\iff \forall\, x, y \in A$ s.t. $xy = 0 \implies x = 0$ or $y = 0$
$\iff A$ is an integral domain. □

Consider a ring homomorphism $f : A \longrightarrow B$.

Claim 1.1

When $\mathfrak{q}$ is a prime ideal of B, then $f^{-1}(\mathfrak{q})$ is a prime ideal of A.

Proof. Consider a homomorphism $g : A \longrightarrow B\big/\mathfrak{q}$ given by

$$g(a) \coloneqq f(a) \pmod{\mathfrak{q}}$$

The kernel of the above homomorphism is given by,

$$\operatorname{Ker}(g) = f^{-1}(q)$$

Using the first homomorphism theorem, we have

$$A\Big/f^{-1}(q) \cong g(A)$$

s □

Note:-

The same claim does not hold for maximal ideals.

Prime ideals are fundamental to the whole of commutative algebra. The following theorem and its corollaries ensure that there is always a sufficient supply of them.

Theorem 1.5

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

Proof. Follows from Zorn's Lemma □

Corollary 1.2

If $\mathfrak{a}$ is an ideal of A, then there exists a maximal ideal $\mathfrak{m}$ such that $\mathfrak{a} \subseteq \mathfrak{m}$.

Proof. Apply the theorem to ${}^{A}/_{\mathfrak{a}}$ □

Corollary 1.3

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

1.4.1 Local Ring and Residue Field

Note that fields contain exactly one maximal ideal. It is not true that a ring containing exactly one maximal ideal is a field.

Definition 1.11 Local Ring and Residue Field

A ring A is called a **local ring** if it contains **exactly one** maximal ideal.
The field ${}^{A}/_{\mathfrak{m}}$ is called the **residue field**.

Note that every field is a local ring.

Proposition 1.2

1. Let A be a ring and $\mathfrak{m} \neq (1)$ be an ideal of A such that every $x \in A \setminus \mathfrak{m}$ is a unit. Then, A is a local ring and $\mathfrak{m}$ is a maximal ideal.

2. Let A be a ring and $\mathfrak{m}$ a maximal ideal of A, such that every element of $1 + \mathfrak{m}$ is a unit in A. Then, A is a local ring.

Proof. Let A be a ring.

1. Consider a maximal ideal $\mathfrak{a}$ of A. If $\mathfrak{a}$ contains a unit, then $\mathfrak{a} = A$ which implies $\mathfrak{a}$ is not maximal. We know that $A \setminus \mathfrak{m}$ contains only units and hence, $\mathfrak{a} \subseteq A \setminus (A \setminus \mathfrak{m})$ which implies $\mathfrak{a} \subseteq \mathfrak{m}$. Since $\mathfrak{a}$ is maximal, this means $\mathfrak{a} = \mathfrak{m}$.

2. Consider an element $x \in A \setminus \mathfrak{m}$. Since $\mathfrak{m}$ is maximal, the ideal generated by x and $\mathfrak{m}$ is (1) and hence, $\exists\, y \in A, t \in \mathfrak{m}$ s.t. $xy + t = 1$. Hence, $xy \in 1 + \mathfrak{m}$ and is therefore a unit. Applying the previous part, we get that A is a local ring.

□

Example 1.1

1. A $= \kappa[x_1, x_2, \ldots, x_n]$ where κ is a field. Let f be an irreducible polynomial. By uniqueness of factorization, the ideal generated by f is a prime ideal.

2. Consider $A = \mathbb{Z}$. Every ideal in $\mathbb{Z}$ is of the form (a) for some $a \in \mathbb{Z}$. (p) is prime if and only if p is a prime number. Clearly, ${}^{\mathbb{Z}}\big/_{(p)}$ is a field.

3. A **principal ideal domain** is a ring A where every ideal is generated by a single element. In a PID, every prime ideal is a maximal ideal.

1.5 Nilradical and Jacobson Radical

Definition 1.12 Nilradical

The set of all nilpotent elements of a ring A, denoted by $\mathfrak{N}$ is called the **nilradical** of A.

$$\mathfrak{N} := \{a \in A \mid \exists\, n \in \mathbb{N} \text{ s.t. } a^n = 0\}$$

Proposition 1.3

The set of all nilpotent elements of a ring A is an ideal. Furthermore, ${}^{A}/_{\mathfrak{N}}$ has no nilpotent elements $\neq 0$.

Proof. Enough to prove the properties of an ideal.

1. (Closed) Let $a, b \in \mathfrak{N}$. Then, $\exists\, n, m \in \mathbb{N}$ s.t. $a^n = b^m = 0$.
   Now, consider $(a+b)^{m+n-1}$.
   $$(a+b)^{m+n-1} = \sum_{i=0}^{m+n-1} \binom{m+n-1}{r} a^r b^{m+n-1-r}$$
   Either $r \geqslant n$ or $m+n-1-r \geqslant m$. Otherwise, we have $m+n-1 \geqslant m+n$ which is clearly a contradiction.
   Therefore, we have $(a+b)^{m+n-1} = 0 \implies a+b \in \mathfrak{N}$.
   Clearly, $(ab)^{mn} = 0 \implies ab \in \mathfrak{N}$.
2. (Absorption) Let $a \in \mathfrak{N}$. Then, $\exists\, n \in \mathbb{N}$ s.t. $a^n = 0$. For any $b \in A$, $(ba)^n = b^n a^n = 0$.
3. (Non Empty) $0 \in \mathfrak{N}$.

Thus, we proved that $\mathfrak{N}$ is an ideal in A.

For the next part, suppose $a + \mathfrak{N}, a \in A$ is nilpotent in ${}^{A}/_{\mathfrak{N}}$.
Then, $\exists\, n \in \mathbb{N}$ s.t. $(a+\mathfrak{N})^n = a^n + \mathfrak{N} = 0 + \mathfrak{N}$.
Clearly, this means $a^n \in \mathfrak{N} \implies \exists\, m \in \mathbb{N}$ s.t. $(a^n)^m = 0 \implies a^{nm} = 0$.
Hence, we have $a \in \mathfrak{N}$.
Therefore, $a + \mathfrak{N}$ is nilpotent in ${}^{A}/_{\mathfrak{N}}$ implies $a + \mathfrak{N} = 0 + \mathfrak{N}$ is the zero element of ${}^{A}/_{\mathfrak{N}}$. □

Proposition 1.4

The nilradical, $\mathfrak{N}$ of a ring A is the intersection of all the prime ideals of A.

Proof. Suppose $\mathfrak{N}'$ denote the intersection of all the prime ideals of A.

First, we prove $\mathfrak{N} \subseteq \mathfrak{N}'$.
Consider any $a \in \mathfrak{N}$. Then, $\exists\, n \in \mathbb{N}$ s.t. $a^n = 0$.
We also know that $0 \in \mathfrak{p}\ \forall$ prime ideals $\mathfrak{p} \implies a^n \in \mathfrak{p} \implies a \in \mathfrak{p}\ \forall$ prime ideals $\mathfrak{p}$.
Hence, we have $a \in \mathfrak{N}'$.

Then, we prove that $a \notin \mathfrak{N} \implies a \notin \mathfrak{N}'$.
(TODO)

□

Definition 1.13 Jacobson Radical

The Jacobson radical of a ring A, denoted by $\mathfrak{R}$ is defined as the intersection of all maximal ideals of A.

Proposition 1.5

$x \in \mathfrak{R} \iff 1 - xy$ is a unit in $A\ \forall\, y \in A$.

Proof. ($\implies$)
Proof by contradiction.
Suppose $x \in \mathfrak{R}$ and $1 - xy$ is not a unit in A. Then, using a result from before, we know that $1 - xy$ is contained in some maximal ideal, say $\mathfrak{m}$.
Now, since $x \in \mathfrak{R} \implies x \in \mathfrak{m}$, we have $1 - xy \in \mathfrak{m} \implies 1 \in \mathfrak{m}$, which is a contradiction.

($\impliedby$)
Proof by contradiction.
Suppose $1 - xy$ is a unit in A for all $y \in A$ and $x \notin \mathfrak{m}$ for some maximal ideal $\mathfrak{m}$.
Then, (x) and $\mathfrak{m}$ generate the entire ring and so we have $u + xy = 1$ for some $u \in \mathfrak{m}$ and some $y \in A$.
This implies $1 - xy \in \mathfrak{m}$ and thus can't be a unit which is a contradiction. □

Note:-

The nilradical is contained in the Jacobson radical.

1.6 Operations on Ideals

Definition 1.14 Operations on Ideals

1. Sum of ideals: Consider 2 ideals $\mathfrak{a}, \mathfrak{b}$ in a ring A. Then, their sum $\mathfrak{a} + \mathfrak{b}$ is defined by

$$\mathfrak{a} + \mathfrak{b} = \{x + y \mid x \in \mathfrak{a}, y \in \mathfrak{b}\}$$

   More generally, we define the sum of a (finite) family of ideals $\{\mathfrak{a}_i\}_{i \in I}$

$$\sum_{i \in I} \mathfrak{a}_i = \left\{ \sum_{i \in I} x_i \mid x_i \in \mathfrak{a}_i \right\}$$

2. Intersection of ideals: Consider 2 ideals $\mathfrak{a}, \mathfrak{b}$ in a ring A. Then, their intersection $\mathfrak{a} \cap \mathfrak{b}$ forms an ideal.

$$\mathfrak{a} \cap \mathfrak{b} = \{x \mid x \in \mathfrak{a} \text{ and } x \in \mathfrak{b}\}$$

3. Product of ideals: Consider 2 ideals $\mathfrak{a}, \mathfrak{b}$ in a ring A. Then, the product of ideals $\mathfrak{ab}$ is defined to be the ideal generated by all products of elements of $\mathfrak{a}$ and $\mathfrak{b}$.

$$\mathfrak{ab} = \left\{ \sum_{i=1}^{n} x_i y_i \mid x_i \in \mathfrak{a}, y_i \in \mathfrak{b}, n \in \mathbb{N} \right\}$$

   Similarly, we can define the product of a (finite) family of ideals $\{\mathfrak{a}_i\}_{i \in I}$

$$\prod_{i \in I} \mathfrak{a}_i = \left\{ \sum_{j=1}^{n} \prod_{i \in I} x_{ji} \mid x_{ji} \in \mathfrak{a}_i, j \in \mathbb{N} \right\}$$

The product is particularly useful in defining the powers of ideals.
$\mathfrak{a}^n$ is generated by elements of the form $x_1 x_2 \ldots x_n$ where $x_i \in \mathfrak{a}$ for all i.
Conventionally, $\mathfrak{a}^0 = (1)$ is defined.

Note that the operations sum, product and intersection are all commutative and associative.
There is also the distributive law

$$\mathfrak{a}(\mathfrak{b} + \mathfrak{c}) = \mathfrak{ab} + \mathfrak{ac}$$

In $\mathbb{Z}$, $\cap$ and $+$ are distributive but this is not true in general.
In general, we have the **modular law**

$$\mathfrak{a} \cap (\mathfrak{b} + \mathfrak{c}) = \mathfrak{a} \cap \mathfrak{b} + \mathfrak{a} \cap \mathfrak{c} \quad \textbf{if } \mathfrak{a} \supseteq \mathfrak{b} \text{ or } \mathfrak{a} \supseteq \mathfrak{c}$$

Again, in $\mathbb{Z}$, we have $(\mathfrak{a}+\mathfrak{b})(\mathfrak{a}\cap\mathfrak{b}) = \mathfrak{a}\mathfrak{b}$ but this is not true in general.
In general, we have

$$(\mathfrak{a}+\mathfrak{b})(\mathfrak{a}\cap\mathfrak{b}) \subseteq \mathfrak{a}\mathfrak{b}$$

We clearly have $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{a}\cap\mathfrak{b}$ and hence, we have

$$\mathfrak{a}\cap\mathfrak{b} = \mathfrak{a}\mathfrak{b} \text{ provided } \mathfrak{a}+\mathfrak{b} = (1)$$

This lets us define coprime (or comaximal) ideals.

Definition 1.15 Coprime (or Comaximal) ideals

Let $\mathfrak{a}, \mathfrak{b}$ be ideals in a ring A. Then, $\mathfrak{a}$ and $\mathfrak{b}$ are coprime (or comaximal) if $\mathfrak{a}+\mathfrak{b} = (1)$.

Thus, for coprime ideals, we have $\mathfrak{a}\cap\mathfrak{b} = \mathfrak{a}\mathfrak{b}$.
Clearly, 2 ideals are coprime if and only if there exist $x \in \mathfrak{a}$ and $y \in \mathfrak{b}$ such that $x + y = 1$.

1.6.1 Set of Rings and Coprime Ideals

Consider rings $A_1, \ldots, A_n$. Then, the **direct product** of these rings is a ring with component-wise addition and multiplication.

$$A \coloneqq \prod_{i=1}^{n} A_i = \{(x_1, \ldots, x_n) \mid x_i \in A_i\}$$

We can also define projections $p_i : A \longrightarrow A_i$ defined by $p_i(x) = x_i$.

Let A be a ring and $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ be ideals in A. Define the homomorphism given by

$$\begin{aligned} \phi : A &\longrightarrow \prod_{i=1}^{n} A \big/ \mathfrak{a}_i \\ x &\longmapsto (x + \mathfrak{a}_1, \ldots, x + \mathfrak{a}_n) \end{aligned}$$

Proposition 1.6

1. If $\mathfrak{a}_i, \mathfrak{a}_j$ are coprime when $i \neq j$, then,
$$\prod_{i=1}^{n} \mathfrak{a}_i = \bigcap_{i=1}^{n} \mathfrak{a}_i$$
2. ϕ is surjective $\iff$ $\mathfrak{a}_i, \mathfrak{a}_j$ are coprime whenever $i \neq j$.
3. ϕ is injective $\iff$ $\bigcap \mathfrak{a}_i = (0)$.

Proof.

1. We prove the claim by induction. $n = 2$ being the base case was done before.
Now, suppose $\prod_{i=1}^{n-1} \mathfrak{a}_i = \bigcap_{i=1}^{n-1} \mathfrak{a}_i = \mathfrak{b}$.
We show that $\mathfrak{b}$ and $\mathfrak{a}_n$ are coprime. Since $\mathfrak{a}_n$ and $\mathfrak{a}_i$ are coprime, for every $1 \leqslant i \leqslant n-1$, we have some $x_i \in \mathfrak{a}_i$ and $y_i \in \mathfrak{a}_n$ such that $x_i + y_i = 1$.
$$\implies x \coloneqq \prod_{i=1}^{n-1} x_i = \prod_{i=1}^{n-1} (1 - y_i) \quad = 1 \pmod{\mathfrak{a}_n}$$
Hence, $\exists\, x \in \mathfrak{b}, y \in \mathfrak{a}_n$ such that $x + y = 1$.
Thus, $\mathfrak{b}$ and $\mathfrak{a}_n$ are coprime.
And hence, we have $\mathfrak{b}\mathfrak{a}_n = \mathfrak{b} \cap \mathfrak{a}_n$.
$$\implies \prod_{i=1}^{n} \mathfrak{a}_i = \bigcap_{i=1}^{n} \mathfrak{a}_i$$

2. ($\implies$)
   We show that $\mathfrak{a}_1$ and $\mathfrak{a}_2$ are coprime.
   Since ϕ is surjective, $\exists\, x \in A$ such that $\phi(x) = (1, 0, \ldots, 0)$.
   Now, we know that $x \equiv 1 \pmod{\mathfrak{a}_1}$ and $x \equiv 0 \pmod{\mathfrak{a}_2}$.
   We have $1 - x \in \mathfrak{a}_1$ and $x \in \mathfrak{a}_2$ but $1 - x + x = 1$.
   $\implies \mathfrak{a}_1$ and $\mathfrak{a}_2$ are coprime.
   Similarly, it can be shown that a_i is coprime to a_j for all $i \neq j$.

   ($\impliedby$)
   It is enough to show that there is an element $x \in A$ such that $\phi(x) = (1, 0, \ldots, 0)$.
   For every i such that $2 \leqslant i \leqslant n$, we have $u_i \in \mathfrak{a}_1, v_i \in \mathfrak{a}_i$ satisfying $u_i + v_i = 1$.
   Consider $x = \prod_{i=1}^{n-1} v_i$. Thus, we have $x \equiv 0 \pmod{\mathfrak{a}_i}$ when $i > 1$ and
   $x \equiv \prod_{i=1}^{n-1} (1 - u_i) \equiv 1 \pmod{\mathfrak{a}_1}$.

3. The kernel of the homomorphism ϕ is clearly $\bigcap \mathfrak{a}_i$.
   If a homomorphism is injective, the kernel is singleton and vice versa.
   Thus, the homomorphism is injective $\iff \bigcap \mathfrak{a}_i = (0)$.

□

1.6.2 Prime Avoidance Lemma

The union of ideals is not in general an ideal.

Lemma 1.2 (Prime Avoidance Lemma)
Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ be prime ideals and $\mathfrak{a}$ be an ideal contained in $\bigcup_{i=1}^{n} \mathfrak{p}_i$. Then, $\mathfrak{a} \subseteq \mathfrak{p}_i$ for some i.

Proof. We perform induction on the statement
For any ideal $\mathfrak{a}$ contained in an arbitrary union of n prime ideals, $\bigcup_{i=1}^{n} \mathfrak{p}_i$, we have $\mathfrak{a} \subseteq \mathfrak{p}_i$ for some i.
Equivalently, for any ideal $\mathfrak{a} \nsubseteq \mathfrak{p}_i \;\forall\, i \implies \mathfrak{a} \nsubseteq \bigcup_{i=1}^{n} \mathfrak{p}_i$

The base case for $n = 1$ is trivial. Let us assume the result for $n - 1$.
We prove by the induction hypothesis by contradiction.
Suppose $\mathfrak{a} \subseteq \bigcup_{i=1}^{n} \mathfrak{p}_i$ and $\mathfrak{a} \nsubseteq \mathfrak{p}_i \;\forall\, i$.

This means $\mathfrak{a} \nsubseteq \displaystyle\bigcup_{j \neq i} \mathfrak{p}_j \;\forall\, i$

$\implies \exists\, x_i \in \mathfrak{a} \setminus \displaystyle\bigcup_{j \neq i} \mathfrak{p}_j$

If for some i, we have $x_i \notin \mathfrak{p}_i$, we get $x_i \notin \displaystyle\bigcup_{i=1}^{n} \mathfrak{p}_i$ and $x_i \in \mathfrak{a}$ which is a contradiction.

Otherwise, we have $x_i \in \mathfrak{p}_i \;\forall\, i$. Consider the element

$$y = \sum_{i=1}^{n} \prod_{j=1, j \neq i}^{n} x_j$$

Clearly for all i, $y \notin \mathfrak{p}_i$ and $y \in \mathfrak{a}$.
Thus, we can conclude that $\mathfrak{a} \nsubseteq \bigcup_{i=1}^{n} \mathfrak{p}_i$ which is clearly a contradiction. □

Corollary 1.4
Let $\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_n$ be ideals and let $\mathfrak{p}$ be a prime ideal such that $\mathfrak{p} \supseteq \bigcap_{i=1}^{n} \mathfrak{a}_i$.
Then, $\mathfrak{p} \supseteq \mathfrak{a}_i$ for some i.
If $\mathfrak{p} = \bigcap \mathfrak{a}_i$, then $\mathfrak{p} = \mathfrak{a}_i$ for some i.

Proof. Proof by contradiction. Suppose $\mathfrak{p} \not\supseteq \mathfrak{a}_i \ \forall\ i$.
Then $\forall\ i$, we have $x_i \in \mathfrak{a}_i, x_i \notin \mathfrak{p}$
$y := \prod_{i=1}^{n} x_i \ \in \ \prod_{i=1}^{n} \mathfrak{a}_i \ \subseteq \ \bigcap \mathfrak{a}_i$
But, $y \notin \mathfrak{p}$ since $\mathfrak{p}$ is a prime ideal but we have $y \in \bigcap \mathfrak{a}_i$ which is a contradiction.

$\mathfrak{p} = \bigcap \mathfrak{a}_i \implies \mathfrak{p} \subseteq \mathfrak{a}_i$. We also showed that $\mathfrak{p} \supseteq \mathfrak{a}_i$ which implies $\mathfrak{p} = \mathfrak{a}_i$. □

1.6.3 Ideal Quotient

Definition 1.16 Ideal Quotient

If $\mathfrak{a}$ and $\mathfrak{b}$ are ideals in a ring A, then their *quotient* is defined as

$$(\mathfrak{a} \colon \mathfrak{b}) := \{x \in A \mid x\mathfrak{b} \subseteq \mathfrak{a}\}$$

which is an ideal.

In particular, $(0 \colon \mathfrak{b})$ is called the *annihilator* of $\mathfrak{b}$ and is denoted by $\operatorname{Ann}(\mathfrak{b})$.
Using this notation, the set of all zero divisors of $\mathfrak{a}$ is given by

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

If $\mathfrak{b}$ is a principal ideal (x), then we write $(\mathfrak{a} \colon x)$ instead.

Example 1.2

Consider A $= \mathbb{Z}$ and $\mathfrak{a} = (m)$ and $\mathfrak{b} = (n)$ where $m = \prod_p p^{\mu_p}$ and $n = \prod_p p^{\nu_p}$.
Then, $(\mathfrak{a} \colon \mathfrak{b}) = (q)$ where $q = \prod_p p^{\gamma_p}$ and $\gamma_p = \max\left(\mu_p - \nu_p, 0\right)$.
Hence, $q = m/\gcd(m, n)$

Proposition 1.7

1. $\mathfrak{a} \subseteq (\mathfrak{a} \colon \mathfrak{b})$
2. $(\mathfrak{a} \colon \mathfrak{b})\mathfrak{b} \subseteq \mathfrak{a}$
3. $((\mathfrak{a} \colon \mathfrak{b}) : \mathfrak{c}) = (\mathfrak{a} \colon \mathfrak{b}\mathfrak{c}) = ((\mathfrak{a} \colon \mathfrak{c}) : \mathfrak{b})$
4. $(\cap_i \mathfrak{a}_i \colon \mathfrak{b}) = \cap_i (\mathfrak{a}_i \colon \mathfrak{b})$
5. $(\mathfrak{a} \colon \sum_i \mathfrak{b}_i) = \cap_i (\mathfrak{a} \colon \mathfrak{b}_i)$

Proof.

1. Follows by definition. $\forall\ x \in \mathfrak{a},\ x\mathfrak{b} \subseteq \mathfrak{a}$.
2. Consider an element $x \in (\mathfrak{a} \colon \mathfrak{b})$. By definition, $x\mathfrak{b} \subseteq \mathfrak{a}$ and hence $(\mathfrak{a} \colon \mathfrak{b})\mathfrak{b} \subseteq \mathfrak{a}$
3. Consider an element $x \in ((\mathfrak{a} \colon \mathfrak{b}) : \mathfrak{c}) \implies x\mathfrak{c} \subseteq (\mathfrak{a} \colon \mathfrak{b})$.
   Thus, for any element $y \in \mathfrak{c}$, we have $xy\mathfrak{b} \subseteq \mathfrak{a} \implies x\mathfrak{b}\mathfrak{c} \subseteq \mathfrak{a} \implies x \in (\mathfrak{a} \colon \mathfrak{b}\mathfrak{c})$.

   Now, consider an element $x \in (\mathfrak{a} \colon \mathfrak{b}\mathfrak{c}) \implies x\mathfrak{b}\mathfrak{c} \subseteq \mathfrak{a}$.
   Thus, for any element $y \in \mathfrak{c}$, we have $xy\mathfrak{b} \subseteq \mathfrak{a} \implies xy \in (\mathfrak{a} \colon \mathfrak{b}) \implies x\mathfrak{c} \subseteq (\mathfrak{a} \colon \mathfrak{b})$
   This implies $x \in ((\mathfrak{a} \colon \mathfrak{b}) : \mathfrak{c})$
4. $x \in (\cap_i \mathfrak{a}_i \colon \mathfrak{b}) \iff x\mathfrak{b} \subseteq \cap_i \mathfrak{a}_i \iff x\mathfrak{b} \subseteq \mathfrak{a}_i \ \forall\ i \iff x \in (\mathfrak{a}_i \colon \mathfrak{b}) \ \forall\ i \iff x \in \cap_i (\mathfrak{a}_i \colon \mathfrak{b})$
5. $x \in (\mathfrak{a} \colon \sum_i \mathfrak{b}_i) \iff x \sum_i \mathfrak{b}_i \subseteq \mathfrak{a} \iff x\mathfrak{b}_i \subseteq \mathfrak{a} \ \forall\ i \iff x \in \cap_i (\mathfrak{a} \colon \mathfrak{b}_i)$

□

1.7 Radical

Definition 1.17 Radical

The *radical* of an ideal $\mathfrak{a}$ is defined as

$$\mathrm{r}(\mathfrak{a}) := \{x \in A \mid x^n \in \mathfrak{a} \text{ for some } n \in \mathbb{N}\}$$

If $\phi : A \longrightarrow {}^{A}/_{\mathfrak{a}}$ is the standard homomorphism, then

$$\mathrm{r}(\mathfrak{a}) = \phi^{-1}\left(\mathfrak{N}_{A/\mathfrak{a}}\right)$$

Proposition 1.8

1. $\mathrm{r}(\mathfrak{a})$ is an ideal
2. $\mathrm{r}(\mathfrak{a})$ is the intersection of all prime ideals containing $\mathfrak{a}$

Proof.

1. Using proposition 1.5 and the stanard homomorphism, we have the result.
2. Using proposition 1.5 on ${}^{A}/_{\mathfrak{a}}$, we have the result.

□

Proposition 1.9

1. $\mathrm{r}(\mathfrak{a}) \supseteq \mathfrak{a}$
2. $\mathrm{r}(\mathrm{r}(\mathfrak{a})) = \mathrm{r}(\mathfrak{a})$
3. $\mathrm{r}(\mathfrak{a}\mathfrak{b}) = \mathrm{r}(\mathfrak{a} \cap \mathfrak{b}) = \mathrm{r}(\mathfrak{a}) \cap \mathrm{r}(\mathfrak{b})$
4. $\mathrm{r}(\mathfrak{a}) = (1) \iff \mathfrak{a} = (1)$
5. $\mathrm{r}(\mathfrak{a} + \mathfrak{b}) = \mathrm{r}(\mathrm{r}(\mathfrak{a}) + \mathrm{r}(\mathfrak{b}))$
6. If $\mathfrak{p}$ is a prime ideal, $\mathrm{r}(\mathfrak{p}^n) = \mathfrak{p} \; \forall \; n \in \mathbb{N}$

Proof.

1. Clearly for any $x \in \mathfrak{a}$, $x^1 \in \mathfrak{a}$ and hence, $x \in \mathrm{r}(\mathfrak{a})$.
2. For any $x \in \mathrm{r}(\mathrm{r}(\mathfrak{a}))$, $x^n \in \mathrm{r}(\mathfrak{a})$ for some $n \in \mathbb{N}$ and this implies $x^{mn} \in \mathfrak{a}$ for some $m \in \mathbb{N}$ and hence, $x \in \mathrm{r}(\mathfrak{a})$.
3. Consider an element $x \in \mathrm{r}(\mathfrak{a}\mathfrak{b})$. By definition, $x^n \in \mathfrak{a}\mathfrak{b}$ for some $n \in \mathbb{N}$ and hence, $x^n \in \mathfrak{a}$ and $x^n \in \mathfrak{b}$.
   Thus, $x \in \mathrm{r}(\mathfrak{a})$ and $x \in \mathrm{r}(\mathfrak{b})$ and hence, $x \in \mathrm{r}(\mathfrak{a}) \cap \mathrm{r}(\mathfrak{b})$.
   Also, $x^n \in \mathfrak{a} \cap \mathfrak{b} \implies x^n \in \mathrm{r}(\mathfrak{a} \cap \mathfrak{b})$.
   Now, we assume $x \in \mathrm{r}(\mathfrak{a} \cap \mathfrak{b})$ and try to prove $x \in \mathrm{r}(\mathfrak{a}\mathfrak{b})$.
   $x^n \in \mathfrak{a}$ and $x^m \in \mathfrak{b}$ for some $n, m \in \mathbb{N}$. This implies $x^{nm} \in \mathfrak{a}$ and $x^{mn} \in \mathfrak{b}$ and hence $x^{2mn} \in \mathfrak{a}\mathfrak{b}$.
4. $\mathfrak{a} = (1) \implies \mathrm{r}(\mathfrak{a}) = (1)$ is obvious. For the other side, assume $\mathrm{r}(\mathfrak{a}) = (1)$.
   This means $1 \in \mathrm{r}(\mathfrak{a}) \implies 1 \in \mathfrak{a}$ since 1 is idempotent. Hence, $\mathfrak{a} = (1)$.
5. Clearly, $\mathfrak{a} \subseteq \mathrm{r}(\mathfrak{a})$ and $\mathfrak{b} \subseteq \mathrm{r}(\mathfrak{b})$. This implies $\mathfrak{a} + \mathfrak{b} \subseteq \mathrm{r}(\mathfrak{a}) + \mathrm{r}(\mathfrak{b})$ and hence $\mathrm{r}(\mathfrak{a} + \mathfrak{b}) \subseteq \mathrm{r}(\mathrm{r}(\mathfrak{a}) + \mathrm{r}(\mathfrak{b}))$.
   Suppose $x \in \mathrm{r}(\mathrm{r}(\mathfrak{a}) + \mathrm{r}(\mathfrak{b}))$. Then $x^n = y + z$ for some $x, y \in A$ with $y^m \in \mathfrak{a}, z^k \in \mathfrak{b}$ and $m, k \in \mathbb{N}$.
   Consider $(x^n)^{m+k-1} = (y+z)^{m+k-1} = c_0 y^{m+k-1} z^0 + c_1 y^{m+k-2} z^1 + \cdots + c_{m+k-1} y^0 z^{m+k-1}$
   $= y^m \left(c_0 y^{k-1} z^0 + c_1 y^{k-2} z^1 + \cdots + c_{k-1} y^0 z^{k-1}\right) + z^k \left(c_k y^{m+1} z^0 + c_{k+1} y^m z^1 + \cdots + c_{m+k-1} y^0 z^m\right)$
   $= y^m \alpha + z^k \beta \in \mathfrak{a} + \mathfrak{b}$. Thus, $x \in \mathrm{r}(\mathfrak{a} + \mathfrak{b})$.

6. We have $\mathrm{r}\left(\mathfrak{p}^n\right) = \mathrm{r}\left(\mathfrak{p}\right)$ for any n using the third part of this proposition.
   Suppose $x \in \mathrm{r}\left(\mathfrak{p}\right) \implies x^m \in \mathfrak{p}$ for some $m \in \mathbb{N}$. Choose m to be the minimum number for which $x^m \in \mathfrak{p}$. If $m = 1$, we are done. Otherwise $x^m = xx^{m-1} \in \mathfrak{p}$. This implies $x \in \mathfrak{p}$ in which case we are done or $x^{m-1} \in \mathfrak{p}$ contradicts the minimality of m.

□

Proposition 1.10

The set of zero-divisors of A,

$$D = \bigcup_{x \neq 0} \mathrm{r}\left(\mathrm{Ann}\left(x\right)\right)$$

Proof. Claim: $x \in \mathrm{r}\left(D\right) \implies x \in D$. It is easy to see that if x^n is a zero divisor, then x is a zero divisor. Hence,

$$D = \mathrm{r}\left(D\right) = \mathrm{r}\left(\bigcup_{x \neq 0} \mathrm{Ann}\left(x\right)\right) = \bigcup_{x \neq 0} \mathrm{r}\left(\mathrm{Ann}\left(x\right)\right)$$ □

Proposition 1.11

Let $\mathfrak{a}, \mathfrak{b}$ be ideals of ring A such that $\mathrm{r}\left(\mathfrak{a}\right)$ and $\mathrm{r}\left(\mathfrak{b}\right)$ are coprime. Then, $\mathfrak{a}$ and $\mathfrak{b}$ are coprime.

Proof. Using the propositions proved above, $\mathrm{r}\left(\mathfrak{a} + \mathfrak{b}\right) = \mathrm{r}\left(\mathrm{r}\left(\mathfrak{a}\right) + \mathrm{r}\left(\mathfrak{b}\right)\right) = \mathrm{r}\left(1\right) = (1)$. Hence, $\mathfrak{a} + \mathfrak{b} = (1)$. □

1.8 Extension and Contraction

Let $f : A \longrightarrow B$ be a ring homomorphism. If $\mathfrak{a}$ is an ideal in A, then $f(\mathfrak{a})$ is not necessarily an ideal in B.

Example 1.3

Let f be an embedding from $\mathbb{Z}$ to $\mathbb{Q}$. And non-zero ideal in $\mathbb{Z}$ taken to $\mathbb{Q}$ will not remain an ideal.

And thus, we define the extension and contraction of ideals.

Definition 1.18 Extension

If $f : A \longrightarrow B$ is a ring homomorphism and $\mathfrak{a}$ is an ideal in A, then the *extension* of $\mathfrak{a}$ by f is the ideal $Bf(\mathfrak{a})$ generated by $f(\mathfrak{a})$ in B, explicitly defined as

$$a^e := \sum y_i f(x_i) \qquad y_i \in B, x_i \in \mathfrak{a}$$

Definition 1.19 Contraction

If $f : A \longrightarrow B$ is a ring homomorphism and $\mathfrak{b}$ is an ideal in B, then the *contraction* of $\mathfrak{b}$, $f^{-1}(\mathfrak{b})$ is always an ideal in A, denoted by $\mathfrak{b}^c$.

Proposition 1.12

Suppose $f : A \longrightarrow B$ is a ring homomorphism. Then,

$$\mathfrak{b} \text{ is prime} \implies \mathfrak{b}^c = f^{-1}(\mathfrak{b}) \text{ is prime}$$

The contractions of prime ideals are prime ideals.

Proof. Suppose $\mathfrak{b}$ is a prime ideal in B. If $f^{-1}(\mathfrak{b}) = 0$, we're done. Otherwise, let $a_1, a_2 \in f^{-1}(\mathfrak{b})$.

Then, $f(a_1), f(a_2) \in \mathfrak{b}$.

$$\begin{aligned} a_1 \cdot a_2 \in f^{-1}(\mathfrak{b}) &\implies f(a_1 \cdot a_2) \in \mathfrak{b} \\ &\implies f(a_1) \cdot f(a_2) \in \mathfrak{b} \\ &\implies f(a_1) \in \mathfrak{b} \text{ or } f(a_2) \in \mathfrak{b} \\ a_1 \cdot a_2 \in f^{-1}(\mathfrak{b}) &\implies a_1 \in f^{-1}(\mathfrak{b}) \text{ or } a_2 \in f^{-1}(\mathfrak{b}) \end{aligned}$$

Hence, $f^{-1}(\mathfrak{b}) = \mathfrak{b}^c$ is a prime ideal in A. □

1.8.1 Factorizing the Homomorphism f

We can factorize the homomorphism f as follows.

$$\begin{tikzcd} A \arrow[r, "p"] & f(A) \arrow[r, "j"] & B \end{tikzcd}$$

where p is a surjective ring homomorphism and j is an injective ring homomorphism.
Then, f is a composition of p and j.
For p, the situation is very simple and using the Correspondence theorem, we can conclude that there is a one-to-one correspondence between the ideals of A and the ideals of $f(A)$ that contain the kernel of p.
For j, the situation is a far more complicated. Consider the example from algebraic number theory.

Example 1.4

Consider $\mathbb{Z} \longrightarrow \mathbb{Z}[i]$ where $i^2 = -1$.
A prime ideal (p) in $\mathbb{Z}$ may or may not stay prime when extended to $\mathbb{Z}[i]$.
The situation is as follows.

1. $(2)^e = \left((1+i)^2\right)$
2. If $p \equiv 1 \pmod 4$ then the extension of p is a product of two distinct prime ideals in $\mathbb{Z}[i]$. (eg. $(5)^e = (2+i)(2-i)$)
3. If $p \equiv 3 \pmod 4$ then the extension of p is a prime ideal in $\mathbb{Z}[i]$.

Of the above, the second case is not a trivial result. It is equivalent to saying that a prime $p \equiv 1 \pmod 4$ can be expressed uniquely as a sum of two integer squares.

1.8.2 Some Properties of Extraction and Contraction

Proposition 1.13

Let $f\colon A \longrightarrow B$ be a ring homomorphism and $\mathfrak{a}$ and $\mathfrak{b}$ are ideals in A and B, respectively. Then,

1. $\mathfrak{a} \subseteq \mathfrak{a}^{ec}, \mathfrak{b} \supseteq \mathfrak{b}^{ce}$
2. $\mathfrak{b}^c = \mathfrak{b}^{cec}, \mathfrak{a}^e = \mathfrak{a}^{ece}$
3. If C is a set of contracted ideals in A and if E is the set of extended ideals in B, then

$$C = \{\mathfrak{a} \mid \mathfrak{a}^{ec} = \mathfrak{a}\} \quad E = \{\mathfrak{b} \mid \mathfrak{b}^{ce} = \mathfrak{b}\}$$

and $\mathfrak{a} \longmapsto \mathfrak{a}^e$ is a bijective map of C onto E whose inverse is $\mathfrak{b} \longmapsto \mathfrak{b}^c$.

Proof.

1. $\mathfrak{a} \subseteq \mathfrak{a}^{ec}$

$$\begin{aligned} a \in \mathfrak{a} &\implies f(a) \in f(\mathfrak{a}) \\ &\implies f(a) \in Bf(\mathfrak{a}) = \mathfrak{a}^e \\ &\implies a \in \mathfrak{a}^{ec} \end{aligned}$$

$\mathfrak{b} \supseteq \mathfrak{b}^{ce}$

$$\implies f(f^{-1}(\mathfrak{b})) \subseteq \mathfrak{b}$$

2. $\mathfrak{b}^c = \mathfrak{b}^{cec}$

$$\mathfrak{b}^c \subseteq (\mathfrak{b}^c)^{ec} \text{ and } \mathfrak{b} \supseteq \mathfrak{b}^{ce} \implies \mathfrak{b}^c \supseteq \mathfrak{b}^{cec}$$

$\mathfrak{a}^e = \mathfrak{a}^{ece}$

$$\mathfrak{a} \subseteq \mathfrak{a}^{ec} \implies \mathfrak{a}^e \subseteq \mathfrak{a}^{ece} \text{ and } \mathfrak{a}^e \supseteq (\mathfrak{a}^e)^{ce}$$

3.

$$\begin{aligned} \mathfrak{a} \in C &\implies \mathfrak{a} = \mathfrak{b}^c = \mathfrak{b}^{cec} = \mathfrak{a}^{ec} \\ \mathfrak{b} \in E &\implies \mathfrak{b} = \mathfrak{a}^e = \mathfrak{a}^{ece} = \mathfrak{b}^{ce} \end{aligned}$$

□

Proposition 1.14

If $f\colon A \longrightarrow B$ is a ring homomorphism and if $\mathfrak{a}_1, \mathfrak{a}_2$ are ideals in A, then

1. $(\mathfrak{a}_1 + \mathfrak{a}_2)^e = \mathfrak{a}_1^e + \mathfrak{a}_2^e$
2. $(\mathfrak{a}_1 \cap \mathfrak{a}_2)^e \subseteq \mathfrak{a}_1^e \cap \mathfrak{a}_2^e$
3. $(\mathfrak{a}_1\mathfrak{a}_2)^e = \mathfrak{a}_1^e\mathfrak{a}_2^e$
4. $(\mathfrak{a}_1 : \mathfrak{a}_2)^e \subseteq (\mathfrak{a}_1 : \mathfrak{a}_2)^e$
5. $r(\mathfrak{a})^e \subseteq r(\mathfrak{a}^e)$

Proposition 1.15

If $f\colon A \longrightarrow B$ is a ring homomorphism and if $\mathfrak{b}_1, \mathfrak{b}_2$ are ideals in B, then

1. $(\mathfrak{b}_1 + \mathfrak{b}_2)^c \supseteq \mathfrak{b}_1^c + \mathfrak{b}_2^c$
2. $(\mathfrak{b}_1 \cap \mathfrak{b}_2)^c = \mathfrak{b}_1^c \cap \mathfrak{b}_2^c$
3. $(\mathfrak{b}_1\mathfrak{b}_2)^c \supseteq \mathfrak{b}_1^c\mathfrak{b}_2^c$
4. $(\mathfrak{b}_1 : \mathfrak{b}_2)^c \subseteq (\mathfrak{b}_1 : \mathfrak{b}_2)^c$
5. $r(\mathfrak{b})^c = r(\mathfrak{b}^c)$

Chapter 2

Modules 1

2.1 Modules and Module Homomorphisms

Definition 2.1: Module

Let A be a ring (commutative, with identity). A *(left) A-module* is an abelian group M (written additively) on which A acts linearly (written multiplicatively).
More precisely, it is a pair (M, μ_A) where M is an abelian group and $\mu_A : A \times M \longrightarrow M$ is a map satisfying the following axioms:

1. $a(x + y) = ax + ay$
2. $(a + b)x = ax + bx$
3. $(ab)x = a(bx)$
4. $1x = x$

for any $a, b \in A$ and $x, y \in M$.

Equivalently, a module is an abelian group M with a ring homomorphism $A \longrightarrow \mathrm{End}(M)$ where $\mathrm{End}(M)$ is the ring of endomorphisms of the abelian group M.

Example 2.1 (Modules)
The following are common examples of modules.

1. The ideals, $\mathfrak{a}$ of a ring A are A modules. In particular, A is itself an A module.
2. If A is a field κ, then κ-modules are κ-vector spaces.
3. If A is $\mathbb{Z}$, then abelian groups are $\mathbb{Z}$-modules.
4. If $A = \kappa[x]$ where κ is a field, an $\kappa[x]$-module is a κ-vector space with a linear transformation.

2.1.1 Homomorphisms of Modules

Definition 2.1
Let M, N be A-modules and $f : M \longrightarrow N$ a map. Then, we say that f is an *A-module homomorphism* or an *A-linear map* if it satisfies:

$$\begin{aligned} f(x + y) &= f(x) + f(y) \qquad \forall\ x, y \in M \\ f(ax) &= a \cdot f(x) \qquad \forall\ a \in A \text{ and } x \in M \end{aligned}$$

Note that if A is a field, then a module homomorphism is the same as a Linear Transformation of vector spaces.

2.1.2 Module of Homomorphisms from M to N

The set of all A-module homomorphisms from M to N can be thought of as a module over A.
Let us define $f+g$ and af for $f,g : M \longrightarrow N$ and $a \in A$ as

$$(f+g)(x) = f(x) + g(x)$$
$$(af)(x) = a \cdot f(x)$$

This module is called the *module of A-module homomorphisms from M to N* and is denoted by $\text{Hom}_A(M,N)$.
For any module M, there is a natural isomorphism

$$\text{Hom}_A(A,M) \cong M$$

The idea being, any A-module homomorphism from A to M is uniquely determined by $f(1)$ which can be any element in M.

2.2 Submodules and Quotient Modules

In simple words, a submodule, M' of M is a normal subgroup of M which is closed under multiplication by elements of A.
The abelian group ${}^{M}/_{M'}$ then inherits the A-module structure from M, defined by

$$a(x+M') = ax + M'$$

Some natural examples of submodules occur during homomorphisms.
Consider the A-ring homomorphism $f : M \longrightarrow N$

$$\text{Ker}(f) = \{x \in M \mid f(x) = 0\}$$

is a submodule of M.
Similarly, the image of f is the set

$$\text{Im}(f) = f(M)$$

is a submodule of N along with the cokernel, which is the quotient submodule of N.

$$\text{Coker}(f) = {}^{N}\Big/_{\text{Im}(f)}$$

2.3 Operation on Submodules

Let M be an A-module and $\{M_i\}_{i\in\mathscr{I}}$ be a family of submodules of M.
Then, the *sum* $\sum M_i$ of the submodules is the set fo all (finite) sums $\sum x_i$ where $x_i \in M_i$ for all i.
The sum is the smallest submodule containing all the M_i.

Proposition 2.1

Suppose $M_1, M_2 \lhd M$ be A-submodules of M. Then,

$$M_1 + M_2 \lhd M$$

Proof. Let $x \in M_1$ and $y \in M_2$ and $a \in A$. We know that $M_1 + M_2$ is a normal subgroup of M.

$$a(x+y) = ax + ay \in M_1 + M_2 \quad \text{since} \quad ax \in M_1 \text{ and } ay \in M_2$$

Hence, $M_1 + M_2 \lhd M$. □

Proposition 2.2

Suppose $M_1, M_2 \lhd M$ be A-submodules of M. Then,

$$M_1 \cap M_2 \lhd M$$

Proof. Clearly, $M_1 \cap M_2$ is a normal subgroup of M.
Consider $x \in M_1 \cap M_2$. Then, $x \in M_1$ and $x \in M_2$ and $ax \in M_1$ and $ax \in M_2$ for all $a \in A$.
$\implies ax \in M_1 \cap M_2 \implies M_1 \cap M_2 \lhd M$. □

Note:-

The intersection $\bigcap M_i$ is again a submodule of M and hence, the submodules of M form a complete lattice with respect to inclusion.

2.3.1 Isomorphism Theorems

Theorem 2.1 First Isomorphism Theorem

Let M, N be A-modules and

$$f : M \longrightarrow N$$

be a A-module homomorphism. Then,

$$M \Big/ \operatorname{Ker} f \cong \operatorname{Im} f$$

Theorem 2.2 Second Isomorphism Theorem

Let M be an A-module and let $L \lhd N \lhd M$ be submodules of M. Then,

$$M/L \Big/ N/L \cong M/N$$

Proof. Define a homomorphism

$$\begin{aligned} \theta : M/L &\longrightarrow M/N \\ x + L &\mapsto x + N \end{aligned}$$

The kernel of this homomorphism is

$$\begin{aligned} x \in \operatorname{Ker}(\theta) &\implies x + L \mapsto 0 + N \\ &\implies x \mapsto 0 + N/L \\ &\implies x \in N/L \\ \therefore \operatorname{Ker}(\theta) &= N/L \end{aligned}$$

Using First Isomorphism Theorem, we get

$$M/L \Big/ N/L \cong M/N$$ □

Theorem 2.3 Third Isomorphism Theorem

Let M be an A-module and let $M_1, M_2 \lhd M$. Then,

$$(M_1 + M_2)/M_1 \cong M_2 \Big/ (M_1 \cap M_2)$$

Proof. Consider the homomorphism defined by

$$\begin{aligned} \theta : M_2 &\longrightarrow (M_1 + M_2)/M_1 \\ x &\longrightarrow x + M_1 \end{aligned}$$

The homomorphism is surjective and the kernel is

$$\begin{aligned}\operatorname{Ker}(\theta) &= \{x \in M_2 \mid x + M_1 = 0 + M_1\} \\ &= \{x \in M_2 \mid x \in M_1\} \\ \operatorname{Ker}(\theta) &= M_1 \cap M_2\end{aligned}$$

Using the first isomorphism theorem, we get

$$(M_1 + M_2) \big/ M_1 \cong M_2 \Big/ (M_1 \cap M_2)$$

□

2.3.2 Ideal Product

We can not, in general define the product of two modules but we can define the product of a module with an ideal.

$$\mathfrak{a}M \coloneqq \{ax \mid a \in A \text{ and } x \in M\}$$

Claim 2.1

If $N, P \lhd M$ are submodules of M, then we can define

$$(N\colon P) \coloneqq \{a \in A \mid aP \subseteq N\}$$

Then $(N\colon P)$ is an ideal of A.

Proof. $a, b \in (N\colon P) \implies aP, bP \subseteq N$.
Clearly, $\implies aP + bP \subseteq N$ and $abP \subseteq N$ and hence, $ab \in (N\colon P)$.
Consider $r \in A$. $arP \subseteq aP \subseteq N$ and hence, $ar \in (N, P)$. □

Particularly, the ideal $(0\colon M)$ is called the *annihilator* of M.

Definition 2.2 Faithful Module

An A-module M is called *faithful* if $\operatorname{Ann}(M) = 0$.

Proposition 2.3

For any A-module M and submodules $N, P \lhd M$,

1. $\operatorname{Ann}(N + P) = \operatorname{Ann}(N) \cap \operatorname{Ann}(P)$
2. $(N\colon P) = \operatorname{Ann}\left((N + P) \big/ N\right)$

Proof.

1. $a \in \operatorname{Ann}(N + P) \implies an = 0 \ \forall\ n \in N$ and $ap = 0 \ \forall\ p \in P$ and hence, $a \in \operatorname{Ann}(N) \cap \operatorname{Ann}(P)$.

   Conversely, $a \in \operatorname{Ann}(N) \cap \operatorname{Ann}(P) \implies a(n + p) = an + ap = 0.$ and this implies $a \in \operatorname{Ann}(N + P)$.

   Hence proved.

2. $a \in (N\colon P) \implies aP \subseteq N \implies a(P + N) \subseteq (0 + N) \implies a \in \operatorname{Ann}\left((N + P) \big/ N\right)$.

   Conversely, $a \in \operatorname{Ann}\left((N + P) \big/ N\right) \implies a(p + N) = (0 + N) \ \forall\ p \in P \implies aP \subseteq N \implies a \in (N\colon P)$.

   Hence proved.

□

2.3.3 Generators

The set

$$Ax := (x) := \{ax \mid a \in A\}$$

for some $x \in M$ is a submodule of M and is called the submodule generated by x.

If

$$M = \sum_{i \in \mathscr{I}} Ax_i$$

then $\{x_i\}_{i \in \mathscr{I}}$ are called the *generators* of M.
This means every element of M can be expressed (not necessarily uniquely) as a finite linear combination of the x_i with coefficients in A.
An A-module M is said to be *finitely generated* if it has a finite set of generators.

2.4 Direct Sum and Product

If M, N are A-modules, then the *direct sum* of M and N is defined as

$$M \oplus N := \{(m, n) \mid m \in M \text{ and } n \in N\}$$

is an A-module with the obvious coordinate wise addition and scalar multiplication.
More generally, if $\{M_i\}_{i \in \mathscr{I}}$ is a family of A-modules, then the *direct sum* of the modules is defined as

$$\bigoplus_{i \in \mathscr{I}} M_i := \{(m_i)_{i \in \mathscr{I}} \mid m_i \in M_i \text{ and finitely many } m_i \neq 0\}$$

If we drop the condition that the m_i are finitely many, then we get the *direct product* of the modules.

$$\prod_{i \in \mathscr{I}} M_i := \{(m_i)_{i \in \mathscr{I}} \mid m_i \in M_i\}$$

If the indexing set is finite, the direct product is the same as the direct sum, but need not be in general.

2.4.1 Ring

Suppose the ring A is a direct product $\prod_{i=1}^{n} A_i$.
Then the set of all elements of the form

$$(0, 0, \cdots, a_i, \cdots, 0)$$

with $a_i \in A_i$ is an ideal $\mathfrak{a}_i$ of A.
(It is not a subring (except in trivial cases) since the identity element 1 is not in the ideal.)
If we consider the ring A as a module over itself, then A is a direct sum of the ideals $\mathfrak{a}_i$.

$$A = \mathfrak{a}_1 \oplus \mathfrak{a}_2 \oplus \cdots \oplus \mathfrak{a}_n$$

The identity element of $\mathfrak{a}_i$, say e_i is an idempotent element in A and we can also observe that

$$\mathfrak{a}_i = (e_i)$$

(Here, we are looking at e_i being an element of the module generating a submodule by the action of the ring where the submodule is the ideal)

2.5 Finitely Generated Modules

Definition 2.3 Free A-module

An A-module M is called *free* if it is isomorphic to an A-module of the form $\bigoplus_{i\in\mathscr{I}} M_i$ where

$$M_i \cong A \,(\text{as an } A\text{-module})$$

The notation $A^{(\mathscr{I})}$ is sometimes used.

Proposition 2.4

M is a finitely generated A-module $\iff$ M is isomorphic to a quotient of A^n for some $n \in \mathbb{N}$.

Proof. ($\implies$) Suppose $x_1, \cdots, x_n$ generate M. Let us define an A-linear map onto M by

$$\phi : A^n \to M$$
$$(a_1, \cdots, a_n) \mapsto a_1x_1 + \cdots + a_nx_n$$

ϕ, being surjective, using the first isomorphism theorem, we can say

$$M \cong A^n \Big/ \mathrm{Ker}(\phi)$$

($\impliedby$) Now, we have a surjective A-linear map A^n onto M.
If $e_i = (0, \cdots, 1, \cdots, 0)$, then clearly, $\{\phi(e_i)\}_{(1\leqslant i\leqslant n)}$ generate M. □

Proposition 2.5

Let M be a finitely generated A-module and $\mathfrak{a}$ be an ideal of A, and let ϕ be an A-module endomorphism of M such that $\phi(M) \subseteq \mathfrak{a}M$. Then ϕ satisfies an equation of the form

$$\phi^n + a_1\phi^{n-1} + \cdots + a_n = 0$$

where $a_i \in \mathfrak{a}$.

Proof. Let $x_1, \cdots, x_n$ be a set of generators of M. Then, each $\phi(x_i) \in \mathfrak{a}M$, and so we can write

$$\phi(x_i) = \sum_{j=1}^{n} a_{ij}x_j \quad \left(1 \leqslant i \leqslant n; a_{ij} \in \mathfrak{a}\right)$$

$$\implies \sum_{j=1}^{n} \left(\delta_{ij}\phi - a_{ij}\right) x_j = 0 \quad \text{where } \delta_{ij} = 1 \text{ if } i = j \text{ and } 0 \text{ otherwise}$$

Suppose $T = \left\{\delta_{ij}\phi - a_{ij}\right\}_{ij}$ be a matrix. We have $Tx = 0$.
Multiplying by $\mathrm{Adj}(T)$ on the left, we get

$$\mathrm{Adj}(T)\; Tx = 0$$
$$\implies \det(T) = 0$$

Expanding $\det(T)$, we get the desired equation. □

Corollary 2.1

Let M be a finitely generated A-module and let $\mathfrak{a}$ be an ideal of A such that $\mathfrak{a}M = M$. Then, there exists an $x \equiv 1 \pmod{\mathfrak{a}}$ such that $xM = 0$.

Proof. Putting ϕ as the identity map, we get

$$x = 1 + a_1 + \cdots + a_n$$

where $a_i \in \mathfrak{a}$. □

2.5.1 Nakayama's Lemma

Theorem 2.4 Nakayama's Lemma

Let M be a finitely generated A-module and let $\mathfrak{a}$ be an ideal of A contained in the jacobson radical $\mathfrak{R}$ of A. Then,

$$\mathfrak{a}M = M \implies M = 0$$

Proof. We have $xM = 0$ for some $x \equiv 1 \pmod{\mathfrak{a}}$ using the corollary above. Now, since $\mathfrak{a}$ is contained in the jacobson radical, we have $\mathfrak{a}$ is a unit since $x \equiv 1 \pmod{\mathfrak{a}}$ and hence

$$M = x^{-1}xM = 0$$

□

Alternate proof. Suppose $M \neq 0$ and let $u_1, \ldots, u_n$ be a minimal set of generators of M.
Then, we have $u_n \in \mathfrak{a}M$ and hence, we have the equation

$$\begin{aligned} u_n &= a_1u_1 + \cdots + a_nu_n \qquad a_i \in \mathfrak{a} \\ \implies (1 - a_n)\, u_n &= a_1u_1 + \cdots + a_{n-1}u_{n-1} \end{aligned}$$

Since $a_n \in \mathfrak{R}$, we get $1 - a_n$ to be a unit and can show that a_n belongs to the submodule generated by $u_1, \ldots, u_{n-1}$ which is a contradiction. □

Corollary 2.2

Let M be a finitely generated A-module, $N \lhd M$, and let $\mathfrak{a} \subseteq \mathfrak{R}$ be an ideal of A. Then,

$$M = \mathfrak{a}M + N \implies M = N$$

Proof. Taking modulo N on both sides, we get

$$M/N = (\mathfrak{a}M + N)/N = \mathfrak{a}M/N = \mathfrak{a}M/N$$

Now, applying Nakayama's lemma, to M/N, we get

$$M/N = 0 \implies M = N$$

□

Proposition 2.6

Let A be a local ring, $\mathfrak{m}$ be its maximal ideal and $k = A/\mathfrak{m}$ be the residue field.
Let M be a finitely generated A-module. Since $M/\mathfrak{m}M$ is annihilated by $\mathfrak{m}$, it is naturally a $A/\mathfrak{m}$-module, that is, a k-vector space and is hence, finite-dimensional.

Let $x_i (1 \leqslant i \leqslant n)$ be elements of M whose images in $M/\mathfrak{m}M$ form a basis in this vector space.
Then, the x_i generate M.

Proof. Let N be a submodule of M generated by x_i.
Then, the composition map

$$N \longrightarrow M \longrightarrow M/\mathfrak{m}M$$

maps N onto $M/\mathfrak{m}M$.
This implies

$$N + \mathfrak{m}M = M \implies N = M$$

using the corollary above. □

Modules 2

2.6 Exact Sequences

A sequence of A-modules and A-module homomorphisms

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

is said to be exact at M_i if

$$\operatorname{Im}(f_i) = \operatorname{Ker}(f_{i+1})$$

The sequence is said to be exact if it is exact at every M_i.
In particular,

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

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

3. $0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$ is exact $\iff$ f is injective and g is surjective.

In the last example, g induces a homomorphism $M \big/ f(M) = \operatorname{Coker}(f)$ onto M''.
A sequence of type 3 is called a *short exact sequence.*
Any long exact sequence of A-modules can be split into short exact sequences.

2.6.1 Right exactness of the functor $\operatorname{Hom}_A(-, N)$

Proposition 2.7
Let

$$M' \xrightarrow{u} M \xrightarrow{v} M'' \longrightarrow 0$$

be a sequence of A-modules and homomorphisms. Then, the sequence is exact if and only if for all A-modules N, the sequence

$$\operatorname{Hom}_A(M', N) \xleftarrow{\bar{u}} \operatorname{Hom}_A(M, N) \xleftarrow{\bar{v}} \operatorname{Hom}_A(M'', N) \longleftarrow 0$$

is exact.

Proof.
$(\Longrightarrow)$
For the if part, suppose that the sequence is exact.
Consider the sequence

$$\operatorname{Hom}_A(M', N) \xleftarrow{\bar{u}} \operatorname{Hom}_A(M, N) \xleftarrow{\bar{v}} \operatorname{Hom}_A(M'', N) \longleftarrow 0$$

for some A-module N.

The maps $\bar{u}$ and $\bar{v}$ are defined as

$$\bar{u}(f) = f \circ u \colon M' \longrightarrow M \longrightarrow N \quad \text{ and } \quad \bar{v}(f'') = f'' \circ v \colon M \longrightarrow M'' \longrightarrow N$$

We need to prove 2 things (exactness at 2 places):

1. $\bar{v}$ is injective or $\operatorname{Ker}\bar{v} = 0$.

2. $\operatorname{Im}\bar{v} = \operatorname{Ker}\bar{u}$.

First, we prove that $\operatorname{Ker}\bar{v} = 0$.

$$\begin{aligned} f'' \in \operatorname{Ker}\bar{v} &\implies f'' \circ v(m) = 0 \ \forall\ m \in M \\ &\implies f'' \circ v(M) = 0 \\ &\implies f''(M'') = 0 \implies f'' = 0 \end{aligned}$$

Now, we prove that

$$\operatorname{Im}\bar{v} = \operatorname{Ker}\bar{u}$$

Consider some $f \in \operatorname{Im}\bar{v}$. We need to show that $f \in \operatorname{Ker}\bar{u}$.
Then, there exists $f'' \in \operatorname{Hom}_A(M'', N)$ such that $f = f'' \circ v$.
This is equivalent to showing that $\bar{u}(f) = 0$ or $f \circ u(M') = 0$.

$$f \circ u(M') = f'' \circ v \circ u(M') = f'' \circ v \circ \operatorname{Im}(u) = f'' \circ v \circ \operatorname{Ker}(v) = f'' \circ 0 = 0$$

Hence, we showed that

$$\operatorname{Im}\bar{v} \subseteq \operatorname{Ker}\bar{u}$$

Now, suppose that $f \in \operatorname{Ker}\bar{u}$. We need to show that $f \in \operatorname{Im}\bar{v}$.
To show that $f \in \operatorname{Im}\bar{v}$, we need to construct a function $f'' \in \operatorname{Hom}_A(M'', N)$ such that $f = \bar{v}(f'') = f'' \circ v$.
We know that v is surjective. So, for every $m'' \in M''$, there exists $m \in M$ such that $v(m) = m''$ and hence, we can define a function f'' given by $f''(m'') = f''(v(m)) = f(m)$.
We need to show that this map is well-defined. Suppose

$$m'' = v(m_1) = v(m_2)$$

Then, we need to prove that $f(m_1) = f(m_2)$.
Since

$$v(m_1) = v(m_2) \implies m_1 - m_2 \in \operatorname{Ker}(v) \subseteq \operatorname{Ker}(f) \qquad f = f'' \circ v$$

This forces $f(m_1) = f(m_2)$ and hence, f'' is well-defined.

($\Longleftarrow$)
Now, given the exactness of the sequence

$$\begin{tikzcd} \operatorname{Hom}_A(M', N) & \operatorname{Hom}_A(M, N) \arrow[l, "\bar{u}"'] & \operatorname{Hom}_A(M'', N) \arrow[l, "\bar{v}"'] & 0 \arrow[l] \end{tikzcd}$$

for all A-modules N, we need to show that the sequence

$$\begin{tikzcd} M' \arrow[r, "u"] & M \arrow[r, "v"] & M'' \arrow[r] & 0 \end{tikzcd}$$

is exact.
Similar to the previous proof, we need to show 2 things:

1. v is surjective or $\operatorname{Im} v = M''$.

2. $\operatorname{Im} u = \operatorname{Ker} v$.

Notice that $\bar{v}$ is injective for all A-modules N and hence, let us put

$$N = M'' \big/ \mathrm{Im}(v)$$

We need to show that $N = 0$.
Consider some $f'' \in \mathrm{Hom}_A\left(M'', M'' \big/ \mathrm{Im}(v)\right)$.
Notice that $\bar{v}(f'') = f'' \circ v = 0$.
Since $\bar{v}$ is injective, we have $f'' = 0$.

$$\implies \mathrm{Hom}_A\left(M'', M'' \big/ \mathrm{Im}(v)\right) = 0 \implies M'' \big/ \mathrm{Im}(v) = 0 \implies M'' = \mathrm{Im}(v)$$

Now, since we know that

$$\mathrm{Ker}(\bar{u}) = \mathrm{Im}(\bar{v}) \implies f'' \circ v \circ u = 0 \ \forall \ f'' \in \mathrm{Hom}_A(M'', N)$$

Putting $f'' = 1$, the identity function, we get

$$v \circ u = 0 \implies \mathrm{Im}(u) \subseteq \mathrm{Ker}(v)$$

Finally, consider

$$N = M \big/ \mathrm{Im}(u)$$

The natural map

$$\phi : M \to M \big/ \mathrm{Im}(u) \quad \in \quad \mathrm{Hom}_A\left(M, M \big/ \mathrm{Im}(u)\right)$$

Notice that

$$\bar{u}(\phi) = \phi \circ u = 0 \implies \phi \in \mathrm{Ker}(\bar{u}) = \mathrm{Im}(\bar{v})$$

Hence, there is a function

$$\psi : M'' \to M \big/ \mathrm{Im}(u) \quad \text{s.t.} \quad \phi = \psi \circ v$$

And so, notice that

$$\mathrm{Ker}(v) \subseteq \mathrm{Ker}(\phi) = \mathrm{Im}(u)$$

And thus,

$$\mathrm{Ker}(v) = \mathrm{Im}(u)$$

and we are done. □

2.6.2 Left exactness of the functor $\mathrm{Hom}_A(M, -)$

Proposition 2.8
Let

$$\begin{tikzcd} 0 \arrow[r] & N' \arrow[r, "u"] & N \arrow[r, "v"] & N'' \end{tikzcd}$$

be a sequence of A-modules and homomorphisms. Then, the sequence is exact if and only if for all A-modules M, the sequence

$$\begin{tikzcd} 0 \arrow[r] & \mathrm{Hom}_A(M, N') \arrow[r, "\bar{u}"] & \mathrm{Hom}_A(M, N) \arrow[r, "\bar{v}"] & \mathrm{Hom}_A(M, N'') \end{tikzcd}$$

is exact.

Proof.
The functions $\bar{u}$ and $\bar{v}$ are defined as

$$\bar{u}(f) = u \circ f \qquad \bar{v}(f) = v \circ f$$

($\Longrightarrow$)
We need to show 2 things:

1. $\bar{u}$ is injective or $\text{Ker}(\bar{u}) = 0$.
2. $\text{Im}(\bar{u}) = \text{Ker}(\bar{v})$.

Consider some $f' \in \text{Hom}_A(M, N')$

$$\begin{aligned} f' \in \text{Ker}(\bar{u}) &\implies \bar{u}(f') = u \circ f' = 0 \\ &\implies \text{Im}(f') \subseteq \text{Ker}(u) = 0 \\ &\implies f' = 0 \implies \text{Ker}(\bar{u}) = 0 \end{aligned}$$

$\text{Im}(\bar{u}) \subseteq \text{Ker}(\bar{v})$ can be shown by proving

$$\bar{v} \circ \bar{u} = 0$$

For some $f' \in \text{Hom}_A(M, N')$,

$$\bar{v} \circ \bar{u}(f') = v \circ u \circ f'$$

We know that

$$v \circ u(n) = 0 \ \forall \ n' \in N' \implies v \circ u \circ f' = 0$$

Now, to prove $\text{Ker}(\bar{v}) \subseteq \text{Im}(\bar{u})$, consider some $f \in \text{Ker}(\bar{v})$. We have

$$\begin{aligned} & v \circ f(n) = 0 \ \forall \ n \in N \\ \implies & \text{Im}(f) \subseteq \text{Ker}(v) = \text{Im}(u) \\ \implies & \exists \ n' \in N' \text{ s.t. } u(n') = f(m) \ \forall \ m \in M \\ & \text{Define } f' : M \to N' \text{ by } f'(m) = n' \end{aligned}$$

Hence, we have

$$\bar{u}(f') = u \circ f' = f \implies f \in \text{Im}(\bar{u}) \implies \text{Ker}(\bar{v}) \subseteq \text{Im}(\bar{u})$$

($\Longleftarrow$)
We need to show 2 things:

1. u is injective or $\text{Ker}(u) = 0$.
2. $\text{Im}(u) = \text{Ker}(v)$.

□

Proposition 2.9
Let

$$\begin{tikzcd} 0 \arrow[r] & M' \arrow[r, "u"] \arrow[d, "f'"'] & M \arrow[r, "v"] \arrow[d, "f"'] & M'' \arrow[r] \arrow[d, "f''"] & 0 \\ 0 \arrow[r] & N' \arrow[r, "u'"'] & N \arrow[r, "v'"'] & N'' \arrow[r] & 0 \end{tikzcd}$$

be a commutative diagram of A-modules and homomorphisms, with the rows exact.
Then, there exists an exact sequence

$$0 \longrightarrow \text{Ker}(f') \xrightarrow{\bar{u}} \text{Ker}(f) \xrightarrow{\bar{v}} \text{Ker}(f'') \xrightarrow{d} \text{Coker}(f') \xrightarrow{\bar{u}'} \text{Coker}(f) \xrightarrow{\bar{v}'} \text{Coker}(f'') \longrightarrow 0$$

in which $\bar{u}, \bar{v}$ are restrictions of u, v and $\bar{u}', \bar{v}'$ are induced by u', v'.
The boundary homomorphism d is defined as

$$\text{If } x'' \in \text{Ker}(f'')$$

2.6.3 Additive Functions over Modules

Definition 2.4 Additive Functions

Let $\mathscr{C}$ be a class of A-modules and let λ be a function on $\mathscr{C}$ with values in $\mathbb{Z}$.
The function λ is said to be *additive* if for every short exact sequence

$$\begin{tikzcd} 0 \arrow[r] & M' \arrow[r, "u"] & M \arrow[r, "v"] & M'' \arrow[r] & 0 \end{tikzcd}$$

in $\mathscr{C}$, we have

$$\lambda(M') - \lambda(M) + \lambda(M'') = 0$$

Proposition 2.10

Let

$$\begin{tikzcd} 0 \arrow[r] & M_0 \arrow[r] & M_1 \arrow[r] & \cdots \arrow[r] & M_n \arrow[r] & 0 \end{tikzcd}$$

be an exact sequence of A-modules in which all the modules and the kernels of the homomorphisms belong to $\mathscr{C}$.
Then, for any additive function λ on $\mathscr{C}$, we have

$$\sum_{i=0}^{n}(-1)^i\lambda(M_i)$$

2.7 Tensor Product of Modules

Definition 2.5 *A*-bilinear

Let M, N, P be three A-modules. A mapping

$$f\colon M \times N \longrightarrow P$$

is said to be A-*bilinear* if
for each $x \in M$, the mapping $y \mapsto f(x,y)$ of N into P is A-linear and
for each $y \in N$, the mapping $x \mapsto f(x,y)$ of M into P is A-linear.

We will construct an A-module T, called the Tensor product of M and N, with the property that the A-bilinear mappings $M \times N \longrightarrow P$ are in a natural one-to-one correspondence with the A-linear mappings $T \longrightarrow P$, for all A-modules P.

Proposition 2.11 Existence of Tensor Product

Let M, N be A-modules. Then, there exists a pair (T, g) consisting of an A-module T and an A-bilinear mapping $g\colon M \times N \longrightarrow T$, with the following property:
Given any A-module P and any A-bilinear mapping

$$f\colon M \times N \longrightarrow P$$

there exists a unique A-linear mapping

$$f'\colon T \longrightarrow P$$

such that

$$f = f' \circ g$$

(in other words, every bilinear function on $M \times N$ factors through T).

Proof. Let C denote the free A-module $A^{(M\times N)}$.
The elements of C are formal linear combinations of elements of $M \times N$ with coefficients in A. That is, they are expressions of the form

$$c \in C \implies c = \sum_{i=1}^{n} a_i \cdot (m_i, n_i) \qquad \Big(a_i \in A, (x_i, y_i) \in M \times N\Big)$$

Let D be a submodule of C generated by all elements of C of the following types

$$\begin{gathered}(x + x', y) - (x, y) - (x', y)\\ (x, y + y') - (x, y) - (x, y')\\ (ax, y) - a \cdot (x, y)\\ (x, ay) - a \cdot (x, y)\end{gathered}$$

Now, let us define

$$T = {}^{C}/_{D}$$

For each basis element (x, y) of C, let $x \otimes y$ denote its image in T.
Then, T is an A-module generated by the elements of the form $x \otimes y$, for $x \in M$ and $y \in N$.
Also, from our definitions, we have

$$\begin{gathered}(x + x') \otimes y' = x \otimes y + x' \otimes y\\ x \otimes (y + y') = x \otimes y + x \otimes y'\\ (ax) \otimes y = a\,(x \otimes y) = x \otimes (ay)\end{gathered}$$

Equivalently, the mapping

$$g\colon M \times N \longrightarrow T$$

denoted by

$$g(x,y) = x \otimes y$$

is A-bilinear.
Any map f of $M \times N$ into an A-module P extends by linearity to an A-module homomorphism

$$f' : C \longrightarrow P$$

Suppose in particular that f is A-bilinear. Then, from the definitions, f' vanishes on all the generators of D and hence, on the whole of D, and therefore induces a well-defined A-linear mapping $f' : T \longrightarrow P$ such that $f'(x \otimes y) = f(x,y)$.
The map f' is uniquely determined by the proposition and hence, satisfies the conditions of the proposition. □

Proposition 2.12 Uniqueness of Tensor Product

The tensor product of M and N is unique up to isomorphism. That is, if (T,g) and (T',g') are two pairs as in the proposition, then there exists a unique isomorphism

$$j : T \longrightarrow T' \qquad \text{s.t.} \qquad j \circ g = g'$$

Proof. Replacing (P,f) with (T',g'), we get a unique

$$j' : T' \longrightarrow T$$

such that

$$g' = j' \circ g$$

Each of the compositions $j' \circ j$ and $j \circ j'$ must be identity and hence, j is an isomorphism. □

Note:-

The notation $x \otimes y$ is inherently ambiguous unless we specify the tensor product to which it belongs.
Suppose M', N' be submodules of M, N respectively. Then, it can happen that $x \otimes y$ as an element of $M \times N$ is zero whilst $x \otimes y$ as an element of $M' \times N'$ is non-zero.
An example is the case where

$$A = \mathbb{Z} \quad M = \mathbb{Z}, N = \mathbb{Z}/2\mathbb{Z} \quad M' = 2\mathbb{Z}, N' = \mathbb{Z}$$

Here, the element $2 \otimes 1$ is zero as an element of $\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ but non-zero as an element of $2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Definition 2.6 Tensor Product

The module thus constructed is called the Tensor product of M and N, and is denoted by $M \otimes_A N$ or $M \otimes N$ when there is no ambiguity.

If $(x_i)_{i \in I}$ and $(y_j)_{j \in J}$ are two families of generators of M and N respectively, then

$$(x_i \otimes y_j)_{i \in I, j \in J}$$

is a family of generators of $M \otimes N$.

Corollary 2.3

Let $x_i \in M$ and $y_i \in N$ be such that

$$\sum x_i \otimes y_i = 0 \qquad \text{in } M \otimes N$$

Then, there exist finitely generated submodules $M_0 \lhd M$ and $N_0 \lhd N$ such that

$$\sum x_i \otimes y_i = 0 \qquad \text{in } M_0 \otimes N_0$$

Proof. In the existence proof, if we had $\sum x_i \otimes y_i = 0$ in $M \otimes N$, then we would have □

We will never need to use the construction of the tensor product but only use the Bilinear property of the tensor product.

2.7.1 Tensor Product of Multilinear Mappings

Instead of starting with bilinear mappings, we could have started with multilinear mappings and then constructed the tensor product.

$$f\colon M_1 \times M_2 \times \cdots \times M_r \longrightarrow P$$

defined in the same way and construct the tensor product

$$T \coloneqq M_1 \otimes M_2 \otimes \cdots \otimes M_r$$

generated by the elements

$$x_1 \otimes x_1 \otimes \cdots \otimes x_r \quad (x_i \in M_i, 1 \leqslant i \leqslant r)$$

Definition 2.7 Tensor Product of Multilinear Mappings

Let $M_1, \cdots, M_r$ be A-modules. Then there exists a pair (T, g) as in the proposition consisting of an A-module T and an A-multilinear mapping

$$g\colon M_1 \times M_2 \times \cdots \times M_r \longrightarrow T$$

with the following property:
Given any A-module P and any A-multilinear mapping

$$f\colon M_1 \times M_2 \times \cdots \times M_r \longrightarrow P$$

there exists a unique A-linear mapping

$$f'\colon T \longrightarrow P$$

such that

$$f' \circ g = f$$

Moreover, if (T, g) and (T', g') are two such pairs, then there exists a unique isomorphism

$$j\colon T \longrightarrow T' \quad \text{s.t.} \quad j \circ g = g'$$

The module T is called the Tensor product of $M_1, \cdots, M_r$ and is denoted by

$$T = M_1 \otimes_A M_2 \otimes_A \cdots \otimes_A M_r$$

2.7.2 Properties of Tensor Product

Proposition 2.13

Let M, N, P be A-modules. Then, there exist unique isomorphisms

1. $M \otimes N \longrightarrow N \otimes M$
2. $(M \otimes N) \otimes P \longrightarrow M \otimes (N \otimes P) \longrightarrow M \otimes N \otimes P$
3. $(M \oplus N) \otimes P \longrightarrow (M \otimes P) \oplus (N \otimes P)$
4. $A \otimes M \longrightarrow M$

Proof.
The point in each case is to show that the obvious isomorphisms are well-defined using the definition of the tensor product.

1. Let us define our homomorphism as

$$\begin{aligned} f\colon M \otimes N &\longrightarrow N \otimes M \\ x \otimes y &\longmapsto y \otimes x \end{aligned}$$

Consider the R-(multi)linear map

$$\begin{aligned} g\colon M \times N &\longrightarrow P = N \otimes M \\ (x, y) &\mapsto y \otimes x \end{aligned}$$

Now, g induces an R-(multi)linear maps

$$M \times N \xrightarrow{g_1} M \otimes N \xrightarrow{f} P = N \otimes M$$

where

$$f(x \otimes y) = y \otimes x$$

and hence, f is well-defined.

To prove that f is an isomorphism, let us construct f^{-1} from $N \otimes M \longrightarrow M \otimes N$ as the natural inverse of f and it is well-defined by symmetry.

2.

□

Exercise 2.1

Let A, B be rings and let M be an A-module, P be a B-module and N an (A, B)-bimodule.
That is, N is simultaneously an A and B module and the two structures are compatible in the sense that

$$a(xb) = (ax)b \ \forall \ a \in A, b \in B, x \in N$$

Then, $M \otimes_A N$ is naturally a B-module and $N \otimes_B P$ is naturally an A-module and we have

$$(M \otimes_A N) \otimes_B P \cong M \otimes_A (N \otimes_B P)$$

2.7.3 Tensors of Homomorphisms

Suppose we have A-linear maps

$$f\colon M \longrightarrow M', \quad g\colon N \longrightarrow N'$$

Define

$$h\colon M \times N \longrightarrow M' \otimes N' \qquad h(x, y) = f(x) \otimes g(y)$$

It can be easily checked that h is an A-bilinear map and hence, induces a homomorphism

$$f \otimes g\colon M \otimes N \longrightarrow M' \otimes N' \qquad (f \otimes g)(x \otimes y) = f(x) \otimes g(y)$$

If we have

$$f'\colon M' \longrightarrow M'', \quad g'\colon N' \longrightarrow N''$$

then clearly, the homomorphisms $(f' \circ f) \otimes (g' \circ g)$ and $(f' \otimes g') \circ (f \otimes g)$ agree on all elements of the form $x \otimes y$ in $M \otimes N$. Since these elements generate $M \otimes N$ as an A-module,

$$(f' \circ f) \otimes (g' \circ g) = (f' \otimes g') \circ (f \otimes g)$$

2.8 Restriction and Extension of scalars

Let

$$f : A \longrightarrow B$$

be a ring homomorphism.

2.8.1 Restriction of Scalars

If we have a B-module N, we can view it as an A-module by defining the action of $a \in A$ on $x \in N$ as

$$a \cdot x \coloneqq f(a) \cdot x$$

The A-module formed is said to be obtained from N by *restricting the scalars*.

> **Proposition 2.14** Restriction of Scalars preserves finitely generatedness
>
> Suppose N is finitely generated as a B-module and let
>
> $$f : A \longrightarrow B$$
>
> be a ring homomorphism. Then, N is finitely generated as an A-module.

Proof. Let $y_1, \cdots, y_n$ generate N over B and let $x_1, \cdots, x_n$ generate B over A. Then, $x_i y_j$ generate N over A. □

2.8.2 Extension of Scalars

Now, let M be an A-module. Since we have seen that B can be regarded as an A-module, we can form an A-module

$$M_B \coloneqq B \otimes_A M$$

In fact, M_B has a natural B-module structure given by

$$b \cdot (b' \otimes x) = bb' \otimes x \quad \forall\, b, b' \in B, x \in M$$

The B-module M_B is said to be obtained from M by *extension of scalars*.

> **Proposition 2.15** Extension of Scalars preserves finitely generatedness
>
> Suppose M is finitely generated as an A-module and let
>
> $$f : A \longrightarrow B$$
>
> be a ring homomorphism. Then, M_B is finitely generated as a B-module.

Proof. If $x_1, \cdots, x_n$ generate M over A, then $1 \otimes x_i$ generate M_B over B. □

2.9 Exactness properties of tensor product

Let

$$f: M \times N \longrightarrow P$$

be a A-bilinear map.
For each $x \in M$, the mapping

$$\begin{aligned} \phi_x : N &\longrightarrow P \\ y &\longmapsto f(x,y) \end{aligned}$$

is a A-linear map from N to P and hence, f gives rise to a A-linear map from $M \longrightarrow \mathrm{Hom}_A(N,P)$.

$$\begin{aligned} \phi : M &\longrightarrow \mathrm{Hom}_A(N,P) \\ x &\longmapsto \phi_x \\ (x,y) &\longmapsto \phi(x)(y) \end{aligned}$$

and is bilinear in $x \in M$ and $y \in N$.
Hence, the set S of all A-bilinear mappings from $M \times N$ to P is in natural one-to-one correspondence with

$$\mathrm{Hom}_A(M, \mathrm{Hom}_A(N,P))$$

On the other hand, S is in one-to-one correspondence with

$$\mathrm{Hom}_A(M \otimes_A N, P)$$

by the universal property of the tensor product.
Hence, we have a canonical isomorphism

$$\boxed{\mathrm{Hom}_A(M \otimes_A N, P) \cong \mathrm{Hom}_A(M, \mathrm{Hom}_A(N,P))}$$

Proposition 2.16 Right Exactness of Tensor Product

Let

$$M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$$

be an exact sequence of A-modules and f and g are A-linear maps. Let N be an A-module.
Then, the sequence

$$M' \otimes_A N \xrightarrow{f \otimes_A 1} M \otimes_A N \xrightarrow{g \otimes_A 1} M'' \otimes_A N \longrightarrow 0$$

where 1 denotes the identity map on N is exact.

Chapter 3

Rings and modules of fractions

3.1 Introduction and Definition

The formation of rings of fractions and the localization of rings is a very important tool in commutative algebra. They correspond to the algebro-geometric picture to concentrating attention on an open set or near a point.

3.1.1 Field of fractions over an integral domain

The procedure by which one constructs $\mathbb{Q}$ from $\mathbb{Z}$ can be extended to any integral domain A and produces the *field* of fractions of A.
Construct the equivalence relation $\sim$ on the pairs of the integral domain A by declaring

$$(a, s) \sim (b, t) \iff a \cdot t - b \cdot s = 0$$

Reflexivity and symmetry are easy to check.

Proof for Transitivity.
Suppose we have $(a, s) \sim (b, t)$ and $(b, t) \sim (c, u)$.
Then we need to prove that $(a, s) \sim (c, u)$.
We have

$$\begin{aligned} at - bs = 0 \text{ and } bu - ct &= 0 \\ \implies atu - bsu &= 0 \\ \implies atu - bct &= 0 \\ \implies t\,(au - bc) &= 0 \end{aligned}$$

Now, we know that $t \neq 0$ and A is an integral domain. Therefore, $au - bc = 0$ and hence

$$(a, s) \sim (c, u)$$

□

This works only if A is an integral domain since proving that the relation is transitive involves cancelling.
That is, the fact that A has no non-trivial zero divisors is crucial.
Hence, we define the field of fractions of A as

$$A \times A^{\times} /_{\sim}$$

where $A^{\times}$ is the set of non-zero elements of A.
It is easy to check that this is a field.

3.1.2 Localization of a ring at a multiplicative subset

Definition 3.1 Multiplicatively Closed Subset

Let A be a ring and S be a subset of A.
Then S is said to be *multiplicatively closed* if $1 \in S$ and S is closed under multiplication.

We can now define the localization of a ring at a multiplicative subset. Let S be a multiplicatively closed subset of A.
Define a relation

$$\sim : A \times S$$

as follows

$$(a, s) \sim (b, t) \iff (at - bs)\, u = 0 \text{ for some } u \in S$$

Clearly, this relation is reflexive and symmetric.

Proof for Transitivity.
Suppose we have $(a, s) \sim (b, t)$ and $(b, t) \sim (c, u)$. Then we need to prove that $(a, s) \sim (c, u)$.
For some $v, w \in S$, we have

$$\begin{aligned} (at - bs)\, v = 0 &\text{ and } (bu - ct)\, w = 0 \\ (at - bs)\, vuw = 0 &\text{ and } (bu - ct)\, wsv = 0 \\ \implies (atuvw - cstvw) = 0 &\implies (au - cs)\, tvw = 0 \end{aligned}$$

Since S is multiplicatively closed, $tvw \in S$. □

Thus, $\sim$ is an equivalence relation.

Definition 3.2 Localization of a ring

We define the localization of A at a multiplicatively closed subset S as

$$S^{-1}A := {}^{A \times S}\big/_{\sim}$$

where $\sim$ is the equivalence relation defined as

$$(a, s) \sim (b, t) \iff (at - bs)\, u = 0 \text{ for some } u \in S$$

The elements of $S^{-1}A$ are denoted by ${}^{a}/_{s}$ where $a \in A$ and $s \in S$.

3.1.3 Localization as a ring of fractions

We can define addition and multiplication on $S^{-1}A$ as follows

$$\begin{aligned} \frac{a}{s} + \frac{b}{t} &= \frac{at + bs}{st} \\ \frac{a}{s} \cdot \frac{b}{t} &= \frac{ab}{st} \end{aligned}$$

The identity element of $S^{-1}A$ is $\frac{1}{1}$.

Claim 3.1

The addition and multiplication of the elements of $S^{-1}A$ is well-defined.

Proof. We need to prove

$$\frac{a}{s} + \frac{b}{t} = \frac{at + bs}{st} = \frac{a_1 t_1 + b_1 s_1}{s_1 t_1} \quad \text{where } \frac{a_1}{s_1} = \frac{a}{s} \quad \text{and } \frac{b_1}{t_1} = \frac{b}{t}$$

We know that for some $u, v \in S$, we have

$$(a_1 s - a s_1)\, u = 0 \text{ and } (b_1 t - b t_1)\, v = 0$$

Simplifying, we have

$$\begin{aligned}(a_1s - as_1)\,tt_1uv = 0 \text{ and } (b_1t - bt_1)\,ss_1uv = 0\\ (a_1t_1st - ats_1t_1)\,uv = 0 \text{ and } (b_1s_1st - bss_1t_1)\,uv = 0\\ \implies \Big((a_1t_1 + b_1s_1)\,st - (at + bs)\,s_1t_1\Big)uv = 0\\ \implies \boxed{\frac{a_1t_1 + b_1s_1}{s_1t_1} = \frac{at + bs}{st}}\end{aligned}$$

Now, we need to prove that

$$\frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st} = \frac{a_1b_1}{s_1t_1}$$

Similarly,

$$\begin{aligned}(a_1s - as_1)\,u = 0 \text{ and } (b_1t - bt_1)\,v = 0\\ (a_1s - as_1)\,b_1tuv = 0 \text{ and } (b_1t - bt_1)\,as_1uv = 0\\ (a_1b_1st - ab_1s_1t)\,uv = 0 \text{ and } (ab_1s_1t - abs_1t_1)\,uv = 0\\ \implies (a_1b_1st - abs_1t_1)\,uv = 0\\ \implies \boxed{\frac{a_1b_1}{s_1t_1} = \frac{ab}{st}}\end{aligned}$$

□

3.2 Some properties of localizations

We will also have a ring homomorphism

$$f\colon A \longrightarrow S^{-1}A \quad \text{defined as } f(a) = \frac{a}{1}$$

Note that this is not injective in general.
For example, consider $A = \mathbb{Z}_6$ and $S = \{1, 3\}$.
We will have $f(0) = \frac{0}{1}$ and $f(2) = \frac{2}{1} = \frac{6}{3} = \frac{0}{1} = f(0)$.

Proposition 3.1 Universal Property of Localization

Let $g\colon A \longrightarrow B$ be a ring homomorphism such that $g(s)$ is a unit for all $s \in S$. Then there exists a unique ring homomorphism

$$h\colon S^{-1}A \longrightarrow B$$

such that $g = h \circ f$.

Proof. For the uniqueness, suppose h satisfies the above property. Then, we have

$$g(a) = h \circ f(a) \quad \forall\ a \in A \implies h\left(\frac{a}{1}\right) = g(a)$$

For any $s \in S$, we have

$$h(s) \cdot h\left(\frac{1}{s}\right) = h\left(\frac{s}{s}\right) = h\left(\frac{1}{1}\right) = g(1) \implies h\left(\frac{1}{s}\right) = g(s)^{-1}$$

Hence, we will have

$$h\left(\frac{a}{s}\right) = g(a) \cdot g(s)^{-1}$$

which is uniquely determined by g.
Consider the map

$$h\colon S^{-1}A \longrightarrow B \quad \text{defined as } h\left(\frac{a}{s}\right) = g(a) \cdot g(s)^{-1}$$

We need to prove that this is well-defined.
For the existence, consider $\frac{a}{s} = \frac{a_1}{s_1}$. Then, we have

$$(a_1 s - a s_1)\, u = 0 \text{ for some } u \in S$$

Applying g, we have

$$(g(a_1)g(s) - g(a)g(s_1))\, g(u) = 0$$

Now, since $g(u)$ is a unit, we have

$$g(a_1)g(s) = g(a)g(s_1) \implies g(a) \cdot g(s)^{-1} = g(a_1) \cdot g(s_1)^{-1}$$

and hence, h is well-defined. □

Proposition 3.2

The ring $S^{-1}A$ and the homomorphism

$$f \colon A \longrightarrow S^{-1}A \quad \text{defined as } f(a) = \frac{a}{1}$$

have the following properties:

1. $s \in S \implies f(s)$ is a unit in $S^{-1}A$
2. $f(a) = 0 \implies as = 0$ for some $s \in S$
3. Every element of $S^{-1}A$ is of the form $f(a) \cdot f(s)^{-1}$ for some $a \in A$ and $s \in S$

Proof.

1. $f(s) = \frac{s}{1}$ and when multiplied by $\frac{1}{s}$, we get 1 which proves that $f(s)$ is a unit.
2. $f(a) = 0 \implies f(a) = \frac{a}{1} = \frac{0}{1} \implies (a \cdot 1 - 0 \cdot 1)\, s = 0$ for some $s \in S$ which implies $as = 0$.
3. Clearly, any element of S is of the form $\frac{a}{s}$ which is precisely $f(a) \cdot f(s)^{-1}$.

□

Conversely, these three conditions determine the ring $S^{-1}A$ up to isomorphism.

Corollary 3.1

If S is a multiplicative subset of A and $g \colon A \longrightarrow B$ is a ring homomorphism such that

1. $s \in S \implies g(s)$ is a unit in B
2. $g(a) = 0 \implies as = 0$ for some $s \in S$
3. Every element of B is of the form $g(a) \cdot g(s)^{-1}$ for some $a \in A$ and $s \in S$

Then, there exists a unique isomorphism

$$h \colon S^{-1}A \longrightarrow B \quad \text{such that} \quad h \circ f = g$$

Proof. Using 1 and the universal property of localization, we have a unique homomorphism

$$h \colon S^{-1}A \longrightarrow B \quad \text{such that} \quad h \circ f = g \quad \text{defined by} \quad h\left(\frac{a}{s}\right) = g(a) \cdot g(s)^{-1}$$

We now need to prove that this is an isomorphism.
Using 3, notice that h is surjective. Consider the kernel of h.

$$\frac{a}{s} \in \operatorname{Ker} h \implies g(a) \cdot g(s)^{-1} = 0 \implies g(a) = 0$$

Using 2, we have $as = 0$ for some $s \in S$ which implies $\frac{a}{s} = \frac{0}{1}$. Hence, $\operatorname{Ker} h = \{0\}$ and h is injective. □

3.2.1 Localization at a prime ideal and an element

Let $\mathfrak{p}$ be a prime ideal of A. Then $S = A \setminus \mathfrak{p}$ is a multiplicatively closed subset of A. In fact,

Claim 3.2

For a ring A,

$$A \setminus \mathfrak{p} \text{ is multiplicatively closed} \iff \mathfrak{p} \text{ is a prime ideal}$$

Proof. Both the statements imply and are implied by

$$a \notin \mathfrak{p} \text{ and } b \notin \mathfrak{p} \implies ab \notin \mathfrak{p} \quad \forall\, a, b \in A$$

□

Definition 3.3 Localization at a prime ideal

Let $\mathfrak{p}$ be a prime ideal of A. We define

$$\boxed{A_{\mathfrak{p}} := S^{-1}A \quad \text{where} \quad S = A \setminus \mathfrak{p}}$$

Claim 3.3

The set of the elements of $A_{\mathfrak{p}}$ of the form

$$\mathfrak{m} := \left\{\tfrac{a}{s} \mid a \in \mathfrak{p}, s \in S\right\}$$

is a maximal ideal of $A_{\mathfrak{p}}$.

Proof. Suppose we have an element $\frac{b}{t}$ such that $\frac{b}{t} \notin \mathfrak{m}$.

$$\tfrac{b}{t} \notin \mathfrak{m} \implies b \notin \mathfrak{p} \implies b \in S$$

Now, this implies that $\frac{b}{t}$ is a unit and hence, $\mathfrak{m}$ is a maximal ideal. □

It proves that if we have an ideal $\mathfrak{a}$ that is not contained in $\mathfrak{m}$, then $\mathfrak{a}$ contains a unit.
Now, this means $\mathfrak{m}$ is the only maximal ideal of $A_{\mathfrak{p}}$.

$$\boxed{A_{\mathfrak{p}} \text{ is a local ring}}$$

The process of passing from A to $A_{\mathfrak{p}}$ is called *localization at a prime ideal.*
In case of $\mathbb{Z}$, $\mathbb{Z}_{(p)}$ is the ring of rational numbers with denominators co-prime to p.

Definition 3.4 Localization at an element

Let $f \in A$. We define

$$\boxed{A_f := S^{-1}A \quad \text{where} \quad S = \{f^n\}_{n \geqslant 0}}$$

The elements of A_f are of the form

$$\frac{a}{f^n} \quad \text{where} \quad a \in A \text{ and } n \geqslant 0$$

3.3 Localization using Modules

The construction of $S^{-1}A$ can be carried out through an A-module M in place of the ring A.
Define the relation

$$\sim : M \times S$$

as follows

$$(m, s) \sim (m', s') \iff \exists\, t \in S \text{ such that } (sm' - s'm)\, t = 0$$

As before, this is an equivalence relation and we define

$$S^{-1}M := (M \times S)/_{\sim}$$

The elements of $S^{-1}M$ are denoted by $\frac{m}{s}$ and

$$S^{-1}M \text{ is a } S^{-1}A\text{-module}$$

with the action

$$\frac{a}{s} \cdot \frac{m}{t} = \frac{am}{st}$$

When we have a prime ideal $\mathfrak{p}$ of A, we can consider

$$M_{\mathfrak{p}} := S^{-1}M \quad \text{where} \quad S = A \setminus \mathfrak{p}$$

and

$$M_f := S^{-1}M \quad \text{where} \quad S = \{f^n\}_{n \geqslant 0}$$

Also, when we have a A-module homomorphism

$$u \colon M \longrightarrow N$$

This gives rise to an $S^{-1}A$-module homomorphism

$$S^{-1}u \colon S^{-1}M \longrightarrow S^{-1}N$$

defined by

$$S^{-1}u\left(\frac{m}{s}\right) = \frac{u(m)}{s}$$

We also have

$$S^{-1}(v \circ u) = \left(S^{-1}v\right) \circ \left(S^{-1}u\right)$$

Proposition 3.3

The operation S^{-1} is exact. That is,

$$M' \xrightarrow{f} M \xrightarrow{g} M'' \text{ is exact at } M \qquad \Longrightarrow \qquad S^{-1}M' \xrightarrow{S^{-1}f} S^{-1}M \xrightarrow{S^{-1}g} S^{-1}M'' \text{ is exact at } S^{-1}M$$

Proof. We have

$$g \circ f = 0 \implies S^{-1}g \circ S^{-1}f = S^{-1}(g \circ f) = 0$$

Hence, we have

$$\operatorname{Im}\left(S^{-1}f\right) \subseteq \operatorname{Ker}\left(S^{-1}g\right)$$

To prove the reserve inclusion, suppose we have an element $\frac{m}{s} \in \operatorname{Ker}\left(S^{-1}g\right)$. Then, we have

$$S^{-1}g\left(\frac{m}{s}\right) = \frac{g(m)}{s} = 0 \implies \exists\ t \in S \text{ such that } tg(m) = 0 \implies tg(m) = g(tm) = 0$$

Hence, we have $tm \in \operatorname{Ker} g = \operatorname{Im} f$.

$$\therefore \exists\ m' \in M' \text{ such that } f(m') = tm \implies f\left(\frac{m'}{st}\right) = \frac{tm}{st} = \frac{m}{s}$$

This proves

$$\operatorname{Ker}\left(S^{-1}g\right) \subseteq \operatorname{Im}\left(S^{-1}f\right)$$

and we are done. □

The above proposition proves that if $M' \lhd M$ is a submodule, then $S^{-1}M' \lhd S^{-1}M$.

Corollary 3.2

Formation of fractions commutes with formation of finite sums, finite intersections and quotients. Precisely, if N, P are submodules of M, then

1. $S^{-1}(N+P) = S^{-1}N + S^{-1}P$
2. $S^{-1}(N \cap P) = S^{-1}N \cap S^{-1}P$
3. The $S^{-1}A$-modules are isomorphic

$$S^{-1}\left({}^{M}/_{N}\right) \cong \left(S^{-1}M\right) \Big/ \left(S^{-1}N\right)$$

Proof.

1. It is easy to check that

$$\frac{n+p}{s} \in S^{-1}(N+P) \text{ where } n \in N, p \in P \iff \frac{n}{s} + \frac{p}{s} \in S^{-1}N + S^{-1}P$$

2. One way is easy. It can be checked that

$$m \in N \cap P \implies \frac{m}{s} \in S^{-1}N \text{ and } \frac{m}{s} \in S^{-1}P \implies \frac{m}{s} \in S^{-1}N \cap S^{-1}P$$

For the other way,

$$\frac{m}{s} \in S^{-1}N \cap S^{-1}P \implies \exists\, n \in N, p \in P \text{ and } s_n, s_p \in S \text{ such that } \frac{m}{s} = \frac{n}{s_n} = \frac{p}{s_p}$$

This implies that

$$\exists\, t \in S \text{ such that } t\left(s_p n - s_n p\right) = 0 \implies w := t s_p n = t s_n p \in N \cap P$$

We now have

$$\frac{m}{s} = \frac{n}{s_n} = \frac{w}{t s_n s_p} \in S^{-1}(N \cap P)$$

3. Consider the exact sequence

$$N \longrightarrow M \longrightarrow {}^{M}/_{N}$$

Since the operation S^{-1} is exact, we have

$$S^{-1}N \longrightarrow S^{-1}M \longrightarrow S^{-1}\left({}^{M}/_{N}\right)$$

is exact and hence,

$$S^{-1}\left({}^{M}/_{N}\right) \cong \left(S^{-1}M\right) \Big/ \left(S^{-1}N\right)$$

□

Proposition 3.4

Let M be an A-module. Then, the $S^{-1}A$ modules are isomorphic

$$S^{-1}M \cong S^{-1}A \otimes_A M$$

More precisely, there is a unique isomorphism

$$f \colon S^{-1}A \otimes_A M \to S^{-1}M$$

such that

$$f\left(\frac{a}{s} \otimes m\right) = \frac{am}{s} \qquad \forall\, a \in A, m \in M, s \in S$$

Proof. The mapping

$$S^{-1}A \times M \longrightarrow S^{-1}M$$

given by

$$\left(\frac{a}{s}, m\right) \mapsto \frac{am}{s}$$

is A-bilinear and hence, by the universal property of tensor products, there is a unique A-module homomorphism

$$f\colon S^{-1}A \otimes_A M \longrightarrow S^{-1}M$$

which proves the uniqueness of f.
Clearly, f is surjective. To prove injectivity, suppose we have

$$\sum_i \frac{a_i}{s_i} \otimes m_i \in \operatorname{Ker} f$$

Let us define

$$s := \prod_i s_i \quad \text{and} \quad t_i := \prod_{j \neq i} s_j$$

Now, we have

$$\sum_i \left(\frac{a_i}{s_i} \otimes m_i\right) = \sum_i \left(\frac{a_i t_i}{s} \otimes m_i\right) = \sum_i \left(\frac{1}{s} \otimes a_i t_i m_i\right) = \frac{1}{s} \otimes \left(\sum_i a_i t_i m_i\right) = \frac{1}{s} \otimes m$$

where $m := \sum_i a_i t_i m_i$ is an element of M.
We have,

$$f\left(\frac{1}{s} \otimes m\right) = 0 \implies \frac{m}{s} = 0 \implies \exists\, t \in S \text{ such that } tm = 0$$

Hence,

$$\frac{1}{s} \otimes m = \frac{t}{st} \otimes m = \frac{1}{st} \otimes tm = \frac{1}{st} \otimes 0 = 0$$

which proves that f is injective. Hence, f is an isomorphism. □

Corollary 3.3

$S^{-1}A$ is a flat A-module.

Proof. TODO □

Proposition 3.5

If M, N are A-modules, there is a unique isomorphism of $S^{-1}A$-modules

$$f\colon S^{-1}M \otimes_{S^{-1}A} S^{-1}N \longrightarrow S^{-1}\left(M \otimes_A N\right)$$

such that

$$f\left(\frac{m}{s} \otimes \frac{n}{t}\right) = \frac{m \otimes n}{st} \qquad \forall\, m \in M, n \in N, s, t \in S$$

In particular, if $\mathfrak{p}$ is any prime ideal, then

$$M_{\mathfrak{p}} \otimes_{A_{\mathfrak{p}}} N_{\mathfrak{p}} \cong \left(M \otimes_A N\right)_{\mathfrak{p}}$$

as $A_{\mathfrak{p}}$-modules.

Proof. TODO Tensors □

3.4 Local Properties

Definition 3.1: Local Property

A property P of a ring A (or of an A-module M) is called a **local property** if

$$A \text{ (or } M\text{) has } P \iff A_{\mathfrak{p}} \text{ (or } M_{\mathfrak{p}}\text{) has } P \qquad \forall\ \mathfrak{p} \in \operatorname{Spec} A$$

where $A_{\mathfrak{p}} \coloneqq S^{-1}A$ and $S \coloneqq A \setminus \mathfrak{p}$ and $\operatorname{Spec} A$ is the set of prime ideals of A.

Proposition 3.6

Let M be an A-module. Then, the following are equivalent:

1. $M = 0$
2. $M_{\mathfrak{p}} = 0$ for all prime ideals $\mathfrak{p}$ of A
3. $M_{\mathfrak{m}} = 0$ for all maximal ideals $\mathfrak{m}$ of A

Proof. $(1 \implies 2 \implies 3)$ is clear. We prove $(3 \implies 1)$.
Suppose 3 holds and $M \neq 0$. Then, there exists $m \in M$ such that $m \neq 0$.
Consider $\mathfrak{a} = \operatorname{Ann}(m)$. Clearly, $\mathfrak{a} \neq A$ and hence, $\mathfrak{a} \subseteq \mathfrak{m}$ for some maximal ideal $\mathfrak{m}$ of A.
Consider the element $\frac{m}{1} \in M_{\mathfrak{m}}$. This element is zero and hence is killed by an element, $a \in A \setminus \mathfrak{m}$.
This impossible since $a \notin \mathfrak{m} \implies a \notin \mathfrak{a}$ but annihilates (x). □

Proposition 3.7

Let $\phi\colon M \longrightarrow N$ be an A-module homomorphism. Then, the following are equivalent:

1. ϕ is injective
2. $\phi_{\mathfrak{p}}\colon M_{\mathfrak{p}} \longrightarrow N_{\mathfrak{p}}$ is injective for all prime ideals $\mathfrak{p}$ of A
3. $\phi_{\mathfrak{m}}\colon M_{\mathfrak{m}} \longrightarrow N_{\mathfrak{m}}$ is injective for all maximal ideals $\mathfrak{m}$ of A

Proof. $(1 \implies 2)$

$$0 \longrightarrow M \longrightarrow N \text{ is exact} \implies 0 \longrightarrow M_{\mathfrak{p}} \longrightarrow N_{\mathfrak{p}} \text{ is exact}$$

and hence, $\phi_{\mathfrak{p}}$ is injective for all $\mathfrak{p}$.
$(2 \implies 3)$ is clear.
$(3 \implies 1)$ Notice that the sequence

$$\begin{tikzcd} 0 \arrow[r] & \ker\phi \arrow[r, "i"] & M \arrow[r, "\phi"] & N \end{tikzcd}$$

is exact and hence,

$$\begin{tikzcd} 0 \arrow[r] & \ker\phi_{\mathfrak{m}} \arrow[r, "i_{\mathfrak{m}}"] & M_{\mathfrak{m}} \arrow[r, "\phi_{\mathfrak{m}}"] & N_{\mathfrak{m}} \end{tikzcd}$$

is exact for all maximal ideals $\mathfrak{m}$ of A.
Since $\operatorname{Im}(i_{\mathfrak{m}}) = \operatorname{Ker}(\phi_{\mathfrak{m}}) = 0$, and using the fact that $i_{\mathfrak{m}}$ is an inclusion, we can conclude that $\operatorname{Ker}(\phi_{\mathfrak{m}}) = 0$ for all maximal ideals $\mathfrak{m}$ of A.
Hence, we have $(\ker\phi)_{\mathfrak{m}} = 0$ for all maximal ideals $\mathfrak{m}$ of A.
Using the previous proposition, we can conclude that $\ker\phi = 0$ and hence, ϕ is injective. □

3.4.1 Flatness as a Local Property

Proposition 3.8

Let M be an A-module. Then, the following are equivalent:

1. M is a flat A-module

2. $M_{\mathfrak{p}}$ is a flat $A_{\mathfrak{p}}$-module for all prime ideals $\mathfrak{p}$ of A
3. $M_{\mathfrak{m}}$ is a flat $A_{\mathfrak{m}}$-module for all maximal ideals $\mathfrak{m}$ of A

Proof. TODO □

3.5 Extended and Contracted Ideals in Rings of Fractions

Let A be a ring and $S \subseteq A$ be a multiplicative subset of A and let

$$\boxed{f\colon A \longrightarrow S^{-1}A \qquad a \mapsto \frac{a}{1}}$$

be the canonical map.
Let

$$\begin{aligned}\mathscr{C} &:= \left\{\mathfrak{a} \lhd A \mid \mathfrak{a} \text{ is a contraction of an ideal of } S^{-1}A\right\}\\ \mathscr{E} &:= \left\{\mathfrak{b} \lhd S^{-1}A \mid \mathfrak{b} \text{ is an extension of an ideal of } A\right\}\end{aligned}$$

If $\mathfrak{a}$ is an ideal in A, then the extension of $\mathfrak{a}$ is $S^{-1}\mathfrak{a}$ where the elements of $S^{-1}\mathfrak{a}$ are of the form $\frac{a}{s}$ where $a \in \mathfrak{a}$ and $s \in S$.

Proposition 3.9

1. Every ideal in $S^{-1}A$ is an extended ideal.
2. If $\mathfrak{a}$ is an ideal in A, then $\mathfrak{a}^{ec} = \cup_{s\in S}(\mathfrak{a} : s)$. Hence, $\mathfrak{a}^{e} = (1) \iff \mathfrak{a}$ meets S.
3. $\mathfrak{a} \in \mathscr{C} \iff$ No element of S is a zero divisor on ${}^{A}/_{\mathfrak{a}}$.
4. The prime ideals of $S^{-1}A$ are in one-to-one correspondence with the prime ideals of A that do not meet S.
5. The operation S^{-1} commutes with formation of finite sums, products, intersections and radicals.

Proof.

1. Let $\mathfrak{b}$ be an ideal in $S^{-1}A$. Consider some element in $\mathfrak{b}$, say $\frac{x}{s}$. Then, $\frac{x}{s} \cdot \frac{s}{1} = \frac{x}{1} \in \mathfrak{b}$.

   Hence, $x \in \mathfrak{b}^{c}$ and $\frac{x}{s} \in \mathfrak{b}^{ce}$. For this ideal, we have $\mathfrak{b} \subseteq \mathfrak{b}^{ce}$.

   Since for any general ideal, we have $\mathfrak{b} \supseteq \mathfrak{b}^{ce}$, we can conclude that $\mathfrak{b} = \mathfrak{b}^{ce}$ and hence, $\mathfrak{b} \in \mathscr{E}$.

2. Notice that any element of $\mathfrak{a}^{e}$ is of the form

   $$\sum_{i=1}^{n} \frac{a_i}{s_i} = \frac{a}{s} \quad \text{for some} \quad a \in \mathfrak{a} \quad \text{and} \quad s \in S$$

   after taking $s = s_1 \cdots s_n$.

   Also, notice that

   $$xs \in \mathfrak{a} \iff x(s) \subseteq \mathfrak{a}$$

   where (s) is the ideal generated by s.

   Now,

   $$\begin{aligned}\mathfrak{a}^{ec} &= \left\{x \in A \mid \frac{x}{1} = \frac{a}{s} \text{ for some } a \in \mathfrak{a}, s \in S\right\}\\ &= \{x \in A \mid xst \in \mathfrak{a} \text{ for some } a \in \mathfrak{a}, s, t \in S\}\\ &= \{x \in A \mid xs \in \mathfrak{a} \text{ for some } s \in S\}\\ &= \{x \in A \mid x(s) \subseteq \mathfrak{a} \text{ for some } s \in S\}\\ &= \cup_{s\in S}\{x \in A \mid x(s) \subseteq \mathfrak{a}\}\\ \mathfrak{a}^{ec} &= \cup_{s\in S}(\mathfrak{a} : s)\end{aligned}$$

   For the next part,

   $$\mathfrak{a}^{e} = \left\{\frac{a}{s} \mid a \in \mathfrak{a}, s \in S\right\}$$

The element $\frac{1}{1} \in \mathfrak{a}^e \iff$ there exists some $a \in \mathfrak{a}$ and $s \in S$ such that $\frac{a}{s} = \frac{1}{1}$.

This corresponds to $at = st$ for some $t \in S$ which is equivalent to $st \in \mathfrak{a}$.

Thus,

$$\frac{1}{1} \in \mathfrak{a}^e \iff \exists\, t \in S \text{ s.t. } t \in \mathfrak{a}$$

3. Notice that

$$\begin{aligned} & \mathfrak{a} \in \mathscr{C} \\ \iff & \mathfrak{a}^{ec} \subseteq \mathfrak{a} \qquad (\text{since } \mathfrak{a}^{ec} = \mathfrak{a} \text{ and } \mathfrak{a}^{ec} \supseteq \mathfrak{a} \text{ holds for any ideal}) \\ \iff & (xs \in \mathfrak{a} \text{ for some } s \in S \implies x \in \mathfrak{a}) \\ \iff & \left(\bar{x} \in {}^{A}/_{\mathfrak{a}}, \quad \bar{x}s = 0 \text{ for some } s \in S \implies \bar{x} = 0\right) \\ \iff & \text{No element of } S \text{ is a zero divisor on } {}^{A}/_{\mathfrak{a}} \end{aligned}$$

4. Consider some prime ideal $\mathfrak{q}$ in $S^{-1}A$. Then, $\mathfrak{q} = \left\{\frac{a}{s} \mid a \in \mathfrak{p}, s \in S\right\}$ for some prime ideal $\mathfrak{p}$ of A.

   If there is an element $\frac{a}{s} \in \mathfrak{q}$ such that $a \in S$, this implies that $\frac{1}{s} \in \mathfrak{q}$ and hence, $\mathfrak{q} = S^{-1}A$.

   Thus, we can assume that $a \notin S$ for any $a \in \mathfrak{p}$ and hence, $\mathfrak{p} \cap S = \emptyset$.

   Conversely, let $\mathfrak{p}$ be a prime ideal in A such that $\mathfrak{p} \cap S = \emptyset$.

   We want to show that $\mathfrak{q} = \left\{\frac{a}{s} \mid a \in \mathfrak{p}, s \in S\right\}$ is a prime ideal in $S^{-1}A$.

   Consider 2 elements $\frac{a}{s}, \frac{b}{t} \notin \mathfrak{q}$. We need to show that $\frac{a}{s} \cdot \frac{b}{t} \notin \mathfrak{q}$.

   Suppose $\frac{a}{s} \cdot \frac{b}{t} \in \mathfrak{q}$. Then, $\frac{ab}{st} \in \mathfrak{q} \implies abu \in \mathfrak{p}$ for some $u \in S$.

   But this implies that $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$ or $u \in \mathfrak{p}$ neither of which is possible.

5. Using the fact that every ideal in $S^{-1}A$ is an extended ideal, we can deduce that S^{-1} commutes with formation of finite sums and products. Intersections has been proven earlier.

   For radicals, we already have $\mathrm{r}(\mathfrak{a})^e \subseteq \mathrm{r}(\mathfrak{a}^e)$.
   Consider some element $\frac{a}{s} \in \mathrm{r}(\mathfrak{a}^e)$. Then, $\left(\frac{a}{s}\right)^n \in \mathfrak{a}^e$ for some $n \geqslant 1$.

   That is, $\frac{a^n}{s^n} \in \mathfrak{a}^e$ and hence, $a^n t \in \mathfrak{a}$ for some $t \in S$. If $t \notin \mathfrak{a}$, we are done.

   $t \in \mathfrak{a}$ TODO

□

Corollary 3.4

If $\mathfrak{N}$ is the nilradical of A, then $S^{-1}\mathfrak{N}$ is the nilradical of $S^{-1}A$.

Proof. S □

Corollary 3.5

If $\mathfrak{p}$ is a prime ideal of A, the prime ideals of a local ring $A_{\mathfrak{p}}$ are in one-to-one correspondence with the prime ideals of A that are contained in $\mathfrak{p}$.

Proof. Consider $S = A \setminus \mathfrak{p}$ in the 4th part of the proposition. □

Note:-

Thus, the passage from A to $A_{\mathfrak{p}}$ cuts of all the prime ideals that are not contained in $\mathfrak{p}$.
In the other direction, the passage from A to $A_{\mathfrak{p}}$ cuts of all the prime ideals except those containing $\mathfrak{p}$.

Hence, if $\mathfrak{p}$ and $\mathfrak{q}$ are prime ideals of A such that $\mathfrak{p} \supseteq \mathfrak{q}$, then localizing at $\mathfrak{p}$ and then taking quotient mod $\mathfrak{q}$ (these operations commute), we are restricting our attention to those prime ideals that lie between $\mathfrak{q}$ and $\mathfrak{p}$.

In particular, if $\mathfrak{p} = \mathfrak{q}$, we will be left with a field, called the residue field of A at $\mathfrak{p}$, which can be obtained either as the field of fractions at $A \big/ \mathfrak{p}$ or as the residue field of the local ring $A_{\mathfrak{p}}$.

Proposition 3.10

Let M be a finitely generated A-module, S a multiplicatively closed subset of A. Then,

$$S^{-1}\left(\operatorname{Ann}(M)\right) = \operatorname{Ann}(S^{-1}M)$$

Proof. If the proposition is true for M and N, then it is true for $M + N$.

$$\begin{aligned} S^{-1}\left(\operatorname{Ann}(M+N)\right) &= S^{-1}\left(\operatorname{Ann}(M) \cap \operatorname{Ann}(N)\right) \\ &= S^{-1}\left(\operatorname{Ann}(M)\right) \cap S^{-1}\left(\operatorname{Ann}(N)\right) \\ &= \operatorname{Ann}(S^{-1}M) \cap \operatorname{Ann}(S^{-1}N) \\ &= \operatorname{Ann}(S^{-1}M + S^{-1}N) \\ &= \operatorname{Ann}(S^{-1}(M+N)) \end{aligned}$$

Thus, it is enough to prove the proposition for M generated by one element.
We know that $M \cong A \Big/ \operatorname{Ann}(M)$ as an A-module. Hence, we have

$$S^{-1}M \cong S^{-1}\left(A \Big/ \operatorname{Ann}(M)\right) \cong S^{-1}A \Big/ S^{-1}\left(\operatorname{Ann}(M)\right)$$

Hence, we have $\operatorname{Ann}(S^{-1}M) = S^{-1}\left(\operatorname{Ann}(M)\right)$. □

Corollary 3.6

If N, P are submodules of an A-module M, and if P is finitely generated, then

$$S^{-1}(N : P) = \left(S^{-1}N : S^{-1}P\right)$$

Proof. We know that

$$(N : P) \cong \operatorname{Ann}\left((N+P) / N\right)$$

and now, we can apply the previous proposition. □

Proposition 3.11

Let $A \longrightarrow B$ be a ring homomorphism and let $\mathfrak{p}$ be a prime ideal in A. Then, $\mathfrak{p}$ is a contraction of a prime ideal of B if and only if $\mathfrak{p}^{ec} = \mathfrak{p}$.

Proof. ($\Longleftarrow$) is clear.
($\Longrightarrow$) Let $\mathfrak{p}^{ec} = \mathfrak{p}$. Let S be the image of $A \setminus \mathfrak{p}$ in B. Then, S is a multiplicatively closed subset of B.
Clearly, $\mathfrak{p}^e$ does not meet S and using (3.9), we can conclude that $S^{-1}B \neq B$ and is hence, contained in a maximal ideal $\mathfrak{m}$ of B.
If $\mathfrak{q}$ is the contraction of $\mathfrak{m}$ in B, then $\mathfrak{q}$ is prime, $\mathfrak{q} \cap S = \emptyset$ and $\mathfrak{p} \subseteq \mathfrak{q}$.
Hence, $\mathfrak{q}^c = \mathfrak{p}$. □

Chapter 4

Primary Decomposition

The decomposition of an ideal into primary ideals is a traditional pillar of ideal theory.
From another point of view primary decomposition provides a generalization of the factorization of an integer as a product of prime-powers.

4.1 Definition

A prime ideal in a ring A is in some sense a generalization of a prime number. The corresponding generalization of a power of a prime number is a primary ideal.

Definition 4.1

An ideal $\mathfrak{q}$ of a ring A is called **primary** if for any $x, y \in A$ $\mathfrak{q} \neq A$ and

$$xy \in \mathfrak{q} \implies x \in \mathfrak{q} \text{ or } y^n \in \mathfrak{q} \text{ for some } n \geqslant 1$$

Proposition 4.1 Equivalent Condition for primary

$\mathfrak{q}$ is primary $\iff$ $A \big/ \mathfrak{q} \neq 0$ and every zero-divisor in $A \big/ \mathfrak{q}$ is nilpotent.

Proof. ($\Longrightarrow$) Consider some zero-divisor $a + \mathfrak{q}$ of $A \big/ \mathfrak{q}$. Then there exists some $b + \mathfrak{q} \neq 0$ such that

$$(a + \mathfrak{q})(b + \mathfrak{q}) = ab + \mathfrak{q} = 0 + \mathfrak{q}$$

which implies that $ab \in \mathfrak{q} \implies ba \in \mathfrak{q}$. By definition of primary ideal, $a^n \in \mathfrak{q}$ or $b \in \mathfrak{q}$.
Since $b \notin \mathfrak{q}$, $a^n \in \mathfrak{q}$ for some $n \geqslant 1$. Then $(a + \mathfrak{q})^n = a^n + \mathfrak{q} = 0 + \mathfrak{q}$.
($\Longleftarrow$) Let $ab \in \mathfrak{q}$. If $a \in \mathfrak{q}$, we are done. Suppose $a \notin \mathfrak{q}$.
Then,

$$ab + \mathfrak{p} = 0 + \mathfrak{p} \text{ but } a + \mathfrak{p} \neq 0 + \mathfrak{p} \implies b + \mathfrak{q} \text{ is a zero-divisor in } A \big/ \mathfrak{q}$$

This implies that $b + \mathfrak{q}$ is nilpotent in $A \big/ \mathfrak{q}$.
Hence, $(b + \mathfrak{q})^n = b^n + \mathfrak{q} = 0 + \mathfrak{q}$ which implies $b^n \in \mathfrak{q}$. □

Proposition 4.2 Smallest prime ideal containing $\mathfrak{q}$

Let $\mathfrak{q}$ be a primary ideal of a ring A. Then, $\mathrm{r}(\mathfrak{q})$ is the smallest prime ideal containing $\mathfrak{q}$.

Proof. Consider some $x, y \in A$ such that $xy \in \mathrm{r}(\mathfrak{q})$. Then, $(xy)^n \in \mathfrak{q}$ for some $n \geqslant 1$.
By definition of primary ideal, $x^n \in \mathfrak{q}$ or $y^{nm} \in \mathfrak{q}$ for some $m \geqslant 1$.
If $x^n \in \mathfrak{q}$, then $x \in \mathrm{r}(\mathfrak{q})$ and if $y^{nm} \in \mathfrak{q}$, then $y \in \mathrm{r}(\mathfrak{q})$ thus implying that $\mathrm{r}(\mathfrak{q})$ is prime.

For the smallest part, let $\mathfrak{p}$ be a prime ideal containing $\mathfrak{q}$. Consider some element $a \in \mathrm{r}(\mathfrak{q})$.
$a^n \in \mathfrak{q} \subseteq \mathfrak{p}$ for some $n \geqslant 1$ implies that $a \in \mathfrak{p}$.
Hence, $\mathrm{r}(\mathfrak{q}) \subseteq \mathfrak{p}$. □

Definition 4.1 $\mathfrak{p}$-primary

An ideal $\mathfrak{q}$ of a ring A is called **$\mathfrak{p}$-primary** if $\mathfrak{q} \neq A$ and $\mathrm{r}(\mathfrak{q}) = \mathfrak{p}$.

4.2 Examples

The primary ideals in $\mathbb{Z}$ are precisely the ideals of the form (p^n) where p is a prime number and $n \geqslant 1$ including the zero ideal (0).

Example 4.1

Consider $A = k[x, y]$ where k is a field, $\mathfrak{q} = (x, y^2)$. Then,

$$A \big/ \mathfrak{q} \quad \cong \quad k[x] \Big/ (y^2)$$

where the zero-divisors are all the multiples of y and are hence nilpotent.
Hence, $\mathfrak{q}$ is primary and it's radical is $\mathfrak{p} = (x, y)$.
Here, we have

$$\mathrm{r}(\mathfrak{q})^2 = \mathfrak{p}^2 \subsetneq \mathfrak{q} \subsetneq \mathfrak{p} = \mathrm{r}(\mathfrak{q})$$

The above example shows that **a primary ideal need not be a power of a prime ideal**.
Conversely, we also show that **a power of a prime ideal** $\mathfrak{p}^n$ is **not necessarily primary** although it's radical is the prime $\mathfrak{p}$.

Example 4.2

Consider $A = k[x, y, z] \Big/ (xy - z^2)$. Let $\bar{x}, \bar{y}, \bar{z}$ denote the images of x, y, z respectively in A.
Consider the ideal $\mathfrak{p} = (\bar{x}, \bar{z})$. Clearly, $\mathfrak{p}$ is a prime ideal since

$$A \big/ \mathfrak{p} \quad \cong \quad k[y]$$

which is an integral domain.
Now, we have $\bar{z}^2 = \bar{x}\bar{y} \in \mathfrak{p}^2$. Clearly, $\bar{x} \notin \mathfrak{p}^2$.
Also, $\bar{y}^n \in \mathfrak{p}^2 \implies \bar{y} \in \mathrm{r}(\mathfrak{p}^2) = \mathfrak{p}$. But, $\bar{y} \notin \mathfrak{p}$ and hence, $\mathfrak{p}^2$ is not primary.

However, the powers of a maximal ideal are primary.

Proposition 4.3 Powers of a maximal $\mathfrak{m}$ are $\mathfrak{m}$-primary

If $\mathrm{r}(\mathfrak{a})$ is maximal, then $\mathfrak{a}$ is primary. In particular, the powers of a maximal ideal are primary.

Proof. Let $\mathrm{r}(\mathfrak{a}) = \mathfrak{m}$ be maximal. The image of $\mathfrak{m}$ in $A / \mathfrak{a}$ is the nilradical of $A / \mathfrak{a}$.
Hence, $A / \mathfrak{a}$ has only one prime ideal, which is the nilradical of $A / \mathfrak{a}$.
Hence, any element of $A / \mathfrak{a}$ is either a unit or nilpotent.
This implies that any zero-divisor in $A / \mathfrak{a}$ is nilpotent.
By proposition 4.1, $\mathfrak{a}$ is primary. □

4.3 Intersections of primary ideals

Lemma 4.1

Let $\mathfrak{q}_i$ where $1 \leqslant i \leqslant n$ are $\mathfrak{p}$-primary ideals of A. Then, $\mathfrak{q} = \bigcap_{i=1}^{n} \mathfrak{q}_i$ is $\mathfrak{p}$-primary.

Proof. We first show $\mathrm{r}(\mathfrak{q}) = \mathfrak{p}$.

$$\mathrm{r}(\mathfrak{q}) = \mathrm{r}\left(\bigcap_{i=1}^{n} \mathfrak{q}_i\right) = \bigcap_{i=1}^{n} \mathrm{r}(\mathfrak{q}_i) = \bigcap_{i=1}^{n} \mathfrak{p} = \mathfrak{p}$$

Now, we show that $\mathfrak{q}$ is primary. Consider some $ab \in \mathfrak{q}$ such that $a \notin \mathfrak{q}$.
There exists an i such that $a \notin \mathfrak{q}_i$. Then, $b \in \mathfrak{p}$.
Since $\mathrm{r}(\mathfrak{q}) = \mathfrak{p}$, we have $b^n \in \mathfrak{q}$ for some $n \geqslant 1$. □

Lemma 4.2

Let $\mathfrak{q}$ be a $\mathfrak{p}$-primary ideal of A and $x \in A$. Then,

1. $x \in \mathfrak{q} \implies (\mathfrak{q} \colon x) = (1)$.
2. $x \notin \mathfrak{q} \implies (\mathfrak{q} \colon x)$ is $\mathfrak{p}$-primary and hence, $\mathrm{r}\left(\mathfrak{q} \colon x\right) = \mathfrak{p}$.
3. $x \notin \mathfrak{p} \implies (\mathfrak{q} \colon x) = \mathfrak{q}$.

Proof.

1. By definition,

$$(\mathfrak{q} \colon x) = \{y \in A \colon yx \in \mathfrak{q}\}$$
$$x \in \mathfrak{q} \implies yx \in \mathfrak{q} \ \forall\ y \in A \implies (\mathfrak{q} \colon x) = (1)$$

2. Consider $xy \in \mathfrak{q}$. As $x \notin \mathfrak{q}$, $y \in \mathfrak{p}$. Hence, we have

$$\mathfrak{q} \subseteq (\mathfrak{q} \colon x) \subseteq \mathfrak{p}$$

   Taking radical, we have

$$\mathrm{r}\left(\mathfrak{q} \colon x\right) = \mathfrak{p}$$

   Consider $yz \in (\mathfrak{q} \colon x)$ with $y \notin \mathfrak{p}$. Then, $yzx \in \mathfrak{q}$ and hence, $zx \in \mathfrak{q}$ which implies that $z \in (\mathfrak{q} \colon x)$.

3. Since $x \notin \mathfrak{p}$, $x^n \notin \mathfrak{q}$ for any $n \geqslant 1$.

$$(\mathfrak{q} \colon x) = \{y \in A \colon yx \in \mathfrak{q}\} = \{y \in A \colon y \in \mathfrak{q}\} = \mathfrak{q}$$

□

4.3.1 Primary decomposition

Definition 4.2: Primary Decomposition

A **primary decomposition** of an ideal $\mathfrak{a}$ of a ring A is an expression of $\mathfrak{a}$ as an intersection of finitely many primary ideals, say $\mathfrak{q}_i$

$$\mathfrak{a} = \bigcap_{i=1}^{n} \mathfrak{q}_i$$

We then say that $\mathfrak{a}$ is **decomposable** or **reducible**.

Note:-

In general, a primary decomposition need not exist. In this chapter, we restrict ourselves to ideals which have a primary decomposition.

Definition 4.2 Minimal Primary Decomposition

A primary decomposition $\mathfrak{a} = \bigcap_{i=1}^{n} \mathfrak{q}_i$ is said to be **minimal** (or irredundant, or reduced, or normal) if

1. $\mathrm{r}(\mathfrak{q}_i) \neq \mathrm{r}(\mathfrak{q}_j)$ for any $i \neq j$.
2. $\mathfrak{q}_i \nsubseteq \bigcap_{j \neq i} \mathfrak{q}_j$ for all i.

Proposition 4.4

Let $\mathfrak{a}$ be an ideal of a ring A with a primary decomposition

$$\mathfrak{a} = \bigcap_{i=1}^{n} \mathfrak{q}_i$$

Then, $\mathfrak{a}$ has a minimal primary decomposition.

Proof. We can achieve the first condition by combining all the $\mathfrak{q}_i$ with the same radical into one using the lemma 4.3.
The second condition can be achieved by removing all the superfluous $\mathfrak{q}_i$. □

4.3.2 Uniqueness of primary decomposition

Theorem 4.1 1st uniqueness theorem

Let $\mathfrak{a}$ be a decomposable ideal and let

$$\mathfrak{a} = \bigcap_{i=1}^{n} \mathfrak{q}_i$$

be a minimal primary decomposition of $\mathfrak{a}$. Let $\mathfrak{p}_i = \mathrm{r}(\mathfrak{q}_i)$. Then, the $\mathfrak{p}_i$ are precisely the prime ideals $\mathrm{r}\,(\mathfrak{a} \colon x)\,(x \in A)$, and hence are independent of the particular decomposition of $\mathfrak{a}$.

Proof. Consider some $x \in A$.

$$(\mathfrak{a} \colon x) = \left(\bigcap_{i=1}^{n} \mathfrak{q}_i : x\right) = \bigcap_{i=1}^{n} (\mathfrak{q}_i : x)$$

Using lemma 4.3, we have

$$(\mathfrak{a} \colon x) = \bigcap_{i=1}^{n} (\mathfrak{q}_i : x) = \bigcap_{x \notin \mathfrak{q}_i}^{n} \mathfrak{p}_i$$

Suppose $\mathrm{r}(\mathfrak{a} \colon x)$ is prime (we assume this in order to show that $\mathfrak{p}_i$ occur in this form and vice versa).
Using proposition 1.11, we have

$$\mathrm{r}\,(\mathfrak{a} \colon x) = \mathfrak{p}_j \text{ for some } j \;\text{ s.t. } x \notin \mathfrak{q}_j$$

Hence, every prime ideal of the form $\mathrm{r}\,(\mathfrak{a} \colon x)$ is one of the $\mathfrak{p}_i$.
Now, we need to show that every $\mathfrak{p}_i$ occurs in the form $\mathrm{r}\,(\mathfrak{a} \colon x)$ for some $x \in A$.
Notice that since the decomposition is minimal, we have

$$\forall\ i,\ \exists\ x_i \notin \mathfrak{q}_i \;\text{ s.t. } x_i \in \bigcap_{j \neq i} \mathfrak{q}_j$$

Hence, $\mathrm{r}\,(\mathfrak{a} \colon x_i) = \mathfrak{p}_i$. □

Note:-

The prime ideals $\mathfrak{p}_i$ are said to **belong** to $\mathfrak{a}$ or **associated** to $\mathfrak{a}$.
The ideal $\mathfrak{a}$ is primary if and only if it has only one associated prime ideal.
The minimal elements of the set of associated prime ideals of $\mathfrak{a}$ are called the **minimal/isolated associated prime ideals** of $\mathfrak{a}$.
The others are called the **embedded associated prime ideals** of $\mathfrak{a}$.

Note:-

Note that in the above proof, coupled with lemma 4.3, we have shown that

$$\forall\ i,\ \exists\ x_i \in A \;\text{ s.t. }\; (\mathfrak{a} \colon x_i) \;\text{ is } \mathfrak{p}_i\text{-primary}$$

Considering ${}^{A}/_{\mathfrak{a}}$ as an A-module, theorem 4.3.2 is equivalent to saying that $\mathfrak{p}_i$ are precisely the prime ideals which occur as $\mathrm{r}\,(\mathrm{Ann}(x))$ for some $x \in {}^{A}/_{\mathfrak{a}}$.

Example 4.3

Consider $A = k[x,y]$ where k is a field. Let $\mathfrak{a} = (x^2, xy)$. Then, $\mathfrak{a}$ is decomposable since

$$\mathfrak{a} = \mathfrak{p}_1 \cap \mathfrak{p}_2^2 \quad \text{where } \mathfrak{p}_1 = (x) \text{ and } \mathfrak{p}_2 = (x,y) \text{ are prime}$$

$\mathfrak{p}_2$ being a maximal implies that $\mathfrak{p}_2^2$ is primary.
We have $\mathrm{r}(\mathfrak{p}_1) = \mathfrak{p}_1$ and $\mathrm{r}(\mathfrak{p}_2^2) = \mathfrak{p}_2$ and hence, $\mathrm{r}(\mathfrak{a}) = \mathfrak{p}_1 \cap \mathfrak{p}_2 = \mathfrak{p}_1$.

In the above example, we have $\mathfrak{p}_1 \subseteq \mathfrak{p}_2$ and hence, $\mathfrak{p}_2$ is an embedded associated prime ideal of $\mathfrak{a}$ while $\mathfrak{p}_1$ is an isolated associated prime ideal of $\mathfrak{a}$.

Proposition 4.5

Let $\mathfrak{a}$ be a decomposable ideal. Then, any prime ideal $\mathfrak{p} \supseteq \mathfrak{a}$ contains a minimal prime ideal belonging to / associated with $\mathfrak{a}$.
Thus, the minimal prime ideals belonging to $\mathfrak{a}$ are precisely the minimal elements of the set of prime ideals containing $\mathfrak{a}$.

Proof. Consider some prime ideal $\mathfrak{p} \supseteq \mathfrak{a}$. Then,

$$\begin{aligned} \mathfrak{p} &\supseteq \bigcap_{i=1}^{n} \mathfrak{q}_i \\ \implies \mathrm{r}(\mathfrak{p}) &\supseteq \bigcap_{i=1}^{n} \mathrm{r}(\mathfrak{q}_i) \\ \implies \mathfrak{p} &\supseteq \bigcap_{i=1}^{n} \mathfrak{p}_i \end{aligned}$$

Hence, by 1.11, we have $\mathfrak{p} \supseteq \mathfrak{p}_i$ for some i which shows that $\mathfrak{p}$ contains a minimal prime ideal belonging to $\mathfrak{a}$. □

Proposition 4.6

Let $\mathfrak{a}$ be a decomposable ideal, and let

$$\mathfrak{a} = \bigcap_{i=1}^{n} \mathfrak{q}_i$$

be a minimal primary decomposition and let $\mathfrak{p}_i = \mathrm{r}(\mathfrak{q}_i)$. Then,

$$\bigcup_{i=1}^{n} \mathfrak{p}_i = \{x \in A \mid (\mathfrak{a} : x) \neq \mathfrak{a}\}$$

In particular, if the zero ideal is decomposable, then the set D of zero-divisors in A is the union of the prime ideals belonging to / associated with the zero ideal.

Proof. If $\mathfrak{a}$ is decomposable, then 0 is decomposable in ${}^{A}/_{\mathfrak{a}}$.

$$0 = \bigcap_{i=1}^{n} \bar{\mathfrak{q}}_i \quad \text{where } \bar{\mathfrak{q}}_i \text{ is the image of } \mathfrak{q}_i \text{ in } {}^{A}/_{\mathfrak{a}}$$

Hence, it is enough to prove the last statement.
We know that

$$D = \bigcup_{x \in A} \mathrm{r}(0 : x)$$

From the proof of theorem 4.3.2, we have

$$\mathrm{r}(0 : x) = \bigcap_{x \notin \mathfrak{q}_j} \mathfrak{p}_j \subseteq \mathfrak{p}_j \text{ for some } j$$

Hence, we have

$$D \subseteq \bigcup_{j=1}^{n} \mathfrak{p}_j$$

Also from the proof of theorem 4.3.2, we have that each $\mathfrak{p}_i$ is of the form $\mathrm{r}\,(0\colon x)$ for some $x \in A$. Hence,

$$\bigcup_{j=1}^{n} \mathfrak{p}_j \subseteq D$$

□

Thus, (the zero ideal being decomposable)

$$D = \bigcup \mathfrak{p}_i \text{ where } \mathfrak{p}_i \text{ is associated to } 0$$
$$\mathfrak{N} = \bigcap \mathfrak{p}_i \text{ where } \mathfrak{p}_i \text{ is minimal and associated to } 0$$

4.4 Primary ideals under localization

Proposition 4.7

Let S be a multiplicatively closed subset of a ring A, and let $\mathfrak{q}$ be a $\mathfrak{p}$-primary ideal of A. Then,

1. $S \cap \mathfrak{p} \neq \phi \implies S^{-1}\mathfrak{q} = S^{-1}A$
2. $S \cap \mathfrak{p} = \phi \implies S^{-1}\mathfrak{q}$ is $S^{-1}\mathfrak{p}$-primary and it's contraction is $\mathfrak{q}$.

Proof.

1. Consider some $s \in S \cap \mathfrak{p}$. Then, $s \in \mathfrak{p} \implies s^n \in \mathfrak{q}$ for some $n \geqslant 1$.

   Hence,

   $$\frac{s^n}{1} \in S^{-1}\mathfrak{q} \implies \frac{s^n}{s^n} = \frac{1}{1} \in S^{-1}\mathfrak{q}$$

   which implies that $S^{-1}\mathfrak{q} = S^{-1}A$.

2. If $S \cap \mathfrak{p} = \phi$, then, using proposition 3.5(4), when $S \cap \mathfrak{p} = \phi$, we have

   $$s \in S \text{ and } as \in \mathfrak{q} \implies a \in \mathfrak{q} \implies \mathfrak{q}^{ec} = \mathfrak{q}$$

   Also from proposition 3.5(5), we have

   $$\mathrm{r}\,(\mathfrak{q}^e) = \mathrm{r}\left(S^{-1}\mathfrak{q}\right) = S^{-1}\mathfrak{p}$$

   To verify that $S^{-1}\mathfrak{q}$ is primary, consider

   $$\frac{a}{s} \cdot \frac{b}{t} \in S^{-1}\mathfrak{q} \implies \frac{ab}{st} \in S^{-1}\mathfrak{q}$$

   This boils down to $ab \in \mathfrak{q}$ and the proposition follows.

□

Definition 4.3 Contraction of an ideal in $S^{-1}A$

For an ideal $\mathfrak{a}$ and a multiplicatively closed subset S, the **contraction** of $\mathfrak{a}$ in $S^{-1}A$ is denoted by

$$S\,(\mathfrak{a}) := \text{Contraction of the ideal } S^{-1}\mathfrak{a} \lhd S^{-1}A \text{ where } \mathfrak{a} \lhd A$$

Proposition 4.8

Let S be a multiplicatively closed subset of a A and let $\mathfrak{a}$ be a decomposable ideal of A. Let

$$\mathfrak{a} = \bigcap_{i=1}^{n} \mathfrak{q}_i \quad \text{s.t.} \quad \mathfrak{p}_i = \mathrm{r}(\mathfrak{q}_i)$$

be a minimal primary decomposition of $\mathfrak{a}$.
Suppose the $\mathfrak{q}_i$ are numbered so that S meets $\mathfrak{p}_{m+1}, \dots, \mathfrak{p}_n$ but not $\mathfrak{p}_1, \dots, \mathfrak{p}_m$. Then,

$$S^{-1}\mathfrak{a} = \bigcap_{i=1}^{m} S^{-1}\mathfrak{q}_i \qquad \text{and} \qquad S(\mathfrak{a}) = \bigcap_{i=1}^{m} \mathfrak{q}_i$$

and these are minimal primary decompositions.

Proof. Using proposition 3.5(5) and proposition 4.4, we have

$$S^{-1}\mathfrak{a} = \bigcap_{i=1}^{n} S^{-1}\mathfrak{q}_i \tag{3.5(5)}$$

$$S^{-1}\mathfrak{a} = \bigcap_{i=1}^{m} S^{-1}\mathfrak{q}_i \tag{4.4}$$

and $S^{-1}\mathfrak{q}_i$ are $S^{-1}\mathfrak{p}_i$-primary for $i = 1, \dots, m$.
Since $\mathfrak{p}_i$ are distinct, $S^{-1}\mathfrak{p}_i$ are distinct and hence, we have a minimal primary decomposition of $S^{-1}\mathfrak{a}$.
Contracting both sides, we get

$$S(\mathfrak{a}) = \left(S^{-1}\mathfrak{a}\right)^c = \bigcap_{i=1}^{m} \left(S^{-1}\mathfrak{q}_i\right)^c = \bigcap_{i=1}^{m} \mathfrak{q}_i$$

using proposition 4.4 again. □

Definition 4.4 Set of associated isolated ideals

A set Σ of prime ideals belonging to / associated with $\mathfrak{a}$ is said to be **isolated** if it satisfies the following condition:

$$\mathfrak{p}' \text{ is a prime ideal associated with } \mathfrak{a} \text{ and } \mathfrak{p}' \subseteq \mathfrak{p} \text{ for some } \mathfrak{p} \in \Sigma \implies \mathfrak{p}' = \mathfrak{p}$$

Proposition 4.9

Let Σ be an isolated set of prime ideals associated with $\mathfrak{a}$ and let

$$S = A \setminus \bigcup_{\mathfrak{p} \in \Sigma} \mathfrak{p}$$

Then, S is multiplicatively closed and for any prime ideal $\mathfrak{p}'$ associated with $\mathfrak{a}$, we have

$$\mathfrak{p}' \in \Sigma \implies \mathfrak{p}' \cap S = \phi$$

$$\mathfrak{p}' \notin \Sigma \implies \mathfrak{p}' \nsubseteq \bigcup_{\mathfrak{p} \in \Sigma} \mathfrak{p} \implies \mathfrak{p}' \cap S \neq \phi \qquad \text{using proposition 1.11}$$

4.4.1 2nd uniqueness theorem

Theorem 4.2

Let $\mathfrak{a}$ be a decomposable ideal and let

$$\mathfrak{a} = \bigcap_{i=1}^{n} \mathfrak{q}_i$$

be a minimal primary decomposition of $\mathfrak{a}$ and let $\{\mathfrak{p}_{i_1}, \mathfrak{p}_{i_2}\}, \cdots, \mathfrak{p}i_m$ be an isolated set of prime ideals in $\mathfrak{a}$. Then,

$$\mathfrak{q}_{i_1} \cap \cdots \cap \mathfrak{q}_{i_m}$$

is independent of the decomposition.

Proof. We know that $\mathfrak{p}_i$ depend only on $\mathfrak{a}$ using theorem 4.3.2.
Also, from proposition 4.4, we have

$$q_{i_1} \cap \cdots \cap \mathfrak{q}_{i_m} = S(\mathfrak{a}) \quad \text{where } S = A \setminus \bigcup_{j=1}^{m} \mathfrak{p}_{i_j}$$

and hence depends only on $\mathfrak{a}$. □

In particular, we have

Corollary 4.1

The isolated primary components, the primary components $\mathfrak{p}_i$ corresponding to minimal prime ideals $\mathfrak{p}_i$ are uniquely determined by $\mathfrak{a}$.

Note:-

On the other hand, the embedded primary components are in general not uniquely determined bt $\mathfrak{a}$. If A is a noetherian ring, then there are in fact infinitely many choices for each embedded component (refer to chapter 8, exercise 1).

Chapter 5

Integral Dependence and Valuations

5.1 Integral Dependence

Definition 5.1: Integral Element

Let B be a ring and $A \subseteq B$ be a subring $(1 \in A)$. An element $x \in B$ is said to be **integral** over A if x is a root of a **monic** polynomial with coefficients in A.

$$x^n + a_1 x^{n-1} + \cdots + a_n = 0$$

Consider the case when $A = \mathbb{Z}$ and $B = \mathbb{Q}$. Suppose a rational number $\frac{r}{s}$ is integral over $\mathbb{Z}$ where $\gcd(r,s) = 1$.
Then, $\frac{r}{s}$ is a root of $x^m + a_1 x^{m-1} + \cdots + a_m = 0$ where $a_i \in \mathbb{Z}$.
Multiplying by s^m, we get

$$r^m + a_1 r^{m-1} s + \cdots + a_m s^m = 0$$

We get that $s \mid r^m$ and hence, $s = \pm 1$. Thus, $\frac{r}{s} \in \mathbb{Z}$.

Proposition 5.1

The following are equivalent

1. $x \in B$ is integral over A.
2. $A[x]$ is a finitely generated A-module.
3. $A[x]$ is contained in a subring C of B such that C is a f.g. A-module.
4. There exists a faithful $A[x]$-module M which is a f.g. A-module.

Proof. $(1 \implies 2)$ From the definition, we have

$$x^{n+r} = -\left(a_1 x^{n-1} + \cdots + a_n\right) x^r \quad \forall\ r \geqslant 0$$

Upon induction, we get that $A[x]$ is generated by $1, x, \ldots, x^{n-1}$.
$(2 \implies 3)$ Take $C = A[x]$.
$(3 \implies 4)$ Take $M = C$, which is a faithful $A[x]$-module since $yC = 0 \implies y \cdot 1 = 0$.
$(4 \implies 1)$ This follows from proposition 2.4 by taking ϕ to be multiplication by x and $\mathfrak{a}$ to be A.
We have that $xM \subseteq M = AM$ and hence, x satisfies a monic polynomial with coefficients in A since M is faithful. □

Corollary 5.1

Let $x_i (1 \leqslant i \leqslant n)$ be elements of B, integral over A. Then, $A[x_1, \ldots, x_n]$ is a finitely generated A-module.

Proof. By induction on n. The case $n = 1$ is covered in proposition 5.1.
Assume $n > 1$ and let $A[x_1, x_2, \cdots, x_{n-1}]$ be f.g. as an A module.

Now, $A[x_1, \dots, x_n - 1][x_n]$ is f.g. as an $A[x_1, \dots, x_{n-1}]$ module since x_n is integral over A and hence $A[x_1, \dots, x_{n-1}]$. Therefore, $A[x_1, \dots, x_n]$ is f.g. as an A-module. □

Corollary 5.2

The set C of elements of B which are integral over A is a subring of B containing A.

Proof. Consider some $x, y \in C$. Then, using $A[x, y]$ is f.g. as an A-module using corollary 5.1.
Hence, $x + y$ and xy are integral over A using proposition 5.1(3). □

Definition 5.1 Integral Closure

Let $A \subseteq B$ be rings. Then,

$$\bar{A} = C := \{x \in B \mid x \text{ is integral over } A\}$$

is called the **integral closure** of A in B.

Definition 5.2 Integrally Closed

Let $A \subseteq B$ be rings and $\bar{A} = C$ be the integral closure of A in B.
Then, A is said to be **integrally closed** in B if $C = A$ or $\bar{A} = A$.

Definition 5.3 Integral ring extension

Let $A \subseteq B$ be rings and $\bar{A} = C$ be the integral closure of A in B.
Then, B is said to be **integral over** A if $C = B$ or $\bar{A} = B$.

Note:-

Let $f: A \longrightarrow B$ be a ring homomorphism so that B is an A-algebra.
Then, f is said to be **integral** or B os said to be an **integral** A-algebra if B is integral over $f(A)$.
We showed that

$$\text{finite type} + \text{integral} = \text{finite}$$

Corollary 5.3 Transitivity of inegral dependence

If $A \subseteq B \subseteq C$ are rings such that B is integral over A and C is integral over B.
Then, C is integral over A.

Proof. Consider some $x \in C$. Then, x is integral over B and hence, satisfies a monic polynomial with coefficients in B.

$$x^n + b_1 x^{n-1} + \dots + b_n = 0 \quad b_i \in B$$

The ring $B' = A[b_1, \dots, b_n]$ is finitely generated as an A-module using corollary 5.1 (Since x is integral over B').
Hence, $B'[x]$ is finitely generated as an A-module using proposition 2.6 and hence x is integral over A using proposition 5.1(3) since $A[x] \subseteq B'[x]$. □

Corollary 5.4

Let $A \subseteq B$ be rings and let $C = \bar{A}$ be the integral closure of A in B.
Then, $C = \bar{A}$ is integrally closed in B.

Proof. We need to show that $\bar{\bar{A}} = \bar{A}$ or $\bar{C} = C$.
Consider some $x \in B$ such that x is integral over C. Then, x is integral over A using corollary 5.1.
Hence, $x \in C$ and hence, $\bar{C} = C$. □

Proposition 5.2 Integral dependence preserved over quotients

Let $A \subseteq B$ be rings and let B be integral over A.

Then, if $\mathfrak{b}$ is an ideal such that

$$\mathfrak{a} = \mathfrak{b}^c = A \cap \mathfrak{b} \implies {}^{B}/_{\mathfrak{b}} \text{ is integral over } {}^{A}/_{\mathfrak{a}}$$

Proof. Consider some $x \in B$. Then, x is integral over A and hence, satisfies a monic polynomial with coefficients in A.

$$x^n + a_1 x^{n-1} + \cdots + a_n = 0 \quad a_i \in A$$

Taking the equation modulo $\mathfrak{b}$, we get

$$(x + \mathfrak{b})^n + (a_1 + \mathfrak{a})(x + \mathfrak{b})^{n-1} + \cdots + (a_n + \mathfrak{a}) = 0$$

since $\mathfrak{a} = \mathfrak{b}^c$. □

Proposition 5.3 Integral dependence preserved over localizations

Let $A \subseteq B$ be rings and let B be integral over A.
If S is a multiplicative subset of A, then $S^{-1}B$ is integral over $S^{-1}A$.

Proof. Consider some $\frac{x}{s} \in S^{-1}B$.
Then, $\frac{x}{s}$ satisfies

$$\left(\frac{x}{s}\right)^n + \frac{a_1}{s}\left(\frac{x}{s}\right)^{n-1} + \cdots + \frac{a_n}{s^n} = 0 \quad a_i \in A$$

which shows that $\frac{x}{s}$ is integral over $S^{-1}A$. □

5.2 The going up theorem

Proposition 5.4

Let $A \subseteq B$ be integral domains and let B be integral over A. Then,

$$A \text{ is a field} \iff B \text{ is a field}$$

Proof. ($\Longrightarrow$) Consider some $x \in B \setminus \{0\}$. Then, x is integral over A and hence, satisfies a monic polynomial with coefficients in A. Consider the monic polynomial of least degree satisfied by x.

$$x^n + a_1 x^{n-1} + \cdots + a_n = 0 \quad a_i \in A$$

Now, we have $a_n \neq 0$. Otherwise, x would satisfy a monic polynomial of degree $< n$.
Therefore, we have

$$\begin{aligned} -a_n &= x\left(x^{n-1} + a_1 x^{n-2} + \cdots + a_{n-1}\right) \\ \implies x^{-1} &= -\frac{1}{a_n}\left(x^{n-1} + a_1 x^{n-2} + \cdots + a_{n-1}\right) \end{aligned}$$

which shows that $x^{-1} \in B$ and hence, B is a field.

($\Longleftarrow$) Conversely, consider some $x \in A \setminus \{0\}$.
Since $x \in B$ and B is a field, we have $x^{-1} \in B$.
Therefore, x^{-1} is integral over A and hence, satisfies a monic polynomial with coefficients in A.

$$x^{-m} + a_1 x^{-m+1} + \cdots + a_n = 0 \quad a_i \in A$$

Multiplying by x^{m-1}, we get

$$x^{-1} = -\left(a_1 + \cdots + a_n x^{m-1}\right)$$

which shows that $x^{-1} \in A$ since $x \in A$ and $a_i \in A \ \forall \ i$.
Hence, A is a field. □

Corollary 5.5

Let $A \subseteq B$ be rings and let B be integral over A.
Let $\mathfrak{q}$ be a prime ideal in B and let $\mathfrak{p} = \mathfrak{q}^c = A \cap \mathfrak{q}$.
Then, $\mathfrak{q}$ is maximal if and only if $\mathfrak{p}$ is maximal.

Proof. Since we know that a contraction of a prime ideal is prime, $\mathfrak{p}$ is prime.
Now, since ${}^{B}\big/_{\mathfrak{q}}$ is integral over ${}^{A}\big/_{\mathfrak{p}}$ which are both integral domains, using proposition 5.2, we get that ${}^{A}\big/_{\mathfrak{p}}$ is a field if and only if ${}^{B}\big/_{\mathfrak{q}}$ is a field.
And hence, $\mathfrak{p}$ is maximal if and only if $\mathfrak{q}$ is maximal. □

Corollary 5.6

Let $A \subseteq B$ be rings and let B is integral over A.
Let $\mathfrak{q}$ and $\mathfrak{q}'$ be prime ideals in B such that $\mathfrak{q} \subseteq \mathfrak{q}'$ and $\mathfrak{q}^c = \mathfrak{q}'^c = \mathfrak{p}$ say.
Then, $\mathfrak{q} = \mathfrak{q}'$.

Proof. Using proposition 5.1, we know that $B_{\mathfrak{p}}$ is integral over $A_{\mathfrak{p}}$.
Let $\mathfrak{m}$ be the extension of $\mathfrak{p}$ in $B_{\mathfrak{p}}$. and let $\mathfrak{n}, \mathfrak{n}'$ be extensions of $\mathfrak{q}, \mathfrak{q}'$ in $B_{\mathfrak{p}}$.
Then, $\mathfrak{m}$ is a maximal ideal of $A_{\mathfrak{p}}$ and $\mathfrak{n}^c = \mathfrak{n}'^c = \mathfrak{m}$.
By corollary 5.2, it follows that $\mathfrak{n}$ and $\mathfrak{n}'$ are maximal such that $\mathfrak{n} \subseteq \mathfrak{n}'$ which implies $\mathfrak{n} = \mathfrak{n}'$ and hence using 3.11 (4), we have $\mathfrak{q} = \mathfrak{q}'$. □

Theorem 5.1

Let $A \subseteq B$ be rings and let B be integral over A.
Let $\mathfrak{p}$ be a prime ideal in A. Then, there exists a prime ideal $\mathfrak{q}$ in B such that $\mathfrak{q} \cap A = \mathfrak{p}$.

Proof. By proposition 5.1, we know that $B_\mathfrak{p}$ is integral over $A_\mathfrak{p}$ and hence the diagram

$$\begin{tikzcd}
A \arrow[r] \arrow[d, "\alpha"'] & B \arrow[d, "\beta"'] \\
A_\mathfrak{p} \arrow[r] & B_\mathfrak{p}
\end{tikzcd}$$

is commutative where the horizontal arrows are inclusions and the vertical arrows are localizations.
Let $\mathfrak{n}$ be a maximal ideal in $B_\mathfrak{p}$. Then, $\mathfrak{n} \cap A_\mathfrak{p}$ is the unique maximal ideal of the local ring $A_\mathfrak{p}$ using corollary 5.2.
If $\mathfrak{q} = \beta^{-1}(\mathfrak{n})$, then $\mathfrak{q}$ is a prime ideal since it is a contraction of a prime ideal.
Hence, we have a prime ideal $\mathfrak{q}$ in B such that $\mathfrak{q} \cap A = \mathfrak{p}$. □

Theorem 5.2 Going up theorem

Let $A \subseteq B$ be rings and let B be integral over A. Let

$$\mathfrak{p}_1 \subseteq \mathfrak{p}_2 \subseteq \cdots \subseteq \mathfrak{p}_n$$

be a chain of prime ideals in A and

$$\mathfrak{q}_1 \subseteq \mathfrak{q}_2 \subseteq \cdots \subseteq \mathfrak{q}_m$$

be a chain of prime ideals $(m < n)$ in B such that

$$\mathfrak{q}_i \cap A = \mathfrak{p}_i \quad \forall\, i \in \{1, \dots, m\}$$

Then, the chain of prime ideals in B can be extended to a chain

$$\mathfrak{q}_1 \subseteq \mathfrak{q}_2 \subseteq \cdots \subseteq \mathfrak{q}_n$$

such that $\mathfrak{q}_i \cap A = \mathfrak{p}_i$ for all $i \in \{1, \dots, n\}$.

Proof. By induction, we can reduce the problem to the case when $n = 2$ and $m = 1$.
Consider the diagram

$$\begin{tikzcd}
A \arrow[r] \arrow[d, "\alpha"'] & B \arrow[d, "\beta"'] \\
A \big/ \mathfrak{p}_1 \arrow[r] & B \big/ \mathfrak{q}_1
\end{tikzcd}$$

where the horizontal arrows are inclusions and the vertical arrows are quotients.
Then, β is integral using proposition 5.1.
By theorem 5.2, there exists a prime ideal $\bar{\mathfrak{q}_2}$, say, in $B \big/ \mathfrak{q}_1$ such that $\bar{\mathfrak{q}_2} \cap A = \bar{\mathfrak{p}_2}$, the image of $\mathfrak{p}_2$ in $\bar{A}$.
Lifting back $\bar{\mathfrak{p}_2}$ to B and we have a prime ideal $\mathfrak{q}_2$ in B such that $\mathfrak{q}_2 \cap A = \mathfrak{p}_2$. □

Chapter 6

Chain Conditions

This chapter mainly focuses on imposing finiteness-conditions. The most convinient way is in the form of chain conditions. These apply to both rings and modules. In this chapter, we consider the case of modules.

6.1 Definitions

Definition 6.1 Ascending Chain Condition(ACC)

Let Σ be a set partially ordered by a relation $\leqslant$.
We say that Σ satisfies the ascending chain condition w.r.t. $\leqslant$ if every increasing sequence

$$x_1 \leqslant x_2 \leqslant \cdots \leqslant x_n \leqslant \cdots$$

in Σ is stationary. That is, $\exists\ n \in \mathbb{N}$ such that

$$x_m = x_n \ \forall\ m \geqslant n$$

Definition 6.2 Descending Chain Condition(DCC)

Let Σ be a set partially ordered by a relation $\leqslant$.
We say that Σ satisfies the descending chain condition w.r.t. $\leqslant$ if every decreasing sequence

$$x_1 \geqslant x_2 \geqslant \cdots \geqslant x_n \geqslant \cdots$$

in Σ is stationary. That is, $\exists\ n \in \mathbb{N}$ such that

$$x_m = x_n \ \forall\ m \geqslant n$$

Definition 6.3 Maximal and Minimal conditions

The Maximal condition is equivalent to the ACC and states that every non-empty subset of Σ has a maximal element.
The Minimal condition is equivalent to the DCC and states that every non-empty subset of Σ has a minimal element.

Definition 6.1: Noetherian (after Emmy Noether)

A ring A (or a module M over a ring A) is said to be *Noetherian* if it satisfies the ascending chain condition w.r.t. the inclusion relation over the set of all ideals of A (or the set of all submodules of M).

Definition 6.2: Artinian (after Emil Artin)

A ring A (or a module M over a ring A) is said to be *Artinian* if it satisfies the descending chain condition w.r.t. the inclusion relation over the set of all ideals of A (or the set of all submodules of M).

6.2 Implications

Proposition 6.1

The following conditions on Σ are equivalent:

1. Every increasing sequence
$$x_1 \leqslant x_2 \leqslant \cdots \leqslant x_n$$
in Σ is stationary.

2. Every non-empty subset of Σ has a maximal element.

Proof.
(1 $\implies$ 2) Proof by contradiction. We can construct an ascending chain of elements if 2 is false.
(2 $\implies$ 1) The set $(x_m)_{m\geqslant 1}$ has a maximal element, say x_n. □

Example 6.1

1. A finite abelian group (as a Z-module) is both Noetherian and Artinian.

2. The ring Z as a Z-module is Noetherian but not Artinian.

Proposition 6.2

M is a Noetherian A-module $\iff$ Every submodule of M is finitely generated.

Proof.
($\implies$) Consider some submodule N of M. We use the maximal condition to prove the result.
Suppose Σ be the set of all finitely generated submodules of N. Σ is non-empty since $0 \in \Sigma$.
Then Σ is partially ordered by the inclusion relation. By the maximal condition, Σ has a maximal element.
Suppose N_0 be a maximal element of Σ. We claim that $N_0 = N$. Otherwise, $\exists\, x \in N$ s.t. $x \notin N_0$.
Then $N_0 + Ax$ is a finitely generated submodule of N which strictly contains N_0 and hence, contradicts the maximality of N_0. Thus, $N_0 = N$ and hence, N is finitely generated.

($\impliedby$) Consider some ascending chain of submodules of M.

$$N_1 \subseteq N_2 \subseteq \cdots \subseteq N_n \subseteq \cdots$$

Consider $N = \bigcup_{n=1}^{\infty} N_i$ which is finitely generated.
Suppose N is generated by $\{x_1, \ldots, x_k\}$. Say $x_i \in N_{n_i}$.
Let $n = \max_{i=1}^{r} n_i$ and we can notice that the chain is stationary after n since

$$N_n = \bigcup_{i=1}^{\infty} N_i$$

□

Theorem 6.1

Consider the SES of A-modules

$$\begin{tikzcd} 0 \arrow[r] & M_1 \arrow[r, "\alpha"] & M_2 \arrow[r, "\beta"] & M_3 \arrow[r] & 0 \end{tikzcd}$$

Then,

$$M_2 \text{ is Noetherian} \iff M_1, M_3 \text{ are Noetherian}$$
$$M_2 \text{ is Artinian} \iff M_1, M_3 \text{ are Artinian}$$

Proof. We will prove the Neotherian case. The Artinian case is similar.
($\Longrightarrow$)
Suppose M_2 is Noetherian.
Let

$$N_1 \subsetneq N_2 \subsetneq \cdots \subsetneq N_n \subsetneq \ldots$$

be some strictly ascending chain of submodules of M_1.
Then, we get

$$\alpha(N_1) \subsetneq \alpha(N_2) \subsetneq \cdots \subsetneq \alpha(N_n) \subsetneq \ldots$$

which is a strictly ascending chain of submodules of M_2. We have a strict containment since α is an inclusion.
This can not happen since M_2 is satisfies ACC.
Thus, M_1 is Noetherian.
Now, consider a strictly ascending chain of submodules of M_3

$$L_1 \subsetneq L_2 \subsetneq \cdots \subsetneq L_n \subsetneq \ldots$$

Then, we get

$$\beta^{-1}(L_1) \subsetneq \beta^{-1}(L_2) \subsetneq \cdots \subsetneq \beta^{-1}(L_n) \subsetneq \ldots$$

which is a strictly ascending chain of submodules of M_2. We have a strict containment since β is a surjection.
This can not happen since M_2 is satisfies ACC. Thus, M_3 is Noetherian.

($\Longleftarrow$)
Suppose M_1 and M_3 are Noetherian.
Consider a strictly ascending chain of submodules of M_2

$$N_1 \subsetneq N_2 \subsetneq \cdots \subsetneq N_n \subsetneq \ldots$$ □

Corollary 6.1

If M_i $(1 \leqslant i \leqslant n)$ are Neotherian (resp. Artinian), then so is $M_1 \oplus M_2 \oplus \cdots \oplus M_n$.

Proof. We apply induction and the proposition on the exact sequence

$$0 \longrightarrow M_n \longrightarrow \bigoplus_{i=1}^{n} M_i \longrightarrow \bigoplus_{i=1}^{n-1} M_i \longrightarrow 0$$ □

Lemma 6.1

Every ideal of a Noetherian (resp. Artinian) ring A is Noetherian (resp. Artinian).

Proof. Consider the ideal$\mathfrak{a}$ of A as a A-module. Construct the SES

$$0 \longrightarrow \mathfrak{a} \longrightarrow A \longrightarrow {}^{A}/_{\mathfrak{a}} \longrightarrow 0$$

Then, by the proposition, $\mathfrak{a}$ is Noetherian (resp. Artinian). □

Proposition 6.3

Let A be a Noetherian (resp. Artinian) ring and M be a finitely generated A-module.
Then, M is Noetherian (resp. Artinian).

Proof. Using the structure theorem of finitely generated A-modules, we can write $M = \bigoplus_{i=1}^{n} \mathfrak{a}_i$ where $\mathfrak{a}_i$ are ideals of A for some $n \in \mathbb{N}$.
Then, by the lemma, $\mathfrak{a}_i$ are Noetherian (resp. Artinian) and using the corollary, we get that M is Noetherian. □

6.3 Chain

Definition 6.4 Chain or Composition series

A *chain* or *composition series* of submodules of a module M is a sequence M_i $(0 \leqslant i \leqslant n)$ of submodules of M such that

$$M = M_0 \supsetneq M_1 \supsetneq \cdots \supsetneq M_n = 0$$

n is called the *length* of the chain denoted by $l(M)$.

Definition 6.5 Maximal Chain

A composition series of M is a maximal chain, (one in which no extra submodules can be inserted) if

$$M_{i-1} \big/ M_i \text{ is simple} \quad \forall\, i \in \{2, \ldots, n\}$$

Proposition 6.4

Suppose M being an A-module has a composition series of length n.
Then every composition series of M has length n and every chain in M can be extended to a composition series.

Proof. Let $l(M)$ denote the least length of a composition series of a module M. (We say $l(M) = \infty$ if M has no composition series.)

Claim 6.1

$$N \subsetneq M \implies l(N) < l(M)$$

Let M_i be a composition series of M of minimal length. Consider the submodules $N_i = N \cap M_i$ of N.
We have

$$N_{i-1} \big/ N_i \subseteq M_{i-1} \big/ M_i$$

and the latter is a simple module and hence,

$$N_{i-1} \big/ N_i = 0 \implies N_{i-1} = N_i \text{ or } M_{i-1} \big/ M_i$$

Hence, removing the repeated submodules, we get a composition series of N of length $l(N) \leqslant l(M)$.
If $l(N) = l(M)$, we have $N_i = M_i, N_{i-1} = M_{i-1}$ and so on till $N_0 = M_0$ and hence $N = M$ which is a contradiction.

Claim 6.2

Any chain in M has length at most $l(M)$.

Consider a chain

$$M = M_0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_k = 0$$

Using the previous claim, we have

$$l(M_0) > l(M_1) > \cdots > l(M_k) = 0$$

and hence $k \leqslant l(M)$
Hence, we can say that any composition series of M has length $l(M)$.

Now, consider a chain. If the length of the chain is less than $l(M)$, it is not a maximal chain and hence, we can extend it to a composition series.
Otherwise, we have a composition series of length $l(M)$. □

Proposition 6.5

M has a composition series $\iff$ M satisfies both ACC and DCC.

Proof.
($\Longrightarrow$) Since M has a composition series, all chains in M are of finite length and hence, M satisfies ACC and DCC.

($\Longleftarrow$) Construct a composition series of M as follows.
Since $M = M_0$ satisfies the maximum condition, it has a maximal submodule $M_1 \subsetneq M_0$.
Similarly, M_1 has a maximal submodule $M_2 \subsetneq M_1$ and so on.
Thus, we get a descending chain of submodules of M and hence, must terminate at some point giving us a composition series. □

Proposition 6.6

The length $l(M)$ is an additive function on the class of all A-modules of finite length.
That is,

$$\begin{tikzcd} 0 \arrow[r] & N \arrow[r, "\alpha"] & M \arrow[r, "\beta"] & L \arrow[r] & 0 \end{tikzcd}$$

is an exact sequence of A-modules, then

1. $l(M) < \infty \iff l(N) < \infty$ and $l(L) < \infty$
2. $l(M) = l(N) + l(L)$

Proof. 1 is obvious from the fact that

$$M \text{ is Noetherian (resp. Artinian)} \iff N \text{ and } L \text{ is Noetherian (resp. Artinian)}$$

Suppose

$$N = N_0 \subsetneq N_1 \subsetneq \cdots \subsetneq N_n = 0$$

and

$$L = L_0 \subsetneq L_1 \subsetneq \cdots \subsetneq L_l = 0$$

Since α is an inclusion, we will have

$$\operatorname{im}(\alpha) = \alpha(N_0) \subsetneq \alpha(N_1) \subsetneq \cdots \subsetneq \alpha(N_n) = 0$$

Also, since β is a surjection, we will have

$$M = \beta^{-1}(L_0) \subsetneq \beta^{-1}(L_1) \subsetneq \cdots \subsetneq \beta^{-1}(L_l) = \beta^{-1}(0) = \ker(\beta)$$

Since $\operatorname{im}(\alpha) = \ker(\beta)$, we have

$$M = \beta^{-1}(L_0) \subsetneq \beta^{-1}(L_1) \subsetneq \cdots \subsetneq \beta^{-1}(L_l) = \alpha(N_0) \subsetneq \alpha(N_1) \subsetneq \cdots \subsetneq \alpha(N_n) = 0$$

The length of this composition series is $l(M) = l(N) + l(L)$. □

Proposition 6.7

For k-vector spaces V, the following conditions are equivalent.

1. Finite dimension
2. Finite length
3. Satisfy ACC
4. Satisfy DCC

Moreover, if any of the conditions is satisfied, then the length is equal to its dimension.

Proof. Trivial. □

Corollary 6.2

Let A be a ring in which the zero ideal is a product

$$\mathfrak{m}_1 \cdot \mathfrak{m}_2 \cdots \mathfrak{m}_n = 0$$

(not necessarily distinct) finite number of maximal ideals.
Then,

$$A \text{ is Noetherian} \iff A \text{ is Artinian}$$

Proof. Consider the chain of ideals of A.

$$A \supsetneq \mathfrak{m}_1 \supseteq \mathfrak{m}_1\mathfrak{m}_2 \supseteq \cdots \supseteq \mathfrak{m}_1\mathfrak{m}_2 \cdots \mathfrak{m}_n = 0$$

Now, each factor ${\mathfrak{m}_1 \cdots \mathfrak{m}_{i-1}} \big/ {\mathfrak{m}_1 \cdots \mathfrak{m}_i}$ is a vector space over field ${A} \big/ {\mathfrak{m}_i}$.
Hence, ACC $\iff$ DCC for each factor and thus, for A. □

Chapter 7

Noetherian rings

7.1 Introduction

Definition 7.1: Noetherian Rings

A ring A is said to be *Noetherian* if it satisfies one of the following equivalent conditions:

1. Every non-empty set of ideals in A has a maximal element.
2. Every ascending chain of ideals in A is stationary.
3. Every ideal in A is finitely generated.

Noetherian Rings are by far the most important class of rings in commutative albergra.
In this chapter, we show that Noetherian rings reproduce themselves under various famililar operations - in particular, we prove the famous basis theorem of Hilbert.

7.2 Basic properties of Noetherian Rings

Proposition 7.1

If A is Neotherian and ϕ is a homomorphism of A onto a ring B, then B is Noetherian.

$$\phi : A \longrightarrow B \qquad \text{is a ring homomorphism}$$

Proof. Using the First Isomorphism Theorem, we have

$$B \cong {}^{A}\Big/_{\text{Ker}(\phi)}$$

We have seen that if A is Noetherian, then so is ${}^{A}\Big/_{\text{Ker}(\phi)}$. Therefore, B is Noetherian. □

Proposition 7.2

Let A be a subring of B and suppose A is Noetherian and B is *finitely generated* as a A-module. Then B is Noetherian (as a ring).

Proof. B is *finitely generated* A-module and is hence, Noetherian as a A-module and hence, is Noetherian as a B-module. □

Proposition 7.3

If A is Noetherian and S is any multiplicatively closed subset of A, then $S^{-1}A$ is Noetherian.

Proof. TODO □

Corollary 7.1

If A is Noetheiran and $\mathfrak{p}$ is a prime ideal of A, then $A_{\mathfrak{p}}$ is Noetherian.

7.3 The Hilbert Basis Theorem

Theorem 7.1 Hilbert Basis Theorem

If A is Noetherian, then the polynomial ring $A[x]$ is Noetherian.

Let $\mathfrak{a}$ be an ideal in $A[x]$. The leading coefficients of the polynomials in $\mathfrak{a}$ form an ideal I in A. Now, since A is Noetherian, I is finitely generated, say

$$I = \langle a_1, \dots, a_n \rangle$$

For each $i = 1, \cdots n$, we have a polynomial f_i in $A[x]$ of the form and let us define r

$$f_i = a_i x^{r_1} + \text{ (lower terms)} \qquad \mathfrak{a}' \coloneqq \langle f_1, \dots, f_n \rangle \subseteq \mathfrak{a}$$

and let $r \coloneqq \max_{i=1}^n r_i$.
Consider some polynomial f in $\mathfrak{a}$.

$$f = ax^m + \text{ (lower terms)} \quad \in \mathfrak{a}$$

We have $a \in I$. If $m \geqslant r$, we write

$$a = u_1 a_1 + \cdots + u_n a_n \quad u_i \in A$$

Now, we can notice that

$$f - \sum_{i=1}^n u_i f_i x^{m-r_1} \quad \in \mathfrak{a}$$

and has a degree $< m$. We can continue this process until we can represent f as a sum

$$f = g + h$$

where g is a polynomial of degree $< r$ in $\mathfrak{a}$ and h is a polynomial in $\mathfrak{a}_1$.
Let M be the A-module generated by $1, x, \cdots, x^{r-1}$. Then, we have

$$M = \left\langle 1, x, \cdots, x^{r-1} \right\rangle \quad \text{and} \quad g \in \mathfrak{a} \cap M$$

We just proved that

$$\mathfrak{a} = (\mathfrak{a} \cap M) + \mathfrak{a}'$$

Since M is a finitely generated A-module, $\mathfrak{a} \cap M \triangleleft M$ and is hence a finitely generated A-module.
If g_i generate $\mathfrak{a} \cap M$, then it is clear that f_i and g_i generate $\mathfrak{a}$.
Thus,

$$A \text{ is Noetherian} \implies A[x] \text{ is Noetherian}$$

Corollary 7.2

If A is Noetherian, then so is $A[x_1, \cdots, x_n]$