

Commutative Algebra

HHH

December 18, 2025

Contents

I	Commutative Ring and Modules	1
I		2
§1	Ideals quotient	2
§2	Primary Decomposition	2
§2.1	Primary (Submodule) Ideals	2
§2.2	Primary Decomposition	4
§3	Contraction and extension of ideal	5
§4	Nil and nilpotent ideals	6
II	Radical Ideals	7
§1	Radical and Nilradical	7
III	Fractions and Localization	9
§1	Rings of Quotient	9
§1.1	Ideals in ring of fractions	10
§2	Localization and Local rings	11
IV	Chain Condition	12
§1	12
§1.1	Equivalent Condition of Chain Condition	12
§2	Normal series and Composition Series of Modules	14
V	Noetherian Modules and Rings	16
§1	Artinian Rings	16
§1.1	16
§1.2	16
§2	Noetherian Modules and Rings	17
VI	Integral	19
§1	Rings Extensions	19
§1.1	integral extension	20
§2	Discrete Valuation Ring	21
§3	Dedekind Domain	22

§3.1	Unique factorization of ideals	22
§3.2	The ideal class group	23
§4	Discrete valuations	24
§5	Integral closures of Dedekind domains	25
VII	Completions	26
§1	Filtered and Graded Modules	26
§2	Filtrations	26
§3	Graded	27
§4	First associated graded ring	27
§5	Second associated graded ring	28
§6	Graded Algebra	28
§7	Krull intersection theorem	29
II	The Structure of Rings	31
VIII	The Structure of Rings	32
§1	Simplicity and Primitivity	32
§1.1	Primitivity	33
§1.2	Jacobson Density Theorem	33
§2	Simple ring	35
IX	Semisimplicity	37
§1	Definitions	37
§2	Structure of semisimple rings	38
§3	Structure of modules over semisimple rings	39
§3.1	Modules over $M_n(D)$	39
§3.2	Modules over semisimple rings	39
§4	Jacobson Radical	40
§4.1	Jacobson radical	40
§4.2	Nakayama's Lemma	41
§5	Characterizations of semisimple rings	42
§6	Algebra	42

Part I

Commutative Ring and Modules

Chapter I

§1 Ideals quotient

Definition 1.1. If $\mathfrak{a}, \mathfrak{b}$ are ideals in a commutative ring R , their **ideal quotient** is

$$(\mathfrak{a} : \mathfrak{b}) = \{x \in R : x\mathfrak{b} \subseteq \mathfrak{a}\}$$

which is an ideal. If \mathfrak{b} is a principal ideal (x) , we shall write $(\mathfrak{a} : x)$ in place of $(\mathfrak{a} : (x))$.

Proposition 1.2. Let R be a commutative ring. Then

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

§2 Primary Decomposition

Throught this section, R be a commutative ring with identity

§2.1 Primary (Submodule) Ideals

Definition 2.1. Let A be a commutative ring with identity and M an A -module.

1. An ideal \mathfrak{q} in A is **primary** if $\mathfrak{q} \neq A$ and if

$$xy \in \mathfrak{q}, x \notin \mathfrak{q} \Rightarrow y^n \in \mathfrak{q} \text{ for some } n > 0.$$

In other words, \mathfrak{q} is primary $\Leftrightarrow R/\mathfrak{q} \neq 0$ and every zero-divisor in R/\mathfrak{q} is nilpotent.

2. A submodule Q of M is primary if $Q \neq M$ and if

$r \in R, m \in M - Q$ and $rm \in Q \Rightarrow r^n M \subset Q$ for some positive integer n

It is equivalent that

- $(Q : M) = \text{Ann}(M/Q)$ is a primary ideal in R
- principal homomorphism $a_{M/Q}$ is injective or nilpotent for each $a \in R$

Remark. If we view A as itself A -module, the two definition are equivalent for A .

Proposition 2.2. Let A be a commutative ring and M an A -module.

1. If \mathfrak{q} is a primary ideal in A , ideal $\mathfrak{p} = \text{Rad}(\mathfrak{q})$ is a prime ideal containing \mathfrak{q} . The radical \mathfrak{p} is called the **associated prime ideal of \mathfrak{q}** or that \mathfrak{q} is **\mathfrak{p} -primary**.
2. If N is a primary submodule of M , $(N : M) = \{r \in A \mid rM \subset N\}$ is a primary ideal in A . Thus $\mathfrak{p} = \text{Rad}(N : M) = \{r \in A \mid r^n M \subset N \text{ for some } n > 0\}$ is a prime ideal in A . The primary submodule N of a module M is said to **belong to a prime ideal \mathfrak{p}** or to be a **\mathfrak{p} -primary submodule** of M .

Theorem 2.3. Let A be a commutative ring, \mathfrak{q} and \mathfrak{p} be ideals in A . Then \mathfrak{q} is primary for \mathfrak{p} if and only if

- (i) $\mathfrak{q} \subset \mathfrak{p} \subset \text{Rad}(\mathfrak{q})$
- (ii) if $ab \in \mathfrak{q}$ and $a \notin \mathfrak{q}$, then $b \in \mathfrak{p}$.

Proof. Suppose (i) and (ii) hold. If $ab \in \mathfrak{q}$ with $a \notin \mathfrak{q}$, then $b \in \mathfrak{p} \subset \text{Rad } \mathfrak{q}$, whence $b^n \in \mathfrak{q}$ for some $n > 0$. Therefore \mathfrak{q} is primary.

To show that \mathfrak{q} is primary for \mathfrak{p} we need only show $\mathfrak{p} = \text{Rad } \mathfrak{q}$. By (i), $\mathfrak{p} \subset \text{Rad } \mathfrak{q}$. If $b \in \text{Rad } \mathfrak{q}$, let n be the least integer such that $b^n \in \mathfrak{q}$. If $n = 1$, $b \in \mathfrak{q} \subset \mathfrak{p}$. If $n > 1$, then $b^{n-1}b = b^n \in \mathfrak{q}$, with $b^{n-1} \notin \mathfrak{q}$ by the minimality of n . By (ii), $b \in \mathfrak{p}$. Thus $b \in \text{Rad } \mathfrak{q}$ implies $b \in \mathfrak{p}$, whence $\text{Rad } \mathfrak{q} \subset \mathfrak{p}$. \square

Corollary 2.4. Let A be a commutative ring with identity, if $\mathfrak{q}_1, \mathfrak{q}_2, \dots, \mathfrak{q}_n$ are \mathfrak{p} -primary, then $\bigcap_{i=1}^n \mathfrak{q}_i$ is also \mathfrak{p} -primary.

Proof. Let $\mathfrak{q} = \bigcap_{i=1}^n \mathfrak{q}_i$. Then by 1.2, $\text{Rad } \mathfrak{q} = \bigcap_{i=1}^n \text{Rad } \mathfrak{q}_i = \bigcap_{i=1}^n \mathfrak{p} = \mathfrak{p}$; in particular, $\mathfrak{q} \subset \mathfrak{p} \subset \text{Rad } \mathfrak{q}$. If $ab \in \mathfrak{q}$ and $a \notin \mathfrak{q}$, then $ab \in \mathfrak{q}_i$ and $a \notin \mathfrak{q}_i$ for some i . Since \mathfrak{q}_i is \mathfrak{p} -primary, $b \in \mathfrak{p}$ by 2.3. Consequently, \mathfrak{q} itself is \mathfrak{p} -primary by 2.3. \square

Proposition 2.5. Clearly every prime ideal is primary. Also the contraction of a primary ideal is primary, for if $f : A \rightarrow B$ and if \mathfrak{q} is a primary ideal in B , then A/\mathfrak{q}^c is isomorphic to a subring of B/\mathfrak{q} .

Proposition 2.6. If $\text{Rad}(\mathfrak{a})$ is maximal, then \mathfrak{a} is primary. In particular, the powers of a maximal ideal \mathfrak{m} are \mathfrak{m} -primary.

Proof. Let $\text{Rad}(\mathfrak{a}) = \mathfrak{m}$. 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 $\pi(\mathfrak{m})$, by (1.8). Hence every element of A/\mathfrak{a} is either a unit or nilpotent, and so every zero-divisor in A/\mathfrak{a} is nilpotent. \square

§2.2 Primary Decomposition

Definition 2.7. Let R be a commutative ring with identity and M an unitary R -module.

1. An ideal \mathfrak{a} of R has a **primary decomposition** if

(i) $\mathfrak{a} = \mathfrak{q}_1 \cap \mathfrak{q}_2 \cap \cdots \cap \mathfrak{q}_n$ with each \mathfrak{q}_i primary

then the primary decomposition is said to be **reduced (or irredundant)** if

(ii) no \mathfrak{q}_i contains $\mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_{i-1} \cap \mathfrak{q}_{i+1} \cap \cdots \cap \mathfrak{q}_n$ and the $\mathfrak{p}_i = \text{Rad } \mathfrak{q}_i$ are all distinct,

2. A submodule N of M has a **primary decomposition** if

(i) $N = Q_1 \cap Q_2 \cap \cdots \cap Q_n$, with each Q_i a \mathfrak{p}_i -primary submodule of M for some prime ideal \mathfrak{p}_i of R .

then the primary decomposition is said to be **reduced** if

(ii) no Q_i contains $Q_1 \cap \cdots \cap Q_{i-1} \cap Q_{i+1} \cap \cdots \cap Q_n$ and the ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ are all distinct,

If $\mathfrak{p}_j \not\subset \mathfrak{p}_i$ for all $j \neq i$, then \mathfrak{p}_i is said to be an **isolated prime** ideal of M . In other words, \mathfrak{p}_i is isolated if it is minimal in the set $\{\mathfrak{p}_1, \dots, \mathfrak{p}_n\}$. If \mathfrak{p}_i is not isolated it is said to be **embedded**.

Theorem 2.8. Let R be a commutative ring with identity and M a unitary module.

1. If an ideal \mathfrak{a} of R has a primary decomposition, then \mathfrak{a} has a reduced primary decomposition.

2. If a submodule N has a primary decomposition, then N has a reduced primary decomposition.

Proof. 1. If $\mathfrak{a} = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n$ (\mathfrak{q}_i primary) and some \mathfrak{q}_i contains $\mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_{i-1} \cap \mathfrak{q}_{i+1} \cap \cdots \cap \mathfrak{q}_n$, then $\mathfrak{a} = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_{i-1} \cap \mathfrak{q}_{i+1} \cap \cdots \cap \mathfrak{q}_n$ is also a primary decomposition. By thus eliminating the superfluous \mathfrak{q}_i (and reindexing) we have $\mathfrak{a} = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_k$ with no \mathfrak{q}_i containing the intersection of the other \mathfrak{q}_j .

Let $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ be the distinct prime ideals in the set $\{\text{Rad } \mathfrak{q}_1, \dots, \text{Rad } \mathfrak{q}_k\}$. Let $\mathfrak{q}'_i (1 \leq i \leq r)$ be the intersection of all the \mathfrak{q} 's that belong to the prime \mathfrak{p}_i , that is,

$$\mathfrak{q}'_i = \bigcap_{\text{Rad}(\mathfrak{q}_j) = \mathfrak{p}_i} \mathfrak{q}_j$$

By 2.4 each \mathfrak{q}'_i is primary for \mathfrak{p}_i . Clearly no \mathfrak{q}'_i contains the intersection of all the other \mathfrak{q}'_i . Therefore, $\mathfrak{a} = \bigcap_{i=1}^k \mathfrak{q}_i = \bigcap_{i=1}^r \mathfrak{q}'_i$, whence \mathfrak{a} has a reduced primary decomposition.

2. It is similar to 1. Note that $(\bigcap Q_i : M) = \bigcap (Q_i : M)$. □

Theorem 2.9. *Let R be a commutative ring with identity. If M is an unitary R -module and N is a proper submodule of M with two reduced primary decompositions,*

$$Q_1 \cap Q_2 \cap \cdots \cap Q_k = N = Q'_1 \cap Q'_2 \cap \cdots \cap Q'_s$$

where Q_i is \mathfrak{p}_i -primary and Q'_j is \mathfrak{p}'_j -primary. Then $k = s$ and (after reordering if necessary) $\mathfrak{p}_i = \mathfrak{p}'_i$ for all $i = 1, 2, \dots, k$. Furthermore if Q_i and Q'_i both are \mathfrak{p}_i -primary and \mathfrak{p}_i is an isolated prime, then $Q_i = Q'_i$.

Theorem 2.10. *Let R be a commutative ring with identity and M an Noetherian unitary R -module. Then every submodule $N \neq M$ has a reduced primary decomposition.*

Proof. Let \mathcal{S} be the set of all submodules of M that do not have a primary decomposition. Clearly no primary submodule is in \mathcal{S} . We must show that \mathcal{S} is actually empty. If \mathcal{S} is nonempty, then \mathcal{S} contains a maximal element C by Theorem 1.4.

Since C is not primary, there exist $r \in R$ and $b \in M - C$ such that $rb \in C$ but $r^n M \not\subset C$ for all $n > 0$. Let $M_n = (C : r^n) = \{x \in M \mid r^n x \in C\}$. Then each M_n is a submodule of M and $M_1 \subset M_2 \subset M_3 \subset \cdots$. By hypothesis there exists $k > 0$ such that $M_i = M_k$ for $i \geq k$. Let D be the submodule $r^k M + C = \{x \in M \mid x = r^k y + c \text{ for some } y \in M, c \in C\}$. Clearly $C \subset M_k \cap D$.

Conversely, if $x \in M_k \cap D$, then $x = r^k y + c$ and $r^k x \in C$, whence $r^{2k} y = r^k (r^k y) = r^k (x - c) = r^k x - r^k c \in C$. Therefore, $y \in M_{2k} = M_k$. Consequently, $r^k y \in C$ and hence $x = r^k y + c \in C$. Therefore $M_k \cap D \subset C$, whence $M_k \cap D = C$. Now $C \neq M_k \neq M$ and $C \neq D \neq M$ since $b \in M_k - C$ and $r^k M \not\subset C$. By the maximality of C in \mathcal{S} , M_k and D must have primary decompositions. Thus C has a primary decomposition, which is a contradiction. Therefore \mathcal{S} is empty and every submodule has a primary decomposition. Consequently, every submodule has a reduced primary decomposition by 2.8. \square

Corollary 2.11. *If R is a commutative Noetherian ring with identity and M is a finitely generated unitary R -module. Then every submodule $N (\neq M)$ of M has a reduced primary decomposition.*

Proof. This is an immediate consequence of 1.6 2.1 and 2.10 \square

§3 Contraction and extension of ideal

Definition 3.1. *Let R be a ring and $f : A \rightarrow B$ be a ring homomorphism,*

1. *the **extension** of ideal \mathfrak{a} of A is the ideal generated by $f(\mathfrak{a})$ in B , denoted by \mathfrak{a}^e .*
2. *the **contraction** of \mathfrak{b} is $f^{-1}(\mathfrak{b})$, denoted by \mathfrak{b}^c .*

Especially if A be a subring of B and $i : A \rightarrow B$, the contraction of ideal of \mathfrak{b} of B is $A \cap \mathfrak{b}$.

Proposition 3.2. .

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 \mathcal{C} is the set of all contracted ideals in A and if \mathcal{E} is the set of all extended ideals in B , then $\mathcal{C} = \{\mathfrak{a} \mid \mathfrak{a}^{ec} = \mathfrak{a}\}, \mathcal{E} = \{\mathfrak{b} \mid \mathfrak{b}^{ce} = \mathfrak{b}\}$, and $\mathfrak{a} \mapsto \mathfrak{a}^e$ is a bijective map, whose inverse is $\mathfrak{b} \mapsto \mathfrak{b}^c$.

Proposition 3.3. .

$$\begin{aligned}
(\mathfrak{a}_1 + \mathfrak{a}_2)^e &= \mathfrak{a}_1^e + \mathfrak{a}_2^e & (\mathfrak{b}_1 + \mathfrak{b}_2)^c &\supseteq \mathfrak{b}_1^c + \mathfrak{b}_2^c, \\
(\mathfrak{a}_1 \cap \mathfrak{a}_2)^e &\subseteq \mathfrak{a}_1^e \cap \mathfrak{a}_2^e & (\mathfrak{b}_1 \cap \mathfrak{b}_2)^c &= \mathfrak{b}_1^c \cap \mathfrak{b}_2^c, \\
(\mathfrak{a}_1 \mathfrak{a}_2)^e &= \mathfrak{a}_1^e \mathfrak{a}_2^e & (\mathfrak{b}_1 \mathfrak{b}_2)^c &\supseteq \mathfrak{b}_1^c \mathfrak{b}_2^c, \\
(\mathfrak{a}_1 : \mathfrak{a}_2)^e &\subseteq (\mathfrak{a}_1^e : \mathfrak{a}_2^e) & (\mathfrak{b}_1 : \mathfrak{b}_2)^c &\subseteq (\mathfrak{b}_1^c : \mathfrak{b}_2^c), \\
\text{Rad}(\mathfrak{a})^e &\subseteq \text{Rad}(\mathfrak{a}^e) & \text{Rad}(\mathfrak{b})^c &= \text{Rad}(\mathfrak{b}^c)
\end{aligned}$$

if \mathfrak{b} is a prime ideal in B , then so \mathfrak{b}^c .

The set \mathcal{C} is closed under the other three operations, and \mathcal{E} is closed under sum and product.

§4 Nil and nilpotent ideals

Definition 4.1. Let R be a ring and \mathfrak{a} be an (left, right, two-sided) ideal of R .

1. \mathfrak{a} of R is **nil** if every element of \mathfrak{a} is a nilpotent element;
2. \mathfrak{a} is **nilpotent** if $\mathfrak{a}^n = 0$ for some integer n .

Theorem 4.2. Let R be a ring.

1. If $a \in R$ is nilpotent, a is both left and right quasiregular with quasi inverse $r = -a + a^2 - a^3 + \cdots + (-1)^{n-1}a^{n-1}$
2. Every nil left ideal is contained in $J(R)$.
3. Thus every nil ring is a radical ring.

Proposition 4.3. If R is a left [resp. right] Noetherian ring, then every nil ideal is nilpotent (Exercise 16).

Chapter II

Radical Ideals

Contents

§1 Radical and Nilradical	7
-------------------------------------	---

R is a commutative ring (with identity) throughout this chapter unless otherwise stated.

§1 Radical and Nilradical

Definition 1.1. Let R be a commutative ring. If \mathfrak{a} is any ideal of R , the ideal

$$\text{Rad}(\mathfrak{a}) = \{x \in R : x^n \in \mathfrak{a} \text{ for some } n \in \mathbb{Z}_{\geq 1}\}$$

is called **radical** of \mathfrak{a} , sometimes denoted by $\sqrt{\mathfrak{a}}$. The radical of 0 (the set of all nilpotent elements in R) is called **nilradical** of R , denoted by $\text{Nil}(R)$.

Proposition 1.2. Let R be a commutative ring. Then

1. $\mathfrak{a} \subset r(\mathfrak{a})$
2. $r(r(\mathfrak{a})) = r(\mathfrak{a})$
3. $r(\mathfrak{a}\mathfrak{b}) = r(\mathfrak{a} \cap \mathfrak{b}) = r(\mathfrak{a}) \cap r(\mathfrak{b})$
4. thus $r(\mathfrak{a}_1\mathfrak{a}_2 \cdots \mathfrak{a}_n) = r(\bigcap \mathfrak{a}_i) = \bigcap r(\mathfrak{a}_i)$ and $r(\mathfrak{a}^n) = r(\mathfrak{a})$
5. $r(\mathfrak{a} + \mathfrak{b}) = r(r(\mathfrak{a}) + r(\mathfrak{b}))$
6. if \mathfrak{p} is prime in R , $r(\mathfrak{p}^n) = r(\mathfrak{p}) = \mathfrak{p}$ for all $n > 0$.
7. $r(\mathfrak{a}) = (1) \Leftrightarrow \mathfrak{a} = (1)$

Proposition 1.3. Let R be a commutative ring. If S is a multiplicative subset which is disjoint from an ideal \mathfrak{a} , then there exists a prime ideal \mathfrak{p} which is maximal in $S = \{\mathfrak{b} : \mathfrak{a} \subset \mathfrak{b} \text{ and } \mathfrak{b} \cap S = \emptyset\}$.

Proof. Since $S \neq \emptyset$ and every ideal in S is properly contained in R , set S is partially ordered by inclusion. By Zorn's Lemma there is an ideal \mathfrak{p} which is maximal in S .

Let $\mathfrak{a}_1, \mathfrak{a}_2$ be ideals of R such that $\mathfrak{a}_1\mathfrak{a}_2 \subset \mathfrak{p}$. If $\mathfrak{a}_1 \not\subset \mathfrak{p}$ and $\mathfrak{a}_2 \not\subset \mathfrak{p}$, then each of the ideals $\mathfrak{p} + \mathfrak{a}_1$ and $\mathfrak{p} + \mathfrak{a}_2$ properly contains \mathfrak{p} and hence must meet S . Consequently, for some $p_i \in \mathfrak{p}$, $a_i \in \mathfrak{a}_i$.

$$p_1 + a_1 = s_1 \in S \quad \text{and} \quad p_2 + a_2 = s_2 \in S$$

Thus $s_1s_2 = p_1p_2 + p_1a_2 + a_1p_2 + a_1a_2 \in \mathfrak{p} + \mathfrak{a}_1\mathfrak{a}_2 \subset \mathfrak{p}$. This is a contradiction since $s_1s_2 \in S$ and $S \cap \mathfrak{p} = \emptyset$. Therefore $\mathfrak{a}_1 \subset \mathfrak{p}$ or $\mathfrak{a}_2 \subset \mathfrak{p}$, whence \mathfrak{p} is prime. \square

Theorem 1.4. *Let R be a commutative rng and an ideal \mathfrak{a} .*

1. *If $\pi : R \rightarrow R/\mathfrak{a}$ is the canonical projection, then $\text{Rad}(\mathfrak{a}) = \pi^{-1}(\text{Nil}(R/\mathfrak{a}))$*
2. *The radical of an ideal \mathfrak{a} is the intersection of the prime ideals which contain \mathfrak{a} , that is,*

$$\text{Rad}(\mathfrak{a}) = \bigcap_{\substack{\mathfrak{a} \subset \mathfrak{p} \\ \mathfrak{p} \text{ is prime}}} \mathfrak{p}$$

Proof. It is clear that

$$\text{Rad}(\mathfrak{a}) \subset \bigcap_{\substack{\mathfrak{a} \subset \mathfrak{p} \\ \mathfrak{p} \text{ is prime}}} \mathfrak{p} := \tilde{\mathfrak{p}}$$

by ?? ?? . If $S = \tilde{\mathfrak{p}} - \text{Rad}(\mathfrak{a})$ is nonempty, whence is a multiplicative subset of R (verify that $x, y \in S \Rightarrow xy \in S$) and disjoint from $\text{Rad}(\mathfrak{a})$, there exist a prime ideal \mathfrak{p}' that contains $\text{Rad}(\mathfrak{a})$ and disjoint from S by 1.3. But $\tilde{\mathfrak{p}} \subset \mathfrak{p}'$ by the definition of $\tilde{\mathfrak{p}}$, this is a contradiction. \square

Proposition 1.5. *If R is a commutative ring with identity $\neq 0$, then $R^\times + \text{Nil}(R) \subset R^\times$.*

Chapter III

Fractions and Localization

Contents

§1	Rings of Quotient	9
§1.1	Ideals in ring of fractions	10
§2	Localization and Local rings	11

§1 Rings of Quotient

A is a commutative ring with identity throughout this section unless otherwise stated.

Definition 1.1. Let A be a commutative ring. A subset S called a **multiplicative subset** of A if S is a submonoid of (A, \times) .

Remark. In general, we always assume that $0 \notin S$.

Definition 1.2. Let S be a multiplicative subset of A and

1. The relation defined on the set $A \times S$ by

$$(a, s) \sim (a', s') \Leftrightarrow s_1 (as' - a's) = 0 \text{ for some } s_1 \in S$$

is an equivalence relation and the equivalence class containing the element (a, s) is denoted by a/s .

2. $S^{-1}R$ is a commutative ring with identity $1/1$, where addition and multiplication are defined by

$$r/s + r'/s' = (rs' + r's)/ss' \quad \text{and} \quad (r/s)(r'/s') = rr'/ss'$$

is called the **ring of fractions** of R by S .

Remark. The map $\varphi_S : A \rightarrow S^{-1}A$ given by $a \mapsto a/1$ is a well-defined homomorphism of rings and $\varphi(S) \subset (S^{-1}A)^\times$.

Theorem 1.3 (Universal property). *Let \mathcal{C} be the category*

- *whose objects are ring-homomorphisms (commutative rings with identity)*

$$f : A \rightarrow B$$

such that for every $s \in S$, the element $f(s)$ is invertible in B .

- *If $f : A \rightarrow B$ and $f' : A \rightarrow B'$ are two objects of \mathcal{C} , a morphism g of f into f' is a homomorphism*

$$g : B \rightarrow B'$$

making the diagram commutative:

We have that $\varphi_S : A \rightarrow S^{-1}A$ is a universal object in this category \mathcal{C} .

Theorem 1.4. *Let S be a multiplicative subset of A .*

1. *If S contains no zero divisors, then φ_S is a monomorphism.*
2. *If A has no zero divisors and $0 \notin S$, then $S^{-1}A$ is an integral domain.*
3. *If $S \subset A^\times$, then φ_S is an isomorphism.*

Definition 1.5. *Let A be a commutative ring and S be the set of all nonzero elements of A that are not zero divisors, then $S^{-1}A$ is called the **complete ring of quotients** of the ring A .*

*The complete ring of quotients of an integral domain A is its **quotient field**, denoted by $\text{Frac}(A)$.*

§1.1 Ideals in ring of fractions

Proposition 1.6. *Let S be a multiplicative subset of a commutative ring A and $\varphi_S : A \rightarrow S^{-1}A$*

1. *If \mathfrak{a} is an ideal in A , then $S^{-1}\mathfrak{a} = \{a/s \mid a \in \mathfrak{a}; s \in S\} = \mathfrak{a}S^{-1}A = \mathfrak{a}^e$.*
2. *If \mathfrak{b} is an ideal in $S^{-1}A$, then $\varphi_S^{-1}(\mathfrak{b})$ coincides with \mathfrak{b}^e*
3. *let \mathfrak{a} be an ideal of A , then $S^{-1}\mathfrak{a} = S^{-1}A$ if and only if $S \cap \mathfrak{a} \neq \emptyset$.*

Corollary 1.7.

$$S^{-1}(I + J) = S^{-1}I + S^{-1}J$$

$$S^{-1}(IJ) = (S^{-1}I)(S^{-1}J)$$

$$S^{-1}(I \cap J) = S^{-1}I \cap S^{-1}J$$

Theorem 1.8. *Let S be a multiplicative subset of a commutative ring A with identity and let I be an ideal in A .*

1. $J^{ce} = J$ for all ideals J of $S^{-1}A$. In other words every ideal in $S^{-1}A$ is of the form $S^{-1}I$ for some ideal I in A . Thus the set \mathcal{E} consists of all ideals of $S^{-1}A$ by 3.2.
2. If \mathfrak{p} is a prime ideal in A and $S \cap \mathfrak{p} = \emptyset$, then $S^{-1}\mathfrak{p}$ is a prime ideal in $S^{-1}A$.
3. there is a one-to-one correspondence between the set $\mathcal{U} = \{\mathfrak{p} : \mathfrak{p} \text{ is prime and disjoint from } S\}$ and the set $\mathcal{V} = \{S^{-1}\mathfrak{p} : S^{-1}\mathfrak{p} \text{ is prime in } S^{-1}A\}$, given by $\mathfrak{p} \mapsto S^{-1}\mathfrak{p}$.

Proof. Let $I = \varphi_S^{-1}(J)$, then $I^e = J^{ce} \subset J$, whence $S^{-1}I \subset J$. Conversely, if $r/s \in J$, then $\varphi_S(r) = rs/s = (r/s)(s^2/s) \in J$, whence $r \in \varphi_S^{-1}(J) = I$. Thus $r/s \in S^{-1}I$ and hence $J \subset S^{-1}I$. \square

§2 Localization and Local rings

Definition 2.1. Let A be a commutative ring with identity, \mathfrak{p} a prime ideal of A and multiplicative subset $S = A - \mathfrak{p}$. The ring of quotients $S^{-1}A$ is called the **localization of A at \mathfrak{p}** and is denoted $A_{\mathfrak{p}}$. If \mathfrak{a} is an ideal in A , then the ideal $\mathfrak{a}^e = S^{-1}\mathfrak{a}$ in $A_{\mathfrak{p}}$.

Remark. We always identify A with its image $\varphi_S(A)$ in $A_{\mathfrak{p}}$ thus A can be considered as a subring of $A_{\mathfrak{p}}$. In this case, the extension ideal $\mathfrak{a}^e = S^{-1}\mathfrak{a} = \mathfrak{a}A_{\mathfrak{p}}$.

Theorem 2.2. Let \mathfrak{p} be a prime ideal in a commutative ring A with identity and localization $A_{\mathfrak{p}}$.

1. There is a one-to-one correspondence between the set $\{\mathfrak{q} : \mathfrak{q} \text{ is prime and contained in } \mathfrak{p}\}$ and the set $\{S^{-1}\mathfrak{q} : S^{-1}\mathfrak{q} \text{ is prime in } A_{\mathfrak{p}}\}$, given by $\mathfrak{q} \mapsto S^{-1}\mathfrak{q}$;
2. The ideal $S^{-1}\mathfrak{p}$ is the unique maximal ideal of $A_{\mathfrak{p}}$.

Definition 2.3. A **local ring** is a commutative ring with identity which has a unique maximal ideal.

Theorem 2.4. The following conditions are equivalent.

1. R is a local ring;
2. all nonunits of R are contained in some ideal $M \neq R$;
3. the nonunits of R form an ideal.
4. for all $r, s \in R$, $r + s = 1_R$ implies r or s is a unit.

Proposition 2.5. Every nonzero homomorphic image of a local ring is local.

Chapter IV

Chain Condition

§1

Definition 1.1. Let R be a ring.

1. A R -module M is said to satisfy the **ascending chain condition (ACC) on submodules** (or to be Noetherian) if for every chain $M_1 \subset M_2 \subset M_3 \subset \cdots$ of submodules of M , there is an integer n such that $M_i = M_n$ for all $i \geq n$.
2. The ring R is **left [resp. right] Noetherian** if R satisfies ACC on submodules as a left [resp. right] R -module. It is equivalent that R satisfies the ascending chain condition on left [resp. right] ideals. R is said to be **Noetherian** if R is both left and right Noetherian.
3. A module N is said to satisfy the **descending chain condition (DCC) on submodules** (or to be Artinian) if for every chain $N_1 \supset N_2 \supset N_3 \supset \cdots$ of submodules of N , there is an integer m such that $N_i = N_m$ for all $i \geq m$.
4. R is **left [resp. right] Artinian** if R satisfies DCC on submodules as a left [resp. right] R -module. It is equivalent that R satisfies the descending chain condition on left [resp. right] ideals. R is said to be **Artinian** if R is both left and right Artinian.

Definition 1.2. Let R be a ring, A module M is said to satisfy the **maximum condition** [resp. minimum condition] on submodules if every nonempty set of submodules of M contains a maximal [resp. minimal] element (with respect to set theoretic inclusion).

§1.1 Equivalent Condition of Chain Condition

Theorem 1.3. A module A satisfies the ascending [resp. descending] chain condition on submodules if and only if A satisfies the maximal [resp. minimal] condition on submodules.

Theorem 1.4. Let R be a ring and $0 \rightarrow A \xrightarrow{f} B \xrightarrow{g} C \rightarrow 0$ be a short exact sequence of R -modules. Then B satisfies the ACC [resp. DCC] on submodules if and only if A and C satisfy it.

Proof. Sufficiency. If B satisfies the ascending chain condition, then so does its submodule $f(A)$. By exactness A is isomorphic to $f(A)$, whence A satisfies the ascending chain condition. If $C_1 \subset C_2 \subset \dots$ is a chain of submodules of C , then $g^{-1}(C_1) \subset g^{-1}(C_2) \subset \dots$ is a chain of submodules of B . Therefore, there is an n such that $g^{-1}(C_i) = g^{-1}(C_n)$ for all $i \geq n$. Since g is an epimorphism by exactness, it follows that $C_i = C_n$ for all $i \geq n$. Therefore, C satisfies the ascending chain condition.

Necessity. Suppose A and C satisfy the ascending chain condition and $B_1 \subset B_2 \subset \dots$ is a chain of submodules of B . For each i let

$$A_i = f^{-1}(f(A) \cap B_i) \quad \text{and} \quad C_i = g(B_i)$$

Let $f_i = f|_{A_i}$ and $g_i = g|_{B_i}$. Verify that for each i the following sequence is exact:

$$0 \rightarrow A_i \xrightarrow{f_i} B_i \xrightarrow{g_i} C_i \rightarrow 0.$$

Verify that $A_1 \subset A_2 \subset \dots$ and $C_1 \subset C_2 \subset \dots$. By hypothesis there exists an integer n such that $A_i = A_n$ and $C_i = C_n$ for all $i \geq n$. For each $i \geq n$ there is a commutative diagram with exact rows:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A_n & \xrightarrow{f_n} & B_n & \xrightarrow{g_n} & C_n & \longrightarrow & 0 \\ & & \downarrow \text{id} & & \downarrow i & & \downarrow \text{id} & & \\ 0 & \longrightarrow & A_i & \xrightarrow{f_i} & B_i & \xrightarrow{g_i} & C_i & \longrightarrow & 0 \end{array}$$

The Short Five Lemma implies that the inclusion map i is an isomorphism, thus be the identity map, whence B satisfies the ascending chain condition. \square

Corollary 1.5. *Let R be a ring, we have*

1. *If M_1 is a submodule of a module M , then M satisfies the ascending [resp. descending] chain condition if and only if M_1 and M/M_1 satisfy it.*
2. *If M_1, \dots, M_n are modules, then the direct sum $M_1 \oplus M_2 \oplus \dots \oplus M_n$ satisfies the ascending [resp. descending] chain condition on submodules if and only if each A_i satisfies it.*

Theorem 1.6. *If R is a left [resp. right] Noetherian [resp. Artinian] ring, then every finitely generated left [resp. right] R -module M is Noetherian [resp. Artinian].*

Proof. If M is finitely generated, then by ?? there is a free unitary R -module F with a finite basis and an epimorphism $\pi : F \rightarrow M$. Since F is a direct sum of a finite number of copies of R by ??, F is left Noetherian [resp. Artinian], whence $M \cong F/\text{Ker } \pi$ is Noetherian [resp. Artinian] by 1.5. \square

§2 Normal series and Composition Series of Modules

Definition 2.1. Let R be a ring and a R -module A .

1. A **normal series** for A is a chain of submodules: $A = A_0 \supset A_1 \supset A_2 \supset \cdots \supset A_n$. The factors of the series are the quotient modules

$$A_i/A_{i+1} \quad (i = 0, 1, \dots, n-1).$$

The **length** of the normal series is the number of proper inclusions (= number of nontrivial factors).

2. A **refinement** of the normal series $A = A_0 \supset A_1 \supset \cdots \supset A_n$ is a normal series obtained by inserting a finite number of additional submodules between the given ones. A **proper refinement** is one which has length larger than the original series.
3. Two normal series are **equivalent** if there is a one-to-one correspondence between the non-trivial factors such that corresponding factors are isomorphic modules. Thus equivalent series necessarily have the same length.
4. A **composition series** for A is a normal series $A = A_0 \supset A_1 \supset A_2 \supset \cdots \supset A_n = 0$ such that each factor A_k/A_{k+1} ($k = 0, 1, \dots, n-1$) is a module with no proper nonempty submodules.

Theorem 2.2. Any two normal series of a module A have refinements that are equivalent. Any two composition series of A are equivalent.

Theorem 2.3. A nonzero module M has a composition series if and only if M satisfies both the ACC and DCC on submodules.

Proof. (\Rightarrow) Suppose A has a composition series S of length n . If either chain condition fails to hold, one, can find submodules

$$A = A_0 \supsetneq A_1 \supsetneq A_2 \supsetneq \cdots \supsetneq A_n \supsetneq A_{n+1}$$

which form a normal series T of length $n+1$. By 2.2, S and T have refinements that are equivalent. This is a contradiction since equivalent series have equal length. For every refinement of the composition series S has the same length n as S , but every refinement of T necessarily has length at least $n+1$. Therefore, A satisfies both chain conditions.

(\Leftarrow) If B is a nonzero submodule of A , let $S(B)$ be the set of all proper submodules C of B . Also define $S(0) = \{0\}$. For each B there is a maximal element B' of $S(B)$ by 1.3. Let S be the set of all submodules of A and define a map $f : S \rightarrow S$ by $f(B) = B'$

Let $A_i = f^{(i)}(A)$, then $A \supset A_1 \supset A_2 \supset \cdots$ is a descending chain by construction, whence for some n , $A_i = A_n$ for all $i \geq n$. Since $A_{n+1} = f(A_n)$, the definition of f shows that $A_{n+1} = A_n$

only if $A_n = 0 = A_{n+1}$. Let m be the smallest integer such that $A_m = 0$. Then $m \leq n$ and $A_k \neq 0$ for all $k < m$. Furthermore for each $k < m$, A_{k+1} is a maximal submodule of A_k such that $A_k \supsetneq A_{k+1}$. Consequently, each A_k/A_{k+1} is nonzero and has no proper submodules by ?? . Therefore, $A \supset A_1 \supset \cdots \supset A_m = 0$ is a composition series for A . \square

Chapter V

Noetherian Modules and Rings

Contents

§1	Artinian Rings	16
§1.1		16
§1.2		16
§2	Noetherian Modules and Rings	17

§1 Artinian Rings

§1.1

Theorem 1.1 (Hopkins-Levitzki). *Let R be a ring. Then*

$$\text{left Artinian} \Leftrightarrow \text{right Artinian} \Rightarrow \text{left Noetherian} + \text{right Noetherian}$$

.

§1.2

In this subsection we shall study commutative Artinian rings.

Theorem 1.2. *Let A be a commutative ring with identity. Then the following conditions are equivalent:*

1. A is Artinian
2. $\text{Spec}(A)$ is finite and $\dim A = 0$
3. A is Noetherian and $\dim A = 0$.
4. A is uniquely (up to isomorphism) a finite direct product of Artin local rings.

Corollary 1.3. *In a commutative Artin ring the nilradical is equal to the Jacobson radical.*

Proposition 1.4. *Let A be an Artin local ring. Then the following are equivalent:*

1. *every ideal in A is principal;*
2. *the maximal ideal \mathfrak{m} is principal;*
3. $\dim_k(\mathfrak{m}/\mathfrak{m}^2) \leq 1$.

§2 Noetherian Modules and Rings

Theorem 2.1. *A module M is Noetherian if and only if every submodule of M is finitely generated. In particular, a commutative ring R is Noetherian if and only if every ideal of R is finitely generated.*

Theorem 2.2. *Recall that a module M is Noetherian.*

1.3 A module M satisfies the ascending [resp. descending] chain condition on submodules if and only if M satisfies the maximal [resp. minimal] condition on submodules.

2.1 A module M satisfies the ACC on submodules if and only if every submodule of M is finitely generated. In particular, a commutative ring R is Noetherian if and only if every ideal of R is finitely generated.

1.6 If R is a left [resp. right] Noetherian [resp. Artinian] ring with identity, then every finitely generated unitary left [resp. right] R -module A satisfies the ACC [resp. DCC] on submodules.

Proposition 2.3. *Let A be Noetherian ring*

Proposition 2.4. *If A is Noetherian and ϕ is a homomorphism, then $B = \phi(A)$ is Noetherian.*

Proposition 2.5. *Let A be a subring of B ; suppose that A is Noetherian and that B is finitely generated as an A -module. Then B is Noetherian (as a ring).*

Proposition 2.6. *If A is Noetherian and S is any multiplicatively closed subset of A , then $S^{-1}A$ is Noetherian.*

Theorem 2.7. *If R is a commutative Noetherian ring with identity, then so is $R[x_1, \dots, x_n]$ and $R[[x]]$*

Proposition 2.8. *If R is a commutative ring with identity and \mathfrak{p} is an ideal which is maximal in the set of all ideals of R which are not finitely generated, then \mathfrak{p} is prime.*

Proof. Suppose $ab \in \mathfrak{p}$ but $a \notin \mathfrak{p}$ and $b \notin \mathfrak{p}$. Then $\mathfrak{p} + (a)$ and $\mathfrak{p} + (b)$ are ideals properly containing \mathfrak{p} and therefore finitely generated by maximality of \mathfrak{p} . Consequently $\mathfrak{p} + (a) = (p_1 + r_1a, \dots, p_n + r_na)$ and $\mathfrak{p} + (b) = (p'_1 + r'_1b, \dots, p'_m + r'_mb)$ for some $p_i, p'_i \in \mathfrak{p}$ and $r_i, r'_i \in R$.

If $J = (\mathfrak{p} : a) = \{r \in R \mid ra \in \mathfrak{p}\}$, then J is an ideal. Since $ab \in \mathfrak{p}$, $(p'_i + r'_ib)a = p'_ia + r'_iab \in \mathfrak{p}$ for all i , whence $\mathfrak{p} \subset \mathfrak{p} + (b) \subset J$. By maximality, J is finitely generated, say $J = (j_1, \dots, j_k)$.

If $x \in \mathfrak{p}$, then $x \in \mathfrak{p} + (a)$ and hence for some $s_i \in R$, $x = \sum_{i=1}^n s_i (p_i + r_i a) = \sum_{i=1}^n s_i p_i + \sum_{i=1}^n s_i r_i a$. Consequently, $(\sum_i s_i r_i) a = x - \sum_i s_i p_i \in \mathfrak{p}$, whence $\sum_i s_i r_i \in J$. Thus for some $t_i \in R$, $\sum_{i=1}^n s_i r_i = \sum_{i=1}^k t_i j_i$ and $x = \sum_{i=1}^n s_i p_i + \sum_{i=1}^k t_i j_i a$. Therefore, \mathfrak{p} is generated by $p_1, \dots, p_n, j_1 a, \dots, j_k a$, which is a contradiction. Thus $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$ and \mathfrak{p} is prime by ?? \square

Theorem 2.9 (I.S.Cohen). *A commutative ring R with identity is Noetherian if and only if every prime ideal of R is finitely generated.*

Proof. Let \mathcal{S} be the set of all ideals of R which are not finitely generated. If \mathcal{S} is nonempty, then use Zorn's Lemma to find a maximal element P of \mathcal{S} . P is prime by Proposition 2.4 and hence finitely generated by hypothesis.

This is a contradiction unless $\mathcal{S} = \emptyset$. Therefore, R is Noetherian by Theorem 1.9. \square

Chapter VI

Integral

§1 Rings Extensions

Definition 1.1. Let S be a commutative ring with identity and R a subring of S containing 1_S .

1. Then S is said to be an **extension ring** of R .
2. An element $s \in S$ is said to be **integral** over R if s is a root of a monic polynomial in $R[x]$.
3. If every element of S is integral over R , S is said to be an **integral extension** of R .
4. The **integral closure** of R in S is the set of elements of S that are integral over R .
5. The ring R is said to be **integrally closed** in S if R is equal to its integral closure in S .

The integral closure of an integral domain R in its field of fractions is called the **normalization** of R . An integral domain is called integrally closed or normal if it is integrally closed in its field of fractions.

Remark. It follows from [corollary 1.3](#) that the integral closure of R in S is a subring of S containing R .

Theorem 1.2. Let S be an extension ring of R and $s \in S$. Then the following conditions are equivalent.

1. s is integral over R
2. Subring $R[s]$ is a finitely generated R -module
3. There is a subring T that $R[s] \subset T \subset S$, which is finitely generated as an R -module;
4. There is a faithful $R[s]$ -submodule M which is finitely generated as an R -module.

Corollary 1.3. Let S be an extension ring of R . Then

1. If S is finitely generated as an R -module, then S is an integral extension of R .

2. If $s_1, \dots, s_t \in S$ are integral over R , then $R[s_1, \dots, s_t]$ is a finitely generated R -module and an integral extension ring of R .
3. If T is an integral extension ring of S and S is an integral extension ring of R , then T is an integral extension ring of R .

Proof. It immediately follows from 1.2 □

Proof. We have a tower of extension rings:

$$R \subset R[s_1] \subset R[s_1, s_2] \subset \cdots \subset R[s_1, \dots, s_t]$$

For each i , s_i is integral over R and hence integral over $R[s_1, \dots, s_{i-1}]$. Since $R[s_1, \dots, s_i] = R[s_1, \dots, s_{i-1}][s_i]$, $R[s_1, \dots, s_i]$ is a finitely generated module over $R[s_1, \dots, s_{i-1}]$ by 1.2. Thus $R[s_1, \dots, s_n]$ is a finitely generated R -module, then $R[s_1, \dots, s_n]$ is an integral extension ring of R by 1. □

Proof. T is obviously an extension ring of R . If $t \in T$, then t is integral over S and therefore the root of some monic polynomial $f \in S[x]$, say $f = \sum_{i=0}^n s_i x^i$. Since f is also a polynomial over the ring $R[s_0, s_1, \dots, s_{n-1}]$, t is integral over $R[s_0, \dots, s_{n-1}]$.

By 1.2 $R[s_0, \dots, s_{n-1}][t]$ is a finitely generated $R[s_0, \dots, s_{n-1}]$ -module. But since S is integral over R , $R[s_0, \dots, s_{n-1}]$ is a finitely generated R -module by 2. Then

$$R[s_0, \dots, s_{n-1}][t] = R[s_0, \dots, s_{n-1}, t]$$

is a finitely generated R -module. Since $R[t] \subset R[s_0, \dots, s_{n-1}, t]$, t is integral over R by 1.2. □

Proposition 1.4. 1. Every unique factorization domain is integrally closed.

2. In particular, the polynomial ring $F[x_1, \dots, x_n]$ (F a field) is integrally closed in its quotient field $F(x_1, \dots, x_n)$.

§1.1 integral extension

Theorem 1.5. Let T be a multiplicative subset of an integral domain R such that $0 \notin T$. If R is integrally closed, then $T^{-1}R$ is an integrally closed integral domain.

Proof. $T^{-1}R$ is an integral domain and R may be identified with a subring of $T^{-1}R$ by 1.2. Extending this identification, the quotient field $Q(R)$ of R may be considered as a subfield of the quotient field $Q(T^{-1}R)$ of $T^{-1}R$. Verify that $Q(R) = Q(T^{-1}R)$.

Let $u \in Q(T^{-1}R)$ be integral over $T^{-1}R$; then for some $r_i \in R$ and $s_i \in T$,

$$u^n + (r_{n-1}/s_{n-1})u^{n-1} + \cdots + (r_1/s_1)u + (r_0/s_0) = 0.$$

Multiply through this equation by s^n , where $s = s_0 s_1 \cdots s_{n-1} \in T$, and conclude that su is integral over R . Since $su \in Q(T^{-1}R) = Q(R)$ and R is integrally closed, $su \in R$. Therefore, $u = su/s \in T^{-1}R$, whence $T^{-1}R$ is integrally closed. \square

Theorem 1.6. *Let S be an integral extension ring of R . Then the following statements hold.*

1. *Assume that S is an integral domain. Then R is a field if and only if S is a field.*
2. *Let \mathfrak{p} be a prime ideal in R . Then there is a prime ideal \mathfrak{q} in S with $\mathfrak{p} = \mathfrak{q} \cap R$.
Moreover, \mathfrak{p} is maximal if and only if \mathfrak{q} is maximal.*
3. *(The Going-up Theorem) Let $\mathfrak{p}_1 \subseteq \mathfrak{p}_2 \subseteq \cdots \subseteq \mathfrak{p}_n$ be a chain of prime ideals in R and suppose there are prime ideals $\mathfrak{q}_1 \subseteq \mathfrak{q}_2 \subseteq \cdots \subseteq \mathfrak{q}_m$ of S with $\mathfrak{p}_i = \mathfrak{q}_i \cap R$, $1 \leq i \leq m$ and $m < n$. Then the ascending chain of ideals can be completed: there are prime ideals $\mathfrak{q}_{m+1} \subseteq \cdots \subseteq \mathfrak{q}_n$ in S such that $\mathfrak{p}_i = \mathfrak{q}_i \cap R$ for all i .*

Theorem 1.7 (The Going-down Theorem). *Assume that S is an integral domain and R is integrally closed in S . Let $\mathfrak{p}_1 \supseteq \mathfrak{p}_2 \supseteq \cdots \supseteq \mathfrak{p}_n$ be a chain of prime ideals in R and suppose there are prime ideals $\mathfrak{q}_1 \supseteq \mathfrak{q}_2 \supseteq \cdots \supseteq \mathfrak{q}_m$ of S with $\mathfrak{p}_i = \mathfrak{q}_i \cap R$, $1 \leq i \leq m$ and $m < n$. Then the descending chain of ideals can be completed: there are prime ideals $\mathfrak{q}_{m+1} \supseteq \cdots \supseteq \mathfrak{q}_n$ in S such that $\mathfrak{p}_i = \mathfrak{q}_i \cap R$ for all i .*

Theorem 1.8. *Let S be an integral extension ring of R and let \mathfrak{q} be a prime ideal in S which lies over a prime ideal \mathfrak{p} in R . Then \mathfrak{q} is maximal in S if and only if \mathfrak{p} is maximal in R .*

Proof. Suppose \mathfrak{q} is maximal in S . By ?? there is a maximal ideal \mathfrak{m} of R that contains \mathfrak{p} and \mathfrak{m} is prime by ?. By ?? there is a prime ideal \mathfrak{q}' in S such that $\mathfrak{q} \subset \mathfrak{q}'$ and \mathfrak{q}' lies over \mathfrak{m} . Since \mathfrak{q}' is prime, $\mathfrak{q}' \neq S$. The maximality of \mathfrak{q} implies that $\mathfrak{q} = \mathfrak{q}'$, whence $\mathfrak{p} = \mathfrak{q} \cap R = \mathfrak{q}' \cap R = \mathfrak{m}$. Therefore, \mathfrak{p} is maximal in R .

Conversely suppose \mathfrak{p} is maximal in R . Since \mathfrak{q} is prime in S , $\mathfrak{q} \neq S$ and there is a maximal ideal N of S containing \mathfrak{q} and N is prime, whence $1_R = 1_S \notin N$. Since $\mathfrak{p} = R \cap \mathfrak{q} \subset R \cap N \subset R$, we must have $\mathfrak{p} = R \cap N$ by maximality. Thus \mathfrak{q} and N both lie over \mathfrak{p} and $\mathfrak{q} \subset N$. Therefore, $\mathfrak{q} = N$ by 1.8. \square

§2 Discrete Valuation Ring

Definition 2.1. *The following conditions on a principal ideal domain are equivalent:*

1. *A has exactly one nonzero prime ideal;*
2. *up to associates, A has exactly one prime element;*
3. *A is local and is not a field.*

*A ring satisfying these conditions is called a **discrete valuation ring**.*

Theorem 2.2. *An integral domain A is a discrete valuation ring if and only if*

- (i) A is noetherian,
- (ii) A is integrally closed, and
- (iii) A has exactly one nonzero prime ideal.

§3 Dedekind Domain

Definition 3.1. *A **Dedekind domain** is an integral domain R satisfying the following equivalent conditions:*

1. R is Noetherian, integrally closed and has Krull dimension one (Every nonzero prime ideal of R is maximal).
2. Every nonzero ideal of R is invertible
3. Every finitely generated torsion-free R -module is free.
4. the localization $R_{\mathfrak{p}}$ at each prime ideal \mathfrak{p} of R is a discrete valuation ring.
5. Every nonzero proper ideal of R can be written as a product of prime ideals of R , and this factorization is unique up to the order of the factors.

Proposition 3.2. *Let A be an integral domain, and let S be a multiplicative subset of A .*

1. *If A is noetherian, then so also is $S^{-1}A$.*
2. *If A is integrally closed, then so also is $S^{-1}A$.*
3. *If A has Krull dimension one, then so also does $S^{-1}A$.*
4. *If A is a Dedekind domain, then so also is $S^{-1}A$.*

Proposition 3.3. *A noetherian integral domain A is a Dedekind domain if and only if, for every nonzero prime ideal \mathfrak{p} in A , the localization $A_{\mathfrak{p}}$ is a discrete valuation ring.*

§3.1 Unique factorization of ideals

Theorem 3.4. *Let A be a Dedekind domain. Every proper nonzero ideal \mathfrak{a} of A can be written in the form*

$$\mathfrak{a} = \mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_n^{r_n}$$

with the \mathfrak{p}_i distinct prime ideals and the $r_i > 0$; the \mathfrak{p}_i and the r_i are uniquely determined.

§3.2 The ideal class group

Definition 3.5. Let R be an integral domain with quotient field K . A **fractional ideal** of R is

- (i) a nonzero R -submodule I of K
- (ii) there exists a nonzero $d \in R$ such that $dI \subset R$ i.e., $(R : I) \cap R \neq \emptyset$

Definition 3.6. If R is an integral domain with quotient field K , then the set of all fractional ideals of R forms a commutative monoid, with identity R and multiplication given by

$$IJ = \left\{ \sum_{i=1}^n a_i b_i \mid a_i \in I; b_i \in J; n \in \mathbb{Z}_{\geq 1} \right\}$$

A fractional ideal I of an integral domain R is said to be **invertible** if $IJ = R$ for some fractional ideal J of R .

Theorem 3.7. Let A be a Dedekind domain. The set $\text{Id}(A)$ of fractional ideals is a group; in fact, it is the free abelian group on the set of nonzero prime ideals.

Definition 3.8. We define the **ideal class group** $\text{Cl}(A)$ of A to be the quotient $\text{Cl}(A) = \text{Id}(A)/\text{P}(A)$ of $\text{Id}(A)$ by the subgroup of principal ideals. The **class number** of A is the order of $\text{Cl}(A)$ (when finite).

In the case that A is the ring of integers \mathcal{O}_K in a number field K , we often refer to $\text{Cl}(\mathcal{O}_K)$ as the ideal class group of K , and its order as the class number of K .

Proposition 3.9. Let R be an integral domain with quotient field K .

1. Indeed for any fractional ideal I the set $I^{-1} = \{a \in K \mid aI \subset R\}$ is easily seen to be a fractional ideal such that $I^{-1}I = II^{-1} \subset R$.
2. The inverse of an invertible fractional ideal I is unique and is $I^{-1} = \{a \in K \mid aI \subset R\}$. If I is invertible and $IJ = JI = R$, then clearly $J \subset I^{-1}$. Conversely, since I^{-1} and J are R -submodules of K , $I^{-1} = RI^{-1} = (JI)I^{-1} = J(II^{-1}) \subset JR = RJ \subset J$, whence $J = I^{-1}$.
3. If I, A, B are fractional ideals of R such that $IA = IB$ and I is invertible, then $A = RA = (I^{-1}I)A = I^{-1}(IB) = RB = B$.
4. If I is an ordinary ideal in R , then $R \subset I^{-1}$.

Lemma 3.10. Let I, I_1, I_2, \dots, I_n be ideals in an integral domain R .

1. The ideal $I_1 I_2 \cdots I_n$ is invertible if and only if each I_j is invertible.
2. If $\mathfrak{p}_1 \cdots \mathfrak{p}_m = I = \mathfrak{q}_1 \cdots \mathfrak{q}_n$, where the \mathfrak{p}_i and \mathfrak{q}_j are prime ideals in R and every \mathfrak{p}_i is invertible, then $m = n$ and (after reindexing) $\mathfrak{p}_i = \mathfrak{q}_i$ for each $i = 1, \dots, m$.

Lemma 3.11. *If I is a fractional ideal of an integral domain R with quotient field K and $f \in \text{Hom}_R(I, R)$, then for all $a, b \in I : af(b) = bf(a)$.*

Lemma 3.12. *Every invertible fractional ideal of an integral domain R with quotient field K is a finitely generated R -module.*

Theorem 3.13. *Let R be an integral domain and I a fractional ideal of R . Then I is invertible if and only if I is a projective R -module.*

§4 Discrete valuations

Definition 4.1. *Let K be a field. A **discrete valuation** on K is a nonzero homomorphism $v : K^\times \rightarrow \mathbb{Z}$ such that $v(a + b) \geq \min(v(a), v(b))$.*

*As v is not the zero homomorphism, its image is a nonzero subgroup of \mathbb{Z} , and is therefore of the form $m\mathbb{Z}$ for some $m \in \mathbb{Z}$. If $m = 1$, then $v : K^\times \rightarrow \mathbb{Z}$ is surjective, and v is said to be **normalized**; otherwise, $x \mapsto m^{-1} \cdot v(x)$ will be a normalized discrete valuation.*

We extend v to a map $K \rightarrow \mathbb{Z} \cup \{\infty\}$ by setting $v(0) = \infty$, where ∞ is a symbol $\geq n$ for all $n \in \mathbb{Z}$.

Remark. *We have*

1. $v(\zeta) = 0$ for some $\zeta \in K^\times$
2. $v(-a) = v(a)$ for all $a \in K$;
3. $v(a + b) = \max\{v(a), v(b)\}$ if $v(a) \neq v(b)$.

We often use "ord" rather than " v " to denote a discrete valuation.

Proposition 4.2. *Let v be a discrete valuation on K , then*

$$A := \{a \in K \mid v(a) \geq 0\}$$

is a principal ideal domain with maximal ideal

$$\mathfrak{m} = \{a \in K \mid v(a) > 0\}$$

If $v(K^\times) = m\mathbb{Z}$, then the ideal \mathfrak{m} is generated by every element of $v^{-1}(m)$.

Definition 4.3. *Let A be a Dedekind domain and let \mathfrak{p} be a prime ideal in A . For any $c \in K^\times$, let $v(c)$ be the exponent of \mathfrak{p} in the factorization of (c) . Then v is a normalized discrete valuation on K , called the **discrete valuation associated to \mathfrak{p}** , denoted by $\text{ord}_{\mathfrak{p}}$.*

Proposition 4.4. *Let x_1, \dots, x_m be elements of a Dedekind domain A , and let $\mathfrak{p}_1, \dots, \mathfrak{p}_m$ be distinct prime ideals of A . For every integer n , there is an $x \in A$ such that*

$$\text{ord}_{\mathfrak{p}_i}(x - x_i) > n, \quad i = 1, 2, \dots, m.$$

§5 Integral closures of Dedekind domains

Theorem 5.1. *Let A be a Dedekind domain with field of fractions K and L/K be a finite separable extension, then the integral closure of A in L is Dedekind domain.*

Definition 5.2. *Let A be a Dedekind domain with field of fractions K , and let B be the integral closure of A in a finite separable extension L of K . A prime ideal \mathfrak{p} of A will factor in B ,*

$$\mathfrak{p}B = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$$

where \mathfrak{P} are distinct prime ideals in B and $e_i \geq 1$,

1. If any of the numbers is > 1 , then we say that \mathfrak{p} is **ramified** in B (or L). The number e_i is called the **ramification index**.

2. We say \mathfrak{P} divides \mathfrak{p} , written $\mathfrak{P} \mid \mathfrak{p}$, if \mathfrak{P} occurs in the factorization of \mathfrak{p} in B .

We then write $e(\mathfrak{P}/\mathfrak{p})$ for the ramification index and $f(\mathfrak{P}/\mathfrak{p})$ for the degree of the field extension $[B/\mathfrak{P} : A/\mathfrak{p}]$ (called the **residue class degree**).

3. \mathfrak{p} is said to **split** (or split completely) in L if $e_i = f_i = 1$ for all i

4. \mathfrak{p} is said to be **inert** in L if $\mathfrak{p}B$ is a prime ideal (so $g = 1 = e$).

Theorem 5.3. *Let m be the degree of L over K , and let $\mathfrak{P}_1, \dots, \mathfrak{P}_g$ be the prime ideals dividing \mathfrak{p} ; then*

$$\sum_{i=1}^g e_i f_i = m$$

where $e_i = e(\mathfrak{P}_i/\mathfrak{p})$ and $f_i = f(\mathfrak{P}_i/\mathfrak{p})$. If L is Galois over K , then all the ramification numbers are equal, and all the residue class degrees are equal, and so

$$efg = m.$$

Chapter VII

Completions

§1 Filtered and Graded Modules

Let A be a commutative ring and M a module.

§2 Filtrations

Definition 2.1. Let A be a ring, \mathfrak{a} an ideal of A and M an A -module.

1. A **filtration** of M one means an sequence of submodules $\mathcal{F} = \{F_i M\}$

$$\cdots \subset F_{n+1}M \subset F_n M \subset F_{n+1}M \subset \cdots \subset M$$

Remark. A descending filtration of M one means a sequence of submodules

$$M = F^0 M \supset F^1 M \supset F^2 M \supset \cdots \supset F^n M \supset \cdots$$

A increasing filtration of M one means a sequence of submodules

$$F_0 M \subset F_1 M \subset F_2 M \subset \cdots \subset F_n M \subset \cdots \subset M$$

with union $\bigcup_{n=0}^{\infty} F_n M = M$.

In this chapter, we shall only consider descending filtrations.

2. We say that it is an **\mathfrak{a} -filtration** if $\mathfrak{a}F^n M \subset F^{n+1} M$ for all n .
3. We say that an \mathfrak{a} -filtration is **\mathfrak{a} -stable** if we have $\mathfrak{a}F^n M = F^{n+1} M$ for all n sufficiently large.

Lemma 2.2. If (M_n) , (M'_n) are stable \mathfrak{a} -filtrations of M , then they have bounded difference: that is, there exists an integer n_0 such that $M_{n+n_0} \subseteq M'_n$ and $M'_{n+n_0} \subseteq M_n$ for all $n \geq 0$.

Proof. Enough to take $M'_n = \mathfrak{a}^n M$. Since $\mathfrak{a}M_n \subseteq M_{n+1}$ for all n , we have $\mathfrak{a}^n M \subseteq M_n$; also $\mathfrak{a}M_n = M_{n+1}$ for all $n \geq n_0$ say, hence $M_{n+n_0} = \mathfrak{a}^n M_{n_0} \subseteq \mathfrak{a}^n M$. \square

§3 Graded

Definition 3.1. The ring A is called a **graded ring** if it is a family $\{A_n\}_{n \geq 0}$ of subgroups of A , such that

$$A = \bigoplus_{n=0}^{\infty} A_n$$

as an abelian group and $A_m A_n \subseteq A_{m+n}$ for all $m, n \geq 0$.

Remark. Thus A_0 is a subring of A , and each A_n is an A_0 -module. Furthermore, $A_+ = \bigoplus_{n>0} A_n$ is an ideal of A .

Definition 3.2. Let A be a graded ring and A -module M .

1. A **graded A -module** is an A -module M together with a family $\{M_n\}_{n \geq 0}$ of subgroups of M such that $M = \bigoplus_{n=0}^{\infty} M_n$ as an abelian group and $A_m M_n \subseteq M_{m+n}$ for all $m, n \geq 0$.
2. Elements of M_n are then called **homogeneous of degree n** .
3. Any element $y \in M$ can be written uniquely as a finite sum $\sum_n y_n$, where $y_n \in M_n$ for all $n \geq 0$, and all but a finite number of the y_n are 0. The non-zero components y_n are called the **homogeneous components** of y .

Remark. Thus each M_n is an A_0 -module.

Definition 3.3. If M, N are graded A -modules, a homomorphism of graded A -modules is an A -module homomorphism $f : M \rightarrow N$ such that $f(M_n) \subseteq N_n$ for all $n \geq 0$.

Proposition 3.4. Let A be a graded ring. Then A is Noetherian if and only if A_0 is Noetherian, and A is finitely generated as A_0 -algebra

§4 First associated graded ring

Definition 4.1. Let A be a ring, ideal \mathfrak{a} and A -module M filtered by \mathfrak{a} -filtration $\{M_n\}$.

1. We can form a **first associated graded ring**

$$S = S_{\mathfrak{a}}(A) = \bigoplus_{n=0}^{\infty} \mathfrak{a}^n$$

$$\mathfrak{a}^0 = A.$$

Remark. It is also a A -algebra called **Rees algebra**, with the homomorphism $A \rightarrow S_{\mathfrak{a}}(A)$ defined by $a \mapsto (a, 0, 0, \dots)$.

2. Then $M_S = \bigoplus_n M_n$ is a graded $S_{\mathfrak{a}}(A)$ -module.

Remark. If A is Noetherian, \mathfrak{a} is generated by x_1, \dots, x_r ; then $S_{\mathfrak{a}}(A) = A[x_1, \dots, x_r]$ and is Noetherian.

Lemma 4.2. Let A be a Noetherian ring, ideal \mathfrak{a} , and M a finitely generated module, with an \mathfrak{a} -filtration. Then M_S is finite over $S_{\mathfrak{a}}(A)$ if and only if the filtration of M is \mathfrak{a} -stable.

Theorem 4.3 (Artin-Rees). Let A be a Noetherian ring, \mathfrak{a} an ideal, M a finite A -module with a stable \mathfrak{a} -filtration. Let N be a submodule, and let $N_n = N \cap M_n$. Then $\{N_n\}$ is a stable \mathfrak{a} -filtration of N .

Corollary 4.4. Let A be a Noetherian ring, M a finite A -module, and N a submodule. Let \mathfrak{a} be an ideal. There exists an integer s such that for all integers $n \geq s$ we have

$$\mathfrak{a}^n M \cap N = \mathfrak{a}^{n-s} (\mathfrak{a}^s M \cap N)$$

§5 Second associated graded ring

Definition 5.1. Let A be a ring, \mathfrak{a} an ideal and M an A -module with an \mathfrak{a} -filtration $\{M_n\}$.

1. We define the **second associated graded ring**

$$\mathrm{gr}_{\mathfrak{a}}(A) = \bigoplus_{n=0}^{\infty} \mathfrak{a}^n / \mathfrak{a}^{n+1}.$$

where $\mathfrak{a}^0 = A$.

2. We define

$$\mathrm{gr}(M) = \bigoplus_{n=0}^{\infty} M_n / M_{n+1}$$

then $\mathrm{gr}(M)$ is a graded $\mathrm{gr}_{\mathfrak{a}}(A)$ -module.

Proposition 5.2. Let A be a Noetherian ring and \mathfrak{a} an ideal. Then

1. $\mathrm{gr}_{\mathfrak{a}}(A)$ is Noetherian.
2. If M is a finitely generated A -module with a stable \mathfrak{a} -filtration, then $\mathrm{gr}(M)$ is a finitely generated graded $\mathrm{gr}_{\mathfrak{a}}(A)$ -module.

§6 Graded Algebra

Definition 6.1. Let K be a commutative ring and A a K -algebra. Then A is called **graded K -algebra** if

- (i) $A = \bigoplus_{n=0}^{\infty} A_n$ is a graded ring,

(ii) each A_n is a K -submodule of A ,

Remark. Thus A becomes a graded A module in a natural way. And $K \hookrightarrow A_0$ be a ring-homomorphism.

Definition 6.2. Let K be a commutative ring and A a K -algebra. A increasing **filtration** of A is

(i) a sequence of K -submodules $F_0 \subset F_1 \subset F_2 \subset \cdots \subset A$ such that

(ii) $F_i F_j \subseteq F_{i+j}$ for all i, j .

(iii) $A = \bigcup_{n=0}^{\infty} F_n$

Then A is called a **filtered K -algebra**.

Definition 6.3. Let K be a commutative ring and A a filtered K -algebra with filtration $\mathcal{F} = \{F_n\}$. We define the **graded K -algebra associated with \mathcal{F}**

$$\text{gr}(A) = \bigoplus_{n=0}^{\infty} F_n / F_{n-1}$$

where $F_{-1} = 0$. Multiplication is defined in the obvious way.

§7 Krull intersection theorem

Lemma 7.1. Let M be a finitely generated module over a commutative ring R with identity. Then M is Noetherian [resp. Artinian] if and only if $R / \text{Ann}(M)$ is a Noetherian [resp. Artinian] ring.

Proof. Let M be generated by m_1, \dots, m_n and assume M satisfies the ascending chain condition. Then $M = Rm_1 + \cdots + Rm_n$ by ???. Consequently, $\text{Ann}(M) = \text{Ann}(m_1) \cap \text{Ann}(m_2) \cap \cdots \cap \text{Ann}(m_n)$, whence there is a monomorphism of rings

$$\theta : R/I \rightarrow R/I_1 \times \cdots \times R/I_n$$

It is easy to see that θ is also an R -module monomorphism. Verify that for each j the map $R/I_j \rightarrow Rb_j$ given by $r + I_j \mapsto rb_j$ is an isomorphism of R -modules.

Since the submodule Rb_j of M necessarily satisfies the ascending chain condition, so does R/I_j . Therefore, $R/I_1 \oplus \cdots \oplus R/I_n$ satisfies the ascending chain condition on R -submodules by 1.5. Consequently its submodule $\text{Im } \theta \cong R/I$ satisfies the ascending chain condition on R -submodules. But every ideal of the ring R/I is an R -submodule of R/I . Therefore, R/I is Noetherian.

Conversely suppose $R / \text{Ann}(M)$ is Noetherian. Verify that M is an $R / \text{Ann}(M)$ -module with $(r + \text{Ann}(M))m = rm$ and that the R/I -submodules of M are precisely the R -submodules. Consequently, M satisfies the ascending chain condition by 1.6. \square

Lemma 7.2. *Let R be a commutative ring with identity, \mathfrak{p} be a prime ideal in R and M be a Noetherian R -module. If N is a \mathfrak{p} -primary submodule of M , then there exists a positive integer k such that $\mathfrak{p}^k M \subset N$, i.e. $\mathfrak{p}^k \subset \mathfrak{q} = (M : N)$*

Proof. Let I be the annihilator of M in R and consider the ring $\bar{R} = R/I$. Denote the coset $r + I \in \bar{R}$ by \bar{r} . Clearly $I \subset (M : N) \subset \mathfrak{p}$, whence $\bar{\mathfrak{p}} = \mathfrak{p}/I$ is an ideal of \bar{R} . M and N are each \bar{R} -modules with $\bar{r}a = ra$ ($r \in R, a \in M$).

We claim that N is a primary \bar{R} -submodule of M . If $\bar{r}a \in N$ with $r \in R$ and $a \in M - N$, then $ra \in N$. Since N is a primary R -submodule, $r^n M \subset N$ for some n , whence $\bar{r}^n M \subset N$ and N is \bar{R} -primary.

Since $\{\bar{r} \in \bar{R} \mid \bar{r}^k M \subset N \text{ for some } k > 0\} = \{\bar{r} \in \bar{R} \mid r^k M \subset N\} = \{\bar{r} \in \bar{R} \mid r \in \mathfrak{p}\} = \bar{\mathfrak{p}}$, $\bar{\mathfrak{p}}$ is a prime ideal of \bar{R} and N is a $\bar{\mathfrak{p}}$ -primary \bar{R} -submodule of M .

Since \bar{R} is Noetherian by 7.1, $\bar{\mathfrak{p}}$ is finitely generated by 2.1. Let $\bar{p}_1, \dots, \bar{p}_s$ ($p_i \in \mathfrak{p}$) be the generators of $\bar{\mathfrak{p}}$. For each i there exists n_i such that $\bar{p}_i^{n_i} M \subset N$. If $m = n_1 + \dots + n_s$, then it follows that $\bar{\mathfrak{p}}^m M \subset N$. The facts-that $\bar{\mathfrak{p}} = \mathfrak{p}/I$ and $IM = 0$ now imply that $\mathfrak{p}^m M \subset N$. \square

Theorem 7.3 (Krull Intersection Theorem). *Let R be a commutative ring with identity, \mathfrak{a} an ideal of R and M a Noetherian R -module. If submodule $N = \bigcap_{n=1}^{\infty} \mathfrak{a}^n M$, then $\mathfrak{a}N = N$.*

Proof. If $\mathfrak{a}N = M$, then $M = \mathfrak{a}N \subset N$, whence $N = M = \mathfrak{a}N$. If $\mathfrak{a}N \neq M$, then by 2.10 $\mathfrak{a}N$ has a reduced primary decomposition:

$$\mathfrak{a}N = Q_1 \cap Q_2 \cap \dots \cap Q_s$$

where each Q_i is a \mathfrak{p}_i -primary submodule of M for some prime ideal \mathfrak{p}_i of R . Since $\mathfrak{a}N \subset N$ in any case, we need only show that $N \subset Q_i$ for every i .

Let i ($1 \leq i \leq s$) be fixed. Suppose first that $\mathfrak{a} \subset \mathfrak{p}_i$. By 7.2 there is an integer m such that $\mathfrak{p}_i^m M \subset Q_i$, whence $N = \bigcap_n \mathfrak{a}^n M \subset \mathfrak{a}^m M \subset \mathfrak{p}_i^m M \subset Q_i$. Now suppose $\mathfrak{a} \not\subset \mathfrak{p}_i$. Then there exists $r \in \mathfrak{a} - \mathfrak{p}_i$. If $N \not\subset Q_i$, then there exists $b \in N - Q_i$. Since $rb \in \mathfrak{a}N \subset Q_i$, $b \notin Q_i$ and Q_i is primary, $r^n M \subset Q_i$ for some $n > 0$. Consequently, $r \in \mathfrak{p}_i$ since Q_i is a \mathfrak{p}_i -primary submodule. This contradicts the choice of $r \in \mathfrak{a} - \mathfrak{p}_i$. Therefore $N \subset Q_i$. \square

Part II

The Structure of Rings

Chapter VIII

The Structure of Rings

Contents

§1	Simplicity and Primitivity	32
§1.1	Primitivity	33
§1.2	Jacobson Density Theorem	33
§2	Simple ring	35

§1 Simplicity and Primitivity

Definition 1.1. A ring R is said to be **simple** if R has no proper two-sided ideals.

Definition 1.2. A left module M over a ring R is said to be **simple** (or **irreducible**) if M has no proper submodules.

Remark. A left ideal \mathfrak{a} of R is a simple left R -module if and only if \mathfrak{a} is a minimal left ideal of R . In this case, we call \mathfrak{a} the **simple left ideal** of R .

Proposition 1.3. Let R be a ring and M be a simple R -module, then

1. $M = Rm$ for every $0 \neq m \in M$.
2. If $0 \neq u \in M$, then $M \cong R/\text{Ann}(u)$, thus $\text{Ann}(u)$ is a left maximal ideal.
Conversely, if \mathfrak{m} is left maximal in R , then R/\mathfrak{m} is a simple R -module with $\text{Ann}(R/\mathfrak{m}) = \mathfrak{m}$.
3. If R is not a division ring, then M is a torsion module. $m \in M$.

Lemma 1.4 (Schur). Let M be a simple module over a ring R and let N_i be any R -module.

1. Every nonzero R -module homomorphism $f : M \rightarrow N_1$ is a monomorphism;
2. Every nonzero R -module homomorphism $g : N_2 \rightarrow M$ is an epimorphism;
3. The endomorphism ring $D = \text{Hom}_R(M, M)$ is a division ring, then M is a vector space over $\text{Hom}_R(M, M)$ with $fa = f(a)$

§1.1 Primitivity

Definition 1.5. Let R be a ring.

1. A ring R is said to be **left [resp. right] primitive** if there exists a simple faithful left [resp. right] R -module.
2. An ideal \mathfrak{a} of a ring R is said to be **left [resp. right] primitive** if the quotient ring R/\mathfrak{a} is a left [resp. right] primitive ring.

Remark. If M is a simple left R -module, then $R/\text{Ann}(M)$ is left primitive with faithful simple left $R/\text{Ann}(M)$ -module M .

Proposition 1.6. Let R be a ring.

1. A simple ring R is primitive.
2. A commutative ring R is primitive if and only if R is a field.

Proof. 1. Since R has an identity, R contains a maximal left ideal \mathfrak{m} by ??, whence R/\mathfrak{m} is a simple R -module. Since $\text{Ann}(R/\mathfrak{m})$ is an ideal of R that does not contain 1_R , $\text{Ann}(R/\mathfrak{m}) = 0$ by simplicity of R . Therefore R/\mathfrak{m} is a faithful R -module.

2. Conversely, let M be a faithful simple left R -module. Then $M \cong R/I$ for some maximal ideal I of R . Therefore, $0 = \text{Ann}(M) = \text{Ann}(R/I) \supset I$. Then $I = 0$ is a maximal ideal of R , thus R is a field. \square

§1.2 Jacobson Density Theorem

Definition 1.7. Let V be a vector space over a division ring D . A subring R of $\text{Hom}_D(V, V)$ is called a **dense ring of endomorphisms** of V if for every positive integer n , every linearly independent subset $\{u_1, \dots, u_n\}$ of V and every arbitrary subset $\{v_1, \dots, v_n\}$ of V , there exists $f \in R$ such that $f(u_i) = v_i$, ($i = 1, 2, \dots, n$).

Theorem 1.8. Let R be a dense ring of endomorphisms of a vector space V over a division ring D . Then R is Artinian if and only if $\dim_D V$ is finite, in which case $R = \text{Hom}_D(V, V) \cong M_n(D)$.

Proof. If R is Artinian and $\dim_D V$ is infinite, then there exists an infinite linearly independent subset $\{u_1, u_2, \dots\}$ of V . By V is a left $\text{Hom}_D(V, V)$ -module and hence a left R -module. For each n let $I_n = \text{Ann}\{u_1, \dots, u_n\}$. Then $I_1 \supset I_2 \supset \dots$ is a descending chain of left ideals of R and hence $I_1 \supsetneq I_2 \supsetneq \dots$ is a properly descending chain, which is a contradiction. Hence $\dim_D V$ is finite.

Conversely if $\dim_D V$ is finite, then V has a finite basis $\{v_1, \dots, v_m\}$. Then $R = \text{Hom}_D(V, V) \cong M_n(D)$ is Artinian. \square

Lemma 1.9. Let M be a simple module over a ring R . Consider M as a vector space over the division ring $D = \text{Hom}_R(M, M)$ by 1.4. If V is a finite dimensional D -subspace of M and $a \in M - V$, then there exists $r \in R$ such that $ra \neq 0$ and $rV = 0$.

Remark. In other words, the element $r \in \text{Ann}_R(V)$ only annihilates D -subspace V .

Proof. The proof is by induction on $n = \dim_D V$. If $n = 0$, then $V = 0$ and $a \neq 0$. Since M is simple, $M = Ra$. Consequently, there exists $r \in R$ such that $ra = a \neq 0$ and $rV = r0 = 0$.

Suppose now $\dim_D V = n > 0$ and the theorem is true for dimensions less than n . Let $\{u_1, \dots, u_{n-1}, u\}$ be a D -basis of V and let $W = \text{span}\{u_1, \dots, u_{n-1}\}$ ($W = 0$ if $n = 1$). Then $V = W \oplus Du$ (vector space direct sum, W may not be an R -submodule of M) the left annihilator $I = \text{Ann}_R(W)$ is a left ideal of R .

Consequently, Iu is an R -submodule of M . Since $u \in M - W$, the induction hypothesis implies that there exists $r \in R$ such that $ru \neq 0$ and $rW = 0$. Consequently $r \in I$ and $0 \neq ru \in Iu$, whence $Iu \neq 0$. Therefore $M = Iu$ by simplicity.

We must find $r \in R$ such that $ra \neq 0$ and $rV = 0$. If no such r exists, $\text{Ann}(a) \subset \text{Ann}(V)$, then we can define a map $\theta : M \rightarrow M$ as follows. For $ru \in Iu = M$ let $\theta(ru) = ra \in M$. We claim that θ is well defined. If $r_1u = r_2u$ ($r_i \in I$), then $(r_1 - r_2)u = 0$, whence $(r_1 - r_2)V = (r_1 - r_2)(W \oplus Du) = 0$. Consequently by hypothesis $(r_1 - r_2)a = 0$. Therefore, $\theta(r_1u) = r_1a = r_2a = \theta(r_2u)$. Verify that $\theta \in \text{Hom}_R(M, M) = D$. Then for every $r \in I$,

$$0 = \theta(ru) - ra = r\theta(u) - ra = r(\theta(u) - a)$$

Therefore $\theta(u) - a \in W$ by induction hypothesis. Consequently

$$a = \theta u - (\theta u - a) \in Du + W = V,$$

which contradicts the fact that $a \notin V$. Therefore, there exists $r \in R$ such that $ra \neq 0$ and $rV = 0$. \square

Theorem 1.10 (Classic Jacobson Density Theorem). *Let R be a primitive ring with a faithful simple R -module M and division ring $D = \text{End}_R(M)$. Then R is a dense ring of endomorphisms of the D -vector space M (viewed $\alpha : R \hookrightarrow \text{Hom}_R(M, M)$ by $r \mapsto \alpha_r$ where $\alpha_r : m \mapsto rm$ in M).*

Remark. If R is not primitive, then R is not a subring of $\text{Hom}_R(M, M)$. But $R/\text{Ann}(M)$ is primitive with faithful simple left $R/\text{Ann}(M)$ -module M with the action of \bar{r} on M which is same as that of r on M , so we also can say that R acts on simple M densely i.e. for every positive integer n , every linearly independent subset $\{u_1, \dots, u_n\}$ and every arbitrary subset $\{v_1, \dots, v_n\}$, there exists $r \in R$ such that $ru_i = v_i$, ($i = 1, 2, \dots, n$).

Proof. It clear that $\alpha : R \rightarrow \text{Hom}_D(M, M)$ is a ring monomorphism since M is faithful. Let $\{u_1, u_2, \dots, u_n\}$ be a D -linearly independent subset and $\{v_1, v_2, \dots, v_n\}$ be an arbitrary subset. For each i let

$$V_i = \text{span}\{u_1, \dots, u_{i-1}, u_{i+1}, \dots, u_n\}.$$

Since U is D -linearly independent, $u_i \notin V_i$. Consequently, by 1.9 there exists $r_i \in R$ such that

$$r_i u_i \neq 0 \text{ and } r_i V_i = 0$$

whence $Rr_i u_i = M$ by simplicity. Therefore exists $t_i \in R$ such that $t_i r_i u_i = v_i$. Let

$$r = t_1 r_1 + t_2 r_2 + \cdots + t_n r_n \in R.$$

Consequently for each $i = 1, 2, \dots, n$

$$\alpha_r(u_i) = (t_1 r_1 + \cdots + t_n r_n) u_i = v_i$$

Therefore $\text{Im } \alpha$ is a dense ring of endomorphisms of the D -vector space M . □

§2 Simple ring

Corollary 2.1. *If R is a nonzero simple ring, then*

$$R \cong \alpha(R) \subseteq \text{End}_D(V)$$

for some faithful simple R -module V and division ring $D = \text{End}_R(V)$.

Corollary 2.2. *If R is a primitive ring, then for some division ring D either R is isomorphic to the endomorphism ring of a finite dimensional vector space over D or for every positive integer m there is a subring R_m of R and an epimorphism of rings $R_m \rightarrow \text{Hom}_D(V_m, V_m)$, where V_m is an m -dimensional vector space over D .*

Proof. In the notation of 1.10,

$$\alpha : R \rightarrow \text{Hom}_D(M, M)$$

is a monomorphism such that $R \cong \text{Im } \alpha$ and $\text{Im } \alpha$ is dense in $\text{Hom}_D(M, M)$. If $\dim_D M = n$ is finite, then $R \cong \text{Im } \alpha = \text{Hom}_D(M, M)$ by 1.8. If $\dim_D A$ is infinite and $\{u_1, u_2, \dots\}$ is an infinite linearly independent set, let V_m be the m -dimensional D -subspace of A spanned by $\{u_1, \dots, u_m\}$. Verify that $R_m = \{r \in R \mid rV_m \subset V_m\}$ is a subring of R . Use the density of $R \cong \text{Im } \alpha$ in $\text{Hom}_D(M, M)$ to show that the map $R_m \rightarrow \text{Hom}_D(V_m, V_m)$ given by $r \mapsto \alpha_r|_{V_m}$ is a well-defined ring epimorphism. □

Theorem 2.3 (Wedderburn-Artin). *The following conditions on a ring R are equivalent.*

1. R is simple Artinian.
2. R is primitive Artinian.
3. R is isomorphic to $M_n(D)$ for some positive integer n and some division ring D .

In this case, D is isomorphic to $\text{Hom}_R(M, M)$ for any simple left R -module M and $n = \dim_D M$.

Proof. (1) \Rightarrow (2) This is clear since a simple ring is primitive.

(2) \Rightarrow (3) Let M be a faithful simple left R -module. By [theorem 1.10](#), R is isomorphic to a dense ring of endomorphisms of the D -vector space M , where $D = \text{Hom}_R(M, M)$. Since R is left Artinian, $\dim_D M$ is finite by [theorem 1.8](#). Therefore $R \cong \text{Hom}_D(M, M) \cong M_n(D)$, where $n = \dim_D M$.

(3) \Rightarrow (1) Since $M_n(D)$ is left Artinian, it suffices to show that $M_n(D)$ is simple. Let \mathfrak{a} be a nonzero two-sided ideal of $M_n(D)$ and let $0 \neq A = (a_{ij}) \in \mathfrak{a}$. Then there exist indices p, q such that $a_{pq} \neq 0$. For any indices i, j , let E_{ij} be the matrix unit whose (i, j) -entry is 1 and all other entries are 0. Then

$$E_{ip}AE_{qj} = a_{pq}E_{ij} \in \mathfrak{a}$$

□

Lemma 2.4. *Let V be a nonzero vector space over a division ring D . If $g : V \rightarrow V$ is a homomorphism of additive groups such that $gf = fg$ for all $f \in \text{Hom}_D(V, V)$, then there exists $\lambda \in D$ such that $g(x) = \lambda x$ for all $x \in V$.*

Lemma 2.5. *Let V be a finite dimensional vector space over a division ring D . If M and N are simple faithful modules over $R = \text{Hom}_D(V, V)$, then M and N are isomorphic R -modules.*

Proof. Since M and N are simple and faithful, we have $\text{Ann}(M) = 0$ and $\text{Ann}(N) = 0$. By [lemma 1.4](#), we have $\text{Hom}_R(M, N) \cong \text{Hom}_D(V, V)$, which is a division ring. Thus M and N are isomorphic as R -modules. □

Proposition 2.6. *For $i = 1, 2$ let V_i be a vector space of finite dimension n_i over the division ring D_i .*

1. *If there is an isomorphism of rings $\text{Hom}_{D_1}(V_1, V_1) \cong \text{Hom}_{D_2}(V_2, V_2)$, then $\dim_{D_1} V_1 = \dim_{D_2} V_2$ and D_1 is isomorphic to D_2 .*
2. *If there is an isomorphism of rings $M_{n_1}(D_1) \cong M_{n_2}(D_2)$, then $n_1 = n_2$ and D_1 is isomorphic to D_2 .*

Chapter IX

Semisimplicity

§1 Definitions

Theorem 1.1. *Let R be a ring and M a left R -module. The following conditions on M are equivalent:*

1. M is the sum of a family of simple submodules.
2. M is the direct sum of a family of simple submodules.
3. Every submodule N is a direct summand of M .

Proof. (1) \Rightarrow (2) Let \mathcal{S} be the set of all families \mathcal{F} of simple submodules of M such that the sum of the members of \mathcal{F} is direct. Since M is the sum of a family of simple submodules, \mathcal{S} is nonempty. Partially order \mathcal{S} by inclusion and let \mathcal{C} be a chain in \mathcal{S} . Then $\mathcal{U} = \bigcup_{\mathcal{F} \in \mathcal{C}} \mathcal{F}$ is an upper bound for \mathcal{C} in \mathcal{S} . By Zorn's lemma there exists a maximal element \mathcal{F}_0 in \mathcal{S} . We claim that $M = \bigoplus_{N \in \mathcal{F}_0} N$. If not, there exists a simple submodule K of M such that

$$K \cap \left(\bigoplus_{N \in \mathcal{F}_0} N \right) = 0.$$

Consequently, $\mathcal{F}_0 \cup \{K\} \in \mathcal{S}$, contradicting the maximality of \mathcal{F}_0 .

(2) \Rightarrow (3) Let $M = \bigoplus_{i \in I} N_i$, where each N_i is a simple submodule of M , and let N be a submodule of M . For each $i \in I$, either $N_i \subset N$ or $N_i \cap N = 0$ by simplicity. Let $J = \{i \in I \mid N_i \subset N\}$ and $K = I - J$. Then

$$M = N \oplus \left(\bigoplus_{i \in K} N_i \right).$$

(3) \Rightarrow (1) Let N be the sum of all simple submodules of M . By hypothesis, $M = N \oplus P$ for some submodule P . □

Remark. A left R -module M satisfying the three conditions is said to be **semisimple**. Similarly one defines a right semisimple module.

Proposition 1.2. *Every submodule and every factor module of a left semisimple module is left semisimple.*

§2 Structure of semisimple rings

Definition 2.1. *A ring R is called **semisimple** if $1 \neq 0$, and if R is semisimple as a left R -module.*

Proposition 2.2. *If R is a semisimple ring, then R is Artinian.*

Proof. Since ${}_R R$ is semisimple module, there exist simple left ideals L_j of R such that

$${}_R R \cong \bigoplus_{j \in J} L_j$$

with projection maps $\pi_j : R \rightarrow L_j$ for each $j \in J$. Since the sum is direct, $\{j_k : \pi_{j_k}(1_R) \neq 0\}$ is finite. Then $J = \{j_k : \pi_{j_k}(1_R) \neq 0\}$ is finite and

$${}_R R \cong L_1 \oplus L_2 \oplus \cdots \oplus L_n$$

Therefore ring R is Artinian. □

Remark. *It is clear that any simple ideal L of R is isomorphic to some L_j , thus R has finitely many minimal left ideals up to isomorphism.*

Lemma 2.3. *If L and L' are minimal left ideals in a ring R , then each of the following statements implies the one below it:*

1. $LL' \neq (0)$.
2. $\text{Hom}_R(L, L') \neq \{0\}$ and there exists $b' \in L'$ with $L' = Lb'$.
3. $L \cong L'$ as left R -modules.

If also $L^2 \neq (0)$, then (iii) implies (i) and the three statements are equivalent.

Theorem 2.4 (Wedderburn-Artin). *If R is a semisimple ring, then we have ring isomorphisms*

$$R \cong \prod_{i=1}^t R_i \cong \prod_{i=1}^t M_{n_i}(D_i)$$

where $R_i \cong M_{n_i}(D_i)$ is a simple ring for each $i \in I$.

Proof. Let $\{L_{j_i}\}_{i=1}^t$ be all distinct simple left ideals of R up to isomorphism and define R_i be the sum

$${}_R R_i := \bigoplus_{L_j \cong L_i} L_j$$

Thus, as left R -modules,

$${}_R R \cong \bigoplus_{i=1}^t {}_R R_i.$$

Then R_i is a two-sided ideal of R by [lemma 2.3](#) and hence a ring with identity element $e_i = \pi_i(1_R)$ (π_i the projection from R to R_i). The projection from R to R_i induce a ring homomorphism

$$R \cong \prod_{i=1}^t R_i$$

It remains to show that each R_i is simple. Let I be a nonzero two-sided ideal of R_i , then I is a left ideal of R . Since R is semisimple, there exists a left ideal J of R such that

$$R = I \oplus J$$

Then

$$R_i = e_i R = e_i I + e_i J \subset I$$

Thus R_i is simple. □

§3 Structure of modules over semisimple rings

§3.1 Modules over $M_n(D)$

Proposition 3.1. *Let $R = M_n(D)$ for some division ring D and positive integer n .*

1. *If S is a left R -module, then*

$${}_R S \cong {}_R D^n$$

2. *every left R -module is isomorphic to $({}_R D^n)^{(I)}$ for some index set I .*

Corollary 3.2. *There is, up to isomorphism, only one simple left module over a Artinian simple ring R ; namely, the left R -module Re , where e is any primitive idempotent of R .*

§3.2 Modules over semisimple rings

Theorem 3.3. *Let semisimple ring*

$$R \cong \prod_{i=1}^t R_i$$

where each $R_i \cong M_{n_i}(D_i)$. Then every left R -module M is isomorphic to

$$\bigoplus_{i=1}^t e_i M \cong \bigoplus_{i=1}^t S_i^{(\kappa_i)}$$

where $e_i M \cong S_i$ is the unique simple left R_i -module and κ_i is a cardinal number. And the decomposition is unique in the sense that if

$$M \cong \bigoplus_{i=1}^t S_i^{(\kappa_i)} \cong \bigoplus_{i=1}^t S_i^{(\kappa'_i)}$$

then $\kappa_i = \kappa'_i$ for each i

Remark. If M is finitely generated, then each κ_i is finite.

§4 Jacobson Radical

Definition 4.1. Let R be a ring. A element $x \in R$ is said to be **right quasi-regular** if there exists $y \in R$ such that $x + y - xy = 0$, y is called a **right quasi-inverse** of x .

Remark. That is, $1 - x$ has a right inverse $1 - y$.

Definition 4.2. A element $a \in R$ is said **right quasi-nilpotent element** if for every $r \in R$, ra is right quasi-regular.

Remark. That is, $1 - ra$ has a right inverse for every $r \in R$.

§4.1 Jacobson radical

Theorem 4.3. Let R be a ring, then the following sets are equal:

1. the intersection of all maximal left ideals of R
- 1' the intersection of all maximal right ideals of R
2. the intersection of all the annihilators of simple left R -modules;
- 2' the intersection of all the annihilators of simple right R -modules;
3. $\{x \in R : x \text{ is right quasi-nilpotent element}\}$
- 3' $\{x \in R : x \text{ is left quasi-nilpotent element}\}$
4. Nakayama's $\{x \in R : \text{for any finitely generated module } M, xM = M \Rightarrow M = 0\}$
5. the ideal J such that R/J is semisimple.

the two-sided ideal is called the **Jacobson radical** of R and is denoted by $J(R)$.

Corollary 4.4. 1. $J(\prod_{i \in I} R_i) = \prod_{i \in I} J(R_i)$.

2. $J(J(R)) = J(R)$.

3. $R/J(R)$ is semisimple.

Proposition 4.5. *If R is an Artinian ring, then the radical $J(R)$ is a nilpotent ideal. Thus $J(R) = \text{Rad}(R)$*

Proof. Since R is Artinian, the descending chain of ideals

$$J(R) \supseteq J(R)^2 \supseteq J(R)^3 \supseteq \cdots$$

stabilizes, say $J(R)^n = J(R)^{n+1}$ for some positive integer n . On the other hand, ${}_R R$ is Noetherian thus $J(R)^n$ is finitely generated submodule of ${}_R R$ and $J(R)^n = 0$ by Nakayama's lemma. \square

Proposition 4.6. *Let R be a ring. $J(M_n R) = M_n(J(R))$.*

Proof. (a) If A is a left R -module, consider the elements of $A^n = A \oplus A \oplus \cdots \oplus A$ (n summands) as column vectors; then A^n is a left $(\text{Mat}_n R)$ -module (under ordinary matrix multiplication).

(b) If A is a simple R -module, A^n is a simple $(\text{Mat}_n R)$ -module.

(c) $J(\text{Mat}_n R) \subset \text{Mat}_n J(R)$.

(d) $\text{Mat}_n J(R) \subset J(\text{Mat}_n R)$. [Hint: prove that $\text{Mat}_n J(R)$ is a left quasi-regular ideal of $\text{Mat}_n R$ as follows. For each $k = 1, 2, \dots, n$ let K_k consist of all matrices (a_{ij}) such that $a_{ij} \in J(R)$ and $a_{ij} = 0$ if $j \neq k$. Show that K_k is a left quasi-regular left ideal of $\text{Mat}_n R$ and observe that $K_1 + K_2 + \cdots + K_n = \text{Mat}_n J(R)$.] \square

Corollary 4.7. *Let R be a ring. If matrix $A \in M_n(J(R))$, then $I - A$ is invertible in $M_n(R)$.*

§4.2 Nakayama's Lemma

Theorem 4.8 (Nakayama's lemma). *Let M be a finitely generated left R -module and a subset $X \subset J(R)$. Then $\mathfrak{a}M = M$ implies $M = 0$.*

Corollary 4.9. *Let M be a finitely generated left R -module, N a submodule of M , left ideal $\mathfrak{a} \subset J(R)$. Then $M = \mathfrak{a}M + N \Rightarrow M = N$.*

Corollary 4.10. *If R is a Noetherian local ring with maximal ideal \mathfrak{m} , then $\bigcap_{n=1}^{\infty} \mathfrak{m}^n = 0$.*

Proposition 4.11. *If R is a local ring, then every finitely generated projective R -module is free.*

Proof. If P is a finitely generated projective R -module, then by ?? there exists a free R -module F with a finite basis and an epimorphism $\pi : F \rightarrow P$. Among all the free R -modules F with this property choose one with a basis $\{x_1, x_2, \dots, x_n\}$ that has a minimal number of elements. Since π is an epimorphism $\{\pi(x_1), \dots, \pi(x_n)\}$ necessarily generate P .

We shall first show that $K = \text{Ker } \pi$ is contained in $\mathfrak{m}F$, where \mathfrak{m} is the unique maximal ideal of R .

If $K \not\subset \mathfrak{m}F$, then there exists $k \in K$ with $k \notin \mathfrak{m}F$. Now $k = r_1 x_1 + r_2 x_2 + \cdots + r_n x_n$ with $r_i \in R$ uniquely determined. Since $k \notin \mathfrak{m}F$, some r_i , say r_1 , is not an element of \mathfrak{m} , thus r_1 is a unit, whence $x_1 - r_1^{-1} k = -r_1^{-1} r_2 x_2 - \cdots - r_1^{-1} r_n x_n$.

Consequently, since $k \in \text{Ker } \pi$, $\pi(x_1) = \pi(x_1 - r_1^{-1}k) = \sum_{i=2}^n -r_1 r_i \pi(x_i)$. Therefore, $\{\pi(x_2), \dots, \pi(x_n)\}$ generates P . Thus if F' is the free submodule of F with basis $\{x_2, \dots, x_n\}$ and $\pi' : F' \rightarrow P$ the restriction of π to F' , then π' is an epimorphism. This contradicts the choice of F as having a basis of minimal cardinality. Hence $K \subset \mathfrak{m}F$.

Since $0 \rightarrow K \xrightarrow{\subset} F \xrightarrow{\pi} P \rightarrow 0$ is exact and P is projective $K \oplus P \cong F$ by ???. Under this isomorphism $(k, 0) \mapsto k$ for all $k \in K$ (see the proof of Theorem IV.1.18), whence F is the internal direct sum $F = K \oplus P'$ with $P' \cong P$. Thus $F = K + P' \subset \mathfrak{m}F + P'$. If $u \in F$, then $u = \sum_i m_i v_i + p_i$ with $m_i \in \mathfrak{m}$, $v_i \in F$, $p_i \in P'$. Consequently, in the R -module F/P' ,

$$u + P' = \sum_i m_i v_i + P' = \sum_i m_i (v_i + P') \in \mathfrak{m}(F/P')$$

whence $\mathfrak{m}(F/P') = F/P'$. Since F is finitely generated, so is F/P' . Therefore $K \cong F/P' = 0$ by ???. Thus $P \cong P' = F$ and P is free. \square

§5 Characterizations of semisimple rings

Theorem 5.1. *The following conditions on a ring R are equivalent:*

1. R is a semisimple ring.
2. Every left R -module is a semisimple module.
3. Every left R -module is injective.
4. Every left R -module is projective.
5. Every short exact sequence of left R -modules splits.
6. R is Artinian and $J(R) = 0$.

§6 Algebra

Definition 6.1. *Let A be an algebra over a commutative ring K with identity.*

1. A **left algebra A -module** is a left K -module M such that M is a left module over the ring A and $k(am) = (ka)m = a(km)$ for all $k \in K$, $a \in A$, $m \in M$. *Indeed,*

$$\begin{cases} (k_1 a_1 + k_2 a_2)(m_1 + m_2) = k_1 a_1 m_1 + k_1 a_1 m_2 + k_2 a_2 m_1 + k_2 a_2 m_2 \\ k(am) = (ka)m = a(km) \\ 1_K m = m, 1_K a = a \end{cases}$$

for all $k \in K$, $a \in A$, $m \in M$

2. A left algebra A -submodule of M is a subset of M which is itself an left algebra A -module.

3. A left algebra A -module M is **simple** (or **irreducible**) if M has no proper A -submodules.
4. A homomorphism $f : M \rightarrow N$ of algebra A -modules is a map that is both a K -module and an A -module homomorphism.

Remark.

Theorem 6.2. *Let A be a K -algebra. The Jacobson radical of the ring A coincides with the Jacobson radical of the algebra A . In particular A is a semisimple ring if and only if A is a semisimple algebra.*

Theorem 6.3. *Let A be a K -algebra.*

- (1) *Every simple algebra A -module is a simple module over the ring A .*
- (2) *Every simple module M over the ring A can be given a unique K -module structure in such a way that M is a simple algebra A -module.*