A COURSE IN COMMUTATIVE ALGEBRA

Ali Reza Naghipour

Department of Mathematics
Shahrekord University
P.O. Box: 115, Shahrekord, IRAN.

[0] Please send all comments and corrections to naghipourar@yahoo.com

Contents

Chapter 1

Primary Decomposition

1.1 Ring Theory Background

In this talks, by a ring we always understand a commutative ring with unit; ring homomorphisms $\varphi : R \longrightarrow S$ are assumed to take the unit element of R into the unit element of S. When we say that R is a subring of S it is understood that the unit element of R and S coincide.

Recall. Let I, J be ideals of a ring R, and let $\{I_\alpha\}_{\alpha\in\Lambda}$ be a family of ideals of R. Then

(1) $I + J := \{a + b | a \in I, b \in J\}$,

(2) $\sum_{\alpha\in\Lambda} I_\alpha := \{\sum_{\alpha\in\Lambda'} x_\alpha | \Lambda'$ is a finite subset of $\Lambda\}$,

(3) $IJ := \{a_1b_1 + a_2b_2 + \ldots + a_nb_n | a_i \in I, b_i \in J\}$,

(4) Spec(R):= the set of all prime ideals of R,

(5) $V(I) := \{\mathfrak{p} \in \text{Spec}(R) | I \subseteq \mathfrak{p}\}$,

(6) $\text{Min}(I) := \text{Min}V(I) = \text{Min}\{\mathfrak{p} \in \text{Spec}(R) | I \subseteq \mathfrak{p}\}$,

(7) $\text{Min}(R) := \text{Min}(0) = \text{Min}(\text{Spec}(R))$,

(8) Max(R):= the set of all maximal ideals of R= Max(Spec(R)),

(9) $\sqrt{I} := \{a \in R | a^n \in I$ for some $n \in \mathbb{N}\} = \bigcap_{\mathfrak{p}\in V(I)} \mathfrak{p} = \bigcap_{\mathfrak{p}\in \text{Min}(I)} \mathfrak{p}$,

(10) $(I :_R J) = (I : J) =: \{a \in R | aJ \subseteq I\}$.

Definition 1.1.1. (Extension and Contraction). Let $f : R \longrightarrow S$ be a ring homomorphism. If I is an ideal in R, the set $f(I)$ is not necessarily an ideal of S. The **extension** I^e (or IS) of I is the ideal

$$I^e = IS := < f(I) > = < f(x) | x \in I > .$$

If J is an ideal in S, then $f^{-1}(J)$ is always an ideal of R. The **contraction** J^c of J is the ideal

$$J^c = f^{-1}(J) = \{x \in R | f(x) \in J\}.$$

Exercise 1. Let I, J, K be ideals of a ring R, and let $\{I_\alpha\}_{\alpha\in\Lambda}$ be a family of ideals of R. Show that:
(1) $(I : J)$ is an ideal of R,
(2) $I \subseteq (I : J)$,
(3) $((I : J) : K) = (I : JK) = ((I : K) : J)$,
(4) $(\bigcap_\alpha I_\alpha : J) = \bigcap_\alpha (I_\alpha : J)$,
(5) $(J : \sum_{\alpha\in\Lambda} I_\alpha) = \bigcap_\alpha (J : I_\alpha)$.

Exercise 2. Let $f : R \longrightarrow S$ be a ring homomorphism and I, I_1, I_2 are ideals of R and J, J_1, J_2 are ideals of S. Show that:
(1) $I \subseteq I^{ec}$ and $J^{ce} \subseteq J$,
(2) $I^{ece} = I^e$ and $J^{cec} = J^c$,
(3) $(I_1 + I_2)^e = I_1^e + I_2^e$ and $(J_1 + J_2)^c \supseteq J_1^c + J_2^c$,
(4) $(I_1 \cap I_2)^e \subseteq I_1^e \cap I_2^e$ and $(J_1 \cap J_2)^c = J_1^c \cap J_2^c$,
(5) $(I_1 I_2)^e = I_1^e I_2^e$ and $(J_1 J_2)^c \supseteq J_1^c J_2^c$,
(6) $(I_1 : I_2)^e \subseteq (I_1^e : I_2^e)$ and $(J_1 : J_2)^c \subseteq (J_1^c : J_2^c)$,

Exercise 3. Let $f : R \longrightarrow S$ be a homomorphism and I, I_1, I_2 are ideals of R and J is an ideal of S. Show that:
(1) $I \subseteq \sqrt{I}$,
(2) $\sqrt{\sqrt{I}} = \sqrt{I}$,
(3) $\sqrt{I_1 I_2} = \sqrt{I_1 \cap I_2} = \sqrt{I_1} \cap \sqrt{I_2}$,

(4) $\sqrt{I_1 + I_2} = \sqrt{\sqrt{I_1} + \sqrt{I_2}}$,

(5) $\sqrt{I} = R \Longleftrightarrow I = R$,

(6) $\sqrt{I_1} + \sqrt{I_2} = R \Longrightarrow I_1 + I_2 = R$,

(7) $\sqrt{I^n} = \sqrt{I}$, for all $n \in \mathbb{N}$,

(8) if $\sqrt{I}$ is finitely generated, then there exists $n \in \mathbb{N}$ such that $(\sqrt{I})^n \subseteq I$,

(9) if $\mathfrak{p}$ is a prime ideal of R, $\sqrt{\mathfrak{p}^n} = \mathfrak{p}$, for all $n \in \mathbb{N}$,

(10) $(\sqrt{I})^e \subseteq \sqrt{I^e}$ and $(\sqrt{J})^c = \sqrt{J^c}$.

Theorem 1.1.2. *Let I be an ideal of a ring R. Then the following are equivalent:*

(1) The set $\mathrm{Min}(I)$ *is finite,*

(2) For any $\mathfrak{p} \in \mathrm{Min}(I)$ *there exists a finitely generated ideal* $\mathfrak{p}^*/I$ *of* R/I *such that* $\mathfrak{p}^* \subseteq \mathfrak{p}$ *and* $\mathrm{Min}(\mathfrak{p}^*)$ *is finite.*

Proof. Without loss of generality we may assume that $I = 0$.

(1) $\Longrightarrow$(2): Let $\mathfrak{p}^* = 0$.

(2) $\Longrightarrow$(1): Let S denote the collection of finitely generated ideals I of R such that $\mathrm{Min}(I)$ is finite. Set

$$T = \{J | J \text{ is an ideal of } R \text{ such that } I \not\subseteq J \text{ for any } I \in S\}.$$

If $0 \notin T$, then $0 \in S$ and hence $\mathrm{Min}(R)$ is finite. Thus we may assume that $0 \in T$. Since the collection T is nonempty and elements of S is finitely generated, T is inductive and hence by Zorn's Lemma has a maximal element $\mathfrak{q}$. We show that $\mathfrak{q}$ is a prime ideal of R. If $\mathfrak{q}$ is not prime then there exist $a, b \in R\backslash\mathfrak{q}$ such that $ab \in \mathfrak{q}$. Therefore there exist $I_1, I_2 \in S$ such that $I_1 \subseteq \mathfrak{q} + Ra$ and $I_2 \subseteq \mathfrak{q} + Rb$. So, we have

$$I_1 I_2 \subseteq (\mathfrak{q} + Ra)(\mathfrak{q} + Rb) \subseteq \mathfrak{q}^2 + \mathfrak{q}Rb + \mathfrak{q}Ra + Rab \subseteq \mathfrak{q}.$$

On the other hand, $\mathrm{Min}(I_1 I_2) \subseteq \mathrm{Min}(I_1) \cup \mathrm{Min}(I_2)$. Therefore $I_1 I_2 \in S$, which is a contradiction. Thus $\mathfrak{q}$ is a prime ideal of R. Let $\mathfrak{p}$ be a minimal prime ideal of R such that $\mathfrak{p} \subseteq \mathfrak{q}$. There exists $\mathfrak{p}^* \in S$ such that $\mathfrak{p}^* \subseteq \mathfrak{p}$. Thus $\mathfrak{q} \notin T$ and this is also a contradiction. □

The following result is the main result of [1].

Theorem 1.1.3. (Anderson's Theorem). *Let I be an ideal of a ring R. If each $\mathfrak{p} \in \mathrm{Min}(I)$ is finitely generated ideal, then $\mathrm{Min}(I)$ is finite.*

Proof. This follows immediately from the above theorem. □

Theorem 1.1.4. *Let R be a ring. Then the following are equivalent:*
(1) R is Artinian.
(2) R is Noetherian and $\mathrm{Spec}(R) = \mathrm{Max}(R)$.

Proof. See Chapter 2 of [10] or Corollary 8.45 of [12]. □

1.2 Primary Ideals

Definition 1.2.1. A proper ideal $\mathfrak{q}$ of a ring R is said to be a **primary** ideal if, for $a, b \in R$, we have

$$ab \in \mathfrak{q} \Longrightarrow a \in \mathfrak{q} \,\text{or}\, b \in \sqrt{\mathfrak{q}}.$$

Lemma and Definition. Let $\mathfrak{q}$ be a primary ideal of R. Then $\mathfrak{p} := \sqrt{\mathfrak{q}}$ is a prime ideal of R, and we say that $\mathfrak{q}$ is $\mathfrak{p}-$primary.

Proof. Let $ab \in \sqrt{\mathfrak{q}}$. Then there is an element $n \in \mathbb{N}$ such that $a^n b^n = (ab)^n \in \mathfrak{q}$. Since $\mathfrak{q}$ is primary, we have that $a^n \in \mathfrak{q}$ or $b^n \in \sqrt{\mathfrak{q}}$. It follows that $a \in \sqrt{\mathfrak{q}}$ or $b \in \sqrt{\sqrt{\mathfrak{q}}} = \sqrt{\mathfrak{q}}$. Therefore, $\sqrt{\mathfrak{q}}$ is a prime ideal and the proof is complete. □

Theorem 1.2.2. *Let $\mathfrak{q}_1, \mathfrak{q}_2, \ldots, \mathfrak{q}_n$ be $\mathfrak{p}-$primary ideals of R. Then $\bigcap_{i=1}^n \mathfrak{q}_i$ is also a $\mathfrak{p}-$primary ideal of R.*

Proof. By Exercise 3(3), we have $\sqrt{\bigcap_{i=1}^n \mathfrak{q}_i} = \bigcap_{i=1}^n \sqrt{\mathfrak{q}_i} = \mathfrak{p}$. Now let $ab \in \bigcap_{i=1}^n \mathfrak{q}_i$ and $a \notin \bigcap_{i=1}^n \mathfrak{q}_i$. Then there exists $1 \leq j \leq n$ such that $a \notin \mathfrak{q}_j$. Since $ab \in \mathfrak{q}_j$ and $\mathfrak{q}_j$ is $\mathfrak{p}-$primary, we have $b \in \sqrt{\mathfrak{q}_j} = \mathfrak{p}$. This proves the theorem. □

Theorem 1.2.3. *Let $\mathfrak{q}$ be an ideal of a ring R, and $\sqrt{\mathfrak{q}} = \mathfrak{m} \in \mathrm{Max}R$. Then $\mathfrak{q}$ is $\mathfrak{m}-$primary.*

Proof. $\mathfrak{q}$ is a proper ideal, since $\mathfrak{q} \subseteq \sqrt{\mathfrak{q}} = \mathfrak{m} \subsetneq R$. Now, let $ab \in \mathfrak{q}$ and $b \notin \sqrt{\mathfrak{q}} = \mathfrak{m}$. Then $bR + \sqrt{\mathfrak{q}} = R$ and so $\sqrt{bR} + \sqrt{\mathfrak{q}} = R$. From the Exercise 3(6), we have $bR + \mathfrak{q} = R$. It follows that $br + q = 1$ for some $r \in R$ and $q \in \mathfrak{q}$. Therefore $a = abr + aq \in \mathfrak{q}$. This proves the theorem. □

Notation. Let I be an ideal of R and $x \in R$. Then $(I : Rx)$ may be denoted simply by $(I : x)$.

Theorem 1.2.4. *Let $\mathfrak{q}$ be a $\mathfrak{p}-$primary ideal of R. Then*
(1) if $x \in \mathfrak{q}$, then $(\mathfrak{q} : x) = R$,
(2) if $x \notin \mathfrak{q}$, then $(\mathfrak{q} : x)$ is $\mathfrak{p}-$primary,
(3) if $x \notin \mathfrak{p}$, then $(\mathfrak{q} : x) = \mathfrak{q}$.

Proof. (1): Trivial.
(2): First we show that $\sqrt{(\mathfrak{q} : x)} = \mathfrak{p}$. We have

$$\mathfrak{q} \subseteq (\mathfrak{q} : x) \subseteq \sqrt{\mathfrak{q}} \Longrightarrow \sqrt{\mathfrak{q}} \subseteq \sqrt{(\mathfrak{q} : x)} \subseteq \sqrt{\mathfrak{q}} \Longrightarrow \sqrt{(\mathfrak{q} : x)} = \sqrt{\mathfrak{q}} = \mathfrak{p}.$$

Now let $ab \in (\mathfrak{q} : x)$ and $a \notin (\mathfrak{q} : x)$. Then $abx \in \mathfrak{q}$ and $ax \notin \mathfrak{q}$. By definition we have $b \in \sqrt{\mathfrak{q}} = \mathfrak{p} = \sqrt{(\mathfrak{q} : x)}$ and so $(\mathfrak{q} : x)$ is $\mathfrak{p}-$primary.

(3): Clearly $(\mathfrak{q} : x) \subseteq \mathfrak{q}$. Now let $a \in (\mathfrak{q} : x)$, then $ax \in \mathfrak{q}$ and hence $a \in \mathfrak{q}$, by definition. □

Theorem 1.2.5. *Let $\varphi : R \longrightarrow S$ be a ring homomorphism, let $\mathfrak{q}$ be a $\mathfrak{p}-$primary ideal of S. Then $\mathfrak{q}^c$ is $\mathfrak{p}^c-$primary ideal of R.*

Proof. $\mathfrak{q}^c$ is proper, since

$$\mathfrak{q} \neq S \Longrightarrow 1_S = \varphi(1_R) \notin \mathfrak{q} \Longrightarrow 1_R \notin \mathfrak{q}^c \Longrightarrow \mathfrak{q}^c \neq R.$$

Now let $ab \in \mathfrak{q}^c$ and $a \notin \mathfrak{q}^c$. Then $\varphi(a)\varphi(b) \in \mathfrak{q}$ and $\varphi(a) \notin \mathfrak{q}$. Therefore $\varphi(b) \in \sqrt{\mathfrak{q}}$ and so $b \in \sqrt{\mathfrak{q}}^c$. Hence the assertion follows from the fact that $\sqrt{\mathfrak{q}^c} = \sqrt{\mathfrak{q}}^c = \mathfrak{p}^c$. □

Exercise 4. Let $\varphi : R \longrightarrow S$ be an epimorphism and let $\mathfrak{q}$ be a $\mathfrak{p}-$primary ideal of R such that $\ker\varphi \subseteq \mathfrak{q}$. Show that $\mathfrak{q}^e$ is $\mathfrak{p}^e-$primary ideal of S.

1.3 Associated prime ideals

Definition 1.3.1. Let N, K be two submodules of an R-module M. We denote the ideal

$$\{a \in R | aK \subseteq N\}$$

by $(N : K)$ (or $(N :_R K)$ if it is desired to emphasize the underlying ring concerned). In special case in which $N = 0$, the ideal $(0 :_R K)$ is called the annihilator of K and denoted by $\mathrm{Ann}_R K$ or $\mathrm{Ann} K$.

If $x \in M$, then $\mathrm{Ann}_R(Rx)$ may be denoted simply by $\mathrm{Ann}_R x$ or $\mathrm{Ann} x$.

Exercise 5. Let N be a submodule of an R-module M, and let $\{N_\alpha\}_{\in\alpha}$ be a family of submodules of M. Show that:
(1) $(\bigcap_\alpha N_\alpha : N) = \bigcap_\alpha (N_\alpha : N)$,
(2) $(N : \sum_{\alpha\in\Lambda} N_\alpha) = \bigcap_\alpha (N : N_\alpha)$.

Definition 1.3.2. Let M be an R-module. Then the set of associated prime ideals of M is defined as follows:

$$\mathrm{Ass}_R M = \mathrm{Ass} M := \{\mathfrak{p} \in \mathrm{Spec} R | \exists 0 \neq x \in M : \mathfrak{p} = \mathrm{Ann} x\}.$$

It is clear that if M and M' are isomorphic R-modules, then $\mathrm{Ass} M = \mathrm{Ass} M'$.

Theorem 1.3.3. *Let M be a module over a Noetherian ring R. Then*

$$M \neq (0) \Longleftrightarrow \mathrm{Ass} M \neq \emptyset.$$

Proof. $(\Longleftarrow)$: Trivial.
$(\Longrightarrow)$: Set

$$\Sigma = \{\mathrm{Ann} x | 0 \neq x \in M\}.$$

Let $\mathrm{Ann} x_0$ be a maximal element of Σ. It is enough to show that $\mathrm{Ann} x_0$ is a prime ideal of R. Let $ab \in \mathrm{Ann} x_0$ and $a \notin \mathrm{Ann} x_0$. Since $\mathrm{Ann} x_0 \subseteq \mathrm{Ann} a x_0$, by the maximality of $\mathrm{Ann} x_0$, we have $\mathrm{Ann} x_0 = \mathrm{Ann} a x_0$. Thus $b \in \mathrm{Ann} x_0$. This proves the theorem. □

Proposition 1.3.4. *Let N be a submodule of an R-module M. Then:*

(1) $\mathrm{Ass}N \subseteq \mathrm{Ass}M$*,*

(2) If $M \cong R/\mathfrak{p}$ *for some* $\mathfrak{p} \in \mathrm{Spec}(R)$*, then* $\mathrm{Ass}M = \{\mathfrak{p}\}$ *(in fact,* $\mathfrak{p} = \mathrm{Ann}_R x$ *for any* $0 \neq x \in M$*),*

(3) $\mathfrak{p} \in \mathrm{Ass}M \Longleftrightarrow \exists M_1 \leq M$ *such that* $M_1 \cong R/\mathfrak{p}$*.*

Proof. (1): Trivial.

(2): Let $\varphi : M \longrightarrow R/\mathfrak{p}$ be an isomorphism. If $0 \neq x \in M$, then $0 \neq \varphi(x) \in R/\mathfrak{p}$ and hence $\mathrm{Ann}_R x = \mathrm{Ann}_R \varphi(x) = \mathfrak{p}$.

(3)($\Rightarrow$): Let $\mathfrak{p} \in \mathrm{Ass}M$. Then there exits $x \in M$ such that $\mathfrak{p} = \mathrm{Ann}x$. Define

$$\begin{aligned} \varphi : R &\longrightarrow Rx \\ r &\longmapsto rx. \end{aligned}$$

Then φ is an epimorphism and $\mathrm{Ker}\varphi = \mathrm{Ann}x = \mathfrak{p}$. Therefore $Rx \cong R/\mathfrak{p}$. Now the assertion follows if we take $M_1 := Rx$.

($\Leftarrow$): Let $M_1 \cong R/\mathfrak{p}$. If $0 \neq x \in M_1$, then $\mathrm{Ann}x = \mathfrak{p}$ by part (1). It follows that $\mathfrak{p} \in \mathrm{Ass}M$. □

This proposition will be used several times in the sequel.

Recall. Let M be an R-module. The set of all zero divisors on M is:

$$Z(M) = \{a \in R | \exists 0 \neq x \in M : ax = 0\}.$$

Theorem 1.3.5. *Let M be a module over a Noetherian ring R. Then*

$$Z(M) = \bigcup_{\mathfrak{p} \in \mathrm{Ass}M} \mathfrak{p}.$$

Proof. $\supseteq$: Trivial.

$\subseteq$: Let $a \in Z(M)$. Then there exists $0 \neq x \in M$ such that $ax = 0$. Let $N = Rx$. By Theorem 1.3.3, $\mathrm{Ass}N \neq \emptyset$. So, there exits $r \in R$ such that $\mathfrak{p} := \mathrm{Ann}rx \in \mathrm{Ass}N$. It follows from Proposition 1.3.4(1) that $a \in \mathfrak{p} \subseteq \bigcup_{\mathfrak{p} \in \mathrm{Ass}M} \mathfrak{p}$. □

Exercise 6. Let M be a non zero R-module and let $\mathfrak{p} \in \mathrm{Spec}R$. Show that:

$$\mathfrak{p} \in \mathrm{Min}(\mathrm{Ann}M) \Longrightarrow \mathfrak{p} \subseteq Z(M).$$

Theorem 1.3.6. *Let M be a non zero finitely generated module over a Noetherian ring R. Then there exists a chain*

$$(0) = M_0 \subseteq M_1 \subseteq \cdots \subseteq M_n = M$$

of submodules of M such that for each i we have $M_i/M_{i-1} \cong R/\mathfrak{p}_i$ with $\mathfrak{p}_i \in$ Spec(R).

Proof. Since $M \neq (0)$, then there exists a submodule M_1 of M such that $M_1 \cong R/\mathfrak{p}_1$ with $\mathfrak{p}_1 \in \mathrm{Spec}(R)$. If $M/M_1 \neq (0)$, then there exists a submodule M_2/M_1 of M/M_1 such that $M_2/M_1 \cong R/\mathfrak{p}_2$ with $\mathfrak{p}_2 \in \mathrm{Spec}(R)$. Since M is Noetherian the above process must terminate, and hence there is $n \in \mathbb{N}$ such that $M/M_n = (0)$. This concludes the proof. □

Theorem 1.3.7. *Let $0 \longrightarrow N \longrightarrow M \longrightarrow K \longrightarrow 0$ be an exact sequence of R-modules. Then*

$$\mathrm{Ass}N \subseteq \mathrm{Ass}M \subseteq \mathrm{Ass}N \cup \mathrm{Ass}K.$$

Proof. Without loss of generality, we may assume $N \subseteq M$ and $K = M/N$. By Proposition 1.3.4(1), $\mathrm{Ass}N \subseteq \mathrm{Ass}M$. Now let $\mathfrak{p} \in \mathrm{Ass}M$. Then there exists a submodule M_1 of M such that $M_1 \cong R/\mathfrak{p}$ with $\mathfrak{p} \in \mathrm{Spec}(R)$. We have two cases:

Case 1: $M_1 \cap N = (0)$. In this case we have $(M_1 + N)/N \cong M_1$ and so $\mathfrak{p} \in \mathrm{Ass}(M_1 + N)/N \subseteq \mathrm{Ass}(M/N)$.

Case 2: $M_1 \cap N \neq (0)$. If $0 \neq x \in M_1 \cap N$, then by Proposition 1.3.4(3), $\mathfrak{p} = \mathrm{Ann}x$ and so $\mathfrak{p} \in \mathrm{Ass}N$. □

Theorem 1.3.8. *Let M be an R-module and let $(0) = M_0 \subseteq M_1 \subseteq \cdots \subseteq M_n = M$ be a chain of submodules of M such that for each i we have $M_i/M_{i-1} \cong R/\mathfrak{p}_i$ with $\mathfrak{p}_i \in \mathrm{Spec}(R)$. Then*

$$\mathrm{Ass}M \subseteq \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}.$$

Proof. We use induction on n. If $n = 1$, there is nothing to prove. Assume inductively that $n > 1$ and the result settled for all $i < n$. From the above theorem and induction hypothesis, we have

$$\text{Ass}M \subseteq \text{Ass}M_{n-1} \cup \text{Ass}(M/M_{n-1}) = \text{Ass}M_{n-1} \cup \{\mathfrak{p}_n\} \subseteq \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}.$$

□

Corollary 1.3.9. *Let M be a finitely generated module over a Noetherian ring R. Then $|\text{Ass}M| < \infty$.*

Proof. The assertion follows from Theorem 1.3.6 and Theorem 1.3.8. □

Theorem 1.3.10. *Let $\{M_i\}_{i=1}^n$ be a family of R-modules. Then*

$$\text{Ass}(\oplus_{i=1}^n M_i) = \cup_{i=1}^n \text{Ass}M_i.$$

Proof. The right-hand side is clearly included in the left-hand side; we prove the converse by induction on n. If $n = 1$, there is nothing to prove. Assume inductively that $n > 1$ and the result settled for all $i < n$. From the exact sequence

$$0 \longrightarrow M_1 \longrightarrow \oplus_{i=1}^n M_i \longrightarrow \oplus_{i=2}^n M_i \longrightarrow 0$$

and the induction hypothesis, we have

$$\text{Ass}(\oplus_{i=1}^n M_i) \subseteq \text{Ass}M_1 \cup \text{Ass}(\oplus_{i=2}^n M_i) \subseteq (\text{Ass}M_1) \cup (\cup_{i=2}^n \text{Ass}M_i) = \cup_{i=1}^n \text{Ass}M_i.$$

□

Exercise 7. Let $\{M_i\}_{i\in I}$ be a family of R-modules. Then

$$\text{Ass}(\oplus_{i\in I} M_i) = \cup_{i\in I} \text{Ass}M_i.$$

Corollary 1.3.11. *Let $\{N_i\}_{i=1}^n$ be a family of submodules of an R-module M. If $N = \cap_{i=1}^n N_i$, then*

$$\text{Ass}(M/N) \subseteq \cup_{i=1}^n \text{Ass}(M/N_i).$$

Proof. It is clear that the map

$$\begin{aligned} \varphi : M/N &\longrightarrow \oplus_{i=1}^{n} M/N_i \\ (x+N) &\longmapsto (x+N_1,\cdots,x+N_n). \end{aligned}$$

is a monomorphism. Hence the Theorem 1.3.11 implies

$$\mathrm{Ass}(M/N) = \mathrm{Ass}\varphi(M/N) \subseteq \mathrm{Ass} \oplus_{i=1}^{n} (M/N_i) = \cup_{i=1}^{n} \mathrm{Ass}(M/N_i).$$

□

Theorem 1.3.12. (Bourbaki's Theorem [3]). *Let M be a Noetherian R-module and $\mathcal{B} \subseteq \mathrm{Ass}M$. Then there exists a submodule N of M such that*

$$\mathrm{Ass}(M/N) = \mathcal{B},$$
$$\mathrm{Ass}N = \mathrm{Ass}M - \mathcal{B}.$$

Proof. Set

$$\Sigma = \{K \leq M | \mathrm{Ass}K \subseteq \mathrm{Ass}M - \mathcal{B}\}.$$

Let N be a maximal element of $\sum$. First we show that $\mathrm{Ass}(M/N) \subseteq \mathcal{B}$. If $\mathfrak{p} \in \mathrm{Ass}(M/N)$, then there exists a submodule F of M such that $F/N \cong R/\mathfrak{p}$ with $\mathfrak{p} \in \mathrm{Spec}R$. By maximality of N and the fact that

$$\mathrm{Ass}F \subseteq \mathrm{Ass}N \cup \mathrm{Ass}(F/N) \subseteq (\mathrm{Ass}M - \mathcal{B}) \cup \{\mathfrak{p}\},$$

we have $\mathfrak{p} \in \mathrm{Ass}F$ and $\mathfrak{p} \notin \mathrm{Ass}M - \mathcal{B}$. Therefore $\mathfrak{p} \in \mathcal{B}$.

Now we show that $\mathrm{Ass}M - \mathcal{B} \subseteq \mathrm{Ass}N$. Let $\mathfrak{p} \in \mathrm{Ass}M - \mathcal{B}$. Then $\mathfrak{p} \in \mathrm{Ass}M$ and $\mathfrak{p} \notin \mathrm{Ass}(M/N)$. So $\mathfrak{p} \in \mathrm{Ass}N$.

Finally, we show that $\mathcal{B} \subseteq \mathrm{Ass}(M/N)$. Let $\mathfrak{p} \in \mathcal{B}$. Then $\mathfrak{p} \notin \mathrm{Ass}M - \mathcal{B}$ and so $\mathfrak{p} \notin \mathrm{Ass}N$. Thus $\mathfrak{p} \in \mathrm{Ass}(M/N)$. □

Exercise 8. *Show that the Bourbaki's Theorem holds even without the assumption that M is Noetherian.*

1.4 Primary Decomposition

Definition 1.4.1. A proper submodule Q of an R-module M is said to be a **primary** submodule if for any $r \in R$ and $x \in M$, we have

$$rx \in Q \Longrightarrow x \in Q \text{ or } r \in \sqrt{\mathrm{Ann} M/Q}.$$

Exercise 9. Let Q be a proper submodule of an R-module M. Then Q is primary submodule if and only if $Z(M/Q) = \sqrt{\mathrm{Ann} M/Q}$.

Lemma and Definition. If Q is a primary submodule of M, then $\mathfrak{p} := \sqrt{\mathrm{Ann} M/Q}$ is a prime ideal of R. We say that Q is a $\mathfrak{p}$-primary submodule of M.

Proof. It is enough to show that $\mathrm{Ann} M/Q$ is a primary ideal of R. Let $ab \in \mathrm{Ann} M/Q$ and $a \notin \mathrm{Ann} M/Q$. Then there is an element $x \in M$ such that $ax \notin Q$. Since $abx \in Q$, by definition we have $b \in \sqrt{\mathrm{Ann} M/Q}$ and so we are done. □

Exercise 10. Let M be an R-module. Show that if $Q_1, \ldots, Q_n$ are $\mathfrak{p}$-primary submodules of M, then so too is $\cap_{i=1}^{n} Q_i$.

Exercise 11. Let M be a module over the Noetherian ring R and $y \in M$ and $\mathfrak{p} \in \mathrm{Spec} R$. Then the maximal element of

$$\Sigma = \{\mathrm{Ann} x | \mathrm{Ann} y \subseteq \mathrm{Ann} x \subseteq \mathfrak{p}\}$$

is a prime ideal of R.

Proof. Let $\mathrm{Ann} x$ be the maximal element of Σ. We show that $\mathrm{Ann} x$ is a prime ideal. Suppose that $ab \in \mathrm{Ann} x$ and $a \notin \mathrm{Ann} x$. We claim that $\mathrm{Ann} ax \subseteq \mathfrak{p}$ Suppose on the contrary that $\mathrm{Ann} ax \nsubseteq \mathfrak{p}$. Let $r \in \mathrm{Ann} ax \setminus \mathfrak{p}$. Then $\mathrm{Ann} x \subseteq \mathrm{Ann} rx \subseteq \mathfrak{p}$. Therefore $\mathrm{Ann} x = \mathrm{Ann} rx$ and hence $a \in \mathrm{Ann} x$, which is a contradiction. Thus we must have $\mathrm{Ann} ax \subseteq \mathfrak{p}$. Then $\mathrm{Ann} x \subseteq \mathrm{Ann} ax \subseteq \mathfrak{p}$ and hence $\mathrm{Ann} x = \mathrm{Ann} ax$. Therefore $b \in \mathrm{Ann} x$. □

Theorem 1.4.2. *Let R be a Noetherian ring and M be a finitely generated R-module. Then*

$$Q \textit{ is } \mathfrak{p}\textit{-primary} \Longleftrightarrow \mathrm{Ass} M/Q = \{\mathfrak{p}\}.$$

Proof. $(\Longrightarrow)$: $\mathfrak{q} \in \mathrm{Ass}M/Q$ implies that $\mathfrak{q} \subseteq Z(M/Q) = \mathfrak{p}$. On the other hand there exists $x \in M$ such that $\mathrm{Ann}M/Q \subseteq \mathrm{Ann}(x+Q) = \mathfrak{q}$. Hence $\sqrt{\mathrm{Ann}M/Q} \subseteq \sqrt{\mathfrak{q}}$ and so $\mathfrak{p} \subseteq \mathfrak{q}$. Therefore $\mathfrak{p} = \mathfrak{q}$ and hence $\mathrm{Ass}M/Q = \{\mathfrak{p}\}$.

$(\Longleftarrow)$: First we show that $\mathfrak{p} = \sqrt{\mathrm{Ann}M/Q}$. Let $\mathfrak{q} \in \mathrm{Min}(\mathrm{Ann}M/Q)$. Assume that $M = Rx_1 + \cdots + Rx_n$. Then

$$\mathrm{Ann}M/Q = \mathrm{Ann}(Rx_1 + \cdots + Rx_n + Q) = \cap_{i=1}^n \mathrm{Ann}(x_i + Q) \subseteq \mathfrak{q}.$$

Since $\mathfrak{q}$ is prime, there exists $1 \leq j \leq n$ such that $\mathrm{Ann}(x_j + Q) \subseteq \mathfrak{q}$. Set

$$\Sigma = \{\mathrm{Ann}(x+Q) | \mathrm{Ann}(x_j + Q) \subseteq \mathrm{Ann}(x+Q) \subseteq \mathfrak{q}\}.$$

Let $\mathrm{Ann}(x_0 + Q)$ be a maximal element of Σ. Then $\mathrm{Ann}(x_0 + Q) \in \mathrm{Spec}(R)$, by Exercise 11. Since

$$\mathrm{Ann}M/Q \subseteq \mathrm{Ann}(x_0 + Q) \subseteq \mathfrak{q},$$

and $\mathfrak{q} \in \mathrm{Min}(\mathrm{Ann}M/Q)$, we have that $\mathfrak{q} = \mathrm{Ann}(x_0 + Q) \in \mathrm{Ass}M/Q$ and hence $\mathfrak{q} = \mathfrak{p}$. Therefore

$$\sqrt{\mathrm{Ann}M/Q} = \bigcap_{\mathfrak{q} \in \mathrm{Min}(\mathrm{Ann}M/Q)} = \mathfrak{p}.$$

Now we have

$$Z(M/Q) = \bigcup_{\mathfrak{p} \in \mathrm{Ass}M/Q} \mathfrak{p} = \mathfrak{p}.$$

Therefore, by Exercise 9 we have Q is $\mathfrak{p}$-primary, which completes the proof. □

Definition 1.4.3. A submodule N of M is said to be **irreducible** if $N = N_1 \cap N_2$ where N_1, N_2 are submodules of M implies $N = N_1$ or $N = N_2$.

Theorem 1.4.4. *Let R be a Noetherian ring. Then every irreducible proper submodule of a finitely generated R-module is primary.*

Proof. Let N be an irreducible proper submodule of M. Suppose to the contrary, $\mathfrak{p}_1, \mathfrak{p}_2 \in \mathrm{Ass}M/N$. Then M/N has distinct submodules N_1/N and N_2/N such that $N_1/N \cong R/\mathfrak{p}_1$ and $N_2/N \cong R/\mathfrak{p}_2$. It is easy to see that $N = N_1 \cap N_2$. So it follows from the above definition that $N = N_1$ or $N = N_2$, a contradiction.

□

Theorem 1.4.5. *Let M be a Noetherian R-module. Then every proper submodule N of M is an intersection of finitely many irreducible submodules of M.*

Proof. Let

$$\Sigma = \{K \leq M | K \text{ is not a finite intersection of irreducible submodules of} M\}.$$

We claim that $\Sigma = \emptyset$. For if not, Σ has a maximal element N. But N is not irreducible and so $N = N_1 \cap N_2$ where N_1 and N_2 are submodules of M and $N \neq N_1$ and $N \neq N_2$. Therefore N_1 and N_2 are finite intersection of irreducible submodules and so is N, a contradiction. □

Definition 1.4.6. A **primary decomposition** of a submodule N of M is the finite intersection $N = Q_1 \cap \ldots \cap Q_n$ where each Q_i is primary submodule of M. A primary decomposition $N = Q_1 \cap \ldots \cap Q_n$ in which Q_i is $\mathfrak{p}_i$-primary is said to be **minimal** if
(1) $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ are different prime ideals of R,
(2) no Q_i can be omitted from the intersection $N = Q_1 \cap \ldots \cap Q_n$.

Exercise 12. (1): **(Existence of Primary Decomposition).** Let M be a Noetherian R-module. Show that every proper submodule N of M has minimal primary decomposition.
(2): **(Uniqueness of Primary Decomposition I).** Let

$$\begin{aligned} N &= Q_1 \cap \ldots \cap Q_n, \text{ where } Q_i \text{ is } \mathfrak{p}_i-\text{primary}, \\ N &= Q'_1 \cap \ldots \cap Q'_m, \text{ where } Q'_i \text{ is } \mathfrak{p}'_i-\text{primary} \end{aligned}$$

be two minimal primary decompositions of N. Show that

$$\{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\} = \operatorname{Ass}(M/N) = \{\mathfrak{p}'_1, \ldots, \mathfrak{p}'_m\}.$$

(3): **(Uniqueness of Primary Decomposition II)** Let

$$\begin{aligned} N &= Q_1 \cap \ldots \cap Q_n, \text{ where } Q_i \text{ is } \mathfrak{p}_i-\text{primary}, \\ N &= Q'_1 \cap \ldots \cap Q'_n, \text{ where } Q'_i \text{ is } \mathfrak{p}_i-\text{primary} \end{aligned}$$

be two minimal primary decompositions of N. If $\mathfrak{p}_j \in \mathrm{Min}\{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$, show that $Q_j = Q'_j$.

We now give an application of primary decomposition which is the starting of the theory of completeness.

Theorem 1.4.7. (Krull's Intersection Theorem). *Let M be a Noetherian R-module and let $\mathfrak{a}$ be an ideal of R. If $N = \bigcap_{i=1}^{\infty} \mathfrak{a}^i M$, then $\mathfrak{a}N = N$.*

Proof. If $\mathfrak{a}N = M$, then the claim is clear, and so we assume that $\mathfrak{a}N$ is a proper submodule of M. Then $\mathfrak{a}N$ has a primary decomposition

$$\mathfrak{a}N = Q_1 \cap \cdots \cap Q_n,$$

where each Q_i is a $\mathfrak{p}_i$-primary submodule of M for some $\mathfrak{p}_i \in \mathrm{Spec}R$. It suffices to show that $N \subseteq Q_i$ for every $1 \leq i \leq n$. Let i $(1 \leq i \leq n)$ be fixed. We show that $N \subseteq Q_i$. Consider two following cases:

Case 1: $\mathfrak{a} \subseteq \mathfrak{p}_i$. Then there is an integer m such that $\mathfrak{p}_i^m M \subseteq Q_i$ (why?). Therefore

$$N = \bigcap_{i=1}^{\infty} \mathfrak{a}^i M \subseteq \mathfrak{a}^m M \subseteq \mathfrak{p}_i^m M \subseteq Q_i.$$

Case 2: $\mathfrak{a} \nsubseteq \mathfrak{p}_i$. Then there exists $r \in \mathfrak{a}$ such that $r \notin \mathfrak{p}_i$. If $N \nsubseteq Q_i$, then there exists $n \in N \setminus Q_i$. Since $rn \in \mathfrak{a}N \subseteq Q_i$, $n \notin Q_i$ and Q_i is primary, $r^m M \subseteq Q_i$ for some $m \geq 0$. It follows that $r \in \mathfrak{p}_i$, which is a contradiction. Therefore $N \subseteq Q_i$. □

The following important result follows easily from the above theorem and Nakayama's Lemma.

Corollary 1.4.8. *Let M be a Noetherian R-module and let $\mathfrak{a}$ be an ideal of R such that $\mathfrak{a} \subseteq J(R)$. Then*

$$\bigcap_{i=1}^{\infty} \mathfrak{a}^i M = 0.$$

1.5 Rings of Fractions

Definition 1.5.1. A **multiplicatively closed subset** of a ring R is a subset S of R such that

(1) $1 \in S$,

(2) $s_1, s_2 \in S \Longrightarrow s_1 s_2 \in S$.

Example 1.5.2. (1): If $\mathfrak{p}$ is a prime ideal of a ring R, then $R \setminus \mathfrak{p}$ is a multiplicatively closed subset of R. More generally, if $\{\mathfrak{p}_i : i \in I\}$ is a family of prime ideals of a ring R, then $R \setminus \cup_{i \in I} \mathfrak{p}_i$ is a multiplicatively closed subset of R.

(2): Let R be a ring. Then the set $S = R \setminus \mathrm{Z}(R)$ is a multiplicatively closed subset of R.

(3): Given any element a of a ring R, the set $S = \{a^n : n \in \mathbb{N}_0\}$ of powers of a is a multiplicatively closed subset of R.

Definition 1.5.3. Let S be a multiplicatively closed subset of R. Define a relation $\sim$ on $R \times S$ as follows. Given any $(a, s), (b, t) \in R \times S$.

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

It is easy to see that the relation $\sim$ is an equivalence relation. Let us denote the equivalence class of $(a, s) \in R \times S$ by a/s, and let $S^{-1}R$ denote the set of equivalence classes of elements of $R \times S$. That is,

$$S^{-1}R = \{a/s \mid a \in R, s \in S\}.$$

Theorem 1.5.4. *$S^{-1}R$ is a commutative ring under the usual rules for calculating with fractions:*

$$(a/s) + (b/t) = (ta + sb)/st, \quad (a/s)(b/t) = (ab)/(st).$$

Proof. Left to the reader as an exercise. □

Example 1.5.5. Let R be an integral domain and $S = R - \{0\}$. Let a/s be a non zero element of $S^{-1}R$. Then $a \neq 0$. It follows that $s/a \in S^{-1}R$ and $(a/s)(s/a) = 1$. Hence $S^{-1}R$ is a field. $S^{-1}R$ is called the **quotient field** or the **field of fractions** of R. Note that in this case the equivalence relation $\sim$ on $R \times S$ takes the simpler form. In fact, we have:

$$a/s = b/t \Longleftrightarrow (a, s) \sim (b, t) \Longleftrightarrow at = bs$$

More generally, if R is a ring and $S = R - Z(R)$, then $S^{-1}R$ is called the **total quotient** ring of R.

Definition 1.5.6. The ring $S^{-1}R$ is called the **ring of fractions** or the **localization** of R with respect to multiplicatively closed subset S. If $\mathfrak{p}$ is a prime ideal of R, then $S = R \setminus \mathfrak{p}$ is a multiplicatively closed subset of R. In this case, we write $R_{\mathfrak{p}}$ for $S^{-1}R$, and call it the localization of R at $\mathfrak{p}$.

The next example explains why $S^{-1}R$ is called localization.

Example 1.5.7. Let $S = R \setminus \mathfrak{p}$, where $\mathfrak{p}$ is a prime ideal of R. The set $\mathfrak{p}S^{-1}R := \{a/s : a \in \mathfrak{p}, s \in S\}$ is an ideal of $S^{-1}R$ and an element of $S^{-1}R$ that is not in $\mathfrak{p}S^{-1}R$ is a unit in $S^{-1}R$. It follows that $\mathfrak{p}S^{-1}R$ is the only maximal ideal of the ring $S^{-1}R$. In other words, $S^{-1}R$ is a local ring.

Exercise 13. Let X be any subset of R. Define $S^{-1}X = \{x/s | x \in X, s \in S\}$. Let I, J be two ideals of R. Show that:
(1) $S^{-1}I$ is an ideal of $S^{-1}R$.
(2) $S^{-1}(I + J) = S^{-1}I + S^{-1}J$,
(3) $S^{-1}(IJ) = (S^{-1}I)(S^{-1}J)$,
(4) $S^{-1}(I \cap J) = (S^{-1}I) \cap (S^{-1}J)$,
(5) $S^{-1}I$ is a proper ideal of $S^{-1}R$ if and only if $S \cap I = \emptyset$.

Definition 1.5.8. The ring homomorphism $\varphi : R \longrightarrow S^{-1}R$ given by $\varphi(a) = a/1$ is called the **natural ring homomorphism**.

Lemma 1.5.9. *Let $\varphi : R \longrightarrow S^{-1}R$ be the natural ring homomorphism, and let I be an ideal of R. Then*

$$I^e = \{\lambda \in S^{-1}R | \lambda = a/s \ \ \textit{for some } a \in I, s \in S\}.$$

Proof. $\supseteq$: It is clear that, for all $a \in I$ and $s \in S$, we have $a/s = (1/s)\varphi(a) \in I^e$.
$\subseteq$: Let $\lambda \in I^e$. There exist $n \in \mathbb{N}$, $h_1, \ldots, h_n \in I$ and $a_1, \ldots, a_n \in R$ such that

$$\lambda = \sum_{i=1}^{n} (a_i/s_i)(h_i/1) = \sum_{i=1}^{n} (a_i h_i)/s_i = a/s.$$

□

Remark. (1): $\lambda = a/s \in I^e \not\Longrightarrow a \in I$,
(2): $\lambda = a/s \in I^e \Longrightarrow \lambda = b/t$ such that $b \in I$.

Lemma 1.5.10. *Let $\varphi : R \longrightarrow S^{-1}R$ be the natural ring homomorphism, and let $\mathfrak{q}$ be a primary ideal of R such that $\mathfrak{q} \cap S = \emptyset$. If $\lambda = a/s \in \mathfrak{q}^e$, then $a \in \mathfrak{q}$. Furthermore $\mathfrak{q}^{ec} = \mathfrak{q}$.*

Proof. Let $\lambda = a/s \in \mathfrak{q}^e$. Then there exist $b \in \mathfrak{q}$ and $t \in S$ such that $b/t = a/s$. Therefore there exits $u \in S$ such that $u(sb - ta) = 0$. Hence $(ut)a = usb \in \mathfrak{q}$. Now $ut \in S$, and since $\mathfrak{q} \cap S = \emptyset$, it follows that $ut \notin \sqrt{\mathfrak{q}}$. But $\mathfrak{q}$ is a primary ideal, and so $a \in \mathfrak{q}$, as required. Now we show that $\mathfrak{q}^{ec} = \mathfrak{q}$. Clearly $\mathfrak{q} \subseteq \mathfrak{q}^{ec}$. For the reverse inclusion, let $a \in \mathfrak{q}^{ec}$. Thus $a/1 \in \mathfrak{q}^e$, and so, by what we have just proved, $a \in \mathfrak{q}$. □

Exercise 14. Let $\varphi : R \longrightarrow S^{-1}R$ be the natural ring homomorphism, and let I, J be ideals of R. Show that:
(1) $(I \cap J)^e = I^e \cap J^e$,
(2) $\sqrt{I}^e = \sqrt{I^e}$,
(3) $I^e = S^{-1}R$ if and only if $I \cap S \neq \emptyset$.

Exercise 15. Let $\varphi : R \longrightarrow S^{-1}R$ be the natural ring homomorphism. Show that:
(1) if $\mathfrak{p} \in \text{Spec}R$ and $\mathfrak{p} \cap S = \emptyset$, then $\mathfrak{p}^e \in \text{Spec}S^{-1}R$,
(2) if $\mathfrak{p} \in \text{Spec}S^{-1}R$, then $\mathfrak{p}^c \in \text{Spec}R$ and $\mathfrak{p}^c \cap S = \emptyset$. Also $\mathfrak{p}^{ce} = \mathfrak{p}$,
(3) $\text{Spec}S^{-1}R = \{\mathfrak{p}^e | \mathfrak{p} \in \text{Spec}R, \mathfrak{p} \cap S = \emptyset\}$.

Theorem 1.5.11. *Let $\varphi : R \longrightarrow S^{-1}R$ be the natural ring homomorphism. Then*

(1) if $\mathfrak{q}$ is a $\mathfrak{p}-$primary ideal of R such that $\mathfrak{q} \cap S = \emptyset$, then $\mathfrak{q}^e$ is a $\mathfrak{p}^e-$primary ideal of $S^{-1}R$,
(2) if $\mathfrak{q}$ is a $\mathfrak{p}-$primary ideal of $S^{-1}R$, then $\mathfrak{q}^c$ is a $\mathfrak{p}^c-$primary ideal of R such that $\mathfrak{q}^c \cap S = \emptyset$. Also $\mathfrak{q}^{ce} = \mathfrak{q}$.
(3) the set of all primary ideals of $S^{-1}R$ is

$$\{\mathfrak{q}^e | \mathfrak{q} \text{ is primary ideal of } R, \mathfrak{q} \cap S = \emptyset\}.$$

Proof. (1): By Exercise 14, we have $\mathfrak{q}^e \neq S^{-1}R$ and $\sqrt{\mathfrak{q}^e} = \sqrt{\mathfrak{q}}^e = \mathfrak{p}^e$. Now let $(a/s)(b/t) \in \mathfrak{q}^e$ and $(b/t) \notin \mathfrak{p}^e$. Then $ab \in \mathfrak{q}$ and $b \notin \mathfrak{p}$. Since $\mathfrak{q}$ is $\mathfrak{p}-$primary, we must have $a \in \mathfrak{q}$, so that $a/s \in \mathfrak{q}^e$. Hence $\mathfrak{q}^e$ is a $\mathfrak{p}^e-$primary ideal of $S^{-1}R$.
(2): By Theorem 1.2.5, $\mathfrak{q}^c$ is a $\mathfrak{p}^c-$primary ideal of R. Now we show that $\mathfrak{q}^{ce} = \mathfrak{q}$. Clearly $\mathfrak{q}^{ce} \subseteq \mathfrak{q}$. For the reverse inclusion, let $a/s \in \mathfrak{q}$. Then

$$a/1 = (s/1)(a/s) \in \mathfrak{q} \Longrightarrow a \in \mathfrak{q}^c$$
$$\Longrightarrow a/1 \in \mathfrak{q}^{ce} \Longrightarrow (a/s) = (1/s)(a/1) \in \mathfrak{q}^{ce}.$$

If $\mathfrak{q}^c \cap S \neq \emptyset$, then $\mathfrak{q} = \mathfrak{q}^{ce} = S^{-1}R$, which is a contradiction. Thus $\mathfrak{q}^c \cap S = \emptyset$ and the proof of part (2) is complete.
(3): Let Ω be the set of all primary ideals of $S^{-1}R$. By part (1), we have

$$\Omega \supseteq \{\mathfrak{q}^e | \mathfrak{q} \text{ is primary ideal of } R, \mathfrak{q} \cap S = \emptyset\}.$$

Now, let $Q \in \Omega$. Suppose that $\mathfrak{q} := Q^c$. Then by part (2), we have $Q = Q^{ce} = \mathfrak{q}^e$ and $\mathfrak{q}$ is primary ideal of R and $\mathfrak{q} \cap S = \emptyset$. It follows that

$$\Omega \subseteq \{\mathfrak{q}^e | \mathfrak{q} \text{ is primary ideal of } R, \mathfrak{q} \cap S = \emptyset\},$$

and the proof of part (3) is complete.

□

Exercise 16. Let R be an integral domain with field of fractions K. Consider any ring of fractions of R as a subring of K. Show that:

$$R = \bigcap_{\mathfrak{m} \in \operatorname{Max} R} R_{\mathfrak{m}}.$$

Exercise 17. Let R be a Noetherian ring, and let $\mathfrak{p} \in \mathrm{Spec}R$ and $\varphi : R \longrightarrow R_{\mathfrak{p}}$ be the natural ring homomorphism. Show that

$$\mathrm{Ker}\varphi = \bigcap_{\mathfrak{q} \text{ is } \mathfrak{p}-\text{primary}} \mathfrak{q}.$$

Exercise 18. Let R be a ring and let $\mathfrak{p}$ a prime ideal of R. Let $\varphi : R \longrightarrow R_{\mathfrak{p}}$ be the natural ring homomorphism. The n**th symbolic power** is defined to be

$$\mathfrak{p}^{(n)} = (\mathfrak{p}^n)^{ec}.$$

Show that

(1) $\mathfrak{p}^{(n)}$ is $\mathfrak{p}$-primary ideal of R,

(2) $\mathfrak{p}^{(n)} = \mathfrak{p}^n \Longleftrightarrow \mathfrak{p}^n$ is $\mathfrak{p}$-primary.

1.6 Modules of Fractions

The construction of $S^{-1}R$ can be carried through with an R-module M in place of the ring R.

Definition 1.6.1. Let M be an R-module and let S be a multiplicatively closed subset of R. Define a relation $\sim$ on $M \times S$ as follows. Given any $(x, s), (y, t) \in M \times S$.

$$(x, s) \sim (y, t) \Longleftrightarrow u(tx - sy) = 0 \text{ for some } u \in S.$$

It is easy to see that the relation $\sim$ is an equivalence relation. Let us denote the equivalence class of $(x, s) \in M \times S$ by x/s, and let $S^{-1}M$ denote the set of equivalence classes of elements of $M \times S$. That is,

$$S^{-1}M = \{x/s \mid x \in M, s \in S\}.$$

Theorem 1.6.2. *If we define addition in $S^{-1}M$ and scalar multiplication by elements of $S^{-1}R$ by*

$$(x/s) + (y/t) = (tx + sy)/st, \quad (a/t)(x/s) = (ax)/(ts),$$

then $S^{-1}M$ becomes an $S^{-1}R$-module.

Exercise 19. Prove the above theorem.

Definition 1.6.3. The module $S^{-1}M$ is called the **module of fractions** or the **localization** of M with respect to multiplicatively closed subset S.

Proposition 1.6.4. *Let S be multiplicatively closed subset of R and $\varphi : M \longrightarrow N$ be an $R-$module homomorphism. Then the induced map*

$$\begin{aligned} S^{-1}\varphi : S^{-1}M &\longrightarrow S^{-1}N \\ x/s &\longmapsto \varphi(x)/s \end{aligned}$$

is an $S^{-1}R$-module homomorphism.

Proof. Assume that $x/s = y/t$. Then there exists $u \in S$ such that $u(tx-su) = 0$. Therefore $u(t\varphi(x) - s\varphi(y)) = 0$ and hence $\varphi(x/s) = \varphi(y/t)$. Hence φ is well-define. Now it is easy to check that $S^{-1}\varphi$ is an $S^{-1}R-$homomorphism □

Exercise 20. Let L, M, N be $R-$modules, and let S be multiplicatively closed subset of R. Let $\varphi, \varphi' : M \longrightarrow N$ and $\psi : N \longrightarrow L$ be $R-$homomorphism. Show that:
(1) $S^{-1}(\varphi + \varphi') = S^{-1}\varphi + S^{-1}\varphi'$,
(2) $S^{-1}(\psi\varphi) = S^{-1}\psi S^{-1}\varphi$,
(3) $S^{-1}(1_M) = 1_{S^{-1}M}$,
(4) if φ is an $R-$isomorphism, then $S^{-1}\varphi$ is an $S^{-1}R-$isomorphism.

Theorem 1.6.5. *Let L, M, N be modules. Then*
(1) If $L \xrightarrow{\psi} M \xrightarrow{\varphi} N$ is an exact sequence of R-modules, then $S^{-1}L \xrightarrow{S^{-1}\psi} S^{-1}M \xrightarrow{S^{-1}\varphi} S^{-1}N$ is an exact sequence of $S^{-1}R$-modules,
(2) if N is a submodule of M, then $S^{-1}(M/N) \cong_{S^{-1}R} S^{-1}(M)/S^{-1}(N)$.

Proof. (1): Since $\varphi\psi = 0$, we have $S^{-1}\varphi S^{-1}\psi = 0$ by part (2) of the above Exercise. Therefore $\mathrm{Im}S^{-1}\psi \subseteq \ker S^{-1}\varphi$. Now we show that $\ker S^{-1}\varphi \subseteq \mathrm{Im}S^{-1}\psi$. Let $x/s \in \ker S^{-1}\varphi$. Then $\varphi(x/s) = \varphi(x)/s = 0$. Thus there exists $u \in S$ such that $u\varphi(x) = 0$, whence $\varphi(ux) = 0$. It follows that there exists $y \in L$ such that $\psi(y) = ux$. Now we have

$$\psi(y/su) = \psi(y)/su = (ux)/(su) = x/s.$$

(2): Follows from (1) by considering the exact sequence $0 \longrightarrow N \longrightarrow M \longrightarrow M/N \longrightarrow 0$. $\square$

Exercise 21. Let M, N be R-modules.
(1)$S^{-1}M \cong_{S^{-1}R} S^{-1}R \otimes_R M$,
(2) $S^{-1}R$ is a flat R-module,
(3) $S^{-1}(M \otimes_R N) \cong_{S^{-1}R} S^{-1}M \otimes_{S^{-1}R} S^{-1}N$.

Exercise 22. Let $\varphi : R \longrightarrow S^{-1}R$ be the natural ring homomorphism, and let N_1, N_2 be submodules of the R-module M. Let I be an ideal of R, and let $a \in R$. Show that:
(1) $S^{-1}(IM) = I^e S^{-1}M$,
(2) $S^{-1}(aM) = (a/1)S^{-1}M$,
(3) $S^{-1}(N_1 + N_2) = S^{-1}N_1 + S^{-1}N_2$,
(4) $S^{-1}(N_1 \cap N_2) = S^{-1}N_1 \cap S^{-1}N_2$,
(5) if M is a finitely generated R-module, then $S^{-1}M$ is a finitely generated $S^{-1}R$-module,
(6) if M is a Noetherian R-module, then $S^{-1}M$ is a Noetherian $S^{-1}R$-module,
(7) if M is an Artinian R-module, then $S^{-1}M$ is an Artinian $S^{-1}R$-module,
(8) if M is a free R-module, then $S^{-1}M$ is a free $S^{-1}R$-module,
(9) if M is a projective R-module, then $S^{-1}M$ is a projective $S^{-1}R$-module,
(10) if M is a flat R-module, then $S^{-1}M$ is a flat $S^{-1}R$-module.

Theorem 1.6.6. *Let L, N be submodules of the module M over the ring R, and let S be multiplicatively closed subset of R. Then*
(1) If N is finitely generated, then $S^{-1}(L :_R N) = (S^{-1}L :_{S^{-1}R} S^{-1}N)$.
(2) If M is finitely generated, then $S^{-1}\mathrm{Ann}_R M = \mathrm{Ann}_{S^{-1}R} S^{-1}M$.

Proof. (1) $\subseteq$: Let $\lambda \in S^{-1}(L :_R N)$, and consider a representation $\lambda = a/s$, where $a \in (L :_R N)$ and $s \in S$. Then $aN \subseteq L$ and hence $(a/s)S^{-1}N \subseteq S^{-1}L$. Therefore $a/s \in (S^{-1}L :_{S^{-1}R} S^{-1}N)$.

$\supseteq$: Let $N = Rx$ and $\lambda = a/s \in (S^{-1}L :_{S^{-1}R} S^{-1}Rx)$. Then $(a/s)(x/1) \in S^{-1}L$. It follows that there exists $u \in S$ such that $uax \in L$. Therefore $(a/s) = (au/su) \in S^{-1}(L :_R Rx)$. Now, let $N = Rx_1 + \cdots + Rx_n$ and $\lambda = a/s \in (S^{-1}L :_{S^{-1}R} S^{-1}N)$. Then

$$\begin{aligned} S^{-1}(L :_R N) &= S^{-1}\bigcap_{i=1}^{n}(L :_R Rx_i) \\ &= \bigcap_{i=1}^{n}(S^{-1}L :_{S^{-1}R} S^{-1}Rx_i) \\ &= (S^{-1}L :_{S^{-1}R} S^{-1}Rx_1 + \cdots + S^{-1}Rx_n) \\ &= (S^{-1}L :_{S^{-1}R} S^{-1}N). \end{aligned}$$

This proves the part (1).

(2): Follows from part (1). □

Theorem 1.6.7. *Let M be a module over a Noetherian ring R, and let S be a multiplicatively closed subset of R. Then*

$$\mathrm{Ass}_{S^{-1}R}S^{-1}M = \{\mathfrak{p}S^{-1}R | \mathfrak{p} \in \mathrm{Ass}_R M \ \ \textit{and} \ \mathfrak{p} \cap S = \emptyset\}.$$

Proof. $\supseteq$: Let $\mathfrak{p} \in \mathrm{Ass}_R M$ be such that $\mathfrak{p} \cap S = \emptyset$. Then $\mathfrak{p}S^{-1}R \in \mathrm{Spec}S^{-1}R$, and there there exists $x \in M$ such that $\mathfrak{p} = \mathrm{Ann}_R x$. It follows that $\mathfrak{p}S^{-1}R = \mathrm{Ann}_{S^{-1}R}x/1 \in \mathrm{Spec}S^{-1}R$, and so $\mathfrak{p}S^{-1}R \in \mathrm{Ass}_{S^{-1}R}S^{-1}M$, as desired.

$\subseteq$: Let $\mathfrak{q} \in \mathrm{Ass}_{S^{-1}R}S^{-1}M$. Since $\mathfrak{q} \in \mathrm{Spec}S^{-1}R$, it follows that there is a $\mathfrak{p} \in \mathrm{Spec}R$ such that $\mathfrak{q} = \mathfrak{p}S^{-1}R$ and $\mathfrak{p} \cap S = \emptyset$. Also there exist $x \in M$ and $s \in S$ such that $\mathfrak{q} = \mathrm{Ann}_{S^{-1}R}x/s$. We have

$$S^{-1}\mathfrak{p} = \mathrm{Ann}_{S^{-1}R}x/s = \mathrm{Ann}_{S^{-1}R}x/1.$$

Let $\mathfrak{p} =< a_1, \ldots, a_n >$. Thus $a_i x/1 = 0_{S^{-1}M}$ for all $i = 1, \ldots, n$. Hence, for each $i = 1, \ldots, n$ there exists $s_i \in S$ such that $s_i a_i x = 0$. Set $s = s_1 \ldots s_n$. We claim that $\mathfrak{p} = \mathrm{Ann}_R sx$. Since $sa_i x = 0$ for all $i = 1, \ldots, n$, we have $\mathfrak{p} \subseteq \mathrm{Ann}_R sx$.

Now, let $r \in \mathrm{Ann}_R sx$. Thus $rsx = 0$, so that $(rs/1)(x/1) = 0_{S^{-1}M}$. Hence $(rs/1) \in \mathrm{Ann}_{S^{-1}R} x/1 = S^{-1}\mathfrak{p}$. Therefore $rs \in \mathfrak{p}$; since $\mathfrak{p}$ is prime and $s \notin \mathfrak{p}$, we have $r \in \mathfrak{p}$. Thus $\mathfrak{p} = \mathrm{Ann}_R sx$ and the proof is complete. □

Definition 1.6.8. Let M be an R-module and let $\mathfrak{p}$ be a prime ideal of R. Suppose that $S = R - \mathfrak{p}$. In this case $S^{-1}M$ and $S^{-1}\varphi$ are denoted by $M_\mathfrak{p}$ and $\varphi_\mathfrak{p}$ respectively. We say that $M_\mathfrak{p}$ is the **localization** of M at $\mathfrak{p}$.

A property $\mathcal{P}$ of a ring R (or of an R-module M) is said to be a **local property** if the following holds.

R (or M) has $\mathcal{P}$ if and only if $R_\mathfrak{p}$ (or $M_\mathfrak{p}$) has $\mathcal{P}$ for all $\mathfrak{p} \in \mathrm{Spec}R$.

The following theorem gives an example of a local property.

Theorem 1.6.9. *Let M be an R-module. Then the following are equivalent:*
(1) $M = 0$,
(2) $M_\mathfrak{p} = 0$ for all $\mathfrak{p} \in \mathrm{Spec}R$,
(3) $M_\mathfrak{m} = 0$ for all $\mathfrak{m} \in \mathrm{Max}R$.

Proof. (1) $\Longrightarrow$ (2) $\Longrightarrow$ (3) are clear.
(3) $\Longrightarrow$ (1): Let $x \in M$ and $\mathfrak{m} \in \mathrm{Max}R$. Then $x/1 \in M_\mathfrak{m} = 0$. Hence there exists $u \in R \setminus \mathfrak{m}$ such that $ux = 0$. If follows that $\mathrm{Ann}x \nsubseteq \mathfrak{m}$. Therefore $\mathrm{Ann}x = R$ and hence $x = 0$. □

Corollary 1.6.10. *Let $\varphi : M \longrightarrow N$ be an R-module homomorphism. Then the following are equivalent:*
(1) φ is injective,
(2) $\varphi_\mathfrak{p}$ is injective for all $\mathfrak{p} \in \mathrm{Spec}R$,
(3) $\varphi_\mathfrak{m}$ is injective for all $\mathfrak{m} \in \mathrm{Max}R$.

Proof. Use the above theorem on $\ker\varphi$. □

Exercise 23. Let $\varphi : M \longrightarrow N$ be an R-module homomorphism. Show that the following are equivalent:
(1) φ is surjective,

(2) $\varphi_{\mathfrak{p}}$ is surjective for all $\mathfrak{p} \in \mathrm{Spec}R$,

(3) $\varphi_{\mathfrak{m}}$ is surjective for all $\mathfrak{m} \in \mathrm{Max}R$.

Exercise 24. Let M be an R-module homomorphism. Show that the following are equivalent:

(1) M is flat,

(2) $M_{\mathfrak{p}}$ is flat for all $\mathfrak{p} \in \mathrm{Spec}R$,

(3) $M_{\mathfrak{m}}$ is flat for all $\mathfrak{m} \in \mathrm{Max}R$.

Exercise 25. Let R be a Noetherian ring, and let $\varphi : M \longrightarrow N$ be an R-module homomorphism. Then φ is injective if and only if $\varphi_{\mathfrak{p}}$ is injective for all $\mathfrak{p} \in \mathrm{Ass}M$.

Exercise 26. Let M and N be two modules over a local ring $(R, \mathfrak{m})$. If $M_{\mathfrak{m}} \cong_{R_{\mathfrak{m}}} N_{\mathfrak{m}}$, prove that $M \cong_R N$.

Exercise 27. Let M be an R-module, let S be a multiplicatively closed subset of R and let $\mathfrak{p} \in \mathrm{Spec}R$ be such that $\mathfrak{p} \cap S = \emptyset$. Prove that

$$\begin{aligned} (S^{-1}R)_{\mathfrak{p}S^{-1}R} &\cong R_{\mathfrak{p}}, \\ (S^{-1}M)_{\mathfrak{p}S^{-1}R} &\cong M_{\mathfrak{p}}. \end{aligned}$$

Exercise 28. (Uniqueness of Primary Decomposition II). Let $\mathfrak{p} \in \mathrm{Min}(\mathrm{Ass}M/N)$. Then the $\mathfrak{p}$-primary component of minimal primary decomposition of N is uniquely determined by M, N and $\mathfrak{p}$.

Proof. Suppose that $N = Q_1 \cap \ldots \cap Q_n$ is a minimal primary decomposition, and that $Q = Q_1$ is the $\mathfrak{p}-$primary component with $\mathfrak{p} = \mathfrak{p}_1$. We show that $Q = \varphi_{\mathfrak{p}}^{-1}(N_{\mathfrak{p}})$, where $\varphi_{\mathfrak{p}} : M \longrightarrow M_{\mathfrak{p}}$ is the natural homomorphism, and therefore it is uniquely determined by M, N and $\mathfrak{p}$. For $i > 1$, $\mathfrak{p}_i \nsubseteq \mathfrak{p}$ and $\mathfrak{p}_i = \sqrt{\mathrm{Ann}M/Q_i}$. It follows that there exist $k \in \mathbb{N}$ and $a_i \in \mathfrak{p}_i \setminus \mathfrak{p}$ such that $a_i^k(M/Q_i) = 0$. Hence $(M/Q_i)_{\mathfrak{p}} = 0$ and so $M_{\mathfrak{p}} = Q_{i\mathfrak{p}}$ for all $i > 1$. We have

$$Q \subseteq \varphi_{\mathfrak{p}}^{-1}(Q_{\mathfrak{p}}) = \varphi_{\mathfrak{p}}^{-1}(Q_{\mathfrak{p}} \cap M_{\mathfrak{p}}) = \varphi_{\mathfrak{p}}^{-1}(Q_{1\mathfrak{p}} \cap Q_{2\mathfrak{p}} \cap \ldots \cap Q_{n\mathfrak{p}}) = \varphi_{\mathfrak{p}}^{-1}(N_{\mathfrak{p}}).$$

It is enough to show that $\varphi_{\mathfrak{p}}^{-1}(N_{\mathfrak{p}}) \subseteq Q$. Let $x \in \varphi_{\mathfrak{p}}^{-1}(N_{\mathfrak{p}}) = \varphi_{\mathfrak{p}}^{-1}(Q_{\mathfrak{p}})$. Then $x/1 = q/t$ for some $q \in Q$ and $t \in R \setminus \mathfrak{p}$. It follows that $(ut)x \in Q$ for some $u \in R \setminus \mathfrak{p}$. Since $ut \in R \setminus \mathfrak{p}$ and Q is $\mathfrak{p}$-primary, we have $x \in Q$. This completes the proof. □

1.7 Support

Definition 1.7.1. Let M be an R-module. The **support** of M is

$$\mathrm{Supp}_R M = \mathrm{Supp} M := \{\mathfrak{p} \in \mathrm{Spec} R | M_{\mathfrak{p}} \neq 0\}.$$

Theorem 1.7.2. *Let M be an R-module. Then*

$$\mathrm{Supp} M = \{\mathfrak{p} \in \mathrm{Spec} R | \mathrm{Ann} x \subseteq \mathfrak{p} \textit{ for some } x \in M\}.$$

Proof. $\subseteq$: Let $\mathfrak{p} \in \mathrm{Supp} M$. Then there is $0 \neq x/s \in M_{\mathfrak{p}}$. It follows that $\mathrm{Ann} x \subseteq \mathfrak{p}$.

$\supseteq$: Let $\mathrm{Ann} x \subseteq \mathfrak{p}$ for some $x \in M$. Then $0 \neq x/1 \in M_{\mathfrak{p}}$ and hence $\mathfrak{p} \in \mathrm{Supp} M$. □

Exercise 29. Let M be a finitely generated R-module. Show that

$$\mathrm{Supp} M = V(\mathrm{Ann} M).$$

Theorem 1.7.3. *Let M be an R-module. Then*

(1) $\mathrm{Ass} M \subseteq \mathrm{Supp} M$*,*

(2) $M \neq 0$ *if and only if* $\mathrm{Supp} M \neq \emptyset$*,*

(3) if R is Noetherian, then $\mathrm{Min}\mathrm{Supp} M \subseteq \mathrm{Ass} M$*,*

(4) if R is Noetherian, then $\mathrm{Min}\mathrm{Supp} M = \mathrm{Min}\mathrm{Ass} M$*.*

Proof. (1) and (2): Trivial.

(3): Let $\mathfrak{p} \in \mathrm{Min}\mathrm{Supp} M$. Then there exists $y \in M$ such that $\mathrm{Ann} y \subseteq \mathfrak{p}$. Set

$$\Sigma = \{\mathrm{Ann} x | \mathrm{Ann} y \subseteq \mathrm{Ann} x \subseteq \mathfrak{p}\}.$$

Let $\mathrm{Ann} x_0$ be a maximal element of Σ. By Exercise 11, $\mathrm{Ann} x_0$ is a prime ideal of R and hence $\mathfrak{p} = \mathrm{Ann} x_0 \in \mathrm{Ass} M$.

(4)$\subseteq$: Let $\mathfrak{p} \in \text{MinSupp}M$. Then by (3), we have $\mathfrak{p} \in \text{Ass}M$. Now let $\mathfrak{q} \in \text{Ass}M$ such that $\mathfrak{q} \subseteq \mathfrak{p}$. By (1), $\mathfrak{q} \in \text{Supp}M$ and hence $\mathfrak{p} = \mathfrak{q}$. Therefore $\mathfrak{p} \in \text{MinAss}M$.

$\supseteq$: Let $\mathfrak{p} \in \text{MinAss}M$. If $\mathfrak{q} \in \text{Supp}M$ and $\mathfrak{q} \subseteq \mathfrak{p}$, then there exists $y \in M$ such that $\text{Ann}y \subseteq \mathfrak{q}$. Set

$$\Sigma = \{\text{Ann}x | \text{Ann}y \subseteq \text{Ann}x \subseteq \mathfrak{q}\}.$$

Let $\text{Ann}x_0$ be a maximal element of Σ. By Exercise 11, $\text{Ann}x_0$ is a prime ideal of R and hence $\mathfrak{p} = \text{Ann}x_0 \in \text{Ass}M$. Therefore $\mathfrak{q} = \mathfrak{p}$ and hence $\mathfrak{p} \in \text{MinSupp}M$. □

Theorem 1.7.4. *Let* $0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$ *be an exact sequence of* R*-modules. Then*

$$\text{Supp}M = \text{Supp}M' \cup \text{Supp}M''.$$

Proof. Let $\mathfrak{p} \in \text{Spec}R$. From the exact sequence $0 \longrightarrow M'_{\mathfrak{p}} \longrightarrow M_{\mathfrak{p}} \longrightarrow M''_{\mathfrak{p}} \longrightarrow 0$, we have

$$\mathfrak{p} \in \text{Supp}M \Longleftrightarrow M_{\mathfrak{p}} \neq 0 \Longleftrightarrow M'_{\mathfrak{p}} \neq 0 \text{ or } M''_{\mathfrak{p}} \neq 0 \Longleftrightarrow \mathfrak{p} \in \text{Supp}M' \cup \text{Supp}M''.$$

□

Theorem 1.7.5. *Let* M *be an* R*-module and let*

$$(0) = M_0 \subseteq M_1 \subseteq \cdots \subseteq M_n = M$$

be a chain of submodules of M *such that for each* i *we have* $M_i/M_{i-1} \cong R/\mathfrak{p}_i$ *with* $\mathfrak{p}_i \in \text{Spec}(R)$. *Then*

$$\text{Ass}M \subseteq \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\} \subseteq \text{Supp}M.$$

Proof. $\text{Ass}M \subseteq \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$, by Theorem 1.3.9. Since

$$(M_i)_{\mathfrak{p}_i}/(M_{i-1})_{\mathfrak{p}_i} = (M_i/M_{i-1})_{\mathfrak{p}_i} \cong (R/\mathfrak{p}_i)_{\mathfrak{p}_i} \cong (R_{\mathfrak{p}_i}/\mathfrak{p}_i R_{\mathfrak{p}_i}) \neq 0,$$

we have $(M_i)_{\mathfrak{p}_i} \neq 0$ and hence $\mathfrak{p}_i \in \text{Supp}M$. Therefore $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\} \subseteq \text{Supp}M$. □

Exercise 30. Let M be an R-module, and let S be a multiplicatively closed subset of R. Show that

$$\mathrm{Supp}_{S^{-1}R}S^{-1}M = \{\mathfrak{p}S^{-1}R | \mathfrak{p} \in \mathrm{Supp}_R M \text{ and } \mathfrak{p} \cap S = \emptyset\}.$$

Exercise 31. Show that if M, N are finitely generated R-modules, then

$$\mathrm{Supp}(M \otimes N) = \mathrm{Supp} M \cap \mathrm{Supp} N.$$

Exercise 32. Show that if R is a Noetherian ring, M is a finitely generated R-module, and N is an R-module, then

$$\mathrm{Ass}\mathrm{Hom}(M, N) = \mathrm{Supp} M \cap \mathrm{Ass} N.$$

Exercise 33. Let R be a Noetherian ring, and let N be a submodule of an R-module M. Show that

$$\mathrm{Ass} M/N \subseteq \mathrm{Ass} M \cup \mathrm{Supp} N.$$

Chapter 2

Integral Extensions

The theory of algebraic field extensions has a useful analogue to ring extensions, which is discussed in this chapter.

2.1 Integral Extensions

Definition 2.1.1. (1): If R is a subring of a ring S we say that S is an **extension ring** of R.
(2): An element s of S is said to be **integral** over R if s is a root of a *monic* polynomial with coefficients in R, that is if there is a relation of the form

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

with $a_i \in R$. If every element of S is integral over R we say that S is **integral** over R, or that S is an **integral extension** of R.
(3): We say that a homomorphism $\varphi : R \longrightarrow S$ is **integral** if and only if S is integral over its subring $\mathrm{Im}\varphi$.

Lemma 2.1.2. (Determinant Trick) *Let R be a subring of S. Let M be an S-module that is finitely generated as an R-module. Let $s \in S$ and let I be an ideal of R such that $sM \subseteq IM$. Then there exits $a_i \in I^i$ for $i = 1, \ldots, n$ such* *that*

$$s^n + a_1 s^{n-1} + \cdots + a_n \in \mathrm{Ann}_S M.$$

Proof. Suppose that $M = Rx_1 + Rx_2 + \cdots + Rx_n$. Then there exist $a_{ij} \in I$ such that $sx_i = \sum_{j=1}^{n} a_{ij} x_j$. Then

$$\begin{pmatrix} s - a_{11} & -a_{12} & \cdots & -a_{1n} \\ -a_{21} & s - a_{22} & \cdots & -a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ -a_{n1} & -a_{n2} & \cdots & s - a_{nn} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

If $A = [a_{ij}]_{n\times n}$, $B = sI_n - A$ and $X = [x_i]_{n\times 1}$, then by Theorem 4 of Chapter 5 of [7], we have

$$(\det B)X = (\det B)I_n X = (\mathrm{adj} B)BX = 0.$$

Hence $\det B \in \mathrm{Ann}_S M$. Finally, it follows from the definition of determinant that

$$\det B = s^n + a_1 s^{n-1} + \cdots + a_n$$

with $a_i \in I^i$ for $i = 1 \ldots, n$. □

Theorem 2.1.3. *Let R be a subring of S, with $s \in S$. The following conditions are equivalent:*
(1) s is integral over R,
(2) $R[s]$ is a finitely generated R-module,
(3) $R[s]$ is contained in a subring R' of S that is a finitely generated R-module,
(4) There is a faithful $R[s]$-module M that is finitely generated as an R-module.

Proof. (1)$\Longrightarrow$(2): From (1) we have $s^{n+r} = -(a_1 s^{n+r-1} + \cdots + a_n s^r)$ for all $r \geq 0$, hence by induction, all positive powers of s lie in the R-module generated by $1, s, \ldots, s^{n-1}$. Hence $R[s]$ is generated (as an R-module) by $1, s, \ldots, s^{n-1}$.
(2)$\Longrightarrow$(3): Take $R' = R[s]$.
(3)$\Longrightarrow$(4): Take $M = R'$, which is a faithful $R[s]$-module (since $a \in \mathrm{Ann}_{R[s]} R' \Longrightarrow$

$a = a1 = 0$).

(4)$\Longrightarrow$(1): Let M be a faithful $R[s]$-module which is finitely generated as R-module. Since M is an $R[s]$-module, $sM \subseteq RM$. Now, we can apply the above lemma with $S = R[s]$ and $I = R$ to see that there exist $n \in \mathbb{N}$ and $a_1 \ldots, a_n \in R$ such that

$$s^n + a_1 s^{n-1} + \cdots + a_n \in \mathrm{Ann}_{R[s]} M = 0.$$

Hence s is integral over R. □

Remark 2.1.4. Suppose that M is finitely generated as an S-module and that S is finitely generated as an R-module. Then M is finitely generated as an R-module. In fact:

$$M = \sum_{i=1}^{m} S x_i, \quad S = \sum_{j=1}^{n} R s_j \Longrightarrow M = \sum_{i=1}^{m} \sum_{j=1}^{n} R s_j x_i.$$

Corollary 2.1.5. *Let R be a subring of S, with $s_1, \ldots, s_n \in S$. If s_1 is integral over R, s_2 is integral over $R[s_1]$, $\ldots$, and s_n is integral over $R[s_1, \ldots, s_{n-1}]$, then $R[s_1, \ldots, s_n]$ is a finitely generated R-module.*

Proof. By induction on n. The case $n = 1$ is part of the above theorem. Assume $n > 1$. Then $R[s_1, \ldots, s_{n-1}]$ is a finitely generated R-module. $R[s_1, \ldots, s_n] = R[s_1, \ldots, s_{n-1}][s_n]$ is a finitely generated $R[s_1, \ldots, s_{n-1}]$-module (by the case $n = 1$, since s_n is integral over $R[s_1, \ldots, s_{n-1}]$). Hence by the above remark $R[s_1, \ldots, s_n]$ is finitely generated as an R-module. □

Corollary 2.1.6. (Transivity of Integral Extensions). *Let $R \subseteq S \subseteq T$ be rings. If S is integral over R and T is integral over S, then T is integral over R.*

Proof. Assume that $t \in T$. Then there exist $n \in \mathbb{N}$ and $a_1, \ldots, a_n \in S$ such that

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

The ring $A = R[a_1, \ldots, a_n]$ is a finitely generated R-module by the above corollary, and $A[t]$ is a finitely generated A-module (since t is integral over A). Hence

$A[t]$ is a finitely generated R-module by the above corollary and therefore t is integral over R by the above theorem (Take $R' = S = A[t]$). □

Remark 2.1.7. Let R be a subring of S and J be an ideal of S. Then it is easy to see that the map

$$\begin{aligned} f : R/J^c &\longrightarrow S/J \\ a + J^c &\longmapsto a + J \end{aligned}$$

is a monomorphism. Thus we can regard R/J^c as a subring of S/J.

Theorem 2.1.8. *Let $R \subseteq S$ be rings, S is integral over R.*
(1) Let J be an ideal of S, and regard R/J^c as a subring of S/J (see the above remark). Then S/J is integral over R/J^c.
(2) Let U be a multiplicatively closed subset of R. Then $U^{-1}S$ is integral over $U^{-1}R$.

Proof. (1): Let $s + J \in S/J$. We must show that $s + J$ is integral over R/J^c. Since $s \in S$ and S is integral over R, we have

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

where $a_i \in R$. Then

$$(s^n + J) + (a_1 s^{n-1} + J) + \cdots + (a_n + J) = 0.$$

Thus

$$(s + J)^n + (a_1 + J)(s + J)^{n-1} + \cdots + (a_n + J) = 0,$$

and hence

$$(s + J)^n + (a_1 + J^c)(s + J)^{n-1} + \cdots + (a_n + J^c) = 0.$$

Therefore $s + J$ is integral over R/J^c.
(2): Let $s/u \in U^{-1}S$ $(s \in S, u \in U)$. Then there is an equation of the form $s^n + a_1 s^{n-1} + \cdots + a_n = 0$, with $a_i \in R$. Thus

$$(s/u)^n + (a_1/u)/(s/u)^{n-1} + \cdots + (a_n/u^n) = 0,$$

which shows that s/u is integral over $U^{-1}R$.

□

Definition 2.1.9. If R is a subring of S, the **integral closure** of R in S is the set $\overline{R}$ of elements of S that are integral over R. We say that R is **integrally closed** in S if $\overline{R} = R$. If we simply say that R is integrally closed without reference to S, we assume that R is an integral domain with fraction field K, and R is integrally closed in K.

Example. A UFD is an integrally closed domain.

Corollary 2.1.10. *Let R be a subring of S.*
(1) $\overline{R}$ is a subring of S which contains R,
(2) $\overline{R}$ is integrally closed in S.

Proof. (1): Note that $R \subseteq \overline{R}$ because each $a \in R$ is a root of $x - a$. If $a, b \in \overline{R}$, then $R[a, b]$ is a finitely generated R-module by Corollary 2.1.5. Hence $a \pm b, ab \in \overline{R}$, by Theorem 2.1.3.
(2): By definition, $R \subseteq \overline{R} \subseteq \overline{\overline{R}}$. By Transivity of Integral Extensions, $\overline{\overline{R}}$ is integral over R, and so $\overline{\overline{R}} \subseteq \overline{R}$. Consequently, $\overline{R} = \overline{\overline{R}}$. □

Theorem 2.1.11. *Let R be a subring of S, and $\overline{R}$ the integral closure of R in S, and U be a multiplicatively closed subset of R. If $\overline{U^{-1}R}$ is the integral closure of $U^{-1}R$ in $U^{-1}S$, then*

$$\overline{U^{-1}R} = U^{-1}\overline{R}.$$

Proof. Since $\overline{R}$ is integral over R, it follows from the above theorem that $U^{-1}\overline{R}$ is integral over $U^{-1}R$ and hence $U^{-1}\overline{R} \subseteq \overline{U^{-1}R}$. Now, let $s/u \in \overline{U^{-1}R}$. We must show that $s/u \in U^{-1}\overline{R}$. There is an equation of the form

$$(s/u)^n + (a_1/u_1)(s/u)^{n-1} + \cdots + (a_n/u_n) = 0,$$

where $a_i \in R$ and $u_i \in U$. Let $u_0 = u_1 \cdots u_n$, and multiply the equation by $(uu_0)^n$ to conclude that

$$(u_0^n s^n/1) + (b_1/1)(u_0^{n-1} s^{n-1}/1) + \cdots + (b_n/1) = 0,$$

where $b_i \in R$. Therefore there exists $v \in U$ such that $v^n(u_0^n s^n + b_1 u_0^{n-1} s^{n-1} + \cdots + b_n) = 0$, so $vu_0 s$ is integral over R. Hence $vu_0 s \in \overline{R}$ and therefore $s/u = vu_0 s/vuu_0 \in U^{-1}\overline{R}$. $\square$

Integral closure is a local property:

Theorem 2.1.12. *Let R be an integral domain. Then the following are equivalent:*
(1) R is integrally closed,
(2) $R_{\mathfrak{p}}$ is integrally closed for all $\mathfrak{p} \in \mathrm{Spec}R$,
(3) $R_{\mathfrak{m}}$ is integrally closed for all $\mathfrak{m} \in \mathrm{Max}R$,

Proof. Let $f : R \longrightarrow \overline{R}$ be the inclusion homomorphism, so that R is integrally closed if and only if f is surjective. By the above theorem, $\overline{R}_{\mathfrak{p}} = \overline{R_{\mathfrak{p}}}$ for all $\mathfrak{p} \in \mathrm{Spec}R$. It follows from Exercise 23 of Chapter 1 that:

$$
\begin{aligned}
R \text{ is integrally closed} &\iff f : R \longrightarrow \overline{R} \text{ is surjective} \\
&\iff f_{\mathfrak{p}} : R_{\mathfrak{p}} \longrightarrow \overline{R}_{\mathfrak{p}} \text{ is surjective for all } \mathfrak{p} \in \mathrm{Spec}R \\
&\iff R_{\mathfrak{p}} \text{ is integrally closed for all } \mathfrak{p} \in \mathrm{Spec}R \\
&\iff f_{\mathfrak{m}} : R_{\mathfrak{m}} \longrightarrow \overline{R}_{\mathfrak{m}} \text{ is surjective for all } \mathfrak{m} \in \mathrm{Max}R \\
&\iff R_{\mathfrak{m}} \text{ is integrally closed for all } \mathfrak{m} \in \mathrm{Max}R.
\end{aligned}
$$

This concludes the proof. $\square$

Exercise 1. (1) Let R be a subring of an integral domain S. Let $\overline{R}$ be the integral closure of R in S. Let f and g be monic polynomials in $S[x]$. If $fg \in \overline{R}[x]$, then both f and g are in $\overline{R}[x]$.
(2) Prove the same result without assuming that S is an integral domain.

Exercise 2. Let R be a subring of a ring S and let $\overline{R}$ be the integral closure of R in S. Prove that $\overline{R}[x]$ is the integral closure of $R[x]$ in $S[x]$.

2.2 The Going Up Theorem

Theorem 2.2.1. *Let $R \subseteq S$ be integral domains, S is integral over R. Then*

$$R \text{ is a field} \Longleftrightarrow S \text{ is a field.}$$

Proof. $\Longrightarrow$: If $0 \neq s \in S$, then there is a relation of the form $s^n + a_1 s^{n-1} + \cdots + a_n = 0$ with $a_i \in R$, and since S is an integral domain, we can assume $a_n \neq 0$. Then

$$s^{-1} = -a_n^{-1}(s^{n-1} + a_1 s^{n-2} + \cdots + a_{n-1}) \in S.$$

$\Longleftarrow$: If $0 \neq a \in R$, then $a^{-1} \in S$, so that there is a relation of the form $a^{-n} + b_1 a^{-n+1} + \cdots + b_n = 0$ with $b_i \in R$. Multiply both sides of this relation by a^{n-1} to get

$$a^{-1} = -(b_1 + b_2 a + \cdots + b_n a^{n-1}) \in R.$$

□

Corollary 2.2.2. *Let R be a subring of the ring S, and suppose that the inclusion homomorphism $\varphi : R \longrightarrow S$ is integral. Let $\mathfrak{q} \in \mathrm{Spec}S$. Then*

$$\mathfrak{q} \in \mathrm{Max}S \Longleftrightarrow \mathfrak{q}^c \in \mathrm{Max}R.$$

Proof. By Theorem 2.1.8, $S/\mathfrak{q}$ is integral over $R/\mathfrak{q}^c$, and both these rings are integral domains. Now by the above theorem we have

$$\mathfrak{q} \in \mathrm{Max}S \Longleftrightarrow S/\mathfrak{q} \text{ is a field} \Longleftrightarrow R/\mathfrak{q}^c \text{ is a field} \Longleftrightarrow \mathfrak{q}^c \in \mathrm{Max}R.$$

This completes the proof. □

Theorem 2.2.3. (The Incomparability Theorem.) *Let R be a subring of the ring S, and suppose that the inclusion homomorphism $\varphi : R \longrightarrow S$ is integral. Suppose that $\mathfrak{q}, \mathfrak{q}' \in \mathrm{Spec}S$ such that $\mathfrak{q} \subseteq \mathfrak{q}'$ and $\mathfrak{q}^c = \mathfrak{q}'^c$. Then $\mathfrak{q} = \mathfrak{q}'$.*

Proof. Let $\mathfrak{p} := \mathfrak{q}^c = \mathfrak{q}'^c$, $U = R \setminus \mathfrak{p}$. Consider the following diagram

$$\begin{array}{ccc} R & \xrightarrow{\varphi} & S \\ \downarrow{\scriptstyle\alpha} & & \downarrow{\scriptstyle\beta} \\ U^{-1}R = R_{\mathfrak{p}} & \xrightarrow{\tau} & U^{-1}S \end{array}$$

We have

$$\varphi^{-1}\beta^{-1}(\mathfrak{q}U^{-1}S) = \varphi^{-1}(\mathfrak{q}) = \mathfrak{p} = \varphi^{-1}(\mathfrak{q}') = \varphi^{-1}\beta^{-1}(\mathfrak{q}'U^{-1}S).$$

From the commutativity of the above diagram, we have

$$\alpha^{-1}\tau^{-1}(\mathfrak{q}U^{-1}S) = \mathfrak{p} = \alpha^{-1}\tau^{-1}(\mathfrak{q}'U^{-1}S).$$

Hence $\tau^{-1}(\mathfrak{q}U^{-1}S) = \mathfrak{p}R_{\mathfrak{p}} = \tau^{-1}(\mathfrak{q}'U^{-1}S)$. Since τ is an integral ring homomorphism and $\mathfrak{p}R_{\mathfrak{p}} \in \text{Max}R_{\mathfrak{p}}$, it follows from the above corollary $\mathfrak{q}U^{-1}S, \mathfrak{q}'U^{-1}S \in \text{Max}U^{-1}S$. But $\mathfrak{q}U^{-1}S \subseteq \mathfrak{q}'U^{-1}S$, and so $\mathfrak{q}U^{-1}S = \mathfrak{q}'U^{-1}S$. Therefore, by the fact that $\mathfrak{q} \cap U = \mathfrak{q}' \cap U = \emptyset$, and Lemma 1.5.10, we deduce that $\mathfrak{q} = \mathfrak{q}'$. □

Remark 2.2.4. The name of the above theorem comes from the following rephrasing of its statement: let R be a subring of the ring S, and suppose that the inclusion homomorphism $\varphi : R \longrightarrow S$ is integral. Two distinct prime ideals of S having the same contraction in R are 'incomparable' in the sense that neither is contained in the other.

Definition 2.2.5. Let $\varphi : R \longrightarrow S$ be the inclusion homomorphism. When $\mathfrak{q} \in \text{Spec}S$ and $\mathfrak{p} = \mathfrak{q}^c = \mathfrak{q} \cap R$, we say that $\mathfrak{q}$ **lies over** $\mathfrak{p}$.

Theorem 2.2.6. (The Lying Over Theorem.) *Let R be a subring of the ring S, and suppose that the inclusion homomorphism $\varphi : R \longrightarrow S$ is integral. Let $\mathfrak{p} \in \text{Spec}R$. Then there exists $\mathfrak{q} \in \text{Spec}S$ such that $\mathfrak{q}^c = \mathfrak{p}$, that is, such that $\mathfrak{q}$ lies over $\mathfrak{p}$.*

Proof. We use similar notation to that use in the proof of the above theorem. Let $\mathfrak{n}$ be a maximal ideal of $U^{-1}S$. Since τ is an integral ring homomorphism, it follows that $\tau^{-1}\mathfrak{n} = \mathfrak{p}R_{\mathfrak{p}}$. If $\mathfrak{q} = \beta^{-1}\mathfrak{n}$, then $\mathfrak{q}$ is prime and we have

$$\mathfrak{q} \cap R = \mathfrak{q}^c = \varphi^{-1}\beta^{-1}\mathfrak{n} = \alpha^{-1}\tau^{-1}\mathfrak{n} = \alpha^{-1}(\mathfrak{p}R_{\mathfrak{p}}) = \mathfrak{p}.$$

□

Theorem 2.2.7. (Going Up Theorem). *Let $\varphi : R \longrightarrow S$ be the inclusion homomorphism, and suppose that φ is integral. Let $m \in \mathbb{N}_0$ and $n \in \mathbb{N}$ with*

$m < n$. Let

$$\mathfrak{p}_0 \subseteq \mathfrak{p}_1 \subseteq \cdots \subseteq \mathfrak{p}_n$$

be a chain of prime ideals of R, and let

$$\mathfrak{q}_0 \subseteq \mathfrak{q}_1 \subseteq \cdots \subseteq \mathfrak{q}_m$$

be a chain of prime ideals of S such that $\mathfrak{q}_i^c = \mathfrak{p}_i\,(0 \leq i \leq m)$. Then the chain $\mathfrak{q}_0 \subseteq \mathfrak{q}_1 \subseteq \cdots \subseteq \mathfrak{q}_m$ can be extended to a chain $\mathfrak{q}_0 \subseteq \mathfrak{q}_1 \subseteq \cdots \subseteq \mathfrak{q}_n$ such that $\mathfrak{q}_i^c = \mathfrak{p}_i\,(0 \leq i \leq n)$.

Proof. By induction we can reduce immediately to the case $m = 0$ and $n = 1$. Consider the following commutative diagram

$$\begin{array}{ccc} R & \xrightarrow{\varphi} & S \\ \Big\downarrow{\scriptstyle\alpha} & & \Big\downarrow{\scriptstyle\beta} \\ R/\mathfrak{p}_0 & \xrightarrow{\tau} & S/\mathfrak{q}_0 \end{array}$$

where $\tau : R/\mathfrak{p}_0 \longrightarrow S/\mathfrak{q}_0$ be the induced homomorphism related to $\varphi : R \longrightarrow S$. Since $\mathfrak{p}_1/\mathfrak{p}_0 \in \mathrm{Spec}R/\mathfrak{p}_0$ and τ is integral ring homomorphism, it follows from the Lying Over Theorem that there exists a prime ideal $\mathfrak{q}_1 \in \mathrm{Spec}S$ with $\mathfrak{q}_1 \supseteq \mathfrak{q}_0$ such that $\tau^{-1}(\mathfrak{q}_1/\mathfrak{q}_0) = \mathfrak{p}_1/\mathfrak{p}_0$. Now, we have

$$\mathfrak{q}_1 \cap R = \mathfrak{q}_1^c = \varphi^{-1}\beta^{-1}(\mathfrak{q}_1/\mathfrak{q}_0) = \alpha^{-1}\tau^{-1}(\mathfrak{q}_1/\mathfrak{q}_0) = \alpha^{-1}(\mathfrak{p}_1/\mathfrak{p}_0) = \mathfrak{p}_1.$$

This completes the proof. □

2.3 The Going Down Theorem

Lemma 2.3.1. *Let R be a subring of the ring S, and suppose that the inclusion homomorphism $\varphi : R \longrightarrow S$ is integral. Let I be an ideal of R. Then*

$$\sqrt{I^e} = \sqrt{IS} = \{s \in S | s^n + a_1 s^{n-1} + \cdots + a_{n-1}s + a_n = 0, \textit{ for some } n \in \mathbb{N}, a_i \in I\}.$$

Proof. $(\supseteq)$: Let $s \in S$ and $s^n + a_1 s^{n-1} + \cdots + a_{n-1}s + a_n = 0$ for some $a_i \in I$. Then $s^n = -(a_1 s^{n-1} + \cdots + a_{n-1}s + a_n) \in I^e$. Hence $s \in \sqrt{I^e}$.

$\subseteq$: Let $s \in \sqrt{I^e}$. Then there exists $a_1, \ldots, a_n \in I$ and $s_1, \ldots, s_n \in S$ such that $s^n = a_1 s_1 + \cdots + a_n s_n$. Since each s_i is integral over R it follows that $M := R[s_1, \ldots, s_n]$ is a finitely generated R-module, and we have $s^n M \subseteq IM$, $\mathrm{Ann}_{R[s^n]} M = 0$. Hence there exist $b_1, \ldots, b_m \in I$ such that

$$(s^n)^m + b_1 (s^n)^{m-1} + \cdots + b_{m-1}(s^n) + b_m = 0.$$

□

Proposition 2.3.2. *Let R be a subring of the ring S, and suppose that the inclusion homomorphism $\varphi : R \longrightarrow S$ is integral, and that R is integrally closed. Let K be the field of fractions of R. Let I be an ideal of R and let $s \in I^e$. Then s is algebraic over K and its minimal polynomial over K has the form*

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

where $a_i \in \sqrt{I}$.

Proof. Clearly s is algebraic over K. Let

$$f = x^n + a_1 x^{n-1} + \cdots + a_n \in K[x]$$

be the minimal polynomial of s over K. We aim to show that $a_1, \ldots, a_n \in \sqrt{I}$. Let F be the splitting field of f over the field of fractions of S. Then there exists $s = s_1, s_2, \ldots, s_n \in F$ such that

$$f = (x - s_1)(x - s_2) \cdots (x - s_n).$$

From the expressions for $a_1, \ldots, a_n$ in terms of the $s_1, \ldots, s_n$, we have $a_1, \ldots, a_n \in R[s_1, \ldots, s_n]$.

By the above lemma, there exist $b_1, \ldots, b_m \in I$ such that

$$s^n + b_1 s^{n-1} + \cdots + b_m = 0.$$

Each s_i is algebraic over K with minimal polynomial f, and so it follows from Algebra II that for each $i = 1, \ldots, n$ there is an isomorphism of fields $\alpha_i : K(s) \longrightarrow K(s_i)$ such that $\alpha_i(s) = s_i$ and $\alpha_i(a) = a$ for all $a \in K$. Hence

$$s_i^n + b_1 s_i^{n-1} + \cdots + b_m = 0$$

for all $i = 1, \dots, n$. In particular, $R[s_1, \dots, s_n]$ is a finitely generated R-module. Since $a_1, \dots, a_n \in R[s_1, \dots, s_n]$, Lemma 2.1.3 implies that $a_1, \dots, a_n$ are all integral over R. But $a_1, \dots, a_n \in K$ and R is integrally closed, hence $a_1, \dots, a_n \in R$.

Let $T := R[s_1, \dots, s_n]$. By the above lemma, $s_1, \dots, s_n \in \sqrt{IT}$. From the expressions for $a_1, \dots, a_n$ in terms of the $s_1, \dots, s_n$, it follows from the above lemma again that each a_i is a root of a monic polynomial in $R[x]$ all of whose coefficients (except leading coefficient) belong to I. Hence, by the above lemma again, and the fact that $a_1, \dots, a_n \in R$, we deduce that $a_1, \dots, a_n \in \sqrt{I}$. □

Theorem 2.3.3. (Going Down Theorem). *Let $\varphi : R \longrightarrow S$ be the inclusion homomorphism, and suppose that φ is integral. Assume that S is integral domain and R is integrally closed. Let $m \in \mathbb{N}_0$ and $n \in \mathbb{N}$ with $m < n$. Let*

$$\mathfrak{p}_0 \supseteq \mathfrak{p}_1 \supseteq \cdots \supseteq \mathfrak{p}_n$$

be a chain of prime ideals of R, and let

$$\mathfrak{q}_0 \supseteq \mathfrak{q}_1 \supseteq \cdots \supseteq \mathfrak{q}_m$$

be a chain of prime ideals of S such that $\mathfrak{q}_i^c = \mathfrak{p}_i \,(0 \leq i \leq m)$. Then the chain $\mathfrak{q}_0 \supseteq \mathfrak{q}_1 \supseteq \cdots \supseteq \mathfrak{q}_m$ can be extended to a chain $\mathfrak{q}_0 \supseteq \mathfrak{q}_1 \supseteq \cdots \supseteq \mathfrak{q}_n$ such that $\mathfrak{q}_i^c = \mathfrak{p}_i \,(0 \leq i \leq n)$.

Proof. By induction, it suffices to consider the case $m = 0$ and $n = 1$. Consider the multiplicatively closed subset

$$U := (R \setminus \mathfrak{p}_2)(S \setminus \mathfrak{q}_1) = \{ab \,|\, a \in R \setminus \mathfrak{p}_2, b \in S \setminus \mathfrak{q}_1\}$$

of S. First we prove the theorem under the assumption that $U \cap \mathfrak{p}_2^e = \emptyset$. Then there exists a prime ideal $\mathfrak{q}_2$ of S such that $\mathfrak{q}_2 \cap U = \emptyset$ and $\mathfrak{p}_2^e \subseteq \mathfrak{q}_2$. Hence $\mathfrak{p}_2 \subseteq \mathfrak{p}_2^{ec} \subseteq q_2^c$, and since $U \cap \mathfrak{p}_2^e = \emptyset$ and $R \setminus \mathfrak{p}_2 \subseteq U$, we must have $\mathfrak{p}_2 = \mathfrak{q}_2^c$. Likewise, since $S \setminus \mathfrak{q}_1 \subseteq U$, we must have $\mathfrak{q}_2 \subseteq \mathfrak{q}_1$.

Finally, we show that $U \cap \mathfrak{p}_2^e = \emptyset$. Let $s \in U \cap \mathfrak{p}_2^e$, and let K be the field of fractions of R. By Proposition 2.3.2, s is algebraic over K and its minimal polynomial over K has the form

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

where $a_1, \ldots, a_n \in \sqrt{\mathfrak{p}_2} = \mathfrak{p}_2$. Since $s \in U$, we can write $s = ab$ for some $a \in R \setminus \mathfrak{p}_2$ and $b \in S \setminus \mathfrak{q}_1$. Clearly

$$x^n + (a_1/a)x^{n-1} + \cdots + (a_n/a^n),$$

is the minimal polynomial of b over K. It now follows from (with $I = R$) that $a_i = d_i a^i$ for some $d_1, \ldots, d_n \in R$. Since $a_i \in \mathfrak{p}_2$ and $a \notin \mathfrak{p}_2$, we have $d_1, \ldots, d_n \in \mathfrak{p}_2$. Hence $b \in \sqrt{\mathfrak{p}_2 S} \subseteq \sqrt{\mathfrak{p}_1 S} \subseteq \mathfrak{q}_1$, which is a contradiction. $\square$

Chapter 3

Dimension Theory

3.1 Dimension Theory

Definition 3.1.1. Let R be a ring.

(1) The **dimension** of R, denoted by $\dim R$, is defined by

$$\dim R = \sup\{n | \exists\ \mathfrak{p}_0, \mathfrak{p}_1, \ldots, \mathfrak{p}_n \in \operatorname{Spec} R \text{ such that } \mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_n\}.$$

(2) Let $\mathfrak{p}$ be a prime ideal of R. The **height** of $\mathfrak{p}$, denoted by $\operatorname{ht}\mathfrak{p}$, is defined by

$$\operatorname{ht}\mathfrak{p} = \sup\{n | \exists\ \mathfrak{p}_0, \mathfrak{p}_1, \ldots, \mathfrak{p}_n \in \operatorname{Spec} R \text{ such that } \mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_n = \mathfrak{p}\}.$$

(3) Let $\mathfrak{a}$ be an ideal of R. The **height** of $\mathfrak{a}$, denoted by $\operatorname{ht}\mathfrak{a}$, is defined by

$$\operatorname{ht}\mathfrak{a} = \min\{\operatorname{ht}\mathfrak{p} | \mathfrak{p} \in \operatorname{Spec} R,\ \mathfrak{a} \subseteq \mathfrak{p}\} = \min\{\operatorname{ht}\mathfrak{p} | \mathfrak{p} \in V(\mathfrak{a})\}.$$

Exercise 1. Let $\mathfrak{a}$ be an ideal of R and $\mathfrak{p} \in \operatorname{Spec} R$. Show that:

(1) $\dim R = \sup\{\operatorname{ht}\mathfrak{p} | \mathfrak{p} \in \operatorname{Spec} R\} = \sup\{\operatorname{ht}\mathfrak{m} | \mathfrak{m} \in \operatorname{Max} R\}$,

(2) $\operatorname{ht}\mathfrak{p} = \dim R_{\mathfrak{p}}$,

(3) $\operatorname{ht}\mathfrak{a} = \min\{\operatorname{ht}\mathfrak{p} | \mathfrak{p} \in \operatorname{Min}(\mathfrak{a})\}$,

(4) $\operatorname{ht}\mathfrak{p} + \dim R/\mathfrak{p} \leq \dim R$.

Definition 3.1.2. Let M be an R-module. The **dimension** of M, denoted by $\dim M$, is defined by

$$\dim M = \sup\{n | \exists\ \mathfrak{p}_0, \mathfrak{p}_1, \ldots, \mathfrak{p}_n \in \operatorname{Supp} M \text{ such that } \mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_n\}.$$

Exercise 2. Let M be an R-module. Show that:

(1) if R is Noetherian, then $\dim M = \sup\{\dim R/\mathfrak{p} \mid \mathfrak{p} \in \mathrm{Ass}(M)\}$,

(2) if M is finitely generated, then $\dim M = \dim R/\mathrm{Ann}(M)$.

Theorem 3.1.3. *Let S be an integral extension over R. Then* $\dim R = \dim S$.

Proof. Let

$$\mathfrak{q}_0 \subset \mathfrak{q}_1 \subset \cdots \subset \mathfrak{q}_n$$

be a chain of prime ideals of S. Then it follows from Incomparability Theorem that

$$\mathfrak{q}_0^c \subset \mathfrak{q}_1^c \subset \cdots \subset \mathfrak{q}_n^c$$

is a chain of prime ideals of R. Hence $\dim S \leq \dim R$.

Now assume that

$$\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_n$$

be a chain of prime ideals of R. By Lying Over Theorem, there exists $\mathfrak{q}_0 \in \mathrm{Spec} S$ such that $\mathfrak{q}_0^c = \mathfrak{p}_0$. It now follows from the Going Up Theorem that there exists a chain

$$\mathfrak{q}_0 \subset \mathfrak{q}_1 \subset \cdots \subset \mathfrak{q}_n$$

of prime ideals of S. Hence $\dim R \leq \dim S$. □

Theorem 3.1.4. (Krull's Principal Ideal Theorem (PIT)). *Let R be a Noetherian ring and $\mathfrak{p}$ be a minimal prime of the principal ideal (a) of R. Then* $\mathrm{ht}\mathfrak{p} \leq 1$.

Proof. We first note that $\mathrm{ht}\mathfrak{p} = \dim R_{\mathfrak{p}}$ and $\mathfrak{p}R_{\mathfrak{p}}$ is a minimal prime ideal of the principal ideal $(a)R_{\mathfrak{p}}$. Thus we may assume that R is a local ring with maximal ideal $\mathfrak{p}$ such that $\mathfrak{p}$ is minimal over a principal ideal (a) of R. Let $\mathfrak{q}$ be any prime ideal of R such that $\mathfrak{q} \subsetneq \mathfrak{p}$. It suffices to show that $\mathrm{ht}\mathfrak{q} = 0$. Consider

$$(a) + \mathfrak{q} \supseteq (a) + \mathfrak{q}^{(2)} \supseteq (a) + \mathfrak{q}^{(3)} \supseteq \cdots,$$

where $\mathfrak{q}^{(n)}$ denotes the nth symbolic power of $\mathfrak{q}$. But $\mathfrak{p}/(a)$ is the only prime ideal of $R/(a)$ since $\mathfrak{p}$ is minimal over (a). Hence $\dim R/(a) = 0$ and so $R/(a)$

is Artinian by Theorem 1.1.3. Hence there is $n \geq 1$ such that $(a) + \mathfrak{q}^{(n)} = (a) + \mathfrak{q}^{(n+1)}$. We claim that $\mathfrak{q}^{(n)} = a\mathfrak{q}^{(n)} + \mathfrak{q}^{(n+1)}$. Clearly $a\mathfrak{q}^{(n)} + \mathfrak{q}^{(n+1)} \subseteq \mathfrak{q}^{(n)}$. Now let $x \in \mathfrak{q}^{(n)}$. Then $x \in (a) + \mathfrak{q}^{(n)} = (a) + \mathfrak{q}^{(n+1)}$, and so we can write $x = ab + y$ for some $b \in R$ and $y \in \mathfrak{q}^{(n+1)}$. Now $ab \in \mathfrak{q}^{(n)}$ and since $a \notin \mathfrak{q}$ and $\mathfrak{q}^{(n)}$ is $\mathfrak{q}$-primary, we see that $b \in \mathfrak{q}^{(n)}$. Thus, $\mathfrak{q}^{(n)} = a\mathfrak{q}^{(n)} + \mathfrak{q}^{(n+1)}$. Hence by by applying Nakayama's Lemma (to the module $\mathfrak{q}^{(n)}/\mathfrak{q}^{(n+1)}$), we obtain $\mathfrak{q}^{(n)} = \mathfrak{q}^{(n+1)}$. It follows from Exercise 2 that $\mathfrak{q}^n R_\mathfrak{q} = \mathfrak{q}^{n+1} R_\mathfrak{q} = \mathfrak{q}(\mathfrak{q}^n R_\mathfrak{q})$. By applying Nakayama's Lemma once again (this time to the $R_\mathfrak{p}$-module $\mathfrak{q}^n R_\mathfrak{q}$), we obtain $\mathfrak{q}^n R_\mathfrak{q} = 0$. This implies that $\mathfrak{q} R_\mathfrak{q}$ is the only prime ideal of $R_\mathfrak{q}$ and $\dim R_\mathfrak{q} = 0$. Hence $\mathrm{ht}\mathfrak{q} = 0$. □

Exercise 3. Let R be a Noetherian ring, and let $\mathfrak{p}, \mathfrak{q} \in \mathrm{Spec}R$. Let $X = \{\mathfrak{p}' \in \mathrm{Spec}R | \mathfrak{p} \subsetneq \mathfrak{p}' \subsetneq \mathfrak{q}\}$. Prove that

$$X \neq \emptyset \Longrightarrow |X| = \infty.$$

The Principal Ideal Theorem lead straightaway to a far-reaching generalization.

Theorem 3.1.5. (Krull's Generalized Principal Ideal Theorem (GPIT)). *Let R be a Noetherian ring and $\mathfrak{p}$ be a minimal prime of an ideal $(a_1, \ldots, a_n)$ of R. Then* $\mathrm{ht}\mathfrak{p} \leq n$.

Proof. By localization at $\mathfrak{p}$, we may again assume R is local with maximal ideal $\mathfrak{p}$ which is minimal over the ideal $(a_1, \ldots, a_n)$ of R. We shall now proceed by induction on n. The case $n = 1$ is the above theorem. Suppose $n > 1$ and the result holds for $n - 1$. Let $\mathfrak{q}$ be any prime ideal of R such that $\mathfrak{q} \subsetneq \mathfrak{p}$ and that there is no prime ideal $\mathfrak{p}'$ of R with $\mathfrak{q} \subsetneq \mathfrak{p}' \subsetneq \mathfrak{p}$. By minimality of $\mathfrak{p}$, we may assume, without loss of generality, that $a_1 \notin \mathfrak{q}$. We note that $\mathfrak{p}$ is minimal prime of $\mathfrak{q} + (a_1)$ and so $\sqrt{\mathfrak{q} + (a_1)} = \mathfrak{p}$. Hence there is an $m \geq 1$ such that $\mathfrak{p}^m \subseteq \mathfrak{q} + (a_1)$. In particular, for $i = 2, \ldots, n$ we can write $a_i^m = y_i + a_1 x_i$ for some $y_i \in \mathfrak{q}$ and $x_i \in R$. Set $J := (y_2 \ldots, y_n)$. It is easy to see that $\mathfrak{p}$ is minimal prime of $J + (a_1)$. Therefore $\mathfrak{p}/J$ is minimal prime over the principal ideal $J + (a_1)/J$ of R/J. Hence $\mathrm{ht}\mathfrak{p}/J \leq 1$, and therefore, $\mathrm{ht}\mathfrak{q}/J \leq 0$. If follows that $\mathfrak{q}$ is a minimal prime of J, and so by induction hypothesis $\mathrm{ht}\mathfrak{q} \leq n-1$. This proves that $\mathrm{ht}\mathfrak{p} \leq n$. $\square$

Exercise 4. Let R be a Noetherian ring, and let $\mathfrak{p}, \mathfrak{q} \in \mathrm{Spec}R$.

(1) Show that $\mathrm{ht}\mathfrak{p} < \infty$. In particular, a local ring has finite dimension.

(2) Let $\mathfrak{p} \subseteq \mathfrak{q}$. Show that $\mathrm{ht}\mathfrak{p} \leq \mathrm{ht}\mathfrak{q}$, and

$$\mathrm{ht}\mathfrak{p} = \mathrm{ht}\mathfrak{q} \Longleftrightarrow \mathfrak{p} = \mathfrak{q}.$$

(3) Let $\mathfrak{a}$ be an ideal of R with $\mathfrak{a} \subseteq \mathfrak{p}$. Show that

$$\mathrm{ht}\mathfrak{a} = \mathrm{ht}\mathfrak{p} \Longrightarrow \mathfrak{p} \in \mathrm{Min}(\mathfrak{a}).$$

There is a useful converse to the Krull's Generalized Principal Ideal Theorem, as follows.

Theorem 3.1.6. (Converse of the GPIT). *Let R be a Noetherian ring and let $\mathfrak{p} \in \mathrm{Spec}R$; suppose that $\mathrm{ht}\mathfrak{p} = n$. Then there exist $a_1, \ldots, a_n \in R$ such that $\mathfrak{p}$ is a minimal prime of $(a_1, \ldots, a_n)$.*

Proof. We use induction on n. If $n = 0$, there is nothing to prove. So suppose, inductively, that $n \geq 1$ and the claim has been proved for smaller values of n. Now let $\mathrm{Min}R = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_m\}$ (see Theorem 1.1.2). But $\mathrm{ht}\mathfrak{p} \geq 1$. So $\mathfrak{p}$ is not contained in any $\mathfrak{p}_i$ and hence $\mathfrak{p} \nsubseteq \bigcup_{i=1}^m \mathfrak{p}_i$. Therefore, there exists $a_1 \in \mathfrak{p} \backslash \bigcup_{i=1}^m \mathfrak{p}_i$. Then $\mathrm{ht}\mathfrak{p}/(a_1) \leq n-1$ and so by the induction hypothesis there exists $a_2, \ldots, a_n \in \mathfrak{p}$ such that $\mathfrak{p}/(a_1)$ is a minimal prime of $(a_2 + (a_1), \ldots, a_n + (a_1))$. It clearly follows that $\mathfrak{p}$ is a minimal prime of $(a_1, \ldots, a_n)$. $\square$

Theorem 3.1.7. *Let R be a Noetherian ring, and let $\mathfrak{a}$ be a proper ideal of R which can be generated by n elements. Let $\mathfrak{p} \in \mathrm{Spec}R$ be such that $\mathfrak{a} \subseteq \mathfrak{p}$. Then*

$$\mathrm{ht}_R\mathfrak{p} - n \leq \mathrm{ht}_{R/\mathfrak{a}}\mathfrak{p}/\mathfrak{a} \leq \mathrm{ht}_R\mathfrak{p}.$$

Proof. It is easy to see that $\mathrm{ht}_{R/\mathfrak{a}}\mathfrak{p}/\mathfrak{a} \leq \mathrm{ht}_R\mathfrak{p}$. Let $\mathfrak{a} = (a_1, \ldots, a_n)$ and $\mathrm{ht}_{R/\mathfrak{a}}\mathfrak{p}/\mathfrak{a} = m$. By the converse of the GPIT, there exist $b_1, \ldots, b_m \in R$ such that $\mathfrak{p}/\mathfrak{a} \in \mathrm{Min}(b_1+\mathfrak{a}, \ldots, b_m+\mathfrak{a})$. It follows that $\mathfrak{p} \in \mathrm{Min}(a_1, \ldots, a_n, b_1, \ldots, b_m)$.

We can deduce from the GPIT that $\mathrm{ht}_R\mathfrak{p} \leq m+n$, and hence $\mathrm{ht}_R\mathfrak{p} - n \leq \mathrm{ht}_{R/\mathfrak{a}}\mathfrak{p}/\mathfrak{a}$. □

Corollary 3.1.8. *Let R be a Noetherian ring, and let $a \in R$ be a non zero divisor. Let $\mathfrak{p} \in \mathrm{Spec}R$ be such that $a \in \mathfrak{p}$. Then*

$$\mathrm{ht}_{R/(a)}\mathfrak{p}/(a) = \mathrm{ht}_R\mathfrak{p} - 1.$$

Proof. It is enough to show that $\mathrm{ht}_{R/(a)}\mathfrak{p}/(a) \neq \mathrm{ht}_R\mathfrak{p}$. If to the contrary $\mathrm{ht}_{R/(a)}\mathfrak{p}/(a) = \mathrm{ht}_R\mathfrak{p} = n$, then there exists the following chain of prime ideals of $R/(a)$

$$\mathfrak{p}_0/(a) \subset \mathfrak{p}_1/(a) \subset \cdots \subset \mathfrak{p}_n/(a) = \mathfrak{p}/(a).$$

Since $\mathrm{ht}_R\mathfrak{p} = n$, we must have $\mathfrak{p}_0 \in \mathrm{Min}R \subseteq \mathrm{Ass}R$. Therefore $a \in Z(R)$, which is a contradiction. □

Lemma 3.1.9. *Let $(R,\mathfrak{m})$ be a local Noetherian ring and let $\mathfrak{a}$ be a proper ideal of R. Then the following are equivalent:*
(1) $\ell_R(R/\mathfrak{a}) < \infty$,
(2) $V(\mathfrak{a}) = \{\mathfrak{m}\}$,
(3) $\mathrm{Min}(\mathfrak{a}) = \{\mathfrak{m}\}$,
(4) $\sqrt{\mathfrak{a}} = \mathfrak{m}$,
(5) there is $n \in \mathbb{N}$ such that $\mathfrak{m}^n \subseteq \mathfrak{a}$,

Proof. (1) $\Longrightarrow$ (2): Since $\ell_R(R/\mathfrak{a}) < \infty$, $R/\mathfrak{a}$ is an Artinian R-module and hence it is also an Artinian ring. It follows that $\mathrm{Spec}R/\mathfrak{a} = \mathrm{Max}R/\mathfrak{a}$ and thus $V(\mathfrak{a}) = \{\mathfrak{m}\}$.
(2) $\Longrightarrow$ (3): is trivial.
(3) $\Longrightarrow$ (4): $\sqrt{\mathfrak{a}} = \bigcap_{\mathfrak{q}\in\mathrm{Min}(\mathfrak{a})}\mathfrak{q} = \mathfrak{m}$.
(4) $\Longrightarrow$ (5): It follows from the fact that R is Noetherian.
(5) $\Longrightarrow$ (1): Since $\mathfrak{m}^n(R/\mathfrak{a}) = 0$, it follows that the R-module $R/\mathfrak{a}$ is both Artinian and Noetherian, and hence $\ell_R(R/\mathfrak{a}) < \infty$. □

Theorem 3.1.10. *Let $(R,\mathfrak{m})$ be a local Noetherian ring. Then*

$$\mathrm{dim}R = \mathrm{Min}\{n \in \mathbb{N}_0 | \exists a_1,\ldots,a_n \in R \text{ such that } \sqrt{(a_1,\ldots,a_n)} = \mathfrak{m}\}.$$

Proof. Let

$$s = \text{Min}\{n \in \mathbb{N}_0 | \exists a_1, \ldots, a_n \in R \text{ such that } \sqrt{(a_1, \ldots, a_n)} = \mathfrak{m}\}.$$

There there exist $a_1, \ldots, a_s \in R$ such that $\sqrt{(a_1, \ldots, a_s)} = \mathfrak{m}$. Then by the above lemma $\mathfrak{m}$ is a minimal prime of $(a_1, \ldots, a_s)$, and so by the GPIT, $\dim R = \text{ht}\mathfrak{m} \leq s$. On the other hand, if $\dim R = \text{ht}\mathfrak{m} = d$, then by the converse of the GPIT, there exist $a_1, \ldots, a_d \in R$ such that $\mathfrak{m}$ is a minimal prime of $(a_1, \ldots, a_d)$. By the above lemma again, we deduce that $\sqrt{(a_1, \ldots, a_d)} = \mathfrak{m}$. This shows that $s \leq \dim R$. □

3.2 Systems of Parameters

We prepare for the study of regular local rings, which play an important role in algebraic geometry.

Theorem 3.1.10 leads us to make the following definition.

Definition 3.2.1. Let $(R, \mathfrak{m})$ be a local ring of dimension d. By a **system of parameters** for R we means elements $a_1, \ldots, a_d \in R$ such that $\sqrt{(a_1, \ldots, a_d)} = \mathfrak{m}$.

Theorem 3.2.2. *Let $(R, \mathfrak{m})$ be a local Noetherian ring, and let $a_1, \ldots, a_n \in \mathfrak{m}$. Then*

$$\dim R - n \leq \dim R/(a_1, \ldots, a_n) \leq \dim R.$$

Moreover, $\dim R/(a_1, \ldots, a_n) = \dim R - n$ *if and only if $a_1, \ldots, a_n$ can be extended to a system of parameters for R.*

Proof. It follows from theorem 3.1.7 that

$$\dim R - n \leq \dim R/(a_1, \ldots, a_n) \leq \dim R.$$

Now let $\mathfrak{a} = (a_1, \ldots, a_n)$ and $d = \dim R$.
$\Longrightarrow$: Suppose that $\dim R/\mathfrak{a} = d - n$. Then $d \geq n$, and by the converse of GPIT, there exist $a_{n+1}, \ldots, a_d \in \mathfrak{m}$ such that $\mathfrak{m}/\mathfrak{a} \in \text{Min}(a_{n+1} + \mathfrak{a}, \ldots, a_d + \mathfrak{a})$. By

Lemma 3.1.9, we have $\sqrt{(a_{n+1}+\mathfrak{a},\ldots,a_d+\mathfrak{a})}=\mathfrak{m}/\mathfrak{a}$. Hence $\sqrt{(a_1,\ldots,a_d)}=\mathfrak{m}$, and therefore $a_1,\ldots,a_d$ is a system of parameters for R.
$\Longleftarrow$: Now suppose that $n\leq d$ and there exist $a_{n+1},\ldots,a_d\in\mathfrak{m}$ such that $a_1,\ldots,a_n,a_{n+1}\ldots,a_d$ form a system of parameters for R. This means that $\sqrt{(a_1,\ldots,a_n,a_{n+1}\ldots,a_d)}=\mathfrak{m}$, so that $\sqrt{(a_{n+1}+\mathfrak{a},\ldots,a_d+\mathfrak{a})}=\mathfrak{m}/\mathfrak{a}$. Hence by the GPIT, we have $\dim R/\mathfrak{a}\leq d-n$. But the result follows from the first part that $d-n\leq\dim R/\mathfrak{a}$. $\square$

The following exercises generalize the concept of system of parameters for modules.

Exercise 5. Let M be a finitely generated module over a local Noetherian ring $(R,\mathfrak{m})$. Show that

$$\dim M=\operatorname{Min}\{n\in\mathbb{N}_0|\exists a_1,\ldots,a_n\in\mathfrak{m}\text{ such that }\ell_R(M/(a_1,\ldots,a_n)M)<\infty\}.$$

Definition 3.2.3. Let $(R,\mathfrak{m})$ be a Noetherian local ring, and let M be a finitely generated R-module with $\dim M=d$. A **system of parameters** for M is a set $\{a_1,\ldots,a_d\}$ of elements of $\mathfrak{m}$ such that

$$\ell_R(M/(a_1,\ldots,a_d)M)<\infty.$$

The above exercise guarantees the existence of such a system.

Exercise 6. Let M be a finitely generated module over a local Noetherian ring $(R,\mathfrak{m})$, and let $a_1,\ldots,a_n\in\mathfrak{m}$. Show that

$$\dim M-n\leq\dim M/(a_1,\ldots,a_n)M\leq\dim M.$$

Moreover, $\dim M/(a_1,\ldots,a_n)M=\dim M-n$ if and only if $a_1,\ldots,a_n$ can be extended to a system of parameters for M.

Exercise 7. Let R be a Noetherian local ring with $\dim R=d$, and let $a_1,\ldots,a_d$ be a system of parameters for R. Let $n_1,\ldots,n_d\in\mathbb{N}$. Prove that $a_1^{n_1},\ldots,a_d^{n_d}$ is a system of parameters for R

We end this section by the Monomial Conjecture of Hochster [6].

Monomial Conjecture. Let R be a Noetherian local ring with $\dim R = d$. Then for any given system of parameters $a_1, \ldots, a_d$ of R

$$a_1^t \ldots a_d^t \notin (a_1^{t+1}, \ldots, a_d^{t+1}) \text{ for all } t \in \mathbb{N}.$$

Monomial Conjecture has also been proved when $\dim R \leq 2$ (cf. [6]). Sharp-Zakeri [13], by using the theory of modules of generalized fractions, proved some results related to Monomial Conjecture for rings of dimension d under the assumption that Monomial Conjecture is valid for rings of dimension $d-1$.

3.3 Regular Rings

Notation. Let M be a finitely generated R-module. The minimum number of generators of M is denoted by $\mu_R(M)$ (or simply by $\mu(M)$).

Theorem 3.3.1. *Let* $(R, \mathfrak{m})$ *be a local Noetherian ring. Then*

$$\dim R \leq \mu(\mathfrak{m}).$$

Proof. Immediate from the GPIT. □

Theorem 3.3.2. *If* $(R, \mathfrak{m})$ *is a local Noetherian ring, then the following conditions are equivalent.*
(1) $\dim R = \mu(\mathfrak{m})$,
(2) $\mathfrak{m}$ *is generated by a system of parameters.*

Proof. (1) $\Longrightarrow$ (2): Is trivial.
(2) $\Longrightarrow$ (1): Suppose that $d = \dim R$ and $\mathfrak{m} = (a_1, \ldots, a_d)$, where $a_1, \ldots, a_d$ is a system of parameters for R. Clearly $\mu(\mathfrak{m}) \leq d$. By the the above theorem, we have $d \leq \mu(\mathfrak{m})$. Hence $d = \mu(\mathfrak{m})$. □

Definition 3.3.3. A local Noetherian ring $(R, \mathfrak{m})$ is said to be **regular** if it satisfies the equivalent conditions of the above theorem. A system of parameters of R which generates $\mathfrak{m}$ is called a **regular system of parameters**.

Definition 3.3.4. Let M be an R-module and let X be a subset of M. We say that X is a **minimal generating set** for M if X generates M but no proper subset of X generates M.

Theorem 3.3.5. *Let M be a module over local ring $(R, \mathfrak{m})$. Let $k = R/\mathfrak{m}$ and $x_1, \ldots, x_n \in M$. Then the following are equivalent:*
(1) $\{x_1, \ldots, x_n\}$ is a minimal generating set for M,
(2) $\{x_1 + \mathfrak{m}M, \ldots, x_n + \mathfrak{m}M\}$ is a basis for k-vector space $M/\mathfrak{m}M$.

Proof. (1) $\Longrightarrow$ (2): We have $(x_1+\mathfrak{m}M, \ldots, x_n+\mathfrak{m}M) = Rx_1+\ldots+Rx_n+\mathfrak{m}M = M/\mathfrak{m}M$. Now let $c_i \in R$ and

$$(c_1 + \mathfrak{m})(x_1 + \mathfrak{m}M) + \cdots + (c_n + \mathfrak{m})(x_n + \mathfrak{m}M) = c_1x_1 + \ldots + c_nx_n + \mathfrak{m}M = 0.$$

If $c_i + \mathfrak{m} \neq 0$ for some $1 \leq i \leq n$, then there exists $d_i \in R$ such that $(c_i+\mathfrak{m})(d_i + \mathfrak{m}) = 1 + \mathfrak{m}$. Hence

$$x_i - d_i(c_1x_1 + \cdots + c_{i-1}x_{i-1} + c_{i+1}x_{i+1} + \cdots + c_nx_n) \in \mathfrak{m}M.$$

This implies that

$$Rx_1 + \cdots + Rx_{i-1} + Rx_i + \cdots + Rx_n + \mathfrak{m}M = Rx_1 + \cdots + Rx_n + \mathfrak{m}M = M.$$

By NAK, $Rx_1 + \cdots + Rx_{i-1} + Rx_{i+1} + \cdots + Rx_n = M$, which is a contradiction. Thus $\{x_1 + \mathfrak{m}M, \ldots, x_n + \mathfrak{m}M\}$ is linearly independent and we have completed the proof.
(2) $\Longrightarrow$ (1): Since $(x_1+\mathfrak{m}M, \ldots, x_n+\mathfrak{m}M) = M/\mathfrak{m}M$, we have $Rx_1+\cdots+Rx_n+\mathfrak{m}M = M$, and therefore $Rx_1 + \cdots + Rx_n = M$, by NAK. Now let $\{y_1, \ldots, y_\ell\}$ be a proper subset of $\{x_1, \ldots, x_n\}$ such that $(y_1, \ldots, y_\ell) = M$. Then

$$(y_1 + \mathfrak{m}M, \ldots, y_\ell + \mathfrak{m}M) = Ry_1 + \cdots + Ry_\ell + \mathfrak{m}M = M/\mathfrak{m}M,$$

which is a contradiction. □

We note an easy consequence of this result.

Corollary 3.3.6. *Let M be a finitely generated module over local ring $(R, \mathfrak{m})$. Let $k = R/\mathfrak{m}$. Then*

(1) M possesses a minimal generating set,

(2) any two minimal generating sets for M have the same cardinality,

(3) $\mu(M) = \dim_k M/\mathfrak{m}M$.

Lemma 3.3.7. *Let $(R, \mathfrak{m})$ be a local Noetherian ring. Let $x \in \mathfrak{m} \setminus \mathfrak{m}^2$. Then*

$$\mu_{R/(x)}(\mathfrak{m}/(x)) = \mu_R(\mathfrak{m}) - 1.$$

Proof. Let $\{a_1 + (x), \ldots, a_n + (x)\}$ be a set of minimal generators of $\mathfrak{m}/(x)$. By Theorem 3.3.5, it suffices to show that $\{a_1+\mathfrak{m}^2, \ldots, a_n+\mathfrak{m}^2, x+\mathfrak{m}^2\}$ is a basis for $R/\mathfrak{m}$-vector space $\mathfrak{m}/\mathfrak{m}^2$. It is easy to see that $(a_1 + \mathfrak{m}^2, \ldots, a_n + \mathfrak{m}^2, x + \mathfrak{m}^2) = \mathfrak{m}/\mathfrak{m}^2$. To show $a_1 + \mathfrak{m}^2, \ldots, a_n + \mathfrak{m}^2, x + \mathfrak{m}^2$ are linearly independent suppose

$$(c_1 + \mathfrak{m})(a_1 + \mathfrak{m}^2) + \cdots + (c_n + \mathfrak{m})(a_n + \mathfrak{m}^2) + (c + \mathfrak{m})(x + \mathfrak{m}^2) = 0, \qquad (*)$$

for some $c_1, \ldots, c_n, c \in R$. This means that

$$(c_1+(x)+\mathfrak{m}/(x))(a_1+(x)+\mathfrak{m}^2/(x))+\cdots+(c_n+(x)+\mathfrak{m}/(x))(a_n+(x)+\mathfrak{m}^2/(x)) = 0.$$

Since $\{a_1 + (x), \ldots, a_n + (x)\}$ is a set of minimal generators of $\mathfrak{m}/(x)$, it follows from Theorem 3.3.5 again that $c_1+(x), \ldots, c_n+(x) \in \mathfrak{m}/(x)$. Hence $c_1, \ldots, c_n \in \mathfrak{m}$. It follows from $(*)$ that $cx \in \mathfrak{m}^2$. Since $x \notin \mathfrak{m}^2$, we must have $c \in \mathfrak{m}$. Therefore $a_1 + \mathfrak{m}^2, \ldots, a_n + \mathfrak{m}^2, x + \mathfrak{m}^2$ are linearly independent, as desired. $\square$

Corollary 3.3.8. *Let $(R, \mathfrak{m})$ be a regular local ring, and let $x \in \mathfrak{m} \setminus \mathfrak{m}^2$. Then $R/(x)$ is a regular local ring and*

$$\dim R/(x) = \dim R - 1.$$

Proof. In view of Theorem 3.1.7, Theorem 3.3.1, Lemma 3.3.7 and the fact that

R is regular, we have

$$\begin{aligned}
\mu_{R/(x)}(\mathfrak{m}/(x)) &\geq \dim R/(x) \\
&= \mathrm{ht}_{R/(x)}(\mathfrak{m}/(x)) \\
&\geq \mathrm{ht}_R\mathfrak{m} - 1 \\
&= \dim R - 1 \\
&= \mu_R(\mathfrak{m}) - 1 \\
&= \mu_{R/(x)}(\mathfrak{m}/(x)),
\end{aligned}$$

from which it is immediate that $R/(x)$ is a regular local ring with dimension $\dim R - 1$. □

The converse of the above corollary is:

Exercise 8. Let $(R, \mathfrak{m})$ be a local Noetherian ring, and x an element of $\mathfrak{m} \setminus \mathfrak{m}^2$ that $x \notin Z(R)$. Let $R/(x)$ be a regular local ring. Show that R is regular.

Theorem 3.3.9. *A regular local ring is an integral domain.*

Proof. Let $(R, \mathfrak{m})$ be a regular local ring. We use induction on $\dim R$. In case $\dim R = 0$, we must have $\mathfrak{m} = 0$, so R is a field, and the result is trivial. Thus we may assume $\dim R \geq 1$. Let $\mathrm{Min} R = \{\mathfrak{p}_1, \dots, \mathfrak{p}_n\}$. By PAT,

$$\mathfrak{m} \not\subseteq \mathfrak{m}^2 \cup \mathfrak{p}_1 \cup \cdots \cup \mathfrak{p}_n.$$

So there exists $x \in \mathfrak{m}$ such that $x \notin \mathfrak{m}^2 \cup \mathfrak{p}_1 \cup \cdots \cup \mathfrak{p}_n$. By Corollary 3.3.8, the local ring $R/(x)$ is regular of dimension $\dim R - 1$. Hence, by induction assumption $R/(x)$ is an integral domain, that is, (x) is a prime ideal and therefore contains a minimal prime ideal of R, say $\mathfrak{p}_1$. If $y \in \mathfrak{p}_1$ is any element, then we may write $y = xa$ for some $a \in R$. Since $x \notin \mathfrak{p}_1$, we must have $a \in \mathfrak{p}_1$. This shows that $\mathfrak{p}_1 = x\mathfrak{p}_1$, which by NAK implies $\mathfrak{p}_1 = 0$, as desired. □

Theorem 3.3.10. *Let $(R, \mathfrak{m})$ be an Noetherian local ring. Then the following are equivalent.*

(1) every non zero ideal of R is principal,

(2) the maximal ideal $\mathfrak{m}$ is principal.

Proof. (1) $\Longrightarrow$ (2): Is trivial.
(2) $\Longrightarrow$ (1): Let $\mathfrak{m} = (x)$. If $\mathfrak{m} = 0$, then R is a field and there is nothing to prove. Therefore we suppose that $\mathfrak{m} \neq 0$. Let $\mathfrak{a}$ be non zero proper ideal of R. By Corollary 1.4.8, we have $\cap_{i=1}^{\infty} \mathfrak{m}^i = 0$ and therefore, there exists $n \in \mathbb{N}$ such that $\mathfrak{a} \subseteq \mathfrak{m}^n$, $\mathfrak{a} \nsubseteq \mathfrak{m}^{n+1}$. Hence, there exists $y \in \mathfrak{a}$ such that $y = ax^n$, $y \notin (x^{n+1})$; consequently $a \notin \mathfrak{m}$ and a is a unit in R. Hence $x^n = a^{-1}y \in \mathfrak{a}$, therefore $\mathfrak{m}^n = (x^n) \subseteq \mathfrak{a}$ and hence $\mathfrak{a} = \mathfrak{m}^n = (x^n)$. It follows that every non zero ideal of R is a power of $\mathfrak{m}$. □

Exercise 9. Let $(R, \mathfrak{m})$ be a local Noetherian integral domain of dimension 1. Show that the following are equivalent.
(1) R is regular,
(2) $\mathfrak{m}$ is principal ideal,
(3) every non zero ideal of R is a power of $\mathfrak{m}$,
(4) there exists $x \in R$ such that every non zero ideal of R has the form x^n, $n \geq 0$,
(5) R is a PID,
(6) R is integrally closed.

Exercise 10. Let R be a Noetherian ring and let $S = R[x_1, \ldots, x_n]$ or $S = R[[x_1, \ldots, x_n]]$. Show that R is regular if and only if S is regular.

At the end of this section, we state without proof results from **Homological Algebra**. The interested reader may refer to Rotman's book [11] for details.

Theorem 3.3.11. (Auslander-Buchsbaum-Nagata). *A regular local ring is UFD.*

Proof. See Theorem 9.64 of [11]. □

There is still no known proof of Theorem 3.3.11 using only classical commutative algebra techniques.

Theorem 3.3.12. (Serre). *Let R be a regular local ring and $\mathfrak{p}$ a prime ideal in R, then $R_{\mathfrak{p}}$ is again regular.*

Proof. See Theorem 9.58 of [11]. □

Chapter 4

Regular Sequences

4.1 Regular Sequences

Definition 4.1.1. Let M be an R-module. An element $a \in R$ is said to be **M-regular** if $a \notin Z(M)$. A sequence of elements $a_1, \dots, a_n \in R$ is called an **M-regular sequence** if
(1) $(a_1, \dots, a_n)M \neq M$, and
(2) for $i = 1 \dots, n$, $a_i \notin Z(M/(a_1, \dots, a_{i-1})M)$.
When all a_i belong to an ideal $\mathfrak{a}$ we say $a_1, \dots, a_n \in R$ is an **M-regular sequence in $\mathfrak{a}$**. If, moreover, there is no $a_{n+1} \in \mathfrak{a}$ such that $a_1, \dots, a_n, a_{n+1}$ is M-regular, then $a_1, \dots, a_n$ is said to be a **maximal M-regular sequence in $\mathfrak{a}$**.

Theorem 4.1.2. *Let R be a Noetherian ring and M an R-module. Any M-regular sequence $a_1, \dots, a_n$ in an ideal $\mathfrak{a}$ can be extended to a maximal M-regular sequence in $\mathfrak{a}$.*

Proof. If $a_1, \dots, a_n$ is not maximal in $\mathfrak{a}$, we can find $a_{n+1} \in \mathfrak{a}$ such that $a_1, \dots, a_n, a_{n+1}$ is an M-regular sequence in $\mathfrak{a}$. Either this process terminates at a maximal M-regular sequence in $\mathfrak{a}$, or it produces a strictly ascending chain of submodules

$$(a_1)M \subsetneq (a_1, a_2)M \subsetneq \cdots .$$

Hence the sequence of ideals

$$(a_1) \subsetneq (a_1, a_2) \subsetneq \cdots$$

is also strictly ascending. Since R is Noetherian, we can exclude this latter possibility. □

The above theorem shows that if R is Noetherian and M a non zero R-module, then maximal M-regular sequence exist. We will prove that all maximal M-regular sequence in an ideal $\mathfrak{a}$ with $\mathfrak{a}M \neq M$ have the same length if M is finitely generated. This allows us to introduce the fundamental notion of grade and depth.

The following simple fact will be repeatedly used throughout this section:

Proposition 4.1.3. *Let M be an R-module and $\mathfrak{a}, \mathfrak{b}$ be two ideals of R. Then*

$$\frac{(M/\mathfrak{a}M)}{\mathfrak{b}(M/\mathfrak{a}M)} \cong \frac{M}{(\mathfrak{a}+\mathfrak{b})M}.$$

Proof. Left to the reader as an exercise. □

Theorem 4.1.4. *Let M be an R-module and $a_1, \ldots, a_n \in R$. Then the following are equivalent.*

(1) $a_1, \ldots, a_n$ is an M-regular sequence.

(2) $a_1, \ldots, a_i$ is an M-regular sequence and $a_{i+1}, \ldots, a_n$ is an $M/(a_1, \ldots, a_i)M$-regular sequence.

Proof. (1) $\Longrightarrow$ (2) : Trivial.

(2) $\Longrightarrow$ (1) : Apply the above proposition with $\mathfrak{a} = (a_1, \ldots, a_i)$ and $\mathfrak{b}$ successively replaced by (a_{i+1}), $(a_{i+1}, a_{i+2}), \ldots$. □

Theorem 4.1.5. *Let M be an R-module and a_1, a_2 be an M-regular sequence. Then $a_1 \notin Z(M/a_2M)$.*

Proof. Suppose that $a_1(x + a_2M) = 0$ for some $x \in M$. Then there exists $y \in M$ such that $a_1x = a_2y$. Since $a_2 \notin Z(M/a_1M)$, this implies $y \in a_1M$, and so $y = a_1y_1$ for some $y_1 \in M$. Since $a_1 \notin Z(M)$, it follows from the equation $a_1x = a_1a_2y_1$ that $x \in a_2M$, as required. □

Theorem 4.1.6. *Let M be an R-module and $a_1, \ldots, a_n$ be an M-regular sequence. Then*
$a_1, \ldots, a_{i-1}, a_{i+1}, a_i, a_{i+2}, \ldots, a_n$ is an M-regular sequence if and only if $a_{i+1} \notin Z(M/(a_1, \ldots, a_{i-1})M)$.

Proof. Follows immediately from Theorem 4.1.4 and 4.1.5. □

Remark 4.1.7. We note that the notion of M-regular sequence depends on the order of the elements in the sequence. In other words, a permutation of a regular sequence need not be regular.

Example 4.1.8. Let $R = k[x, y, z]$, where k is a field. Then $x, y(1-x), z(1-x)$ is an R-regular sequence, but $y(1-x), z(1-x), x$ is not, because $z(1-x) \in Z(R/y(1-x))$.

Theorem 4.1.9. *Let M be a finitely generated module over a Noetherian ring R and let $a_1, \ldots, a_n$ be an M-regular sequence in $J(R)$. Then any permutation of the a_i is also an M-regular sequence.*

Proof. We use induction on n. Let $n = 2$ and a_1, a_2 be an M-regular sequence. We show that a_2, a_1 is also an M-regular sequence. By Theorem 4.1.5, it suffices to show that $a_2 \notin Z(M)$. Let $N = (0 :_M a_2)$. We shall prove $N = 0$. Let $x \in N$. By definition of N, we have $a_2x = 0$. Since $a_2 \notin Z(M/a_1M)$, we have $x \in a_1M$, say $x = a_1y$ with $y \in M$. Then $a_2x = a_1a_2y = 0$. But $a_1 \notin Z(M)$, hence $a_2y = 0$ and therefore $y \in N$. We have proved $N = a_1N$. By NAK, $N = 0$, as desired. Now Let $n > 2$ and $a_1, \ldots, a_n$ be an M-regular sequence. Every permutation is a product of transpositions of adjacent elements. Therefore it is enough to show that $a_1, \ldots, a_{i-1}, a_{i+1}, a_i, a_{i+2}, \ldots, a_n$ is an M-regular sequence. Let $\overline{M} = M/(a_1, \ldots, a_{i-1})M$. By the case $n = 2$, a_{i+1}, a_i is an $\overline{M}$-regular sequence. Hence By the above theorem $a_1, \ldots, a_{i-1}, a_{i+1}, a_i, a_{i+2}, \ldots, a_n$ is an M-regular sequence. □

Let M be a finitely generated module over a Noetherian ring R. In the following theorem, we show that all maximal M-regular sequences in an ideal $\mathfrak{a}$ of R with $\mathfrak{a}M \neq M$ have the same length. This allows us to introduce the fundamental notions of grade and depth.

Theorem 4.1.10. (Rees). *Let M be a finitely generated module over a Noetherian ring R and let $\mathfrak{a}$ be an ideal of R. Assume that $\mathfrak{a}M \neq M$. Then any maximal M-regular sequences in $\mathfrak{a}$ have the same length.*

Proof. It suffices to prove the following: If $a_1, \ldots, a_n$ is a maximal M-regular sequence in $\mathfrak{a}$ and $b_1, \ldots, b_n$ is an M-regular sequence in $\mathfrak{a}$, then $b_1, \ldots, b_n$ is a maximal M-regular sequence in $\mathfrak{a}$. We prove this result by induction on n.

Case $n = 1$. We must show that: If $a_1 \notin Z(M)$, $b_1 \notin Z(M)$ and $\mathfrak{a} \subseteq Z(M/a_1M)$, then $\mathfrak{a} \subseteq Z(M/b_1M)$. By PAT, there exist $x \in M \setminus a_1M$ and $\mathfrak{p} \in \operatorname{Spec} R$ such that $\mathfrak{a} \subseteq \mathfrak{p} = \operatorname{Ann}(x + a_1M)$. Therefore $\mathfrak{a}x \subseteq a_1M$, and so $b_1x = a_1x_1$ for some $x_1 \in M$. We claim that $\mathfrak{a}x_1 \subseteq b_1M$ and $x_1 \notin b_1M$. For the first point, we have $a_1\mathfrak{a}x_1 = b_1\mathfrak{a}x \subseteq a_1b_1M$, and since $a_1 \notin Z(M)$ we must have $\mathfrak{a}x_1 \subseteq b_1M$. For the second point, suppose to the contrary that $x_1 \in b_1M$. Then there exists $x_2 \in M$ such that $x_1 = b_1x_2$. Therefore $b_1x = a_1x_1 = b_1a_1x_2$. Since $b_1 \notin Z(M)$, we must have $x \in a_1M$, which is a contradiction.

Case $n > 1$. Let $K_i = M/(a_1, \ldots, a_{i-1})M$ and $L_i = M/(b_1, \ldots, b_{i-1})M$ for $i = 1 \ldots, n$. It follows from PAT that there is $c \in \mathfrak{a}$ such that

$$c \notin Z(K_1) \cup \cdots \cup Z(K_n) \cup Z(L_1) \cup \cdots \cup Z(L_n). \qquad (*)$$

Since $c \notin Z(K_n)$, we have that $a_1, \ldots, a_{n-1}, c$ is an M-regular sequence in $\mathfrak{a}$. By $(*)$ and repeated application of Theorem 4.1.6, we have that $c, a_1, \ldots, a_{n-1}$ is an M-regular sequence in $\mathfrak{a}$. In exactly the same way, we have that $c, b_1, \ldots, b_{n-1}$ is an M-regular sequence in $\mathfrak{a}$. By the case $n = 1$, c is also a maximal K_n-regular sequence, and hence $c, a_1, \ldots, a_{n-1}$ is a maximal M-regular sequence in $\mathfrak{a}$. Let $N = M/cM$. Then $a_1, \ldots, a_{n-1}$ and $b_1, \ldots, b_{n-1}$ are two N-regular sequences in $\mathfrak{a}$. Since $a_1, \ldots, a_{n-1}$ is a maximal N-regular sequence in $\mathfrak{a}$, it follows from the induction hypothesis that $b_1, \ldots, b_{n-1}$ is a maximal N-regular sequence in $\mathfrak{a}$. Therefore $b_1, \ldots, b_{n-1}, c$ is a maximal M-regular sequence in $\mathfrak{a}$. By the another application of the case $n = 1$, we obtain that b_n is a maximal L_n-regular, and hence $b_1, \ldots, b_{n-1}, b_n$ is a maximal M-regular sequence in $\mathfrak{a}$, as required. □

Remark 4.1.11. For an alternative homological proof, see for example [9].

Exercise 1. Let R be a Noetherian local ring and M a finitely generated R-module. Let $a_1, \ldots, a_n$ be an M-regular sequence. Then

$$\dim M/(a_1, \ldots, a_n)M = \dim M - n.$$

4.2 Grade and Depth

Definition 4.2.1. Let M be a finitely generated module over a Noetherian ring R, and let $\mathfrak{a}$ be an ideal of R such that $\mathfrak{a}M \neq M$. Then the common length of the maximal M-regular sequence in $\mathfrak{a}$ is called the **grade** of $\mathfrak{a}$ on M, denoted by

$$\mathrm{grade}(\mathfrak{a}, M).$$

If $(R, \mathfrak{m})$ is a local ring, then the grade of $\mathfrak{m}$ on M is called the **depth** of M, denoted by

$$\mathrm{depth} M.$$

Exercise 2. Let $\mathfrak{a}$ and $\mathfrak{b}$ be ideals of a Noetherian ring R, M a finite R-module. Show that

(1) $\mathrm{grade}(\mathfrak{a}, M) = \inf\{\mathrm{depth} M_{\mathfrak{p}} : \mathfrak{p} \in V(\mathfrak{a})\}$,

(2) $\mathrm{grade}(\mathfrak{a}, M) = \mathrm{grade}(\sqrt{\mathfrak{a}}, M)$,

(3) $\mathrm{grade}(\mathfrak{a}\mathfrak{b}, M) = \mathrm{grade}(\mathfrak{a} \cap \mathfrak{b}, M) = \inf\{\mathrm{grade}(\mathfrak{a}, M), \mathrm{grade}(\mathfrak{b}, M)\}$,

(4) if S is a multiplicatively closed subset of R, then

$$\mathrm{grade}(\mathfrak{a}, M) \leq \mathrm{grade}(S^{-1}\mathfrak{a}, S^{-1}M),$$

(5) if $a_1, \dots, a_n$ is an M-regular sequence in $\mathfrak{a}$, then

$$\begin{aligned}\operatorname{grade}(\mathfrak{a}, M) - n &= \operatorname{grade}(\mathfrak{a}, M/(a_1, \dots, a_n)M) \\ &= \operatorname{grade}(\mathfrak{a}/(a_1, \dots, a_n), M/(a_1, \dots, a_n)M).\end{aligned}$$

We end this section by establishing an upper bound for depth$M$. We need the following theorem.

Theorem 4.2.2. *Let $(R, \mathfrak{m})$ be a Noetherian local ring and let M be a non zero finitely generated R-module. Then*

$$\operatorname{depth} M \leq \dim R/\mathfrak{p} \ \textit{ for all } \mathfrak{p} \in \operatorname{Ass}(M).$$

Proof. We use induction on $n = \operatorname{depth} M$. If $n = 0$ there is nothing to prove. If $n > 0$, then there an element $a \in \mathfrak{m}$ such that $a \notin Z(M)$. Let $\mathfrak{p} \in \operatorname{Ass} M$ and set

$$\Sigma = \{Rz | 0 \neq z \in M, \ \mathfrak{p}z = 0\}.$$

$\Sigma \neq \emptyset$, since $\mathfrak{p} \in \operatorname{Ass} M$. Let Rz_0 be a maximal element of Σ. We aim to show that $z_0 \notin aM$. If to the contrary that $z_0 \in aM$, then $z_0 = ay$ with $y \in M$ and $\mathfrak{p}y = 0$, since $a \notin Z(M)$. It follows that $Ry \in \Sigma$. By maximality of Rz_0, we have $Ry = Rz_0$ and hence $Ry = Ray$. By NAK, we have $y = 0$, which is a contradiction. Therefore $z_0 \notin aM$ and hence $\mathfrak{p} \subseteq Z(M/aM)$. By PAT, there exists $\mathfrak{q} \in \operatorname{Ass}(M/aM)$ such that $\mathfrak{p} \subseteq \mathfrak{q}$. Since $a \in \mathfrak{q}$ and $a \notin \mathfrak{p}$, we have $\mathfrak{p} \neq \mathfrak{q}$, and therefore by induction hypothesis

$$\operatorname{depth} M = 1 + \operatorname{depth} M/aM \leq 1 + \dim R/\mathfrak{q} \leq \dim R/\mathfrak{p}.$$

□

Corollary 4.2.3. *Let M be a non zero finitely generated module over the Noetherian local ring R. Then*

$$\operatorname{depth} M \leq \dim M.$$

Proof. By the above theorem, we have

$$\operatorname{depth} M \leq \sup\{\dim R/\mathfrak{p} | \mathfrak{p} \in \operatorname{Ass} M\} = \dim M.$$

□

Corollary 4.2.4. *Let R be a Noetherian ring and $\mathfrak{a}$ an ideal of R. Then*

$$\text{grade}(\mathfrak{a}, R) \leq \text{ht}\mathfrak{a}.$$

Proof. Since

$$\begin{aligned} \text{grade}(\mathfrak{a}, R) &= \inf\{\text{depth}R_\mathfrak{p} : \mathfrak{p} \in V(\mathfrak{a})\}, \\ \text{ht}\mathfrak{a} &= \inf\{\dim R_\mathfrak{p} : \mathfrak{p} \in V(\mathfrak{a})\}, \end{aligned}$$

the assertion follows from the above corollary. □

4.3 Cohen-Macaulay Rings and Modules

Over the past several decades Cohen-Macaulay rings have played a central role in the solutions to many important problems in commutative algebra, algebraic geometry, invariant theory and combinatorics. In the words of Hochster, "life is really worth living" in a Cohen-Macaulay ring (see [4], p. 57).

Definition 4.3.1. Let $(R, \mathfrak{m})$ be a Noetherian local ring and M is a non zero finitely generated R-module. We say that M is **Cohen-Macaulay** module (abbreviated to C-M module) if $\text{depth}M = \dim M$. If R is a Cohen-Macaulay R-module then R is called a **Cohen-Macaulay ring**. We say M is maximal Cohen-Macaulay if $\dim M = \dim R$.

Definition 4.3.2. Let R be Noetherian ring and M an R-module. We say that M is a Cohen-Macaulay R-module if $M_\mathfrak{m}$ is a Cohen-Macaulay $R_\mathfrak{m}$-module for each maximal ideal $\mathfrak{m} \in \text{Supp}M$.

Theorem 4.3.3. *Let $(R, \mathfrak{m})$ be a Noetherian local ring and M a non zero Cohen-Macaulay module. Then*
(1) $\text{depth}M = \dim R/\mathfrak{p}$ *for all* $\mathfrak{p} \in \text{Ass}M$,
(2) $\text{grade}(\mathfrak{a}, M) = \dim M - \dim M/\mathfrak{a}M$ *for all ideals* $\mathfrak{a} \subseteq \mathfrak{m}$,
(3) $a_1, \ldots, a_n$ *is an M-regular sequence* $\Longleftrightarrow \dim M/(a_1, \ldots, a_n)M = \dim M - n$,

(4) $a_1, \ldots, a_n$ is an M-regular sequence if and only if it is part of a system of parameters.

Proof. (1): In view of Theorem 4.2.2, $\text{depth} M \leq \dim R/\mathfrak{p} \leq \dim M$ for all $\mathfrak{p} \in \text{Ass} M$. Since M is Cohen-Macaulay, it follows that $\text{depth} M = \dim R/\mathfrak{p}$ for all $\mathfrak{p} \in \text{Ass} M$.

(2) We use induction on $n = \text{grade}(\mathfrak{a}, M)$. If $n = 0$, then there exists $\mathfrak{p} \in \text{Ass} M$ such that $\mathfrak{a} \subseteq \mathfrak{p}$. It follows from (1) that

$$\dim R/\mathfrak{p} \leq \dim M/\mathfrak{a}M \leq \dim M \leq \dim R/\mathfrak{p}.$$

Hence $\dim M/\mathfrak{a}M = \dim M$. If $n > 0$, we choose $x \in \mathfrak{a}$ such that $x \notin Z(M)$. Then

$$\begin{aligned} \text{grade}(\mathfrak{a}, M/xM) &= \text{grade}(\mathfrak{a}, M) - 1, \\ \text{depth}(M/xM) &= \text{depth}(M) - 1, \\ \dim(M/xM) &= \dim(M) - 1. \end{aligned}$$

The argument is complete by induction.

(3) It is enough to prove this when $n = 1$.

$\Longrightarrow$: Follows from Exercise 1.

$\Longleftarrow$: Let $a_1 \in R$ and $\dim(M/a_1M) = \dim M - 1$. Assume to the contrary that $a_1 \in Z(M)$. Then there exists $\mathfrak{p} \in \text{Ass} M$ such that $a_1 \in \mathfrak{p}$. Therefore

$$\dim M = \dim R/\mathfrak{p} \leq \dim M/a_1M,$$

which is a contradiction. Hence a_1 is M-regular.

(4) Follows from an Exercise 6 of Chapter 3 and part (3) above. □

Theorem 4.3.4. *Let R be a Noetherian ring and M a finitely generated R-module. Let $a_1, \ldots, a_n$ be an M-regular sequence. Then*

$$M \text{ is Cohen-Macaulay} \Longrightarrow M/(a_1, \ldots, a_n)M \text{ is Cohen-Macaulay},$$

The converse holds if R is local.

Proof. By the definition of Cohen-Macaulay module, we may assume that R is local. Let $a_1, \ldots, a_n$ be an M-regular sequence. Then

$$\begin{aligned} \text{depth}(M/(a_1, \ldots, a_n)M) &= \text{depth}(M) - n, \\ \dim(M/(a_1, \ldots, a_n)M) &= \dim(M) - n. \end{aligned}$$

Thus M is Cohen-Macaulay, if and only if $M/(a_1, \ldots, a_n)M$ is so. □

Theorem 4.3.5. *Let M be a Cohen-Macaulay module over Noetherian local ring $(R, \mathfrak{m})$. Then*
(1) $M_\mathfrak{p}$ is Cohen-Macaulay $R_\mathfrak{p}$-module for every $\mathfrak{p} \in \text{Spec}R$,
(2) $\text{grade}(\mathfrak{p}, M) = \text{depth}M_\mathfrak{p}$ for every $\mathfrak{p} \in \text{Supp}M$.

Proof. (1): If $M_\mathfrak{p} = 0$, there is nothing to prove. So let $\mathfrak{p} \in \text{Supp}M$. We know

$$\text{grade}(\mathfrak{p}, M) \leq \text{depth}M_\mathfrak{p} \leq \dim M_\mathfrak{p}.$$

So we will prove $\text{grade}(\mathfrak{p}, M) = \dim M_\mathfrak{p}$ by induction on $\text{grade}(\mathfrak{p}, M)$. If $\text{grade}(\mathfrak{p}, M) = 0$, then $\mathfrak{p} \subseteq Z(M)$. By PAT there exists $\mathfrak{p}' \in \text{Ass}M$ such that $\text{Ann}M \subseteq \mathfrak{p} \subseteq \mathfrak{p}'$. Since M is Cohen-Macaulay, it follows from Theorems 1.7.3(4) and 4.3.3(1) that

$$\text{Ass}M = \text{Min}(\text{Ass}M) = \text{Min}(\text{Supp}M).$$

Hence $\mathfrak{p} = \mathfrak{p}' \in \text{Min}(\text{Supp}M)$. Therefore $\mathfrak{p}R_\mathfrak{p} \in \text{Min}(\text{Supp}M_\mathfrak{p})$ and hence $\dim M_\mathfrak{p} = 0$. Now let $\text{grade}(\mathfrak{p}, M) > 0$. Let $a \in \mathfrak{p}$ be an M-regular element. The element $a/1 \in R_\mathfrak{p}$ is then $M_\mathfrak{p}$-regular and therefore we have

$$\begin{aligned} &\dim(M/aM)_\mathfrak{p} = \dim M_\mathfrak{p}/aM_\mathfrak{p} = \dim M_\mathfrak{p} - 1 \\ &\text{grade}(\mathfrak{p}, M/aM) = \text{grade}(\mathfrak{p}, M) - 1. \end{aligned}$$

Since M/aM is Cohen-Macaulay, it follows by induction that $\text{grade}(\mathfrak{p}, M/aM) = \dim(M/aM)_\mathfrak{p}$, which completed the proof.
(2): follows from the proof of (1). □

Exercise 3. Let R be a Noetherian ring. Suppose M is is Cohen-Macaulay R-module and S is a multiplicatively closed set in R. Show that $S^{-1}M$ is a Cohen-Macaulay $S^{-1}R$-module.

Corollary 4.3.6. *Let R be local Noetherian and M a Cohen-Macaulay R-module. Then* $\dim M = \dim M_{\mathfrak{p}} + \dim M/\mathfrak{p}M$ *for every* $\mathfrak{p} \in \mathrm{Supp} M$.

Proof. Let $\mathfrak{p} \in \mathrm{Supp} M$. Then $M_{\mathfrak{p}}$ is Cohen-Macaulay $R_{\mathfrak{p}}$-module and by Theorems 4.3.5 and 4.3.3(2), we have,

$$\dim M_{\mathfrak{p}} = \mathrm{depth} M_{\mathfrak{p}} = \mathrm{grade}(\mathfrak{p}, M) = \dim M - \dim M/\mathfrak{p}M.$$

This completes the proof. □

Corollary 4.3.7. *Let R be a Cohen-Macaulay ring and $\mathfrak{a}$ be a proper ideal of R. Then* $\mathrm{grade}(\mathfrak{a}, R) = \mathrm{ht}\mathfrak{a}$. *If R is Cohen-Macaulay local, then*

$$\mathrm{ht}\mathfrak{a} + \dim R/\mathfrak{a} = \dim R.$$

Proof. We have

$$\begin{aligned} \mathrm{grade}(\mathfrak{a}, R) &= \inf\{\mathrm{depth} R_{\mathfrak{p}} : \mathfrak{p} \in V(\mathfrak{a})\}, \\ \mathrm{ht}\mathfrak{a} &= \inf\{\dim R_{\mathfrak{p}} : \mathfrak{p} \in V(\mathfrak{a})\}. \end{aligned}$$

By Theorem 4.3.5, $\mathrm{grade}(\mathfrak{a}, R) = \mathrm{ht}\mathfrak{a}$. By this and Theorem 4.3.3, $\mathrm{ht}\mathfrak{a} + \dim R/\mathfrak{a} = \dim R$. □

Definition 4.3.8. Let R be a Noetherian ring and $\mathfrak{a}$ a proper ideal, and let $\mathrm{Ass}_R(R/\mathfrak{a}) = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$. We say that $\mathfrak{a}$ is **unmixed** if $\mathrm{ht}\mathfrak{p}_i = \mathrm{ht}\mathfrak{a}$ for all i.

Exercise 4. Let R be a Noetherian ring. Then the following are equivalent.
(1) R is a Cohen-Macaulay ring,
(2) $R_{\mathfrak{p}}$ is a Cohen-Macaulay ring for all $\mathfrak{p} \in \mathrm{Spec}(R)$,
(3) every ideal $\mathfrak{a}$ generated by $\mathrm{ht}\mathfrak{a}$ elements is unmixed,
(4) $\mathrm{grade}(\mathfrak{a}, R) = \mathrm{ht}\mathfrak{a}$ for all ideals $\mathfrak{a}$ of R,
(5) $\mathrm{grade}(\mathfrak{p}, R) = \mathrm{ht}\mathfrak{p}$ for all $\mathfrak{p} \in \mathrm{Spec}(R)$,
(6) $\mathrm{grade}(\mathfrak{m}, R) = \mathrm{ht}\mathfrak{m}$ for all $\mathfrak{m} \in \mathrm{Max}(R)$,
(7) all ideal $\mathfrak{a}$ of R which satisfy the condition $\mathrm{ht}\mathfrak{a} = \mu(\mathfrak{a})$ are generated by an R-regular sequence,
(8) every ideal $\mathfrak{a}$ generated by an R-regular sequence is unmixed,

(9) for any prime ideal $\mathfrak{p}$ of R of height≥ 1 there exists a set of parameters of the ring $R_{\mathfrak{p}}$ which is an R-regular sequence.

Exercise 5. Let R be a Noetherian ring and let $S = R[x_1, \dots, x_n]$ or $S = R[[x_1, \dots, x_n]]$. Show that R is a Cohen-Macaulay ring if and only if S is a Cohen-Macaulay ring.

Our next goal is to show that a regular local ring is Cohen-Macaulay.

Theorem 4.3.9. *Let $(R, \mathfrak{m})$ be a regular local ring of dimension d, and let $a_1, \dots, a_t \in \mathfrak{m}$, where $1 \leq t \leq d$. Then the following are equivalent.*
(1) $a_1, \dots, a_t$ can be extended to a regular system of parameters for R,
(2) $R/(a_1, \dots, a_t)$ is a regular local ring of dimension $d - t$.

Proof. (1) $\Longrightarrow$ (2): Let $\mathfrak{a} = (a_1, \dots, a_t)$. Let $a_1, \dots, a_t, a_{t+1}, \dots, a_d$ be a regular system of parameters for R. By Theorem 3.2.2, dim$R/\mathfrak{a} = d - t$. But $\mathfrak{m}/\mathfrak{a} = (a_{t+1} + \mathfrak{a}, \dots, a_d + \mathfrak{a})$, hence $R/\mathfrak{a}$ is regular.
(2) $\Longrightarrow$ (1): Let $(a_{t+1} + \mathfrak{a}, \dots, a_d + \mathfrak{a}) = \mathfrak{m}/\mathfrak{a}$. Then it is easy to see that $(a_1, \dots, a_t, a_{t+1}, \dots, a_d) = \mathfrak{m}$. Thus $a_1, \dots, a_t$ extend to a regular system of parameters for R. □

Theorem 4.3.10. *Let $(R, \mathfrak{m})$ be a Noetherian local ring of dimension d. Then the following are equivalent.*
(1) R is regular,
(2) $\mathfrak{m}$ can be generated by an R-regular sequence $a_1, \dots, a_d$.

Proof. (1) $\Longrightarrow$ (2): Let $\mathfrak{m} = (a_1, \dots, a_d)$ and $1 \leq i \leq d$. By the above theorem $R/(a_1, \dots, a_i)$ is regular. Therefore $R/(a_1, \dots, a_i)$ is domain and a_{i+1} is not zero divisor of $R/(a_1, \dots, a_i)$. Thus $a_1, \dots, a_t$ is an R-regular sequence.
(2) $\Longrightarrow$ (1): Trivial. □

Corollary 4.3.11. *A regular local ring is Cohen-Macaulay.*

Proof. Let R be a regular local ring. Let $d = \dim R$ and $\mathfrak{m} = (a_1, \ldots, a_d)$, where $a_1, \ldots, a_d$ is an R-regular sequence. By definition of depth, $d \leq \operatorname{depth} R$. It follows from Corollary 4.2.3 that $d = \operatorname{depth} R$, so R is Cohen-Macaulay. □

For more detailed texts on commutative algebra, we refer the interested reader to [2], [5], [8] and [9].

Bibliography

[1] Anderson, D. D. *A note on minimal prime ideals.* Proc. Amer. Math. Soc. **122**(1994), 13-14.

[2] Atiyah, M. F., MacDonald, I. G. (1969). *Introduction to Commutative Algebra.* Addison-Wesley.

[3] Bourbaki, N. (1972). *Commutative Algebra.* Hermann.

[4] Bruns, W., Herzog, J. (1993). *Cohen-Macaulay Rings.* Cambridge: Cambridge University Press.

[5] Eisenbud, D. (1995). *Commutative Algebra with a View Toward Algebraic Geometry.* Springer-Verlag.

[6] Hochster, M. (1973). *Contracted ideals from integral extensions of regular rings.* Nagoya Math. J., **51**, 25-43.

[7] Hoffman, K., Kunze, R. (1971). *Linear Algebra.* Prentice-Hall.

[8] Kaplansky, I. (1974). *Commutative Rings.* The University of Chicago Press.

[9] Matsumura, H. (1986). *Commutative Ring Theory.* Cambridge: Cambridge University Press.

[10] Naghipour, A. R. *Advanced Algebra.* Notes in preparation.

[11] Rotman, J. (1979). *An Introduction to Homological Algebra*. Academic Press. New York. San Francisco. London.

[12] Sharp, R. Y. (2000). *Steps in Commutative Algebra*. Cambridge: Cambridge University Press.

[13] Sharp, R. Y., Zakeri, H. (1985). *Generalized fractions and the monomial conjecture*. J. Algebra, (2)92, 380-388.