Communicative Algebra $\sim \bigstar$

Renko Usami

2077.1.1

Contents

Chapter 1

Basic Properties of Rings and Ideals

Throughout this chapter, unless otherwise stated, all rings are assumed to be commutative with identity.

1.1 Nilpotents and Radicals

Definition 1.1. Let A be a ring. An element $a \in A$ is called *nilpotent* if there exists an integer $n > 0$ such that

$$a^n = 0.$$

Proposition 1.2. *Let A be a commutative ring. The set*

$$\mathrm{Nil}(A) = \{x \in A \mid x^n = 0 \text{ for some } n > 0\}$$

of all nilpotent elements of A is an ideal of A.

Proof. Let $x, y \in \mathrm{Nil}(A)$. Suppose $x^n = 0$ and $y^m = 0$. For $r \in A$,

$$(rx)^n = r^n x^n = 0,$$

so $rx \in \mathrm{Nil}(A)$. Also,

$$(x+y)^{n+m-1} = \sum_{i=0}^{n+m-1} \binom{n+m-1}{i} x^i y^{n+m-1-i}.$$

For each term in the sum, either $i \geq n$ or $n+m-1-i \geq m$. Hence each term is zero. Thus $x+y$ is nilpotent. Therefore $\mathrm{Nil}(A)$ is an ideal. □

Definition 1.3. The ideal $\mathrm{Nil}(A)$ is called the *nilradical* of A.

Proposition 1.4. *The nilradical of A is the intersection of all prime ideals of A:*

$$\mathrm{Nil}(A) = \bigcap_{\mathfrak{p} \in \mathrm{Spec}\, A} \mathfrak{p}.$$

Proof. Let $x \in \mathrm{Nil}(A)$, say $x^n = 0$. If $\mathfrak{p}$ is a prime ideal, then $0 \in \mathfrak{p}$, hence $x^n \in \mathfrak{p}$, so $x \in \mathfrak{p}$. Thus

$$\mathrm{Nil}(A) \subseteq \bigcap_{\mathfrak{p} \in \mathrm{Spec}\, A} \mathfrak{p}.$$

Conversely, suppose $f \notin \mathrm{Nil}(A)$. Consider the set of ideals

$$\Sigma = \{I \subseteq A \mid f^n \notin I \text{ for all } n \geq 1\}.$$

This set is nonempty since $(0) \in \Sigma$, and it is inductive under inclusion. By Zorn's lemma, Σ has a maximal element $\mathfrak{p}$.

We claim that $\mathfrak{p}$ is prime. Suppose $xy \in \mathfrak{p}$ but $x \notin \mathfrak{p}$ and $y \notin \mathfrak{p}$. Then by maximality of $\mathfrak{p}$, the ideals $\mathfrak{p} + (x)$ and $\mathfrak{p} + (y)$ are not in Σ. Hence there exist $m, n > 0$ such that

$$f^m \in \mathfrak{p} + (x), \qquad f^n \in \mathfrak{p} + (y).$$

Write

$$f^m = p_1 + ax, qquadf^n = p_2 + by$$

with $p_1, p_2 \in \mathfrak{p}$ and $a, b \in A$. Then

$$f^{m+n} = (p_1 + ax)(p_2 + by) \in \mathfrak{p},$$

since $xy \in \mathfrak{p}$. This contradicts $\mathfrak{p} \in \Sigma$. Therefore $\mathfrak{p}$ is prime.

Since $f \notin \mathfrak{p}$, f is not contained in the intersection of all prime ideals. Hence

$$\bigcap_{\mathfrak{p} \in \mathrm{Spec}\, A} \mathfrak{p} \subseteq \mathrm{Nil}(A).$$

□

1.2 The Jacobson Radical

Definition 1.5. The *Jacobson radical* of A, denoted $\mathrm{Jac}(A)$, is the intersection of all maximal ideals of A:

$$\mathrm{Jac}(A) = \bigcap_{\mathfrak{m} \in \mathrm{Max}\, A} \mathfrak{m}.$$

Proposition 1.6. *An element $x \in A$ lies in $\mathrm{Jac}(A)$ if and only if $1 - xy$ is a unit in A for every $y \in A$.*

Proof. Suppose $1 - xy$ is not a unit for some $y \in A$. Then $(1 - xy)$ is contained in some maximal ideal $\mathfrak{m}$. If $x \in \mathrm{Jac}(A)$, then $x \in \mathfrak{m}$, so $xy \in \mathfrak{m}$. Therefore

$$1 = (1 - xy) + xy \in \mathfrak{m},$$

a contradiction. Hence $x \notin \mathrm{Jac}(A)$.

Conversely, suppose $x \notin \mathrm{Jac}(A)$. Then $x \notin \mathfrak{m}$ for some maximal ideal $\mathfrak{m}$. Since $\mathfrak{m} + (x) = A$, there exist $y \in A$ and $m \in \mathfrak{m}$ such that

$$xy + m = 1.$$

Thus $1 - xy = m \in \mathfrak{m}$, so $1 - xy$ is not a unit. This proves the equivalence. □

1.3 Direct Sums and Direct Products

As in module theory, we can define direct sums and direct products of ideals. For a family of ideals $(\mathfrak{a}_i)_{i\in I}$, we set

$$\prod_{i\in I}\mathfrak{a}_i = \{(x_i)_{i\in I} \mid x_i \in \mathfrak{a}_i\},$$

and

$$\bigoplus_{i\in I}\mathfrak{a}_i = \{(x_i)_{i\in I} \in \prod_{i\in I}\mathfrak{a}_i \mid x_i = 0 \text{ for all but finitely many } i\}.$$

If I is finite, then the direct sum and direct product coincide.

1.4 Coprime Ideals and the Chinese Remainder Theorem

Definition 1.7. Two ideals $\mathfrak{a}, \mathfrak{b} \subseteq A$ are called *coprime* if

$$\mathfrak{a} + \mathfrak{b} = A.$$

Proposition 1.8. *If $\mathfrak{a}$ and $\mathfrak{b}$ are coprime ideals, then*

$$\mathfrak{a} \cap \mathfrak{b} = \mathfrak{a}\mathfrak{b}.$$

Proof. Clearly $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{a} \cap \mathfrak{b}$. Conversely, since $\mathfrak{a} + \mathfrak{b} = A$, there exist $y \in \mathfrak{a}$ and $z \in \mathfrak{b}$ such that

$$y + z = 1.$$

If $x \in \mathfrak{a} \cap \mathfrak{b}$, then

$$x = x(y + z) = xy + xz.$$

Here $xy \in \mathfrak{b}\mathfrak{a}$ and $xz \in \mathfrak{a}\mathfrak{b}$. Hence $x \in \mathfrak{a}\mathfrak{b}$. □

Theorem 1.9. *A maximal ideal is a prime ideal.*

Proof. Let $\mathfrak{m}$ be a maximal ideal. Then $A/\mathfrak{m}$ is a field, hence an integral domain. Therefore $\mathfrak{m}$ is prime. □

Theorem 1.10. *A prime ideal of a principal ideal domain is maximal.*

Proof. Let A be a PID and let $\mathfrak{p} \neq (0)$ be a prime ideal. Write $\mathfrak{p} = (r)$. Suppose

$$\mathfrak{p} \subseteq I \subseteq A.$$

Then $I = (s)$ for some $s \in A$. Since $(r) \subseteq (s)$, we have $r = ts$ for some $t \in A$. Since $\mathfrak{p}$ is prime, either $t \in \mathfrak{p}$ or $s \in \mathfrak{p}$. If $s \in \mathfrak{p}$, then $(s) \subseteq \mathfrak{p}$, so $I = \mathfrak{p}$. If $t \in \mathfrak{p}$, then $t = ur$, hence

$$r = ts = urs.$$

Since A is a domain and $r \neq 0$, we get $1 = us$, so s is a unit and $I = A$. Hence $\mathfrak{p}$ is maximal. □

Proposition 1.11. *Let $x \in A$. Then $x \in \mathrm{Jac}(A)$ if and only if $1 - xy$ is a unit for all $y \in A$.*

Proof. This is the Jacobson radical criterion proved above. □

Definition 1.12. Let $A_1, \ldots, A_n$ be rings. Their direct product is

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

If A is a ring and $\mathfrak{a}_i$ are ideals of A, define

$$\Phi : A \longrightarrow \prod_{i=1}^{n} A/\mathfrak{a}_i$$

by

$$\Phi(x) = (x + \mathfrak{a}_1, \ldots, x + \mathfrak{a}_n).$$

Proposition 1.13 (Chinese remainder theorem)**.** *Let $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ be ideals of A.*

(i) If $\mathfrak{a}_i$ and $\mathfrak{a}_j$ are coprime whenever $i \neq j$, then

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

(ii) The map Φ is surjective if and only if $\mathfrak{a}_i$ and $\mathfrak{a}_j$ are coprime whenever $i \neq j$.

(iii) The map Φ is injective if and only if

$$\bigcap_{i=1}^{n} \mathfrak{a}_i = (0).$$

Proof. For (i), use induction on n. The case $n = 2$ was proved above. Suppose the claim holds for $n - 1$. Let

$$\mathfrak{b} = \mathfrak{a}_1 \cdots \mathfrak{a}_{n-1}.$$

Then $\mathfrak{b} = \bigcap_{i=1}^{n-1} \mathfrak{a}_i$. It remains to show that $\mathfrak{b}$ and $\mathfrak{a}_n$ are coprime. For each $i < n$, choose $x_i \in \mathfrak{a}_i$ and $y_i \in \mathfrak{a}_n$ such that

$$x_i + y_i = 1.$$

Then

$$\prod_{i=1}^{n-1} x_i \in \mathfrak{b},$$

and

$$\prod_{i=1}^{n-1} x_i \equiv 1 \pmod{\mathfrak{a}_n}.$$

Hence $\mathfrak{b} + \mathfrak{a}_n = A$.

For (ii), suppose first that the ideals are pairwise coprime. To show surjectivity, it is enough to produce, for each i, an element $x_i \in A$ such that

$$x_i \equiv 1 \pmod{\mathfrak{a}_i}, \qquad x_i \equiv 0 \pmod{\mathfrak{a}_j} \quad (j \neq i).$$

This follows from the preceding construction. Conversely, if Φ is surjective, then for each pair $i \neq j$ there exists $x \in A$ with

$$x \equiv 1 \pmod{\mathfrak{a}_i}, \qquad x \equiv 0 \pmod{\mathfrak{a}_j}.$$

Thus $1 \in \mathfrak{a}_i + \mathfrak{a}_j$, so $\mathfrak{a}_i$ and $\mathfrak{a}_j$ are coprime.

For (iii), $\ker \Phi = \bigcap_i \mathfrak{a}_i$. □

Proposition 1.14. *Let $\mathfrak{p}$ be a prime ideal and let $\mathfrak{a}_i$ be ideals. If*

$$\bigcap_{i=1}^{n} \mathfrak{a}_i \subseteq \mathfrak{p},$$

then $\mathfrak{a}_i \subseteq \mathfrak{p}$ for some i.

Proof. Assume no $\mathfrak{a}_i$ is contained in $\mathfrak{p}$. For each i, choose

$$x_i \in \mathfrak{a}_i \setminus \mathfrak{p}.$$

Then $x_1 \cdots x_n \in \bigcap_i \mathfrak{a}_i$, hence $x_1 \cdots x_n \in \mathfrak{p}$. Since $\mathfrak{p}$ is prime, some $x_i \in \mathfrak{p}$, a contradiction. □

Proposition 1.15. *Let $\mathfrak{a}$ be an ideal such that $\mathfrak{a} \subseteq \bigcup_{i=1}^{n} \mathfrak{p}_i$, where $\mathfrak{p}_i$ are prime ideals. Then $\mathfrak{a} \subseteq \mathfrak{p}_i$ for some i.*

Proof. This is the prime avoidance lemma. We prove it by induction on n. The case $n = 1$ is clear. Suppose the statement is true for $n - 1$.

Assume $\mathfrak{a} \not\subseteq \mathfrak{p}_i$ for all i. By the induction hypothesis, for each i there exists

$$x_i \in \mathfrak{a} \setminus \bigcup_{j \neq i} \mathfrak{p}_j.$$

Since $\mathfrak{a} \subseteq \bigcup_i \mathfrak{p}_i$, we must have $x_i \in \mathfrak{p}_i$. Set

$$y = x_1 x_2 \cdots x_{n-1} + x_n.$$

Then $y \in \mathfrak{a}$. For $i < n$, the product $x_1 \cdots x_{n-1}$ lies in $\mathfrak{p}_i$, while $x_n \notin \mathfrak{p}_i$, so $y \notin \mathfrak{p}_i$. Also, $x_1 \cdots x_{n-1} \notin \mathfrak{p}_n$ whereas $x_n \in \mathfrak{p}_n$, so $y \notin \mathfrak{p}_n$. This contradicts $\mathfrak{a} \subseteq \bigcup_i \mathfrak{p}_i$. □

1.5 Ideal Quotients and Annihilators

Definition 1.16. If $\mathfrak{a}$ and $\mathfrak{b}$ are ideals of A, their *ideal quotient* is

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

Example 1.17. (i) $\big((x) : (y)\big) = (x)$ in $k[x, y]$.

(ii) $\big((x) : (x, y)\big) = (x)$ in $k[x, y]$.

Definition 1.18. The *annihilator* of an ideal $\mathfrak{b}$ is

$$\operatorname{Ann}(\mathfrak{b}) = \{x \in A \mid x\mathfrak{b} = 0\} = (0 : \mathfrak{b}).$$

Definition 1.19. If $\mathfrak{a}$ is an ideal of A, the *radical* of $\mathfrak{a}$ is

$$r(\mathfrak{a}) = \{x \in A \mid x^n \in \mathfrak{a} \text{ for some } n \geq 1\}.$$

Equivalently, if $\phi : A \to A/\mathfrak{a}$ is the quotient map, then

$$r(\mathfrak{a}) = \phi^{-1}\big(\mathrm{Nil}(A/\mathfrak{a})\big).$$

Exercise 1.20. Let $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$ be ideals of A. Then:

(i) $(\mathfrak{a} : \mathfrak{b}) \supseteq \mathfrak{a}$.

(ii) $(\mathfrak{a} : \mathfrak{b})\mathfrak{b} \subseteq \mathfrak{a}$.

(iii) $\big((\mathfrak{a} : \mathfrak{b}) : \mathfrak{c}\big) = (\mathfrak{a} : \mathfrak{b}\mathfrak{c})$.

(iv) $(\bigcap_i \mathfrak{a}_i : \mathfrak{b}) = \bigcap_i (\mathfrak{a}_i : \mathfrak{b})$.

(v) $(\mathfrak{a} : \sum_i \mathfrak{b}_i) = \bigcap_i (\mathfrak{a} : \mathfrak{b}_i)$.

Exercise 1.21. For ideals $\mathfrak{a}, \mathfrak{b}$ of A, one has:

(i) $r(\mathfrak{a}) \supseteq \mathfrak{a}$.

(ii) $r(r(\mathfrak{a})) = r(\mathfrak{a})$.

(iii) $r(\mathfrak{a}\mathfrak{b}) = r(\mathfrak{a} \cap \mathfrak{b}) = r(\mathfrak{a}) \cap r(\mathfrak{b})$.

(iv) $r(\mathfrak{a}) = A$ if and only if $\mathfrak{a} = A$.

(v) $r(\mathfrak{a} + \mathfrak{b}) = r(r(\mathfrak{a}) + r(\mathfrak{b}))$.

(vi) If $\mathfrak{p}$ is prime, then $r(\mathfrak{p}^n) = \mathfrak{p}$ for all $n > 0$.

Proposition 1.22. *The radical of an ideal $\mathfrak{a}$ is the intersection of all prime ideals containing $\mathfrak{a}$:*

$$r(\mathfrak{a}) = \bigcap_{\mathfrak{p} \supseteq \mathfrak{a}} \mathfrak{p}.$$

Proof. This follows by applying the description of the nilradical to $A/\mathfrak{a}$. □

Proposition 1.23. *The set of all zero divisors of A is*

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

Proof. If a is a zero divisor, then $ax = 0$ for some $x \neq 0$, so $a \in \mathrm{Ann}(x) \subseteq r(\mathrm{Ann}(x))$. Conversely, if $a \in r(\mathrm{Ann}(x))$ for some $x \neq 0$, then $a^n x = 0$ for some $n > 0$, so a is a zero divisor. □

1.6 Extension and Contraction of Ideals

Definition 1.24. Let $f : A \to B$ be a ring homomorphism and let $\mathfrak{a}$ be an ideal of A. The *extension* of $\mathfrak{a}$ to B is the ideal

$$\mathfrak{a}^e = Bf(\mathfrak{a})$$

generated by $f(\mathfrak{a})$.

Definition 1.25. Let $\mathfrak{b}$ be an ideal of B. The *contraction* of $\mathfrak{b}$ to A is

$$\mathfrak{b}^c = f^{-1}(\mathfrak{b}).$$

Proposition 1.26. *Let $f : A \to B$ be a ring homomorphism. Then:*

(i) $\mathfrak{a} \subseteq \mathfrak{a}^{ec}$ *for every ideal* $\mathfrak{a} \subseteq A$.

(ii) $\mathfrak{b}^{ce} \subseteq \mathfrak{b}$ *for every ideal* $\mathfrak{b} \subseteq B$.

Proof. Both statements follow directly from the definitions. □

Proposition 1.27. *Let $\mathfrak{a}, \mathfrak{b} \subseteq A$ be ideals such that $r(\mathfrak{a})$ and $r(\mathfrak{b})$ are coprime. Then $\mathfrak{a}$ and $\mathfrak{b}$ are coprime.*

Proof. Since $r(\mathfrak{a}) + r(\mathfrak{b}) = A$, we have $1 = x + y$ with $x \in r(\mathfrak{a})$ and $y \in r(\mathfrak{b})$. Then $x^m \in \mathfrak{a}$ and $y^n \in \mathfrak{b}$ for some m, n. Expanding $(x + y)^{m+n-1} = 1$ shows that $1 \in \mathfrak{a} + \mathfrak{b}$. □

Exercise 1.28. Let $f : A \to B$ be a ring homomorphism, let $\mathfrak{a}, \mathfrak{a}'$ be ideals of A, and let $\mathfrak{b}, \mathfrak{b}'$ be ideals of B. Then:

(i) $(\mathfrak{a}_1 + \mathfrak{a}_2)^e = \mathfrak{a}_1^e + \mathfrak{a}_2^e$.

(ii) $(\mathfrak{a}_1\mathfrak{a}_2)^e = \mathfrak{a}_1^e\mathfrak{a}_2^e$.

(iii) $(\mathfrak{b}_1 \cap \mathfrak{b}_2)^c \supseteq \mathfrak{b}_1^c \cap \mathfrak{b}_2^c$.

(iv) $(\mathfrak{b}_1 + \mathfrak{b}_2)^c \supseteq \mathfrak{b}_1^c + \mathfrak{b}_2^c$.

(v) $(\mathfrak{b}_1\mathfrak{b}_2)^c \supseteq \mathfrak{b}_1^c\mathfrak{b}_2^c$.

(vi) $r(\mathfrak{a})^e \subseteq r(\mathfrak{a}^e)$.

(vii) $r(\mathfrak{b}^c) = r(\mathfrak{b})^c$.

1.7 Affine Algebraic Sets

Let k be a field. The affine n-space over k is the set

$$\mathbb{A}_k^n = k^n.$$

If $S \subseteq k[x_1, \ldots, x_n]$ is a set of polynomials, define

$$V(S) = \{a \in \mathbb{A}_k^n : f(a) = 0 \text{ for all } f \in S\}.$$

A subset of $\mathbb{A}_k^n$ of the form $V(S)$ is called an *affine algebraic set*. Since $V(S) = V((S))$, it is enough to consider sets of the form $V(I)$, where $I \subseteq k[x_1, \ldots, x_n]$ is an ideal.

Conversely, if $X \subseteq \mathbb{A}_k^n$, define

$$I(X) = \{f \in k[x_1, \ldots, x_n] : f(a) = 0 \text{ for all } a \in X\}.$$

Then $I(X)$ is an ideal of $k[x_1, \ldots, x_n]$.

Proposition 1.29. *Let $I, J \subseteq k[x_1, \ldots, x_n]$ be ideals. Then:*

(i) $V(0) = \mathbb{A}_k^n$ *and* $V((1)) = \varnothing$;

(ii) *if* $I \subseteq J$, *then* $V(J) \subseteq V(I)$;

(iii) $V(I+J) = V(I) \cap V(J)$;

(iv) $V(IJ) = V(I \cap J) = V(I) \cup V(J)$.

Proof. The first three statements follow immediately from the definitions. For (iv), if $a \in V(I) \cup V(J)$, then every element of IJ vanishes at a, so $a \in V(IJ)$. Conversely, if $a \notin V(I) \cup V(J)$, choose $f \in I$ and $g \in J$ with $f(a) \neq 0$ and $g(a) \neq 0$. Then $(fg)(a) \neq 0$, so $a \notin V(IJ)$. Since $IJ \subseteq I \cap J$ and $V(IJ) = V(I) \cup V(J)$, the same equality holds for $V(I \cap J)$. □

Definition 1.30. If $X \subseteq \mathbb{A}_k^n$ is an affine algebraic set, its *coordinate ring* is

$$k[X] = k[x_1, \ldots, x_n]/I(X).$$

1.8 Hilbert's Nullstellensatz

The following theorems explain the precise relation between algebraic sets and ideals when the base field is algebraically closed. Their proofs will be given in Chapter 4, after Hilbert's basis theorem and Zariski's lemma.

Theorem 1.31 (Weak Nullstellensatz)**.** *Let* k *be an algebraically closed field. Then every maximal ideal of* $k[x_1, \ldots, x_n]$ *is of the form*

$$(x_1 - a_1, \ldots, x_n - a_n)$$

for a unique point $a = (a_1, \ldots, a_n) \in \mathbb{A}_k^n$.

Thus maximal ideals of $k[x_1, \ldots, x_n]$ correspond to points of affine space.

Theorem 1.32 (Hilbert's Nullstellensatz)**.** *Let* k *be an algebraically closed field and let* $I \subseteq k[x_1, \ldots, x_n]$ *be an ideal. Then*

$$I(V(I)) = \mathrm{Rad}(I).$$

Consequently, affine algebraic subsets of $\mathbb{A}_k^n$ correspond to radical ideals of $k[x_1, \ldots, x_n]$.

1.9 The Prime Spectrum

Definition 1.33. The *prime spectrum* of a ring A is

$$\mathrm{Spec}(A) = \{\mathfrak{p} \subseteq A \mid \mathfrak{p} \text{ is a prime ideal}\}.$$

For an ideal $\mathfrak{a} \subseteq A$, define

$$V(\mathfrak{a}) = \{\mathfrak{p} \in \mathrm{Spec}(A) \mid \mathfrak{a} \subseteq \mathfrak{p}\}.$$

The closed sets of $\mathrm{Spec}(A)$ are defined to be the sets of the form $V(\mathfrak{a})$. This topology is called the *Zariski topology.*

Example 1.34. (1) $\mathrm{Spec}(\mathbb{Z}) = \{(0), (p) : p \text{ prime}\}$.

(2) $\mathrm{Spec}(k) = \{(0)\}$ if k is a field.

(3) $\operatorname{Spec}(\mathbb{R}[x]) = \{(0), (x-a), (x^2+bx+c) : a, b, c \in \mathbb{R},\ b^2 - 4c < 0\}$.

(4) $\operatorname{Spec}(\mathbb{C}[x]) = \{(0), (x-a) : a \in \mathbb{C}\}$.

Definition 1.35. A topological space X is *irreducible* if $X \neq \varnothing$ and every pair of nonempty open subsets of X intersects. Equivalently, every nonempty open set is dense in X, or X cannot be written as the union of two proper closed subsets.

Theorem 1.36. *The space* $\operatorname{Spec}(A)$ *is irreducible if and only if the nilradical of* A *is prime.*

Proof. Suppose first that $\operatorname{Nil}(A)$ is not prime. Then there exist $x, y \notin \operatorname{Nil}(A)$ such that $xy \in \operatorname{Nil}(A)$. Hence

$$x^n \neq 0, \quad y^m \neq 0, \quad (xy)^r = 0$$

for suitable m, n, r. Let $\mathfrak{a} = (x)$ and $\mathfrak{b} = (y)$. Then

$$V(\mathfrak{a}) \cup V(\mathfrak{b}) = V(\mathfrak{a}\mathfrak{b}) = \operatorname{Spec}(A),$$

while neither $V(\mathfrak{a})$ nor $V(\mathfrak{b})$ is the whole space. Thus $\operatorname{Spec}(A)$ is reducible.

Conversely, suppose $\operatorname{Spec}(A)$ is reducible. Then

$$\operatorname{Spec}(A) = V(\mathfrak{a}) \cup V(\mathfrak{b}) = V(\mathfrak{a}\mathfrak{b})$$

with $V(\mathfrak{a}), V(\mathfrak{b})$ proper closed subsets. Thus $\mathfrak{a}\mathfrak{b} \subseteq \operatorname{Nil}(A)$, while neither $\mathfrak{a}$ nor $\mathfrak{b}$ is contained in $\operatorname{Nil}(A)$. Hence $\operatorname{Nil}(A)$ is not prime. □

Definition 1.37. For $f \in A$, define

$$X_f = \{\mathfrak{p} \in \operatorname{Spec}(A) \mid f \notin \mathfrak{p}\}.$$

These are called the *basic open sets* of $\operatorname{Spec}(A)$.

Proposition 1.38. *For* $f, g \in A$, *the following hold:*

(i) $X_f \cap X_g = X_{fg}$.

(ii) $X_f = \varnothing$ *if and only if* f *is nilpotent.*

(iii) $X_f = \operatorname{Spec}(A)$ *if and only if* f *is a unit.*

(iv) $X_f = X_g$ *if and only if* $r((f)) = r((g))$.

(v) X_f *is compact.*

(vi) $X_f \subseteq X_g$ *if and only if* $f \in r((g))$.

(vii) $X_f = \operatorname{Spec}(A) \setminus V((f))$.

Moreover, the sets X_f *form a basis of the Zariski topology on* $\operatorname{Spec}(A)$.

Proof. The identities follow from the definitions and from the radical description in terms of prime ideals. For compactness, suppose

$$X_f \subseteq \bigcup_i X_{g_i}.$$

Then

$$V((g_i)_{i \in I}) \subseteq V((f)),$$

so $f \in r((g_i)_{i\in I})$. Hence for some n,

$$f^n \in (g_{i_1}, \dots, g_{i_m})$$

for finitely many indices $i_1, \dots, i_m$. Therefore

$$X_f \subseteq X_{g_{i_1}} \cup \cdots \cup X_{g_{i_m}}.$$

□

Remark 1.39. In algebraic geometry, one uses these properties to define affine schemes. The space $\mathrm{Spec}(A)$ together with its structure sheaf is an affine scheme, and a scheme is a locally ringed space which is covered by affine schemes.

1.10 Morphisms of Spectra

Proposition 1.40. *Let $\varphi : A \to B$ be a ring homomorphism. Let $X = \mathrm{Spec}(A)$ and $Y = \mathrm{Spec}(B)$. If $\mathfrak{q} \in Y$, then*

$$\varphi^{-1}(\mathfrak{q}) \in X.$$

Thus φ induces a map

$$\varphi^* : Y \longrightarrow X, \qquad \mathfrak{q} \longmapsto \varphi^{-1}(\mathfrak{q}).$$

Moreover:

(i) If $\mathfrak{b}$ is an ideal of B, then

$$(\varphi^*)^{-1}(V(\mathfrak{b}^c)) = V(\mathfrak{b}).$$

(ii) If $\mathfrak{a}$ is an ideal of A, then

$$(\varphi^*)^{-1}(V(\mathfrak{a})) = V(\mathfrak{a}^e).$$

(iii) The map φ^* is continuous.

(iv) If $\psi : B \to C$ is another ring homomorphism, then

$$(\psi \circ \varphi)^* = \varphi^* \circ \psi^*.$$

(v) If φ is surjective, then φ^* is a homeomorphism from $\mathrm{Spec}(B)$ onto the closed subset $V(\ker \varphi)$ of $\mathrm{Spec}(A)$.

Proof. If $\mathfrak{q}$ is prime in B, then $\varphi^{-1}(\mathfrak{q})$ is prime in A. Indeed, if $ab \in \varphi^{-1}(\mathfrak{q})$, then $\varphi(a)\varphi(b) \in \mathfrak{q}$, so $\varphi(a) \in \mathfrak{q}$ or $\varphi(b) \in \mathfrak{q}$.

The formulas for inverse images of closed sets follow directly from the definitions of extension and contraction of ideals. Hence φ^* is continuous.

Functoriality is immediate:

$$(\psi \circ \varphi)^{-1}(\mathfrak{r}) = \varphi^{-1}(\psi^{-1}(\mathfrak{r})).$$

If φ is surjective, then ideals of B correspond to ideals of A containing $\ker \varphi$. Under this correspondence prime ideals correspond to prime ideals, and the induced map identifies $\mathrm{Spec}(B)$ with $V(\ker \varphi)$. □

Remark 1.41. This defines morphisms of affine schemes. For general schemes, morphisms are defined in a similar way by gluing affine morphisms.

Chapter 2

Modules

Throughout this chapter, A denotes a commutative ring with identity, and all modules are A-modules unless otherwise stated.

2.1 Finitely Generated Modules and Nakayama's Lemma

Proposition 2.1. *Let M be an A-module. Then M is finitely generated if and only if there exists a finitely generated free A-module F and a surjective homomorphism*

$$F \twoheadrightarrow M.$$

Proof. If F is finitely generated and $F \twoheadrightarrow M$, then the images of a finite set of generators of F generate M.

Conversely, suppose $M = (x_1, \ldots, x_n)$. Define

$$\varphi : A^n \longrightarrow M, \qquad (a_1, \ldots, a_n) \longmapsto \sum_{i=1}^{n} a_i x_i.$$

Then φ is surjective. Hence M is a quotient of the finitely generated free module A^n. □

Proposition 2.2. *Let M be a finitely generated A-module, let $\mathfrak{a}$ be an ideal of A, and let $\varphi \in \mathrm{Hom}_A(M, M)$. If*

$$\varphi(M) \subseteq \mathfrak{a}M,$$

then there exist $a_1, \ldots, a_n \in \mathfrak{a}$ such that

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

as an endomorphism of M.

Proof. Let $x_1, \ldots, x_n$ generate M. Since $\varphi(M) \subseteq \mathfrak{a}M$, for each i we can write

$$\varphi(x_i) = \sum_{j=1}^{n} a_{ij} x_j,$$

with $a_{ij} \in \mathfrak{a}$. Put $T = (t_{ij})$, where

$$t_{ij} = \delta_{ij}\varphi - a_{ij}.$$

Then

$$\sum_{j=1}^{n} t_{ij}x_j = 0 \qquad (1 \le i \le n).$$

Multiplying by the adjugate matrix of T, we obtain

$$\det(T)x_i = 0 \qquad (1 \le i \le n).$$

Since the x_i generate M, $\det(T)$ acts as zero on M. Expanding $\det(T)$ gives a monic polynomial in φ of degree n whose non-leading coefficients lie in $\mathfrak{a}$. □

Corollary 2.3 (Nakayama's Lemma)**.** *Let M be a finitely generated A-module and let $\mathfrak{a}$ be an ideal contained in the Jacobson radical* $\mathrm{Jac}(A)$*. If*

$$\mathfrak{a}M = M,$$

then $M = 0$.

Proof. Apply the previous proposition to $\varphi = \mathrm{id}_M$. We obtain

$$1 + a_1 + \cdots + a_n = 0$$

as an endomorphism of M, where each $a_i \in \mathfrak{a}$. Thus

$$u = 1 + (a_1 + cdots + a_n)$$

annihilates M. Since $a_1 + \cdots + a_n \in \mathfrak{a} \subseteq \mathrm{Jac}(A)$, the element u is a unit. Hence $M = uM = 0$. □

Corollary 2.4. *Let $(A, \mathfrak{m})$ be a local ring and let M be a finitely generated A-module. If $N \subseteq M$ and*

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

then $M = N$.

Proof. Apply Nakayama's lemma to M/N. Since

$$M/N = \mathfrak{m}(M/N),$$

and $\mathfrak{m} = \mathrm{Jac}(A)$, we get $M/N = 0$. □

Corollary 2.5. *Let $(A, \mathfrak{m})$ be a local ring and let M be a finitely generated A-module. If $x_1, \ldots, x_n \in M$ have images which span the vector space $M/\mathfrak{m}M$ over $A/\mathfrak{m}$, then $x_1, \ldots, x_n$ generate M.*

Proof. Let $N = (x_1, \ldots, x_n)$. The assumption means

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

The preceding corollary gives $M = N$. □

Remark 2.6. For a finitely generated module M over a local ring $(A, \mathfrak{m})$, the quotient $M/\mathfrak{m}M$ is a finite-dimensional vector space over the residue field $A/\mathfrak{m}$.

2.2 Exact Sequences

Definition 2.7. Let $f : M \to N$ be an A-module homomorphism. The *cokernel* of f is

$$\operatorname{coker}(f) = N/\operatorname{im}(f).$$

It is a quotient module of N.

Definition 2.8. A sequence of A-modules and A-module homomorphisms

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

is called *exact at* M_i if

$$\operatorname{im}(f_i) = \ker(f_{i+1}).$$

The sequence is called *exact* if it is exact at every term.

Proposition 2.9. *Let*

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$$

be a short exact sequence of A-modules. If M' and M'' are finitely generated, then M is finitely generated.

Proof. Choose generators $x_1, \ldots, x_r$ for M' and generators $\bar{y}_1, \ldots, \bar{y}_s$ for M''. Lift each $\bar{y}_j$ to an element $y_j \in M$. We claim that

$$x_1, \ldots, x_r, y_1, \ldots, y_s$$

generate M.

Indeed, for $m \in M$, its image in M'' is a linear combination of the $\bar{y}_j$. Subtracting the corresponding linear combination of the y_j from m, we get an element of $\ker(M \to M'') = \operatorname{im}(M' \to M)$, hence a linear combination of the x_i. □

Proposition 2.10. *Consider a commutative diagram of A-modules with exact rows*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M' & \xrightarrow{u} & M & \xrightarrow{v} & M'' & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle f'} & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle f''} & & \\ 0 & \longrightarrow & N' & \xrightarrow[u']{} & N & \xrightarrow[v']{} & N'' & \longrightarrow & 0. \end{array}$$

Then the induced sequence

$$0 \longrightarrow \ker(f') \longrightarrow \ker(f) \longrightarrow \ker(f'') \longrightarrow \operatorname{coker}(f') \longrightarrow \operatorname{coker}(f) \longrightarrow \operatorname{coker}(f'') \longrightarrow 0$$

is exact.

Proof. This is the snake lemma. We give the full construction.

The maps

$$\ker(f') \to \ker(f), \qquad \ker(f) \to \ker(f'')$$

are induced by u and v respectively. The maps

$$\operatorname{coker}(f') \to \operatorname{coker}(f), \qquad \operatorname{coker}(f) \to \operatorname{coker}(f'')$$

are induced by u' and v' respectively. These induced maps are well-defined by commutativity of the diagram.

It remains to define the connecting homomorphism

$$\delta : \ker(f'') \longrightarrow \operatorname{coker}(f').$$

Let $x'' \in \ker(f'')$. Since $v : M \to M''$ is surjective, choose $x \in M$ such that $v(x) = x''$. Then

$$v'(f(x)) = f''(v(x)) = f''(x'') = 0.$$

Thus $f(x) \in \ker(v') = \operatorname{im}(u')$. Hence there exists $y' \in N'$ such that

$$u'(y') = f(x).$$

Define

$$\delta(x'') = y' + \operatorname{im}(f') \in \operatorname{coker}(f').$$

We check that δ is well-defined. First, suppose that $y'_1, y'_2 \in N'$ both satisfy $u'(y'_i) = f(x)$. Since u' is injective, $y'_1 = y'_2$.

Next, suppose that $x_1, x_2 \in M$ are two lifts of x''. Then $v(x_1 - x_2) = 0$, so $x_1 - x_2 \in \ker(v) = \operatorname{im}(u)$. Hence $x_1 - x_2 = u(z')$ for some $z' \in M'$. Applying f and using commutativity gives

$$f(x_1) - f(x_2) = f(u(z')) = u'(f'(z')).$$

If $u'(y'_i) = f(x_i)$, then

$$u'(y'_1 - y'_2 - f'(z')) = 0.$$

Since u' is injective, $y'_1 - y'_2 = f'(z')$. Thus y'_1 and y'_2 determine the same class in $\operatorname{coker}(f')$. Therefore δ is well-defined. It is immediate from the construction that δ is a homomorphism.

Now we verify exactness.

At $\ker(f')$ and $\ker(f)$, exactness follows from exactness of the top row: if $x \in \ker(f)$ maps to 0 in $\ker(f'')$, then $v(x) = 0$, so $x = u(x')$ for some $x' \in M'$. Then

$$u'(f'(x')) = f(u(x')) = f(x) = 0,$$

and since u' is injective, $f'(x') = 0$. Hence x' lies in $\ker(f')$.

At $\ker(f'')$, let $x'' \in \ker(f'')$. If x'' is in the image of $\ker(f) \to \ker(f'')$, then $x'' = v(x)$ with $f(x) = 0$. In the construction of δ, we may take $y' = 0$, hence $\delta(x'') = 0$. Conversely, suppose $\delta(x'') = 0$. Choose $x \in M$ with $v(x) = x''$, and choose $y' \in N'$ with $u'(y') = f(x)$. The condition $\delta(x'') = 0$ means that $y' = f'(z')$ for some $z' \in M'$. Then

$$f(x - u(z')) = f(x) - u'(f'(z')) = 0,$$

and

$$v(x - u(z')) = v(x) = x''.$$

Thus x'' is the image of an element of $\ker(f)$.

At $\operatorname{coker}(f')$, let $y' \in N'$. Its class in $\operatorname{coker}(f')$ maps to zero in $\operatorname{coker}(f)$ if and only if $u'(y') \in \operatorname{im}(f)$, say $u'(y') = f(x)$. Then

$$f''(v(x)) = v'(f(x)) = v'(u'(y')) = 0,$$

so $v(x) \in \ker(f'')$, and by construction $\delta(v(x))$ is the class of y'. Hence the kernel of $\operatorname{coker}(f') \to \operatorname{coker}(f)$ is the image of δ.

At $\operatorname{coker}(f)$, exactness follows from exactness of the bottom row. A class $y + \operatorname{im}(f)$ maps to zero in $\operatorname{coker}(f'')$ if and only if

$$v'(y) \in \operatorname{im}(f'').$$

Choose $x'' \in M''$ with $f''(x'') = v'(y)$, and lift x'' to $x \in M$. Then

$$v'(y - f(x)) = v'(y) - f''(v(x)) = 0,$$

so $y - f(x) = u'(y')$ for some $y' \in N'$. Hence the class of y in $\operatorname{coker}(f)$ comes from the class of y' in $\operatorname{coker}(f')$.

Finally, the map $\operatorname{coker}(f) \to \operatorname{coker}(f'')$ is surjective because $v' : N \to N''$ is surjective. This completes the proof. □

2.3 Additive Functions on Exact Sequences

Definition 2.11. Let $\mathcal{C}$ be a class of A-modules and let

$$\lambda : \mathcal{C} \longrightarrow \mathbb{Z}$$

be a function. We say that λ is *additive* if, for every short exact sequence

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$$

whose terms lie in $\mathcal{C}$, one has

$$\lambda(M) = \lambda(M') + \lambda(M'').$$

Example 2.12. If F is a field and $\mathcal{C}$ is the class of finite-dimensional vector spaces over F, then

$$\lambda(V) = \dim_F V$$

is additive.

Proposition 2.13. *Let*

$$0 \longrightarrow M_0 \xrightarrow{f_1} M_1 \xrightarrow{f_2} \cdots \xrightarrow{f_n} M_n \longrightarrow 0$$

be an exact sequence of A-modules, and suppose all M_i and all kernels $\ker(f_i)$ belong to a class $\mathcal{C}$ on which λ is additive. Then

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

Proof. Break the long exact sequence into short exact sequences

$$0 \longrightarrow \ker(f_i) \longrightarrow M_i \longrightarrow \ker(f_{i+1}) \longrightarrow 0.$$

Applying additivity and summing with alternating signs gives a telescoping sum. □

2.4 Tensor Products

Definition 2.14. Let M and N be A-modules. A *bilinear map* from $M \times N$ to an A-module P is a map

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

which is A-linear in each variable.

The tensor product of M and N is an A-module $M \otimes_A N$ together with a bilinear map

$$\tau : M \times N \longrightarrow M \otimes_A N$$

such that for every A-module P and every bilinear map $f : M \times N \to P$, there exists a unique A-linear map

$$\tilde{f} : M \otimes_A N \longrightarrow P$$

with $f = \tilde{f} \circ \tau$.

Remark 2.15. We write $x \otimes y$ for $\tau(x, y)$. The tensor product is unique up to unique isomorphism by its universal property.

Proposition 2.16. *Let M and N be A-modules. The module $M \otimes_A N$ is generated by symbols $x \otimes y$, subject to the relations*

$$(x + x') \otimes y = x \otimes y + x' \otimes y,$$

$$x \otimes (y + y') = x \otimes y + x \otimes y',$$

and

$$(ax) \otimes y = x \otimes (ay) = a(x \otimes y).$$

Proof. Take the free A-module on the set $M \times N$ and quotient by the submodule generated by the relations above. The induced map $M \times N \to M \otimes_A N$ is bilinear and satisfies the required universal property. □

Proposition 2.17 (Canonical isomorphisms)**.** *For A-modules M, N, P, there are natural isomorphisms*

(i) $M \otimes_A N \cong N \otimes_A M$;

(ii) $(M \otimes_A N) \otimes_A P \cong M \otimes_A (N \otimes_A P)$;

(iii) $A \otimes_A M \cong M$;

(iv) $(M \oplus N) \otimes_A P \cong (M \otimes_A P) \oplus (N \otimes_A P)$.

Proof. Each isomorphism is induced by the corresponding bilinear or multilinear universal property. For example, $a \otimes x \mapsto ax$ gives $A \otimes_A M \to M$, with inverse $x \mapsto 1 \otimes x$. □

Proposition 2.18 (Change of rings)**.** *Let $A \to B$ be a ring homomorphism, let M be an A-module, let P be a B-module, and let N be a module which is simultaneously an A-module and a B-module with compatible structures. Then $M \otimes_A N$ has a natural B-module structure. In particular, if M and N are B-modules, then $M \otimes_A N$ is a B-module, and $N \otimes_B P$ is an A-module by restriction of scalars.*

Proof. Define

$$b \cdot (x \otimes y) = x \otimes (by).$$

The compatibility conditions and the defining relations of the tensor product show that this is well-defined. The remaining assertions follow by restriction or extension of scalars. □

Proposition 2.19. *Let $f : M \to M'$ and $g : N \to N'$ be A-module homomorphisms. Then there is a unique A-module homomorphism*

$$f \otimes g : M \otimes_A N \longrightarrow M' \otimes_A N'$$

such that

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

Proof. The map $(x, y) \mapsto f(x) \otimes g(y)$ is bilinear, so the universal property gives the desired homomorphism. □

Proposition 2.20. *Let $\mathfrak{a}, \mathfrak{b}$ be ideals of A and let M be an A-module. Then*

$$(A/\mathfrak{a}) \otimes_A (A/\mathfrak{b}) \cong A/(\mathfrak{a} + \mathfrak{b}),$$

and

$$(A/\mathfrak{a}) \otimes_A M \cong M/\mathfrak{a}M.$$

Proof. For the first isomorphism, define

$$(\bar{x}, \bar{y}) \longmapsto \overline{xy} \in A/(\mathfrak{a} + \mathfrak{b}).$$

This is A-bilinear and induces a map

$$(A/\mathfrak{a}) \otimes_A (A/\mathfrak{b}) \to A/(\mathfrak{a} + \mathfrak{b}).$$

The inverse sends $\bar{z}$ to $\bar{z} \otimes \bar{1}$. The second isomorphism is obtained similarly from the bilinear map

$$(\bar{a}, m) \longmapsto am + \mathfrak{a}M.$$

Its inverse sends $m + \mathfrak{a}M$ to $\bar{1} \otimes m$. □

2.5 Hom and Tensor

Theorem 2.21 (Tensor-Hom Adjunction)**.** *Let R be a ring, let B be an (R, S)-bimodule, let C be a left S-module, and let A be a left R-module. Then there is a natural isomorphism*

$$\mathrm{Hom}_R(B \otimes_S C, A) \cong \mathrm{Hom}_S(C, \mathrm{Hom}_R(B, A)).$$

Proof. Given $f : B \otimes_S C \to A$, define $\theta(f) : C \to \mathrm{Hom}_R(B, A)$ by

$$\theta(f)(c)(b) = f(b \otimes c).$$

Conversely, given $g : C \to \mathrm{Hom}_R(B, A)$, define

$$\tilde{g} : B \times C \to A, \qquad \tilde{g}(b, c) = g(c)(b).$$

This map is balanced over S, hence induces $B \otimes_S C \to A$. These constructions are inverse and natural. □

Proposition 2.22. *Let*

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$$

be an exact sequence of A-modules, and let N be any A-module. Then

$$0 \longrightarrow \mathrm{Hom}_A(N, M') \longrightarrow \mathrm{Hom}_A(N, M) \longrightarrow \mathrm{Hom}_A(N, M'')$$

is exact.

Proof. The functor $\mathrm{Hom}_A(N, -)$ is left exact. Injectivity at the first term follows because $M' \to M$ is injective. If a map $N \to M$ becomes zero in $\mathrm{Hom}_A(N, M'')$, then its image lies in M', hence it factors uniquely through M'. This proves exactness. □

Example 2.23. The functor $\mathrm{Hom}_A(N, -)$ need not be right exact. For example, over $\mathbb{Z}$ the sequence

$$0 \longrightarrow \mathbb{Z} \xrightarrow{\times 2} \mathbb{Z} \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow 0$$

is exact, but applying $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/2\mathbb{Z}, -)$ does not preserve right exactness.

2.6 Flat Modules

Definition 2.24. Let N be an A-module. Consider the functor

$$T_N : M \longmapsto M \otimes_A N.$$

The module N is called *flat* if T_N is exact, that is, whenever

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$$

is exact, the sequence

$$0 \longrightarrow M' \otimes_A N \longrightarrow M \otimes_A N \longrightarrow M'' \otimes_A N \longrightarrow 0$$

is exact.

Proposition 2.25. *The following are equivalent for an A-module N:*

(i) *N is flat.*

(ii) *For every exact sequence $0 \to M' \to M \to M'' \to 0$, the sequence*

$$0 \to M' \otimes_A N \to M \otimes_A N \to M'' \otimes_A N \to 0$$

is exact.

(iii) *For every injective homomorphism $M' \hookrightarrow M$, the induced map*

$$M' \otimes_A N \longrightarrow M \otimes_A N$$

is injective.

(iv) *For every ideal $\mathfrak{a} \subseteq A$, the natural map*

$$\mathfrak{a} \otimes_A N \longrightarrow N, \qquad a \otimes n \longmapsto an$$

is injective.

Proof. The equivalence of (i), (ii), and (iii) follows because tensoring is always right exact. Thus exactness of tensoring is equivalent to preservation of injections.

Clearly (iii) implies (iv), by applying it to the inclusion $\mathfrak{a} \hookrightarrow A$.

Conversely, assume (iv). Let $M' \hookrightarrow M$ be injective. To prove that $M' \otimes_A N \to M \otimes_A N$ is injective, take an element

$$u = \sum_{i=1}^{r} x_i \otimes n_i \in M' \otimes_A N$$

which maps to zero in $M \otimes_A N$. Let $F = A^r$ with basis $e_1, \dots, e_r$, and define $F \to M'$ by $e_i \mapsto x_i$. Let K be its kernel. The element u comes from $\sum e_i \otimes n_i \in F \otimes_A N$. The condition that u maps to zero in $M \otimes_A N$ means that the corresponding relations among the x_i already come from the submodule of relations after mapping to M. Reducing to the finitely generated submodule of F generated by those relations and using (iv) for the ideal generated by the coefficients gives that $u = 0$ in $M' \otimes_A N$.

Equivalently, one may use the standard equational criterion for flatness: condition (iv) implies that every finite relation in M among elements of M' is generated by relations already in M'. Hence $M' \otimes_A N \to M \otimes_A N$ is injective. Therefore (iii) holds. □

Proposition 2.26. *Let $A \to B$ be a ring homomorphism and let M be a flat A-module. Then $B \otimes_A M$ is a flat B-module.*

Proof. For every B-module N,

$$N \otimes_B (B \otimes_A M) \cong N \otimes_A M.$$

Since M is flat over A, the functor $N \mapsto N \otimes_A M$ is exact on the underlying A-modules. Hence $B \otimes_A M$ is flat over B. □

Definition 2.27. An A-module M is called *faithfully flat* if

(i) M is flat;

(ii) for every nonzero A-module N, one has $M \otimes_A N \neq 0$.

Proposition 2.28. *Let M be a flat A-module. The following are equivalent:*

(i) *M is faithfully flat.*

(ii) *For every nonzero A-module N, $N \otimes_A M \neq 0$.*

(iii) *For every maximal ideal $\mathfrak{m}$ of A, $M/\mathfrak{m}M \neq 0$.*

(iv) *For every maximal ideal $\mathfrak{m}$ of A, $\mathfrak{m}M \neq M$.*

Proof. The equivalence of (i) and (ii) is the definition. Since

$$(A/\mathfrak{m}) \otimes_A M \cong M/\mathfrak{m}M,$$

(i) implies (iii), and (iii) is equivalent to (iv).

Assume (iii), and let N be a nonzero A-module. Choose $0 \neq x \in N$, and let $Ax \subseteq N$ be the cyclic submodule it generates. There is a maximal ideal $\mathfrak{m}$ containing $\operatorname{Ann}(x)$, so $A/\mathfrak{m}$

is a quotient of Ax. Since tensoring by the flat module M is exact, if $N \otimes_A M = 0$, then also $Ax \otimes_A M = 0$, and hence

$$(A/\mathfrak{m}) \otimes_A M = 0,$$

contrary to (iii). Therefore $N \otimes_A M \neq 0$. □

Proposition 2.29. *Let A be a ring, let $\mathfrak{a}$ be an ideal, and let M be an A-module. Then*

$$(A/\mathfrak{a}) \otimes_A M \cong M/\mathfrak{a}M.$$

In particular, if $(A, \mathfrak{m})$ is local and M is faithfully flat, then $M/\mathfrak{m}M \neq 0$.

Proof. The isomorphism has already been constructed above. The last statement follows from faithful flatness and the fact that $A/\mathfrak{m} \neq 0$. □

Proposition 2.30. *Let*

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$$

be exact. If M' and M'' are finitely generated, then M is finitely generated.

Proof. This was proved earlier by lifting generators of M'' to M and adjoining generators of M'. □

Chapter 3

Localization

Localization is one of the most important constructions in commutative algebra. Algebraically, it is the process of forcing certain elements to become units. Geometrically, it is the operation of restricting attention to a neighborhood of a point.

3.1 Localization of Rings

Definition 3.1. Let A be a ring. A subset $S \subseteq A$ is called *multiplicatively closed* if

$$1 \in S$$

and

$$s, t \in S \implies st \in S.$$

Definition 3.2. Let $S \subseteq A$ be a multiplicatively closed subset. Define an equivalence relation on $A \times S$ by

$$(a, s) \sim (b, t)$$

if there exists $u \in S$ such that

$$u(at - bs) = 0.$$

The equivalence class of (a, s) is denoted by

$$\frac{a}{s}.$$

The set of equivalence classes is denoted by $S^{-1}A$.

We define addition and multiplication by

$$\frac{a}{s} + \frac{b}{t} = \frac{at + bs}{st},$$

and

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

Then $S^{-1}A$ is a ring, called the *localization* or the *ring of fractions* of A with respect to S.

There is a natural ring homomorphism

$$f : A \longrightarrow S^{-1}A, \qquad a \longmapsto \frac{a}{1}.$$

Proposition 3.3 (Universal Property of Localization)**.** *Let $g : A \to B$ be a ring homomorphism such that $g(s)$ is a unit in B for every $s \in S$. Then there exists a unique ring homomorphism*

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

such that

$$g = h \circ f.$$

Explicitly,

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

Proof. First we check uniqueness. If such an h exists, then

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

Thus h is uniquely determined.

For existence, define

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

Suppose

$$\frac{a}{s} = \frac{b}{t}.$$

Then there exists $u \in S$ such that

$$u(at - bs) = 0.$$

Applying g gives

$$g(u)(g(a)g(t) - g(b)g(s)) = 0.$$

Since $g(u)$ is a unit, we get

$$g(a)g(t) = g(b)g(s).$$

Hence

$$g(a)g(s)^{-1} = g(b)g(t)^{-1}.$$

Therefore h is well-defined. It is straightforward to check that h is a ring homomorphism. □

Proposition 3.4. *The localization map $f : A \to S^{-1}A$ satisfies the following properties.*

(i) If $s \in S$, then $f(s)$ is a unit in $S^{-1}A$.

(ii) If $f(a) = 0$, then $as = 0$ for some $s \in S$.

(iii) Every element of $S^{-1}A$ is of the form

$$f(a)f(s)^{-1}$$

for some $a \in A$ and $s \in S$.

Proof. For (i), we have

$$\frac{s}{1} \cdot \frac{1}{s} = 1.$$

For (ii), if

$$\frac{a}{1} = 0,$$

then by the definition of the equivalence relation there exists $s \in S$ such that

$$sa = 0.$$

For (iii), every element is by definition of the form a/s. □

Corollary 3.5. *Let $g : A \to B$ be a ring homomorphism satisfying the following conditions:*

(i) $g(s)$ is a unit in B for all $s \in S$;

(ii) if $g(a) = 0$, then $as = 0$ for some $s \in S$;

(iii) every element of B is of the form $g(a)g(s)^{-1}$.

Then the induced homomorphism

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

is an isomorphism.

Proof. By the universal property, there is a unique homomorphism

$$h : S^{-1}A \to B$$

with

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

Condition (iii) implies that h is surjective. If

$$h\left(\frac{a}{s}\right) = 0,$$

then $g(a) = 0$. By condition (ii), there exists $t \in S$ such that $ta = 0$. Hence

$$\frac{a}{s} = 0$$

in $S^{-1}A$. Thus h is injective. □

Remark 3.6. If A is an integral domain and

$$S = A \setminus \{0\},$$

then $S^{-1}A$ is the field of fractions of A.

Definition 3.7. A ring A is called a *local ring* if it has a unique maximal ideal.

Let $\mathfrak{p} \in \mathrm{Spec}(A)$. Then

$$S = A \setminus \mathfrak{p}$$

is multiplicatively closed. We write

$$A_{\mathfrak{p}} = S^{-1}A.$$

Proposition 3.8. *Let $\mathfrak{p} \in \operatorname{Spec}(A)$. Then $A_{\mathfrak{p}}$ is a local ring. Its unique maximal ideal is*

$$\mathfrak{p}A_{\mathfrak{p}} = \left\{ \frac{a}{s} : a \in \mathfrak{p},\ s \notin \mathfrak{p} \right\}.$$

Proof. Let

$$\mathfrak{m} = \mathfrak{p}A_{\mathfrak{p}}.$$

If

$$\frac{a}{s} \notin \mathfrak{m},$$

then $a \notin \mathfrak{p}$. Hence $a \in S$, so

$$\frac{a}{s}$$

is a unit in $A_{\mathfrak{p}}$. Thus every element outside $\mathfrak{m}$ is a unit. Therefore every proper ideal is contained in $\mathfrak{m}$, and $\mathfrak{m}$ is the unique maximal ideal. □

Remark 3.9. The process

$$A \longmapsto A_{\mathfrak{p}}$$

is called *localization at the prime ideal* $\mathfrak{p}$. It algebraically captures the behavior of A near the point $\mathfrak{p} \in \operatorname{Spec}(A)$.

3.2 Localization of Modules

Let M be an A-module and let $S \subseteq A$ be multiplicatively closed. Define an equivalence relation on $M \times S$ by

$$(m, s) \sim (m', s')$$

if there exists $t \in S$ such that

$$t(s'm - sm') = 0.$$

The equivalence class of (m, s) is denoted by

$$\frac{m}{s}.$$

Definition 3.10. The set of equivalence classes is denoted by $S^{-1}M$. It is an $S^{-1}A$-module with operations

$$\frac{m}{s} + \frac{m'}{s'} = \frac{s'm + sm'}{ss'},$$

and

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

If $S = A \setminus \mathfrak{p}$, we write

$$M_{\mathfrak{p}} = S^{-1}M.$$

A homomorphism $u : M \to N$ induces a homomorphism

$$S^{-1}u : S^{-1}M \longrightarrow S^{-1}N, \qquad \frac{m}{s} \longmapsto \frac{u(m)}{s}.$$

Thus localization defines a functor from the category of A-modules to the category of $S^{-1}A$-modules.

Proposition 3.11. *The localization functor*

$$M \longmapsto S^{-1}M$$

is exact. That is, if

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

is exact at M, then

$$S^{-1}M' \xrightarrow{S^{-1}f} S^{-1}M \xrightarrow{S^{-1}g} S^{-1}M''$$

is exact at $S^{-1}M$.

Proof. Since $g \circ f = 0$, we have

$$S^{-1}g \circ S^{-1}f = 0,$$

so

$$\mathrm{im}(S^{-1}f) \subseteq \ker(S^{-1}g).$$

Conversely, suppose

$$\frac{m}{s} \in \ker(S^{-1}g).$$

Then

$$\frac{g(m)}{s} = 0$$

in $S^{-1}M''$. Hence there exists $t \in S$ such that

$$tg(m) = 0.$$

Thus

$$g(tm) = 0,$$

so $tm \in \ker(g) = \mathrm{im}(f)$. Hence there exists $m' \in M'$ such that

$$f(m') = tm.$$

Therefore

$$\frac{m}{s} = \frac{tm}{ts} = \frac{f(m')}{ts} = (S^{-1}f)\left(\frac{m'}{ts}\right).$$

Thus

$$\ker(S^{-1}g) = \mathrm{im}(S^{-1}f).$$

□

Proposition 3.12. *For every A-module M, there is a natural isomorphism*

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

It is given by

$$\frac{a}{s} \otimes m \longmapsto \frac{am}{s}.$$

Proof. The map

$$S^{-1}A \times M \longrightarrow S^{-1}M, \qquad \left(\frac{a}{s}, m\right) \longmapsto \frac{am}{s}$$

is A-balanced, so it induces an $S^{-1}A$-module homomorphism

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

Every element of $S^{-1}M$ has the form

$$\frac{m}{s},$$

which is the image of

$$\frac{1}{s} \otimes m.$$

Thus the map is surjective.

If

$$\frac{m}{s} = 0,$$

then there exists $t \in S$ such that $tm = 0$. Hence

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

This proves injectivity. □

Corollary 3.13. *The A-module $S^{-1}A$ is flat.*

Proof. The functor

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

is naturally isomorphic to the exact functor

$$S^{-1}(-).$$

Hence $S^{-1}A$ is flat over A. □

Proposition 3.14. *Let M, N be A-modules. Then there is a natural isomorphism of $S^{-1}A$-modules*

$$S^{-1}M \otimes_{S^{-1}A} S^{-1}N \cong S^{-1}(M \otimes_A N).$$

It is given by

$$\frac{m}{s} \otimes \frac{n}{t} \longmapsto \frac{m \otimes n}{st}.$$

Proof. Using the previous proposition, we compute

$$S^{-1}M \otimes_{S^{-1}A} S^{-1}N \cong (S^{-1}A \otimes_A M) \otimes_{S^{-1}A} (S^{-1}A \otimes_A N).$$

By associativity of tensor products, this is naturally isomorphic to

$$S^{-1}A \otimes_A (M \otimes_A N) \cong S^{-1}(M \otimes_A N).$$

The explicit formula follows from these identifications. □

3.3 Local Properties

Definition 3.15. A property $\mathcal{P}$ of rings, or of modules, is called a *local property* if an object has $\mathcal{P}$ precisely when all of its localizations at prime ideals have $\mathcal{P}$.

Proposition 3.16. *Let M be an A-module. The following are equivalent.*

(i) $M = 0$.

(ii) $M_{\mathfrak{p}} = 0$ *for all* $\mathfrak{p} \in \operatorname{Spec}(A)$.

(iii) $M_{\mathfrak{m}} = 0$ *for all maximal ideals* $\mathfrak{m} \in \operatorname{Max}(A)$.

Proof. Clearly (i) implies (ii), and (ii) implies (iii).

Assume (iii). Suppose $M \neq 0$, and choose $0 \neq x \in M$. Then

$$\operatorname{Ann}(x) \neq A.$$

Hence $\operatorname{Ann}(x)$ is contained in some maximal ideal $\mathfrak{m}$. The element

$$\frac{x}{1} \in M_{\mathfrak{m}}$$

is nonzero. Indeed, if $x/1 = 0$, then there exists $s \notin \mathfrak{m}$ such that $sx = 0$, so $s \in \operatorname{Ann}(x) \subseteq \mathfrak{m}$, a contradiction. Hence $M_{\mathfrak{m}} \neq 0$. □

Proposition 3.17. *Let $\varphi : M \to N$ be a homomorphism of A-modules. The following are equivalent.*

(i) φ *is injective.*

(ii) $\varphi_{\mathfrak{p}} : M_{\mathfrak{p}} \to N_{\mathfrak{p}}$ *is injective for all* $\mathfrak{p} \in \operatorname{Spec}(A)$.

(iii) $\varphi_{\mathfrak{m}} : M_{\mathfrak{m}} \to N_{\mathfrak{m}}$ *is injective for all maximal ideals* $\mathfrak{m} \in \operatorname{Max}(A)$.

Proof. The implication (i) ⇒ (ii) follows from the exactness of localization, and (ii) ⇒ (iii) is trivial.

For (iii) ⇒ (i), let

$$K = \ker(\varphi).$$

Then

$$K_{\mathfrak{m}} = \ker(\varphi_{\mathfrak{m}}) = 0$$

for every maximal ideal $\mathfrak{m}$. By the previous proposition, $K = 0$. Hence φ is injective. □

Proposition 3.18. *For an A-module M, the following are equivalent.*

(i) M *is flat over* A.

(ii) $M_{\mathfrak{p}}$ *is flat over* $A_{\mathfrak{p}}$ *for every* $\mathfrak{p} \in \operatorname{Spec}(A)$.

(iii) $M_{\mathfrak{m}}$ *is flat over* $A_{\mathfrak{m}}$ *for every maximal ideal* $\mathfrak{m} \in \operatorname{Max}(A)$.

Proof. If M is flat, then localization gives

$$M_{\mathfrak{p}} \cong A_{\mathfrak{p}} \otimes_A M,$$

and therefore $M_{\mathfrak{p}}$ is flat over $A_{\mathfrak{p}}$. Thus (i) implies (ii), and (ii) implies (iii).

Assume (iii). To prove that M is flat, it suffices to show that for every injective homomorphism

$$N \longrightarrow Q$$

of A-modules, the induced map

$$N \otimes_A M \longrightarrow Q \otimes_A M$$

is injective. Localizing at every maximal ideal $\mathfrak{m}$, we get

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

and similarly for Q. Since $M_{\mathfrak{m}}$ is flat, the localized map is injective for every maximal ideal $\mathfrak{m}$. By the previous proposition, the original map is injective. Hence M is flat. □

Let

$$f : A \longrightarrow S^{-1}A$$

be the natural homomorphism. If $\mathfrak{a}$ is an ideal of A, its extension to $S^{-1}A$ is

$$\mathfrak{a}^e = S^{-1}\mathfrak{a}.$$

If $\mathfrak{b}$ is an ideal of $S^{-1}A$, its contraction to A is

$$\mathfrak{b}^c = f^{-1}(\mathfrak{b}).$$

Proposition 3.19. *Let $S \subseteq A$ be multiplicatively closed.*

(i) Every ideal of $S^{-1}A$ is extended from an ideal of A.

(ii) For every ideal $\mathfrak{a} \subseteq A$,

$$\mathfrak{a}^{ec} = \bigcup_{s \in S} (\mathfrak{a} : s),$$

where

$$(\mathfrak{a} : s) = \{x \in A : sx \in \mathfrak{a}\}.$$

(iii) An ideal $\mathfrak{a}$ of A is contracted from $S^{-1}A$ if and only if no element of S is a zero-divisor in $A/\mathfrak{a}$.

(iv) Prime ideals of $S^{-1}A$ are in one-to-one correspondence with prime ideals of A which do not meet S.

(v) Localization commutes with finite sums, finite products, finite intersections, and taking radicals.

Proof. Let $\mathfrak{b}$ be an ideal of $S^{-1}A$. If

$$\frac{x}{s} \in \mathfrak{b},$$

then

$$\frac{x}{1} = \frac{s}{1}\frac{x}{s} \in \mathfrak{b}.$$

Thus every element of $\mathfrak{b}$ is obtained from an element of its contraction. Hence

$$\mathfrak{b} = (\mathfrak{b}^c)^e.$$

For (ii), we have

$$x \in \mathfrak{a}^{ec}$$

if and only if

$$\frac{x}{1} \in S^{-1}\mathfrak{a}.$$

This holds if and only if there exist $a \in \mathfrak{a}$ and $s \in S$ such that

$$\frac{x}{1} = \frac{a}{s}.$$

Equivalently, there exists $t \in S$ such that

$$t(sx - a) = 0.$$

Thus

$$tsx = ta \in \mathfrak{a},$$

so $x \in (\mathfrak{a} : ts)$. Conversely, if $sx \in \mathfrak{a}$ for some $s \in S$, then

$$\frac{x}{1} = \frac{sx}{s} \in S^{-1}\mathfrak{a}.$$

Hence

$$\mathfrak{a}^{ec} = \bigcup_{s \in S} (\mathfrak{a} : s).$$

For (iii), $\mathfrak{a}$ is contracted if and only if

$$\mathfrak{a} = \mathfrak{a}^{ec}.$$

By (ii), this is equivalent to the condition that whenever $sx \in \mathfrak{a}$ for some $s \in S$, then $x \in \mathfrak{a}$. This says precisely that no element of S is a zero-divisor in $A/\mathfrak{a}$.

For (iv), if $\mathfrak{q} \in \operatorname{Spec}(S^{-1}A)$, then $\mathfrak{q}^c$ is a prime ideal of A and

$$\mathfrak{q}^c \cap S = \varnothing.$$

Conversely, if $\mathfrak{p} \in \operatorname{Spec}(A)$ and

$$\mathfrak{p} \cap S = \varnothing,$$

then

$$S^{-1}\mathfrak{p}$$

is a prime ideal of $S^{-1}A$. These two operations are inverse to each other by (i).

The statements about finite sums, products, intersections, and radicals follow by checking membership after writing elements as fractions. □

Corollary 3.20. *For a prime ideal $\mathfrak{p} \in \operatorname{Spec}(A)$, the prime ideals of $A_\mathfrak{p}$ are in one-to-one correspondence with the prime ideals*

$$\mathfrak{q} \subseteq \mathfrak{p}$$

of A.

Proof. Apply the prime ideal correspondence to

$$S = A \setminus \mathfrak{p}.$$

A prime ideal $\mathfrak{q}$ of A does not meet S precisely when

$$\mathfrak{q} \subseteq \mathfrak{p}.$$

□

3.4 Support

Definition 3.21. Let A be a ring and let M be an A-module. The *support* of M is

$$\operatorname{Supp}(M) = \{\mathfrak{p} \in \operatorname{Spec}(A) : M_{\mathfrak{p}} \neq 0\}.$$

Proposition 3.22. *Let M be an A-module.*

(i) $M \neq 0$ *if and only if* $\operatorname{Supp}(M) \neq \varnothing$.

(ii)

$$\operatorname{Supp}(A/\mathfrak{a}) = V(\mathfrak{a}).$$

(iii) If

$$0 \to M' \to M \to M'' \to 0$$

is exact, then

$$\operatorname{Supp}(M) = \operatorname{Supp}(M') \cup \operatorname{Supp}(M'').$$

(iv) If

$$M = \sum_i M_i,$$

then

$$\operatorname{Supp}(M) = \bigcup_i \operatorname{Supp}(M_i).$$

(v) If M is finitely generated, then

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

(vi) If M and N are finitely generated, then

$$\operatorname{Supp}(M \otimes_A N) = \operatorname{Supp}(M) \cap \operatorname{Supp}(N).$$

Proof. For (i), use the local criterion for vanishing proved above.

For (ii),

$$(A/\mathfrak{a})_{\mathfrak{p}} \cong A_{\mathfrak{p}}/\mathfrak{a}A_{\mathfrak{p}}.$$

This is nonzero exactly when

$$\mathfrak{a} \subseteq \mathfrak{p}.$$

Hence

$$\operatorname{Supp}(A/\mathfrak{a}) = V(\mathfrak{a}).$$

For (iii), localize the short exact sequence at $\mathfrak{p}$:

$$0 \to M'_{\mathfrak{p}} \to M_{\mathfrak{p}} \to M''_{\mathfrak{p}} \to 0.$$

Then $M_{\mathfrak{p}} = 0$ if and only if both $M'_{\mathfrak{p}} = 0$ and $M''_{\mathfrak{p}} = 0$.

For (iv), localization commutes with sums.

For (v), if $\mathfrak{p} \in \operatorname{Supp}(M)$, then there exists $x \in M$ such that

$$\frac{x}{1} \neq 0$$

in $M_{\mathfrak{p}}$. This implies that no element of $A \setminus \mathfrak{p}$ annihilates x. Hence

$$\operatorname{Ann}(M) \subseteq \mathfrak{p}.$$

Conversely, if M is finitely generated and

$$M_{\mathfrak{p}} = 0,$$

then for generators $x_1, \ldots, x_n$ of M, there are elements $s_i \notin \mathfrak{p}$ such that

$$s_i x_i = 0.$$

Then

$$s = s_1 \cdots s_n \notin \mathfrak{p}$$

annihilates M, so

$$\operatorname{Ann}(M) \not\subseteq \mathfrak{p}.$$

Thus

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

For (vi), localizing at $\mathfrak{p}$ gives

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

If one of $M_{\mathfrak{p}}$ and $N_{\mathfrak{p}}$ is zero, then the tensor product is zero. Conversely, if both are nonzero and finitely generated over the local ring $A_{\mathfrak{p}}$, then their tensor product is nonzero by Nakayama's lemma. Hence the equality of supports follows. □

3.5 Saturated Multiplicative Sets

Definition 3.23. A multiplicatively closed subset S of a ring A is called *saturated* if

$$xy \in S \quad \Longleftrightarrow \quad x \in S \text{ and } y \in S.$$

Proposition 3.24. *A multiplicatively closed subset S of A is saturated if and only if*

$$A \setminus S$$

is a union of prime ideals.

Proof. If S is saturated and $xy \notin S$, then at least one of x, y is not in S. This shows that $A \setminus S$ behaves like a union of prime ideals.

Conversely, suppose

$$A \setminus S = \bigcup_{\lambda} \mathfrak{p}_\lambda$$

is a union of prime ideals. If $xy \in S$ and $x \notin S$, then $x \in \mathfrak{p}_\lambda$ for some λ. Since $\mathfrak{p}_\lambda$ is prime, $xy \in \mathfrak{p}_\lambda$, a contradiction. Thus $x \in S$. Similarly $y \in S$. Hence S is saturated. □

Remark 3.25. The nontrivial direction may also be proved using Zorn's lemma: if S is not a union of complements of prime ideals, one constructs a maximal ideal disjoint from S and proves that it is prime.

3.6 Contraction of Prime Ideals

Proposition 3.26. *Let*

$$f : A \longrightarrow B$$

be a ring homomorphism and let $\mathfrak{p} \in \operatorname{Spec}(A)$. *Then* $\mathfrak{p}$ *is the contraction of a prime ideal of* B *if and only if*

$$\mathfrak{p}^{ec} = \mathfrak{p},$$

where extension and contraction are taken with respect to f.

Proof. If $\mathfrak{p} = \mathfrak{q}^c$ for some $\mathfrak{q} \in \operatorname{Spec}(B)$, then

$$\mathfrak{p}^{ec} \subseteq \mathfrak{q}^c = \mathfrak{p},$$

and the reverse inclusion is automatic. Hence

$$\mathfrak{p}^{ec} = \mathfrak{p}.$$

Conversely, assume

$$\mathfrak{p}^{ec} = \mathfrak{p}.$$

Let $\overline{S}$ be the image of $A \setminus \mathfrak{p}$ in $B/\mathfrak{p}^e$. Since

$$\mathfrak{p}^{ec} = \mathfrak{p},$$

the set $\overline{S}$ does not contain zero. Hence, after localizing $B/\mathfrak{p}^e$ at $\overline{S}$, we get a nonzero ring. Choose a maximal ideal in this localization and contract it back to B. This gives a prime ideal $\mathfrak{q}$ of B whose contraction is $\mathfrak{p}$. □

3.7 Faithfully Flat Extensions

Definition 3.27. An A-module M is called *faithfully flat* if it is flat and for every nonzero A-module N,

$$M \otimes_A N \neq 0.$$

Proposition 3.28. *Let* B *be a flat* A*-algebra. The following are equivalent.*

(i) For every ideal $\mathfrak{a}$ *of* A,

$$\mathfrak{a}^{ec} = \mathfrak{a}.$$

(ii) The map

$$\operatorname{Spec}(B) \longrightarrow \operatorname{Spec}(A)$$

is surjective.

(iii) For every maximal ideal $\mathfrak{m}$ *of* A*,*

$$\mathfrak{m}B \neq B.$$

(iv) B *is faithfully flat as an* A*-module.*

Proof. We prove the equivalences.

First, (i) implies (ii). Let $\mathfrak{p} \in \operatorname{Spec}(A)$. By (i),

$$\mathfrak{p}^{ec} = \mathfrak{p}.$$

By the previous proposition, $\mathfrak{p}$ is the contraction of a prime ideal of B. Hence $\operatorname{Spec}(B) \to \operatorname{Spec}(A)$ is surjective.

The implication (ii) implies (iii) is immediate: if $\mathfrak{m}B = B$, then no prime ideal of B can contract to $\mathfrak{m}$.

Assume (iii). Let M be a nonzero A-module. Choose $0 \neq x \in M$ and let

$$M' = Ax.$$

Then

$$M' \cong A/\mathfrak{a}$$

for some proper ideal $\mathfrak{a}$. Choose a maximal ideal $\mathfrak{m}$ containing $\mathfrak{a}$. Since $\mathfrak{m}B \neq B$, there exists a prime ideal of B lying over $\mathfrak{m}$. Hence

$$B \otimes_A A/\mathfrak{a} \cong B/\mathfrak{a}B \neq 0.$$

Since B is flat, the injection

$$M' \hookrightarrow M$$

gives an injection

$$B \otimes_A M' \hookrightarrow B \otimes_A M.$$

Thus

$$B \otimes_A M \neq 0.$$

Therefore B is faithfully flat.

Finally, assume (iv). For any ideal $\mathfrak{a} \subseteq A$, the map

$$A/\mathfrak{a} \longrightarrow B/\mathfrak{a}B$$

is injective because tensoring with B is faithful. This is exactly the statement

$$\mathfrak{a}^{ec} = \mathfrak{a}.$$

Thus (iv) implies (i). □

Proposition 3.29. *Let $f : A \to B$ be a flat homomorphism of rings. Let $\mathfrak{q} \in \mathrm{Spec}(B)$ and set*

$$\mathfrak{p} = \mathfrak{q}^c.$$

Then the induced map

$$\mathrm{Spec}(B_{\mathfrak{q}}) \longrightarrow \mathrm{Spec}(A_{\mathfrak{p}})$$

is surjective.

Proof. Since B is flat over A, the localization $B_{\mathfrak{q}}$ is flat over $A_{\mathfrak{p}}$. Moreover, $B_{\mathfrak{q}}$ is a local ring whose maximal ideal contracts to the maximal ideal of $A_{\mathfrak{p}}$. Hence $B_{\mathfrak{q}}$ is faithfully flat over $A_{\mathfrak{p}}$. By the preceding proposition, the induced map on spectra is surjective. □

Chapter 4

Primary Decomposition

Throughout this chapter, A denotes a commutative ring with identity.

4.1 Primary Ideals

Definition 4.1. An ideal $\mathfrak{q}$ of A is called *primary* if $\mathfrak{q} \neq A$ and whenever

$$xy \in \mathfrak{q},$$

then either $x \in \mathfrak{q}$ or $y^n \in \mathfrak{q}$ for some $n > 0$.

Equivalently, $\mathfrak{q}$ is primary if $A/\mathfrak{q} \neq 0$ and every zero-divisor in $A/\mathfrak{q}$ is nilpotent. Indeed, if $\overline{x}\overline{y} = 0$ and $\overline{x} \neq 0$, then $xy \in \mathfrak{q}$ and $x \notin \mathfrak{q}$, hence $y^n \in \mathfrak{q}$ for some $n > 0$.

Proposition 4.2. *If $\mathfrak{q}$ is a primary ideal, then* $\operatorname{rad}(\mathfrak{q})$ *is the smallest prime ideal containing $\mathfrak{q}$.*

Proof. It is clear that $\mathfrak{q} \subseteq \operatorname{rad}(\mathfrak{q})$ and that $\operatorname{rad}(\mathfrak{q})$ is contained in every prime ideal containing $\mathfrak{q}$. Hence it suffices to prove that $\operatorname{rad}(\mathfrak{q})$ is prime.

Let $xy \in \operatorname{rad}(\mathfrak{q})$. Then $(xy)^n = x^n y^n \in \mathfrak{q}$ for some $n > 0$. If $x \notin \operatorname{rad}(\mathfrak{q})$, then $x^n \notin \mathfrak{q}$. Since $\mathfrak{q}$ is primary and $x^n y^n \in \mathfrak{q}$, it follows that $(y^n)^m = y^{nm} \in \mathfrak{q}$ for some $m > 0$. Thus $y \in \operatorname{rad}(\mathfrak{q})$. Therefore $\operatorname{rad}(\mathfrak{q})$ is prime. □

Definition 4.3. If $\mathfrak{q}$ is primary and $\operatorname{rad}(\mathfrak{q}) = \mathfrak{p}$, then $\mathfrak{q}$ is called $\mathfrak{p}$-*primary*.

Example 4.4. The primary ideals in $\mathbb{Z}$ are (0) and (p^n), where p is prime and $n \geq 1$. The ideal (p^n) is (p)-primary.

Example 4.5. In $k[x, y]$, the ideal $(x, y)^n$ is (x, y)-primary. More generally, if $\mathfrak{m}$ is a maximal ideal, then every ideal $\mathfrak{q}$ such that

$$\mathfrak{m}^N \subseteq \mathfrak{q} \subseteq \mathfrak{m}$$

for some $N > 0$ is $\mathfrak{m}$-primary.

Lemma 4.6. *Let $\mathfrak{q}$ be a $\mathfrak{p}$-primary ideal and let $x \in A$.*

(i) If $x \in \mathfrak{q}$, then $(\mathfrak{q} : x) = A$.

(ii) If $x \notin \mathfrak{q}$, then $\operatorname{rad}(\mathfrak{q} : x) = \mathfrak{p}$.

(iii) If $x \notin \mathfrak{p}$, then $(\mathfrak{q} : x) = \mathfrak{q}$.

Proof. (i) is immediate from the definition of the ideal quotient.

For (ii), suppose $x \notin \mathfrak{q}$. If $y \in \operatorname{rad}(\mathfrak{q} : x)$, then $y^n x \in \mathfrak{q}$ for some $n > 0$. Since $x \notin \mathfrak{q}$ and $\mathfrak{q}$ is primary, we get $y \in \operatorname{rad}(\mathfrak{q}) = \mathfrak{p}$. Thus $\operatorname{rad}(\mathfrak{q} : x) \subseteq \mathfrak{p}$. Conversely, if $y \in \mathfrak{p}$, then $y^n \in \mathfrak{q}$ for some $n > 0$, hence $y^n x \in \mathfrak{q}$, so $y \in \operatorname{rad}(\mathfrak{q} : x)$. Therefore $\operatorname{rad}(\mathfrak{q} : x) = \mathfrak{p}$.

For (iii), let $y \in (\mathfrak{q} : x)$. Then $xy \in \mathfrak{q}$. Since $x \notin \mathfrak{p} = \operatorname{rad}(\mathfrak{q})$, no power of x lies in $\mathfrak{q}$. By primaryness, $y \in \mathfrak{q}$. Hence $(\mathfrak{q} : x) \subseteq \mathfrak{q}$, while the reverse inclusion is obvious. □

Lemma 4.7. *If $\mathfrak{q}_1, \ldots, \mathfrak{q}_n$ are $\mathfrak{p}$-primary ideals, then*

$$\mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n$$

is also $\mathfrak{p}$-primary.

Proof. Let $\mathfrak{q} = \bigcap_i \mathfrak{q}_i$. Then

$$\operatorname{rad}(\mathfrak{q}) = \bigcap_i \operatorname{rad}(\mathfrak{q}_i) = \mathfrak{p}.$$

Suppose $xy \in \mathfrak{q}$ and $x \notin \mathfrak{q}$. Then $x \notin \mathfrak{q}_j$ for some j. Since $xy \in \mathfrak{q}_j$ and $\mathfrak{q}_j$ is $\mathfrak{p}$-primary, we have $y \in \mathfrak{p}$. Hence $y^N \in \mathfrak{q}_i$ for each i and some exponent N sufficiently large. Therefore $y^N \in \mathfrak{q}$, so $\mathfrak{q}$ is primary. Since its radical is $\mathfrak{p}$, it is $\mathfrak{p}$-primary. □

4.2 Primary Decompositions

Definition 4.8. A *primary decomposition* of an ideal $\mathfrak{a}$ is an expression

$$\mathfrak{a} = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n$$

as a finite intersection of primary ideals. An ideal admitting such a decomposition is called *decomposable*.

Definition 4.9. A primary decomposition

$$\mathfrak{a} = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n$$

is called *minimal* if

(i) the prime ideals $\operatorname{rad}(\mathfrak{q}_i)$ are distinct;

(ii) no $\mathfrak{q}_i$ contains the intersection of the remaining primary components, equivalently no component can be omitted.

Every primary decomposition can be made minimal: components with the same radical can be replaced by their intersection, and redundant components can be omitted.

Definition 4.10. Let $\mathfrak{a}$ be a decomposable ideal and let

$$\mathfrak{a} = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n$$

be a minimal primary decomposition. The prime ideals

$$\mathfrak{p}_i = \operatorname{rad}(\mathfrak{q}_i)$$

are called the *prime ideals associated with* $\mathfrak{a}$, or the *associated prime ideals belonging to* $\mathfrak{a}$.

4.3 The First Uniqueness Theorem

Theorem 4.11 (First Uniqueness Theorem)**.** *Let $\mathfrak{a}$ be a decomposable ideal of A, and let*

$$\mathfrak{a} = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n$$

be a minimal primary decomposition. Put $\mathfrak{p}_i = \operatorname{rad}(\mathfrak{q}_i)$. Then the prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ are precisely the prime ideals which occur among the ideals

$$\operatorname{rad}(\mathfrak{a} : x), \qquad x \in A.$$

In particular, the set $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$ is independent of the chosen minimal primary decomposition.

Proof. For $x \in A$, we have

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

and hence

$$\operatorname{rad}(\mathfrak{a} : x) = \bigcap_{i=1}^{n} \operatorname{rad}(\mathfrak{q}_i : x).$$

By the lemma above, if $x \notin \mathfrak{q}_i$, then $\operatorname{rad}(\mathfrak{q}_i : x) = \mathfrak{p}_i$; if $x \in \mathfrak{q}_i$, then $(\mathfrak{q}_i : x) = A$ and contributes nothing to the radical. Therefore

$$\operatorname{rad}(\mathfrak{a} : x) = \bigcap_{x \notin \mathfrak{q}_i} \mathfrak{p}_i.$$

Thus if $\operatorname{rad}(\mathfrak{a} : x)$ is prime, then it is equal to one of the $\mathfrak{p}_i$.

Conversely, fix i. Since the decomposition is minimal, there exists

$$x \in \bigcap_{j \neq i} \mathfrak{q}_j$$

with $x \notin \mathfrak{q}_i$. Then

$$(\mathfrak{a} : x) = (\mathfrak{q}_i : x),$$

because all other components become the unit ideal after taking the quotient by x. Hence

$$\operatorname{rad}(\mathfrak{a} : x) = \operatorname{rad}(\mathfrak{q}_i : x) = \mathfrak{p}_i.$$

Thus each $\mathfrak{p}_i$ occurs in this way, and the set of such primes is intrinsic to $\mathfrak{a}$. □

Definition 4.12. Among the associated prime ideals of $\mathfrak{a}$, the minimal elements are called the *minimal prime ideals associated with* $\mathfrak{a}$. The remaining associated prime ideals are called *embedded prime ideals*.

Proposition 4.13. *Let $\mathfrak{a}$ be decomposable. Every prime ideal containing $\mathfrak{a}$ contains an associated prime ideal of $\mathfrak{a}$. Consequently, the minimal prime ideals over $\mathfrak{a}$ are precisely the minimal associated primes of $\mathfrak{a}$.*

Proof. Let $\mathfrak{a} = \bigcap_i \mathfrak{q}_i$ be a minimal primary decomposition and let $\mathfrak{p}_i = \operatorname{rad}(\mathfrak{q}_i)$. If $\mathfrak{p} \supseteq \mathfrak{a}$ is prime, then

$$\prod_i \mathfrak{q}_i \subseteq \bigcap_i \mathfrak{q}_i = \mathfrak{a} \subseteq \mathfrak{p}.$$

Since $\mathfrak{p}$ is prime, $\mathfrak{q}_i \subseteq \mathfrak{p}$ for some i, hence $\mathfrak{p}_i = \operatorname{rad}(\mathfrak{q}_i) \subseteq \mathfrak{p}$.

If $\mathfrak{p}$ is minimal over $\mathfrak{a}$, the associated prime $\mathfrak{p}_i \subseteq \mathfrak{p}$ must equal $\mathfrak{p}$. This proves that the minimal primes over $\mathfrak{a}$ are associated, and the converse follows from the preceding containment statement. □

4.4 Associated Prime Ideals of Modules

The preceding definition of associated primes of an ideal is best understood through modules.

Definition 4.14. Let M be an A-module. A prime ideal $\mathfrak{p}$ is called an *associated prime* of M if there exists $x \in M$ such that

$$\mathfrak{p} = \operatorname{Ann}_A(x).$$

The set of all associated primes of M is denoted by

$$\operatorname{Ass}_A(M).$$

Remark 4.15. For an ideal $\mathfrak{a}$, the associated prime ideals belonging to $\mathfrak{a}$ are exactly the associated primes of the module $A/\mathfrak{a}$:

$$\operatorname{Ass}_A(A/\mathfrak{a}) = \{\text{associated prime ideals belonging to } \mathfrak{a}\}.$$

Indeed, for $\overline{x} \in A/\mathfrak{a}$, one has

$$\operatorname{Ann}_A(\overline{x}) = (\mathfrak{a} : x).$$

Proposition 4.16. *Assume that A is Noetherian. If M is a nonzero finitely generated A-module, then $\operatorname{Ass}_A(M)$ is nonempty.*

Proof. Consider the set

$$\{\operatorname{Ann}_A(x) : 0 \neq x \in M\}.$$

Since A is Noetherian, this set has a maximal element, say $\operatorname{Ann}_A(x)$. We claim that $\operatorname{Ann}_A(x)$ is prime.

Suppose $ab \in \operatorname{Ann}_A(x)$ and $a \notin \operatorname{Ann}_A(x)$. Then $ax \neq 0$. Moreover,

$$\operatorname{Ann}_A(x) \subseteq \operatorname{Ann}_A(ax),$$

since every element annihilating x also annihilates ax. By maximality, we have

$$\operatorname{Ann}_A(ax) = \operatorname{Ann}_A(x).$$

But $b(ax) = abx = 0$, so $b \in \operatorname{Ann}_A(ax) = \operatorname{Ann}_A(x)$. Hence $\operatorname{Ann}_A(x)$ is prime. □

Proposition 4.17. *Assume that A is Noetherian and that $\mathfrak{q}$ is $\mathfrak{p}$-primary. Then*

$$\operatorname{Ass}_A(A/\mathfrak{q}) = \{\mathfrak{p}\}.$$

Proof. Let $\mathfrak{r} \in \mathrm{Ass}_A(A/\mathfrak{q})$. Then $\mathfrak{r} = \mathrm{Ann}_A(\overline{x}) = (\mathfrak{q} : x)$ for some $x \notin \mathfrak{q}$. Since $\mathfrak{r}$ is prime and

$$\mathrm{rad}(\mathfrak{q} : x) = \mathfrak{p}$$

by the lemma on ideal quotients, we get $\mathfrak{r} = \mathfrak{p}$. Thus $\mathrm{Ass}_A(A/\mathfrak{q}) \subseteq \{\mathfrak{p}\}$.

The module $A/\mathfrak{q}$ is nonzero and finitely generated over the Noetherian ring A, so its set of associated primes is nonempty. Hence $\mathrm{Ass}_A(A/\mathfrak{q}) = \{\mathfrak{p}\}$. □

Proposition 4.18. *Let*

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$$

be an exact sequence of A-modules. Then

$$\mathrm{Ass}_A(M') \subseteq \mathrm{Ass}_A(M) \subseteq \mathrm{Ass}_A(M') \cup \mathrm{Ass}_A(M'').$$

Proof. The first inclusion is immediate, since an element of M' may be regarded as an element of M.

For the second inclusion, let $\mathfrak{p} = \mathrm{Ann}_A(x)$ for some $x \in M$. Then $Ax \simeq A/\mathfrak{p}$. Consider the intersection $Ax \cap M'$.

If $Ax \cap M' = 0$, then the composite $Ax \hookrightarrow M \twoheadrightarrow M''$ is injective, so $A/\mathfrak{p}$ embeds into M''. Hence $\mathfrak{p} \in \mathrm{Ass}_A(M'')$.

If $Ax \cap M' \neq 0$, choose a nonzero element $ax \in Ax \cap M'$. Since $ax \neq 0$, we have $a \notin \mathfrak{p}$. For any $r \in A$,

$$r(ax) = 0 \quad \Longleftrightarrow \quad ra \in \mathfrak{p}.$$

Because $\mathfrak{p}$ is prime and $a \notin \mathfrak{p}$, this is equivalent to $r \in \mathfrak{p}$. Thus $\mathrm{Ann}_A(ax) = \mathfrak{p}$, and so $\mathfrak{p} \in \mathrm{Ass}_A(M')$. □

Corollary 4.19. *If A is Noetherian and M is a finitely generated A-module, then* $\mathrm{Ass}_A(M)$ *is finite.*

Proof. If $M = 0$, there is nothing to prove. Otherwise, choose $x \in M$ such that $\mathrm{Ann}_A(x) = \mathfrak{p}$ is prime. Then $Ax \simeq A/\mathfrak{p}$, and we have an exact sequence

$$0 \longrightarrow A/\mathfrak{p} \longrightarrow M \longrightarrow M/Ax \longrightarrow 0.$$

Since M is Noetherian, repeating this process gives a finite filtration whose successive quotients are of the form $A/\mathfrak{p}_i$. The exact sequence proposition implies that

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

Hence $\mathrm{Ass}_A(M)$ is finite. □

Proposition 4.20. *Assume that A is Noetherian and M is a finitely generated A-module. Then the set of zero-divisors on M is*

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

Here an element $a \in A$ is a zero-divisor on M if $ax = 0$ for some nonzero $x \in M$.

Proof. If $a \in \mathfrak{p} = \mathrm{Ann}_A(x)$ for some associated prime $\mathfrak{p}$, then $ax = 0$ and a is a zero-divisor on M.

Conversely, suppose a is a zero-divisor on M. Then $ax = 0$ for some $0 \neq x \in M$. Consider the cyclic submodule Ax. Since A is Noetherian, Ax has an associated prime $\mathfrak{p} = \mathrm{Ann}_A(y)$ for some nonzero $y \in Ax$. Write $y = bx$. Since $ax = 0$, we also have

$$ay = abx = b(ax) = 0.$$

Thus $a \in \mathrm{Ann}_A(y) = \mathfrak{p}$. The inclusion $Ax \subseteq M$ gives $\mathfrak{p} \in \mathrm{Ass}_A(M)$, and hence a lies in the union of the associated primes of M. □

Proposition 4.21. *Let A be Noetherian and let M be a nonzero finitely generated A-module. Every minimal element of* $\mathrm{Supp}(M)$ *belongs to* $\mathrm{Ass}_A(M)$.

Proof. Let $\mathfrak{p}$ be minimal in $\mathrm{Supp}(M)$. Localize at $\mathfrak{p}$. Then $M_\mathfrak{p} \neq 0$, and $A_\mathfrak{p}$ is Noetherian. Hence $\mathrm{Ass}_{A_\mathfrak{p}}(M_\mathfrak{p})$ is nonempty. Any associated prime of $M_\mathfrak{p}$ corresponds to a prime ideal of A contained in $\mathfrak{p}$ and lying in $\mathrm{Supp}(M)$. By minimality it must be $\mathfrak{p}$. Therefore $\mathfrak{p} \in \mathrm{Ass}_A(M)$. □

Remark 4.22. For a decomposable ideal $\mathfrak{a}$, the zero-divisors of $A/\mathfrak{a}$ are precisely the elements contained in the union of the associated prime ideals belonging to $\mathfrak{a}$.

4.5 Localization of Primary Decompositions

Lemma 4.23. *Let S be a multiplicatively closed subset of A, and let $\mathfrak{q}$ be a $\mathfrak{p}$-primary ideal.*

(i) If $S \cap \mathfrak{p} \neq \varnothing$, then $S^{-1}\mathfrak{q} = S^{-1}A$.

(ii) If $S \cap \mathfrak{p} = \varnothing$, then $S^{-1}\mathfrak{q}$ is an $S^{-1}\mathfrak{p}$-primary ideal of $S^{-1}A$, and its contraction to A is $\mathfrak{q}$.

Proof. If $s \in S \cap \mathfrak{p}$, then $s^n \in \mathfrak{q}$ for some $n > 0$. Hence $s^n/s^n = 1$ belongs to $S^{-1}\mathfrak{q}$, so $S^{-1}\mathfrak{q} = S^{-1}A$.

Now suppose $S \cap \mathfrak{p} = \varnothing$. The radical of $S^{-1}\mathfrak{q}$ is $S^{-1}\mathfrak{p}$. To check primaryness, suppose

$$\frac{x}{s}\frac{y}{t} \in S^{-1}\mathfrak{q},$$

and $x/s \notin S^{-1}\mathfrak{q}$. Then for some $u \in S$ we have $uxy \in \mathfrak{q}$. Since $x/s \notin S^{-1}\mathfrak{q}$, no multiple of x by an element of S lies in $\mathfrak{q}$. By primaryness, $y \in \mathfrak{p}$, hence a power of y/t lies in $S^{-1}\mathfrak{q}$. Thus $S^{-1}\mathfrak{q}$ is primary.

Finally, if $a/1 \in S^{-1}\mathfrak{q}$, then $sa \in \mathfrak{q}$ for some $s \in S$. Since $s \notin \mathfrak{p}$ and $\mathfrak{q}$ is $\mathfrak{p}$-primary, we get $a \in \mathfrak{q}$. Thus the contraction of $S^{-1}\mathfrak{q}$ is exactly $\mathfrak{q}$. □

Proposition 4.24. *Let S be a multiplicatively closed subset of A, and let*

$$\mathfrak{a} = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n$$

be a minimal primary decomposition with $\mathrm{rad}(\mathfrak{q}_i) = \mathfrak{p}_i$. *Then*

$$S^{-1}\mathfrak{a} = \bigcap_{S \cap \mathfrak{p}_i = \varnothing} S^{-1}\mathfrak{q}_i.$$

After omitting redundant components, this is a minimal primary decomposition of $S^{-1}\mathfrak{a}$.

Proof. Localization commutes with finite intersections, so

$$S^{-1}\mathfrak{a} = S^{-1}\mathfrak{q}_1 \cap \cdots \cap S^{-1}\mathfrak{q}_n.$$

If $S \cap \mathfrak{p}_i \neq \varnothing$, then $S^{-1}\mathfrak{q}_i = S^{-1}A$ and the corresponding component disappears. If $S \cap \mathfrak{p}_i = \varnothing$, then $S^{-1}\mathfrak{q}_i$ is $S^{-1}\mathfrak{p}_i$-primary. Removing possible redundant components gives a minimal primary decomposition. □

4.6 The Second Uniqueness Theorem

Definition 4.25. Let $\mathfrak{a}$ be decomposable. A set Σ of associated prime ideals of $\mathfrak{a}$ is called *isolated* if whenever

$$\mathfrak{p} \in \Sigma, \qquad \mathfrak{p}' \in \operatorname{Ass}_A(A/\mathfrak{a}), \qquad \mathfrak{p}' \subseteq \mathfrak{p},$$

then $\mathfrak{p}' \in \Sigma$.

Equivalently, an isolated set is downward closed among the associated primes. In particular, the set of minimal associated primes is isolated.

Theorem 4.26 (Second Uniqueness Theorem)**.** *Let $\mathfrak{a}$ be a decomposable ideal, and let*

$$\mathfrak{a} = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n$$

be a minimal primary decomposition. Put $\mathfrak{p}_i = \operatorname{rad}(\mathfrak{q}_i)$. If

$$\Sigma = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_m\}$$

is an isolated set of associated prime ideals of $\mathfrak{a}$, then the ideal

$$\mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_m$$

is independent of the chosen minimal primary decomposition.

Proof. Let

$$S = A \setminus (\mathfrak{p}_1 \cup \cdots \cup \mathfrak{p}_m).$$

This is a multiplicatively closed subset of A: if $s, t \in S$ and $st \in \mathfrak{p}_i$ for some i, then since $\mathfrak{p}_i$ is prime, either $s \in \mathfrak{p}_i$ or $t \in \mathfrak{p}_i$, a contradiction.

We claim that for $i \leq m$ one has $S \cap \mathfrak{p}_i = \varnothing$, while for $j > m$ one has $S \cap \mathfrak{p}_j \neq \varnothing$. The first assertion is clear from the definition of S. For the second, suppose $S \cap \mathfrak{p}_j = \varnothing$. Then

$$\mathfrak{p}_j \subseteq \mathfrak{p}_1 \cup \cdots \cup \mathfrak{p}_m.$$

By prime avoidance, $\mathfrak{p}_j \subseteq \mathfrak{p}_i$ for some $i \leq m$. Since Σ is isolated and $\mathfrak{p}_j$ is an associated prime contained in $\mathfrak{p}_i \in \Sigma$, it follows that $\mathfrak{p}_j \in \Sigma$, contradiction. Hence $S \cap \mathfrak{p}_j \neq \varnothing$ for every $j > m$.

Localizing the decomposition at S, all components corresponding to $j > m$ disappear, and we obtain

$$S^{-1}\mathfrak{a} = S^{-1}\mathfrak{q}_1 \cap \cdots \cap S^{-1}\mathfrak{q}_m.$$

Now contract this equality back to A. Since $S \cap \mathfrak{p}_i = \varnothing$ for $i \leq m$, the contraction of $S^{-1}\mathfrak{q}_i$ is $\mathfrak{q}_i$. Therefore

$$(S^{-1}\mathfrak{a})^c = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_m.$$

The left-hand side depends only on $\mathfrak{a}$ and on the isolated set Σ, not on the chosen minimal primary decomposition. Hence $\mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_m$ is independent of the decomposition. □

Corollary 4.27. *The primary components corresponding to the minimal associated primes of a decomposable ideal are uniquely determined.*

Proof. The set of minimal associated primes is isolated, so the result follows from the Second Uniqueness Theorem. In particular, if a minimal associated prime occurs alone in an isolated set, its corresponding primary component is unique. □

Chapter 5

Noetherian Rings and Dimension Theory

5.1 Chain Conditions

Definition 5.1. Let M be an A-module.

(i) M is called *Noetherian* if it satisfies the ascending chain condition on submodules: every ascending chain

$$M_1 \subseteq M_2 \subseteq M_3 \subseteq \cdots$$

of submodules is eventually stationary.

(ii) M is called *Artinian* if it satisfies the descending chain condition on submodules: every descending chain

$$M_1 \supseteq M_2 \supseteq M_3 \supseteq \cdots$$

of submodules is eventually stationary.

A ring A is called Noetherian, respectively Artinian, if it is so as an A-module.

Proposition 5.2. *Let M be an A-module and let $N \subseteq M$ be a submodule. Then:*

(i) M is Noetherian if and only if both N and M/N are Noetherian;

(ii) M is Artinian if and only if both N and M/N are Artinian.

Proof. We prove the Noetherian case; the Artinian case is dual.

Suppose first that M is Noetherian. Any ascending chain of submodules of N is also an ascending chain of submodules of M, hence stabilizes. Thus N is Noetherian. If

$$\overline{M}_1 \subseteq \overline{M}_2 \subseteq \cdots$$

is an ascending chain in M/N, then the inverse images of the $\overline{M}_i$ in M form an ascending chain of submodules of M, hence stabilize. Therefore the chain in M/N also stabilizes.

Conversely, suppose that N and M/N are Noetherian, and let

$$M_1 \subseteq M_2 \subseteq \cdots$$

be an ascending chain of submodules of M. Then the chains

$$M_1 \cap N \subseteq M_2 \cap N \subseteq \cdots$$

and

$$(M_1 + N)/N \subseteq (M_2 + N)/N \subseteq \cdots$$

stabilize. Hence there exists r such that for all $i \geq r$ both

$$M_i \cap N = M_r \cap N, \qquad (M_i + N)/N = (M_r + N)/N.$$

We claim that $M_i = M_r$ for all $i \geq r$. Let $x \in M_i$. Since $(M_i + N)/N = (M_r + N)/N$, there are $y \in M_r$ and $n \in N$ such that $x = y + n$. Then $n = x - y \in M_i \cap N = M_r \cap N$, so $n \in M_r$. Hence $x \in M_r$. This proves the claim. □

Corollary 5.3. *Let*

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$$

be an exact sequence of A-modules. Then M is Noetherian, respectively Artinian, if and only if both M' and M'' are so.

Proposition 5.4. *An A-module M is Noetherian if and only if every submodule of M is finitely generated.*

Proof. Suppose first that M is Noetherian, and let $N \subseteq M$. If N were not finitely generated, choose $x_1 \in N$. Since N is not generated by x_1, choose $x_2 \in N \setminus Ax_1$. Continuing in this way gives a strictly increasing chain

$$Ax_1 \subsetneq Ax_1 + Ax_2 \subsetneq Ax_1 + Ax_2 + Ax_3 \subsetneq \cdots,$$

contradicting the Noetherian condition.

Conversely, suppose every submodule of M is finitely generated. Let

$$M_1 \subseteq M_2 \subseteq \cdots$$

be an ascending chain and put $N = \bigcup_i M_i$. Then N is a submodule of M, hence is generated by finitely many elements $x_1, \ldots, x_r$. Each x_j belongs to some M_{n_j}; if $n = \max n_j$, then all x_j lie in M_n, so $N = M_n$. Hence the chain stabilizes. □

Corollary 5.5. *If A is Noetherian and M is a finitely generated A-module, then M is Noetherian.*

Proof. If M is generated by n elements, then there is a surjection $A^n \twoheadrightarrow M$. Since A is Noetherian, so is A^n, and hence so is every quotient of A^n. □

5.2 Artinian Rings

Lemma 5.6. *Let R be a ring and suppose that $\mathfrak{m}_1, \ldots, \mathfrak{m}_r$ are prime ideals such that*

$$\mathfrak{m}_1 \cdots \mathfrak{m}_r = 0.$$

Then R is Artinian if and only if R is Noetherian and every prime ideal of R is one of the $\mathfrak{m}_i$.

Proof. Suppose first that R is Artinian. Then R is Noetherian by the Hopkins–Levitzki theorem below. Moreover every prime ideal of an Artinian ring is maximal, and the spectrum of an Artinian ring is finite. Thus the prime ideals are among finitely many maximal ideals.

Conversely, suppose R is Noetherian and $\operatorname{Spec}(R) = \{\mathfrak{m}_1, \dots, \mathfrak{m}_r\}$ consists of maximal ideals. Since

$$\operatorname{Nil}(R) = \bigcap_{i=1}^{r} \mathfrak{m}_i,$$

and R is Noetherian, the nilradical is nilpotent. Hence for some N we have

$$\operatorname{Nil}(R)^N = 0.$$

Thus a product of finitely many maximal ideals is zero. The successive quotients in the filtration determined by this product are vector spaces over fields $R/\mathfrak{m}_i$ and have finite length. Therefore R has finite length as a module over itself, hence is Artinian. □

Theorem 5.7 (Hopkins–Levitzki)**.** *Every Artinian ring is Noetherian.*

Proof. Let A be an Artinian ring. First, every prime ideal of A is maximal. Indeed, if $\mathfrak{p}$ is prime, then $A/\mathfrak{p}$ is an Artinian domain. In an Artinian domain every nonzero element is a unit: for $0 \neq x$, the descending chain

$$(x) \supseteq (x^2) \supseteq (x^3) \supseteq \cdots$$

stabilizes, say $(x^n) = (x^{n+1})$. Then $x^n = ax^{n+1}$ for some a, so $x^n(1 - ax) = 0$. Since $A/\mathfrak{p}$ is a domain and $x^n \neq 0$, we get $ax = 1$. Thus $A/\mathfrak{p}$ is a field and $\mathfrak{p}$ is maximal.

Next, A has only finitely many maximal ideals. If there were infinitely many distinct maximal ideals $\mathfrak{m}_1, \mathfrak{m}_2, \dots$, then the descending chain

$$\mathfrak{m}_1 \supseteq \mathfrak{m}_1\mathfrak{m}_2 \supseteq \mathfrak{m}_1\mathfrak{m}_2\mathfrak{m}_3 \supseteq \cdots$$

would stabilize. But maximal ideals are pairwise comaximal, and stabilization would force a contradiction after reducing modulo one of the later maximal ideals.

Let $\mathfrak{m}_1, \dots, \mathfrak{m}_r$ be the maximal ideals of A. Since the Jacobson radical

$$J = \bigcap_{i=1}^{r} \mathfrak{m}_i$$

is nil in an Artinian ring, it is nilpotent; say $J^N = 0$. We obtain a finite filtration

$$A \supseteq J \supseteq J^2 \supseteq \cdots \supseteq J^N = 0.$$

Each quotient J^i/J^{i+1} is a module over A/J. But by the Chinese remainder theorem,

$$A/J \cong \prod_{i=1}^{r} A/\mathfrak{m}_i$$

is a finite product of fields, hence is semisimple. Therefore each quotient has finite length, and so A has finite length as an A-module. In particular A is Noetherian. □

Theorem 5.8. *For a ring A, the following are equivalent:*

(i) *A is Artinian;*

(ii) *A is Noetherian and every prime ideal of A is maximal;*

(iii) *A is Noetherian and* $\dim A = 0$.

Proof. The equivalence of (ii) and (iii) is the definition of Krull dimension in terms of chains of prime ideals.

If A is Artinian, then by the previous theorem it is Noetherian, and the proof above shows that every prime ideal is maximal.

Conversely, suppose A is Noetherian and every prime ideal is maximal. Since A is Noetherian, it has only finitely many minimal prime ideals. But every prime is minimal and maximal, so $\mathrm{Spec}(A)$ is finite. The nilradical is nilpotent in a Noetherian ring, and a product of powers of the finitely many maximal ideals is zero. Thus A has finite length and hence is Artinian. □

Corollary 5.9. *Let $(A, \mathfrak{m})$ be a Noetherian local ring. Then A is Artinian if and only if $\mathfrak{m}$ is nilpotent.*

Proof. If A is Artinian, its nilradical is the unique prime ideal $\mathfrak{m}$, hence $\mathfrak{m}$ is nilpotent. Conversely, if $\mathfrak{m}^N = 0$, then the filtration

$$A \supseteq \mathfrak{m} \supseteq \cdots \supseteq \mathfrak{m}^N = 0$$

has quotients which are finite-dimensional vector spaces over $A/\mathfrak{m}$, because A is Noetherian. Hence A has finite length, so it is Artinian. □

Theorem 5.10 (Structure of Artinian Rings)**.** *Let A be an Artinian ring, and let $\mathfrak{m}_1, \ldots, \mathfrak{m}_r$ be its maximal ideals. Then there exist integers $n_i > 0$ such that*

$$A \cong A/\mathfrak{m}_1^{n_1} \times \cdots \times A/\mathfrak{m}_r^{n_r}.$$

In particular, every Artinian ring is a finite product of Artinian local rings.

Proof. Since A is Artinian, its Jacobson radical is nilpotent. Hence for some N,

$$(\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_r)^N = 0.$$

Thus $\mathfrak{m}_1^N \cdots \mathfrak{m}_r^N = 0$. The ideals $\mathfrak{m}_i^N$ are pairwise comaximal, and the Chinese remainder theorem gives

$$A \cong \prod_{i=1}^{r} A/\mathfrak{m}_i^N.$$

Each factor is local and Artinian. □

5.3 Minimal Prime Ideals

Proposition 5.11. *A Noetherian ring has only finitely many minimal prime ideals.*

Proof. Let A be Noetherian. Consider the set of ideals I of A such that A/I has infinitely many minimal prime ideals. If the set is nonempty, choose a maximal element I. Replacing A by A/I, it suffices to prove that if A itself is a maximal counterexample, then we reach a contradiction.

The zero ideal cannot be prime, otherwise A would have a unique minimal prime. Hence there exist nonzero ideals $\mathfrak{a}, \mathfrak{b}$ with

$$\mathfrak{a}\mathfrak{b} = 0.$$

For instance, take nonzero elements a, b with $ab = 0$ and let $\mathfrak{a} = (a)$, $\mathfrak{b} = (b)$. Every minimal prime of A contains either $\mathfrak{a}$ or $\mathfrak{b}$. Therefore the minimal primes of A occur among the minimal primes of $A/\mathfrak{a}$ and of $A/\mathfrak{b}$.

By maximality of $I = 0$, both $A/\mathfrak{a}$ and $A/\mathfrak{b}$ have only finitely many minimal prime ideals. Hence so does A, a contradiction. □

Remark 5.12. This result is one of the first signs that the Noetherian hypothesis makes the topology of $\mathrm{Spec}(A)$ manageable: the space has only finitely many irreducible components.

5.4 Hilbert Basis Theorem

Theorem 5.13 (Hilbert Basis Theorem)**.** *If A is Noetherian, then the polynomial ring*

$$A[x_1, \ldots, x_n]$$

is Noetherian.

Proof. It suffices to prove the case $n = 1$. Let $I \subseteq A[x]$ be an ideal. For each $d \geq 0$, let J_d be the ideal of A consisting of leading coefficients of polynomials in I of degree d, together with 0. Then

$$J_0 \subseteq J_1 \subseteq J_2 \subseteq \cdots$$

is an ascending chain of ideals of A, hence stabilizes. Let N be such that $J_d = J_N$ for all $d \geq N$.

For each $0 \leq d \leq N$, choose finitely many polynomials in I of degree d whose leading coefficients generate J_d. Let $f_1, \ldots, f_r$ be the finite collection of all these chosen polynomials, and let $I' = (f_1, \ldots, f_r) \subseteq I$.

We claim that $I = I'$. Suppose not, and choose $f \in I \setminus I'$ of minimal degree. Let $d = \deg f$, and let a be its leading coefficient. If $d \leq N$, then a is an A-linear combination of the leading coefficients of the chosen polynomials of degree d. Subtracting the corresponding A-linear combination from f gives an element of $I \setminus I'$ of smaller degree, contradiction.

If $d > N$, then $a \in J_d = J_N$. Hence a is an A-linear combination of the leading coefficients of the chosen polynomials of degree at most N. Multiplying those polynomials by suitable powers of x, we again subtract an element of I' from f and reduce the degree. This contradicts the choice of f. Therefore $I = I'$, so every ideal is finitely generated. □

Corollary 5.14. *If A is Noetherian and B is a finitely generated A-algebra, then B is Noetherian.*

Proof. There is a surjective A-algebra homomorphism

$$A[x_1, \dots, x_n] \twoheadrightarrow B.$$

The source is Noetherian by Hilbert's basis theorem, and a quotient of a Noetherian ring is Noetherian. □

5.5 Primary Decomposition in Noetherian Rings

Definition 5.15. An ideal $\mathfrak{a}$ of A is called *irreducible* if whenever

$$\mathfrak{a} = \mathfrak{b} \cap \mathfrak{c},$$

then either $\mathfrak{a} = \mathfrak{b}$ or $\mathfrak{a} = \mathfrak{c}$.

Lemma 5.16. *In a Noetherian ring, every ideal is a finite intersection of irreducible ideals.*

Proof. Suppose not. Let Σ be the set of ideals which cannot be written as a finite intersection of irreducible ideals. Since A is Noetherian, Σ has a maximal element $\mathfrak{a}$. The ideal $\mathfrak{a}$ is not irreducible, so

$$\mathfrak{a} = \mathfrak{b} \cap \mathfrak{c}$$

with $\mathfrak{a} \subsetneq \mathfrak{b}$ and $\mathfrak{a} \subsetneq \mathfrak{c}$. By maximality, both $\mathfrak{b}$ and $\mathfrak{c}$ are finite intersections of irreducible ideals. Hence so is $\mathfrak{a}$, contradiction. □

Lemma 5.17. *In a Noetherian ring, every irreducible ideal is primary.*

Proof. It is enough to prove the assertion for the zero ideal, after replacing A by $A/\mathfrak{a}$.

Assume that (0) is irreducible. Suppose $xy = 0$ and $y \neq 0$. We must show that x is nilpotent. Consider the ascending chain of annihilators

$$\operatorname{Ann}(x) \subseteq \operatorname{Ann}(x^2) \subseteq \operatorname{Ann}(x^3) \subseteq \cdots.$$

Since A is Noetherian, this chain stabilizes; choose n such that

$$\operatorname{Ann}(x^n) = \operatorname{Ann}(x^{n+1}).$$

We claim that

$$(x^n) \cap (y) = 0.$$

Indeed, if $z \in (x^n) \cap (y)$, then $z = ax^n = by$ for some $a, b \in A$. Since $xy = 0$, we have $xz = 0$, hence $ax^{n+1} = 0$. Thus $a \in \operatorname{Ann}(x^{n+1}) = \operatorname{Ann}(x^n)$, so $z = ax^n = 0$.

Since (0) is irreducible and $y \neq 0$, the equality $(x^n) \cap (y) = 0$ forces $(x^n) = 0$. Hence x is nilpotent. Therefore (0) is primary. □

Theorem 5.18 (Lasker–Noether)**.** *Every ideal in a Noetherian ring has a primary decomposition.*

Proof. By the first lemma, every ideal is a finite intersection of irreducible ideals. By the second lemma, every irreducible ideal is primary. Thus every ideal is a finite intersection of primary ideals. □

Corollary 5.19. *Every algebraic subset of k^n can be written as a finite union of irreducible affine algebraic sets.*

Proof. Let $X = V(I) \subseteq k^n$. Since $k[x_1, \ldots, x_n]$ is Noetherian, I has a primary decomposition

$$I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_r.$$

Then

$$V(I) = V(\mathfrak{q}_1) \cup \cdots \cup V(\mathfrak{q}_r).$$

After omitting redundant components and taking radicals, this gives a finite decomposition into irreducible closed subsets. □

5.6 Krull Dimension

Definition 5.20. Let $\mathcal{M}$ be a partially ordered set. A *chain* in $\mathcal{M}$ is a totally ordered subset. The *length* of a finite chain

$$x_0 < x_1 < \cdots < x_n$$

is n. The dimension of $\mathcal{M}$ is the supremum of the lengths of chains in $\mathcal{M}$.

Definition 5.21. Let X be a topological space. The *dimension* of X is the supremum of the lengths of chains

$$X_0 \subsetneq X_1 \subsetneq \cdots \subsetneq X_n$$

of irreducible closed subsets of X.

Definition 5.22. Let A be a ring. The *Krull dimension* of A is

$$\dim A = \dim \operatorname{Spec}(A).$$

Equivalently, $\dim A$ is the supremum of all integers n for which there is a chain of prime ideals

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n.$$

Definition 5.23. Let $\mathfrak{p} \in \operatorname{Spec}(A)$. The *height* of $\mathfrak{p}$ is

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

equivalently the supremum of the lengths of chains of prime ideals ending at $\mathfrak{p}$:

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n = \mathfrak{p}.$$

Definition 5.24. Let A be an algebra over a field k. The *transcendence degree* of A over k is

$$\operatorname{trdeg}_k(A) = \sup\{|T| : T \subseteq A \text{ is finite and algebraically independent over } k\}.$$

Theorem 5.25. *Let k be a field, and let B be an integral domain which is a finitely generated k-algebra. Let $K(B)$ be the field of fractions of B. Then:*

(i) $\dim B = \operatorname{trdeg}_k K(B)$;

(ii) for every $\mathfrak{p} \in \operatorname{Spec}(B)$,

$$\operatorname{ht}(\mathfrak{p}) + \dim(B/\mathfrak{p}) = \dim B.$$

Proof. We give the standard proof in the form used later for affine algebras. Choose algebraically independent elements $x_1, \dots, x_d \in B$ such that B is algebraic over $k[x_1, \dots, x_d]$; after replacing the x_i by suitable linear combinations, one obtains a finite integral extension

$$k[x_1, \dots, x_d] \subseteq B.$$

The polynomial ring $k[x_1, \dots, x_d]$ has dimension d, and integral extensions preserve dimensions of chains of prime ideals by lying over and going up. Thus $\dim B = d = \operatorname{trdeg}_k K(B)$.

For the second assertion, localize at $\mathfrak{p}$ and pass to the quotient $B/\mathfrak{p}$. Chains ending at $\mathfrak{p}$ correspond to chains in $B_{\mathfrak{p}}$, while chains starting at $\mathfrak{p}$ correspond to chains in $B/\mathfrak{p}$. The dimension formula follows from the same normalization argument and the fact that transcendence degree drops by the height of $\mathfrak{p}$. □

Remark 5.26. The proof above uses the normalization theorem and the going-up theorem. These will be treated more systematically in the chapter on integral dependence. Here the statement is included because it explains why dimension is tied to Noetherianity and finite generation.

5.7 Affine Algebras

Definition 5.27. Let k be a field. A k-algebra A is called an *affine k-algebra* if it is finitely generated as a k-algebra. If in addition A has no nonzero nilpotent elements, then A is called an affine algebra without nilpotents.

Theorem 5.28. *Let A be an affine k-algebra. Then*

$$\dim A = \operatorname{trdeg}_k(A).$$

Proof. If A is a domain, this is the theorem above. In general, since A is Noetherian, it has finitely many minimal prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_r$. The irreducible components of $\operatorname{Spec}(A)$ are the spectra of $A/\mathfrak{p}_i$, and

$$\dim A = \max_i \dim(A/\mathfrak{p}_i).$$

Each $A/\mathfrak{p}_i$ is an affine domain over k, so

$$\dim(A/\mathfrak{p}_i) = \operatorname{trdeg}_k K(A/\mathfrak{p}_i).$$

Taking the maximum over the minimal primes gives the desired equality. □

Lemma 5.29 (Zariski's Lemma)**.** *Let k be a field and let A be a finitely generated k-algebra. If A is a field, then A is algebraic over k.*

Proof. Write $A = k[x_1, \ldots, x_n]$. Choose a maximal algebraically independent subset among the x_i, say $x_1, \ldots, x_r$. Then A is algebraic over $k[x_1, \ldots, x_r]$. If $r > 0$, then A is integral over a localization of the polynomial ring $k[x_1, \ldots, x_r]$. But a field integral over a domain forces the base to be a field, whereas $k[x_1, \ldots, x_r]$ is not a field for $r > 0$. Hence $r = 0$, and all x_i are algebraic over k. □

Corollary 5.30. *Let k be a field and let A be a finitely generated k-algebra. If $\mathfrak{m}$ is a maximal ideal of A, then $A/\mathfrak{m}$ is a finite algebraic extension of k.*

Proof. The quotient $A/\mathfrak{m}$ is both a field and a finitely generated k-algebra. Hence it is algebraic over k by Zariski's lemma. Since it is finitely generated as a k-algebra and algebraic over k, it is finite-dimensional as a k-vector space. □

Theorem 5.31 (Weak Nullstellensatz)**.** *Let k be an algebraically closed field. Then every maximal ideal of $k[x_1, \ldots, x_n]$ is of the form*

$$(x_1 - a_1, \ldots, x_n - a_n)$$

for a unique point $a = (a_1, \ldots, a_n) \in k^n$.

Proof. Let $\mathfrak{m} \subseteq k[x_1, \ldots, x_n]$ be a maximal ideal. Then

$$K = k[x_1, \ldots, x_n]/\mathfrak{m}$$

is a field which is finitely generated as a k-algebra. By Zariski's lemma, K is algebraic over k. Since k is algebraically closed, the image of each x_i in K is an element $a_i \in k$. Hence the quotient map

$$k[x_1, \ldots, x_n] \longrightarrow K$$

is evaluation at the point $a = (a_1, \ldots, a_n)$, and its kernel is

$$(x_1 - a_1, \ldots, x_n - a_n).$$

Thus $\mathfrak{m}$ has the required form. Uniqueness of the point is immediate from the generators. □

Theorem 5.32 (Hilbert's Nullstellensatz)**.** *Let k be an algebraically closed field and let $I \subseteq k[x_1, \ldots, x_n]$ be an ideal. Then*

$$I(V(I)) = \mathrm{Rad}(I).$$

Proof. It is clear that

$$\mathrm{Rad}(I) \subseteq I(V(I)),$$

because if $f^N \in I$, then f vanishes at every common zero of I.

Conversely, suppose $f \notin \mathrm{Rad}(I)$. Let

$$A = k[x_1, \ldots, x_n]/I,$$

and let $\overline{f}$ be the image of f in A. Since $f \notin \mathrm{Rad}(I)$, the element $\overline{f}$ is not nilpotent. Hence the localization

$$A_{\overline{f}}$$

is nonzero. Choose a maximal ideal of this nonzero ring. Its contraction to A is a prime ideal not containing $\overline{f}$, and its inverse image in $k[x_1, \dots, x_n]$ is contained in a maximal ideal $\mathfrak{m}$ containing I but not containing f.

By the weak Nullstellensatz, this maximal ideal is the ideal of a point $a \in k^n$. Since $I \subseteq \mathfrak{m}$, we have $a \in V(I)$, while $f \notin \mathfrak{m}$ means $f(a) \neq 0$. Therefore $f \notin I(V(I))$. This proves

$$I(V(I)) \subseteq \operatorname{Rad}(I),$$

and hence equality. □

Theorem 5.33. *Let $A \neq 0$ be an affine k-algebra. The following are equivalent:*

(i) $\dim A = 0$*;*

(ii) A is algebraic over k;

(iii) A is finite-dimensional as a k-vector space;

(iv) A is Artinian;

(v) $\operatorname{Spec}(A) = \operatorname{Max}(A)$ *is finite.*

Proof. If A is finite-dimensional over k, then it is Artinian as a ring. Hence (iii) implies (iv). If A is Artinian, then every prime ideal is maximal, so $\dim A = 0$ and $\operatorname{Spec}(A)$ is finite. Thus (iv) implies (i) and (v).

Assume $\dim A = 0$. Since A is Noetherian, it is Artinian by the Artinian criterion above. Then A is a finite product of Artinian local rings, and each residue field is a finite algebraic extension of k by Zariski's lemma. It follows that A is finite-dimensional over k. Thus (i) implies (iii), and (iii) clearly implies that A is algebraic over k.

Finally, if A is algebraic over k and finitely generated as a k-algebra, then A is finite-dimensional over k. This proves the equivalence. □

5.8 The Principal Ideal Theorem

Theorem 5.34 (Principal Ideal Theorem)**.** *Let A be a Noetherian ring, and let $\mathfrak{p} \in \operatorname{Spec}(A)$ be minimal over a principal ideal (x). Then*

$$\operatorname{ht}(\mathfrak{p}) \leq 1.$$

Proof. Localizing at $\mathfrak{p}$, we may assume that $(A, \mathfrak{p})$ is a Noetherian local ring and that $\mathfrak{p}$ is minimal over (x). Then $\mathfrak{p}$ is the only prime ideal containing (x), so

$$\operatorname{rad}((x)) = \mathfrak{p}.$$

Thus $A/(x)$ is a Noetherian local ring of dimension zero, hence Artinian. Therefore $\mathfrak{p}^n \subseteq (x)$ for some n.

Suppose, toward a contradiction, that there is a chain

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \mathfrak{p}$$

of prime ideals. Since $\mathfrak{p}^n \subseteq (x)$, the element x lies in $\mathfrak{p}$ and controls the nilpotence of the maximal ideal in the quotient. Applying Nakayama's lemma to the $A_{\mathfrak{p}}$-module $\mathfrak{p}_1 A_{\mathfrak{p}}/(x)$, one obtains that $\mathfrak{p}_1 A_{\mathfrak{p}}$ must be either zero or equal to $\mathfrak{p} A_{\mathfrak{p}}$, contradicting the strict inclusions. Hence no such chain exists, and $\operatorname{ht}(\mathfrak{p}) \leq 1$. □

Theorem 5.35 (Generalized Principal Ideal Theorem)**.** *Let A be a Noetherian ring, and let $\mathfrak{p}$ be a prime ideal minimal over an ideal generated by n elements,*

$$\mathfrak{a} = (x_1, \dots, x_n).$$

Then

$$\operatorname{ht}(\mathfrak{p}) \leq n.$$

Proof. We argue by induction on n. The case $n = 1$ is the principal ideal theorem.

Assume $n > 1$ and let $\mathfrak{q}$ be a prime ideal strictly contained in $\mathfrak{p}$. We need to bound the length of chains below $\mathfrak{p}$. Passing to $A/(x_1)$ and applying the induction hypothesis to the image of $(x_2, \dots, x_n)$, every prime minimal over the image has height at most $n - 1$. The principal ideal theorem accounts for the first generator x_1. Combining these two bounds gives

$$\operatorname{ht}(\mathfrak{p}) \leq n.$$

Equivalently, any chain of primes ending at $\mathfrak{p}$ can be shortened after quotienting by one generator, and the remaining part has length at most $n - 1$. □

Corollary 5.36. *Let $(A, \mathfrak{m})$ be a Noetherian local ring. If $\mathfrak{m}$ can be generated by n elements, then*

$$\dim A \leq n.$$

Proof. Apply the generalized principal ideal theorem to the ideal $\mathfrak{m}$. Since $\mathfrak{m}$ is minimal over itself, its height is at most n. But

$$\dim A = \operatorname{ht}(\mathfrak{m}).$$

□

Remark 5.37. This corollary is one of the first links between dimension and the minimal number of generators of the maximal ideal. It is the starting point for the later notion of regular local rings.

Chapter 6

Projective and Injective Modules

This chapter collects some additional module-theoretic material which is useful both in commutative algebra and in homological algebra. The guiding principle is that projective modules behave like free modules from the point of view of lifting maps, while injective modules behave dually from the point of view of extending maps.

The material in this chapter also prepares the language of resolutions, even though we shall not develop derived functors here. In particular, projective modules are the natural objects used to build projective resolutions, while injective modules are the natural objects used to build injective resolutions.

6.1 Direct Summands and Retracts

Let R be a ring and let M be an R-module. Recall that if S and T are submodules of M, then M is the internal direct sum of S and T if

$$M = S + T, \qquad S \cap T = 0.$$

Equivalently, every $m \in M$ can be written uniquely as

$$m = s + t, \qquad s \in S, \quad t \in T.$$

In that case we write

$$M = S \oplus T.$$

Definition 6.1. A submodule $S \subseteq M$ is called a *direct summand* of M if there exists a submodule $T \subseteq M$ such that

$$M = S \oplus T.$$

Definition 6.2. A submodule $S \subseteq M$ is called a *retract* of M if there exists an R-linear map

$$\rho : M \longrightarrow S$$

such that

$$\rho|_S = \mathrm{id}_S \,.$$

Equivalently, if $i : S \hookrightarrow M$ is the inclusion, then

$$\rho \circ i = \mathrm{id}_S \,.$$

Proposition 6.3. *A submodule $S \subseteq M$ is a direct summand of M if and only if it is a retract of M.*

Proof. Suppose first that $M = S \oplus T$. Define

$$\rho : M \longrightarrow S, \qquad \rho(s+t) = s.$$

This is an R-linear map and clearly $\rho|_S = \mathrm{id}_S$. Hence S is a retract of M.

Conversely, suppose that $\rho : M \to S$ satisfies $\rho|_S = \mathrm{id}_S$. Let

$$T = \ker \rho.$$

For any $m \in M$, we have

$$m = \rho(m) + (m - \rho(m)).$$

Here $\rho(m) \in S$, and

$$\rho(m - \rho(m)) = \rho(m) - \rho^2(m) = \rho(m) - \rho(m) = 0,$$

so $m - \rho(m) \in T$. Hence $M = S + T$.

If $x \in S \cap T$, then $x \in S$ and $\rho(x) = 0$. But $\rho|_S = \mathrm{id}_S$, so $x = \rho(x) = 0$. Thus $S \cap T = 0$, and hence

$$M = S \oplus T.$$

□

Remark 6.4. Equivalently, direct summands can be described using idempotents. A submodule $S \subseteq M$ is a direct summand if and only if there exists an idempotent endomorphism

$$e : M \longrightarrow M, \qquad e^2 = e,$$

such that

$$S = \mathrm{im}(e).$$

Indeed, if $M = S \oplus T$, then projection onto S is idempotent. Conversely, if $e^2 = e$, then

$$M = \mathrm{im}(e) \oplus \ker(e).$$

6.2 Free Modules

Definition 6.5. Let $(M_i)_{i \in I}$ be a family of R-modules. The direct product

$$\prod_{i \in I} M_i$$

is the cartesian product equipped with coordinatewise addition and scalar multiplication. The direct sum

$$\bigoplus_{i \in I} M_i$$

is the submodule consisting of all elements with finite support.

6.3 Hom and Direct Sums

The direct product and direct sum are characterized by universal properties. These universal properties are often most conveniently expressed using the Hom functor.

Proposition 6.6. *Let A be an R-module and let $(B_i)_{i\in I}$ be a family of R-modules. Then there is a natural isomorphism*

$$\mathrm{Hom}_R\left(A, \prod_{i\in I} B_i\right) \cong \prod_{i\in I} \mathrm{Hom}_R(A, B_i).$$

Proof. A homomorphism

$$f : A \longrightarrow \prod_{i\in I} B_i$$

is uniquely determined by its component maps

$$p_i \circ f : A \longrightarrow B_i,$$

where p_i is the projection. Conversely, a family of homomorphisms $f_i : A \to B_i$ determines the homomorphism

$$a \longmapsto (f_i(a))_{i\in I}.$$

These constructions are inverse to each other and are natural in all variables. □

Proposition 6.7. *Let $(A_i)_{i\in I}$ be a family of R-modules and let B be an R-module. Then there is a natural isomorphism*

$$\mathrm{Hom}_R\left(\bigoplus_{i\in I} A_i, B\right) \cong \prod_{i\in I} \mathrm{Hom}_R(A_i, B).$$

Proof. A homomorphism

$$f : \bigoplus_{i\in I} A_i \longrightarrow B$$

is uniquely determined by its restrictions to the summands

$$f_i : A_i \longrightarrow B.$$

Conversely, given a family $(f_i)_{i\in I}$ with $f_i : A_i \to B$, define f on a finite sum by

$$f\left(\sum_i a_i\right) = \sum_i f_i(a_i).$$

This is well-defined because every element of the direct sum has finite support. The two constructions are inverse to each other. □

Remark 6.8. The second formula involves a direct product on the right, not a direct sum. There is no finite-support condition on a family of maps $A_i \to B$. In general,

$$\mathrm{Hom}_R\left(A, \bigoplus_{i\in I} B_i\right) \ncong \bigoplus_{i\in I} \mathrm{Hom}_R(A, B_i).$$

Such an isomorphism holds under suitable finiteness assumptions on A, for example when A is finitely generated.

Definition 6.9. An R-module F is called *free* if it is isomorphic to a direct sum of copies of R:

$$F \cong \bigoplus_{i \in I} R.$$

Equivalently, F has a basis, that is, a subset $(e_i)_{i \in I}$ such that every $f \in F$ can be written uniquely as a finite sum

$$f = \sum_{i \in I} a_i e_i, \qquad a_i \in R.$$

Proposition 6.10. *Every R-module is a quotient of a free R-module. More precisely, if $(m_i)_{i \in I}$ is a set of generators for M, then there is a surjective homomorphism*

$$\bigoplus_{i \in I} R \longrightarrow M$$

sending the i-th basis element to m_i.

Proof. Let $F = \bigoplus_{i \in I} Re_i$. Define

$$\varphi : F \longrightarrow M, \qquad \varphi(e_i) = m_i.$$

This extends uniquely to an R-linear map. Since the elements m_i generate M, the map φ is surjective. Therefore

$$M \cong F / \ker \varphi.$$

□

Corollary 6.11. *An R-module M is finitely generated if and only if it is a quotient of a finite free R-module.*

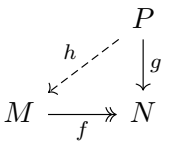
6.4 Projective Modules

Projective modules are modules for which maps can be lifted through surjections. They should be thought of as modules which behave like free modules.

Definition 6.12. An R-module P is called *projective* if for every surjective homomorphism $f : M \twoheadrightarrow N$ and every homomorphism $g : P \to N$, there exists a homomorphism $h : P \to M$ such that

$$f \circ h = g.$$

Equivalently, every diagram



can be completed by a lifting h.

Example 6.13. Every free R-module is projective.

Proof. Let F be free with basis $(e_i)_{i\in I}$, and let $f : M \twoheadrightarrow N$ be surjective. Given $g : F \to N$, choose for each i an element $m_i \in M$ with

$$f(m_i) = g(e_i).$$

There is a unique homomorphism $h : F \to M$ such that $h(e_i) = m_i$. Then $f \circ h = g$ on the basis, hence everywhere. □

Proposition 6.14. *An R-module P is projective if and only if the functor*

$$\mathrm{Hom}_R(P, -)$$

is exact.

Proof. The functor $\mathrm{Hom}_R(P, -)$ is always left exact. Thus it remains to understand surjectivity on the right.

Suppose P is projective. Let

$$M \twoheadrightarrow N$$

be a surjective homomorphism. To say that

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

is surjective means precisely that every map $P \to N$ lifts to a map $P \to M$. This is exactly the definition of projectivity.

Conversely, if $\mathrm{Hom}_R(P, -)$ sends every surjection to a surjection, then every map $P \to N$ lifts through every surjection $M \twoheadrightarrow N$. Hence P is projective. □

Proposition 6.15. *For an R-module P, the following are equivalent.*

(i) *P is projective.*

(ii) *Every short exact sequence*

$$0 \longrightarrow A \longrightarrow B \longrightarrow P \longrightarrow 0$$

splits.

(iii) *P is a direct summand of a free R-module.*

Proof. (i)⇒(ii). Let

$$0 \longrightarrow A \longrightarrow B \xrightarrow{\pi} P \longrightarrow 0$$

be exact. Since P is projective, the identity map $\mathrm{id}_P : P \to P$ lifts through π. Hence there exists $s : P \to B$ such that

$$\pi \circ s = \mathrm{id}_P .$$

Thus the sequence splits.

(ii)⇒(iii). Choose a surjection $F \twoheadrightarrow P$ from a free module F. Then we have a short exact sequence

$$0 \longrightarrow K \longrightarrow F \longrightarrow P \longrightarrow 0.$$

By assumption this sequence splits, so P is a direct summand of F.

(iii)⇒(i). Suppose $F = P \oplus Q$ with F free. Since F is projective, and projectivity passes to direct summands, P is projective. Indeed, given a surjection $M \twoheadrightarrow N$ and a map $P \to N$, extend it by zero on Q to a map $F = P \oplus Q \to N$. Lift this map to $F \to M$, and then restrict to P. □

Corollary 6.16. *Every direct summand of a projective module is projective.*

Corollary 6.17. *Every direct sum of projective modules is projective.*

Proof. Let $(P_i)_{i\in I}$ be a family of projective modules. For each i, write P_i as a direct summand of a free module F_i. Then

$$\bigoplus_i P_i$$

is a direct summand of the free module $\bigoplus_i F_i$. Hence it is projective. □

Proposition 6.18. *If P and Q are projective modules over a commutative ring R, then $P \otimes_R Q$ is projective.*

Proof. Write P and Q as direct summands of free modules F and G. Then $P \otimes_R Q$ is a direct summand of $F \otimes_R G$. Since $F \otimes_R G$ is free, $P \otimes_R Q$ is projective. □

6.5 Projective Bases

The following characterization is often useful because it gives an explicit way to recognize projective modules.

Theorem 6.19 (Dual basis lemma)**.** *Let P be an R-module. Then P is projective if and only if there exist families*

$$(a_i)_{i\in I} \subseteq P, \qquad (\alpha_i)_{i\in I} \subseteq \mathrm{Hom}_R(P, R),$$

such that for each $x \in P$ only finitely many $\alpha_i(x)$ are nonzero and

$$x = \sum_{i\in I} \alpha_i(x) a_i.$$

Such a pair of families is called a projective basis *of P.*

Proof. Suppose first that P is projective. Choose a free module

$$F = \bigoplus_{i\in I} Re_i$$

and maps

$$P \xrightarrow{s} F \xrightarrow{\pi} P$$

such that $\pi \circ s = \mathrm{id}_P$. Let $e_i^* : F \to R$ be the coordinate function. Set

$$a_i = \pi(e_i), \qquad \alpha_i = e_i^* \circ s.$$

For $x \in P$, the element $s(x)$ has finite support, hence only finitely many $\alpha_i(x)$ are nonzero. Moreover,

$$x = \pi(s(x)) = \pi\left(\sum_i e_i^*(s(x))e_i\right) = \sum_i \alpha_i(x) a_i.$$

Thus (a_i, α_i) is a projective basis.

Conversely, suppose such families exist. Let $F = \bigoplus_{i\in I} Re_i$. Define

$$s : P \longrightarrow F, \qquad s(x) = \sum_i \alpha_i(x) e_i,$$

and

$$\pi : F \longrightarrow P, \qquad \pi(e_i) = a_i.$$

Then

$$\pi(s(x)) = \sum_i \alpha_i(x) a_i = x.$$

Hence $\pi \circ s = \mathrm{id}_P$, so P is a direct summand of the free module F. Therefore P is projective. □

6.6 Finitely Presented Modules

Definition 6.20. An R-module M is called *finitely presented* if there is an exact sequence

$$R^m \longrightarrow R^n \longrightarrow M \longrightarrow 0$$

with $m, n < \infty$. Equivalently, M has finitely many generators and finitely many relations.

Remark 6.21. Every finitely presented module is finitely generated. The converse is false in general, but it becomes true over Noetherian rings.

Proposition 6.22. *Every finitely generated projective R-module is finitely presented.*

Proof. Let P be finitely generated and projective. Choose a surjection

$$R^n \twoheadrightarrow P.$$

Since P is projective, this surjection splits. Hence P is a direct summand of R^n. We may write

$$R^n \cong P \oplus Q.$$

Then Q is finitely generated, since it is a quotient of R^n. Thus there is a surjection $R^m \twoheadrightarrow Q$. Composing with the inclusion $Q \hookrightarrow R^n$ gives a map

$$R^m \longrightarrow R^n$$

whose cokernel is P. Therefore P is finitely presented. □

Lemma 6.23 (Schanuel)**.** *Suppose we have two exact sequences*

$$0 \longrightarrow K \longrightarrow P \longrightarrow M \longrightarrow 0$$

and

$$0 \longrightarrow K' \longrightarrow P' \longrightarrow M \longrightarrow 0,$$

where P and P' are projective. Then

$$K \oplus P' \cong K' \oplus P.$$

Proof. Let $\pi : P \to M$ and $\pi' : P' \to M$ be the given surjections. Form the fiber product

$$E = P \times_M P' = \{(p, p') \in P \oplus P' : \pi(p) = \pi'(p')\}.$$

Projection onto the first factor gives an exact sequence

$$0 \longrightarrow K' \longrightarrow E \longrightarrow P \longrightarrow 0.$$

Since P is projective, this sequence splits. Hence

$$E \cong K' \oplus P.$$

Similarly, projection onto the second factor gives an exact sequence

$$0 \longrightarrow K \longrightarrow E \longrightarrow P' \longrightarrow 0,$$

which splits because P' is projective. Hence

$$E \cong K \oplus P'.$$

Combining the two isomorphisms gives

$$K \oplus P' \cong K' \oplus P.$$

□

Corollary 6.24. *Let R be Noetherian. Then every finitely generated R-module is finitely presented.*

Proof. Let M be finitely generated. Choose a surjection

$$R^n \twoheadrightarrow M.$$

Let K be its kernel. Since R is Noetherian, R^n is a Noetherian module. Therefore the submodule $K \subseteq R^n$ is finitely generated. Choose a surjection $R^m \twoheadrightarrow K$. Then

$$R^m \longrightarrow R^n \longrightarrow M \longrightarrow 0$$

is exact, so M is finitely presented. □

6.7 Injective Modules

Injective modules are dual to projective modules. Instead of lifting maps through surjections, they extend maps across injections.

Definition 6.25. An R-module E is called *injective* if for every injective homomorphism $i : A \hookrightarrow B$ and every homomorphism $f : A \to E$, there exists a homomorphism $g : B \to E$ such that

$$g \circ i = f.$$

Equivalently, every diagram

$$\begin{array}{ccc} A & \xhookrightarrow{i} & B \\ {\scriptstyle f}\downarrow & \swarrow_{g} & \\ E & & \end{array}$$

can be completed by an extension g.

Proposition 6.26. *An R-module E is injective if and only if the contravariant functor*

$$\mathrm{Hom}_R(-, E)$$

is exact.

Proof. The functor $\mathrm{Hom}_R(-, E)$ is always left exact as a contravariant functor. Thus the only question is whether maps extend across injections. Given an injection $A \hookrightarrow B$, exactness of

$$\mathrm{Hom}_R(B, E) \longrightarrow \mathrm{Hom}_R(A, E) \longrightarrow 0$$

means precisely that every map $A \to E$ extends to a map $B \to E$. This is the injectivity condition. □

Proposition 6.27. *For an R-module E, the following are equivalent.*

(i) E is injective.

(ii) Every short exact sequence

$$0 \longrightarrow E \longrightarrow M \longrightarrow N \longrightarrow 0$$

splits.

Proof. (i)⇒(ii). If $E \hookrightarrow M$ is the inclusion, then the identity map $\mathrm{id}_E : E \to E$ extends to a map $M \to E$. This extension is a retraction, so the sequence splits.

(ii)⇒(i). Suppose $A \hookrightarrow B$ and $f : A \to E$ are given. Consider the pushout of $A \hookrightarrow B$ and $f : A \to E$:

$$P = (B \oplus E)/\{(a, -f(a)) : a \in A\}.$$

Then there is a natural injection $E \hookrightarrow P$, and by assumption the short exact sequence

$$0 \longrightarrow E \longrightarrow P \longrightarrow B/A \longrightarrow 0$$

splits. Let $r : P \to E$ be a retraction. The composite

$$B \longrightarrow P \xrightarrow{r} E$$

extends f. Hence E is injective. □

Corollary 6.28. *Every direct summand of an injective module is injective.*

Proposition 6.29. *A direct product of injective R-modules is injective.*

Proof. Let $(E_i)_{i \in I}$ be injective modules. Then

$$\mathrm{Hom}_R(-, \prod_i E_i) \cong \prod_i \mathrm{Hom}_R(-, E_i).$$

A product of exact sequences of modules is exact. Hence $\mathrm{Hom}_R(-, \prod_i E_i)$ is exact, and $\prod_i E_i$ is injective. □

Remark 6.30. A direct sum of injective modules need not be injective over an arbitrary ring. Over a Noetherian ring, however, direct sums of injective modules are injective. This is a deeper theorem and will not be used here.

6.8 Baer's Criterion

Baer's criterion reduces injectivity to the extension of maps defined on ideals.

Theorem 6.31 (Baer's criterion)**.** *An R-module E is injective if and only if for every ideal $I \subseteq R$, every R-linear map*

$$f : I \longrightarrow E$$

extends to an R-linear map

$$R \longrightarrow E.$$

Proof. If E is injective, then every map $I \to E$ extends across the inclusion $I \hookrightarrow R$.

Conversely, suppose the stated condition holds. Let $A \subseteq B$ be a submodule and let $f : A \to E$ be an R-linear map. We want to extend f to all of B.

By Zorn's lemma, choose a maximal pair (A', f'), where $A \subseteq A' \subseteq B$ and $f' : A' \to E$ extends f. We claim that $A' = B$.

If not, choose $b \in B \setminus A'$. Let

$$I = \{r \in R : rb \in A'\}.$$

Then I is an ideal of R. Define

$$\varphi : I \longrightarrow E, \qquad \varphi(r) = f'(rb).$$

By assumption, φ extends to a map $\widetilde{\varphi} : R \to E$. Put $e = \widetilde{\varphi}(1)$.

Define a map on $A' + Rb$ by

$$f''(a + rb) = f'(a) + re.$$

This is well-defined: if $a + rb = 0$, then $rb = -a \in A'$, so $r \in I$, and

$$re = \widetilde{\varphi}(r) = \varphi(r) = f'(rb) = -f'(a).$$

Thus f'' extends f' to a strictly larger submodule, contradicting maximality. Therefore $A' = B$, and E is injective. □

6.9 Divisible Modules and Injective Embeddings

Definition 6.32. Let R be an integral domain. An R-module M is called *divisible* if for every nonzero $r \in R$ and every $m \in M$, there exists $x \in M$ such that

$$rx = m.$$

Proposition 6.33. *Let R be an integral domain. Every injective R-module is divisible.*

Proof. Let E be injective, let $0 \neq r \in R$, and let $e \in E$. Consider the ideal $(r) \subseteq R$ and the homomorphism

$$(r) \longrightarrow E, \qquad r \longmapsto e.$$

By Baer's criterion this extends to a homomorphism $R \to E$. If x is the image of 1, then

$$rx = e.$$

Thus E is divisible. □

Proposition 6.34. *Let R be a principal ideal domain. An R-module E is injective if and only if it is divisible.*

Proof. We have already shown that injective modules over a domain are divisible. Conversely, assume that E is divisible. By Baer's criterion, it suffices to show that every map $I \to E$ from an ideal of R extends to R. Since R is a PID, either $I = 0$ or $I = (a)$ for some nonzero $a \in R$. If $f : (a) \to E$ is a homomorphism, divisibility gives $x \in E$ such that

$$ax = f(a).$$

Then the map $R \to E$ sending 1 to x extends f. Hence E is injective. □

Example 6.35. The abelian group $\mathbb{Q}/\mathbb{Z}$ is divisible, hence injective as a $\mathbb{Z}$-module.

Theorem 6.36. *Every R-module can be embedded into an injective R-module.*

Proof. First consider the underlying abelian group of M. Every abelian group embeds into an injective abelian group; for example, it embeds into a product of copies of $\mathbb{Q}/\mathbb{Z}$.

Let

$$M \hookrightarrow D$$

be an embedding of abelian groups, where D is an injective abelian group. Then

$$\mathrm{Hom}_{\mathbb{Z}}(R, D)$$

becomes an R-module by

$$(r\varphi)(s) = \varphi(sr).$$

Define

$$\Phi : M \longrightarrow \mathrm{Hom}_{\mathbb{Z}}(R, D), \qquad \Phi(m)(r) = rm.$$

Here we view rm inside D. The map Φ is R-linear and injective, because evaluation at 1 recovers m.

It remains to see that $\mathrm{Hom}_{\mathbb{Z}}(R, D)$ is injective as an R-module. For any R-module N, there is a natural isomorphism

$$\mathrm{Hom}_R(N, \mathrm{Hom}_{\mathbb{Z}}(R, D)) \cong \mathrm{Hom}_{\mathbb{Z}}(N, D),$$

where N is regarded as an abelian group on the right. Since D is injective as an abelian group, the functor $\mathrm{Hom}_{\mathbb{Z}}(-, D)$ is exact. Therefore $\mathrm{Hom}_R(-, \mathrm{Hom}_{\mathbb{Z}}(R, D))$ is exact, and $\mathrm{Hom}_{\mathbb{Z}}(R, D)$ is injective as an R-module. □

Remark 6.37. The theorem is the starting point for injective resolutions. Dually, every module admits a projective resolution because every module is a quotient of a free, hence projective, module. These two facts are the basic reason that projective and injective modules play such a central role in homological algebra.

Chapter 7

Integral Dependence

7.1 Integral Elements

Integral dependence is a refinement of algebraic dependence. The main point is that, instead of merely satisfying a polynomial equation, an integral element satisfies a monic polynomial equation. This small condition is what makes integral extensions behave like finite maps in geometry.

Definition 7.1. Let $A \subseteq B$ be rings. An element $x \in B$ is said to be *integral over* A if it satisfies a monic polynomial with coefficients in A, that is, if there exist $a_1, \dots, a_n \in A$ such that

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

If every element of B is integral over A, then B is called an *integral extension* of A.

The following criterion is the basic tool for working with integral elements. It is often called the determinant trick.

Lemma 7.2 (Determinant trick)**.** *Let B be an A-algebra, let M be a finitely generated A-module, and let $x \in B$. Suppose that multiplication by x maps M into itself. Then there exists a monic polynomial*

$$T^n + a_1 T^{n-1} + \cdots + a_n \in A[T]$$

such that

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

In particular, if M is a faithful $A[x]$-module, then x is integral over A.

Proof. Let $m_1, \dots, m_n$ generate M as an A-module. Since $xM \subseteq M$, we may write

$$x m_i = \sum_{j=1}^{n} a_{ij} m_j, \qquad a_{ij} \in A.$$

Equivalently,

$$\sum_{j=1}^{n} (\delta_{ij} x - a_{ij}) m_j = 0$$

for every i. Let $C = (\delta_{ij}x - a_{ij})$ be the corresponding matrix. Multiplying the column vector $(m_1, \ldots, m_n)^t$ by the adjugate matrix of C, we obtain

$$\det(C)m_i = 0$$

for every i. Since the m_i generate M, we have $\det(C)M = 0$. The determinant $\det(C)$ is a monic polynomial in x with coefficients in A. This proves the assertion. □

Proposition 7.3. *Let $A \subseteq B$ be rings and let $x \in B$. The following are equivalent.*

(i) x is integral over A.

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

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

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

Proof. (i)⇒(ii). Suppose that

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

Then every power x^m with $m \geq n$ can be written as an A-linear combination of $1, x, \ldots, x^{n-1}$. Hence $A[x]$ is generated as an A-module by

$$1, x, \ldots, x^{n-1}.$$

(ii)⇒(iii) is immediate by taking $C = A[x]$.

(iii)⇒(iv). Take $M = C$. Since $A[x] \subseteq C$, the ring $A[x]$ acts on C by multiplication. This action is faithful, because if an element of $A[x]$ acts as zero on C, then in particular it annihilates $1 \in C$, hence it is zero.

(iv)⇒(i). Since M is an $A[x]$-module, multiplication by x maps M into itself. Applying the determinant trick gives a monic polynomial $f(T) \in A[T]$ such that $f(x)M = 0$. Since M is faithful as an $A[x]$-module, $f(x) = 0$. Hence x is integral over A. □

Theorem 7.4 (Generated by integral elements)**.** *Let $A \subseteq B$ be rings and suppose that*

$$B = A[x_1, \ldots, x_n].$$

Then the following are equivalent.

(i) Each x_i is integral over A.

(ii) B is integral over A.

(iii) B is a finitely generated A-module.

Proof. It is clear that (ii) implies (i). We prove (i)⇒(iii) by induction on n. For $n = 1$ this is the previous proposition. In general, put

$$A' = A[x_1, \ldots, x_{n-1}].$$

By induction, A' is finite over A. Since x_n is integral over A, it is also integral over A', so $A'[x_n]$ is finite over A'. Therefore $B = A'[x_n]$ is finite over A.

Finally, if B is finite as an A-module, then for every $x \in B$ the subring $A[x]$ acts faithfully on the finite A-module B by multiplication. The criterion above shows that x is integral over A. Hence B is integral over A. □

Corollary 7.5. *If $x_1, \ldots, x_n \in B$ are integral over A, then $A[x_1, \ldots, x_n]$ is a finitely generated A-module.*

Proposition 7.6. *The set of all elements of B which are integral over A is a subring of B.*

Proof. Let $x, y \in B$ be integral over A. By the preceding corollary, $A[x, y]$ is a finite A-module. Since $x + y$, $x - y$, and xy all belong to $A[x, y]$, the criterion above implies that they are integral over A. Thus the integral elements form a subring. □

Definition 7.7. The subring of B consisting of elements integral over A is called the *integral closure* of A in B.

If A is an integral domain with field of fractions K, then A is said to be *integrally closed* if it is equal to its integral closure in K. An integrally closed domain is also called a *normal domain*.

Definition 7.8. Let A be an integral domain. The *normalization* of A is the integral closure of A in its field of fractions.

Proposition 7.9. *Every unique factorization domain is integrally closed.*

Proof. Let A be a UFD and let $x = a/b \in \mathrm{Frac}(A)$ be integral over A, where $a, b \in A$ are chosen coprime. Suppose

$$x^n + c_1 x^{n-1} + \cdots + c_n = 0, \qquad c_i \in A.$$

Multiplying by b^n gives

$$a^n + c_1 a^{n-1} b + \cdots + c_n b^n = 0.$$

Thus b divides a^n. Since a and b are coprime in a UFD, b is a unit. Hence $x \in A$. □

7.2 Basic Properties of Integral Extensions

Proposition 7.10 (Transitivity)**.** *Let $A \subseteq B \subseteq C$ be rings. If B is integral over A and C is integral over B, then C is integral over A.*

Proof. Let $x \in C$. Since x is integral over B, there exist $b_1, \ldots, b_n \in B$ such that

$$x^n + b_1 x^{n-1} + \cdots + b_n = 0.$$

Each b_i is integral over A. Hence $A[b_1, \ldots, b_n]$ is a finite A-module. Since x is integral over $A[b_1, \ldots, b_n]$, the ring $A[b_1, \ldots, b_n, x]$ is finite over $A[b_1, \ldots, b_n]$, hence finite over A. Therefore x is integral over A. □

Proposition 7.11. *Let $A \subseteq B$ be an integral extension.*

(i) If $\mathfrak{b}$ is an ideal of B and $\mathfrak{a} = \mathfrak{b} \cap A$, then $B/\mathfrak{b}$ is integral over $A/\mathfrak{a}$.

(ii) If S is a multiplicatively closed subset of A, then $S^{-1}B$ is integral over $S^{-1}A$.

Proof. (i) Let $\overline{x} \in B/\mathfrak{b}$ be the image of $x \in B$. Since x is integral over A, it satisfies a monic equation over A. Passing to the quotient gives a monic equation for $\overline{x}$ over $A/\mathfrak{a}$.

(ii) Let $x/s \in S^{-1}B$. If

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

then dividing by s^n gives a monic equation for x/s over $S^{-1}A$. □

Proposition 7.12. *Let $A \subseteq B$ be integral domains, and suppose that B is integral over A. Then B is a field if and only if A is a field.*

Proof. Suppose first that A is a field. Let $0 \neq y \in B$. Choose an integral equation for y over A of minimal degree:

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

Then $a_n \neq 0$, for otherwise the equation could be divided by y. Therefore

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

Since $a_n \in A^\times$, this shows that y is invertible in B.

Conversely, suppose that B is a field. Let $0 \neq x \in A$. Then $x^{-1} \in B$. Since B is integral over A, the element x^{-1} satisfies

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

Multiplying by x^{n-1} gives

$$x^{-1} = -(a_1 + a_2 x + \cdots + a_n x^{n-1}) \in A.$$

Thus every nonzero element of A is invertible, so A is a field. □

Corollary 7.13. *Let $A \subseteq B$ be an integral extension, let $\mathfrak{q} \in \operatorname{Spec}(B)$, and put $\mathfrak{p} = \mathfrak{q} \cap A$. Then $\mathfrak{q}$ is maximal if and only if $\mathfrak{p}$ is maximal.*

Proof. The extension $A/\mathfrak{p} \subseteq B/\mathfrak{q}$ is integral and both rings are domains. Apply the preceding proposition. □

7.3 Lying Over and Going Up

Theorem 7.14 (Lying over)**.** *Let $A \subseteq B$ be an integral extension. For every $\mathfrak{p} \in \operatorname{Spec}(A)$, there exists $\mathfrak{q} \in \operatorname{Spec}(B)$ such that*

$$\mathfrak{q} \cap A = \mathfrak{p}.$$

Thus the induced map

$$\operatorname{Spec}(B) \longrightarrow \operatorname{Spec}(A)$$

is surjective.

Proof. Let $S = A \setminus \mathfrak{p}$. Then $S^{-1}B$ is integral over $A_\mathfrak{p}$. Choose a maximal ideal $\mathfrak{n}$ of $S^{-1}B$. Its contraction to $A_\mathfrak{p}$ is maximal by the previous corollary, therefore equal to $\mathfrak{p}A_\mathfrak{p}$. Contracting $\mathfrak{n}$ back to B gives a prime ideal $\mathfrak{q}$ with $\mathfrak{q} \cap A = \mathfrak{p}$. □

Theorem 7.15 (Going up)**.** *Let $A \subseteq B$ be an integral extension. Let*

$$\mathfrak{p}_1 \subseteq \mathfrak{p}_2 \subseteq \cdots \subseteq \mathfrak{p}_n$$

be a chain of prime ideals of A. Suppose that prime ideals

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

of B have already been chosen, where $m < n$, and suppose that

$$\mathfrak{q}_i \cap A = \mathfrak{p}_i \qquad (1 \leq i \leq m).$$

Then the chain can be extended: there exist prime ideals

$$\mathfrak{q}_{m+1} \subseteq \cdots \subseteq \mathfrak{q}_n$$

of B such that

$$\mathfrak{q}_i \cap A = \mathfrak{p}_i$$

for all i.

Proof. It suffices to lift one step. Suppose $\mathfrak{q}_m$ lies over $\mathfrak{p}_m$ and $\mathfrak{p}_m \subseteq \mathfrak{p}_{m+1}$. Consider the integral extension

$$A/\mathfrak{p}_m \subseteq B/\mathfrak{q}_m.$$

The ideal $\mathfrak{p}_{m+1}/\mathfrak{p}_m$ is prime in $A/\mathfrak{p}_m$. By lying over, there exists a prime ideal of $B/\mathfrak{q}_m$ lying over it. Its inverse image in B is a prime ideal $\mathfrak{q}_{m+1}$ containing $\mathfrak{q}_m$ and satisfying $\mathfrak{q}_{m+1} \cap A = \mathfrak{p}_{m+1}$. Repeating this proves the theorem. □

Corollary 7.16. *Let $A \subseteq B$ be an integral extension. Then*

$$\dim A = \dim B.$$

Moreover, if $\mathfrak{q} \in \operatorname{Spec}(B)$ and $\mathfrak{p} = \mathfrak{q} \cap A$, then

$$\operatorname{ht}(\mathfrak{q}) \leq \operatorname{ht}(\mathfrak{p}).$$

Proof. Going up lifts chains in A to chains in B, so $\dim A \leq \dim B$. Conversely, if

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

is a chain in B, then the contractions

$$\mathfrak{q}_i \cap A$$

form a strictly increasing chain in A. Strictness follows from the incomparability property for integral extensions: two prime ideals of B lying over the same prime of A cannot be properly contained in one another. Thus $\dim B \leq \dim A$.

The same contraction argument applied to chains ending at $\mathfrak{q}$ gives the height inequality. □

7.4 Integral Dependence on Ideals

Definition 7.17. Let $A \subseteq B$ be rings and let $\mathfrak{a}$ be an ideal of A. An element $x \in B$ is said to be *integral over* $\mathfrak{a}$ if it satisfies an equation

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

with

$$a_i \in \mathfrak{a}^i \qquad (1 \leq i \leq n).$$

Lemma 7.18. *Let $A \subseteq B$ be rings, let $\mathfrak{a}$ be an ideal of A, and let C be the integral closure of A in B. Then every element of B which is integral over $\mathfrak{a}$ lies in*

$$\sqrt{\mathfrak{a}C}.$$

Proof. If x is integral over $\mathfrak{a}$, then

$$x^n + a_1 x^{n-1} + \cdots + a_n = 0, \qquad a_i \in \mathfrak{a}^i.$$

In particular x is integral over A, hence $x \in C$. The same equation shows that

$$x^n \in \mathfrak{a}C,$$

because each term $a_i x^{n-i}$ lies in $\mathfrak{a}C$. Hence $x \in \sqrt{\mathfrak{a}C}$. □

Proposition 7.19. *Let $A \subseteq B$ be integral domains, let A be integrally closed, and let $x \in B$ be integral over an ideal $\mathfrak{a}$ of A. Suppose that x is algebraic over $K = \mathrm{Frac}(A)$, and let*

$$f(T) = T^n + a_1 T^{n-1} + \cdots + a_n$$

be the minimal polynomial of x over K. Then

$$a_i \in \sqrt{\mathfrak{a}^i}$$

for every i.

Proof. Let $x = x_1, x_2, \ldots, x_n$ be the conjugates of x in an algebraic closure of K. Since x is integral over $\mathfrak{a}$, every conjugate x_j is also integral over $\mathfrak{a}$. Therefore the elementary symmetric functions

$$a_i = (-1)^i e_i(x_1, \ldots, x_n)$$

are integral over $\mathfrak{a}^i$. Since $a_i \in K$ and A is integrally closed, $a_i \in A$. By the previous lemma, $a_i \in \sqrt{\mathfrak{a}^i}$. □

7.5 Integrally Closed Domains and Going Down

Proposition 7.20. *Let A be an integral domain. The following are equivalent.*

(i) A is integrally closed.

(ii) $A_{\mathfrak{p}}$ is integrally closed for every prime ideal $\mathfrak{p}$ of A.

(iii) $A_{\mathfrak{m}}$ is integrally closed for every maximal ideal $\mathfrak{m}$ of A.

Proof. (i)⇒(ii). Let $x \in \mathrm{Frac}(A)$ be integral over $A_{\mathfrak{p}}$. Clearing denominators in an integral equation for x shows that there exists $s \in A \setminus \mathfrak{p}$ such that sx is integral over A. Since A is integrally closed, $sx \in A$, so $x \in A_{\mathfrak{p}}$.

(ii)⇒(iii) is immediate.

(iii)⇒(i). Let $x \in \mathrm{Frac}(A)$ be integral over A. Then x is integral over $A_{\mathfrak{m}}$ for every maximal ideal $\mathfrak{m}$, and hence $x \in A_{\mathfrak{m}}$ for every $\mathfrak{m}$. Since

$$A = \bigcap_{\mathfrak{m} \in \mathrm{Max}(A)} A_{\mathfrak{m}}$$

inside $\mathrm{Frac}(A)$, we get $x \in A$. □

Theorem 7.21 (Going down)**.** *Let $A \subseteq B$ be an integral extension of integral domains. Suppose that A is integrally closed and that B is finite as an A-module. Let*

$$\mathfrak{p}_1 \subseteq \mathfrak{p}_2$$

be prime ideals of A, and let $\mathfrak{q}_2 \in \mathrm{Spec}(B)$ lie over $\mathfrak{p}_2$. Then there exists $\mathfrak{q}_1 \in \mathrm{Spec}(B)$ such that

$$\mathfrak{q}_1 \subseteq \mathfrak{q}_2, \qquad \mathfrak{q}_1 \cap A = \mathfrak{p}_1.$$

Consequently, chains of prime ideals in A can be lifted downward along a given chain in B.

Proof. The standard proof uses the preceding result on integral dependence over ideals. After localizing at $\mathfrak{p}_1$ and quotienting by $\mathfrak{q}_2$, the problem is reduced to showing that a prime minimal under a given prime has the prescribed contraction. If the contraction were smaller than expected, one chooses an element of the maximal ideal of the base outside the contraction and applies the proposition on the coefficients of the minimal polynomial. The integrally closed hypothesis forces the relevant coefficients into the required radical ideals, giving a contradiction. □

Corollary 7.22. *Under the hypotheses of going down, if $\mathfrak{q} \in \mathrm{Spec}(B)$ and $\mathfrak{p} = \mathfrak{q} \cap A$, then*

$$\mathrm{ht}(\mathfrak{q}) = \mathrm{ht}(\mathfrak{p}).$$

Proof. The inequality $\mathrm{ht}(\mathfrak{q}) \leq \mathrm{ht}(\mathfrak{p})$ follows from integral dependence. The reverse inequality follows by lifting chains in $A_{\mathfrak{p}}$ downward to chains in $B_{\mathfrak{q}}$. □

7.6 Integral Morphisms of Spectra

Proposition 7.23. *Let $\varphi : A \to B$ be an integral homomorphism. Then the induced map*

$$\varphi^* : \mathrm{Spec}(B) \longrightarrow \mathrm{Spec}(A)$$

is a closed map.

Proof. It suffices to show that the image of a closed subset of the form $V(\mathfrak{b})$ is closed. Put

$$\mathfrak{a} = \varphi^{-1}(\mathfrak{b}).$$

We claim that

$$\varphi^*(V(\mathfrak{b})) = V(\mathfrak{a}).$$

The inclusion $\subseteq$ is clear. Conversely, let $\mathfrak{p} \in V(\mathfrak{a})$. Consider the induced integral extension

$$A/\mathfrak{a} \longrightarrow B/\mathfrak{b}.$$

By lying over, there exists a prime ideal of $B/\mathfrak{b}$ lying over $\mathfrak{p}/\mathfrak{a}$. Its inverse image is a prime ideal $\mathfrak{q} \in V(\mathfrak{b})$ with $\varphi^{-1}(\mathfrak{q}) = \mathfrak{p}$. Hence $\mathfrak{p}$ belongs to the image of $V(\mathfrak{b})$. □

7.7 Noether Normalization

We now turn to affine algebras. Noether normalization is one of the most important bridges between arbitrary affine algebras and polynomial rings. It says that every nonzero affine algebra is finite over a polynomial subalgebra. Geometrically, this means that every affine variety admits a finite dominant map onto an affine space of the same dimension.

Definition 7.24. Let K be a field. An *affine K-algebra* is a finitely generated K-algebra. An affine K-algebra which is an integral domain is called an *affine K-domain*.

Theorem 7.25 (Noether Normalization)**.** *Let $A \neq 0$ be an affine algebra over a field K. Then there exist algebraically independent elements*

$$c_1, \ldots, c_n \in A$$

such that A is integral over

$$C = K[c_1, \ldots, c_n].$$

Equivalently, C is a polynomial ring over K, and A is a finitely generated C-module. Moreover, if $c_1, \ldots, c_n$ are algebraically independent and A is integral over $K[c_1, \ldots, c_n]$, then

$$n = \dim A.$$

Proof. Write

$$A = K[x_1, \ldots, x_m]/I.$$

We argue by induction on m. If $I = 0$, then A is already a polynomial ring and there is nothing to prove.

Assume $I \neq 0$ and choose a nonzero polynomial $f \in I$. We make a change of variables so that f becomes monic in one variable. Choose an integer d larger than all exponents occurring in f, and set

$$y_i = x_i - x_1^{d^{i-1}} \qquad (2 \leq i \leq m).$$

After rewriting f in the variables

$$x_1, y_2, \ldots, y_m,$$

the powers of x_1 appearing in the leading terms become distinct. Hence there is a unique highest power of x_1, and after multiplying by a nonzero scalar we obtain a relation of the form

$$x_1^N + h(x_1, y_2, \ldots, y_m) = 0$$

in A, where

$$\deg_{x_1} h < N.$$

Thus the image of x_1 in A is integral over the subalgebra generated by the images of $y_2, \ldots, y_m$. If

$$B = K[y_2 + I, \ldots, y_m + I] \subseteq A,$$

then A is integral over B.

By the induction hypothesis, B is integral over a polynomial subalgebra $K[c_1, \dots, c_n]$ with algebraically independent generators. By transitivity of integral dependence, A is integral over $K[c_1, \dots, c_n]$.

Finally, since integral extensions preserve Krull dimension and $K[c_1, \dots, c_n]$ is a polynomial ring of dimension n, we get $n = \dim A$. □

Remark 7.26. If K is infinite and $A = K[a_1, \dots, a_m]$, then one can often choose the normalizing parameters c_i as suitable linear combinations of the original generators. This is useful geometrically because it says that after a generic linear change of coordinates, the first $\dim A$ coordinates behave like independent parameters.

Example 7.27. Let

$$A = K[x_1, x_2]/(x_1x_2 - 1).$$

Write $\overline{x}_i$ for the image of x_i in A. The algebra A is not integral over $K[\overline{x}_1]$ or over $K[\overline{x}_2]$. However, if

$$c = \overline{x}_1 - \overline{x}_2,$$

then

$$\overline{x}_1^2 - c\overline{x}_1 - 1 = 0.$$

Thus $\overline{x}_1$ is integral over $K[c]$, and then $\overline{x}_2 = \overline{x}_1 - c$ is also integral over $K[c]$. Hence A is integral over the polynomial subalgebra $K[c]$.

7.8 Consequences for Dimension

Theorem 7.28 (Dimension and transcendence degree)**.** *Let A be an affine K-domain. Then*

$$\dim A = \operatorname{trdeg}_K \operatorname{Frac}(A).$$

More generally, if A is a nonzero affine K-algebra and $\mathfrak{p}$ runs over the minimal prime ideals of A, then

$$\dim A = \max_{\mathfrak{p}} \operatorname{trdeg}_K \operatorname{Frac}(A/\mathfrak{p}).$$

Proof. For a domain, Noether normalization gives a polynomial subring

$$C = K[c_1, \dots, c_n] \subseteq A$$

such that A is integral over C. Therefore

$$\dim A = \dim C = n.$$

Moreover $\operatorname{Frac}(A)$ is algebraic over $\operatorname{Frac}(C) = K(c_1, \dots, c_n)$, so the transcendence degree is also n. The general case follows by passing to the irreducible components $A/\mathfrak{p}$ for minimal prime ideals $\mathfrak{p}$. □

Theorem 7.29 (Maximal chains in affine domains)**.** *Let A be an affine domain and let*

$$0 = \mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_r$$

be a maximal chain of prime ideals. Then

$$r = \dim A.$$

More generally, if A is an affine algebra and

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_r$$

is a maximal chain, then

$$r = \dim(A/\mathfrak{p}_0).$$

Proof. The proof uses Noether normalization and going down. After replacing A by $A/\mathfrak{p}_0$, we may assume that A is an affine domain and $\mathfrak{p}_0 = 0$. Choose a polynomial subalgebra

$$C = K[c_1, \ldots, c_n] \subseteq A$$

such that A is integral over C. Since C is a UFD, it is normal. Going down applies to the integral extension $C \subseteq A$. The behavior of heights under going down then shows that every maximal chain in A has the same length as a maximal chain in the polynomial ring C, namely n. Since $n = \dim A$, the result follows. □

Corollary 7.30 (Dimension and height)**.** *Let A be an affine domain, or more generally an equidimensional affine algebra. If $I \subseteq A$ is an ideal, then*

$$\operatorname{ht}(I) = \dim A - \dim(A/I).$$

Proof. For prime ideals this follows by comparing maximal chains of prime ideals through I. The general case follows by passing to the prime ideals minimal over I. □

Corollary 7.31 (Height of maximal ideals)**.** *Let A be an affine algebra with minimal prime ideals*

$$\mathfrak{p}_1, \ldots, \mathfrak{p}_s.$$

If $\mathfrak{m} \in \operatorname{Max}(A)$, then

$$\operatorname{ht}(\mathfrak{m}) = \max\{\dim(A/\mathfrak{p}_i) : \mathfrak{p}_i \subseteq \mathfrak{m}\}.$$

In particular, if A is an affine domain or, more generally, equidimensional, then every maximal ideal has height $\dim A$.

Theorem 7.32 (Principal ideal theorem for affine domains)**.** *Let A be an affine domain, or more generally an equidimensional affine algebra, and let*

$$I = (a_1, \ldots, a_n) \subseteq A.$$

If $\mathfrak{p}$ is minimal over I, then

$$\dim(A/\mathfrak{p}) \geq \dim A - n.$$

In particular, if $I \neq A$, then

$$\dim(A/I) \geq \dim A - n.$$

If equality holds, then A/I is equidimensional.

Proof. By the principal ideal theorem,

$$\operatorname{ht}(\mathfrak{p}) \leq n.$$

Using the dimension-height formula above gives

$$\dim(A/\mathfrak{p}) = \dim A - \operatorname{ht}(\mathfrak{p}) \geq \dim A - n.$$

The remaining assertions follow by taking minimal primes over I. □

7.9 Normalization of Affine Domains

Theorem 7.33. *Let A be an affine domain. Then the normalization of A is again an affine domain.*

Proof. By Noether normalization, there is a polynomial subalgebra

$$R = K[c_1, \ldots, c_n] \subseteq A$$

such that A is integral over R. Hence $\mathrm{Frac}(A)$ is a finite field extension of $\mathrm{Frac}(R)$. Since R is a polynomial ring, it is normal. The integral closure of a polynomial ring in a finite field extension of its fraction field is finite as an R-module. Therefore the normalization of A is finite over R, hence finitely generated as a K-algebra. □

Corollary 7.34 (Normalization of affine varieties)**.** *Let X be an irreducible affine variety over an algebraically closed field K. Then there exists a normal affine variety $\widetilde{X}$ and a finite surjective morphism*

$$\widetilde{X} \longrightarrow X$$

which is an isomorphism over the normal locus of X.

Proof. Let $A = K[X]$ be the coordinate ring of X, and let $\widetilde{A}$ be the normalization of A. By the theorem, $\widetilde{A}$ is again an affine K-domain. Let $\widetilde{X}$ be the affine variety corresponding to $\widetilde{A}$. The inclusion $A \subseteq \widetilde{A}$ induces a morphism

$$\widetilde{X} \longrightarrow X.$$

The morphism is finite and surjective because $\widetilde{A}$ is integral over A. Over a point where the local ring of X is normal, the localized normalization coincides with the local ring itself, so the fiber consists of a single point. □

Chapter 8

Completion and the Artin–Rees Lemma

8.1 Motivation

The purpose of completion is to pass from finite-order approximations to an object which remembers all finite-order approximations at once.

The most basic example is the polynomial ring $k[x]$ at the ideal (x). The quotient

$$k[x]/(x^n)$$

remembers the Taylor expansion of a polynomial only up to degree $n-1$. Thus the inverse system

$$k[x]/(x) \longleftarrow k[x]/(x^2) \longleftarrow k[x]/(x^3) \longleftarrow \cdots$$

records better and better infinitesimal information near the origin. The inverse limit is

$$\varprojlim_n k[x]/(x^n) \cong k[[x]].$$

Thus completion is a way of adjoining formal Taylor expansions.

More generally, if A is a ring and $\mathfrak{a} \subseteq A$ is an ideal, then the quotients

$$A/\mathfrak{a}^n$$

should be viewed as infinitesimal neighborhoods of the closed subset defined by $\mathfrak{a}$. Passing to

$$\widehat{A} = \varprojlim_n A/\mathfrak{a}^n$$

means remembering all these infinitesimal neighborhoods simultaneously.

There is also a geometric way to phrase the same idea. Localization focuses attention near a point, while completion looks even more closely by retaining formal infinitesimal data around that point. For instance, if

$$A = k[x_1, \ldots, x_n], \qquad \mathfrak{m} = (x_1, \ldots, x_n),$$

then

$$\widehat{A_{\mathfrak{m}}} \cong k[[x_1, \ldots, x_n]].$$

This is the algebraic analogue of replacing functions near a point by formal Taylor series.

The Artin–Rees lemma is the main technical result which makes completion behave well with respect to submodules. If $N \subseteq M$, then the filtration induced on N from the $\mathfrak{a}$-adic filtration of M is

$$N \cap \mathfrak{a}^n M.$$

One wants this filtration to be equivalent to the intrinsic $\mathfrak{a}$-adic filtration $\mathfrak{a}^n N$ on N. The Artin–Rees lemma says that this is true over Noetherian rings.

8.2 Topological Abelian Groups

Definition 8.1. A *topological group* is a group G together with a topology such that the multiplication map

$$G \times G \longrightarrow G, \qquad (x, y) \longmapsto xy,$$

and the inverse map

$$G \longrightarrow G, \qquad x \longmapsto x^{-1},$$

are continuous.

Proposition 8.2. *Let G be a topological group. If $\{e\}$ is closed, then the diagonal*

$$\Delta = \{(x, x) : x \in G\} \subseteq G \times G$$

is closed. Hence G is Hausdorff.

Proof. Consider the continuous map

$$G \times G \longrightarrow G, \qquad (x, y) \longmapsto xy^{-1}.$$

The diagonal is the inverse image of $\{e\}$ under this map. Hence Δ is closed. A topological space is Hausdorff if and only if its diagonal is closed, so G is Hausdorff. □

Proposition 8.3. *Let X be a topological space. Then X is Hausdorff if and only if for every $x \in X$,*

$$\bigcap_{U \ni x} \overline{U} = \{x\},$$

where U runs over all neighborhoods of x.

Proof. If X is Hausdorff and $y \neq x$, choose disjoint neighborhoods U of x and V of y. Then $y \notin \overline{U}$. Hence y does not belong to the intersection.

Conversely, suppose the stated condition holds. If $x \neq y$, then there is a neighborhood U of x such that $y \notin \overline{U}$. Thus $X \setminus \overline{U}$ is a neighborhood of y disjoint from U, so X is Hausdorff. □

Proposition 8.4. *Let G be a topological abelian group. Then G is Hausdorff if and only if*

$$\bigcap_{U} U = \{0\},$$

where U runs over all neighborhoods of 0.

Proof. In a topological group, translation by any element is a homeomorphism. Thus neighborhoods of any point are translates of neighborhoods of zero. Applying the previous proposition at the identity gives the claim. □

Lemma 8.5. *Let H be the intersection of all neighborhoods of 0 in a topological abelian group G. Then:*

(i) H is a subgroup of G;

(ii) $H = \overline{\{0\}}$;

(iii) G/H is Hausdorff;

(iv) if G is Hausdorff, then $H = 0$.

Proof. The intersection of all neighborhoods of 0 is stable under addition and inverses, because addition and inverse are continuous at 0. Moreover, an element lies in the closure of $\{0\}$ exactly when it belongs to every neighborhood of 0. Therefore $H = \overline{\{0\}}$. The quotient by the closure of 0 is Hausdorff. The final assertion is immediate. □

8.3 Completion of Topological Abelian Groups

Definition 8.6. Let G be a topological abelian group. A sequence (x_n) in G is a *Cauchy sequence* if for every neighborhood U of 0 there exists N such that

$$x_m - x_n \in U$$

for all $m, n \geq N$.

Two Cauchy sequences (x_n) and (y_n) are said to be equivalent if

$$x_n - y_n \to 0.$$

The set of equivalence classes of Cauchy sequences is denoted by $\widehat{G}$.

The sum of two Cauchy sequences is again Cauchy, and equivalent sequences give equivalent sums. Hence $\widehat{G}$ is an abelian group. There is a canonical homomorphism

$$G \longrightarrow \widehat{G}$$

which sends $x \in G$ to the class of the constant Cauchy sequence $(x, x, x, \ldots)$.

Remark 8.7. The kernel of the canonical map $G \to \widehat{G}$ is the intersection of all neighborhoods of 0. Thus the map is injective precisely when G is Hausdorff.

Definition 8.8. Let X be a topological space and let $x \in X$. A neighborhood basis of x is a collection of open neighborhoods $\mathcal{B}_x$ such that for every open neighborhood U of x, there is $V \in \mathcal{B}_x$ with

$$x \in V \subseteq U.$$

Let G be a topological abelian group. Suppose that the neighborhoods of 0 admit a basis consisting of subgroups

$$G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \cdots .$$

Then each quotient G/G_n is given the discrete topology, and we have an inverse system

$$G/G_0 \longleftarrow G/G_1 \longleftarrow G/G_2 \longleftarrow \cdots .$$

Proposition 8.9. *With notation as above, there is a natural isomorphism*

$$\widehat{G} \cong \varprojlim_n G/G_n.$$

Proof. Let (x_n) be a Cauchy sequence in G. For each r, the sequence $(x_n + G_r)$ is eventually constant in G/G_r. These eventual values are compatible under the transition maps, so a Cauchy sequence defines an element of $\varprojlim G/G_r$.

Conversely, let $(\overline{x}_r)_r \in \varprojlim G/G_r$. Choose representatives $x_r \in G$ of $\overline{x}_r$. Compatibility implies that for $m \geq n$,

$$x_m - x_n \in G_n.$$

Thus (x_n) is a Cauchy sequence. The two constructions are inverse to one another modulo the equivalence relation on Cauchy sequences. □

Example 8.10. Consider $\mathbb{Z}$ with the p-adic topology. A basis of neighborhoods of 0 is given by

$$p^n\mathbb{Z}, \qquad n \geq 0.$$

Then

$$\widehat{\mathbb{Z}} \cong \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}.$$

This ring is denoted by $\mathbb{Z}_p$ and is called the ring of p-adic integers.

8.4 Inverse Systems and Exactness

Definition 8.11. An *inverse system* of abelian groups is a sequence of abelian groups $(A_n)_{n\geq 0}$ together with homomorphisms

$$A_{n+1} \longrightarrow A_n.$$

The inverse limit is

$$\varprojlim A_n = \left\{ (a_n) \in \prod_{n\geq 0} A_n : a_n \text{ is the image of } a_{n+1} \text{ for all } n \right\}.$$

Proposition 8.12. *Let*

$$0 \longrightarrow (A_n) \xrightarrow{f_n} (B_n) \xrightarrow{g_n} (C_n) \longrightarrow 0$$

be an exact sequence of inverse systems. If all transition maps

$$A_{n+1} \longrightarrow A_n$$

are surjective, then

$$0 \longrightarrow \varprojlim A_n \longrightarrow \varprojlim B_n \longrightarrow \varprojlim C_n \longrightarrow 0$$

is exact.

Proof. Injectivity on the left and exactness in the middle follow from the fact that inverse limits are defined as subgroups of products.

We prove surjectivity. Let

$$c = (c_n) \in \varprojlim C_n.$$

Choose $b_n \in B_n$ such that $g_n(b_n) = c_n$. These choices need not be compatible. Suppose that $b_0, \ldots, b_n$ have been chosen compatibly. Choose any $b'_{n+1} \in B_{n+1}$ mapping to c_{n+1}. The image of b'_{n+1} in B_n differs from b_n by an element of $\ker(g_n) = \mathrm{im}(f_n)$. Hence there exists $a_n \in A_n$ which corrects this difference. Since $A_{n+1} \to A_n$ is surjective, lift a_n to $a_{n+1} \in A_{n+1}$. Replacing b'_{n+1} by

$$b'_{n+1} - f_{n+1}(a_{n+1})$$

gives a compatible lift. Continuing inductively gives an element of $\varprojlim B_n$ mapping to c. □

Corollary 8.13. *Let*

$$0 \longrightarrow G' \longrightarrow G \longrightarrow G'' \longrightarrow 0$$

be an exact sequence of abelian groups. Suppose that G is equipped with a topology defined by a descending sequence of subgroups (G_n), and give G' and G'' the induced topologies

$$G'_n = G' \cap G_n, \qquad G''_n = (G_n + G')/G'.$$

Then

$$0 \longrightarrow \widehat{G'} \longrightarrow \widehat{G} \longrightarrow \widehat{G''}$$

is exact. If the transition maps for G' are surjective, then the last map is also surjective.

Proof. Apply the preceding proposition to the short exact sequences

$$0 \longrightarrow G'/G'_n \longrightarrow G/G_n \longrightarrow G''/G''_n \longrightarrow 0.$$

□

Corollary 8.14. *If G' is a closed subgroup of G, and G/G' is equipped with the quotient topology, then*

$$\widehat{G/G'} \cong \widehat{G}/\widehat{G'}$$

whenever the completions are taken with respect to subgroup bases as above.

8.5 Adic Topology and Completion of Modules

Let A be a ring and let $\mathfrak{a} \subseteq A$ be an ideal. The powers

$$\mathfrak{a}^n$$

form a descending sequence of ideals and therefore define a topology on A. This is called the $\mathfrak{a}$-*adic topology*. The completion of A for this topology is

$$\widehat{A} = \varprojlim_n A/\mathfrak{a}^n.$$

If M is an A-module, then the submodules

$$\mathfrak{a}^n M$$

define the $\mathfrak{a}$-*adic topology* on M, and the completion of M is

$$\widehat{M} = \varprojlim_n M/\mathfrak{a}^n M.$$

Definition 8.15. A *filtration* of an A-module M is a descending sequence of submodules

$$M = M_0 \supseteq M_1 \supseteq M_2 \supseteq \cdots.$$

Let $\mathfrak{a}$ be an ideal of A. The filtration (M_n) is called an $\mathfrak{a}$-*filtration* if

$$\mathfrak{a} M_n \subseteq M_{n+1}$$

for all n. It is called *stable* if

$$\mathfrak{a} M_n = M_{n+1}$$

for all sufficiently large n.

Lemma 8.16. *Let (M_n) and (M'_n) be stable $\mathfrak{a}$-filtrations on the same A-module M. Then they define the same topology on M.*

Proof. Since (M_n) is stable, there is n_0 such that

$$M_{n_0+r} = \mathfrak{a}^r M_{n_0}$$

for all $r \geq 0$. Since (M'_n) is an $\mathfrak{a}$-filtration, for some integer s we have

$$M_{n_0} \subseteq M'_s.$$

It follows that

$$M_{n_0+r} = \mathfrak{a}^r M_{n_0} \subseteq \mathfrak{a}^r M'_s \subseteq M'_{s+r}.$$

This gives one system of containments. By symmetry, the reverse containments also hold after shifting the indices. Hence the two filtrations define the same topology. □

8.6 Associated Graded Objects

Let A be a ring and let $\mathfrak{a} \subseteq A$ be an ideal. Define

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

If M is an A-module with an $\mathfrak{a}$-filtration (M_n), define

$$M^* = \operatorname{gr}(M) = \bigoplus_{n \geq 0} M_n/M_{n+1}.$$

Then A^* is a graded ring and M^* is a graded A^*-module.

Proposition 8.17. *Let $R = \bigoplus_{n \geq 0} R_n$ be a graded ring. Then R is Noetherian if and only if R_0 is Noetherian and R is a finitely generated R_0-algebra.*

Proof. If R is Noetherian, then R_0 is a quotient of R/R_+ and hence is Noetherian. Moreover the ideal

$$R_+ = \bigoplus_{n>0} R_n$$

is finitely generated. Taking homogeneous generators of R_+ shows that R is finitely generated over R_0.

Conversely, if R_0 is Noetherian and R is a finitely generated R_0-algebra, then R is Noetherian by Hilbert's basis theorem. □

Lemma 8.18. *Let A be a Noetherian ring, let $\mathfrak{a} \subseteq A$ be an ideal, and let M be a finitely generated A-module. Let (M_n) be an $\mathfrak{a}$-filtration of M. Then the following are equivalent:*

(i) (M_n) is stable;

(ii) M^* is a finitely generated A^*-module.

Proof. Assume that (M_n) is stable. Then for all sufficiently large n,

$$M_{n+1} = \mathfrak{a}M_n.$$

Thus the higher homogeneous pieces of M^* are generated by finitely many lower homogeneous pieces. Since M is Noetherian, these lower pieces are finitely generated, and so M^* is a finitely generated A^*-module.

Conversely, suppose that M^* is finitely generated over A^*. Take homogeneous generators of M^* of degrees at most N. Then for $n \geq N$, the degree $n+1$ part of M^* is generated from degree n by the degree-one part

$$\mathfrak{a}/\mathfrak{a}^2$$

of A^*. This means precisely that

$$M_{n+1} = \mathfrak{a}M_n$$

for all sufficiently large n. Hence the filtration is stable. □

8.7 The Artin–Rees Lemma

Lemma 8.19 (Artin–Rees Lemma)**.** *Let A be a Noetherian ring, let $\mathfrak{a} \subseteq A$ be an ideal, let M be a finitely generated A-module, and let $M' \subseteq M$ be a submodule. Then there exists an integer $k \geq 0$ such that*

$$\mathfrak{a}^n M \cap M' = \mathfrak{a}^{n-k}(\mathfrak{a}^k M \cap M')$$

for all $n \geq k$.

Proof. For each n, set

$$M'_n = M' \cap \mathfrak{a}^n M.$$

Then (M'_n) is an $\mathfrak{a}$-filtration of M'. We want to show that it is stable.

Consider the associated graded module

$$M^* = \bigoplus_{n\geq 0} \mathfrak{a}^n M/\mathfrak{a}^{n+1}M$$

over

$$A^* = \bigoplus_{n\geq 0} \mathfrak{a}^n/\mathfrak{a}^{n+1}.$$

The filtration (M'_n) gives a graded submodule

$$(M')^* = \bigoplus_{n\geq 0} M'_n/M'_{n+1}$$

of M^*. Since A is Noetherian and M is finitely generated, A^* is Noetherian and M^* is a finitely generated A^*-module. Hence $(M')^*$ is finitely generated over A^*.

By the previous lemma, the filtration (M'_n) is stable. Therefore there exists k such that

$$M'_n = \mathfrak{a}^{n-k} M'_k$$

for all $n \geq k$, i.e.

$$\mathfrak{a}^n M \cap M' = \mathfrak{a}^{n-k}(\mathfrak{a}^k M \cap M').$$

□

8.8 Krull's Intersection Theorem

Theorem 8.20 (Krull's Intersection Theorem)**.** *Let A be a Noetherian ring, let $\mathfrak{a} \subseteq A$ be an ideal contained in the Jacobson radical of A, and let M be a finitely generated A-module. Then*

$$\bigcap_{n\geq 0} \mathfrak{a}^n M = 0.$$

Proof. Let

$$M' = \bigcap_{n\geq 0} \mathfrak{a}^n M.$$

Applying the Artin–Rees lemma to the inclusion $M' \subseteq M$, there exists $k \geq 0$ such that

$$M' \cap \mathfrak{a}^n M = \mathfrak{a}^{n-k}(M' \cap \mathfrak{a}^k M)$$

for all $n \geq k$. But $M' \subseteq \mathfrak{a}^n M$ for every n, so

$$M' = M' \cap \mathfrak{a}^n M.$$

Taking $n = k + 1$, we get

$$M' = \mathfrak{a} M'.$$

Since M' is finitely generated, Nakayama's lemma gives

$$M' = 0.$$

□

Remark 8.21. The Noetherian hypothesis is essential. For example, let A be the ring of smooth functions on $\mathbb{R}$ and let $\mathfrak{m}$ be the ideal of functions vanishing at 0. The function

$$f(x) = \begin{cases} e^{-1/x^2}, & x \neq 0, \\ 0, & x = 0 \end{cases}$$

vanishes to all orders at 0, so it belongs to $\bigcap_n \mathfrak{m}^n$, but it is not zero.

Corollary 8.22. *Let A be a Noetherian domain and let $\mathfrak{a} \subseteq A$ be a proper ideal. Then*

$$\bigcap_{n \geq 0} \mathfrak{a}^n = 0.$$

Proof. Choose a maximal ideal $\mathfrak{m}$ containing $\mathfrak{a}$ and localize at $\mathfrak{m}$. Then

$$\bigcap_{n} \mathfrak{a}^n A_{\mathfrak{m}} = 0$$

by Krull's intersection theorem. If $x \in \bigcap_n \mathfrak{a}^n$, then $x/1 = 0$ in $A_{\mathfrak{m}}$, so some element outside $\mathfrak{m}$ annihilates x. Since A is a domain, this implies $x = 0$. □

Corollary 8.23. *Let A be a Noetherian ring and let $\mathfrak{a} \subseteq A$ be an ideal. Then*

$$\bigcap_{n \geq 0} \mathfrak{a}^n$$

is the set of elements annihilated by some element of the form $1 - a$, where $a \in \mathfrak{a}$.

Proof. This is the standard form of Krull's intersection theorem obtained by applying the preceding argument to the stable submodule $\bigcap_n \mathfrak{a}^n$ and using the determinant trick instead of the local form of Nakayama's lemma. □

8.9 Exactness of Completion

Theorem 8.24. *Let A be a Noetherian ring, let $\mathfrak{a} \subseteq A$ be an ideal, and let*

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$$

be an exact sequence of finitely generated A-modules. If all three modules are equipped with their $\mathfrak{a}$-adic filtrations, then

$$0 \longrightarrow \widehat{M'} \longrightarrow \widehat{M} \longrightarrow \widehat{M''} \longrightarrow 0$$

is exact.

Proof. The quotient topology induced on M'' by M is the same as its $\mathfrak{a}$-adic topology. Indeed,

$$\mathfrak{a}^n M'' = (\mathfrak{a}^n M + M')/M'.$$

The topology induced on M' from M is given by

$$M' \cap \mathfrak{a}^n M.$$

By the Artin–Rees lemma, this is a stable $\mathfrak{a}$-filtration on M', hence it defines the same topology as the $\mathfrak{a}$-adic filtration $\mathfrak{a}^n M'$.

Therefore, after passing to the quotient systems

$$0 \longrightarrow M'/(M' \cap \mathfrak{a}^n M) \longrightarrow M/\mathfrak{a}^n M \longrightarrow M''/\mathfrak{a}^n M'' \longrightarrow 0,$$

and taking inverse limits, the exactness result for inverse systems gives the desired exact sequence of completions. □

Proposition 8.25. *Let A be a Noetherian ring, let $\mathfrak{a} \subseteq A$ be an ideal, and let M be a finitely generated A-module. Then there is a natural isomorphism*

$$\widehat{A} \otimes_A M \cong \widehat{M}.$$

Proof. First suppose that M is free of finite rank. Then the result follows because completion commutes with finite direct sums.

For general finitely generated M, choose an exact sequence

$$F_1 \longrightarrow F_0 \longrightarrow M \longrightarrow 0$$

with F_0, F_1 finite free. By exactness of completion and right exactness of tensor product, both $\widehat{M}$ and $\widehat{A} \otimes_A M$ are obtained as cokernels of the corresponding maps

$$\widehat{F_1} \longrightarrow \widehat{F_0}.$$

Thus they are naturally isomorphic. □

Corollary 8.26. *Let A be a Noetherian ring and let $\widehat{A}$ be its $\mathfrak{a}$-adic completion. Then $\widehat{A}$ is flat over A.*

Proof. By the preceding proposition, tensoring a finitely generated module with $\widehat{A}$ agrees with completion. Since completion is exact on finitely generated modules, $\widehat{A}$ is flat over A. □

8.10 Some Properties of the Completed Ring

Proposition 8.27. *Let A be a Noetherian ring and let $\widehat{A}$ be its $\mathfrak{a}$-adic completion. Then:*

(i) $\mathfrak{a}\widehat{A}$ *is contained in the Jacobson radical of* $\widehat{A}$*;*

(ii) $(\mathfrak{a}\widehat{A})^n = \mathfrak{a}^n \widehat{A}$ *for all* $n \geq 0$*;*

(iii) the natural map induces an isomorphism

$$A/\mathfrak{a}^n \cong \widehat{A}/\mathfrak{a}^n \widehat{A}$$

for every n;

(iv) $\widehat{A}$ *is complete for the* $\mathfrak{a}\widehat{A}$*-adic topology.*

Proof. Since A is Noetherian, $\mathfrak{a}$ is finitely generated. Thus

$$\mathfrak{a}\widehat{A} = \widehat{\mathfrak{a}}.$$

Applying exactness of completion to

$$0 \longrightarrow \mathfrak{a}^n \longrightarrow A \longrightarrow A/\mathfrak{a}^n \longrightarrow 0$$

gives

$$\widehat{A}/\mathfrak{a}^n \widehat{A} \cong A/\mathfrak{a}^n.$$

This proves (ii) and (iii), and (iv) follows by taking the inverse limit.

For (i), consider the exact sequence

$$A/\mathfrak{a} \longrightarrow \widehat{A}/\mathfrak{a}\widehat{A}.$$

It is an isomorphism by (iii). Hence every maximal ideal of $\widehat{A}$ contains $\mathfrak{a}\widehat{A}$, so $\mathfrak{a}\widehat{A}$ is contained in the Jacobson radical. □

Proposition 8.28. *Let $(A, \mathfrak{m})$ be a Noetherian local ring. Then its $\mathfrak{m}$-adic completion $\widehat{A}$ is a Noetherian local ring, and its maximal ideal is*

$$\mathfrak{m}\widehat{A}.$$

Proof. By the previous proposition, $\mathfrak{m}\widehat{A}$ is contained in the Jacobson radical of $\widehat{A}$, and

$$\widehat{A}/\mathfrak{m}\widehat{A} \cong A/\mathfrak{m}$$

is a field. Hence $\mathfrak{m}\widehat{A}$ is the unique maximal ideal. □

8.11 Zariski Rings

Definition 8.29. Let A be a ring and let $\mathfrak{a} \subseteq A$ be an ideal. The ring A is called a *Zariski ring* for the $\mathfrak{a}$-adic topology if every ideal of A is closed in the $\mathfrak{a}$-adic topology.

Proposition 8.30. *Let A be a Noetherian ring and let $\mathfrak{a} \subseteq A$ be an ideal. Then A is a Zariski ring for the $\mathfrak{a}$-adic topology if and only if*

$$\mathfrak{a} \subseteq \operatorname{Jac}(A).$$

Proof. Assume first that $\mathfrak{a} \subseteq \operatorname{Jac}(A)$. Let M be a finitely generated A-module and let $M' \subseteq M$ be a submodule. By the Artin–Rees lemma, the topology induced on M' from M is equivalent to the $\mathfrak{a}$-adic topology. Applying Krull's intersection theorem to M/M' gives that M' is closed in M. In particular, every ideal of A is closed.

Conversely, suppose every ideal of A is closed. If $\mathfrak{a}$ were not contained in the Jacobson radical, then there would be a maximal ideal $\mathfrak{m}$ not containing $\mathfrak{a}$. Then

$$\mathfrak{m} + \mathfrak{a} = A.$$

It follows that $\mathfrak{m} + \mathfrak{a}^n = A$ for all n, so the closure of $\mathfrak{m}$ is all of A, contradicting the assumption that $\mathfrak{m}$ is closed. Hence $\mathfrak{a} \subseteq \operatorname{Jac}(A)$. □

Proposition 8.31. *Let A be a Noetherian ring, let $\mathfrak{a} \subseteq A$ be an ideal, and let $\widehat{A}$ be the $\mathfrak{a}$-adic completion. Then $\widehat{A}$ is a Zariski ring for the $\mathfrak{a}\widehat{A}$-adic topology.*

Proof. By the properties of the completed ring, $\mathfrak{a}\widehat{A}$ is contained in the Jacobson radical of $\widehat{A}$. The preceding proposition applies. □

8.12 Filtered Homomorphisms and Associated Graded Maps

Let $\varphi : M \to N$ be a homomorphism of filtered groups, with filtrations (M_n) and (N_n). Suppose that

$$\varphi(M_n) \subseteq N_n$$

for all n. Then φ induces homomorphisms

$$\mathrm{gr}(\varphi) : \mathrm{gr}(M) \to \mathrm{gr}(N)$$

and

$$\widehat{\varphi} : \widehat{M} \to \widehat{N}.$$

Lemma 8.32. *Let*

$$M \xrightarrow{\varphi} N \xrightarrow{\psi} P$$

be homomorphisms of filtered groups such that the filtrations are compatible with the maps. If the induced sequence

$$\mathrm{gr}(M) \xrightarrow{\mathrm{gr}(\varphi)} \mathrm{gr}(N) \xrightarrow{\mathrm{gr}(\psi)} \mathrm{gr}(P)$$

is exact, then the sequence on completions

$$\widehat{M} \xrightarrow{\widehat{\varphi}} \widehat{N} \xrightarrow{\widehat{\psi}} \widehat{P}$$

is exact, provided the filtrations are complete and separated.

Proof. The proof is obtained by lifting elements degree by degree. If an element maps to zero in the completion of P, its initial form lies in the kernel of $\mathrm{gr}(\psi)$, hence comes from the image of $\mathrm{gr}(\varphi)$. Subtracting such a lift raises the filtration degree. Iterating this process and using completeness gives a preimage in $\widehat{M}$. □

8.13 The Completion Theorem

Proposition 8.33. *Let A be a ring, let $\mathfrak{a} \subseteq A$ be an ideal, and let M be an A-module with an $\mathfrak{a}$-filtration (M_n). Suppose that A is complete in the $\mathfrak{a}$-adic topology and that M is Hausdorff in its filtration topology. If $\mathrm{gr}(M)$ is a finitely generated $\mathrm{gr}_{\mathfrak{a}}(A)$-module, then M is a finitely generated A-module.*

Proof. Choose homogeneous generators of $\mathrm{gr}(M)$, and lift them to elements $m_1, \dots, m_r \in M$. Let N be the submodule of M generated by these lifts. The induced map

$$N \longrightarrow M$$

is surjective on associated graded modules. Hence the cokernel has zero associated graded module. Since M/N is Hausdorff and complete, this forces $M/N = 0$. Thus $M = N$, so M is finitely generated. □

Theorem 8.34. *Let A be a Noetherian ring and let $\mathfrak{a} \subseteq A$ be an ideal. Then the $\mathfrak{a}$-adic completion $\widehat{A}$ is Noetherian.*

Proof. The associated graded ring of $\widehat{A}$ with respect to $\mathfrak{a}\widehat{A}$ is naturally isomorphic to

$$\mathrm{gr}_{\mathfrak{a}}(A).$$

Since A is Noetherian, $\mathrm{gr}_{\mathfrak{a}}(A)$ is a Noetherian graded ring. By the preceding proposition, ideals of $\widehat{A}$ are finitely generated. Hence $\widehat{A}$ is Noetherian. □

Corollary 8.35. *If A is Noetherian, then the formal power series ring*

$$A[[x_1, \ldots, x_n]]$$

is Noetherian.

Proof. For $n = 1$, the ring $A[[x]]$ is the (x)-adic completion of the Noetherian ring $A[x]$. Hence $A[[x]]$ is Noetherian. The general case follows by induction on n. □

Chapter 9

Dedekind Domains and Discrete Valuation Rings

The purpose of this chapter is to explain why one-dimensional normal Noetherian rings behave like the ring of integers. The local form of such a ring is a discrete valuation ring. Globally, the appropriate object is a Dedekind domain. Thus the theory of discrete valuation rings is the local theory of Dedekind domains, and the unique factorization of ideals in a Dedekind domain is obtained by reducing to this local theory.

Throughout this chapter, unless otherwise stated, all rings are commutative with identity and all domains are integral domains.

9.1 Valuation Rings

Definition 9.1. Let K be a field. A subring $V \subseteq K$ is called a *valuation ring* of K if for every nonzero $x \in K$ one has

$$x \in V \quad \text{or} \quad x^{-1} \in V.$$

Equivalently, K is the field of fractions of V and every element of K is comparable with 1 under divisibility by elements of V.

Proposition 9.2. *Let V be a valuation ring of K. Then:*

(i) V is a local ring.

(ii) Its maximal ideal is

$$\mathfrak{m}_V = \{x \in V : x^{-1} \notin V\}.$$

(iii) V is integrally closed in K.

Proof. Let

$$\mathfrak{m}_V = \{x \in V : x^{-1} \notin V\}.$$

If $x \in V \setminus \mathfrak{m}_V$, then $x^{-1} \in V$, so x is a unit. Conversely, if x is a unit of V, then $x^{-1} \in V$, hence $x \notin \mathfrak{m}_V$. Thus $V \setminus \mathfrak{m}_V$ is exactly the set of units of V. It remains only to see that $\mathfrak{m}_V$ is an ideal. If $x \in \mathfrak{m}_V$ and $a \in V$, then ax cannot be a unit of V, for otherwise x would be a unit. Hence $ax \in \mathfrak{m}_V$. If $x, y \in \mathfrak{m}_V$ and $x + y$ were a unit, then

$$1 = (x+y)(x+y)^{-1} = x(x+y)^{-1} + y(x+y)^{-1}.$$

Since a valuation ring compares divisibility, one of x/y or y/x belongs to V whenever $x, y \neq 0$. Suppose $x = ay$ with $a \in V$. Then $x + y = (a + 1)y$, so if $x + y$ is a unit, then y is a unit, a contradiction. The case $y = bx$ is the same. Thus $x + y \in \mathfrak{m}_V$, and V is local.

Now let $z \in K$ be integral over V. If $z \notin V$, then $z^{-1} \in V$ and z^{-1} is not a unit. Suppose

$$z^n + a_1 z^{n-1} + \cdots + a_n = 0, \qquad a_i \in V.$$

Multiplying by z^{-n} gives

$$1 + a_1 z^{-1} + a_2 z^{-2} + \cdots + a_n z^{-n} = 0.$$

Each term $a_i z^{-i}$ belongs to the maximal ideal $\mathfrak{m}_V$, hence their sum belongs to $\mathfrak{m}_V$. This says $1 \in \mathfrak{m}_V$, a contradiction. Hence $z \in V$. Therefore V is integrally closed. □

Proposition 9.3. *The ideals of a valuation ring are totally ordered by inclusion. In particular, prime ideals of a valuation ring are totally ordered by inclusion.*

Proof. Let I, J be ideals of V. Suppose $I \not\subseteq J$ and choose $x \in I \setminus J$. For any $y \in J$, if $y/x \notin V$, then $x/y \in V$, so $x = (x/y)y \in J$, a contradiction. Hence $y/x \in V$ and $y = (y/x)x \in I$. Thus $J \subseteq I$. Therefore any two ideals are comparable. □

9.2 Discrete Valuations

Definition 9.4. Let K be a field. A *discrete valuation* on K is a surjective group homomorphism

$$v : K^\times \longrightarrow \mathbb{Z}$$

from the multiplicative group of K to the additive group of $\mathbb{Z}$, such that

$$v(x + y) \geq \min\{v(x), v(y)\}$$

whenever $x, y, x + y$ are nonzero. We usually extend v by setting $v(0) = \infty$.

Definition 9.5. Given a discrete valuation v on K, define

$$V_v = \{x \in K : v(x) \geq 0\}.$$

This is called the *valuation ring* associated to v.

Proposition 9.6. *Let v be a discrete valuation on K. Then V_v is a local domain with maximal ideal*

$$\mathfrak{m}_v = \{x \in K : v(x) > 0\}.$$

Moreover, if $\pi \in K$ satisfies $v(\pi) = 1$, then every nonzero element $x \in K$ can be written uniquely in the form

$$x = u\pi^n,$$

where $u \in V_v^\times$ and $n = v(x) \in \mathbb{Z}$.

Proof. If $x, y \in V_v$, then

$$v(x + y) \geq \min\{v(x), v(y)\} \geq 0,$$

so $x + y \in V_v$, and $v(xy) = v(x) + v(y) \geq 0$, so $xy \in V_v$. Thus V_v is a subring of K. Its units are precisely the elements with valuation 0, because $x^{-1} \in V_v$ if and only

if $v(x^{-1}) = -v(x) \geq 0$. Hence the nonunits are exactly those elements with positive valuation, and they form the maximal ideal $\mathfrak{m}_v$.

If $v(\pi) = 1$ and $x \neq 0$, put $n = v(x)$. Then $v(x\pi^{-n}) = 0$, so $u = x\pi^{-n}$ is a unit of V_v, and $x = u\pi^n$. Uniqueness follows immediately from the value of $v(x)$ and from the fact that an element of valuation zero is a unit. □

9.3 Discrete Valuation Rings

Definition 9.7. A domain A is called a *discrete valuation ring*, or *DVR*, if there exists a discrete valuation v on its field of fractions K such that

$$A = \{x \in K : v(x) \geq 0\}.$$

Proposition 9.8. *Let A be a DVR with maximal ideal $\mathfrak{m}$. Then A is a principal ideal domain with a unique nonzero prime ideal. More precisely, if $\pi \in A$ has valuation 1, then*

$$\mathfrak{m} = (\pi)$$

and every nonzero ideal of A is of the form (π^n) for a unique $n \geq 0$.

Proof. Let I be a nonzero ideal of A. Choose an element $x \in I$ with $v(x)$ minimal among the values $v(y)$ for nonzero $y \in I$. Write $x = u\pi^n$, where u is a unit and $n = v(x)$. Then $(x) = (\pi^n)$. For every $y \in I$, we have $v(y) \geq n$, so $y \in (\pi^n)$. Thus $I = (\pi^n)$.

The nonunits of A are precisely the elements of positive valuation, so the maximal ideal is (π). Any nonzero prime ideal is of the form (π^n) with $n \geq 1$. It is prime only when $n = 1$, since (π^n) with $n > 1$ contains π^n but not π^{n-1} nor π. Therefore (π) is the unique nonzero prime ideal. □

Remark 9.9. A generator π of the maximal ideal of a DVR is called a *uniformizer*. Every nonzero element of the field of fractions can be written as a unit times a power of the uniformizer. Thus a DVR is the algebraic analogue of a ring in which there is exactly one irreducible element, up to units.

9.4 Characterizations of DVRs

Theorem 9.10 (Characterizations of DVRs)**.** *Let A be a Noetherian local domain with maximal ideal $\mathfrak{m}$ and field of fractions K. Assume A is not a field. The following are equivalent:*

(i) A is a discrete valuation ring.

(ii) A is a principal ideal domain.

(iii) $\mathfrak{m}$ is a principal ideal.

(iv) $\dim A = 1$ and A is integrally closed.

(v) A is a Noetherian valuation ring.

Proof. (i)⇒(ii) follows from the preceding proposition.

(ii)⇒(iii) is immediate, since every ideal of a PID is principal.

(iii)⇒(i). Write $\mathfrak{m} = (\pi)$. Since A is Noetherian local and not a field, Krull's intersection theorem gives

$$\bigcap_{n \geq 0} \mathfrak{m}^n = 0.$$

For every nonzero $x \in A$, there is a unique $n \geq 0$ such that $x \in \mathfrak{m}^n \setminus \mathfrak{m}^{n+1}$. Since $\mathfrak{m}^n = (\pi^n)$, we may write $x = u\pi^n$ with $u \notin \mathfrak{m}$, hence u is a unit. Extending this expression to $K = \mathrm{Frac}(A)$ defines a discrete valuation by

$$v\left(\frac{x}{y}\right) = v(x) - v(y).$$

Then $A = \{z \in K : v(z) \geq 0\}$, so A is a DVR.

(i)⇒(iv). A DVR is a PID, hence integrally closed. It has exactly one nonzero prime ideal, namely its maximal ideal, so its dimension is one.

(iv)⇒(iii). Since A is Noetherian local of dimension one, its maximal ideal is minimal over any nonzero principal ideal. Choose $0 \neq x \in \mathfrak{m}$. By the principal ideal theorem, every minimal prime over (x) has height at most one; since A is a domain and $x \neq 0$, such a minimal prime is nonzero, hence must be $\mathfrak{m}$. Therefore $\mathfrak{m}$ is the radical of (x). Thus for some $r > 0$, $\mathfrak{m}^r \subseteq (x)$.

Choose r minimal such that $\mathfrak{m}^r \subseteq (x)$, and choose $y \in \mathfrak{m}^{r-1}$ with $y \notin (x)$. Then $\mathfrak{m}y \subseteq (x)$. Put $z = x/y \in K$. Since $y \notin (x)$, we have $z^{-1} = y/x \notin A$. On the other hand, for every $a \in \mathfrak{m}$, $ay \in (x)$, hence $a/z = ay/x \in A$, so $\mathfrak{m}z^{-1} \subseteq A$. One shows from this that z^{-1} is integral over A if $\mathfrak{m}$ is not principal; this contradicts the integrally closed hypothesis. Hence $\mathfrak{m}$ is principal. More concretely, the standard determinant trick applied to the finite A-module $\mathfrak{m}$ and multiplication by z^{-1} gives integrality. Thus $\mathfrak{m}$ must be principal.

(i)⇒(v) is clear, since a DVR is a Noetherian valuation ring.

(v)⇒(iii). In a Noetherian valuation ring, every ideal is comparable. Since $\mathfrak{m}$ is finitely generated, say by $x_1, \ldots, x_n$, comparability of principal ideals implies that one of the ideals (x_i) contains all the others. Hence $\mathfrak{m} = (x_i)$ is principal. This proves (iii), and the theorem follows. □

9.5 Dedekind Domains

Definition 9.11. A domain A is called a *Dedekind domain* if it is Noetherian, integrally closed, and has Krull dimension one.

Example 9.12. Every principal ideal domain which is not a field is a Dedekind domain. Indeed, a PID is Noetherian, integrally closed, and every nonzero prime ideal is maximal.

Example 9.13. The ring $\mathbb{Z}$ is a Dedekind domain. More generally, the ring of integers of a number field is a Dedekind domain, although proving this requires more number theory than we develop here.

Proposition 9.14. *Let A be a Dedekind domain and let $\mathfrak{p}$ be a nonzero prime ideal. Then the localization $A_{\mathfrak{p}}$ is a discrete valuation ring.*

Proof. Since localization preserves Noetherianity, $A_{\mathfrak{p}}$ is Noetherian. Since integral closedness localizes, $A_{\mathfrak{p}}$ is integrally closed. Its prime ideals correspond to prime ideals of A contained in $\mathfrak{p}$. Since A has dimension one and $\mathfrak{p} \neq 0$, the only prime ideals contained in $\mathfrak{p}$ are (0) and $\mathfrak{p}$. Therefore $A_{\mathfrak{p}}$ is a one-dimensional Noetherian local integrally closed domain. By the characterization theorem above, $A_{\mathfrak{p}}$ is a DVR. □

Proposition 9.15. *Let A be a Noetherian domain of dimension one. Then A is a Dedekind domain if and only if $A_{\mathfrak{p}}$ is a DVR for every nonzero prime ideal $\mathfrak{p}$.*

Proof. If A is Dedekind, this follows from the preceding proposition.

Conversely, suppose that $A_{\mathfrak{p}}$ is a DVR for every nonzero prime ideal $\mathfrak{p}$. Then $A_{\mathfrak{p}}$ is integrally closed for every nonzero prime $\mathfrak{p}$. Also $A_{(0)}$ is the field of fractions of A, hence integrally closed. Integral closedness is a local property for domains: if an element of $\mathrm{Frac}(A)$ is integral over A, then it belongs to every $A_{\mathfrak{p}}$, hence belongs to A. Therefore A is integrally closed. Since A is Noetherian of dimension one by assumption, it is Dedekind. □

9.6 Fractional Ideals

Definition 9.16. Let A be a domain with field of fractions K. A *fractional ideal* of A is a nonzero A-submodule $I \subseteq K$ such that there exists $0 \neq d \in A$ with

$$dI \subseteq A.$$

A fractional ideal I is called *invertible* if there exists a fractional ideal J such that

$$IJ = A.$$

In this case J is denoted I^{-1}.

Definition 9.17. For a fractional ideal I define

$$I^{-1} = \{x \in K : xI \subseteq A\}.$$

This is again a fractional ideal when A is Noetherian and I is finitely generated.

Proposition 9.18. *Every nonzero fractional ideal of a Dedekind domain is invertible.*

Proof. It suffices to prove the assertion locally. Let I be a nonzero fractional ideal of a Dedekind domain A. For each nonzero prime $\mathfrak{p}$, the localization $I_{\mathfrak{p}}$ is a fractional ideal of the DVR $A_{\mathfrak{p}}$, hence is principal:

$$I_{\mathfrak{p}} = (\pi_{\mathfrak{p}}^{n_{\mathfrak{p}}})$$

for some integer $n_{\mathfrak{p}}$. Therefore

$$(II^{-1})_{\mathfrak{p}} = I_{\mathfrak{p}}(I_{\mathfrak{p}})^{-1} = A_{\mathfrak{p}}$$

for every nonzero prime $\mathfrak{p}$. Localizing at (0) also gives the field K. Hence II^{-1} localizes to $A_{\mathfrak{p}}$ at every prime ideal $\mathfrak{p}$, so $II^{-1} = A$. Thus I is invertible. □

Remark 9.19. The preceding proof uses the local-global principle for ideals: two fractional ideals of a Noetherian domain are equal if and only if their localizations at all prime ideals are equal. In practice it is enough to check maximal ideals.

9.7 Unique Factorization of Ideals

Theorem 9.20 (Unique Factorization of Ideals)**.** *Let A be a Dedekind domain. Every nonzero proper ideal I of A can be written uniquely in the form*

$$I = \mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_r^{n_r},$$

where the $\mathfrak{p}_i$ are distinct nonzero prime ideals and $n_i > 0$.

Proof. We first prove existence. Since A is Noetherian, if there were a nonzero proper ideal which is not a product of prime ideals, there would be a maximal such ideal I. The ideal I is not prime, so there exist $a, b \notin I$ with $ab \in I$. Then $I + (a)$ and $I + (b)$ strictly contain I, hence each is a product of prime ideals. Moreover

$$(I + (a))(I + (b)) \subseteq I.$$

Using invertibility of nonzero ideals, multiplying by I^{-1} and comparing ideal inclusions shows that I itself must be a product of prime ideals, a contradiction. Hence every nonzero proper ideal is such a product.

For uniqueness, localize at a nonzero prime $\mathfrak{p}$. Since $A_\mathfrak{p}$ is a DVR, every localized ideal is a power of $\mathfrak{p}A_\mathfrak{p}$. If

$$I = \prod_i \mathfrak{p}_i^{n_i} = \prod_j \mathfrak{q}_j^{m_j},$$

then localizing at $\mathfrak{p}$ gives

$$IA_\mathfrak{p} = (\mathfrak{p}A_\mathfrak{p})^n$$

where n is the exponent with which $\mathfrak{p}$ occurs in the factorization, and $n = 0$ if $\mathfrak{p}$ does not occur. The integer n is uniquely determined by the valuation of the DVR $A_\mathfrak{p}$. Thus every prime and every exponent is uniquely determined. □

Corollary 9.21. *In a Dedekind domain, every nonzero ideal is generated by at most two elements.*

Proof. This is a standard consequence of unique factorization of ideals and the Chinese remainder theorem. If

$$I = \prod_{i=1}^{r} \mathfrak{p}_i^{n_i},$$

choose $a \in I$ with prescribed valuations $v_{\mathfrak{p}_i}(a) = n_i$ at the finitely many primes occurring in I and nonnegative valuation elsewhere. Then one can choose $b \in I$ whose image generates the remaining local components modulo aA. Locally at each prime $\mathfrak{p}$, the ideal $(a, b)A_\mathfrak{p}$ equals $IA_\mathfrak{p}$. Hence $(a, b) = I$. □

9.8 The Ideal Class Group

Definition 9.22. Let A be a Dedekind domain. The set of nonzero fractional ideals of A forms an abelian group under multiplication. The subgroup of principal fractional ideals is

$$\{xA : x \in K^\times\}.$$

The quotient group

$$\mathrm{Cl}(A) = \{\text{nonzero fractional ideals of } A\}/\{\text{principal fractional ideals}\}$$

is called the *ideal class group* of A.

Proposition 9.23. *A Dedekind domain A is a principal ideal domain if and only if*

$$\mathrm{Cl}(A) = 0.$$

Proof. If A is a PID, every nonzero ideal is principal, and hence every fractional ideal is principal. Thus the class group is trivial.

Conversely, if $\mathrm{Cl}(A) = 0$, then every nonzero fractional ideal is principal. In particular, every nonzero integral ideal of A is principal. Hence A is a PID. □

Remark 9.24. The class group measures the failure of unique factorization of elements. In a Dedekind domain, ideals always factor uniquely into prime ideals. The obstruction to unique factorization of elements is precisely that prime ideals need not be principal.

9.9 Dedekind Domains and Curves

Remark 9.25. Dedekind domains appear naturally in algebraic geometry. If X is a nonsingular affine curve and $A = \Gamma(X, \mathcal{O}_X)$ is its coordinate ring, then A is a Dedekind domain. The local ring at a closed point is a DVR, and the valuation measures the order of vanishing at that point. Thus the factorization

$$I = \prod_{\mathfrak{p}} \mathfrak{p}^{n_{\mathfrak{p}}}$$

is the algebraic analogue of writing a divisor as a sum of points with multiplicities.

Chapter 10

Regular Local Rings and Smoothness

This chapter is meant to connect the commutative algebra developed so far with the local geometry of affine varieties. The guiding principle is the following: local rings are algebraic models of neighborhoods of points, and regular local rings are algebraic models of smooth neighborhoods.

The central slogan of the chapter is

$$p \in X \text{ is smooth} \quad \Longleftrightarrow \quad \mathcal{O}_{X,p} \text{ is a regular local ring.}$$

This is one of the basic bridges between commutative algebra and algebraic geometry.

10.1 Local Rings Revisited

Let $(A, \mathfrak{m})$ be a local ring. The ideal $\mathfrak{m}$ consists of the elements which vanish at the distinguished point, and the residue field

$$k = A/\mathfrak{m}$$

is the field of values at that point. When $A = \mathcal{O}_{X,p}$ is the local ring of an affine variety X at a point p, an element of A is a rational function which is regular in a neighborhood of p, and $\mathfrak{m}$ consists of those functions whose value at p is zero.

The quotient $\mathfrak{m}/\mathfrak{m}^2$ measures first-order vanishing. This is the algebraic source of tangent spaces.

Definition 10.1. Let $(A, \mathfrak{m}, k)$ be a local ring. The k-vector space

$$\mathfrak{m}/\mathfrak{m}^2$$

is called the *cotangent space* of A. Its dual

$$(\mathfrak{m}/\mathfrak{m}^2)^* = \mathrm{Hom}_k(\mathfrak{m}/\mathfrak{m}^2, k)$$

is called the *tangent space* of A.

Remark 10.2. The terminology comes from geometry. If $A = \mathcal{O}_{X,p}$, then elements of $\mathfrak{m}$ are functions vanishing at p, while elements of $\mathfrak{m}^2$ vanish to at least second order. Therefore $\mathfrak{m}/\mathfrak{m}^2$ records the linear, or first-order, parts of functions at p.

Example 10.3. Let

$$A = k[x_1, \dots, x_n]_{(x_1,\dots,x_n)}.$$

Then A is a local ring with maximal ideal

$$\mathfrak{m} = (x_1, \dots, x_n)A.$$

The images of $x_1, \dots, x_n$ form a basis of $\mathfrak{m}/\mathfrak{m}^2$, so

$$\dim_k \mathfrak{m}/\mathfrak{m}^2 = n.$$

This agrees with the fact that the tangent space of affine n-space at the origin has dimension n.

10.2 Derivations and Tangent Vectors

The dual definition of tangent space has a useful intrinsic interpretation in terms of derivations.

Definition 10.4. Let A be a k-algebra and let M be an A-module. A k-linear map

$$D : A \longrightarrow M$$

is called a *k-derivation* if

$$D(ab) = aD(b) + bD(a)$$

for all $a, b \in A$. The set of all such derivations is denoted by

$$\mathrm{Der}_k(A, M).$$

Let $(A, \mathfrak{m}, k)$ be a local k-algebra, and regard $k = A/\mathfrak{m}$ as an A-module. If

$$D : A \longrightarrow k$$

is a k-derivation, then for $x, y \in \mathfrak{m}$ we have

$$D(xy) = xD(y) + yD(x) = 0,$$

because x and y act as zero on k. Hence D vanishes on $\mathfrak{m}^2$ and gives a k-linear map $\mathfrak{m}/\mathfrak{m}^2 \to k$.

Conversely, any k-linear map $\mathfrak{m}/\mathfrak{m}^2 \to k$ extends uniquely to a derivation $A \to k$ by sending constants in k to zero and using the decomposition of first-order parts.

Proposition 10.5. *Let $(A, \mathfrak{m}, k)$ be a local k-algebra. There is a natural isomorphism*

$$\mathrm{Der}_k(A, k) \cong (\mathfrak{m}/\mathfrak{m}^2)^*.$$

Proof. A derivation $D : A \to k$ vanishes on $k \subseteq A$ and on $\mathfrak{m}^2$, as explained above. Thus it induces a k-linear map $\mathfrak{m}/\mathfrak{m}^2 \to k$.

Conversely, a linear functional $\lambda : \mathfrak{m}/\mathfrak{m}^2 \to k$ defines a first-order operator on A by extracting the linear part of an element and applying λ. The Leibniz rule holds because the product of two elements of $\mathfrak{m}$ vanishes in $\mathfrak{m}/\mathfrak{m}^2$. These two constructions are inverse to each other. □

Remark 10.6. This proposition explains why the tangent space is the dual of $\mathfrak{m}/\mathfrak{m}^2$ rather than $\mathfrak{m}/\mathfrak{m}^2$ itself: tangent vectors are directional derivatives, hence linear functionals on first-order functions.

10.3 Embedding Dimension

Definition 10.7. Let $(A, \mathfrak{m}, k)$ be a Noetherian local ring. The *embedding dimension* of A is

$$\operatorname{edim}(A) = \dim_k \mathfrak{m}/\mathfrak{m}^2.$$

By Nakayama's lemma, $\dim_k \mathfrak{m}/\mathfrak{m}^2$ is the minimal number of generators of the maximal ideal $\mathfrak{m}$. Thus embedding dimension is an intrinsic algebraic measure of how many local coordinates are needed to describe the point.

Proposition 10.8. *Let $(A, \mathfrak{m}, k)$ be a Noetherian local ring. If $\mathfrak{m}$ can be generated by r elements, then*

$$\dim A \leq r.$$

Consequently,

$$\dim A \leq \operatorname{edim}(A).$$

Proof. Suppose $\mathfrak{m} = (x_1, \ldots, x_r)$. Then $A/(x_1, \ldots, x_r)$ is a field, hence has dimension zero. Applying Krull's principal ideal theorem successively shows that each time one quotients by one element, the dimension drops by at most one. Therefore $\dim A \leq r$. Taking r to be the minimal number of generators of $\mathfrak{m}$ gives the second assertion by Nakayama's lemma. □

10.4 Regular Local Rings

Definition 10.9. Let $(A, \mathfrak{m}, k)$ be a Noetherian local ring. We say that A is a *regular local ring* if

$$\dim A = \dim_k \mathfrak{m}/\mathfrak{m}^2.$$

Equivalently,

$$\dim A = \operatorname{edim}(A).$$

The inequality

$$\dim A \leq \operatorname{edim}(A)$$

always holds for Noetherian local rings. Thus regularity says that there are no extra tangent directions beyond those forced by the dimension.

Example 10.10. The local ring

$$k[x_1, \ldots, x_n]_{(x_1, \ldots, x_n)}$$

is regular. Indeed, its dimension is n, and the maximal ideal is minimally generated by $x_1, \ldots, x_n$.

Example 10.11. Let

$$A = k[x, y]_{(x,y)}/(y^2 - x^3).$$

The maximal ideal is generated by the images of x and y, so

$$\dim_k \mathfrak{m}/\mathfrak{m}^2 = 2.$$

But A is a one-dimensional local domain, since it is the local ring of a plane curve. Hence

$$\dim A = 1 < 2 = \operatorname{edim}(A),$$

so A is not regular. Geometrically, this is the cusp singularity at the origin.

10.5 One-Dimensional Regular Local Rings

The one-dimensional case connects regular local rings with DVRs.

Theorem 10.12. *Let $(A, \mathfrak{m})$ be a Noetherian local domain of dimension one. Then the following are equivalent.*

(i) *A is a regular local ring.*

(ii) *$\mathfrak{m}$ is principal.*

(iii) *A is a discrete valuation ring.*

Proof. Since $\dim A = 1$, the ring A is regular if and only if

$$\dim_{A/\mathfrak{m}} \mathfrak{m}/\mathfrak{m}^2 = 1.$$

By Nakayama's lemma, this is equivalent to saying that $\mathfrak{m}$ is generated by one element. Thus (i) and (ii) are equivalent.

If A is a DVR, then its maximal ideal is generated by a uniformizer, so (iii) implies (ii).

Conversely, suppose $\mathfrak{m} = (t)$. Since A is a one-dimensional Noetherian local domain, every nonzero proper ideal is $\mathfrak{m}$-primary. For a nonzero element $x \in A$, there is a largest integer n such that $x \in (t^n)$. Then $x = t^n u$ with $u \notin \mathfrak{m}$, hence u is a unit. It follows that every nonzero ideal is generated by a power of t. Therefore A is a principal ideal domain with a unique nonzero prime ideal, hence a DVR. □

Corollary 10.13. *A one-dimensional Noetherian local domain is a DVR if and only if it is regular.*

This corollary explains why DVRs are the correct local rings for smooth curves. At a nonsingular point of a curve, there is a single uniformizing parameter.

10.6 Local Rings of Affine Varieties

Recall from Chapter 1 that an affine algebraic set over an algebraically closed field k is a subset

$$X = V(I) \subseteq \mathbb{A}^n_k.$$

Its coordinate ring is

$$k[X] = k[x_1, \ldots, x_n]/I(X),$$

where $I(X)$ is the ideal of all polynomials vanishing on X.

For a point $p \in X$, let $\mathfrak{m}_p \subseteq k[X]$ be the maximal ideal of functions vanishing at p. The local ring of X at p is

$$\mathcal{O}_{X,p} = k[X]_{\mathfrak{m}_p}.$$

This is the ring of rational functions on X which are regular in a neighborhood of p.

Definition 10.14. The Zariski tangent space of X at p is

$$T_p X = (\mathfrak{m}_p/\mathfrak{m}_p^2)^*.$$

Thus the tangent space is constructed purely from the local ring.

10.7 The Jacobian Description of the Tangent Space

Suppose

$$X = V(f_1, \ldots, f_r) \subseteq \mathbb{A}_k^n,$$

and let

$$p = (a_1, \ldots, a_n) \in X.$$

The Jacobian matrix at p is

$$J(p) = \left(\frac{\partial f_i}{\partial x_j}(p) \right)_{i,j}.$$

Theorem 10.15 (Jacobian description of the tangent space)**.** *With notation as above,*

$$T_p X \cong \ker J(p) \subseteq k^n.$$

Equivalently, a vector $v = (v_1, \ldots, v_n) \in k^n$ is tangent to X at p if and only if

$$\sum_{j=1}^{n} \frac{\partial f_i}{\partial x_j}(p) v_j = 0$$

for all $i = 1, \ldots, r$.

Proof. Let $v \in k^n$. The directional derivative at p defines a derivation

$$D_v : k[x_1, \ldots, x_n] \longrightarrow k, \qquad D_v(g) = \sum_{j=1}^{n} \frac{\partial g}{\partial x_j}(p) v_j.$$

This derivation descends to the quotient coordinate ring $k[X]$ if and only if it vanishes on the ideal $(f_1, \ldots, f_r)$. This is equivalent to the displayed system of linear equations. Since tangent vectors are derivations $k[X] \to k$, the result follows from the identification of derivations with the dual of $\mathfrak{m}_p/\mathfrak{m}_p^2$. □

Corollary 10.16. *If $X = V(f) \subseteq \mathbb{A}_k^n$ is a hypersurface, then*

$$T_p X = \ker \left(\frac{\partial f}{\partial x_1}(p), \ldots, \frac{\partial f}{\partial x_n}(p) \right).$$

In particular, if at least one partial derivative of f is nonzero at p, then $\dim_k T_p X = n - 1$.

10.8 Smooth Points

For an affine variety, the dimension of the tangent space is always at least the local dimension. Smoothness means that equality holds.

Definition 10.17. Let X be an affine variety over an algebraically closed field k, and let $p \in X$. We say that p is a *smooth point* of X if

$$\dim_k T_p X = \dim \mathcal{O}_{X,p}.$$

Otherwise p is called a *singular point.*

Since

$$T_pX = (\mathfrak{m}_p/\mathfrak{m}_p^2)^*,$$

we have

$$\dim_k T_pX = \operatorname{edim}(\mathcal{O}_{X,p}).$$

Thus the definition says exactly that the local ring is regular.

Theorem 10.18. *Let X be an affine variety and let $p \in X$. Then*

$$p \text{ is smooth on } X \iff \mathcal{O}_{X,p} \text{ is a regular local ring.}$$

Proof. By definition,

$$p \text{ is smooth} \iff \dim_k T_pX = \dim \mathcal{O}_{X,p}.$$

But

$$\dim_k T_pX = \dim_k \mathfrak{m}_p/\mathfrak{m}_p^2.$$

Therefore smoothness is equivalent to

$$\dim_k \mathfrak{m}_p/\mathfrak{m}_p^2 = \dim \mathcal{O}_{X,p},$$

which is precisely the definition of regularity of the local ring $\mathcal{O}_{X,p}$. □

10.9 The Jacobian Criterion

The previous theorem gives an intrinsic characterization of smoothness. The Jacobian criterion gives a concrete way to check it.

Theorem 10.19 (Jacobian criterion)**.** *Let*

$$X = V(f_1, \dots, f_r) \subseteq \mathbb{A}_k^n$$

be an affine variety over an algebraically closed field k, and let $p \in X$. Then p is smooth if and only if

$$\operatorname{rank} J(p) = n - \dim \mathcal{O}_{X,p}.$$

Equivalently,

$$\dim_k \ker J(p) = \dim \mathcal{O}_{X,p}.$$

Proof. By the Jacobian description of the tangent space,

$$T_pX \cong \ker J(p).$$

Hence

$$\dim_k T_pX = n - \operatorname{rank} J(p).$$

The point p is smooth if and only if

$$\dim_k T_pX = \dim \mathcal{O}_{X,p}.$$

Substituting the expression above gives the desired equality. □

Remark 10.20. For a hypersurface $X = V(f) \subseteq \mathbb{A}_k^n$, the Jacobian criterion says that a point $p \in X$ is singular if and only if

$$f(p) = 0, \qquad \frac{\partial f}{\partial x_1}(p) = \cdots = \frac{\partial f}{\partial x_n}(p) = 0.$$

Thus singularities of hypersurfaces are exactly the common zeros of the equation and all its first partial derivatives.

10.10 Examples

Example 10.21 (A smooth parabola)**.** Let

$$X = V(y - x^2) \subseteq \mathbb{A}^2_k.$$

Then

$$J = (-2x, 1).$$

At every point, the rank of J is 1. Since X is a curve, its local dimension is 1, and

$$2 - \operatorname{rank} J = 1.$$

Therefore every point of X is smooth.

Example 10.22 (The cusp)**.** Let

$$X = V(y^2 - x^3) \subseteq \mathbb{A}^2_k.$$

The Jacobian row is

$$(-3x^2, 2y).$$

At the origin this is $(0, 0)$, so

$$\dim_k T_{(0,0)}X = 2.$$

But X is a curve, so the local dimension is 1. Hence the origin is singular. This agrees with the algebraic computation

$$\dim_k \mathfrak{m}/\mathfrak{m}^2 = 2 > 1 = \dim \mathcal{O}_{X,(0,0)}.$$

Example 10.23 (A node)**.** Let

$$X = V(y^2 - x^2(x + 1)) \subseteq \mathbb{A}^2_k.$$

At the origin the Jacobian row is again zero, so the tangent space has dimension 2, while the curve has dimension 1. Hence the origin is singular. In this case the singularity has two tangent directions, unlike the cusp.

10.11 Further Directions

Regular local rings are the algebraic incarnation of smooth local geometry. They appear throughout algebraic geometry in many forms.

- Normality is weaker than regularity; regular local rings are normal, but normal rings may still have singularities.
- Completion studies formal neighborhoods of points. For a smooth point, the completed local ring resembles a formal power series ring.
- Etale morphisms and smooth morphisms generalize the idea of local coordinate systems to relative algebraic geometry.
- Resolution of singularities asks whether singular local rings can be replaced by regular ones after suitable birational modifications.

Thus the local geometry of an algebraic variety is encoded in the algebraic structure of its local ring.