

# Commutative Algebra 1

Labix

May 18, 2025

**Abstract**

## Contents

<b>1</b>	<b>Ideals Of a Commutative Ring</b>	<b>4</b>
1.1	Basic Operations on Ideals . . . . .	4
1.2	The Nilradical of Commutative Rings . . . . .	5
1.3	The Jacobson Radical of Commutative Rings . . . . .	7
1.4	The Radical of an Ideal . . . . .	7
1.5	The Correspondence between Ideals and the Quotient . . . . .	9
1.6	Extensions and Contractions of Ideals . . . . .	11
1.7	Minimal Prime Ideals . . . . .	13
<b>2</b>	<b>Basic Notions of Commutative Rings</b>	<b>14</b>
2.1	Noetherian Commutative Rings . . . . .	14
2.2	Artinian Commutative Rings . . . . .	15
2.3	Local Rings . . . . .	16
2.4	Revisiting the Polynomial Ring . . . . .	17
<b>3</b>	<b>Modules over a Commutative Ring</b>	<b>20</b>
3.1	Cayley-Hamilton Theorem . . . . .	20
3.2	Nakayama's Lemma . . . . .	21
3.3	Change of Rings . . . . .	22
3.4	Properties of the Hom Set . . . . .	23
3.5	More on Exact Sequences . . . . .	24
<b>4</b>	<b>Algebra Over a Commutative Ring</b>	<b>26</b>
4.1	Commutative Algebras . . . . .	26
4.2	Free Commutative Algebras . . . . .	26
4.3	Finiteness Properties of Algebras . . . . .	27
<b>5</b>	<b>Localization</b>	<b>28</b>
5.1	Localization of Modules . . . . .	28
5.2	Localization at Single Elements and Away from Prime Ideals . . . . .	30
5.3	The Localization Map . . . . .	30
5.4	Ideals of a Localization . . . . .	32
5.5	Localization of Graded Rings . . . . .	34
5.6	Local Properties . . . . .	34
<b>6</b>	<b>Primary Decomposition</b>	<b>36</b>
6.1	The Annihilator and Associated Primes . . . . .	36
6.2	The Support of a Module . . . . .	38
6.3	Primary Ideals . . . . .	40
6.4	Primary Decomposition . . . . .	41
6.5	The Two Uniqueness Theorems . . . . .	42
6.6	Symbolic Powers . . . . .	43
<b>7</b>	<b>Integral Dependence</b>	<b>44</b>
7.1	Integral Elements . . . . .	44
7.2	Integral Closure . . . . .	44
7.3	Four Main Theorems of Integral Extensions . . . . .	46
7.4	Zariski's Lemma . . . . .	47
7.5	Normal Domains . . . . .	48
<b>8</b>	<b>Introduction to Dimension Theory for Rings</b>	<b>51</b>
8.1	Krull Dimension . . . . .	51
8.2	Noether Normalization Lemma . . . . .	52
8.3	Height of Prime Ideals . . . . .	53
8.4	The Length of Modules over Commutative Rings . . . . .	54
8.5	Structure Theorem for Artinian Rings . . . . .	55

<b>9</b>	<b>Valuation and Valuation Rings</b>	<b>57</b>
9.1	Valuation Rings . . . . .	57
9.2	Discrete Valuation Rings . . . . .	58
<b>10</b>	<b>Dedekind Domains</b>	<b>62</b>
10.1	Fractional Ideals . . . . .	62
10.2	Invertible Ideals . . . . .	62
10.3	Dedekind Domains . . . . .	64
10.4	Prime Factorization of Ideals . . . . .	65

# 1 Ideals Of a Commutative Ring

## 1.1 Basic Operations on Ideals

Recall that  $(R, +, \cdot)$  is a ring if the following axioms hold.

- $(R, +)$  is an abelian group.
- Multiplicative Associativity:  $x \cdot (y \cdot z) = (x \cdot y) \cdot z$ .
- Multiplicative Identity: There exists  $1_R \in R$  such that  $x \cdot 1_R = x = 1_R \cdot x$  for all  $x \in R$ .
- Left distributivity:  $r \cdot (x + y) = r \cdot x + r \cdot y$  for all  $r, x, y \in R$ .
- Right distributivity:  $(x + y) \cdot r = x \cdot r + y \cdot r$  for all  $r, x, y \in R$ .

A ring  $R$  is commutative if

$$x \cdot y = y \cdot x$$

for all  $x, y \in R$ .

Let  $R$  be a commutative ring. Recall that an ideal of  $R$  is a subset  $I \subseteq R$  such that

- If  $a, b \in I$ , then  $a + b \in I$ .
- If  $r \in R$  and  $a \in I$ , then  $ra \in I$ .

**Lemma 1.1.1** Let  $R$  be a commutative ring. Let  $I, J$  be ideals of  $R$ . Let  $P$  be a prime ideal of  $R$ . Then the following are equivalent.

- $IJ \subseteq P$ .
- $I \cap J \subseteq P$ .
- $I \subseteq P$  or  $J \subseteq P$ .

### Proof

- (1)  $\implies$  (2): Let  $f \in I \cap J$ . Then  $f \in I$  and  $f \in J$  implies that  $f^2 \in IJ \subseteq P$ . Since  $P$  is prime, we conclude that  $f \in P$ .
- (2)  $\implies$  (3): Suppose that  $f \in I$  and  $f \notin P$ . For any  $g \in J$ , we have  $fg \in I \cap J \subseteq P$ . Since  $P$  is prime and  $f \notin P$ , we have  $g \in P$ . Thus  $J \subseteq P$ .
- (3)  $\implies$  (1): Without loss of generality suppose that  $I \subseteq P$ . Then  $IJ \subseteq I \subseteq P$ .

■

**Proposition 1.1.2 (Prime Avoidance)** Let  $R$  be a commutative ring. Let  $I_1, \dots, I_n$  be ideals of  $R$ . Let  $P_1, \dots, P_k$  be prime ideals of  $R$ .

- Let  $I$  be an ideal of  $R$ . If  $I \subseteq \bigcup_{i=1}^k P_i$ , then  $I \subseteq P_i$  for some  $i$ .
- Let  $P$  be an ideal of  $R$ . If  $\bigcap_{i=1}^n I_i \subseteq P$ , then  $I_i \subseteq P$  for some  $i$ .
- Let  $P$  be an ideal of  $R$ . If  $P = \bigcap_{i=1}^n I_i$ , then  $I_i = P$  for some  $i$ .

### Proof

- We prove the contrapositive by induction  $k$ . When  $k = 1$ , the case is clear. Suppose that  $I \not\subseteq P_i$  for  $1 \leq i \leq k-1$  implies  $I \not\subseteq \bigcup_{i=1}^{k-1} P_i$ . Now suppose that  $I \not\subseteq P_i$  for  $1 \leq i \leq k$ . By induction hypothesis, for each  $i$ , there exists  $x_j \in I$  such that  $x_j \notin \bigcup_{j \neq i} P_j$ . So  $x_j \notin P_i$  for  $j \neq i$ . There are two cases. If  $x_j \notin P_j$  for some  $j$ , then  $x_j \notin \bigcup_{j \neq i} P_j \cup P_j = \bigcup_{j=1}^k P_j$  so we are done. If  $x_j \in P_j$  for all  $j$ , then consider the element  $y = \sum_{i=1}^k \prod_{j \neq i} x_j \in I$ . Notice

that  $x_j \in P_j$  for  $j \neq i$  implies that  $\prod_{j \neq i} x_j$  lie in  $P_k$  for any  $k \neq i$ . It is not an element of  $P_i$  because  $P_i$  is prime and  $x_j \notin P_i$  for  $j \neq i$ . Then we conclude that  $y$  does not lie in  $P_i$  for any  $i$ . Hence  $y \notin \bigcup_{i=1}^k P_i$  and we are done.

- We prove the contrapositive. Suppose that  $I_i \not\subseteq P$  for all  $i$ . Then for each  $i$ , there exists  $x_i \in I_i$  such that  $x_i \notin P$ . Then  $\prod_{i=1}^n x_i \in \bigcap_{i=1}^n I_i$  is not an element of  $P$  since  $P$  is a prime ideal. Hence we are done.
- By the above, we have that  $P = \bigcap_{i=1}^n I_i$  implies that  $I_i \subseteq P$  for some  $i$ . Then  $P = \bigcap_{i=1}^n I_i \subseteq I_i$  implies that  $P = I_i$ .

■

**Example 1.1.3** There is an isomorphism given by

$$\frac{\mathbb{Z}[x]}{(x+1, x^2+2)} \cong \mathbb{Z}/3\mathbb{Z}$$

**Proof** Using the above propositions, we have that

$$\begin{aligned} \frac{\mathbb{Z}[x]}{(x+1, x^2+2)} &= \frac{\mathbb{Z}[x]}{(x+1) + (x^2+2)} \\ &\cong \frac{\mathbb{Z}[x]/(x+1)}{(3)} \end{aligned}$$

Indeed, the ideal  $(x^2+2)$  corresponds to the ideal  $(3)$  in  $\frac{\mathbb{Z}[x]}{(x+1)}$  because the remainder of  $x^2+2$  divided by  $(x+1)$  is  $(3)$ . Now  $\mathbb{Z}[x]/(x+1) \cong \mathbb{Z}$  by the evaluation homomorphism. Thus quotienting by the ideal  $(3)$  gives the field  $\mathbb{Z}/3\mathbb{Z}$ . ■

Let  $R$  be a commutative ring. Recall that two ideals  $I, J$  are coprime if  $I + J = R$ . In particular, this implies that  $IJ = I \cap J$ . Then the Chinese Remainder theorem reads as

$$\frac{R}{\prod_{i=1}^k I_i} = \frac{R}{\bigcap_{i=1}^k I_i} \cong \prod_{i=1}^k \frac{R}{I_i}$$

## 1.2 The Nilradical of Commutative Rings

Let  $R$  be a ring. Recall that an element  $r \in R$  is nilpotent if  $r^n = 0_R$  for some  $n \in \mathbb{N}$ . When  $R$  is commutative, we can form an ideal out of nilpotent elements.

**Definition 1.2.1 (Nilradicals)** Let  $R$  be a commutative ring. Define the nilradical of  $R$  to be

$$N(R) = \{r \in R \mid r \text{ is nilpotent}\}$$

Note that this is different from nilpotent ideals, as nilpotency is a property of an ideal. However the Nilradical ideal is a nil ideal and every sub-ideal of the nilradical is a nil ideal.

**Proposition 1.2.2** Let  $R$  be a ring and  $N(R)$  its nilradical. Then the following are true.

- $N(R)$  is an ideal of  $R$
- $N(R/N(R)) = 0$

**Proof**

- Suppose that  $r, s$  are nilpotent, meaning that  $r^n = 0$  and  $s^m = 0$ . Then  $(r + s)^{n+m} = 0$ . Moreover, if  $t \in R$  then  $t \cdot r$  is also nilpotent
- Let  $r \notin N(R)$ . Every element  $r + N(R) \in R/N(R)$  has the property that  $r^n \neq 0$ . Consider  $(r + N(R))^n = r^n + N(R)$ . If  $r^n \in N(R)$  then  $r^n = u$  for some nilpotent  $u$ , which means that  $r^n$  is nilpotent and thus  $r$  is nilpotent, a contradiction. This means that  $r + N(R) \notin N(R/N(R))$  for all  $r \notin N(R)$  and thus  $N(R/N(R)) = 0$

■

**Proposition 1.2.3** Let  $R$  be a commutative ring. Then we have

$$N(R) = \bigcap_{\substack{P \text{ is a prime} \\ \text{ideal of } R}} P$$

**Proof** Let  $x \in N(R)$ . Let  $P$  be an arbitrary prime ideal. Since  $x$  is nilpotent,  $x^n = 0$  for some  $n \in \mathbb{N}$ . If  $x \notin P$ , then  $x^2 \notin P$  since  $P$  is a prime ideal. Recursively we see that  $x^k \notin P$  for all  $k \in \mathbb{N} \setminus \{0\}$ . But  $x^n = 0 \in P$  is a contradiction. Hence  $N(R) \subseteq \bigcap_{P \in \text{Spec}(R)} P$ .

Now suppose that  $x \in R$  is not nilpotent. Consider the set

$$\Sigma = \{I \trianglelefteq R \mid x^k \notin I \text{ for all } k \geq 1\}$$

Notice that  $(0) \in \Sigma$  and hence it is non-empty. Let  $I_1 \subseteq I_2 \subseteq \dots$  be a chain in  $\Sigma$ . Define  $I = \bigcup_{k=1}^{\infty} I_k$ . I claim that  $I \in \Sigma$ . First of all if  $a, b \in I$  and  $r \in R$ , then  $a \in I_m$  and  $b \in I_n$  for some  $m, n \geq 1$ . Then  $a, b \in I_{\max\{m, n\}}$  so that  $a + b \in I_{\max\{m, n\}} \subseteq I$ . Also  $ra \in I_m \subseteq I$  since  $I_m$  is an ideal. Hence  $I$  itself is an ideal of  $R$ . Suppose for a contradiction that  $x^n \in I$  for some  $n$ . Then  $x^n \in I_k$  for some  $k$ . This is a contradiction since  $I_k \in \Sigma$ . Thus we know that  $I \in \Sigma$ . In particular,  $I$  is an upper bound of  $I_1 \subseteq I_2 \subseteq \dots$ . By Zorn's lemma, we conclude that  $\Sigma$  has a maximal element, say  $P$ .

Suppose for a contradiction that  $P$  is not a prime ideal. Let  $ab \in P$  and  $a, b \notin P$ . Then  $P \subset P + (a), P + (b)$ . Since  $P$  is maximal in  $\Sigma$ ,  $P + (a)$  and  $P + (b)$  cannot be in  $\Sigma$ , and there exists  $x^m \in P + (a)$  and  $x^n \in P + (b)$  for some  $m, n$ . Then

$$x^{m+n} = x^m \cdot x^n \in (P + (a))(P + (b)) = P + (ab)$$

Hence  $P + (ab) \notin \Sigma$ . But  $ab \in P$  implies that  $P + (ab) = P$ . We have reached a contradiction. Thus  $P$  is a prime ideal that does not contain  $x$ . We show that  $x \notin N(R)$  implies  $x \notin P$  for some prime ideal  $P$ . The contrapositive of this statement is  $x \in P$  for all prime ideals  $P$  implies  $x \in N(R)$ . Hence we are done. ■

**Example 1.2.4** Consider the ring

$$R = \frac{\mathbb{C}[x, y]}{(x^2 - y, xy)}$$

Then its nilradical is given by  $N(R) = (x, y)$ .

**Proof** Notice that in the ring  $R$ ,  $x^3 = x(x^2) = xy = 0$  and  $y^3 = x^6 = (x^3)^2 = 0$  and hence  $x$  and  $y$  are both nilpotent elements of  $R$ . By definition of the nilradical, we conclude that  $(x, y) \subseteq N(R)$ . Now  $(x, y)$  is a maximal ideal of  $\mathbb{C}[x, y]$  because  $\mathbb{C}[x, y]/(x, y) \cong \mathbb{C}$ . Also notice that  $(x, y) \subseteq$

$(x^2 - y, xy)$  because for any element  $f(x)(x^2 - y) + g(x)(xy) \in (x^2 - y, xy)$ , we have that

$$\begin{aligned} f(x)(x^2 - y) + g(x)(xy) &\in (x^2 - y, xy) = (xf(x))x - f(x)y + (g(x)x)y \\ &= (xf(x))x + (xg(x) - f(x))y \in (x, y) \end{aligned}$$

By the correspondence theorem,  $(x, y)/(x^2 - y)$  is an maximal ideal of  $R$ . In particular,  $(x, y)$  is also a prime ideal. But the  $N(R)$  is the intersection of all prime ideals and hence  $N(R) \subseteq (x, y)$ . We conclude that  $N(R) = (x, y)$ . ■

**Definition 1.2.5 (Reduced Rings)** Let  $R$  be a commutative ring. We say that  $R$  is reduced if  $N(R) = 0$ .

### 1.3 The Jacobson Radical of Commutative Rings

Let  $R$  be a commutative ring. Recall that the Jacobson radical of a ring is defined to be

$$J(R) = \bigcap_{m \text{ a maximal ideal}} m$$

since left and right maximal ideals coincide in  $R$ . Properties of the Jacobson radical include:

- $J(R/J(R)) = 0$ .

**Lemma 1.3.1** Let  $R$  be a commutative ring. Then  $x \in J(R)$  if and only if  $1 - xy \in R^\times$  for all  $y \in R$ .

**Proof** Suppose that  $x \notin J(R)$ . Then  $x \notin m$  for some maximal ideal  $m$ . Then  $R = m + (x)$  since  $m$  is maximal. Then there exists  $p \in m$  and  $y \in R$  such that  $1 = p + xy$ . Then  $1 - xy = p \in m \notin R^\times$ .

Suppose that  $1 - xy \notin R^\times$  for some  $y \in R$ . Then  $(1 - xy)$  is a proper ideal of  $R$ . Then there exists a maximal ideal  $m$  such that  $(1 - xy) \subseteq m$ . If  $x \in m$  then  $yx \in m$  which implies that  $1 = xy + 1 - xy \in m$ . This is a contradiction and so  $x \notin m$ . Hence  $x \notin J(R)$ . ■

**Lemma 1.3.2** Let  $R$  be a commutative ring. Then  $x \in R$  is a unit if and only if  $[x] \in R/J(R)$  is a unit.

**Proof** Suppose that  $x \in R$  is a unit. Then there exists  $y \in R$  such that  $xy = 1$ . Then  $[x][y] = [1]$  so we are done. Now suppose that  $[x][y] = [1]$  for some  $y \in R$ . Then there exists  $m \in J(R)$  such that  $xy = 1 + m$ . By the above lemma,  $1 + m$  is a unit hence  $x$  is a unit. ■

### 1.4 The Radical of an Ideal

The radical of an ideal is a very different notion from the radical of module.

**Definition 1.4.1 (Radical of an Ideal)** Let  $I$  be an ideal of a ring  $R$ . Define the radical of  $I$  to be

$$\sqrt{I} = \{r \in R \mid r^n \in I \text{ for some } n \in \mathbb{N}\}$$

**Proposition 1.4.2** Let  $R$  be a commutative ring. Let  $I$  be an ideal. Then the following are true.

- $I \subseteq \sqrt{I}$
- $\sqrt{\sqrt{I}} = \sqrt{I}$
- $\sqrt{I^m} = \sqrt{I}$  for all  $m \geq 1$
- $\sqrt{I} = R$  if and only if  $I = R$

**Proof**

- Let  $r \in I$ . Then  $r^1 \in I$ . Thus by choosing  $n = 1$  we shows that  $r^n \in I$ . Thus  $r \in \sqrt{I}$ .
- By the above, we already know that  $\sqrt{I} \subseteq \sqrt{\sqrt{I}}$ . So let  $r \in \sqrt{\sqrt{I}}$ . Then there exists some  $n \in \mathbb{N}$  such that  $r^n \in \sqrt{I}$ . But  $r^n \in \sqrt{I}$  means that there exists some  $m \in \mathbb{N}$  such that  $(r^n)^m \in I$ . But  $nm \in \mathbb{N}$  is a natural number such that  $r^{nm} \in I$ . Hence  $r \in \sqrt{I}$  and so we conclude.
- Since  $I^m \subseteq I$ , we know that  $\sqrt{I^m} \subseteq \sqrt{I}$ . Let  $x \in \sqrt{I}$ . Then  $x^n \in I$  for some  $n \in \mathbb{N}$ . Then we have  $(x^n)^m = x^{n+m} \in I^m$  so that  $x \in \sqrt{I^m}$ .
- Clearly if  $I = R$  then  $I \subseteq \sqrt{I}$  implies that  $\sqrt{I} = R$ . Conversely,  $\sqrt{I} = R$  implies that  $1 \in \sqrt{I}$  and hence  $1 \in I$ . Hence  $I = R$ .

■

**Proposition 1.4.3** Let  $R$  be a commutative ring. Let  $I, J$  be ideals of  $R$ . Then the following are true.

- If  $I \subseteq J$  then  $\sqrt{I} \subseteq \sqrt{J}$
- $\sqrt{IJ} = \sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$
- $\sqrt{I+J} = \sqrt{\sqrt{I} + \sqrt{J}}$

**Proof**

- Let  $x \in \sqrt{I}$ . Then  $x^n \in I$  for some  $n \in \mathbb{N}$ . Then  $x^n \in J$  so  $x \in \sqrt{J}$ .
- Since  $IJ \subseteq I \cap J \subseteq I, J$ , we already have  $\sqrt{IJ} \subseteq \sqrt{I \cap J} \subseteq \sqrt{I} \cap \sqrt{J}$ . Let  $x \in \sqrt{I} \cap \sqrt{J}$ . Then there exists  $n, m \in \mathbb{N}$  such that  $x^n \in I$  and  $x^m \in J$ . Then  $x^n \cdot x^m = x^{n+m} \in IJ$  implies that  $x \in \sqrt{IJ}$ .
- Since  $I, J \subseteq I+J$ , we have  $\sqrt{I} + \sqrt{J} \subseteq \sqrt{I+J}$  so that  $\sqrt{\sqrt{I} + \sqrt{J}} \subseteq \sqrt{I+J}$ . On the other hand,  $I \subseteq \sqrt{I}$  and  $J \subseteq \sqrt{J}$  implies that  $I+J \subseteq \sqrt{I} + \sqrt{J}$ . Then  $\sqrt{I+J} \subseteq \sqrt{\sqrt{I} + \sqrt{J}}$  and so we are done.

■

**Lemma 1.4.4** Let  $R$  be a commutative ring. Then we have

$$N(R) = \sqrt{(0)}$$

**Proof** True from definitions.

■

**Lemma 1.4.5** Let  $R$  be a commutative ring. Let  $I$  be an ideal of  $R$ . Let  $\pi : R \rightarrow R/I$  be the quotient homomorphism. Then we have

$$\sqrt{I} = \pi^{-1} \left( N \left( \frac{R}{I} \right) \right)$$

**Proof** Let  $x \in R$ . Then we have that  $x^n \in I$  if and only if  $\pi(x^n) = x^n + I = I$  if and only if  $x + I \in N(R/I)$ .

■

**Proposition 1.4.6** Let  $R$  be a commutative ring. Let  $I$  be an ideal. Then

$$\sqrt{I} = \bigcap_{\substack{p \text{ a prime ideal} \\ I \subseteq p \subseteq R}} p$$



**Proof** Write  $\pi : R \rightarrow R/I$  the quotient homomorphism. Using prp1.2.3 and the correspondence theorem, we have that

$$\sqrt{I} = \pi^{-1} \left( \bigcap_{\substack{P \text{ is a prime} \\ \text{ideal of } R}} P \right) = \bigcap_{\substack{P \text{ is a prime} \\ \text{ideal of } R}} \pi^{-1}(P) = \bigcap_{\substack{p \text{ a prime ideal} \\ I \subseteq p \subseteq R}} p$$

■

**Definition 1.4.7 (Radical Ideals)** Let  $R$  be a commutative ring. Let  $I$  be an ideal of  $R$ . We say that  $I$  is radical if

$$\sqrt{I} = I$$

In particular, by the above lemma it follows that the radical of an ideal is a radical ideal.

**Lemma 1.4.8** Let  $R$  be a ring. Let  $P$  be a prime ideal of  $R$ . Then  $P$  is radical.

**Proof** We already know that  $P \subseteq \sqrt{P}$ . Let  $x \in \sqrt{P}$ . Then  $x^n \in P$  for some  $n \in \mathbb{N}$ . Since  $P$  is prime, by inducting downwards we deduce that  $x \in P$ . Thus  $P$  is radical. ■

We conclude that there is an inclusion of types of ideal in which each inclusion is strict:

$$\text{Maximal ideals} \subset \text{Prime ideals} \subset \text{Radical ideals}$$

**Proposition 1.4.9** Let  $R$  be a commutative ring. Let  $I$  be an ideal of  $R$ . Then  $R/I$  is reduced if and only if  $I$  is a radical ideal.

So radical, prime and maximal ideals all have characterizations using the quotient ring:

- $I$  is maximal if and only if  $R/I$  is a field.
- $I$  is prime if and only if  $R/I$  is an integral domain.
- $I$  is radical if and only if  $R/I$  is reduced.

## 1.5 The Correspondence between Ideals and the Quotient

**Definition 1.5.1 (Max Spectrum of a Ring)** Let  $A$  be a commutative ring. Define the max spectrum of  $A$  to be

$$\text{maxSpec}(A) = \{m \subseteq A \mid m \text{ is a maximal ideal of } A\}$$

**Definition 1.5.2 (Spectrum of a Ring)** Let  $A$  be a commutative ring. Define the spectrum of  $A$  to be

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

**Example 1.5.3** Consider the following commutative rings.

- $\text{Spec}(\mathbb{Z}/6\mathbb{Z}) = \{(2 + 6\mathbb{Z}), (3 + 6\mathbb{Z})\}$
- $\text{Spec}(\mathbb{Z}/8\mathbb{Z}) = \{(2 + 8\mathbb{Z})\}$
- $\text{Spec}(\mathbb{Z}/24\mathbb{Z}) = \{(2 + 24\mathbb{Z}), (3 + 24\mathbb{Z})\}$
- $\text{Spec}(\mathbb{R}[x]) = \{(f) \mid f \text{ is irreducible}\}$

**Proof**

- The only ideals of  $\mathbb{Z}/6\mathbb{Z}$  are  $(2 + 6\mathbb{Z})$  and  $(3 + 6\mathbb{Z})$ . We need to find which ones are prime ideals. Now  $\mathbb{Z}/6\mathbb{Z} \setminus (2 + 6\mathbb{Z})$  consists of  $1 + 6\mathbb{Z}$ ,  $3 + 6\mathbb{Z}$  and  $5 + 6\mathbb{Z}$ . No multiplication of these elements give an element of  $(2 + 6\mathbb{Z})$ . So any two elements in  $\mathbb{Z}/6\mathbb{Z}$  which multiply to an

element of  $(2 + 6\mathbb{Z})$  must contain one element that lie in  $(2 + 6\mathbb{Z})$ . Hence  $(2 + 6\mathbb{Z})$  is prime. This is similar for  $(3 + 6\mathbb{Z})$ . Hence  $\text{Spec}(\mathbb{Z}/6\mathbb{Z}) = \{(2 + 6\mathbb{Z}), (3 + 6\mathbb{Z})\}$ .

- The only ideals of  $\mathbb{Z}/8\mathbb{Z}$  are  $(2 + 8\mathbb{Z})$  and  $(4 + 8\mathbb{Z})$ . A similar argument as above shows that  $(2 + 8\mathbb{Z})$  is a prime ideal. However,  $6 + 8\mathbb{Z} \notin (4 + 8\mathbb{Z})$  while  $(6 + 8\mathbb{Z})^2 = 4 + 8\mathbb{Z} \in (4 + 8\mathbb{Z})$  which shows that  $(4 + 8\mathbb{Z})$  is not a prime ideal.
- A similar proof as above ensues.
- Recall that  $\mathbb{R}[x]$  is a principal ideal domain. Let  $I = (f)$  be a prime ideal of  $\mathbb{R}[x]$ . Then  $f$  is irreducible. Thus every prime ideal of  $\mathbb{R}[x]$  is of the form  $(f)$  for  $f$  an irreducible polynomial.

■

**Lemma 1.5.4** Let  $R, S$  be commutative rings. Let  $f_1 : R \times S \rightarrow R$  and  $f_2 : R \times S \rightarrow S$  denote the projection maps. Then the map

$$f_1^* \amalg f_2^* : \text{Spec}(R) \amalg \text{Spec}(S) \rightarrow \text{Spec}(R \times S)$$

is a bijection.

**Proof** The core of the proof is the fact that  $P$  is a prime ideal of  $R \times S$  if and only if  $P = R \times Q$  or  $P = V \times S$  for either a prime ideal  $Q$  of  $R$  or a prime ideal  $V$  of  $S$ . It is clear that if  $Q$  is a prime ideal of  $S$  and  $V$  is a prime ideal of  $R$ , then  $R \times Q$  and  $V \times S$  are both prime ideals of  $R \times S$ .

So suppose that  $P$  is a prime ideal in  $R \times S$ . Let  $e_1 = (1, 0)$  and  $e_2 = (0, 1)$ . Since  $P \neq R \times S$ , at least one of  $e_1$  or  $e_2$  is not in  $P$ . Without loss of generality assume that  $e_1 \notin P$ . But  $e_1 e_2 = 0 \in P$  and  $P$  being prime implies that  $e_2 \in P$ . Since  $e_2$  is the identity of  $\{0\} \times S \cong S$ , we conclude that  $\{0\} \times S \subseteq P$ . By the correspondence theorem, the projection map  $f_1 : R \times S \rightarrow R$  gives a bijection between prime ideals of  $R \times S$  that contain  $\{0\} \times S$  and prime ideals of  $R$ . So  $f_1(P)$  is a prime ideal of  $R$ . Thus  $P = f_1(P) \times S$  which is exactly what we wanted.

Now the bijection is clear.  $f_1^* \amalg f_2^*$  sends a prime ideal  $P$  of  $R$  to  $P \times S$  and it sends a prime ideal  $Q$  of  $S$  to  $R \times Q$ . This map is surjective by the above argument. It is injective by inspection. ■

**Theorem 1.5.5** Let  $R$  be a commutative ring. Let  $I$  be an ideal of  $R$ . Denote  $\varphi$  to be the inclusion preserving one-to-one bijection

$$\{\text{Ideals of } R \text{ containing } I\} \xrightarrow{1:1} \{\text{Ideals of } R/I\}$$

from the correspondence theorem for rings. In other words,  $\varphi(A) = A/I$ . Let  $J \subseteq R$  be an ideal containing  $I$ . Then the following are true.

- $J$  is a radical ideal if and only if  $\varphi(J) = J/I$  is a radical ideal.
- $J$  is a prime ideal if and only if  $\varphi(J) = J/I$  is a prime ideal.
- $J$  is a maximal ideal if and only if  $\varphi(J) = J/I$  is a maximal ideal.

**Proof**

- Let  $J$  be a radical ideal. Suppose that  $r + I \in \sqrt{J/I}$ . This means that  $(r + I)^n = r^n + I \in J/I$  for some  $n \in \mathbb{N}$ . But this means that  $r^n \in J$ . This implies that  $r \in \sqrt{J} = J$ . Thus  $r + I \in J/I$  and we conclude that  $\sqrt{J/I} \subseteq J/I$ . Since we also have  $J/I \subseteq \sqrt{J/I}$ , we conclude.

Now suppose that  $J/I$  is a radical ideal. Let  $r \in \sqrt{J}$ . This means that  $r^n \in J$  for some  $n \in \mathbb{N}$ . Now  $r^n + I = (r + I)^n \in J/I$  implies that  $r + I \in \sqrt{J/I} = J/I$ . Hence  $r \in J$  and so  $\sqrt{J} \subseteq J$ . Since we also have that  $J \subseteq \sqrt{J}$ , we conclude.

- Let  $J$  be a prime ideal. Then  $R/J$  is an integral domain. By the second isomorphism theorem, we have that  $R/J \cong (R/I)/(J/I)$  and hence  $(R/I)/(J/I)$  is also an integral domain. Hence  $J/I$  is a prime ideal. The converse is also true.
- Let  $J$  be a maximal ideal. Then  $R/J$  is a field. By the second isomorphism theorem, we have that  $R/J \cong (R/I)/(J/I)$  and hence  $(R/I)/(J/I)$  is also a field. Hence  $J/I$  is a maximal ideal. The converse is also true.

Another way to write the bijections is via spectra:

$$\text{Spec}(R/I) \xleftarrow{1:1} \{P \in \text{Spec}(R) \mid I \subseteq P\}$$

and

$$\text{maxSpec}(R/I) \xleftarrow{1:1} \{m \in \text{maxSpec}(R) \mid I \subseteq m\}$$

## 1.6 Extensions and Contractions of Ideals

**Definition 1.6.1 (Extension of Ideals)** Let  $R, S$  be commutative rings. Let  $f : R \rightarrow S$  be a ring homomorphism. Let  $I$  be an ideal of  $R$ . Define the extension  $I^e$  of  $I$  to  $S$  to be the ideal

$$I^e = \langle f(i) \mid i \in I \rangle$$

**Proposition 1.6.2** Let  $R, S$  be commutative rings. Let  $f : R \rightarrow S$  be a ring homomorphism. Let  $I, I_1, I_2$  be an ideal of  $R$ . Then the following are true regarding the extension of ideals.

- If  $I_1 \subseteq I_2$ , then  $I_1^e \subseteq I_2^e$ .
- Closed under sum:  $(I_1 + I_2)^e = I_1^e + I_2^e$
- $(I_1 \cap I_2)^e \subseteq I_1^e \cap I_2^e$
- Closed under products:  $(I_1 I_2)^e = I_1^e I_2^e$
- $(\sqrt{I})^e \subseteq \sqrt{I^e}$

**Proof**

- Let  $x \in I_1^e$ . Then  $x = \sum s_k f(i_k)$  for some  $i_k \in I_1$ . Then  $i_k \in I_2$  implies that  $x \in I_2^e$ .
- Since  $I_1, I_2 \subseteq I_1 + I_2$ , we have  $I_1^e + I_2^e \subseteq (I_1 + I_2)^e$ . Conversely, let  $x \in (I_1 + I_2)^e$ . Then  $x = \sum s_k f(i_k)$  for  $i_k \in I_1 + I_2$ . Then we have

$$x = \sum_{i_k \in I_1} s_k f(i_k) + \sum_{i_k \in I_2} s_k f(i_k) \in I_1^e + I_2^e$$

so we conclude.

- Since  $I_1 \cap I_2 \subseteq I_1, I_2$  we are done.
- It suffices to check the generators lie in each other. Let  $x \in I_1 I_2$ . Then  $x = \sum i_k j_k$  for some  $i_k \in I_1$  and  $j_k \in I_2$ . Then  $f(x) = \sum f(i_k) f(j_k)$ . Since  $f(i_k) \in I_1^e$  and  $f(j_k) \in I_2^e$ , then  $f(x) \in I_1^e I_2^e$  so we conclude that  $(I_1 I_2)^e \subseteq I_1^e I_2^e$ . Conversely, suppose that  $x \in I_1^e I_2^e$ . Then  $x = \sum f(i_k) f(j_k)$  for  $i_k \in I_1$  and  $j_k \in I_2$ . Since  $f$  is a ring homomorphism, we have that

$$x = \sum f(i_k) f(j_k) = f\left(\sum i_k j_k\right)$$

Since  $\sum i_k j_k \in I_1 I_2$ , we conclude that  $x \in I_1^e I_2^e$ .

- We have that

$$(\sqrt{I})^e = \left( f(i) \mid i \in \bigcap_{\substack{P \text{ prime} \\ I \subseteq P}} P \right) \subseteq f\left( \bigcap_{\substack{P \text{ prime} \\ I \subseteq P}} f(P) \right) \subseteq f\left( \bigcap_{\substack{Q \text{ prime} \\ I^e \subseteq Q}} f(f^{-1}(Q)) \right)$$

The last inclusion follows since for  $I^e \subseteq Q$ , we must have that  $I \subseteq f^{-1}(Q)$ . Then we have that

$$(\sqrt{I})^e = f \left( \bigcap_{\substack{Q \text{ prime} \\ I^e \subseteq Q}} Q \right) = \sqrt{I^e}$$

and so we are done. ■

**Definition 1.6.3 (Contraction of Ideals)** Let  $R, S$  be commutative rings. Let  $f : R \rightarrow S$  be a ring homomorphism. Let  $J$  be an ideal of  $S$ . Define the contraction  $J^c$  of  $J$  to  $R$  to be the ideal

$$J^c = f^{-1}(J)$$

**Proposition 1.6.4** Let  $R, S$  be commutative rings. Let  $f : R \rightarrow S$  be a ring homomorphism. Let  $J, J_1, J_2$  be an ideal of  $S$ . Then the following are true regarding the extension of ideals.

- If  $J_1 \subseteq J_2$ , then  $J_1^c \subseteq J_2^c$ .
- $(J_1 + J_2)^c \supseteq J_1^c + J_2^c$
- Closed under intersections:  $(J_1 \cap J_2)^c = J_1^c \cap J_2^c$
- $(J_1 J_2)^c \supseteq J_1^c J_2^c$
- Closed under taking radicals:  $\text{rad}(J)^c = \text{rad}(J^c)$

**Proof**

- Clear since  $f^{-1}(J_1) \subseteq f^{-1}(J_2)$  for  $J_1 \subseteq J_2$ .
  - Since  $J_1, J_2 \subseteq J_1 + J_2$ , we have that  $J_1^c + J_2^c \subseteq (J_1 + J_2)^c$ .
  - Since  $J_1 \cap J_2 \subseteq J_1, J_2$ , we have that  $(J_1 \cap J_2)^c \subseteq J_1^c \cap J_2^c$ . Let  $x \in J_1^c \cap J_2^c$ . Then we have  $f(x) \in J_1, J_2$  so that  $f(x) \in J_1 \cap J_2$ . Hence  $x \in (J_1 \cap J_2)^c$ .
  - Suppose that  $x \in J_1^c$  and  $y \in J_2^c$ . Then  $f(xy) = f(x)f(y) \in J_1^c J_2^c$ . Hence  $xy \in J_1^c J_2^c$ .
  -
- 

**Proposition 1.6.5** Let  $R, S$  be commutative rings. Let  $f : R \rightarrow S$  be a ring homomorphism. Let  $I$  be an ideal of  $R$  and let  $J$  be an ideal of  $S$ . Then the following are true.

- $I \subseteq I^{ec}$
- $J^{ce} \subseteq J$
- $I^e = I^{ece}$
- $J^c = J^{cec}$

**Proof**

- Let  $x \in I$ . Then  $f(x) \in I^e$ . Thus  $x \in f^{-1}(I^e)$ .
  - Since  $J^{ce}$  is generated by  $f(x)$  for all  $x \in J^c$ , it suffices to check that  $f(x) \in J$  for all  $x \in J^c$ . But  $x \in J^c$  implies that  $f(x) \in J$  so we are done.
  - Since  $I \subseteq I^{ec}$ , we know that  $I^e \subseteq I^{ece}$ . Also, from the second item we take  $J = I^e$  to get  $I^{ece} \subseteq I^e$ .
  - From the first item, take  $I = J^c$  to get  $J^c \subseteq J^{cec}$ . Also, since  $J^{ce} \subseteq J$ , we have that  $J^{cec} \subseteq J^c$ .
-

**Example 1.6.6** Let  $S$  be a commutative ring and let  $R \subseteq S$  be a subring. Let  $f : R \rightarrow S$  be the inclusion map. Let  $I \subseteq R$  be an ideal of  $R$  and let  $J \subseteq S$  be an ideal of  $S$ . Then the following are true.

- $I^e = S \cdot I$ .
- $J^e = J \cap R$ .

## 1.7 Minimal Prime Ideals

**Definition 1.7.1 (Minimal Prime Ideals)** Let  $R$  be a commutative ring. Let  $I$  be an ideal of  $R$ . Let  $P$  be a prime ideal of  $R$ . We say that  $P$  is a minimal prime ideal over  $I$  if for any other prime ideal  $Q \supseteq I$  containing  $I$ , we have  $P \subseteq Q$ .

**Proposition 1.7.2** Let  $R$  be a commutative ring. Let  $I$  be an ideal of  $R$ . Then a minimal prime ideal over  $I$  exists.

## 2 Basic Notions of Commutative Rings

### 2.1 Noetherian Commutative Rings

We recall some facts about Noetherian rings. In the following, let  $R$  be a commutative ring, although they are also true if  $R$  is non-commutative if we take all modules defined below to be left (right)  $R$ -modules.

- If we have a short exact sequence of  $R$ -modules:

$$0 \longrightarrow M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3 \longrightarrow 0$$

Then  $M_2$  is Noetherian if and only if  $M_1$  and  $M_3$  are Noetherian.

- If  $M$  and  $N$  are  $R$ -modules, then  $M \oplus N$  is Noetherian if and only if  $M$  and  $N$  are Noetherian.
- If  $M$  is an  $R$ -module and  $N$  is an  $R$ -submodule of  $M$ , then  $M$  is Noetherian if and only if  $N$  and  $M/N$  are Noetherian.
- If  $R$  is Noetherian and  $I$  is an ideal of  $R$ , then  $R/I$  is Noetherian.
- Later when once has seen localization, we can also prove that: If  $R$  is Noetherian then  $S^{-1}R$  is Noetherian for any multiplicative subset  $S$  of  $R$ .

**Proposition 2.1.1** Let  $R$  be a Noetherian commutative ring. Let  $I$  be an ideal of  $R$ . Then there exists  $n \in \mathbb{N}$  such that

$$\sqrt{I}^n \subseteq I \subseteq \sqrt{I}$$

**Proof** It is clear that  $I \subseteq \sqrt{I}$ . Since  $R$  is Noetherian,  $\sqrt{I}$  is finitely generated by say  $x_1, \dots, x_n$ . Then  $x_i^{n_i} \in I$  for some  $n_i \in \mathbb{N}$ . Let  $m = 1 + \sum_{i=1}^n (n_i - 1)$ . Then  $\sqrt{I}^m$  is generated by  $x_1^{r_1} \cdots x_n^{r_n}$  for  $\sum_{i=1}^n r_i = m$ . If  $r_i < n_i$  for  $i$  then

$$m = \sum_{i=1}^n r_i \leq \sum_{i=1}^n (n_i - 1) < m$$

is a contradiction. Hence there exists some  $i$  for which  $r_i \geq n_i$ . Thus  $x_1^{r_1} \cdots x_n^{r_n} \in I$ . Thus  $\sqrt{I}^m \subseteq I$ . ■

**Proposition 2.1.2** Let  $R$  be a Noetherian commutative ring. Then  $N(R)$  is a nilpotent ideal.

**Proof** By the above, there exists  $n \in \mathbb{N}$  such that  $(N(R))^n = \sqrt{(0)}^n \subseteq (0) \subseteq \sqrt{(0)}$ . Hence  $(N(R))^n = (0)$  for some  $n \in \mathbb{N}$ . ■

#### Proposition 2.1.3

Let  $R$  be a Noetherian commutative ring. Let  $I$  be an ideal of  $R$ . Then  $I$  has only finitely many minimal prime ideals.

**Proof**

Define the set

$$\mathcal{F} = \{I \subseteq R \mid I \text{ is an ideal of } R \text{ that has infinitely many minimal prime ideals}\}$$

Assume for a contradiction that the set is non-empty. Since  $R$  is Noetherian, every chain in  $\mathcal{F}$  has a maximal element. Let  $I$  be such a maximal element of the set.  $I$  is not a prime ideal because prime ideals only have one minimal prime ideal by definition. This means that there exists  $a, b \notin I$  such that  $ab \in I$ . Now  $I + (a)$  and  $I + (b)$  both contain  $I$ , and since  $ab \in I$  we have that  $(I + (a))(I + (b)) \subseteq I$ . For any minimal prime ideal  $P$  of  $I$ , we have that  $(I + (a))(I + (b)) \subseteq I \subseteq P$  implies that  $(I + (a)) \subseteq P$  or  $(I + (b)) \subseteq P$ . This shows that the set of minimal prime ideals of  $I$  is a subset of the union of the set of minimal prime ideals of  $I + (a)$  and  $I + (b)$ , and so without loss of generality,  $I + (a)$  has infinitely many minimal prime ideals. But then  $I + (a)$  strictly contains  $I$  and  $I + (a) \in \mathcal{F}$ . This is a contradiction since  $I$  is assumed to be maximal. ■

## 2.2 Artinian Commutative Rings

Let  $R$  be a commutative ring. Recall that  $R$  is Artinian if any descending chain of ideals

$$I_1 \supseteq I_2 \supseteq \cdots$$

terminates at finitely many steps, meaning  $I_k = I_{k+n}$  for some  $k \in \mathbb{N}$ .

Generally, if  $R$  is Artinian then the following are true.

- $J(R)$  is a nilpotent ideal.
- $R$  is Noetherian.
- $R$  has finite length.

There are also properties of Artinian rings that only commutative rings can realize.

**Proposition 2.2.1** Let  $R$  be an integral domain. Then  $R$  is Artinian if and only if  $R$  is a field.

**Proof** It is clear that every field is Artinian. Conversely, let  $R$  be Artinian. Consider the following descending chain of ideals in  $R$ :

$$R \supseteq (x) \supseteq (x^2) \supseteq$$

for any  $0 \neq x \in R$ . Since  $R$  is Artinian, the chain terminates and  $(x^n) = (x^{n+1})$  for some  $n \in \mathbb{N}$ . Then there exists  $y \in R$  such that  $x^n = yx^{n+1}$ . This means that  $x^n(1 - yx) = 0$ . Since  $R$  is an integral domain,  $R$  has no nilpotents. Hence  $x^n$  is non-zero and  $1 = xy$ . Thus  $x$  has an inverse so that  $R$  is a field. ■

**Proposition 2.2.2** Let  $R$  be an Artinian commutative ring. Then the following are true.

- $\text{Spec}(R) = \text{maxSpec}(R)$ .
- $N(R) = J(R)$

**Proof** Let  $P$  be a prime ideal. Since quotients of Artinian rings are Artinian,  $R/P$  is Artinian. Since  $R/P$  is also an integral domain, we conclude by the above that  $R/P$  is a field. Hence  $P$  is maximal.

Since every prime ideal in  $R$  is maximal, we have that

$$N(R) = \bigcap_{P \text{ a prime ideal}} P = \bigcap_{P \text{ a maximal ideal}} P = J(R)$$

and so we conclude. ■

**Proposition 2.2.3** Let  $R$  be a commutative ring. If  $R$  is Artinian, then  $R$  has finitely many maximal ideals.

**Proof** Consider the collection

$$\{m_1 \cap \cdots \cap m_k \mid m_1, \dots, m_k \text{ are maximal ideals of } R\}$$

of  $R$ -submodules of  $R$ . Since  $R$  is Artinian, every collection of  $R$ -submodules of  $R$  has a minimal element. Hence this collection also has a minimal element, say  $m_1 \cap \cdots \cap m_k$ . Let  $m$  be another maximal ideal of  $R$ . Then

$$m \cap m_1 \cap \cdots \cap m_k \subseteq m_1 \cap \cdots \cap m_k$$

Since  $m_1 \cap \cdots \cap m_k$  is minimal, they are equal. By prime avoidance, we conclude that  $m \supseteq m_i$  for some  $i$ . Since they are maximal, we have  $m = m_i$ . Hence  $m_1, \dots, m_k$  gives the full list of distinct maximal ideals of  $R$ . ■

## 2.3 Local Rings

**Definition 2.3.1 (Local Rings)** Let  $R$  be a commutative ring. We say that  $R$  is a local ring if it has a unique maximal ideal  $m$ . In this case, we say that  $R/m$  is the residue field of  $R$ .

**Example 2.3.2** Consider the following commutative rings.

- $\mathbb{Z}/6\mathbb{Z}$  is not a local ring.
- $\mathbb{Z}/8\mathbb{Z}$  is a local ring.
- $\mathbb{Z}/24\mathbb{Z}$  is not a local ring.
- $\mathbb{R}[x]$  is not a local ring.

**Proof**

- The only ideals of  $\mathbb{Z}/6\mathbb{Z}$  are  $(2 + 6\mathbb{Z})$  and  $(3 + 6\mathbb{Z})$ . They do not contain each other and so they are both maximal.
- The only ideals of  $\mathbb{Z}/8\mathbb{Z}$  are  $(2 + 8\mathbb{Z})$  and  $(4 + 8\mathbb{Z})$ . But  $(2 + 8\mathbb{Z}) \supseteq (4 + 8\mathbb{Z})$ . Hence  $\mathbb{Z}/8\mathbb{Z}$  has a unique maximal ideal.
- A similar proof as above ensues.
- Any irreducible polynomial  $f \in \mathbb{R}[x]$  is such that  $(f)$  is a maximal ideal. Indeed the evaluation homomorphism gives an isomorphism  $\frac{\mathbb{R}[x]}{(f)} \cong \mathbb{R}$ .

■

**Proposition 2.3.3** Let  $R$  be a ring and  $I$  an ideal of  $R$ . Then  $I$  is the unique maximal ideal of  $R$  if and only if  $I$  is the set containing all non-units of  $R$ .

**Proof** Let  $I$  be the unique maximal ideal of  $R$ . Clearly  $I$  does not contain any unit else  $I = R$ . Now suppose that  $r$  is a non-unit. Suppose that  $r \notin I$ . Define  $J = \{sr | s \in R\}$ . Clearly  $J$  is an ideal. It must be contained in some maximal ideal. Since  $I$  is the unique maximal ideal,  $J \subseteq I$ . But this means that  $r \in I$ , a contradiction. Thus every non-unit is in  $I$ . Suppose that  $I$  contains all non-units of  $R$ . Let  $r \notin I$ . Then there exists  $s \notin I$  such that  $rs = 1$ . Then  $(r + I)(s + I) = 1 + I$  in  $R/I$ . This means that every element of  $R/I$  has a multiplicative inverse which means that  $R/I$  is a field and thus  $I$  is a maximal ideal. Now let  $J \neq I$  be another maximal ideal. Then  $J$  contains some unit  $r$ . This implies that  $J = R$  and thus  $I$  is the unique maximal ideal.

■

**Example 2.3.4** Let  $k$  be a field. Then the ring of power series  $k[[x]]$  is a local ring.

**Proof** Let  $M$  be the set of all non-units of  $k[[x]]$ . I first show that  $f \in M$  if and only if the constant term of  $f$  is non-zero. Let  $g$  be a power series. Then the  $n$ th coefficient of  $f \cdot g$  is given by

$$c_n = \sum_{k=0}^n a_k b_{n-k}$$

If the constant term of  $f$  is 0, then  $c_0 = 0$  and so  $f \cdot g \neq 1$ . Now if the constant term of  $f$  is  $a_0 \neq 0$ , then set  $b_0 = \frac{1}{a_0}$ . Now we can use the formula  $0 = c_n$  to deduce

$$b_n = -\frac{\sum_{k=1}^n a_k b_{n-k}}{a_0}$$

This is such that  $a_n \cdot b_n = 0$ . Define  $g = \sum_{k=0}^{\infty} b_k x^k$ . Then  $f \cdot g = 1$ . Thus  $f$  is a unit.

By the above proposition, we conclude that  $M$  is the unique maximal ideal of  $k[[x]]$ .

■



**Proposition 2.3.5** Let  $R$  be a commutative ring. Then the following are equivalent.

- $R$  has exactly one prime ideal. (It is given by  $N(R)$ ).
- Every element of  $R$  is either a unit or nilpotent.
- $N(R)$  is a maximal ideal.

Under these equivalent assumptions,  $(R, N(R))$  is a local ring.

**Proof**

- (1)  $\implies$  (2): We know that  $N(R)$  is a prime ideal, hence it is the unique prime ideal and unique maximal ideal. Thus  $R$  is a local ring. By the above, elements of  $R \setminus N(R)$  are units and element of  $N(R)$  are nilpotent.
- (2)  $\implies$  (3): It is clear that every nilpotent is a non-unit. By assumption, non-units of  $R$  are nilpotents. Hence  $N(R)$  is the set of all non-units. Since  $N(R)$  is an ideal, by the above we conclude that  $(R, N(R))$  is a local ring. In particular,  $N(R)$  is the unique maximal ideal of  $R$ .
- (3)  $\implies$  (1): Suppose that  $N(R)$  is a maximal ideal. Let  $P \neq R$  be a prime ideal of  $R$ . Since  $N(R)$  is the intersection of all prime ideals, we have  $N(R) \subseteq P$ . By the correspondence theorem,  $P$  corresponds to a prime ideal of  $R/N(R)$ . But  $R/N(R)$  is a field, and since  $P \neq R$  we must have that  $P = N(R)$ . Thus  $N(R)$  is the unique prime ideal of  $R$ .

■

**Proposition 2.3.6** Let  $R$  be a Noetherian commutative ring. Then the following are equivalent.

- $R$  is an Artinian local ring.
- $R$  has a nilpotent maximal ideal.
- $R$  has a unique proper radical ideal.
- $R$  has a unique prime ideal.
- $N(R)$  is a maximal ideal of  $R$ .

**Proof**

- (1)  $\implies$  (2): Let  $R$  be Artinian and local. By 2.1.4 we have  $N(R) = J(R) = m$  since  $J(R)$  is the intersection of all maximal ideals. Since  $R$  is Noetherian, by 2.1.3  $N(R) = m$  is nilpotent.

■

Since every Artinian ring is Noetherian, the above proposition implies the following.

**Corollary 2.3.7** Let  $R$  be an Artinian commutative ring. Then the following are true.

- $R$  is local.
- $N(R)$  is the unique maximal ideal of  $R$ .
- $N(R)$  is the unique prime ideal of  $R$ .
- $N(R)$  is the unique radical ideal of  $R$ .
- $N(R)$  is a nilpotent ideal.

We will discuss more of local rings in the topic of localizations.

## 2.4 Revisiting the Polynomial Ring

**Lemma 2.4.1** Let  $R$  be a commutative ring. Then  $R[x]$  has infinitely many irreducible polynomials.

**Proof** If not, then there exists a finite list of irreducible polynomials  $f_1, \dots, f_k$ . Then  $1 + f_1, \dots, f_k$  is not divisible by  $f_1, \dots, f_k$  and so must contain a monic irreducible factor not equal to  $f_1, \dots, f_k$ . This is a contradiction. ■

**Proposition 2.4.2** Let  $R$  be a commutative ring. Then we have

$$N(R[x]) = N(R)[x]$$

**Proof** Let  $f = \sum_{k=0}^n a_k x^k \in N(R)[x]$ . Then each  $a_k$  is nilpotent in  $R$ , and there exists  $n_k \in \mathbb{N}$  such that  $a_k^{n_k} = 0$ . This also proves that  $a_k x^k$  is nilpotent. Since the sum of nilpotents is a nilpotent, we conclude that  $f$  is nilpotent.

Now suppose that  $f \in N(R[x])$ . We induct on the degree of  $f$ . Let  $\deg(f) = 0$ . Then  $f$  is nilpotent and  $f$  lies in  $R$ . Thus  $f \in N(R)[x]$ . Now suppose that the claim is true for  $\deg(f) \leq n - 1$ . Let  $\deg(g) = n$  with leading coefficient  $b_n$ . Since  $g$  is nilpotent in  $R[x]$ , there exists  $m \in \mathbb{N}$  such that  $g^m = 0$ . Then in particular,  $b_n^m = 0$  so that  $b_n$  is nilpotent. Then  $b_n x^n$  is also nilpotent. Now since  $N(R[x])$  is an ideal of  $R[x]$ , we have that  $g - b_n x^n \in N(R[x])$ . By inductive hypothesis,  $g - b_n x^n \in N(R)[x]$ . Since  $N(R)$  is an ideal of  $R$ , we have that  $N(R)[x]$  is an ideal of  $R[x]$ . So  $g = (g - b_n x^n) + b_n x^n \in N(R)[x]$ . Thus we are done. ■

**Theorem 2.4.3 (Hilbert's Basis Theorem)** Let  $R$  be a commutative ring. If  $R$  is Noetherian, then  $R[x]$  is a Noetherian ring.

**Proof** It suffices to show that every ideal of  $R[x]$  is finitely generated. Let  $I$  be an ideal of  $R[x]$ . Let  $I^{\leq n}$  be the ideal generated by

$$I^{\leq n} = \{f \in I \mid \deg(f) \leq n\}$$

Notice that  $I^{\leq n}$  is an  $R$ -submodule of  $\bigoplus_{i=0}^n R \cdot x^i$ . Since  $R$  is Noetherian,  $I^{\leq n}$  is finitely generated as an  $R$ -module. In particular,  $I^{\leq n}$  is finitely generated as an  $R[x]$ -module with the same finite generating set.

I claim that the chain of ideals

$$I^{\leq 0} \subseteq I^{\leq 1} \subseteq \dots \subseteq I^{\leq k} \subseteq I = \bigcup_{i=0}^{\infty} I^{\leq i}$$

of  $R[x]$  eventually stabilizes. Let  $LC(f)$  be the leading coefficient of  $f \in R[x]$ . The define

$$LC(I) = \{LC(f) \mid f \in I\}$$

Notice that  $LC(I)$  is an ideal of  $R$ . Since  $R$  is Noetherian,  $LC(I)$  is finitely generated as an  $R$ -module by say  $a_1, \dots, a_r$ . This means that there exists  $f_1, \dots, f_r \in R[x]$  such that  $LC(f_i) = a_i$ . Let  $d = \max\{\deg(f_1), \dots, \deg(f_r)\}$ . Without loss of assumption we can replace  $f_i$  with  $x^{d-\deg(f_i)} f_i$  so that  $f_1, \dots, f_r$  have the same degree  $d$ .

I claim that  $I^{\leq n} = I^{\leq n+1}$  for  $n \geq d$ .  $I^{\leq n} \subseteq I^{\leq n+1}$  is trivial. Suppose that  $f \in I^{\leq n+1}$ . If  $\deg(f) \leq n$  then we are done. So suppose that  $\deg(f) = n + 1$ . Then the leading coefficient of  $f$  is a linear combination of the leading coefficients of  $f_1, \dots, f_r$ . So there exists  $b_1, \dots, b_r \in R$  such that  $LC(f) = \sum_{i=1}^r b_i LC(f_i)$ . Then  $f - (\sum_{i=1}^r b_i f_i) x^{n+1-d} \in I^{\leq n}$ . Since  $\sum_{i=1}^r b_i f_i \in I^{\leq d} \subseteq I^{\leq n}$ , we conclude that  $f \in I^{\leq n}$ . We conclude. ■

Some more important results from Groups and Rings and Rings and Modules include:

- If  $R$  is an integral domain, then  $R[x]$  is an integral domain.
- $R$  is a UFD if and only if  $R[x]$  is a UFD
- If  $F$  is a field, then  $F[x]$  is an Euclidean domain, a PID and a UFD
- If  $F$  is a field, then the ideal generated by  $p$  is maximal if and only if  $p$  is irreducible.

Regarding ideals of the polynomial ring, the following may be useful:

- $I[x]$  is an ideal of  $R$
- There is an isomorphism  $\frac{R[x]}{I[x]} \cong \frac{R}{I}[x]$  given by the map

$$\left( f = \sum_{k=0}^n a_k x^k + I[x] \right) \mapsto \left( \sum_{k=0}^n (a_k + I) x^k \right)$$

- If  $I$  is a prime ideal of  $R$ , then  $I[x]$  is a prime ideal of  $R[x]$ .

### 3 Modules over a Commutative Ring

Recall from Rings and Modules that a module consists of an abelian group  $M$  and a ring  $R$  such that there is a binary operation  $\cdot : R \times M \rightarrow M$  that mimic the notion of a group action:

- For  $r, s \in R$ ,  $s \cdot (r \cdot m) = (sr) \cdot m$  for all  $m \in M$ .
- For  $1_R \in R$  the multiplicative identity,  $1_R \cdot m = m$  for all  $m \in M$ .

When  $R$  is a commutative ring, the first axiom is relaxed so that the resulting element of  $M$  makes no difference whether you apply  $r$  first or  $s$  first. This makes module act even more similarly than fields (although one still need the notion of a basis, which appears in free modules). Therefore the first section concerns transferring techniques in linear algebra such as the Cayley Hamilton theorem to module over a ring that mimic the notion of vector spaces.

#### 3.1 Cayley-Hamilton Theorem

**Definition 3.1.1 (Characteristic Polynomial)** Let  $R$  be a commutative ring. Let  $A \in M_{n \times n}(R)$  be a matrix. Define the characteristic polynomial of  $A$  to be the polynomial

$$c_A(x) = \det(A - xI)$$

**Theorem 3.1.2 (Cayley-Hamilton Theorem for Rings)** Let  $R$  be a commutative ring. Let  $A \in M_{n \times n}(R)$  be a matrix. Then  $c_A(A) = 0$ .

**Theorem 3.1.3 (Cayley-Hamilton Theorem for Modules)** Let  $R$  be a commutative ring. Let  $M$  be a finitely generated  $R$ -module. Let  $I$  be an ideal of  $R$ . Let  $\varphi \in \text{End}_R(M)$ . If  $\varphi(M) \subseteq IM$ , then there exists  $a_1, \dots, a_{n-1} \in I$  such that

$$\varphi^n + a_1\varphi^{n-1} + \dots + a_{n-1}\varphi + \text{id}_M = 0 : M \rightarrow M$$

**Proof** Suppose that  $M$  is generated by  $x_1, \dots, x_n$ . There exists a surjective map  $\rho : R^n \rightarrow M$  given by  $(r_1, \dots, r_n) \mapsto \sum_{k=1}^n r_k x_k$ . Since  $\varphi(M) \subseteq IM$ , we have that

$$\varphi(x_k) = \sum_{i=1}^n r_{ki} x_i$$

for some  $r_{ki} \in I$ . Write  $A$  to be the matrix  $A = (a_{ki})$ . We now have a commutative diagram: In other words, we have the diagram:

$$\begin{array}{ccc} R^n & \xrightarrow{\rho} & M \\ A \downarrow & & \downarrow \varphi \\ R^n & \xrightarrow{\rho} & M \end{array}$$

By Cayley-Hamilton theorem, we have that  $c_A(A) = 0$  is the zero function. For all  $x \in R^n$ , we have that

$$\begin{aligned} c_A(A)(x) &= 0 \\ c_A(Ax) &= 0 \\ \rho(c_A(Ax)) &= \rho(0) \\ c_A(\rho(Ax)) &= 0 && (\rho \text{ is } R\text{-linear}) \\ c_A(\varphi(\rho(x))) &= 0 && (\text{Diagram is commutative}) \end{aligned}$$

Since  $\rho$  is surjective, we conclude that for any  $m \in M$ , the above calculation gives  $c_A(\varphi(m)) = 0$  so that  $c_A(\varphi)$  is the zero map. ■

**Proposition 3.1.4** Let  $R$  be a commutative ring. Let  $M$  be a finitely generated  $R$ -module. Let  $\phi : M \rightarrow M$  be a surjective  $R$ -module homomorphism. Then  $\phi$  is an isomorphism.

**Proof** Consider  $M$  as an  $R[\phi]$ -module via the action  $\phi \cdot m = \phi(m)$ . Notice that  $(\phi)M = M$  since  $\phi$  is surjective. By the Cayley-Hamilton theorem, there exists  $\alpha_1, \dots, \alpha_{n-1} \in R$  such that

$$\text{id}^n + \alpha_1 \phi \text{id}^{n-1} + \dots + \alpha_{n-1} \phi \text{id} + \text{id} = 0 : M \rightarrow M$$

This simplifies to the equation

$$(\alpha_1 + \dots + \alpha_{n-1})\phi(m) + m = 0$$

for all  $m \in M$ .

We want to show that  $\phi$  is injective. Suppose that  $\phi(m) = 0$  for some  $m \in M$ . From the above equation, we see that  $m = 0$ . Hence  $\phi$  is an isomorphism. ■

## 3.2 Nakayama's Lemma

**Lemma 3.2.1 (Nakayama's Lemma I)** Let  $R$  be a commutative ring. Let  $M$  be a finitely generated  $R$ -module. Let  $I$  be an ideal of  $R$ . If  $IM = M$ , then there exists  $r \in R$  such that  $rM = 0$  and  $r - 1 \in I$ .

**Proof** Choose  $\varphi = \text{id}_M$ . Then  $\varphi$  is surjective so that  $M = \varphi(M) \subseteq IM$ . By cor 4.1.3, there exists  $r_1, \dots, r_n \in I$  such that  $(1 + r_1 + \dots + r_n)M = 0$ . By choosing  $r = 1 + r_1 + \dots + r_n$ , we see that  $rM = 0$  and  $r - 1 \in I$  so that we conclude. ■

**Lemma 3.2.2 (Nakayama's Lemma II)** Let  $R$  be a commutative ring. Let  $M$  be a finitely generated  $R$ -module. Let  $I$  be an ideal of  $R$  such that  $I \subseteq J(R)$  and  $IM = M$ . Then  $M = 0$ .

**Proof** By Nakayama's lemma I, there exists  $r \in R$  such that  $rM = 0$  and  $r - 1 \in I \subseteq J(R)$ . By 2.3.8, we have that  $1 - (r - 1)(-1) = r \in R^\times$ . This means that  $r$  is invertible. Hence  $rM = 0$  implies  $M = r^{-1}rM = 0$ . ■

**Corollary 3.2.3** Let  $R$  be a commutative ring. Let  $M$  be a finitely generated  $R$ -module. Let  $I$  be an ideal of  $R$  such that  $I \subseteq J(R)$ . Let  $N$  be an  $R$ -submodule of  $M$ . If

$$M = IM + N$$

then  $M = N$ .

**Proof** Since quotients of finitely generated modules are finitely generated, we know that  $M/N$  is finitely generated. Define the map

$$\phi : IM + N \rightarrow I \frac{M}{N}$$

by  $\phi(im + n) = i(m + N)$ . This map is clearly surjective. Now I claim that  $\ker(\phi) = N$ . For any  $im + n \in \ker(\phi)$ , we see that  $i(m + N) = N$  means that  $im \in N$ . Hence  $im + n \in N$ . On the other hand, if  $im + n \in N$  then  $im \in N$ . But this means that  $im + N = N$ . Hence  $im + n \in \ker(\phi)$ . By the first isomorphism theorem for modules, we conclude that

$$\frac{M}{N} = \frac{IM + N}{N} \cong I \frac{M}{N}$$

We can now apply Nakayama's lemma II to conclude that  $M/N = 0$  so that  $M = N$ . ■

**Corollary 3.2.4** Let  $(R, m)$  be a local ring. Let  $m$  be a maximal ideal of  $R$ . Let  $M$  be a finitely generated  $R$ -module. Then the following are true.

- $M/mM$  is a finite dimensional vector space over  $R/m$ .
- $a_1, \dots, a_n \in M$  generates  $M$  as an  $R$ -module if and only if  $a_1 + mM, \dots, a_n + mM$  generates  $M/mM$  as a  $R/m$  vector space.
- $a_1, \dots, a_n \in M$  is a minimal set of generators of  $M$  as an  $R$ -module if and only if  $a_1 + mM, \dots, a_n + mM$  is a basis for  $M/mM$  as a  $R/m$  vector space.

**Proof** Since the projection map  $\pi : M \rightarrow M/mM$  is surjective, clearly any set of generators of  $M$  is a set of generators for  $M/mM$ . This also shows that if  $M$  is finitely generated then  $M/mM$  is a finite dimensional  $R/m$ -vector space.

For the other direction, suppose that  $a_1 + mM, \dots, a_n + mM$  generates  $M/mM$  as an  $R/m$ -vector space. Define  $N = Ra_1 + \dots + Ra_n \leq M$ . Set  $I = J(R) = m$ . We want to show that  $M = IM + N$ . It is clear that  $IM + N \leq M$ . If  $x \in M$ , then there exists  $r_k \in R$  such that  $x + mM = r_1(a_1 + mM) + \dots + r_n(a_n + mM)$ . In particular, this means that

$$x - \sum_{k=1}^n r_k a_k \in mM$$

Hence  $x \in IM + N$ . We can now apply the above corollary to deduce that  $M = N = Ra_1 + \dots + Ra_n$  so that  $M$  is generated by  $a_1, \dots, a_n$ . And so we are done.

Suppose that  $a_1, \dots, a_n$  generate  $M$ . The above shows that  $a_1 + mM, \dots, a_n + mM$  spans  $M/mM$ . So suppose for a contradiction that  $a_1, \dots, a_n$  is a minimal generating set but  $a_1 + mM, \dots, a_n + mM$  is not a basis for  $M/mM$ . This means that after relabelling,  $a_1 + mM, \dots, a_{n-1} + mM$  spans  $M/mM$ . By the above, this means that  $a_1, \dots, a_{n-1}$  generate  $M$ . This is a contradiction of the minimality of the generating set  $a_1, \dots, a_n$ . Hence  $a_1 + mM, \dots, a_n + mM$  is a basis for  $M/mM$ .

Now suppose that  $a_1 + mM, \dots, a_n + mM$  is a basis for  $M/mM$ . We have seen above that  $a_1, \dots, a_n$  generate  $M$ . If this is not minimal, then there is some smaller generating set  $b_1, \dots, b_k$  that still generates  $M$  where  $k < n$ . By the above,  $b_1 + mM, \dots, b_k + mM$  spans  $M/mM$  hence  $n = \dim_{R/m}(M/mM) \leq k$ . This is a contradiction since  $k < n$ . Hence we are done. ■

### 3.3 Change of Rings

**Definition 3.3.1 (Extension of Scalars)** Let  $R, S$  be commutative rings. Let  $\varphi : R \rightarrow S$  be a ring homomorphism. Let  $M$  be an  $R$ -module. Define the extension of  $M$  to the ring  $S$  to be the  $S$ -module

$$S \otimes_R M$$

**Definition 3.3.2 (Restriction of Scalars)** Let  $R, S$  be commutative rings. Let  $\varphi : R \rightarrow S$  be a ring homomorphism. Let  $M$  be an  $S$ -module. Define the restriction of  $M$  to the ring  $R$  to be the  $R$ -module  $M$  equipped with the action

$$r \cdot_R m = \varphi(r) \cdot_S m$$

for all  $r \in R$ .

**Theorem 3.3.3** Let  $R, S$  be commutative rings. Let  $\varphi : R \rightarrow S$  be a ring homomorphism. Then there is an isomorphism

$$\text{Hom}_S(S \otimes_R M, N) \cong \text{Hom}_R(M, N)$$

for any  $R$ -module  $M$  and  $S$ -module  $N$  given as follows.

- For  $f \in \text{Hom}_S(S \otimes_R M, N)$ , define the map  $f^+ \in \text{Hom}_R(M, N)$  by

$$f^+(m) = f(1 \otimes m)$$

- For  $g \in \text{Hom}_R(M, N)$ , define the map  $g^- \in \text{Hom}_S(S \otimes_R M, N)$  by

$$g^-(s \otimes m) = s \cdot g(m)$$

### 3.4 Properties of the Hom Set

Let  $R$  be a ring. Let  $M, N$  be  $R$ -modules. Recall that in Rings and Modules that  $\text{Hom}_R(M, N)$  is a  $Z(R)$ -modules. When  $R$  is commutative,  $Z(R) = R$  so that the Hom set becomes an  $R$ -module.

**Proposition 3.4.1** Let  $R$  be a commutative ring. Let  $M, N$  be  $R$ -modules. Then

$$\text{Hom}_R(M, N)$$

is an  $R$ -module with the following binary operations.

- For  $\phi, \varphi : M \rightarrow N$  two  $R$ -module homomorphisms, define  $\phi + \varphi : M \rightarrow N$  by  $(\phi + \varphi)(m) = \phi(m) + \varphi(m)$  for all  $m \in M$
- For  $\phi : M \rightarrow N$  an  $R$ -module homomorphism and  $r \in R$ , define  $r\phi : M \rightarrow N$  by  $(r\phi)(m) = r \cdot \phi(m)$  for all  $m \in M$ .

**Proof** We first show that the addition operation gives the structure of a group.

- Since  $M$  is associative as an additive group, associativity follows
- Clearly the zero map  $0 \in \text{Hom}_R(M, N)$  acts as the additive inverse since for any  $\phi \in \text{Hom}_R(M, N)$ , we have that  $\phi(m) + 0 = 0 + \phi(m) = \phi(m)$  since  $0$  is the additive identity for  $M$
- For every  $\phi \in \text{Hom}_R(M, N)$ , the map taking  $m$  to  $-\phi(m)$  also lies in  $\text{Hom}_R(M, N)$ . Since  $-\phi(m)$  is the inverse of  $\phi(m)$  in  $M$  for each  $m \in M$ , we have that  $-\phi$  is the inverse of  $\phi$

We now show that

- Let  $r, s \in R$ , we have that  $((sr)\phi)(m) = (sr) \cdot \phi(m) = s \cdot (r \cdot \phi(m)) = s(r\phi)(m)$  and hence we showed associativity.
- It is clear that  $1_R \in R$  acts as the identity of the operation.

Thus we are done. ■

**Proposition 3.4.2** Let  $R$  be a ring. Let  $I$  be an indexing set. Let  $M_i, N$  be  $R$ -modules for  $i \in I$ . Then the following are true.

- There is an isomorphism

$$\text{Hom} \left( \bigoplus_{i \in I} M_i, N \right) \cong \bigoplus_{i \in I} \text{Hom}(M_i, N)$$

- There is an isomorphism

$$\text{Hom} \left( \prod_{i \in I} M_i, N \right) \cong \prod_{i \in I} \text{Hom}(M_i, N)$$

**Definition 3.4.3 (Induced Map of Hom)** Let  $R$  be a commutative ring. Let  $M_1, M_2, N$  be  $R$ -modules. Let  $f : M_1 \rightarrow M_2$  be an  $R$ -module homomorphism. Define the induced map

$$f^* : \text{Hom}_R(M_2, N) \rightarrow \text{Hom}_R(M_1, N)$$

by the formula  $\varphi \mapsto \varphi \circ f$

**Lemma 3.4.4** Let  $R$  be a commutative ring. Let  $M_1, M_2, N$  be  $R$ -modules. Let  $f : M_1 \rightarrow M_2$  be an  $R$ -module homomorphism. Then the induced map

$$f^* : \text{Hom}(M_2, N) \rightarrow \text{Hom}(M_1, N)$$

is an  $R$ -module homomorphism.

### 3.5 More on Exact Sequences

**Proposition 3.5.1** Let  $R$  be a commutative ring. Let the following be an exact sequence of  $R$ -modules.

$$0 \longrightarrow M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3 \longrightarrow 0$$

Let  $N$  be an  $R$ -module. Then the following two sequences

$$0 \longrightarrow \text{Hom}_R(M_3, N) \longrightarrow \text{Hom}_R(M_2, N) \longrightarrow \text{Hom}_R(M_1, N)$$

$$\text{Hom}_R(N, M_1) \longrightarrow \text{Hom}_R(N, M_2) \longrightarrow \text{Hom}_R(N, M_3) \longrightarrow 0$$

are exact.

#### Proof

- We first show that  $g^*$  is injective. Let  $\phi, \rho \in \text{Hom}(C, G)$  such that  $g^*(\phi) = g^*(\rho)$ . This means that  $\phi \circ g = \rho \circ g$ . Let  $c \in C$ . Since  $g$  is surjective, there exists  $b \in B$  such that  $g(b) = c$ . Then

$$\phi(c) = \phi(g(b)) = \rho(g(b)) = \rho(c)$$

Hence  $\phi = \rho$ .

Now we show that  $\text{im}(g^*) \subseteq \ker(f^*)$ . Let  $g^*(\phi) \in \text{Hom}(B, G)$  for  $\phi \in \text{Hom}(C, G)$ . We want to show that  $f^*(g^*(\phi)) = 0$ . But we have that

$$(\phi \circ g \circ f)(a) = \phi(g(f(a))) = \phi(0) = 0$$

since  $\text{im}(f) = \ker(g)$ . Thus we conclude.

Finally we show that  $\ker(f^*) \subseteq \text{im}(g^*)$ . Let  $f^*(\phi) = 0$  for  $\phi \in \text{Hom}(B, G)$ . This means that  $\phi \circ f = 0$  or in other words,  $\text{im}(f) \subseteq \ker(\phi)$ . Since  $\phi(k) = 0$  for all  $k \in \text{im}(f)$ ,  $\phi$  descends to a map  $\bar{\phi} : \frac{B}{\text{im}(f)} \rightarrow G$ . But  $\text{im}(f) = \ker(g)$  hence this is equivalent to a map  $\bar{\phi} : \frac{B}{\ker(g)} \rightarrow G$ . But by the first isomorphism theorem and the fact that  $g$  is surjective, we conclude that  $\bar{g} : \frac{B}{\ker(g)} \xrightarrow{g} C$ , where  $b + \ker(g) \mapsto g(b)$ . Thus we have constructed a map  $\bar{\phi} \circ \bar{g}^{-1} : C \rightarrow G$  given by  $g(b) \mapsto b + \ker(g) \mapsto \phi(b)$ . But now  $g^*(\bar{\phi} \circ \bar{g}^{-1})$  is the map defined by

$$b \mapsto g(b) \mapsto b + \ker(g) \mapsto \phi(b)$$

and so this map is exactly  $\phi$ . Thus  $\phi \in \text{im}(g^*)$ . ■

**Example 3.5.2** Applying  $\text{Hom}_{\mathbb{Z}}(-, \mathbb{Z}/p\mathbb{Z})$  to the short exact sequence

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

does not give a sequence that is exact on the right.



**Proof** The new sequence is now

$$0 \longrightarrow \mathbb{Z}/p\mathbb{Z} \xrightarrow{\text{id}_{\mathbb{Z}/p\mathbb{Z}}} \mathbb{Z}/p\mathbb{Z} \xrightarrow{0} \mathbb{Z}/p\mathbb{Z}$$

Evidently the 0 map is not surjective. ■

**Proposition 3.5.3** Let  $R$  be a commutative ring. Let the following be an exact sequence of  $R$ -modules.

$$0 \longrightarrow M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3 \longrightarrow 0$$

Let  $N$  be an  $R$ -module. Then the following sequence

$$M_1 \otimes N \xrightarrow{f \otimes \text{id}_N} M_2 \otimes N \xrightarrow{g \otimes \text{id}_N} M_3 \otimes N \longrightarrow 0$$

is exact.

However, one can observe that we did not imply that  $M_1 \otimes N \rightarrow M_2 \otimes N$  is injective. Indeed, this is because tensoring does not preserve injections.

## 4 Algebra Over a Commutative Ring

### 4.1 Commutative Algebras

**Definition 4.1.1 (Commutative Algebras)** Let  $R$  be a commutative ring. A commutative  $R$ -algebra is an  $R$ -algebra  $A$  that is commutative.

**Proposition 4.1.2** Let  $R$  be a commutative ring. Then the following are equivalent characterizations of a commutative  $R$ -algebra.

- $A$  is a commutative  $R$ -algebra
- $A$  is a commutative ring together with a ring homomorphism  $f : R \rightarrow A$

**Proof** Suppose that  $A$  is an  $R$ -algebra. Then define a map  $f : R \rightarrow A$  by  $f(r) = r \cdot 1$  where  $r \cdot 1$  is the module operation on  $A$ . Then clearly this is a ring homomorphism.

Suppose that  $A$  is a commutative ring together with a ring homomorphism  $f : R \rightarrow A$ . Define an action  $\cdot : R \times A \rightarrow A$  by  $r \cdot a = f(r)a$ . Then this action clearly allows  $A$  to be an  $R$ -module. ■

Under the correspondence of associative algebra, the above proposition gives a another correspondence between the first one.

$$\left\{ (A, R) \mid \begin{array}{l} A \text{ is a commutative} \\ R\text{-algebra} \end{array} \right\} \xleftrightarrow{1:1} \left\{ \phi : R \rightarrow A \mid \begin{array}{l} \phi \text{ is a ring homomorphism} \\ \text{such that } f(R) \subseteq Z(A) = A \end{array} \right\}$$

In particular, the construction above are inverses of each other so that it gives the one-to-one correspondence.

### 4.2 Free Commutative Algebras

Let  $R$  be a commutative ring. Let  $X$  be a set. Recall that we defined  $R\langle X \rangle$  to be the free (non-commutative)  $R$ -algebra over  $X$ . Explicitly, if  $W = \{x_1 \cdots x_n \mid x_1, \dots, x_n \in X\}$  is the set of words on  $X$ , then

$$R\langle X \rangle = \bigoplus_{w \in W} R \cdot w$$

together with multiplication defined by  $(x_1 \cdots x_n) \cdot (y_1 \cdots y_m) = x_1 \cdots x_n \cdot y_1 \cdots y_m$ .

**Definition 4.2.1 (Free Commutative Algebra over a Ring)** Let  $R$  be a commutative ring. Let  $X$  be a set. Define the free commutative  $R$ -algebra over  $X$  to be the quotient

$$\text{Free}_R(X) = \frac{R\langle X \rangle}{\langle x_i x_j - x_j x_i \mid x_i, x_j \in X \rangle}$$

**Proposition 4.2.2 (Universal Property of Free Commutative Algebras)** Let  $R$  be a commutative ring. Let  $X$  be a set. The free commutative algebra  $\text{Free}_R(X)$  satisfies the following universal property.

- Universal Property: If  $A$  is a commutative  $R$ -algebra, then for every  $f : X \rightarrow A$  a map of sets, there exists a unique homomorphism of algebras  $\varphi : \text{Free}_R(X) \rightarrow A$  such that  $\varphi(x_i) = f(x_i)$  for each  $x_i \in X$ . In other words, the following diagram commutes:

$$\begin{array}{ccc} X & \xrightarrow{\iota} & \text{Free}_R(X) \\ & \searrow f & \downarrow \exists! \varphi \\ & & A \end{array}$$

where  $\iota : X \rightarrow \text{Free}_R(X)$  is the inclusion.

- $\text{Free}_R(X)$  is the unique  $R$ -algebra (up to unique isomorphism) that satisfies this property.

**Proposition 4.2.3** Let  $R$  be a commutative ring. Let  $X$  be a set. Then there is an  $R$ -algebra isomorphism

$$\text{Free}_R(X) \cong R[X]$$

with the polynomial ring over  $X$ .

### 4.3 Finiteness Properties of Algebras

**Definition 4.3.1 (Finitely Generated Algebras)** Let  $R$  be a commutative ring. Let  $A$  be a commutative  $R$ -algebra. We say that  $A$  is finitely generated if there exists  $a_1, \dots, a_n \in A$  such that every element  $a \in A$  can be written as a polynomial in  $a_1, \dots, a_n$ . This means that

$$a = \sum_{i_1, \dots, i_n} r_{i_1, \dots, i_n} a_1^{i_1} \cdots a_n^{i_n}$$

Finitely generated algebras are also called algebra of finite type.

**Theorem 4.3.2** Let  $A$  be a commutative algebra over a ring  $R$ . Then the following are equivalent.

- $A$  is a finitely generated algebra over  $R$
- There exists elements  $a_1, \dots, a_n \in A$  such that the evaluation homomorphism

$$\phi : R[x_1, \dots, x_n] \rightarrow A$$

given by  $\phi(f) = f(a_1, \dots, a_n)$  is a surjection

- There is an isomorphism

$$A \cong \frac{R[x_1, \dots, x_n]}{I}$$

for some ideal  $I$

**Definition 4.3.3 (Finitely Presented Algebra)** Let  $R$  be a ring. Let  $A = R[x_1, \dots, x_n]/I$  be a finitely generated algebra over  $R$  for some ideal  $I$ . We say that  $A$  is finitely presented if  $I$  is finitely generated.

**Lemma 4.3.4** Let  $R$  be a ring, considered as an algebra over  $\mathbb{Z}$ . If  $R$  is finitely generated over  $\mathbb{Z}$ , then  $R$  is finitely presented.

**Proof** Trivial since  $\mathbb{Z}$  is a principal ideal domain. ■

**Definition 4.3.5 (Finite Algebras)** Let  $R$  be a commutative ring. Let  $A$  be an  $R$ -algebra. We say that  $A$  is finite if  $A$  is finitely generated as an  $R$ -module.

**Example 4.3.6** Let  $R$  be a commutative ring. Then  $R[x]$  is a finitely generated algebra over  $R$  but is not a finite  $R$ -algebra.

## 5 Localization

### 5.1 Localization of Modules

**Definition 5.1.1 (Multiplicative Set)** Let  $R$  be a commutative ring.  $S \subseteq R$  is a multiplicative set if  $1 \in S$  and  $S$  is closed under multiplication:  $x, y \in S$  implies  $xy \in S$

**Definition 5.1.2 (Localization of a Module)** Let  $R$  be a commutative ring and  $S \subseteq R$  be a multiplicative set. Let  $M$  be a  $R$ -module. Define the ring of fractions of  $M$  with respect to  $S$  by

$$S^{-1}M = \left\{ \frac{m}{s} \mid m \in M, s \in S \right\} / \sim$$

where  $\sim$  is defined by

$$\frac{m}{s} \sim \frac{m'}{s'} \text{ if and only if } \exists v \in S \text{ such that } v(mu' - m'u) = 0$$

**Lemma 5.1.3** Let  $R$  be a commutative ring. Let  $M$  be an  $R$ -module. Let  $S \subseteq R$  be a multiplicative subset. Then  $S^{-1}M$  is a well defined  $S^{-1}R$ -module with operation given by

$$\left( \frac{r}{s_1}, \frac{m}{s_2} \right) \mapsto \frac{r \cdot m}{s_1 s_2}$$

**Definition 5.1.4 (Induced Map of Localization)** Let  $R$  be a commutative ring. Let  $S \subseteq R$  be a multiplicative subset. Let  $M, N$  be  $R$ -modules. Let  $\phi : M \rightarrow N$  be an  $R$ -module homomorphism. Define the induced map

$$S^{-1}\phi : S^{-1}M \rightarrow S^{-1}N$$

by the formula  $\frac{m}{s} \mapsto \frac{\phi(m)}{s}$ .

**Lemma 5.1.5** Let  $R$  be a commutative ring. Let  $S \subseteq R$  be a multiplicative subset. Let  $M, N$  be  $R$ -modules. Let  $\phi : M \rightarrow N$  be an  $R$ -module homomorphism. Then the induced map

$$S^{-1}\phi : S^{-1}M \rightarrow S^{-1}N$$

is a well defined ring homomorphism.

**Lemma 5.1.6** Let  $R$  be a commutative ring. Let  $S \subseteq R$  be a multiplicative subset. Let  $M, N, K$  be  $R$ -modules. Let  $f : M \rightarrow N$  and  $g : N \rightarrow K$  be  $R$ -module homomorphisms. Then the following are true.

- Composition:  $S^{-1}(g \circ f) = S^{-1}g \circ S^{-1}f : S^{-1}M \rightarrow K$ .
- Identity:  $S^{-1}\text{id}_M = \text{id}_{S^{-1}M}$

**Proposition 5.1.7** Let  $R$  be a commutative ring. Let  $S \subseteq R$  be a multiplicative subset. Let the following be an exact sequence of  $R$ -modules.

$$M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3$$

Then the following is an exact sequence of  $S^{-1}R$ -modules.

$$S^{-1}M_1 \xrightarrow{f} S^{-1}M_2 \xrightarrow{g} S^{-1}M_3$$

**Proof** Since  $\text{im}(f) = \ker(g)$ , we have that  $g \circ f = 0$  which implies that  $0 = S^{-1}0 = S^{-1}(g \circ f) = S^{-1}g \circ S^{-1}f$ . Hence  $\text{im}(S^{-1}f) \subseteq \ker(S^{-1}g)$ . Conversely, let  $m_2/s \in \ker(S^{-1}g)$ . Then  $g(m_2)/s = 0$  and so  $g(tm_2) = tg(m_2) = 0$  for some  $t \in S$ . Since  $\text{im}(f) = \ker(g)$ , there exists  $m_1 \in M_1$  such that  $f(m_1) = tm_2$ . Then we have

$$(S^{-1}f)(m_1/ts) = f(m_1)/ts = tm_2/ts = m_2/s$$

Hence  $m_2/s \in \text{im}(S^{-1}(f))$ . ■

**Corollary 5.1.8** Let  $R$  be a commutative ring. Let  $S \subseteq R$  be a multiplicative subset. Let  $M$  be an  $R$ -module. Then the following are true.

- Localization commutes with quotients: If  $N$  is an  $R$ -submodule of  $M$ , then

$$S^{-1} \frac{M}{N} \cong \frac{S^{-1}M}{S^{-1}N}$$

as  $S^{-1}R$ -modules.

- Localization commutes with products: If  $N$  is an  $R$ -module, then

$$S^{-1}(M \times N) \cong S^{-1}M \times S^{-1}N$$

as  $S^{-1}R$ -modules.

- Localization commutes with internal sums: If  $N_1, N_2$  are  $R$ -submodules of  $M$ , then

$$S^{-1}(N_1 + N_2) \cong S^{-1}N_1 + S^{-1}N_2$$

as  $S^{-1}R$ -submodules of  $S^{-1}M$ .

- Localization commutes with intersections: If  $N_1, N_2$  are  $R$ -submodules of  $M$ , then

$$S^{-1}(N_1 \cap N_2) = S^{-1}N_1 \cap S^{-1}N_2$$

as  $S^{-1}R$ -submodules of  $S^{-1}M$ .

**Proof** Consider the exact sequences:

$$0 \longrightarrow N \xrightarrow{\text{incl.}} M \xrightarrow{\text{proj.}} M/N \longrightarrow 0$$

$$0 \longrightarrow M \xrightarrow{\text{incl.}} M \times N \xrightarrow{\text{proj.}} N \longrightarrow 0$$

$$0 \longrightarrow N_1 \xrightarrow{\text{incl.}} N_1 + N_2 \xrightarrow{\text{proj.}} N_2 \longrightarrow 0$$

$$0 \longrightarrow N_1 \cap N_2 \xrightarrow{n \mapsto (n, n)} N_1 \times N_2 \xrightarrow{(n_1, n_2) \mapsto n_1 - n_2} N_1 + N_2 \longrightarrow 0$$

respectively and apply the above proposition. ■

**Lemma 5.1.9** Let  $R$  be a commutative ring. Let  $S \subseteq R$  be a multiplicative subset. Let  $M, N$  be  $R$ -modules. Let  $\phi : M \rightarrow N$  be an  $R$ -module homomorphism. Then the following are true.

- Localization commutes with kernels:

$$S^{-1} \ker(\phi) \cong \ker(S^{-1}\phi)$$

- Localization commutes with cokernels:

$$S^{-1} \frac{N}{\text{im}(\phi)} \cong \frac{S^{-1}N}{\text{im}(S^{-1}\phi)}$$

- Localization commutes with images:

$$S^{-1}(\text{im } \phi) \cong \text{im}(S^{-1}\phi)$$

**Proof** Consider the exact sequences:

$$0 \longrightarrow \ker(\phi) \hookrightarrow M \xrightarrow{\phi} N$$

$$M \xrightarrow{\phi} N \longrightarrow \frac{M}{\operatorname{im}(\phi)} \longrightarrow 0$$

$$0 \longrightarrow \ker(\phi) \longrightarrow M \longrightarrow \operatorname{im}(\phi) \longrightarrow 0$$

respectively and apply 5.3.6. ■

**Proposition 5.1.10** Let  $R$  be a commutative ring. Let  $M$  be an  $R$ -module. Then there is an isomorphism

$$S^{-1}M \cong S^{-1}R \otimes_R M$$

of  $S^{-1}R$ -modules given by  $\frac{m}{s} \mapsto \frac{1}{s} \otimes m$ .

## 5.2 Localization at Single Elements and Away from Prime Ideals

**Lemma 5.2.1** Let  $R$  be a commutative ring. Let  $f \in R$  be non-zero. Then the set  $\{f^n \mid n \in \mathbb{N}\}$  is a multiplicative set.

**Definition 5.2.2 (Localization at an Element)** Let  $R$  be a commutative ring. Let  $M$  be an  $R$ -module. Let  $f \in R$  be non-zero. Define the localization of  $M$  at  $f$  to be the ring

$$M_f = \{f^n \mid n \in \mathbb{N}\}^{-1}M$$

**Lemma 5.2.3** Let  $R$  be a commutative ring. Let  $f \in R$  be non-zero. Then there is an  $R$ -algebra isomorphism

$$R_f \cong R \left[ \frac{1}{f} \right]$$

given by  $\frac{a}{f^k} \mapsto a \cdot \frac{1}{f^k}$ .

**Lemma 5.2.4** Let  $R$  be a commutative ring and  $P$  a prime ideal of  $R$ . Then  $R \setminus P$  is a multiplicative set.

**Proof** By definition,  $xy \in P$  implies  $x \in P$  or  $y \in P$ , since  $R \setminus P$  removes all these elements, we have that  $x \notin P$  and  $y \notin P$  implies that  $xy \notin P$ . ■

**Definition 5.2.5 (Localization at Prime Ideals)** Let  $R$  be a commutative ring. Let  $M$  be an  $R$ -module. Let  $P$  be a prime ideal. Denote

$$M_P = (R \setminus P)^{-1}M$$

the localization of  $M$  at  $P$ .

## 5.3 The Localization Map

**Proposition 5.3.1** Let  $R$  be a commutative ring. Let  $S$  be a multiplicative subset of  $R$ . Then the following are true.

- $(S^{-1}R, +, \times)$  is a ring
- The map  $k : R \rightarrow S^{-1}R$  defined by  $r \mapsto r/1$  is a ring homomorphism, called the localization map.

**Proof**

- Define addition by  $\frac{r}{s} + \frac{r'}{s'} = \frac{rs' + r's}{ss'}$  and multiplication by  $\frac{r}{s} \cdot \frac{r'}{s'} = \frac{rr'}{ss'}$ . Clearly addition is abelian, and has identity  $\frac{0}{1}$  and inverse  $\frac{-r}{s}$  for any  $\frac{r}{s} \in S^{-1}R$ . Multiplication also has identity  $\frac{1}{1}$ .

■

**Lemma 5.3.2** Let  $R$  be a commutative ring. Let  $S$  be a multiplicative subset of  $R$ . Then localization map  $R \rightarrow S^{-1}R$  is injective if and only if  $S$  does not contain zero divisors.

**Proof** Suppose that  $R \rightarrow S^{-1}R$  is injective. Then  $sr = 0$  implies  $r = 0$  for all  $s \in S$ . Hence  $S$  does not contain zero divisors. Suppose that  $S$  does not contain zero divisors. Then  $sr = 0$  implies that  $r = 0$  since  $S$  has no zero divisors. Hence the localization map is injective. ■

**Proposition 5.3.3 (Universal Property)** Let  $R$  be a commutative ring. Let  $S$  be a multiplicative set. Then  $S^{-1}R$  and the localization map  $k : R \rightarrow S^{-1}R$  satisfies the following universal property.

- For any commutative ring  $B$  and ring homomorphism  $\phi : R \rightarrow B$  such that  $\phi(s) \in B^\times$  for all  $s \in S$ , there exists a unique ring homomorphism  $\psi : S^{-1}R \rightarrow B$  such that the following diagram commutes:

$$\begin{array}{ccc} R & \xrightarrow{k} & S^{-1}R \\ & \searrow \phi & \downarrow \exists! \psi \\ & & B \end{array}$$

- $S^{-1}R$  is the unique commutative ring (up to unique isomorphism) that has such a property.

**Lemma 5.3.4** Let  $R$  be a commutative ring. If  $R$  is an integral domain, then the following are true.

- If  $S$  is a multiplicative subset of  $R$  such that  $0 \notin S$ , then  $S^{-1}R$  is an integral domain.
- $\text{Frac}(R) = (0)$ .
- The localization map induces a ring isomorphism

$$R \cong \bigcap_{m \text{ a maximal ideal}} R_m$$

**Proof**

- Suppose that  $0 = \frac{a}{s} \cdot \frac{b}{t}$ . By the equivalence relation this is the same as saying that  $uab = 0$  for some  $u \in S$ . Since  $R$  is an integral domain and  $0 \neq S$ , we conclude that  $u \notin S$  so that  $ab = 0$ . Again since  $R$  is an integral domain this implies that  $a = 0$  or  $b = 0$ . Hence either  $a/s = 0$  or  $b/t = 0$  in  $S^{-1}R$ . Hence  $S^{-1}R$  is an integral domain.
- Trivial.
- Clearly the map is well defined. Moreover, since for each maximal ideal  $m$ ,  $0 \notin R \setminus m$ . Hence the localization map is injective. Suppose for a contradiction that the localization map is not surjective. Then there exists  $x$  in the intersection such that  $x \neq r/1$  for all  $r \in R$ . Consider the ideal  $I = \{r \in R \mid rx = s/1 \text{ for some } s \in R\}$ . Since  $1 \notin R$ ,  $I$  is a proper ideal. So there exists a maximal ideal  $m$  containing  $I$ . But  $x$  also cannot lie in  $R_m$  and hence the intersection. Indeed, if  $x \in R_m$ , then  $x = a/b$  for some  $a \in R$  and  $b \notin m$ . Then  $bx = a \in R$  implies that  $b \in I$ . This is a contradiction to  $b \notin m$ . Thus no such  $x$  exists. Hence the localization map is surjective.

■

## 5.4 Ideals of a Localization

**Definition 5.4.1** (Ideals Closed Under Division) Let  $R$  be a commutative ring. Let  $I$  be an ideal of  $R$ . Let  $S \subseteq R$  be a multiplicative subset. We say that  $I$  is closed under division by  $s$  if for all  $s \in S$  and  $a \in R$  such that  $sa \in I$ , we have  $a \in I$ .

**Lemma 5.4.2** Let  $R$  be a commutative ring. Let  $I$  be an ideal of  $R$ . Let  $S \subseteq R$  be a multiplicative subset. Then we have

$$I^e = S^{-1}I$$

**Proof** Let  $f : R \rightarrow S^{-1}R$  be the localization map. Then  $f(I) \subseteq S^{-1}I$  implies that  $I^e \subseteq S^{-1}I$ . Conversely, suppose that  $i/s \in S^{-1}I$ . Then  $i/s = (1/s) \cdot f(i) \in I^e$ . Hence  $I^e = S^{-1}I$ . ■

**Proposition 5.4.3** Let  $R$  be a commutative ring. Let  $S$  be a multiplicative subset of  $R$ . Let  $P$  be a prime ideal of  $R$ . Then the following are true.

- $S^{-1}P$  is a prime ideal of  $S^{-1}R$  if and only if  $S \cap P = \emptyset$ .
- $S^{-1}P = S^{-1}R$  if and only if  $S \cap P \neq \emptyset$ .

**Proof** Recall that  $R/P$  is an integral domain if  $P$  is prime. Since  $S^{-1}$  commutes with quotients, we have that

$$\frac{S^{-1}R}{S^{-1}P} \cong S^{-1} \frac{R}{P}$$

If  $S \cap P = \emptyset$ , then  $0 \in P$  implies that  $0 \notin S$ . This means that  $0 \notin \phi(S)$ . By 5.3.1 we conclude that  $S^{-1}(R/P)$  is an integral domain. Hence  $S^{-1}P$  is a prime ideal. If  $S \cap P \neq \emptyset$ , suppose that  $x \in S \cap P$ . Then ????? ■

**Theorem 5.4.4** Let  $R$  be a commutative ring. Let  $I$  be an ideal of  $R$ . Let  $S \subseteq R$  be a multiplicative subset. Let  $\phi : R \rightarrow S^{-1}R$  denote the localization map. Then there is a one-to-one bijection

$$\{J \mid J \text{ is an ideal of } S^{-1}R\} \xrightarrow{1:1} \{I \mid \begin{array}{l} I \text{ is an ideal of } R \text{ and} \\ I \text{ is closed under division by } S \end{array}\}$$

whose map is given by  $J \mapsto J^c = \phi^{-1}(J)$  and inverse is given by  $I \mapsto I^e = S^{-1}I$ .

**Proof** We first show that our map of sets are well defined. Let  $J$  be an ideal of  $S^{-1}R$ . We first show that  $\phi^{-1}(J)$  is closed under division by  $S$ . Suppose that  $s \in S$  and  $r \in R$  such that  $sr \in \phi^{-1}(J)$ . Then  $sr/1 \in J$ . Now since  $J$  is an ideal of  $S^{-1}R$ , we know that  $1/s \cdot sr/1 \in J$ . But  $1/s \cdot sr/1 = r/1 = \phi(r)$ . This means that  $\phi(r) \in J$  and hence  $r \in \phi^{-1}(J)$ . Thus  $\phi^{-1}(J)$  is an ideal closed under division by  $S$ .

Now let  $I$  be an ideal of  $R$  closed under division. I claim that  $S^{-1}I$  is an ideal of  $S^{-1}R$ . Let  $a/s, b/t \in S^{-1}I$ . Then  $a/s + b/t = (at + bs)/st$ . Since  $I$  is an ideal, we know that  $at + bs \in I$ . Also since  $S$  is a multiplicative subset,  $st \in S$ . Hence  $(at + bs)/st \in S^{-1}I$ . Now let  $a/s \in S^{-1}I$  and  $r/t \in S^{-1}R$ . Then  $(a/s) \cdot (r/t) = ar/st$ . Since  $I$  is an ideal,  $ar \in I$ . Thus  $ar/st \in S^{-1}I$  so that  $I$  is an ideal.

It remains to show that the two maps are inverses of each other. Let  $J$  be an ideal of  $S^{-1}R$ . We want to show that  $J = S^{-1}(\phi^{-1}(J))$ . Let  $a/s \in J$ . Since  $J$  is an ideal, we have  $\phi(a) = a/1 = 1/s \cdot a/s \in J$ . Hence  $a \in \phi^{-1}J$  so that  $a/s \in S^{-1}\phi^{-1}(J)$ . Thus  $J \subseteq S^{-1}(\phi^{-1}(J))$ . Now by 1.5.5 the extension of the contraction of  $J$  is a subset of  $J$ . Hence we conclude.

On the other hand, we also want to show that  $I = \phi^{-1}(S^{-1}I)$ . Again by 1.5.5 we know that  $I \subseteq \phi^{-1}(S^{-1}I)$ . Conversely, let  $x \in \phi^{-1}(S^{-1}I)$ . Then  $\phi(x) = x/1 \in S^{-1}I$ . This means that  $x/1 = b/t$  for some  $b \in I$  and  $t \in S$ . Then there exists  $u \in S$  such that  $uxt = ub$ . Since  $b \in I$ ,



$ub \in I$  hence  $uxt \in I$ . Since  $ut \in S$  and  $I$  is closed under division, we have  $x \in I$ .

This shows that  $S^{-1}(-)$  and  $\phi^{-1}(-)$  are mutual inverses of each others. Thus we conclude. ■

Using the theorem we conclude that every ideal of  $S^{-1}R$  is of the form  $S^{-1}I$  for some ideal  $I$  of  $R$  such that  $I$  is closed under division by  $S$ .

**Proposition 5.4.5** Let  $R$  be a commutative ring. Let  $I$  be an ideal of  $R$ . Let  $S \subseteq R$  be a multiplicative subset. Then the above bijection restricts to the following bijection

$$\text{Spec}(S^{-1}R) \xrightarrow{1:1} \left\{ I \mid \begin{array}{l} I \text{ is a prime ideal of } R \\ \text{and } I \cap S = \emptyset \end{array} \right\}$$

**Proof** Let  $\phi : R \rightarrow S^{-1}R$  be the localization map. From the above we know that  $Q = S^{-1}\phi^{-1}(Q)$  for any prime ideal  $Q$  of  $S^{-1}R$ . This implies that  $S^{-1}\phi^{-1}(Q)$  is prime. By 5.4.3 this implies that  $\phi^{-1}(Q) \cap S = \emptyset$ . Thus the map  $J \mapsto \phi^{-1}(J)$  induces a well defined map on our given sets of prime ideals.

Conversely, by 5.4.3 we know that if  $P$  is a prime ideal of  $R$  such that  $S \cap P = \emptyset$ , then  $S^{-1}P$  is a prime ideal of  $S^{-1}R$ . Hence the inverse map is also well defined on our domain and codomain. By the above theorem it is already a bijection, hence we are done. ■

**Proposition 5.4.6** Let  $R$  be a commutative ring. Let  $P$  be a prime ideal of  $R$ . Then the above bijection gives

$$\text{Spec}(R_P) \xrightarrow{1:1} \left\{ I \mid \begin{array}{l} I \text{ is a prime ideal of } R \\ \text{and } I \subseteq P \end{array} \right\}$$

**Proof** Notice that the condition that  $I \cap S = \emptyset$  in the above proposition translates to  $I \cap (R \setminus P) = \emptyset$ , which is the same as saying  $I \subseteq P$ . ■

**Proposition 5.4.7** Let  $R$  be a commutative ring and let  $P$  be a prime ideal of  $R$ . Then  $R_P$  is a local ring with unique maximal ideal given by

$$PR_P = \left\{ \frac{r}{s} \mid r \in P, s \notin P \right\}$$

**Proof** We show that  $PR_P$  is the only unique maximal ideal. Suppose that  $I$  is an ideal in  $R_P$  such that  $I$  is not a subset of  $PR_P$ . Then there exists  $a/s \in I$  such that  $a \notin P$  and  $s \notin P$ . It is clear that  $s/a$  is then an element of  $R_P$ . So  $a/s$  is invertible. Hence  $I = R_P$ . ■

Be wary that in general localizations does not result in a local ring. This happens only when we are localizing with respect to a prime ideal. The importance of prime ideals is not explicit in the above because only using prime ideals  $P$  can  $R \setminus P$  be a multiplicative set which ultimately allows localization to make sense.

**Proposition 5.4.8 (Localization of a Localization)** Let  $R$  be a commutative ring. Let  $S$  be a multiplicative subset of  $R$ . Let  $P$  be a prime ideal of  $R$  such that  $S^{-1}P$  is a prime ideal of  $S^{-1}R$ . Then

$$(S^{-1}R)_{S^{-1}P} \cong R_P$$

**Proof** Define a map  $S^{-1}R \rightarrow R_P$  by the identity map. This is well defined because if  $s \in S$ , then we know  $S^{-1}P$  is a prime ideal implies  $S \cap P = \emptyset$ , so  $s \notin P$ . Thus  $r/s$  is a well defined fraction in  $R_P$ . Since it is just the identity map, it is a well defined ring homomorphism. Now let  $r/s \in S^{-1}R \setminus S^{-1}P$ . Then  $r \notin P$  implies that  $r$  is invertible in  $R_P$ . Hence  $r/s \cdot s/r = 1$  in  $R_P$ .

Thus  $r/s$  is invertible in  $R_P$ . Thus we can invoke the universal property to obtain a unique map

$$(S^{-1}R)_{S^{-1}P} \rightarrow R_P$$

Conversely, define a map  $R \rightarrow (S^{-1}R)_{S^{-1}P}$  by the identity map  $r \mapsto (r/1)/(1/1)$ . This is well defined because  $1 \notin P$  implies  $1/1 \in S^{-1}R \setminus S^{-1}P$ . Clearly this is a well defined ring homomorphism. For  $s \in S$ , notice that  $(s/1)/(1/1)$  is invertible in  $(S^{-1}R)_{S^{-1}P}$  via the element  $(1/s)/(1/1)$ . Thus we can invoke the universal property of  $S^{-1}R$  to obtain a unique map

$$S^{-1}R \rightarrow (S^{-1}R)_{S^{-1}P}$$

We now have two unique maps going both directions between  $S^{-1}R$  and  $(S^{-1}R)_{S^{-1}P}$ . This implies that they are isomorphic. ■

**Lemma 5.4.9** Let  $R$  be a commutative ring. Let  $S \subseteq R$  be a multiplicative subset of  $R$ . If  $R$  is Noetherian, then  $S^{-1}R$  is Noetherian.

**Proof** Follows from the correspondence of ideals in localizations. ■

## 5.5 Localization of Graded Rings

**Proposition 5.5.1** Let  $R = \bigoplus_{i=0}^{\infty} R_i$  be a commutative ring that is graded. Let  $P$  be a homogeneous prime ideal of  $R$ . Then  $R_P$  is a graded ring in which the grading structure is given as follows:  $f/g \in R_P$  has degree  $\deg(f) - \deg(g)$ .

**Definition 5.5.2 (Localization of a Graded Ring)** Let  $R = \bigoplus_{i=0}^{\infty} R_i$  be a commutative ring that is graded. Let  $P$  be a homogeneous prime ideal of  $R$ . Define the localization of  $R$  with respect to  $P$  to be

$$(R_P)_0 = \{f \in R_P \mid f \text{ lies in the 0th graded component of } R_P\}$$

**Proposition 5.5.3** Let  $R = \bigoplus_{i=0}^{\infty} R_i$  be a commutative ring that is graded. Let  $P$  be a homogeneous prime ideal of  $R$ . Then  $(R_P)_0$  is a local ring with unique maximal ideal given by

$$(PR_P) \cap (R_P)_0$$

## 5.6 Local Properties

**Definition 5.6.1 (Local Properties of Elements)** Let  $R$  be a commutative ring. Let  $M$  be an  $R$ -module. A property of an element of  $M$  is local if the following is true.  $m \in M$  has the property if and only if  $m \in M_P$  has the property.

**Lemma 5.6.2** Let  $R$  be a commutative ring. Let  $M$  be an  $R$ -module. Then  $x \in M$  being the zero element is a local property.

**Proof** Suppose that  $x = 0$  in  $M$ . Then clearly  $x = 0$  in both  $M_P$  and  $M_m$  for all prime ideals  $P$  and maximal ideals  $m$ . Now let  $x = 0$  in  $M_m$  for all maximal ideals  $m$ . This means that there exists  $a_m \in R \setminus m$  such that  $a_m x = 0$ . Let  $I$  be the ideal

$$I = \sum_{m \text{ a maximal ideal}} a_m R \subseteq R$$

Since  $a_m \in I$  but  $a_m \notin m$ , we must have that  $I$  is not contained in any maximal ideals. Hence  $I = R$ . Then there exists  $r_i \in R$  such that  $1 = \sum_{i=1}^n r_i a_{m_i}$  for some  $a_{m_i} \in R \setminus m_i$ . Then we have

$$x = \sum_{i=1}^n (r_i a_{m_i} x) = 0 \in M$$

**Definition 5.6.3 (Local Properties of Modules)** Let  $R$  be a commutative ring. A property of  $R$ -modules is local if for any  $R$ -modules  $M$ , the following are equivalent.

- $M$  has the property
- $M_P$  has the property for all prime ideals  $P$
- $M_m$  has the property for all maximal ideals  $m$

**Lemma 5.6.4** Let  $R$  be a commutative ring. Let  $M$  be an  $R$ -module. Then the module being 0 is a local property.

**Proof** If  $M = 0$ , then clearly  $M_P = 0$  and  $M_m = 0$  for all prime ideals  $P$  and maximal ideals  $m$ . Then using 5.6.2 we conclude that if  $M_m = 0$  for all maximal ideals  $m$ , then  $M = 0$ . ■

**Proposition 5.6.5 (Injectivity and Surjectivity are Local Properties)** Let  $R$  be a commutative ring. Let  $M, N$  be  $R$ -modules. Let  $\phi : M \rightarrow N$  be an  $R$ -module homomorphism. Let  $S$  be a multiplicative subset of  $R$ . Then the following are equivalent.

- $\phi$  is injective (surjective)
- For each prime ideal  $P$  of  $R$ , the induced map  $\phi_P : S^{-1}M \rightarrow S^{-1}N$  is injective (surjective)
- For each maximal ideal  $m$  of  $R$ , the induced map  $\phi_m : S^{-1}M \rightarrow S^{-1}N$  is injective (surjective)

More local properties: nilpotent

Non-local properties: freeness, domain

**Proposition 5.6.6 (Exactness is Local)** Let  $R$  be a commutative ring. Let  $M_1, M_2, M_3$  be  $R$ -modules. Let  $f : M_1 \rightarrow M_2$  and  $g : M_2 \rightarrow M_3$  be  $R$ -module homomorphisms. Then the following conditions are equivalent.

- The following sequence is exact:

$$M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3$$

- The following sequence is exact:

$$(M_1)_P \xrightarrow{f_P} (M_2)_P \xrightarrow{g_P} (M_3)_P$$

for all prime ideals  $P$  of  $R$ .

- The following sequence is exact:

$$(M_1)_m \xrightarrow{f_m} (M_2)_m \xrightarrow{g_m} (M_3)_m$$

for all maximal ideals  $m$  of  $R$ .

**Proof** (1)  $\implies$  (2), (3) is clear since localization preserves exact sequences. It remains to show that (3)  $\implies$  (1). Let  $x \in M$ . Then we have that  $g_m(f_m(x)) = 0$  for all maximal ideals  $m$ . Since being 0 is a local property, we conclude that  $g(f(x)) = 0$ . Hence  $\text{im}(f) \subseteq \ker(g)$ . Since kernels and images and quotients commute with localizations, we have that

$$\left( \frac{\ker(g)}{\text{im}(f)} \right)_m \cong \frac{\ker(g_m)}{\text{im}(f_m)} = 0$$

Since being a zero module is a local property, we conclude that  $\text{im}(f) = \ker(g)$ . ■

## 6 Primary Decomposition

### 6.1 The Annihilator and Associated Primes

Let  $R$  be a commutative ring. Let  $M$  be an  $R$ -module. Recall that we define the annihilator of a subset  $S \subseteq M$  to be the ideal

$$\text{Ann}_R(S) = \{r \in R \mid rs = 0 \text{ for all } s \in S\}$$

When  $R$  is a commutative ring, the annihilator is a two sided ideal and consequently has some nice properties.

**Proposition 6.1.1** Let  $R$  be a commutative ring. Let  $M$  be an  $R$ -module. Let  $\text{Ann}_R(x)$  for  $x \in M$  be a maximal element in the set

$$\{\text{Ann}_R(x) \mid 0 \neq x \in M\}$$

Then  $\text{Ann}_R(x)$  is a prime ideal.

**Proof** Suppose that  $ab \in \text{Ann}_R(x)$  and  $b \notin \text{Ann}_R(x)$ . Notice that if  $rx = 0$  then  $r(bx) = brx = 0$  so that  $r$  annihilates  $bx$ . Hence  $\text{Ann}_R(x) \subseteq \text{Ann}_R(bx)$ . Since  $x$  is non-zero and  $b \notin I$ ,  $bx$  is also non-zero hence  $\text{Ann}_R(bx)$  lies in the given set of annihilators. Since  $\text{Ann}_R(x)$  is maximal we conclude that

$$\text{Ann}_R(x) = \text{Ann}_R(bx)$$

But  $ab$  annihilates  $x$  by definition so that  $a$  annihilates  $bx$ . Hence  $a \in \text{Ann}_R(bx) = \text{Ann}_R(x)$ . Hence  $\text{Ann}_R(x)$  is prime. ■

Recall that if  $S \subseteq M$  is a subset and  $R$  is not a commutative ring, then in general we only have the relation

$$\text{Ann}_R(\langle S \rangle) \subseteq \text{Ann}_R(S)$$

**Proposition 6.1.2** Let  $R$  be a commutative ring. Let  $M$  be an  $R$ -module. Let  $S \subseteq M$  be a subset. Then

$$\text{Ann}_R(\langle S \rangle) = \text{Ann}_R(S)$$

**Definition 6.1.3 (Associated Prime)** Let  $R$  be a commutative ring. Let  $M$  be an  $R$ -module. Let  $P$  be a prime ideal of  $R$ . We say that  $P$  is an associated prime of  $M$  if

$$\text{Ann}_R(m) = P$$

for some  $m \in M$ .

**Lemma 6.1.4** Let  $R$  be a Noetherian commutative ring. Let  $M$  be an  $R$ -module. If  $M \neq 0$ , then  $\text{Ass}(M) \neq \emptyset$ .

**Proof** By 6.1.1, there exists  $x \in M$  such that  $\text{Ann}_R(x)$  is a prime ideal. ■

**Lemma 6.1.5** Let  $R$  be a commutative ring. Let  $M$  be an  $R$ -module. Let  $P$  be a prime ideal of  $R$ . Then  $P$  is an associated prime of  $M$  if and only if  $R/P$  is isomorphic to a submodule of  $M$ .

**Proof** If  $P$  is an associated prime, then  $P = \text{Ann}_R(m)$  for some  $0 \neq m \in M$ . Then  $\langle m \rangle \cong \frac{R}{\text{Ann}_R(m)}$  so that  $R/P$  is isomorphic to a submodule of  $M$ . Conversely, if  $R/P \cong N \leq M$  for some submodule  $N$ , notice that  $R/P$  is cyclic and so  $N$  is generated by one element  $n \in N$ . Then  $P = \text{Ann}_R(n)$ . ■

**Definition 6.1.6 (Set of Associated Prime)** Let  $R$  be a commutative ring. Let  $M$  be an  $R$ -module. Define the set of associated primes of  $M$  to be

$$\text{Ass}(M) = \{P \in \text{Spec}(R) \mid P \text{ is an associated prime of } M\}$$

Another way to think about the set of associated primes of  $M$  is that

$$\text{Ass}(M) = \{\text{Ann}_R(m) \mid \text{Ann}_R(m) \in \text{Spec}(R)\}$$

**Lemma 6.1.7** Let  $R$  be a Noetherian commutative ring. Let  $M$  be an  $R$ -module. Then we have

$$\bigcup_{P \in \text{Ass}(M)} P = \{r \in R \mid r \text{ is a zero divisor of } M\} \cup \{0\}$$

**Proof** If  $r \in R$  is a non-zero zero divisor of  $M$ , then  $rm = 0$  for some  $0 \neq m \in M$ . Then  $r \in \text{Ann}_R(m)$ . By 6.1.1,  $r$  is contained some prime ideal that is an annihilator. Hence  $r$  lies in the union in the left. Conversely, if  $r$  lies in some annihilator then clearly  $r$  is a zero divisor, or  $r = 0$ . ■

**Proposition 6.1.8**

Let  $R$  be a commutative ring. Let  $S$  be a multiplicative subset of  $R$ . Let  $M$  be an  $S^{-1}R$ -module. Then we have

$$\text{Ass}_{S^{-1}R}(S^{-1}M) = \text{Ass}_R(S^{-1}M)$$

**Proof**

**Proposition 6.1.9**

Let  $R$  be a Noetherian commutative ring. Let  $S$  be a multiplicative subset of  $R$ . Let  $M$  be an  $R$ -module. Then the following are true.

- Considering  $\text{Spec}(S^{-1}R)$  as a subset of  $\text{Spec}(R)$  by the correspondence of prime ideals of localization, we have

$$\text{Ass}_R(S^{-1}M) = \text{Ass}_R(M) \cap \text{Spec}(S^{-1}R)$$

- Let  $P$  be a prime ideal of  $R$ . Then  $P \in \text{Ass}_R(M)$  if and only if  $PR_P \in \text{Ass}_{R_P}(M_P)$ .

**Proof**

Suppose that  $P \in \text{Ass}_R(S^{-1}M)$ . Let  $\varphi$  denote the localization map. Then  $P = \text{Ann}_R(m/s)$  for some  $m/s \in S^{-1}M$ . But  $p/t \in P$  annihilates  $m/s$  if and only if  $p$  annihilates  $m$ . Hence by lifting  $P$  back to  $R$  by the correspondence,  $\varphi^{-1}(P) = \text{Ann}_R(m)$  and must also be a prime lying in  $\text{Spec}(S^{-1}R)$ .

Conversely, if  $P \in \text{Spec}(S^{-1}R)$  annihilates  $m \in M$ , then it must also annihilate  $m/1$ . And  $m/1$  is annihilated by  $r/s \in S^{-1}R$  if  $r$  annihilates  $m$  in  $M$ . Thus we conclude. ■

**Proposition 6.1.10** Let  $R$  be a commutative ring. Let the following be an exact sequence of  $R$ -modules.

$$0 \longrightarrow M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3 \longrightarrow 0$$

Then we have

$$\text{Ass}(M_2) \subseteq \text{Ass}(M_1) \cup \text{Ass}(M_3)$$

**Example 6.1.11** Consider the short exact sequence

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

Then  $\text{Ass}(\mathbb{Z}) \subset \text{Ass}(\mathbb{Z}) \cup \text{Ass}(\mathbb{Z}/2\mathbb{Z})$  is a strict subset.

**Proof** Clearly  $(2) \subseteq \mathbb{Z}$  annihilates  $\mathbb{Z}/2\mathbb{Z}$  but does not annihilate  $\mathbb{Z}$ . ■

**Theorem 6.1.12 (Disassembly of an  $R$ -Module)** Let  $R$  be a Noetherian commutative ring. Let  $M$  be a finitely generated  $R$ -module. Then there exists a chain of  $R$ -submodules

$$0 = M_0 \subset M_1 \subset \cdots \subset M_k = M$$

such that

$$\frac{M_i}{M_{i-1}} \cong \frac{R}{P_i}$$

for some prime ideal  $P_i$  of  $R$ .

**Proof** If  $M$  is trivial then we are done. So suppose that  $M \neq \{0\}$ . We define the  $R$ -submodules inductively.

- When  $n = 1$ ,  $\text{Ass}(M) \neq \emptyset$ , say  $P_1 \in \text{Ass}(M)$ . Since  $P_1$  is an annihilator,  $M_1 = R/P_1$  is an  $R$ -submodule of  $M$ .
- Assume that  $M_1 \subset \cdots \subset M_i$  is constructed. If  $M_i = M$  then we are done. If not, then  $M/M_i \neq \{0\}$  and  $P_{i+1} \in \text{Ass}(M/M_i) \neq \emptyset$ . Then  $N = R/P_{i+1}$  is an  $R$ -submodule of  $M/M_i$ . By the correspondence theorem for  $R$ -modules,  $N$  corresponds to an  $R$ -submodule  $M_{i+1}$  of  $M$  containing  $M_i$ .

The process eventually terminates since  $M$  is Noetherian. ■

**Proposition 6.1.13** Let  $R$  be a Noetherian commutative ring. Let  $M$  be a finitely generated  $R$ -module. Let  $P_1, \dots, P_n \in \text{Spec}(R)$  be the prime ideals appearing in the disassembly of  $M$ . Then

$$\text{Ass}(M) \subseteq \{P_1, \dots, P_n\}$$

**Proof** We induct on the length of the disassembly. When  $n = 0$  the result is trivial. Suppose that the result holds true for all  $R$ -modules whose length of disassembly is  $\leq k$ . Let  $M$  be an  $R$ -module whose disassembly has length  $k+1$ . Let  $\varphi : M/M_k \rightarrow R/P_k$  be the isomorphism given in the disassembly. Let  $m \in M$  be such that  $\text{Ann}_R(m)$  is a prime ideal. If  $m \in M_k$  then by inductive hypothesis we are done. So suppose that  $m \notin M_k$ . If  $r$  annihilates  $m$ , then  $r$  annihilates  $\varphi(m)$  in  $R/P_k$ . Hence ■

**Definition 6.1.14 (Embedded Associated Primes)** Let  $R$  be a commutative ring. Let  $M$  be an  $R$ -module. Let  $I \in \text{Ass}(M)$  be an associated prime. We say that  $I$  is embedded if  $I$  is not minimal in  $\text{Ass}(M)$ .

## 6.2 The Support of a Module

**Definition 6.2.1 (Support of a Module)** Let  $A$  be a commutative ring. Let  $M$  be an  $A$ -module. The support of  $M$  is the subset

$$\text{Supp}(M) = \{P \text{ a prime ideal of } A \mid M_P \neq 0\}$$

**Lemma 6.2.2** Let  $R$  be a commutative ring. Let the following be an exact sequence of  $R$ -modules.

$$0 \longrightarrow M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3 \longrightarrow 0$$

Then we have

$$\text{Supp}(M_2) = \text{Supp}(M_1) \cup \text{Supp}(M_3)$$

**Proposition 6.2.3** Let  $R$  be a commutative ring. Let  $M$  be a finitely generated  $R$ -module. Then

$$\text{Supp}(M) = \{P \in \text{Spec}(R) \mid \text{Ann}_R(M) \subseteq P\}$$

**Proof** We first show the case when  $M$  is generated by one element  $m \in M$ . Let  $P \in \text{Supp}(M)$ . Then  $M_P \neq 0$  and so  $m/1 \neq 0 \in M_P$ . This means that for all  $s \in R \setminus P$ , we have  $sm \neq 0$ . Then  $R \setminus P \cap \text{Ann}_R(m) = \emptyset$ . Then  $P \supseteq \text{Ann}_R(m) = \text{Ann}_R(M)$ . Conversely, suppose that  $P \notin \text{Supp}(M)$ . Then  $M_P = 0$  and so  $m/1 = 0$ . So there exists  $s \in R \setminus P$  such that  $sm = 0$ . Hence  $R \setminus P \cap \text{Ann}_R(m) \neq \emptyset$  and so  $\text{Ann}_R(M) = \text{Ann}_R(m)$  is not a subset of  $P$ .

Now suppose that  $M$  is finitely generated by  $m_1, \dots, m_k$ . Then we have

$$\begin{aligned}
 \text{Supp}(M) &= \bigcup_{i=1}^k \text{Supp}(R \cdot m_i) \\
 &= \bigcup_{i=1}^k \{P \in \text{Spec}(R) \mid \text{Ann}_R(m_i) \subseteq P\} \\
 &= \bigcup_{i=1}^k \{P \in \text{Spec}(R) \mid \text{Ann}_R(m_i) \subseteq P\} \\
 &= \left\{ P \in \text{Spec}(R) \mid \bigcap_{i=1}^k \text{Ann}_R(m_i) \subseteq P \right\} \quad (\text{Imm1.1.2}) \\
 &= \{P \in \text{Spec}(R) \mid \text{Ann}_R(M) \subseteq P\}
 \end{aligned}$$

■

**Lemma 6.2.4** Let  $R$  be a commutative ring. Let  $M$  be a finitely generated  $R$ -module. Let  $P_1, \dots, P_n \in \text{Spec}(R)$  be a complete list of distinct minimal prime ideals over  $\text{Ann}_R(M)$ . Then we have

$$\text{Supp}(M) = \bigcup_{k=1}^n \{P \in \text{Spec}(R) \mid P_k \subseteq P\}$$

**Proof** We induct on the length of the diassembly of  $M$ . If  $n = 1$ , then  $M$  is simple, and  $M \cong R/P$  with  $P = \text{Ann}_R(M)$ . Now suppose the result is true for  $\leq n - 1$ . Let  $0 = M_0 \subset \dots \subset M_n = M$  be the diassembly of  $M$ . Then we obtain an exact sequence of the form

$$0 \longrightarrow M_{n-1} \xrightarrow{f} M \xrightarrow{g} \frac{M}{M_{n-1}} \longrightarrow 0$$

In particular, we have  $\text{Supp}(M) = \text{Supp}(M/M_{n-1}) \cup \text{Supp}(M_{n-1})$ . By induction, we have  $\text{Supp}(M_{n-1}) = \bigcup_{i=1}^{n-1} \{P \in \text{Spec}(R) \mid P_i \subseteq P\}$ , and similarly for the simple module  $M/M_{n-1}$  we have the result of the case  $n = 1$ . Hence we are done. ■

Let  $R$  be a commutative ring. Let  $M$  be an  $R$ -module. Let  $P_1, \dots, P_n \in \text{Spec}(R)$  be the prime ideals appearing in the diassembly of  $M$ . Then summarizing the above, we have

$$\text{Ass}(M) \subseteq \{P_1, \dots, P_n\} \subseteq \text{Supp}(M) = \{P \in \text{Spec}(R) \mid \text{Ann}_R(M) \subseteq P\}$$

It turns out that the minimal primes of the four sets coincide.

**Proposition 6.2.5** Let  $R$  be a Noetherian commutative ring. Let  $M$  be a finitely generated  $R$ -module. Let  $P_1, \dots, P_n \in \text{Spec}(R)$  be the prime ideals appearing in the diassembly of  $M$ . Then the following sets are equal.

- $\{P \in \text{Spec}(R) \mid P \text{ is minimal in } \text{Supp}(M)\}.$
- $\{P \in \text{Spec}(R) \mid P \text{ is minimal in } \text{Ass}(M)\}.$
- $\{P \in \text{Spec}(R) \mid P \text{ is a minimal prime ideal over } \text{Ann}_R(M)\}.$
- $\{P \in \text{Spec}(R) \mid P \text{ is minimal in } \{P_1, \dots, P_n\}\}.$

**Proof**

- (1) = (4): By the above lemma, we have

$$\text{Supp}(M) = \bigcup_{i=1}^n \{P \in \text{Spec}(R) \mid P_i \subseteq P\} = \bigcup_{P \in \{P_1, \dots, P_n\} \text{ minimal}} \{Q \in \text{Spec}(R) \mid P_k \subseteq Q\}$$

If  $P$  is minimal in  $\text{Supp}(M)$ , then it is minimal in the union. Then  $P \in \{Q \in \text{Spec}(R) \mid P_k \subseteq Q\}$  for some minimal  $P_k$ . If  $P \neq P_k$  then evidently  $P$  is not minimal, hence  $P = P_k$ . The converse is similar.

- (1) = (3): By 6.2.3,  $\text{Supp}(M) = \{P \in \text{Spec}(R) \mid \text{Ann}_R(M) \subseteq P\}$  means that  $P$  is a minimal prime ideal over  $\text{Ann}_R(M)$  if and only if  $P$  is minimal in  $\text{Supp}(M)$ .

■

### 6.3 Primary Ideals

**Definition 6.3.1 (Primary Ideals)** Let  $R$  be a commutative ring. Let  $Q$  be a proper ideal of  $R$ . We say that  $Q$  is a primary ideal of  $R$  if  $fg \in Q$  implies  $f \in Q$  or  $g^m \in Q$  for some  $m > 0$ .

**Lemma 6.3.2** Let  $R$  be a commutative ring. Let  $Q$  be an ideal of  $R$ . Then the following are true.

- If  $Q$  is a prime ideal, then  $Q$  is a primary ideal.
- If  $\sqrt{Q}$  is a maximal ideal, then  $Q$  is a primary ideal.

**Proof** Let  $fg \in Q$ . Since  $Q$  is prime,  $f \in Q$  or  $g \in Q$  and so we are done.

Let  $fg \in Q$  and  $f \notin Q$ . Let  $I = \{g \in R \mid fg \in Q\}$ . Clearly  $Q \subseteq I$ . Moreover  $1 \notin I$ . Hence  $I$  is a proper ideal. Then we have  $m = \sqrt{Q} \subseteq \sqrt{I}$ . Hence  $I \subseteq \sqrt{I} = m$  since  $m$  is maximal. This shows that  $g \in I$  implies  $g \in m = \sqrt{Q}$ . Hence we are done. ■

**Lemma 6.3.3** Let  $\phi : R \rightarrow S$  be a ring homomorphism and  $Q$  be a primary ideal in  $S$ . Then  $\phi^{-1}(Q)$  is primary in  $R$ .

**Proposition 6.3.4** Let  $R$  be a commutative ring. Let  $Q$  be a proper ideal of  $R$ . Then  $Q$  is primary if and only if every zero divisor in  $R/Q$  is nilpotent.

**Lemma 6.3.5** Let  $R$  be a commutative ring. Let  $Q$  be a primary ideal of  $R$ . Then the following are true.

- $\sqrt{Q}$  is a prime ideal.
- $\sqrt{Q}$  is minimal among primes that contain  $Q$ .

**Definition 6.3.6 (P-Primary Ideals)** Let  $R$  be a commutative ring. Let  $P$  be a prime ideal. Let  $Q$  be an ideal. We say that  $Q$  is a  $P$ -primary ideal of  $R$  if the following are true.

- $Q$  is a primary ideal.
- $\sqrt{Q} = P$ .

**Lemma 6.3.7** Let  $R$  be a commutative ring. Let  $P$  be a prime ideal. Let  $Q_1, Q_2$  be  $P$ -primary ideals. Then  $Q_1 \cap Q_2$  is a  $P$ -primary ideal.

**Proposition 6.3.8** Let  $R$  be a Noetherian commutative ring. Let  $P$  be a prime ideal of  $R$ . Let  $Q$  be a proper ideal. Then  $Q$  is  $P$ -primary if and only if  $\text{Ass}(R/Q) = \{P\}$ .



**Proof** Let  $Q$  be a  $P$ -primary ideal. We know that  $\text{Ass}(R/Q)$  is non-empty. So let  $I$  be a prime ideal such that  $I \in \text{Ass}(R/Q)$ . Clearly  $Q \subseteq I$ . There exists  $[r] \in R/Q$  where  $[r] \neq 0$  such that  $\text{Ann}_R([r]) = I$ . Let  $x \in I \setminus \{0\}$ . Then  $[xr] = [x] \cdot [r] = 0 \in R/Q$  implies that  $[x]$  is a zero divisor of  $R/Q$ . By 6.3.4, we conclude that  $[x] \in N(R/Q)$ . Then by lemma 1.4.5, we have  $x \in \sqrt{Q} = P$ . Hence we have  $Q \subseteq I \subseteq \sqrt{Q} = P$ . Taking radical gives  $I = P$  since  $I$  is a prime ideal. Hence  $\text{Ass}(R/Q) = \{P\}$ .

Now suppose that  $\text{Ass}(R/Q) = \{P\}$ . Let  $xy \in Q$ . Suppose that  $x \notin Q$ . Then we have  $[x] \cdot [y] = [xy] = 0 \in R/Q$ . Hence  $y \in \text{Ann}_R([x])$ . But we also have

$$\sqrt{\text{Ann}_R([x])} = \bigcap_{\substack{I \text{ is a minimal prime} \\ \text{ideal over } \text{Ann}_R([x])}} I = \bigcap_{\substack{I \text{ is minimal} \\ \text{in } \text{Ass}([x])}} I = P$$

Similarly, we know that

$$\sqrt{\text{Ann}_R(R/Q)} = \bigcap_{\substack{I \text{ is a minimal prime} \\ \text{ideal over } \text{Ann}_R(R/Q)}} I = \bigcap_{\substack{I \text{ is minimal} \\ \text{in } \text{Ass}(R/Q)}} I = P$$

Then  $y \in \text{Ann}_R([x])$  implies that  $y \in \sqrt{\text{Ann}_R([x])} = P = \sqrt{\text{Ann}_R(R/Q)}$ . This means that  $y^n \in \text{Ann}_R(R/Q)$  for some  $n \in \mathbb{N}$ . Hence  $y^n \in Q$ . ■

**Lemma 6.3.9** Let  $R$  be a Noetherian commutative ring. Let  $P$  be a prime ideal. Let  $Q$  be  $P$ -primary. Then we have

$$P^n \subseteq Q \subseteq P$$

for some  $n \in \mathbb{N}$ .

**Proof** Since  $R$  is Noetherian,  $P$  is finitely generated. Suppose that  $P = (f_1, \dots, f_k)$ . Since  $\sqrt{Q} = P$ , we have  $f_i^{n_i} \in Q$  for some  $n_i \in \mathbb{N}$ . Then for any monomial of degree  $m > \sum_{i=1}^k (n_i - 1)$  is a multiple of  $f_i^{n_i}$  for some  $1 \leq i \leq k$ . Hence  $P^m \subseteq Q$ . ■

**Example 6.3.10** Let  $k$  be a field. Let  $I = (x^2, xy) \subseteq k[x, y]$ . Then we have

$$(x^2) \subseteq I \subseteq (x)$$

but  $I$  is not primary. In particular, this shows that the condition in the above lemma is not a sufficient condition for ideals to be primary.

**Proof**  $I$  is not primary because  $xy \in I$  but  $x \notin I$  and  $y^n \notin I$  for any  $n \in \mathbb{N}$ . ■

**Corollary 6.3.11** Let  $R$  be a Noetherian commutative ring. Let  $m$  be a maximal ideal of  $R$ . Let  $Q$  be a proper ideal. Then the following are equivalent.

- $Q$  is  $m$ -primary.
- $\text{Ass}(R/Q) = \{m\}$
- There exists  $n \in \mathbb{N}$  such that  $m^n \subseteq Q \subseteq m$ .

**Proof** By the above proposition we have (1)  $\iff$  (2). The above lemma also shows that (1)  $\implies$  (3). Finally, suppose that  $m^n \subseteq Q \subseteq m$ . Then taking radicals give  $m = \sqrt{m^n} \subseteq \sqrt{Q} \subseteq \sqrt{m} = m$ . By 6.3.3 we conclude that  $Q$  is  $m$ -primary. ■

## 6.4 Primary Decomposition

We want to express ideal  $I$  in  $R$  as  $I = P_1^{e_1} \cdots P_n^{e_n}$  similar to a factorization of natural numbers, for some prime ideals  $P_1, \dots, P_n$ . However this notion fails and thus we have the following new type of ideal.

**Definition 6.4.1 (Primary Decompositions)** Let  $A$  be a commutative ring. Let  $I$  be an ideal of  $A$ . A primary decomposition  $I$  consists of primary ideals  $Q_1, \dots, Q_r$  of  $A$  such that

$$I = Q_1 \cap \dots \cap Q_r$$

**Example 6.4.2** Let  $k$  be a field. For any  $\alpha \in k$ , the ideal  $(x^2, xy) \subseteq k[x, y]$  has a primary decomposition given by

$$(x^2, xy) = (x) \cap (x^2, y - \alpha x)$$

**Proof** Since  $(x)$  is a prime ideal, it is a  $(x)$ -primary ideal. ■

**Definition 6.4.3 (Minimal Primary Decompositions)** Let  $A$  be a commutative ring. Let  $I$  be an ideal of  $A$ . Let

$$I = Q_1 \cap \dots \cap Q_r$$

be a primary decomposition of  $I$ . We say that the decomposition is minimal if the following are true.

- Each  $\sqrt{Q_i}$  are distinct for  $1 \leq i \leq r$
- Removing a primary ideal changes the intersection. This means that for any  $i$ ,  $I \neq \bigcap_{j \neq i} Q_j$

**Theorem 6.4.4** Let  $R$  be a Noetherian commutative ring. Let  $I$  be a proper ideal of  $R$ . Then  $I$  admits a minimal primary decomposition.

**Definition 6.4.5 (Prime Divisors of an Ideal)** Let  $R$  be a commutative ring. Let  $I$  be an ideal of  $R$ . We say that a prime ideal  $P$  of  $R$  is a prime divisor of  $I$  if  $P = \sqrt{Q}$  for some ideal  $Q$  that lies in a minimal primary decomposition of  $I$ .

## 6.5 The Two Uniqueness Theorems

**Theorem 6.5.1 (First Uniqueness Theorem)**

Let  $R$  be a Noetherian commutative ring. Let  $I$  be an ideal of  $R$ . Let

$$I = \bigcap_{i=1}^k Q_i$$

be a minimal primary decomposition of  $I$ , where each  $Q_i$  is  $P_i$ -primary. Then we have

$$\text{Ass}(R/I) = \{P_1, \dots, P_k\}$$

Moreover,  $\text{Ass}(R/I)$  is unique.

**Theorem 6.5.2 (Second Uniqueness Theorem)**

Let  $R$  be a Noetherian commutative ring. Let  $I$  be an ideal of  $R$ . Let

$$I = \bigcap_{i=1}^k Q_i$$

be a minimal primary decomposition of  $I$ , where each  $Q_i$  is  $P_i$ -primary. Let  $P$  be a minimal element of  $\text{Ass}(R/I) = \{P_1, \dots, P_n\}$ . Let  $\varphi : R \rightarrow R_P$  be the localization map. Then we have

$$Q_i = \varphi^{-1}(I_P)$$

Moreover, the primary decomposition is uniquely determined by the minimal  $P$  in  $\text{Ass}(R/I)$ .

## 6.6 Symbolic Powers

**Definition 6.6.1** (Symbolic Powers)

Let  $R$  be a Noetherian commutative ring. Denote  $\varphi : R \rightarrow R_P$  the localization map with respect to the prime ideal  $P$ . Let  $I$  be an ideal of  $R$ . Define the  $n$ th symbolic power of  $I$  to be

$$I^{(n)} = \bigcap_{P \in \text{Ass}(R/I)} \varphi^{-1}(I^n R_P)$$

## 7 Integral Dependence

### 7.1 Integral Elements

**Definition 7.1.1 (Integral Elements)** Let  $B$  be a commutative ring and let  $A \subseteq B$  be a subring. Let  $b \in B$ . We say that  $b$  is integral over  $A$  if there exists a monic polynomial  $p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in A[x]$  such that  $p(b) = 0$ .

When  $A$  and  $B$  are field, this is a familiar notion in Field and Galois theory.

**Lemma 7.1.2** Let  $K$  be a field. Let  $F \subseteq K$  be a subfield. Let  $k \in K$ . Then  $k$  is integral over  $F$  if and only if  $k$  is algebraic over  $F$ .

**Proposition 7.1.3** Let  $B$  be a commutative ring and let  $A \subseteq B$ . Let  $b \in B$ . Then the following are equivalent.

- $b$  is integral over  $A$
- $A[b] \subseteq B$  is finitely generated  $A$ -submodule.
- There exists an  $A$  sub-algebra  $A' \subseteq B$  such that  $A[b] \subseteq A'$  and  $A'$  is finitely generated as an  $A$ -module.

**Proof**

- (1)  $\implies$  (2): Since  $b$  is integral over  $A$ ,  $b^n = a_{n-1}b^{n-1} + \cdots + a_1b + a_0$ . Hence  $A[b] = \bigoplus_{i=0}^{n-1} A \cdot b^i$  is a finitely generated  $A$ -module.
- (2)  $\implies$  (3): Choose  $A' = A[b]$ .
- (3)  $\implies$  (1). By assumption,  $A'$  is a finitely generated  $A$ -module. Let  $\phi : A' \rightarrow A'$  be the ring homomorphism defined by  $\phi(x) = bx$ . By Cayley-Hamilton theorem, there exists  $a_1, \dots, a_{n-1} \in A$  such that

$$\phi^n + a_{n-1}\phi^{n-1} + \cdots + a_1\phi + a_0 = 0$$

Since  $\phi$  is the multiplication by  $b$  map, we have

$$(b^n + a_{n-1}b^{n-1} + \cdots + a_1b + a_0)(y) = 0$$

for all  $y \in A'$ . Choosing  $y = 1$ , we see that  $b$  is integral over  $A$ . ■

**Lemma 7.1.4** Let  $A \subseteq B$  be commutative rings. Then  $B$  is a finitely generated  $A$ -module if and only if  $B = A[x_1, \dots, x_n]$  for some  $x_1, \dots, x_n \in B$  that is integral over  $A$ .

**Proof** Induct on  $n$  and use the fact that  $x_i$  is integral over  $A$  if and only if  $A[x_i]$  is a finitely generated  $A$ -module, and the fact that  $x_i$  is integral over  $A[x_1, \dots, x_{i-1}]$ . ■

**Proposition 7.1.5** Let  $B$  be a commutative ring and let  $A \subseteq B$  be a subring. Let  $b_1, b_2 \in B$  be integral over  $A$ . Then  $b_1 + b_2$  and  $b_1b_2$  are both integral over  $A$ .

### 7.2 Integral Closure

**Definition 7.2.1 (Integral Closure)** Let  $B$  be a commutative ring. Let  $A \subseteq B$  be a subring. Define the subring

$$\overline{A} = \{b \in B \mid b \text{ is integral over } A\}$$

to be the integral closure of  $A$  in  $B$ .

**Example 7.2.2** The integral closure of  $\mathbb{Z} \subseteq \mathbb{Q}$  is  $\mathbb{Z}$ .

**Proposition 7.2.3** Let  $B$  be a commutative ring. Let  $A \subseteq B$  be a subring. Let  $S$  be a multiplicatively closed subset of  $A$ . Then

$$\overline{S^{-1}A} = S^{-1}\overline{A}$$

**Definition 7.2.4 (Integral Extensions)** Let  $B$  be a commutative ring and let  $A \subseteq B$  be a subring. We say that  $B$  is integral over  $A$  if  $\overline{A} = B$ . We also say that  $B$  is the integral extension of  $A$ .

**Lemma 7.2.5** Let  $A \subseteq B \subseteq C$  be commutative rings. Then  $C$  is integral over  $B$  and  $B$  is integral over  $A$  if and only if  $C$  is integral over  $A$ .

**Proposition 7.2.6** Let  $A, B$  be commutative rings such that  $A \subset B$  is an integral extension. Then the following are true.

- Let  $J$  be an ideal of  $B$ . Then  $\frac{B}{J}$  is integral over  $\frac{A}{J \cap A}$ .
- Let  $S$  be a multiplicative subset of  $B$ . Then  $S^{-1}B$  is integral over  $S^{-1}A$ .

**Proof** Suppose that  $J$  is an ideal of  $B$ . Let  $b + J \in B/J$ . Since  $b \in B$  and  $B$  is integral over  $A$ , there exists  $a_0, \dots, a_{n-1} \in A$  such that

$$b^n + a_{n-1}b^{n-1} + \dots + a_1b + a_0 = 0$$

Reduction to  $J$  gives

$$(b + J)^n + (a_{n-1} + J)(b + J)^{n-1} + \dots + (a_1 + J)(b + J) + (a_0 + J) = J$$

This shows that  $b + J$  is an integral element of  $A/J \cap A$  because each  $a_i + J$  is an element of  $A/J \cap A$  by restriction to  $A$ .

Let  $b/s \in S^{-1}B$ . Since  $B$  is integral over  $A$ , there exists  $a_0, \dots, a_{n-1} \in A$  such that

$$b^n + a_{n-1}b^{n-1} + \dots + a_1b + a_0 = 0$$

Dividing  $s^n$  on both sides give

$$\frac{b^n}{s^n} + \frac{a_{n-1}}{s} \frac{b^{n-1}}{s^{n-1}} + \dots + \frac{a_1}{s^{n-1}} \frac{b}{s} + \frac{a_0}{s^n} = 0$$

This shows that  $b/s$  is an integral element of  $S^{-1}A$ . ■

**Lemma 7.2.7** Let  $A, B$  be integral domains such that  $A \subset B$  is an integral extension. Then  $A$  is a field if and only if  $B$  is a field.

**Proof** Suppose that  $A$  is a field. Let  $0 \neq b \in B$ . Then there exists  $a_0, \dots, a_{n-1} \in A$  such that

$$b^n + a_{n-1}b^{n-1} + \dots + a_1b + a_0 = 0$$

for smallest of such  $n \in \mathbb{N}$ . Rearranging gives

$$b(b^{n-1} + a_{n-1}b^{n-2} + \dots + a_1) = -a_0$$

Notice that  $a_0 \neq 0$  because otherwise it contradicts the minimality of  $n$ . Since  $A$  is a field, we can

divide  $-a_0 \neq 0$  on both sides to find an inverse of  $b$ . Hence  $B$  is a field.

Now assume that  $B$  is a field. Let  $0 \neq a \in A$ . Since  $B$  is a field,  $a^{-1} \in B$  is such that there exists  $a_0, \dots, a_{n-1} \in A$  such that

$$a^{-n} + a_{n-1}a^{-(n-1)} + \dots + a_1a^{-1} + a_0 = 0$$

Multiplying  $a^{n-1}$  on both sides and rearranging, we get

$$a^{-1} = -(a_{n-1} + \dots + a_1a^{n-2} + a_0a^{n-1})$$

This shows that  $a^{-1} \in A$ . Hence  $A$  is a field. ■

**Definition 7.2.8 (Integrally Closed)** Let  $B$  be a commutative ring. Let  $A \subseteq B$  be a subring. We say that  $A$  is integrally closed in  $B$  if  $\bar{A} = A$ .

**Theorem 7.2.9 (Gauss's Lemma)** Let  $B$  be a commutative ring. Let  $A \subseteq B$  be a subring. Suppose that  $A$  is integrally closed in  $B$ . Then the following are true.

- If  $f, g \in B[x]$  are monic polynomials such that  $fg \in A[x]$ , then  $f, g \in A[x]$ .
- If  $f \in A[x]$  is irreducible, then  $f$  is irreducible as a polynomial in  $B[x]$ .

**Proof** Clearly the first statement implies the second. We first prove that for any monic polynomial  $f \in B[x]$ , there exists a ring  $C$  such that  $B \subseteq C$  and  $f$  factorizes as a product of linear terms in  $C[x]$ . To show this, we induct on  $n$ . If  $n = 1$  then we are done. Suppose that the hypothesis is true for some  $k \in \mathbb{N}$ . Suppose that  $\deg(f) = k + 1$ . ■

### 7.3 Four Main Theorems of Integral Extensions

We want to compare prime ideals between integral extensions.

**Lemma 7.3.1** Let  $A, B$  be rings such that  $A \subset B$  is an integral extension. Let  $Q$  be a prime ideal of  $B$ . Then  $Q \cap A$  is a maximal ideal of  $A$  if and only if  $Q$  is a maximal ideal of  $B$ .

**Proof** By 7.2.6, we know that  $B/Q$  is integral over  $A/Q \cap A$ . By 7.2.7,  $B/Q$  is a field if and only if  $A/Q \cap A$  is a field. Hence  $Q$  is a maximal ideal of  $B$  if and only if  $Q \cap A$  is a maximal ideal of  $A$ . ■

**Theorem 7.3.2 (The Lying Over Theorem)**

Let  $A, B$  be rings such that  $A \subset B$  is an integral extension. Let  $P$  be a prime ideal of  $A$ . Then there exists a prime ideal  $Q$  of  $B$  such that  $P = Q \cap A$ .

**Proof**

Let  $\alpha : A \rightarrow A_P$  and  $\beta : B \rightarrow B_P$  be the localization maps. Consider the following commutative diagram.

$$\begin{array}{ccc} A & \hookrightarrow & B \\ \alpha \downarrow & & \downarrow \beta \\ A_P & \hookrightarrow & B_P \end{array}$$

Since  $PB_P$  is the unique maximal ideal of  $B_P$ , we know that  $PA_P = PB_P \cap A_P$  is the unique maximal ideal of  $A_P$ . On the other hand, we also know that  $\beta^{-1}(PB_P)$  is a prime ideal of  $B$ . By commutativity of the diagram, we have that  $P$  is mapped to  $\beta^{-1}(PB_P)$ . Then by definition of extension we have that  $\beta^{-1}(PB_P) \cap A = P$ . ■

**Theorem 7.3.3 (The Incomparability Theorem)** Let  $A, B$  be rings such that  $A \subset B$  is an integral extension. If  $Q_1 \neq Q_2$  are distinct prime ideals of  $B$  such that  $Q_1 \cap A = P = Q_2 \cap A$ , then  $Q_1 \not\subseteq Q_2$  and  $Q_2 \not\subseteq Q_1$ .

**Proof**

We prove the contrapositive statement. That is, if  $Q_1, Q_2$  are prime ideals of  $B$  such that  $Q_1 \cap A = P = Q_2 \cap B$  and  $Q_1 \subseteq Q_2$ , then  $Q_1 = Q_2$ .

Let  $\alpha : A \rightarrow A_P$  and  $\beta : B \rightarrow B_P$  be the localization maps. Consider the following commutative diagram.

$$\begin{array}{ccc} A & \hookrightarrow & B \\ \alpha \downarrow & & \downarrow \beta \\ A_P & \hookrightarrow & B_P \end{array}$$

Since  $PB_P$  is the unique maximal ideal of  $B_P$ , we know that  $PA_P = PB_P \cap A_P$  is the unique maximal ideal of  $A_P$ . On the other hand, we also know that  $\beta^{-1}(PB_P)$  is a prime ideal of  $B$ . By commutativity of the diagram, we have that  $P$  is mapped to  $\beta^{-1}(PB_P)$ . Then by definition of extension we have that  $\beta^{-1}(PB_P) \cap B = P$ .

Let  $Q_1, Q_2$  be as given. We have that

$$(Q_1 \cap A)A_P = PA_P = (Q_2 \cap A)A_P$$

is the same maximal ideal of  $A_P$  since they both contract to  $P$  in  $A$ . By the above lemma,  $(Q_1 \cap A)B_P$  and  $(Q_2 \cap A)B_P$  are both maximal ideals of  $B_P$ . By commutativity of the diagram,  $(Q_1 \cap A)B_P = Q_1B_P$  and  $(Q_2 \cap A)B_P = Q_2B_P$ . Since  $Q_1 \subseteq Q_2$ , we have that  $Q_1B_P \subseteq Q_2B_P$ . Since  $Q_1B_P$  and  $Q_2B_P$  are both maximal ideals, they must be equal. Hence by contraction we deduce that  $Q_1 = Q_2$ . ■

**Theorem 7.3.4 (The Going-Up Theorem)** Let  $A, B$  be commutative rings such that  $A \subset B$  is an integral extension. Let  $0 \leq m < n$ . Consider the following situation

$$\begin{array}{ccc} B & Q_1 \subseteq \cdots \subseteq Q_m & \text{(Prime ideals of } B) \\ \uparrow & & \\ A & P_1 \subseteq \cdots \subseteq P_m \subseteq P_{m+1} \subseteq \cdots \subseteq P_n & \text{(Prime ideals of } A) \end{array}$$

where  $Q_i \cap A = P_i$  for  $1 \leq i \leq m$ . Then there exists prime ideals  $Q_{m+1}, \dots, Q_n$  of  $B$  such that the following are true.

- $Q_{m+1} \subseteq \cdots \subseteq Q_n$
- $Q_i \cap A = P_i$  for  $m+1 \leq i \leq n$

Moreover, if the chain of prime ideals of  $A$  is strictly increasing the new chain of prime ideals in  $B$  is strictly increasing.

**Proof** By induction, it suffices to prove the case  $m = 1$  and  $n = 2$ . This means that we want to find a prime ideal  $Q_2$  such that  $Q_1 \subseteq Q_2$  and  $Q_2 \cap A = P_2$ . By 7.2.6,  $B/Q_1$  is integral over  $A/P_1$ . Since  $P_2/P_1$  is a prime in  $A/P_1$  by the correspondence theorem, by 7.3.2 there exists a prime ideal  $Q_2/Q_1$  in  $B/Q_1$  such that  $Q_2/Q_1 \cap A/P_1 = P_2/P_1$ . This implies that  $Q_2 \cap A = P_2$ .

Finally, suppose that the chain of prime ideals in  $A$  is strictly increasing. Suppose for a contradiction that  $Q_i = Q_{i+1}$ . Then we must have  $P_i = Q_i \cap A = Q_{i+1} \cap A = P_{i+1}$ , a contradiction. ■

## 7.4 Zariski's Lemma

**Lemma 7.4.1** Let  $F$  be a field. Let  $f \in F[x]$  be a polynomial. Then the localization  $F[x]_f$  is not a field.

**Proof** By 1.8.1,  $F[x]$  has infinitely many irreducible polynomials. Then there exists a monic irreducible polynomial  $g$  that does not divide  $f$ . Assume for a contradiction that  $F[x]_f$  is a field. Then  $g/1$  is invertible. So there exists  $h \in F[x]$  and  $n \in \mathbb{N}$  such that  $1 = g \cdot \frac{h}{f^n}$ . This means that

there exists  $m \in \mathbb{N}$  such that  $ghf^m = f^{n+m} \in F[x]$ . If  $n + m = 0$ , then  $g$  is a unit, a contradiction. Otherwise,  $g$  divides  $f^{n+m}$ . Since  $g$  is irreducible,  $g$  divides  $f$  and is also a contradiction. Hence  $F[x]_f$  is not a field. ■

**Theorem 7.4.2 (Zariski's Lemma)** Let  $F$  be a field. Let  $K/F$  be a field extension. Then  $K/F$  is a finite field extension if and only if  $K$  is finitely generated as an  $F$ -algebra.

**Proof** Since  $K$  is finitely generated as an  $F$ -algebra, there exists  $x_1, \dots, x_n \in K$  such that every element in  $K$  can be written as a polynomial in  $x_1, \dots, x_n$ . This means that  $K = F(x_1, \dots, x_n)$  as fields. Suppose for a contradiction that  $K/F$  is not an algebraic (integral) extension. Without loss of generality, suppose that  $F(x_1, \dots, x_r)/F$  is transcendental (not integral) and  $K/F(x_1, \dots, x_r)$  is algebraic (integral).

Let  $L = F(x_1, \dots, x_{r-1})$ . Consider the transcendental (not integral) extension  $L(x_r)/L$ . Now  $K$  is generated as an  $L$ -algebra by the elements  $x_1, \dots, x_n$ . Since  $K/L(x_r)$  is integral, there exists monic polynomials  $p_i \in L(x_r)[y]$  such that  $p_i(x_i) = 0$ . Since  $L(x_r)$  is the field of fractions of the polynomial ring  $L[x_r]$ , each coefficient of  $p_i$  can be expressed as a fraction  $g/h$  for  $g, h \in L(x_r)$  and  $h \neq 0$ . Let  $f$  be the product of all denominators of the coefficient of  $p_i$  for all  $i$ . Then  $p_i \in L[x_r]_f[y]$ . So every  $x_1, \dots, x_n$  satisfies a monic polynomial with coefficients in  $L[x_r]_f$ . Hence the  $L[x_r]_f$  subalgebra of  $K$  generated by  $x_1, \dots, x_n$  is integral over  $L[x_r]_f$ . By 7.2.7,  $L[x_r]_f$  is a field. This is a contradiction to the above lemma. Hence we are done. ■

There is a correspondence between the different terms used in Field and Galois Theory and Commutative Algebra

Field Extension $K/F$	$B$ an $A$ -algebra
$x \in K$ is algebraic	$b \in B$ is integral
$K/F$ is an algebraic extension	$A \subseteq B$ is an integral extension
The algebraic closure $F < \bar{F} < K$	The integral closure $A \subseteq \bar{A} \subseteq B$
$K/F$ is a finite extension	$S$ is a finitely generated $R$ -algebra

**Corollary 7.4.3** Let  $F$  be an algebraically closed field. Let  $K$  be a field that is also a finitely generated algebra over  $F$ . Then  $K = F$ .

**Proof** By Zariski's lemma,  $K/F$  is a finite field extension. Let  $x \in K$ . Let  $f$  be the minimal polynomial of  $x$ . Since  $F$  is algebraically closed,  $f$  is linear. Hence  $x \in F$ . ■

**Corollary 7.4.4** Let  $F$  be an algebraically closed field. Then we have

$$\max\text{Spec}(F[x_1, \dots, x_n]) = \{(x_1 - a_1, \dots, x_n - a_n) \mid (a_1, \dots, a_n) \in F^n\}$$

**Proof** Let  $m$  be a maximal ideal of  $F[x_1, \dots, x_n]$ . Then  $F[x_1, \dots, x_n]/m$  is a finitely generated  $F$ -algebra that is a field. By the above, we have that  $F[x_1, \dots, x_n]/m \cong F$ . Then there exists  $a_i \in F$  such that  $a_i$  corresponds to  $x_i + m$  by the isomorphism. This means that  $a_i + m = x_i + m$ , or  $(x_i - a_i) \in m$ . Hence  $(x_1 - a_1, \dots, x_n - a_n) \subseteq m$ . Since  $(x_1 - a_1, \dots, x_n - a_n)$  is maximal by the evaluation homomorphism, we conclude that  $m = (x_1 - a_1, \dots, x_n - a_n)$ . ■

## 7.5 Normal Domains

We now concern ourselves with integral domains. Let  $R$  be an integral domain. A special fact about  $R$  is that the canonical homomorphism  $R \rightarrow R_{(0)} = \text{Frac}(R)$  is an injection. This means that we can think of  $R$  as living inside of  $\text{Frac}(R)$  while preserving all the structure of  $R$ .

**Definition 7.5.1 (Normal Domains)** Let  $R$  be an integral domain. We say that  $R$  is normal if  $R$  is integrally closed in  $\text{Frac}(R)$ .



**Proposition 7.5.2** Let  $R$  be a normal domain. Let  $S$  be a multiplicative subset of  $R$ . Then  $S^{-1}R$  is a normal domain.

**Proof** We want to show that  $S^{-1}R$  is integrally closed in  $\text{Frac}(R) = \text{Frac}(S^{-1}R)$ . This means that we want to show  $\overline{S^{-1}R} = S^{-1}R$ . It is clear that  $S^{-1}R \subseteq \overline{S^{-1}R}$ . So let  $g \in \overline{S^{-1}R}$ . Suppose that  $p(x) = x^n + \sum_{k=0}^{n-1} a_k x^k \in (S^{-1}R)[x]$  such that  $p(g) = 0$ . Choose  $s \in S$  such that  $sa_i \in R$  for  $0 \leq i \leq n-1$ . Then notice that  $sg \in S^{-1}R$  satisfies the monic polynomial

$$q(x) = x^n + \sum_{k=0}^{n-1} s^{n-k} a_k x^k$$

since  $q(sg) = s^n g^n + \sum_{k=0}^{n-1} s^n a_k x^k = s^n p(g) = 0$ . But  $q$  is a polynomial in  $R$  since  $s^{n-k} a_k \in R$ . Thus we have that  $sg \in \overline{R} = R$  since  $R$  is normal. This means that  $g \in S^{-1}R$  and hence we conclude. ■

**Proposition 7.5.3** Let  $R$  be a commutative ring. If  $R$  is a UFD, then  $R$  is normal.

**Proof** Let  $a/b \in \text{Frac}(R)$  that is integral. Assume that  $a, b$  do not have common factors. Then there exists  $r_0, \dots, r_{n-1} \in R$  such that

$$\frac{a^n}{b^n} + r_{n-1} \frac{a^{n-1}}{b^{n-1}} + \dots + r_1 \frac{a}{b} + r_0 = 0$$

Rearranging, we get

$$a^n = -b(r_{n-1}a^{n-1} + \dots + r_1a^{n-2} + r_0b^{n-1})$$

This shows that any irreducible element dividing  $b$  also divides  $a^n$ , and hence  $a$ . Since  $a$  and  $b$  do not have common factors, this means that no irreducible element divides  $b$ . Since  $R$  is a UFD,  $b$  must be a unit. Hence  $a/b \in R$ . ■

**Example 7.5.4** The integral closure of  $\mathbb{Z}$  in  $\mathbb{Q}[i]$  is  $\mathbb{Z}[i]$ .

**Proof** If  $a+bi \in \mathbb{Z}[i]$ , then  $p(x) = x^2 - 2ax + a^2 + b^2$  is a monic polynomial such that  $p(a+bi) = 0$ . Conversely, let  $z \in \mathbb{Q}[i]$  lie in the integral closure of  $\mathbb{Z}$ . Then  $z$  is also an integral element of  $\mathbb{Z}[i]$ . Since  $\mathbb{Z}[i]$  is a UFD,  $\mathbb{Z}[i]$  is a normal domain and so is integrally closed in  $\text{Frac}(\mathbb{Z}[i]) = \mathbb{Q}[i]$ . So  $z \in \overline{\mathbb{Z}[i]} = \mathbb{Z}[i]$  shows that  $\overline{\mathbb{Z}} \subseteq \mathbb{Z}[i]$ . ■

**Proposition 7.5.5 (Normal is a Local Property)** Let  $R$  be an integral domain. Then the following are equivalent.

- $R$  is normal
- $R_P$  is normal for all prime ideals  $P$
- $R_m$  is normal for all maximal ideals  $m$ .

**Proof** Notice that an integral domain  $R$  is normal if and only if the canonical inclusion map  $R \hookrightarrow \overline{R}$  is surjective. Since surjectivity is a local property, this map is surjective if and only if for all prime ideals  $P$  of  $R$ ,  $R_P \hookrightarrow \overline{R}_P$  is surjective. But  $\overline{R}_P = \overline{R_P}$  by the above. Hence  $R \hookrightarrow \overline{R}$  is surjective if and only if  $R_P \rightarrow \overline{R_P}$  is surjective. Hence  $R$  is normal if and only if  $R_P$  is normal for all prime ideals  $P$  of  $R$ . The similar holds for all maximal ideals. ■

Atiyah-Macdonald

**Proposition 7.5.6** Let  $R$  be a normal domain. Then  $R[x]$  is a normal domain.

**Proposition 7.5.7** Let  $R$  be a normal domain. Let  $\text{Frac}(R) < K$  be an algebraic extension. Let  $a \in K$ . Then  $a$  is integral over  $R$  if and only if the minimal polynomial  $\min(\text{Frac}(R), a) \in R[x]$ .

**Proof** Suppose that  $\min(\text{Frac}(R), a) \in R[x]$ . Then  $\min(\text{Frac}(R), a)(a) = 0$  and  $\min(\text{Frac}(R), a)$  is monic by definition. Hence  $a$  is integral over  $R$ .

Now suppose that  $a \in K$  is integral over  $R$ . Let  $\overline{K}$  be the algebraic closure of  $K$ . Then  $\min(\text{Frac}(R), a)$  splits into monic irreducible polynomials

$$\min(\text{Frac}(R), a)(x) = (x - a_1) \cdots (x - a_n) \in \overline{K}[x]$$

for  $a_1, \dots, a_n \in \overline{K}$ . Since  $a$  is integral over  $R$ , there exists a monic polynomial  $g \in R[x]$  such that  $g(a) = 0$ . By definition of the minimal polynomial, we have  $\min(\text{Frac}(R), a)$  divides  $g$ . Hence  $g(a_i) = 0$  for each  $i$  and that  $a_1, \dots, a_n$  are integral over  $R$ . Now the coefficients of  $\min(\text{Frac}(R), a)$  are sums and products of  $a_1, \dots, a_n$ , and hence are also integral over  $R$ . But  $R$  is a normal domain so the coefficients of  $\min(\text{Frac}(R), a)$  lie in  $R$ . ■

## 8 Introduction to Dimension Theory for Rings

### 8.1 Krull Dimension

**Definition 8.1.1 (Krull Dimension)** Let  $R$  be a commutative ring. Define the Krull dimension of  $R$  to be

$$\dim(R) = \max\{t \in \mathbb{N} \mid p_0 \subset \cdots \subset p_t \text{ for } p_0, \dots, p_t \text{ prime ideals}\}$$

In particular, notice that a commutative ring  $R$  has  $\dim(R) = 0$  if and only if every prime ideal is maximal.

**Lemma 8.1.2** Let  $R$  be a commutative ring. Let  $I$  be an ideal of  $R$ . Then we have  $\dim(R) \geq \dim(R/I)$ .

**Lemma 8.1.3**

Let  $R, S$  be commutative rings such that  $R \subseteq S$  is an integral extension. Then we have

$$\dim(R) = \dim(S)$$

**Proof** Let  $P_0 \subset \cdots \subset P_n$  be a strictly increasing chain of prime ideals of  $R$ . By the going up theorem, we obtain an increasing chain of prime ideals  $Q_0 \subseteq \cdots \subseteq Q_n$  in  $S$ . Hence  $\dim(R) \leq \dim(S)$ .

Conversely, suppose that  $Q_0 \subset \cdots \subset Q_n$  is a strictly increasing chain of prime ideals in  $S$ . Then  $\varphi^{-1}(Q_0) \subset \cdots \subset \varphi^{-1}(Q_n)$  is an increasing chain of prime ideals of  $R$ . Hence  $\dim(S) \leq \dim(R)$ . ■

**Lemma 8.1.4** Let  $R$  be a commutative ring. Then the following are true.

- If  $R$  is a field, then  $\dim(R) = 0$
- If  $R$  is Artinian, then  $\dim(R) = 0$

**Proof** Let  $R$  be a field. Then the only proper prime ideal of  $R$  is  $(0)$ . In particular,  $(0)$  forms the only chain of prime ideals in  $R$ . Hence  $\dim(R) = 0$ .

Now let  $R$  be Artinian. Let  $P$  be a prime ideal of  $R$ . Then  $R/P$  is an integral domain. Moreover, every quotient of an Artinian ring is Artinian. Hence  $R/P$  is Artinian. By prp1.3.1, we conclude that  $R/P$  is a field. Hence  $P$  is a maximal ideal. Any chain of prime ideals of  $R$  must terminate at the first prime ideal since it is maximal. Hence  $\dim(R) = 0$ . ■

**Definition 8.1.5 (Dimension of Modules)** Let  $R$  be a commutative ring. Let  $M$  be an  $R$ -module. Define the dimension of  $M$  to be

$$\dim(M) = \dim\left(\frac{R}{\text{Ann}_R(M)}\right)$$

**Proposition 8.1.6**

Let  $R$  be a commutative ring. Let  $M$  be an  $R$ -module. Then we have

$$\dim(M) = \sup\{\dim(R/P) \mid P \in \text{Ass}(M)\}$$

**Proof** We know that the set of all minimal prime ideals of  $\text{Ass}(M)$  is equal to the set of all minimal prime ideals over  $\text{Ann}_R(M)$  by 6.2.5. Any maximal chain of prime ideals over  $\text{Ann}_R(M)$  must also start at one of these minimal prime ideals. Hence by the correspondence theorem we have  $\sup\{\dim(R/P) \mid P \in \text{Ass}(M)\} = \dim(R/\text{Ann}_R(M))$ . ■

## 8.2 Noether Normalization Lemma

### Lemma 8.2.1

Let  $k$  be a field. Let  $T$  be a finite set of monomials in  $k[x_1, \dots, x_n]$ . Then there exists  $w_1, \dots, w_{n-1}$  such that for any two  $a_{k_1, \dots, k_n} x_1^{k_1} \cdots x_n^{k_n}, b_{r_1, \dots, r_n} x_1^{r_1} \cdots x_n^{r_n} \in T$ ,  $(k_1, \dots, k_n) \neq (r_1, \dots, r_n)$  implies that

$$\sum_{i=1}^{n-1} w_i k_i + k_n \neq \sum_{i=1}^{n-1} w_i r_i + r_n$$

**Proof** We induct on  $n$ . When  $n = 1$  then we are done. When  $n \geq 2$ , we can write each monomial in  $T$  as a monomial in  $x_2, \dots, x_n$  to apply the inductive hypothesis and obtain  $w_2, \dots, w_n$ . Then set  $w_1 > \max\{\sum_{i=2}^{n-1} w_i k_i + k_n \mid (k_1, \dots, k_n) \text{ represents a monomial in } T\}$ . For  $(k_1, \dots, k_n) \neq (r_1, \dots, r_n)$  there are two cases. If  $(k_2, \dots, k_n) \neq (r_2, \dots, r_n)$ , then by inductive hypothesis we have  $\sum_{i=2}^{n-1} w_i k_i + k_{n-1} \neq \sum_{i=2}^{n-1} w_i r_i + r_{n-1}$ . Since  $w_1$  is larger than these two numbers, we must have that  $\sum_{i=1}^{n-1} w_i k_i + k_n \neq \sum_{i=1}^{n-1} w_i r_i + r_n$ . Otherwise, if  $(k_2, \dots, k_n) = (r_2, \dots, r_n)$  but  $k_1 \neq r_1$ , then  $w_1 k_1 \neq w_1 r_1$  and so we are done. ■

### Theorem 8.2.2 (Noether Normalization Lemma)

Let  $k$  be a field. Let  $R$  be a finitely generated  $k$ -algebra with the isomorphism  $R \cong \frac{k[x_1, \dots, x_n]}{I}$  for some ideal  $I$ . Then there exists  $y_1, \dots, y_d \in R$  for some  $0 \leq d \leq n$  such that the following are true.

- $y_1, \dots, y_d$  are algebraically independent.
- $R$  is finitely generated over  $k[y_1, \dots, y_d]$ .
- $d = \dim(R)$ .

### Proof

Since  $R$  is a finitely generated  $k$ -algebra, we have  $R \cong \frac{k[x_1, \dots, x_n]}{I}$  for some  $n \in \mathbb{N}$  and some ideal  $I$ . We induct on  $n$ . When  $n = 1$ , we have  $R \cong \frac{k[x]}{I}$ . Since  $k[x]$  is a PID,  $I = (f)$  for some  $f \in k[x]$ . If  $f = 0$ , then we are done. So suppose that  $f \neq 0$ . Then  $R$  is generated as a  $k$ -vector space by  $1, x, \dots, x^{\deg(f)-1}$ . Thus  $R$  is finitely generated over  $k[x]$ .

Now suppose that  $n \geq 2$ . If each  $x_1, \dots, x_n$  are algebraically independent then we are done. So suppose not. Then I claim that there is a  $k$ -subalgebra  $S$  of  $R$  generated by  $n - 1$  elements such that  $R$  is finitely generated over  $S$ . Since  $x_1, \dots, x_n$  are not algebraically independent, there exists a polynomial in  $k$  such that  $f(x_1, \dots, x_n) = 0$ . For  $r_1, \dots, r_{n-1} \in \mathbb{N}$ , write  $z_i = x_i - x_n^{r_i}$ . Then we have

$$f(z_1 + x_n^{r_1}, \dots, z_{n-1} + x_n^{r_{n-1}}, x_n) = 0$$

If the polynomial  $f$  has coefficients  $a_{k_1, \dots, k_n}$ , then expanding out the expression, we have

$$\sum a_{k_1, \dots, k_n} \prod_{i=1}^{n-1} (z_i + x_n^{r_i})^{k_i} x_n^{k_n} = 0$$

Each term in the summand has a unique term with highest order of  $x_n$  after expanding, which is given by  $a_{k_1, \dots, k_n} x_n^{\sum_{i=1}^{n-1} r_i k_i + k_n}$ . By the above lemma, we can find  $r_1, \dots, r_{n-1}$  such that  $(k_1, \dots, k_n) \neq (j_1, \dots, j_n)$  implies that  $\sum_{i=1}^{n-1} r_i k_i + k_n \neq \sum_{i=1}^{n-1} r_i j_i + j_n$ . Then this means that there is a unique term that achieves the maximum of  $\sum_{i=1}^{n-1} r_i k_i + k_n$ . This proves that the highest term of  $f$  as a polynomial in  $x_n$  has coefficient  $a_{k_1, \dots, k_n}$  for some  $k_1, \dots, k_n$ . Dividing out  $f$  by this coefficient, we deduce that  $x_n$  is an integral element over  $k[z_1, \dots, z_{n-1}]$ . This proves that  $S = k[z_1, \dots, z_{n-1}]$  is a  $k$ -subalgebra of  $R$  such that  $R$  is finitely generated over  $S$ .

By the inductive hypothesis, there exists  $y_1, \dots, y_d$  for some  $0 \leq d \leq n - 1$  such that  $y_1, \dots, y_d$  are algebraically independent and  $S$  is finitely generated over  $k[y_1, \dots, y_d]$ . Since  $R$  is finitely generated over  $S$  and  $S$  is finitely generated over  $k[y_1, \dots, y_d]$ , we conclude that  $R$  is finitely generated over  $k[y_1, \dots, y_d]$ .

It remains to show that  $d = \dim(R)$ . Since  $R$  is integral over  $S = k[y_1, \dots, y_d]$ , we have  $\dim(R) =$

$\dim(S)$  and so it suffices to show that  $d = \dim(S)$ . We induct on  $d$ . When  $d = 0$ , then  $S = k$  and so  $\dim(S) = 0$ . Now let  $d > 0$ . Then  $0 \subset (y_1) \subset (y_1, y_2) \subset \cdots \subset (y_1, \dots, y_d)$  is a chain of prime ideals in  $S$  so that  $d \leq \dim(S)$ . Conversely, suppose that  $0 \subset P_1 \subset \cdots \subset P_n$  is a strictly increasing chain of prime ideals in  $S$ . Let  $0 \neq u \in P_1$ . By the Noether normalization lemma, because first variable is always trivially algebraically independent, there exists  $t_2, \dots, t_d \in S$  such that  $S$  is integral over  $T = k[u, t_2, \dots, t_d]$ . By the inductive hypothesis, we have  $d - 1 = \dim(T/(u))$ . By the going up theorem,  $0 \subset P_1 \cap T \subset \cdots \subset P_n \cap T$  is a strictly increasing chain of prime ideals in  $T$ . Then in  $T/(P_1 \cap T)$  the chain becomes a strictly increasing chain of prime ideals of length  $n - 1$ . Since  $\dim(T/(P_1 \cap T)) \leq \dim(T/(u))$ , we have that  $n - 1 \leq d - 1$  and hence  $\dim(S) \leq d$ . ■

### Proposition 8.2.3

Let  $k$  be a field. Let  $R$  be a finitely generated  $k$ -algebra that is an integral domain. Then we have

$$\dim(R) = \text{trdeg}_k(\text{Frac}(R))$$

**Proof** By the Noether normalization lemma, there exists algebraically independent elements  $y_1, \dots, y_{\dim(R)}$  such that  $R$  is finitely generated over  $k[y_1, \dots, y_{\dim(R)}]$ . Then  $\text{Frac}(R)$  is algebraic over  $\text{Frac}(k[y_1, \dots, y_{\dim(R)}]) = k(y_1, \dots, y_{\dim(R)})$ . Hence  $\text{trdeg}_k(\text{Frac}(R)) = \dim(R)$ . ■

### Corollary 8.2.4

Let  $k$  be a field. Then we have

$$\dim(k[x_1, \dots, x_n]) = n$$

**Proof** The transcendence degree of  $\text{Frac}(k[x_1, \dots, x_n]) = k(x_1, \dots, x_n)$  is  $n$ . ■

## 8.3 Height of Prime Ideals

**Definition 8.3.1 (Height of a Prime Ideal)** Let  $R$  be a commutative ring. Let  $p$  be a prime ideal of  $R$ . Define the height of  $p$  to be

$$\text{ht}(p) = \max\{t \in \mathbb{N} \mid p_0 \subset \cdots \subset p_t = p \text{ for } p_0, \dots, p_t \text{ prime ideals}\}$$

**Lemma 8.3.2** Let  $R$  be a commutative ring. Then

$$\dim(R) = \max\{\text{ht}(P) \mid P \in \text{Spec}(R)\}$$

**Lemma 8.3.3** Let  $R$  be a commutative ring. Let  $P$  be a prime ideal of  $R$ . Then

$$\text{ht}(P) = \dim(R_P)$$

**Proof** Let  $\dim(R_P) = n$ . Then there exists a strict chain of prime ideals of  $R_P$  of length  $n$  (and no chain of prime ideals of length  $> n$ ). By prp5.4.6, prime ideals of  $R_P$  are in bijection with prime ideals of  $R$  that  $P$  contains. Hence the maximal chain of prime ideals of length  $n$  correspond to a chain of prime ideals in  $R$  that contain  $P$ , of length  $n$ . Hence  $\dim(R_P) = n \leq \text{ht}(P)$ . Conversely, let  $m = \text{ht}(P)$ . Then there exists a strict chain of prime ideals that are subsets of  $P$ , that are of length  $m$ . By the same correspondence, the chain of prime ideals correspond to a chain of prime ideals in  $R_P$  of length  $m$ . Hence  $\text{ht}(P) = m \leq \dim(R_P)$ .

The two inequalities combine to show that  $\dim(R_P) = \text{ht}(P)$ . ■

**Lemma 8.3.4** Let  $R$  be a commutative ring. Let  $P$  be a prime ideal of  $R$ . Then

$$\dim(R) \geq \dim(R/P) + \text{ht}_R(P)$$

**Proposition 8.3.5** Let  $k$  be a field. Let  $R$  be a finitely generated  $k$ -algebra that is an integral domain. Then we have

$$\dim(A) = \dim(A/P) + \text{ht}_A(P)$$

**Proposition 8.3.6 (Dimension is a Local Concept)** Let  $R$  be a commutative ring. Then the following numbers are equal.

- The Krull dimension  $\dim(R)$
- The supremum  $\sup\{\dim(R_m) \mid m \text{ is a maximal ideal of } R\}$
- The supremum  $\sup\{\text{ht}_R(m) \mid m \text{ is a maximal ideal of } R\}$

**Corollary 8.3.7** Let  $(R, m)$  be a local ring. Then

$$\dim(R) = \dim(R_m) = \text{ht}_R(m)$$

**Theorem 8.3.8 (Krull's Principal Ideal Theorem)** Let  $R$  be a Noetherian ring. Let  $I$  be a proper and principal ideal of  $R$ . Let  $p$  be the smallest prime ideal containing  $I$ . Then

$$\text{ht}_R(p) \leq 1$$

## 8.4 The Length of Modules over Commutative Rings

Let  $R$  be a ring. Recall that the length of an  $R$ -module  $M$  is defined to be the supremum

$$l_R(M) = \sup\{n \in \mathbb{N} \mid 0 = M_0 \subset M_1 \subset \cdots \subset M_n = M\}$$

**Lemma 8.4.1** Let  $(R, m)$  be a local ring and let  $M$  be an  $R$ -module. If  $mM = 0$ , then

$$l_A(M) = \dim_{A/m}(M)$$

### Example 8.4.2

Let  $(R, m)$  be a local ring. Then we have

$$l_R\left(\frac{m^n}{m^{n+1}}\right) = \dim_{R/m}\left(\frac{m^n}{m^{n+1}}\right)$$

#### Proof

Follows from above. ■

### Lemma 8.4.3

Let  $R$  be a commutative ring. Let  $M$  be a finitely generated  $R$ -module. Let  $m$  be a maximal ideal such that  $m^{n-1}M \neq 0$  and  $m^n M = 0$ . Then  $l_R(M) < \infty$ .

#### Proof

For  $1 \leq i \leq n$ , consider the exact sequence

$$0 \longrightarrow m^i M \longrightarrow m^{i-1} M \longrightarrow \frac{m^{i-1} M}{m^i M} \longrightarrow 0$$

We have that  $l_R(m^{i-1} M / m^i M) = l_R(m^{i-1} M) - l_R(m^i M)$ . Then summing over  $i$  gives

$$\sum_{i=1}^n l_R\left(\frac{m^{i-1} M}{m^i M}\right) = l_R(M) - l_R(m^n M) = l_R(M)$$

Since  $m^i M$  is  $R$ -submodule of  $M$  it is finitely generated. Hence  $m^i M / m^{i+1} M$  is a finite dimensional  $R/m$  vector space. Hence  $l_R(M)$  is also finite. ■

**Lemma 8.4.4**

Let  $R$  be a commutative ring. Let  $M$  be an  $R$ -module. Let  $S$  be a multiplicative subset of  $R$ . Then we have

$$l_R(M) \geq l_R(S^{-1}M)$$

**8.5 Structure Theorem for Artinian Rings**

Let  $R$  be a ring. Let  $M$  be an  $R$ -module. Recall that a composition series for  $M$  is a sequence of  $R$ -submodules

$$0 = M_0 \subset M_1 \subset \cdots \subset M_k = M$$

such that  $\frac{M_{i+1}}{M_i}$  is a simple  $R$ -module for  $1 \leq i < k$ .

**Proposition 8.5.1** Let  $R \neq 0$  be a commutative ring. Then  $R$  is Artinian if and only if  $R$  is Noetherian and  $\dim(R) = 0$ .

**Proof** Let  $R$  be Artinian. In Rings and Modules, the Akizuki-Hopkins-Levitzki theorem proves that  $R$  is Noetherian. Moreover, lmm8.1.4 shows that  $\dim(R) = 0$ .

Now let  $R$  be Noetherian and  $\dim(R) = 0$ . This means that every prime ideal of  $R$  is maximal. Let  $S$  be the set of all ideals of  $R$  that admit a composition series. I claim that  $S$  is non-empty. Let  $T = \{\text{Ann}_R(x) \mid 0 \neq x \in R\}$ . By 6.1.1, the maximal element  $\text{Ann}_R(x)$  in  $T$  is a prime ideal. Since  $\dim(R) = 0$  we have  $\text{Ann}(x)$  is a maximal ideal.  $R/\text{Ann}(x)$  is a field (and hence a simple  $R$ -module). The multiplication map  $r \mapsto rx$  has kernel  $\text{Ann}(x)$ . Hence the induced map  $R/\text{Ann}(x) \rightarrow R$  is injective, and we can consider  $R/\text{Ann}(x)$  as a subring of  $R$ . Together with the fact that it is a simple  $R$ -module makes it an  $R$ -submodule with composition series length of 1. Hence  $S$  is non-empty.

Let  $N_1 \subseteq N_2 \subseteq \cdots$  be a chain in  $S$ . Since  $R$  is Noetherian, the chain terminates with some ideal  $I \in S$ . If  $I = R$ , then  $R$  has a composition series. If  $I \neq R$ , then  $R/I$  is non-zero. Choose a prime ideal  $P$  of  $R$  such that  $I \subseteq P \neq R$  (this always exists since we can choose maximal ideals). Then we have  $0 \neq R/P \subseteq R/I$ . Let  $p : R \rightarrow R/I$  be the projection map. Let  $T = p^{-1}(R/P)$ . Then we have that  $N \subset T \subseteq M$  and  $T/N \cong R/P$ . Since  $\dim(R) = 0$ ,  $P$  is maximal hence  $R/P$  is a field (and a simple  $R$ -module). This proves that  $T \in S$ . But this contradicts the maximality of  $N$ . Hence  $N = R \in T$ . Thus  $R$  has a composition series. From Rings and Modules we know that this implies  $R$  is Noetherian. Hence we conclude. ■

**Example 8.5.2** Let  $k$  be a field. The  $k[x]$ -module  $\frac{k[x, x^{-1}]}{k[x]}$  is Artinian but not Noetherian.

**Proof** It is not Noetherian because it is not finitely generated. Write  $M = \frac{k[x, x^{-1}]}{k[x]}$ . For the Artinian result, we first show that if  $N \leq \frac{k[x, x^{-1}]}{k[x]}$  and for all  $n \in \mathbb{N}$  there exists  $f + k[x] \in \frac{k[x, x^{-1}]}{k[x]}$  such that  $f$  contains the term  $1/x^n$ , then  $N = \frac{k[x, x^{-1}]}{k[x]}$ .

By assumption, for any  $n \in \mathbb{N}$ , there exists  $f \in k[x, x^{-1}]$  such that  $f$  contains the term  $1/x^n$ . If  $\deg(f) < -n$ , then we can multiply  $f$  with  $x^{\deg(f)+n}$  to get a polynomial  $g$  such that  $\deg(g) = -n$ . So denote  $f_n + N$  the element in  $N$  such that  $\deg(f_n) = -n$ . Then by multiplying with a suitable coefficient  $\alpha$ ,  $f_n - \alpha f_{n-1}$  contains only  $1/x^n$ . Hence  $N$  contains  $1/x^n$  for all  $n \in \mathbb{N}$  as  $k[x]$ -module. Since these elements generate  $\frac{k[x, x^{-1}]}{k[x]}$  as a  $k$ -module, they also generate as a  $k[x]$ -module. Hence  $N = \frac{k[x, x^{-1}]}{k[x]}$ .

This means that if  $N$  is a proper sub-module, there exists a minimal  $n \in \mathbb{N}$  such that  $1/x^n \in N$  and  $1/x^{n+1} \notin N$ . Hence every  $N$  is a finitely generated  $k$ -module, or in other words,  $N$  is a finite dimensional vector space. Thus any decreasing chain of  $k[x]$ -submodules must terminate by a

dimension argument. ■

**Theorem 8.5.3 (Structure Theorem for Commutative Artinian Rings)** Let  $R$  be an Artinian commutative ring. Then  $R$  decomposes into a direct product of Artinian local rings

$$R \cong \bigoplus_{i=1}^k R_i$$

Moreover, the decomposition is unique up to reordering of the direct product.

**Proof** Let  $m_1, \dots, m_k$  be the full list of distinct maximal ideals of  $R$ . Then

$$\prod_{i=1}^k m_i^n = 0$$

for some  $n \in \mathbb{N} \setminus \{0\}$ . The ideals  $m_i^n$  and  $m_j^n$  are pairwise coprime for  $i \neq j$ . Hence by the Chinese Remainder Theorem we obtain ring isomorphisms

$$\begin{aligned} R &\cong \frac{R}{0} \\ &\cong \frac{R}{\prod_{i=1}^k m_i^n} \\ &\cong \frac{R}{\bigcap_{i=1}^k m_i^n} && (m_i^n \text{ and } m_j^n \text{ pairwise coprime}) \\ &\cong \bigoplus_{i=1}^k \frac{R}{m_i^n} && (\text{CRT}) \end{aligned}$$

By the correspondence of maximal ideals,  $R/m_i^n$  has a unique maximal ideal  $m_i/m_i^n$ . Hence it is local. Also since  $R$  is Artinian,  $R/m_i^n$  is Artinian. Thus we are done. ■



## 9 Valuation and Valuation Rings

### 9.1 Valuation Rings

**Definition 9.1.1 (Valuation Rings)** Let  $R$  be an integral domain. We say that  $R$  is a valuation ring if for all  $x \in \text{Frac}(R)$  and  $x \neq 0$ , then either  $x$  or  $x^{-1}$  is in  $R$ .

**Lemma 9.1.2** Let  $R$  be an integral domain. Then  $R$  is a valuation ring if and only if the ideals of  $R$  are totally ordered by inclusion.

**Proof** Let  $R$  be a valuation ring. Let  $I, J$  be ideals of  $R$ . If  $I$  is not a subset of  $J$ , there exists  $x \in I$  such that  $x \notin J$ . Then for any  $0 \neq y \in J$ ,  $x/y \in \text{Frac}(R) \setminus R$  since otherwise  $y$  is a unit in  $J$  so that  $J = R$  and  $I \subseteq R$ . Then  $y/x \in R$  so that  $y = x(y/x) \in I$ . Hence  $J \subseteq I$ .

Now suppose that the ideals of  $R$  are totally ordered by inclusion. ■

**Lemma 9.1.3** Let  $R$  be a valuation ring. Then the following are true.

- $R$  is a local ring.
- $R$  is normal.

**Proof** Since all ideals of  $R$  are totally ordered, there is only one unique maximal ideal.

Let  $x \in \text{Frac}(R)$  be integral over  $R$ . Then

$$x^n + r_{n-1}x^{n-1} + \cdots + r_1x + r_0 = 0$$

for some  $r_0, \dots, r_{n-1} \in R$ . If  $x \in R$  then we are done. If  $x \notin R$  then since  $R$  is a valuation ring,  $x^{-1} \in R$ . Then

$$x = -(r_1 + r_2x^{-1} + \cdots + r_nx^{1-n}) \in R$$

so that  $R$  is normal. ■

**Definition 9.1.4 (Totally Ordered Group)** Let  $G$  be an abelian group. We say that  $G$  is a totally ordered group if there is a total order " $\leq$ " on  $G$  such that  $a \leq b$  implies  $ca \leq cb$  for all  $a, b, c \in G$ .

**Definition 9.1.5 (Valuation on a Field)** Let  $K$  be a field. Let  $G$  be a totally ordered abelian group. A valuation on  $K$  with values in  $G$  is a map  $v : K^\times \rightarrow G$  such that for all  $x, y \in K^\times$ , we have

- $v(xy) = v(x) + v(y)$  ( $v$  is a group homomorphism)
- $v(x + y) \geq \min\{v(x), v(y)\}$

We use the convention that  $v(0) = \infty$ .

**Definition 9.1.6 (Associated Valuation Ring)** Let  $K$  be a field and  $v : K \rightarrow \mathbb{Z}$  a discrete valuation. Define the associated valuation ring of  $K$  to be the subring

$$R_v = \{x \in K \mid v(x) \geq 0\}$$

**Lemma 9.1.7** Let  $K$  be a field. Let  $v$  be a discrete valuation on  $K$ . Then  $R_v$  is a valuation ring.

**Definition 9.1.8 (Discrete Valuations)** Let  $K$  be a field. A discrete valuation on  $K$  is a valuation  $v : K^\times \rightarrow \mathbb{Z}$ .

**Definition 9.1.9 (Normalized Discrete Valuations)** Let  $(K, v)$  be a discrete valuation ring. We say that it is normalized if  $v$  is surjective.

**Lemma 9.1.10** Let  $K$  be a field with a discrete valuation  $v$ . Then  $v(K^\times) = n\mathbb{Z}$  for some  $n \in \mathbb{N}$ .

**Lemma 9.1.11 (Normalization of a Discrete Valuation)** Let  $K$  be a field with a discrete valuation  $v$  such that  $v(K^\times) = n\mathbb{Z}$  for some  $n \in \mathbb{N}$ . Define the normalization of  $v$  to be the valuation  $v_N : K^\times \rightarrow \mathbb{Z}$  defined by

$$v_N(k) = \frac{1}{n}v(k)$$

for all  $k \in K^\times$ .

Therefore we always work on normalized discrete valuations.

## 9.2 Discrete Valuation Rings

**Definition 9.2.1 (Discrete Valuation Rings)** Let  $R$  be a commutative ring. We say that  $R$  is a discrete valuation ring if there exists a field  $K$  and a discrete valuation  $v$  on  $K$  such that

$$R = R_v$$

is the associated valuation ring of  $K$ .

**Lemma 9.2.2** Let  $R$  be a discrete valuation ring with valuation  $v$ . Then  $0 \neq u \in R$  is a unit if and only if  $v(u) = 0$ . In particular, the maximal ideal of  $R$  is given by

$$\{r \in R \mid v(r) > 0\}$$

**Proof** Let  $R$  be a discrete valuation ring. Suppose that  $x \in R$  is a unit. Then  $v(x^{-1}) = -v(x)$ . Then  $-v(x), v(x) \geq 0$  implies  $v(x) = 0$ . Now if  $v(y) > 0$ , suppose for contradiction that  $u \in R$  is an inverse of  $y$ , then

$$0 = v(1) = v(uy) = v(u) + v(y)$$

But  $v(y) > 0$  implies that  $v(u) < 0$  which implies that  $u \notin R$ , a contradiction. ■

**Example 9.2.3** Let  $n \in \mathbb{N}$ . Define  $\text{ord}_n : \mathbb{Q} \rightarrow \mathbb{Z}$  as follows. For  $p/q \in \mathbb{Q}$ , let  $p = p'n^i$  and  $q = q'n^j$  such that  $\gcd(p', n) = \gcd(q', n) = 1$ . Then define

$$\text{ord}_n\left(\frac{p}{q}\right) = \text{ord}_n\left(n^{i-j}\frac{p'}{q'}\right) = i - j$$

Then  $\text{ord}_n$  is a discrete valuation if and only if  $n$  is prime. In this case, the valuation ring of  $\text{ord}_n$  is given by

$$R_{\text{ord}_n} = \mathbb{Z}_n$$

**Proof** Suppose that  $n$  is a prime. Let  $n^s p_1/q_1 \in \mathbb{Q}$  and  $n^t p_2/q_2$  be in lowest terms. Then  $n^{s+t}(p_1 p_2/q_1 q_2)$  is in lowest terms since  $n$  is prime. Then we have

$$\text{ord}_n(n^{s+t}(p_1 p_2/q_1 q_2)) = s + t = v(n^s p_1/q_1) + v(n^t p_2/q_2)$$

Without loss of generality, suppose that  $s \leq t$ . Then  $n^s p_1/q_1 + n^t p_2/q_2 = n^s(p_1/q_1 + n^{t-s} p_2/q_2)$  is in lowest terms since  $n$  is prime. Then we have

$$v(n^s p_1/q_1 + n^t p_2/q_2) = v(n^s(p_1/q_1 + n^{t-s} p_2/q_2)) = s = \min\{v(n^s p_1/q_1), v(n^t p_2/q_2)\}$$

Thus  $\text{ord}_n$  is a discrete valuation.

If  $n$  is composite, without loss of generality suppose that  $n = pq$  for  $p$  and  $q$  primes.

The valuation ring of  $\text{ord}_n$  for  $n$  prime is given by

$$R_{\text{ord}_n} = \left\{ \frac{p}{q} \in \mathbb{Q} \mid n \text{ does not divide } q \right\}$$

Hence  $R_{\text{ord}_n} = \mathbb{Z}_n$ . ■

**Definition 9.2.4 (Uniformizing Parameter)** Let  $R$  be a discrete valuation ring with valuation  $v$ . A uniformizing parameter for  $R$  is an element  $t \in R$  such that  $v(t) = 1$ .

**Proposition 9.2.5** Let  $R$  be a discrete valuation ring with valuation  $v$ . Let  $t \in R$  be a uniformizing parameter of  $R$ . Then the following are true.

- Every  $r \in R \setminus \{0\}$  can be written in the form

$$r = ut^n$$

for some unit  $u$  and  $n \geq 0$ .

- The valuation of any element  $r = ut^n \in R$  is given by

$$v(ut^n) = n$$

- The set of all ideals of  $R$  is given by

$$\{(t^n) \mid n \in \mathbb{N} \setminus \{0\}\}$$

In particular, the unique maximal ideal of  $R$  is  $(t)$ .

**Proof**

- If  $x \in R$  is a unit then we are done. If not, then consider the element  $u = t^{-n}x$  for  $n = v(x)$ . Then we have

$$v(u) = v(t^{-n}x) = -n + v(x) = 0$$

Hence  $u$  is a unit. Multiplying  $t^n$  on both sides of  $u = t^{-n}x$  proves that  $x = ut^n$  for some unit  $u$  and  $n \in \mathbb{N}$ .

- It follows that the valuation of  $r = ut^n$  is  $n$ .
- Let  $I$  be an ideal of  $R$ . Let  $n = \min\{v(x) \mid x \in I\}$ . or all  $x \in I$ , we can write  $x$  as  $x = ut^k$  for some unit  $u$  and  $k \geq n$ . Hence  $I \subseteq (t^n)$ . Since  $n$  is a minimum, there exists  $x \in I$  such that  $x = ut^n$  for some unit  $u$  and  $n \in \mathbb{N}$ . Then  $u^{-1}x = t^n \in I$  since  $I$  is an ideal. Hence  $I = (t^n)$ . It follows that the unique maximal ideal of  $R$  is given by  $(t)$ . ■

The rest of the section devotes efforts to recognizing discrete valuation rings.

**Proposition 9.2.6 (Equivalent Characterizations of DVRs I)** Let  $R$  be an integral domain. Then the following are equivalent.

- $R$  is a discrete valuation ring.
- $R$  is local, a PID and not a field.
- $R$  is Noetherian, local,  $\dim(R) = 1$  and normal.
- $R$  is Noetherian, local,  $\dim(R) > 0$  and the unique maximal ideal  $m$  is principal.
- $R$  is a UFD with a unique irreducible element up to multiplication of a unit

**Proof**

- (1)  $\implies$  (2): We have seen that valuation rings are local. It is a PID by 9.2.5. It is not a field

since  $R$  is a local ring with non-trivial unique maximal ideal.

- (2)  $\implies$  (3): Every PID is Noetherian and normal and every prime ideal is maximal. But local rings have a unique maximal ideal. The maximal ideal is non-trivial since  $R$  is not a field. Hence  $\dim(R) = 1$ .
- (3)  $\implies$  (4): By Nakayama's lemma,  $m \neq m^2$ . I claim that any  $x \in m \setminus m^2$  generates  $m$ . Since  $\dim(R) = 1$ , we have  $\text{Spec}(R) = \{(0), m\}$ . Assume for a contradiction that  $m/(x) \neq \{0\}$ . By Imm6.2.4, we have  $\text{Ass}(m/(x)) \neq \{0\}$ . By our assumption for contradiction, we can only have  $\text{Ass}(m/(x)) = \{m\}$ . By definition, this means that there exists  $0 \neq [y] \in m/(x)$  such that  $\text{Ann}_R([y]) = m$ . In other words,  $ym \subseteq (x)$ . Considering everything inside  $\text{Frac}(R)$ , we have  $y/x \in \text{Frac}(R)$  is such that  $y/x \notin R$  and  $y/x \cdot m \subseteq R$ . There are now two cases.

Case 1:  $y/x \cdot m = R$ .

Then  $1 = yt/x$  for some  $t \in m$ , which means that  $x = yt$  and  $x \in ym \subseteq m^2$ . This is a contradiction.

Case 2:  $y/x \cdot m = m$ . Then the multiplication map  $z \mapsto y/x \cdot z$  satisfies the hypothesis of the Cayley-Hamilton theorem, and there exists  $a_0, \dots, a_{n-1} \in R$  such that

$$(y/x)^n + a_{n-1}(y/x)^{n-1} + \dots + a_1(y/x) + a_0 = 0$$

But then this proves that  $y/x$  is integral over  $R$ . Since  $R$  is normal,  $y/x \in R$ . This is also a contradiction.

Thus  $m$  is a PID.

- (4)  $\implies$  (1): Suppose that  $m = (x)$  for some  $x \in R$ . If  $x$  is nilpotent, then  $\dim(R) = 0$  and a contradiction. I claim that  $\bigcap_{i=1}^{\infty} (x^i) = \{0\}$ . Suppose that  $t$  lies in the intersection. Then  $t = yx$  for some  $y \in R$ . If  $y$  is not in the intersection, then there exists  $n \in \mathbb{N}$  such that  $y$  is non-zero in  $(x^n)/(x^{n+1})$ . By Nakayama's lemma,  $y$  generates  $(x^n)$  and so  $t$  generates  $(x^{n+1})$ . Then  $t \notin (x^{n+2})$  is a contradiction. In particular, there for any  $y \in R$ , we have  $y \in (x^n) \setminus (x^{n+1})$  for some  $n \in \mathbb{N}$ . This means that  $y = ux^n$  for some  $u \notin (x)$ . In particular,  $u$  is a unit. Similarly,  $z = vx^m$  for  $v$  a unit. Then  $yz = uvx^{n+m}$  is non-zero. Hence  $R$  is an integral domain. Then the map  $ux^n \mapsto n$  is a valuation.
- (5)  $\implies$  (1): Let  $t$  be the unique irreducible element. Define a map  $v : \text{Frac}(R) \rightarrow \mathbb{Z}$  as follows. Since  $R$  is a UFD, every element in  $R$  can be uniquely written as  $zt^n$  for  $z$  a unit and  $n \in \mathbb{N}$ . Also, every element in  $\text{Frac}(R)$  can be uniquely written as  $zt^n$  for  $z$  a unit in  $n \in \mathbb{Z}$ . Then define  $v(zt^n) = n$ . It is clear that  $v$  is a valuation. Its associated valuation ring is then precisely  $R$ .

■

**Proposition 9.2.7 (Equivalent Characterizations of DVRs II)** Let  $R$  be an integral domain that is Noetherian and local with unique maximal ideal  $m$ . Then the following are equivalent.

- $R$  is a discrete valuation ring.
- $\dim(R) = 1$  and  $R$  is normal.
- $R$  is not a field and  $m$  is principal.
- $\dim(R) = 1$  and  $\dim_{R/m}(m/m^2) = 1$  ( $R$  is a regular local ring)
- $I = m^k$  for all non-zero ideals  $I$  of  $R$
- There exists  $t \in R$  and  $k > 0$  such that  $I = (t^k)$  for all non-zero ideal  $I$  of  $R$

**Proof** The proposition is an immediate consequence of the above.

■

**Proposition 9.2.8** Let  $R$  be a Noetherian integral domain and  $\dim(R) = 1$ . Then  $R$  is normal if and only if  $R_m$  is a discrete valuation ring for all maximal ideals  $m$ .

In summary, if  $R$  is a discrete valuation ring, then  $R$  has the following properties.

- $R$  is integrally closed and in particular is normal.
- $R$  is a PID and in particular is a UFD and an integral domain.
- $R$  is Noetherian and local
- $R$  has Krull dimension 1.
- $\dim_{R/m}(m/m^2) = 1$  (these are called regular local rings as we will see in Commutative Algebra 2)
- Every ideal  $I$  of  $R$  is equal to the power  $m^k$  of the maximal ideal  $m$ . In particular if  $m$  is generated by the uniformizing parameter  $t$ , then  $I = (t^k)$  in this case.
- Such a  $t$  is an irreducible element (that is unique up to multiplication by a unit), and every element of  $R$  can be written as  $ut^n$  for  $u$  a unit and  $n \in \mathbb{N}$ .

There is a simple diagram of relationships between DVRs and some other standard types of commutative rings.

$$\text{DVRs} \subset \text{PIDs} \subset \text{UFDs} \subset \text{Normal Domains} \subset \text{Integral Domains}$$

## 10 Dedekind Domains

### 10.1 Fractional Ideals

**Definition 10.1.1 (Fractional Ideal)** Let  $R$  be an integral domain. Let  $I$  be a  $R$ -submodule of  $\text{Frac}(R)$ . We say that  $I$  is a fractional ideal of  $R$  if there exists  $r \in R \setminus \{0\}$  such that  $rI \subseteq R$ .

While  $I$  is not exactly an ideal of  $R$ , we can think of it as if it were an ideal because it is isomorphic to an actual ideal of  $R$ .

**Lemma 10.1.2** Let  $R$  be an integral domain. Let  $I$  be a fractional ideal of  $R$  where  $rI \subseteq R$  for some  $r \in R \setminus \{0\}$ . Then there is an  $R$ -module isomorphism

$$I \cong rI \subseteq R$$

given by  $i \mapsto ri$ .

**Proof** I claim that there is an  $R$ -module isomorphism  $I \cong rI$  for  $rI \subseteq R$  given by  $i \mapsto ri$ . The kernel of this  $R$ -module homomorphism is given by  $\{i \in I \mid ri = 0\}$ . But  $ri = 0$  if and only if  $r = 0$  or  $i = 0$ . Since  $r \neq 0$  we must have  $i = 0$  so that the kernel is trivial. Moreover, this  $R$ -module homomorphism is surjective since for any  $k \in rI$  it can be written as  $k = ri$  for some  $i$ . Then  $i \in I$  maps to  $ri$  under the morphism. Hence  $I \cong rI$  as  $R$ -modules. ■

**Example 10.1.3** The  $\mathbb{Z}$ -submodule  $\mathbb{Z} \cdot \frac{1}{2}$  of  $\mathbb{Q}$  is a fractional ideal.

**Proof** Indeed, we have  $2(\mathbb{Z} \cdot \frac{1}{2}) = \mathbb{Z}$ , and we think of  $\mathbb{Z} \cdot \frac{1}{2}$  as a  $\mathbb{Z}$ -module isomorphic to  $\mathbb{Z}$ . ■

**Lemma 10.1.4** Let  $R$  be an integral domain. Let  $I$  be a fractional ideal of  $R$ . If  $R$  is Noetherian, then  $I$  is finitely generated.

**Proof** Let  $R$  be Noetherian. Since  $I$  is isomorphic to  $rI$  for some non-zero  $r \in R$ , and  $rI$  is an ideal of  $R$ ,  $R$  being Noetherian implies that  $rI$  is finitely generated and hence  $I$  is finitely generated. ■

### 10.2 Invertible Ideals

**Definition 10.2.1 (Inverse of an Ideal)** Let  $R$  be an integral domain. Let  $I$  be an  $R$ -submodule of  $\text{Frac}(R)$ . Define

$$I^{-1} = \{s \in \text{Frac}(R) \mid sI \subseteq R\}$$

**Lemma 10.2.2** Let  $R$  be an integral domain. Let  $I$  be an  $R$ -submodule of  $\text{Frac}(R)$ . Then there is an  $R$ -module isomorphism

$$I^{-1} \cong \text{Hom}_R(I, R)$$

given by  $s \mapsto (r \mapsto sr)$ .

**Proof** Denote  $\varphi_s : I \rightarrow R$  the multiplication by  $s$  map for  $s \in I^{-1}$ . It is clear that the given map is an  $R$ -module homomorphism. The map is injective since  $R$  is an integral domain. It remains to show that the map is surjective. Let  $\varphi \in \text{Hom}_R(I, R)$ . For any  $r \in R$  and  $i \in I$ , we have

$$\varphi(r \cdot i) = r \cdot \varphi(i)$$

**Definition 10.2.3 (Invertible Ideals)** Let  $R$  be an integral domain. Let  $I$  be an  $R$ -submodule of  $\text{Frac}(R)$ . We say that  $I$  is invertible if there exists an  $R$ -submodule of  $J$  of  $R$  such that  $JI = R$ .

**Lemma 10.2.4** Let  $R$  be an integral domain. Let  $I \subseteq R$  be a subset. Then  $I$  is an ideal if and only if  $I$  is a fractional ideal.

**Proof** Clearly if  $I$  is a fractional ideal, then  $I$  is an ideal. Conversely, if  $I$  is an ideal then  $rI \subseteq R$  for all  $r \in R$  implies that  $I$  is a fractional ideal. ■

**Proposition 10.2.5** Let  $R$  be an integral domain. Let  $I$  be an  $R$ -submodule of  $\text{Frac}(R)$ . Then  $I$  is invertible if and only if  $I^{-1}I = R$ .

**Proof** Clearly if  $I^{-1}I = R$  then  $I$  is invertible. Now suppose that  $JI = R$  for some  $R$ -submodule  $J$  of  $\text{Frac}(R)$ . Then we have

$$R = JI \subseteq I^{-1}I = R$$

by definition of  $I^{-1}$ . Hence  $JI = I^{-1}I$ . Multiplying  $J$  on both sides and using the fact that  $R$  is commutative, we have that  $J = I^{-1}$ . ■

**Lemma 10.2.6** Let  $R$  be an integral domain. Let  $I$  be an invertible ideal of  $R$ . Then for any prime ideal  $P$  of  $R$ , the ideal  $IR_P$  of  $R_P$  is a principal ideal.

**Proof** Since  $I^{-1}I = R$ , write  $1 = \sum_{i=1}^k s_i a_i$  for  $s_i \in I^{-1}$  and  $a_i \in I$ . Since  $1 \notin P$ , at least one of  $s_i a_i$  is not in  $P$ . Then  $s_i a_i$  is a unit in  $PR_P$  and so  $a_i$  generates  $IR_P$ . ■

**Proposition 10.2.7** Let  $R$  be an integral domain. Let  $I$  be an  $R$ -submodule of  $\text{Frac}(R)$ . Then the following are true.

- If  $I$  is a non-zero principal ideal of  $R$ , then  $I$  is invertible.
- If  $I$  is invertible, then  $I$  is fractional.
- If  $I$  is invertible, then  $I$  is finitely generated.

**Proof**

- Suppose that  $I = (a)$  for  $a \in R$ . Then clearly we have  $(1/a)(a) = R$ .
- Let  $I$  be invertible. Since  $I^{-1}I = R$ , we can write  $1 = \sum_{i=1}^n s_i a_i$  for  $s_i \in I^{-1}$  and  $a_i \in I$ . Then for any  $r \in R$ , we have  $b = \sum_{i=1}^n s_i (a_i b)$  where  $a_i b \in R$ . Let  $s$  be the product of the denominators of  $s_i$ . Then  $sb \in R$ . Hence  $I$  is a fractional ideal.
- Let  $I$  be invertible. Since  $I^{-1}I = R$ , we can write  $1 = \sum_{i=1}^n s_i a_i$  for  $s_i \in I^{-1}$  and  $a_i \in I$ . Then for any  $x \in R$ , we have  $x = \sum_{i=1}^n (s_i x) a_i$ . Since  $s_i \in I^{-1}$  and  $x \in R$ , we have  $s_i x \in R$ . Hence  $x$  can be written as a  $R$ -linear combination of  $a_1, \dots, a_n$ . Hence  $I$  is finitely generated. ■

**Proposition 10.2.8** Let  $R$  be an integral domain. Let  $I$  be an  $R$ -submodule of  $\text{Frac}(R)$ . Then  $I$  is invertible if and only if the following are true.

- $I$  is fractional.
- $I$  is finitely generated.
- For any prime ideal  $P$  of  $R$ ,  $IR_P$  is a principal ideal of  $R_P$ .

**Proof** We have seen the forward direction already. Now suppose that  $I$  satisfies the three listed conditions. I claim that  $(I^{-1})_P = (I_P)^{-1}$ . Let  $r/s \in (I^{-1})_P$  and  $a/b \in I_P$ . Then clearly  $r/s \cdot a/b \in R_P$  so that  $r/s \in (I_P)^{-1}$ . Conversely, suppose that  $I = R(a_1, \dots, a_n)$ . Let  $x \in (I_P)^{-1}$ . Then  $xa_i \in R_P$ . This means that there exists  $c_i \in R \setminus P$  such that  $xa_i c_i \in R$ . Set  $c = c_1 \cdots c_n$ . Then clearly  $cx \in I^{-1}$  so that  $x \in (I^{-1})_P$ .

Suppose that  $I^{-1}I \neq R$ . Since  $I^{-1}I$  is a proper ideal of  $R$ , there exists a maximal ideal  $m$  of  $R$  containing  $I^{-1}I$ . By the correspondence of ideals for localization, we have  $(I^{-1})_m I_m = (I_m)^{-1} I_m \subseteq$

$mR_m$ . This is a contradiction since the above proposition together with the fact that  $IR_m$  is a principal ideal of  $R_m$  should imply that  $(I_m)^{-1}I_m = R_m$ . ■

**Proposition 10.2.9** Let  $R$  be an integral domain. Let  $P$  be a non-zero prime ideal of  $R$ . If  $R$  is Noetherian and  $P$  is invertible, then  $R_P$  is a discrete valuation ring.

**Proof** Let  $R$  be a Noetherian integral domain and  $P$  a non-zero invertible prime ideal. We know that  $PR_P$  is the unique maximal ideal of the local ring  $R_P$ . By the above prp,  $PR_P$  is a principal ideal. Thus  $R_P$  is now a Noetherian local ring with principal maximal ideal. By prp10.4.6 in Commutative Algebra 1, we conclude that  $R_P$  is a discrete valuation ring. ■

### 10.3 Dedekind Domains

**Definition 10.3.1 (Dedekind Domains)** Let  $R$  be an integral domain. We say that  $R$  is a dedekind domain if every non-zero ideal  $I$  of  $R$  is invertible.

Dedekind sought for an integral domain whose ideals can be factorized uniquely as a product of primes.

**Proposition 10.3.2** Let  $R$  be an integral domain that is not a field. Then the following are equivalent.

- Every non-zero ideal  $I$  of  $R$  is invertible ( $I^{-1}I = R$ ).
- $R$  is Noetherian,  $\dim(R) = 1$  and normal
- $R$  is Noetherian,  $\dim(R) = 1$  and for any non-zero maximal ideal  $m$  of  $R$ ,  $R_m$  is a discrete valuation ring.
- $R$  is Noetherian,  $\dim(R) = 1$  and every primary ideal in  $R$  is a prime power.

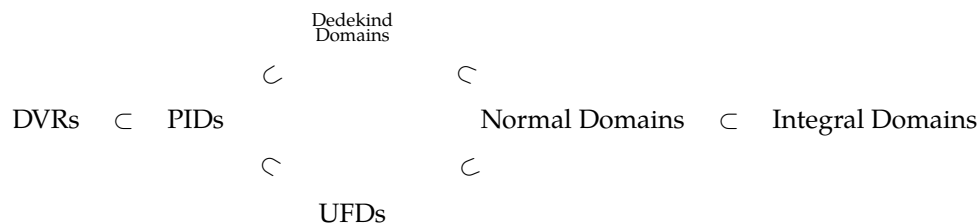
**Proof**

- (1)  $\implies$  (2): For any ideal  $I$  of  $R$ ,  $I$  is invertible. By 10.2.6,  $I$  is finitely generated. Then every  $R$ -submodule of  $R$  is finitely generated and so  $R$  is Noetherian. For any prime ideal  $P$  of  $R$ , 10.2.8 implies that  $R_P$  is a discrete valuation ring since  $P$  by assumption is invertible. Then  $R_P$  is a normal domain for any prime ideal  $P$ . Since normality is a local condition, we conclude that  $R$  is a normal domain.
- (2)  $\implies$  (3): For any maximal ideal  $m$  of  $R$ ,  $R_m$  is Noetherian since localization preserves Noetherianity. Also,  $R_m$  is local. Since normality is a local condition,  $R_m$  is also normal. Finally, we have  $\dim(R_m) = \dim(R) = 1$ . Hence by the equivalent characterizations of DVRs, we conclude that  $R_m$  is a DVR.
- (3)  $\implies$  (1): Let  $I \subseteq R$  be a fractional ideal of  $R$ . We know by 10.1.4 that  $I$  is finitely generated. Since  $R_m$  is a normal Noetherian local ring of dimension 1, the ideal  $I_m$  of  $R_m$  must be principal. By 10.2.7 we conclude that  $I$  is invertible. ■

By virtue of the fourth item, we can think of Dedekind domains as a patching up of local discrete valuation rings.

We summarize the relation between Dedekind domains and other types of domains in the following diagram:





In particular, DVRs, PIDs and Dedekind domains are 1-dimensional. Moreover, notice that the only difference between DVRs and Dedekind domains is that DVRs are local rings. They both share the fact that they are Noetherian,  $\dim(R) = 1$  and normal.

## 10.4 Prime Factorization of Ideals

**Definition 10.4.1 (Prime Factorization of Ideals)** Let  $R$  be a commutative ring. Let  $I$  be an ideal of  $R$ . A prime factorization of  $I$  consists of maximal ideals  $P_1, \dots, P_k$  such that the following are true.

- For some  $n_1, \dots, n_k \in \mathbb{N} \setminus \{0\}$ , we have

$$I = P_1^{n_1} \cdots P_k^{n_k}$$

- Each  $P_1, \dots, P_n \in \text{Ass}(I)$  is an associated prime ideal of  $I$ .
- The factorization is unique up to permutation.

**Proposition 10.4.2** Let  $R$  be an integral domain. Then  $R$  is a Dedekind domain if and only if every ideal of  $R$  has a prime factorization.

**Proposition 10.4.3** Let  $R$  be a Dedekind domain. For any prime ideal  $P$  of  $R$ , denote  $v_i : \text{Frac}(R_P) \rightarrow \mathbb{Z}$  the discrete valuation of  $R_P$ . Then for any  $a \in R \setminus \{0\}$ , we have

$$(a) = P_1^{v_1(a)} \cdots P_n^{v_n(a)}$$

for  $P_1, \dots, P_n \in \text{Ass}((a))$ .

**Proposition 10.4.4** Let  $R$  be a Dedekind domain. Let  $I$  and  $J$  be ideals of  $R$  whose prime factorization is given by

$$I = P_1^{a_1} \times \cdots \times P_n^{a_n} \quad \text{and} \quad J = P_1^{b_1} \times \cdots \times P_n^{b_n}$$

for  $P_1, \dots, P_n$  distinct prime ideals of  $R$ . Then the following are true.

- $I + J = P_1^{\min\{a_1, b_1\}} \times \cdots \times P_n^{\min\{a_n, b_n\}}$
- $I \cap J = P_1^{\max\{a_1, b_1\}} \times \cdots \times P_n^{\max\{a_n, b_n\}}$
- $IJ = P_1^{a_1+b_1} \times \cdots \times P_n^{a_n+b_n}$

**Proposition 10.4.5** Let  $R$  be a Dedekind domain. Let  $I$  be an ideal of  $R$ . Then the following are true.

- For any  $a \in I$ , there exists  $b \in R$  such that  $I = (a, b)$ .
- $I$  is can be finitely generated by two elements.