

# Commutative Algebra 1

Labix

October 28, 2024

**Abstract**

## Contents

<b>1</b>	<b>Basic Notions of Commutative Rings</b>	<b>3</b>
1.1	Local Rings . . . . .	3
1.2	Hilbert's Basis Theorem . . . . .	4
1.3	Spectra of a Ring . . . . .	4
<b>2</b>	<b>Ideals Of a Commutative Ring</b>	<b>6</b>
2.1	Operations on Ideals . . . . .	6
2.2	Radical Ideals . . . . .	6
2.3	Nilradical and Jacobson Ideals . . . . .	8
2.4	Extensions and Contractions of Ideals . . . . .	10
2.5	Revisiting the Polynomial Ring . . . . .	11
<b>3</b>	<b>Simplifying Generators of an Ideal</b>	<b>13</b>
3.1	Ordering on the Monomials . . . . .	13
3.2	Monomial Ideals . . . . .	14
3.3	Groebner Bases . . . . .	14
<b>4</b>	<b>Modules over a Commutative Ring</b>	<b>15</b>
4.1	Cayley-Hamilton Theorem . . . . .	15
4.2	Nakayama's Lemma . . . . .	16
4.3	Change of Rings . . . . .	17
<b>5</b>	<b>Algebra Over a Commutative Ring</b>	<b>18</b>
5.1	Commutative Algebras . . . . .	18
5.2	Finitely Generated Algebra . . . . .	18
<b>6</b>	<b>Localization</b>	<b>20</b>
6.1	Localization of a Ring . . . . .	20
6.2	Localization at a Prime Ideal . . . . .	21
6.3	Properties of Localization . . . . .	21
6.4	Localization of a Module . . . . .	22
<b>7</b>	<b>Primary Decomposition</b>	<b>23</b>
7.1	Support of a Module . . . . .	23
7.2	Associated Prime . . . . .	23
7.3	Primary Ideals . . . . .	23
7.4	Primary Decomposition . . . . .	23
<b>8</b>	<b>Integral Dependence</b>	<b>25</b>
8.1	Integral Extensions . . . . .	25
8.2	The Going-Up and Going-Down Theorems . . . . .	26
8.3	Dedekind Domains . . . . .	26
<b>9</b>	<b>Discrete Valuation Rings</b>	<b>27</b>
9.1	Discrete Valuation Rings . . . . .	27
<b>10</b>	<b>Dimension Theory for Rings</b>	<b>29</b>
10.1	Dimension and Height . . . . .	29
10.2	Length of a Module . . . . .	29
10.3	The Hilbert Polynomial . . . . .	30
10.4	Global Dimension of a Ring . . . . .	31

# 1 Basic Notions of Commutative Rings

## 1.1 Local Rings

### Definition 1.1.1: 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 1.1.2

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 1.1.3

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 1.1.4

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  $k[[x]]$ .  $\square$

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

## 1.2 Hilbert's Basis Theorem

### Theorem 1.2.1: Hilbert's Basis Theorem

Let  $R$  be a commutative ring. If  $R$  is Noetherian, then

$$R[x_1, \dots, x_n]$$

is a Noetherian ring.

### Proposition 1.2.2

Let  $R$  be a commutative ring. Let  $I$  be an ideal of  $R$ . If  $R$  is Noetherian then  $R/I$  is Noetherian.

### Theorem 1.2.3

Let  $R = \bigoplus_{i=1}^n R_i$  be a graded ring. Then  $R$  is Noetherian if and only if  $R_0$  is Noetherian and  $R$  is finitely generated as an  $R_0$ -module.

## 1.3 Spectra of a Ring

### Definition 1.3.1: Max Spectrum of a Ring

Let  $A$  be a commutative ring. Define the max spectrum of  $A$  to be

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

### Definition 1.3.2: 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 1.3.3

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 1.3.4

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  $P \neq R$ , 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.

□

## 2 Ideals Of a Commutative Ring

### 2.1 Operations on Ideals

#### Proposition 2.1.1

Let  $R$  be a commutative ring. Let  $S, T \subseteq R$  be subsets of  $R$ . Then

$$\langle S \cup T \rangle = \langle S \rangle + \langle T \rangle$$

#### Proposition 2.1.2

Let  $R$  be a commutative ring. Let  $I, J$  be ideals of  $R$ . Suppose that  $I \subseteq J$ . Let  $\bar{J}$  denote the ideal of  $R/I$  corresponding to  $J$  under the correspondence theorem. Then there is an isomorphism

$$\frac{R/I}{\bar{J}} \cong \frac{R}{I+J}$$

given by the formula  $(r + I) + \bar{J} \mapsto r + (I + J)$ .

#### Example 2.1.3

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  $\mathbb{Z}/3\mathbb{Z}$ .  $\square$

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

- If  $I$  and  $J$  are coprime, then  $IJ = I \cap J$
- Chinese Remainder Theorem: If  $I$  and  $J$  are coprime, then there is an isomorphism

$$\frac{R}{I \cap J} \cong \frac{R}{I} \times \frac{R}{J}$$

### 2.2 Radical Ideals

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

#### Definition 2.2.1: 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 2.2.2**

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 show 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.  $\square$

**Proposition 2.2.3**

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

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

*Proof.*

- Let  $x \in \sqrt{IJ}$ . Then  $x^n \in IJ$ . This means that there exists  $i \in I$  and  $j \in J$  such that  $x^n = ij$ . Since  $I$  and  $J$  are two sided ideals, we can conclude that  $x^n = ij \in I, J$ . Hence  $x^n = ij \in I \cap J$ . We conclude that  $x \in \sqrt{I \cap J}$ . Now let  $x \in \sqrt{I \cap J}$ . Then there exists  $n \in \mathbb{N}$  such that  $x^n \in I \cap J$ . Then  $x^n \in I$  and  $x^n \in J$  implies that  $x^{2n} = x^n \cdot x^n \in IJ$ . We conclude that  $x \in \sqrt{IJ}$ .  $\square$

**Proposition 2.2.4**

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

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

**Definition 2.2.5: 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 2.2.6**

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

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

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

**Theorem 2.2.7**

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

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

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:

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

and

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

## 2.3 Nilradical and Jacobson Ideals

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 2.3.1: Nilradicals

Let  $R$  be a 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 2.3.2

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 2.3.3**

Let  $R$  be a commutative ring. The nilradical of  $R$  is the intersection of all prime ideals of  $R$ .

*Proof.* We want to show that

$$N(R) = \bigcap_{P \in \text{Spec}(R)} P$$

Trivially  $N(R)$  is a prime ideal. Now suppose that  $r \in R$  is in the intersection of all prime ideals. Then  $r^n$  also lies in every prime ideal.

□

**Example 2.3.4**

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  $(x, y) \supseteq (x^2 - y, xy)$  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 2.3.5: Reduced Rings**

Let  $R$  be a commutative ring. We say that  $R$  is reduced if  $N(R) = 0$ .

**Proposition 2.3.6**

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.

Recall the notion of the Jacobson radical from Rings and Modules. Let  $R$  be a ring. The Jacobson radical of  $R$  is the radical

$$J(R) = \text{rad}(R) = \bigcap_{\substack{S \trianglelefteq R \\ R \text{ is cosimple}}} S$$

of  $R$  considered as a left  $R$ -module. But when  $R$  is a commutative ring, this description can be simplified.

### Proposition 2.3.7

Let  $R$  be a commutative ring. Then

$$J(R) = \bigcap_{m \in \max\text{Spec}(R)} m$$

*Proof.* Submodules of  $R$  are precisely ideals of  $R$  and cosimple ideals are ideals  $I$  of  $R$  for which  $R/I$  is simple. But if  $R/I$  is simple, then  $R/I$  contains no ideals which means that  $R/I$  is a field. So  $I$  is a maximal ideal.  $\square$

Recall some properties of the Jacobson radical from Rings and Modules. For a (not necessarily commutative ring  $R$ ),

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

### Proposition 2.3.8

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.*  $\square$

## 2.4 Extensions and Contractions of Ideals

### Definition 2.4.1: 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 2.4.2

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.

- 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:  $(I_1 I_2)^e = I_1^e I_2^e$
- $(I_1/I_2)^e \subseteq I_1^e/I_2^e$
- $\text{rad}(I)^e \subseteq \text{rad}(I^e)$

### Definition 2.4.3: 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 2.4.4**

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.

- $(J_1 + J_2)^e \supseteq J_1^e + J_2^e$
- Closed under intersections:  $(J_1 \cap J_2)^e = J_1^e \cap J_2^e$
- $(J_1 J_2)^e \supseteq J_1^e J_2^e$
- $(J_1/J_2)^e \subseteq J_1^e/J_2^e$
- Closed under taking radicals:  $\text{rad}(J)^e = \text{rad}(J^e)$

**Proposition 2.4.5**

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.

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

**2.5 Revisiting the Polynomial Ring****Proposition 2.5.1**

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.  $\square$

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 maybe 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 Simplifying Generators of an Ideal

#### 3.1 Ordering on the Monomials

Recall that a monomial in  $R[x_1, \dots, x_n]$  is an element in the polynomial ring of the form  $x_1^{a_1} \cdots x_n^{a_n}$ . For simplicity we write this as  $x^{(a_1, \dots, a_n)}$ .

##### Definition 3.1.1: Monomial Ordering

A monomial ordering on a polynomial ring  $k[x_1, \dots, x_n]$  is a relation  $>$  on  $\mathbb{N}^n$ . This means that the following are true.

- $>$  is a total ordering on  $\mathbb{N}^n$
- If  $a > b$  and  $c \in \mathbb{N}^n$  then  $a + c > b + c$
- $>$  is a well ordering on  $\mathbb{N}^n$  (any nonempty subset of  $\mathbb{N}^n$  has a smallest element)

##### Definition 3.1.2: Lexicographical Order

Let  $a = (a_1, \dots, a_n)$  and  $b = (b_1, \dots, b_n)$  in  $\mathbb{N}^n$ . We say that  $a >_{\text{lex}} b$  if in the first nonzero entry of  $a - b$  is positive.

In practise this means that the we value more powers of  $x_1$

##### Definition 3.1.3: Graded Lex Order

Let  $a = (a_1, \dots, a_n)$  and  $b = (b_1, \dots, b_n)$  in  $\mathbb{N}^n$ . We say that  $a >_{\text{grlex}} b$  if either of the following holds.

- $|a| = \sum_{k=1}^n a_k > \sum_{k=1}^n b_k = |b|$
- $|a| = |b|$  and  $a >_{\text{lex}} b$

##### Definition 3.1.4: Graded Lex Order

Let  $a = (a_1, \dots, a_n)$  and  $b = (b_1, \dots, b_n)$  in  $\mathbb{N}^n$ . We say that  $a >_{\text{grlex}} b$  if either of the following holds.

- $|a| = \sum_{k=1}^n a_k > \sum_{k=1}^n b_k = |b|$
- $|a| = |b|$  and the last nonzero entry of  $a - b$  is negative.

In practise we value lower powers of the last variable  $x_n$ .

##### Proposition 3.1.5

The above three orders are all monomial orderings of  $k[x_1, \dots, x_n]$ .

##### Definition 3.1.6: Multidegree

Let  $f \in k[x_1, \dots, x_n]$  be a polynomial in the form  $f = \sum_{v \in \mathbb{N}^n} c_v x^v$ . Define the multidegree of  $f$  to be

$$\text{multideg}(f) = \max_{>} \{v \in \mathbb{N}^n | a_v \neq 0\}$$

where  $>$  is a monomial ordering on  $k[x_1, \dots, x_n]$ .

##### Definition 3.1.7: Leading Objects

Let  $f \in k[x_1, \dots, x_n]$  be a polynomial in the form  $f = \sum_{v \in \mathbb{N}^n} c_v x^v$ .

- Define the leading coefficient of  $f$  to be  $\text{LC}(f) = c_{\text{multideg}(f)} \in k$
- Define the leading monomial of  $f$  to be  $\text{LM}(f) = x_{\text{multideg}(f)} \in k$
- Define the leading term of  $f$  to be  $\text{LT}(f) = \text{LC}(f) \cdot \text{LM}(f)$

**Proposition 3.1.8: Division Algorithm in  $k[x_1, \dots, x_n]$** **3.2 Monomial Ideals****Definition 3.2.1: Monomial Ideals**

An ideal  $I \subset k[x_1, \dots, x_n]$  is said to be a monomial ideal if  $I$  is generated by a set of monomials  $\{x^v | v \in A\}$  for some  $A \subset \mathbb{N}^n$ . In this case we write

$$I = \langle x^v | v \in A \rangle$$

**Lemma 3.2.2**

Let  $I = \langle x^v | v \in A \rangle$  be an ideal of  $k[x_1, \dots, x_n]$ . Then a monomial  $x^w$  lies in  $I$  if and only if  $x^v | x^w$  for some  $v \in A$ . Moreover, if  $f = \sum_{w \in \mathbb{N}^n} c_w x^w \in k[x_1, \dots, x_n]$  lies in  $I$ , then each  $x^w$  is divisible by  $x^v$  for some  $v \in A$ .

**Theorem 3.2.3: Dickson's Lemma**

Every monomial ideal is finitely generated. In particular, every monomial ideal  $I = \langle x^v | v \in A \rangle$  is of the form

$$I = \langle x^{v_1}, \dots, x^{v_n} \rangle$$

where  $v_1, \dots, v_n \in A$ .

**3.3 Groebner Bases**

## 4 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.

### 4.1 Cayley-Hamilton Theorem

#### Definition 4.1.1: 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 4.1.2: Cayley-Hamilton Theorem

Let  $R$  be a commutative ring. Let  $A \in M_{n \times n}(R)$  be a matrix. Then  $c_A(A) = 0$ .

#### Corollary 4.1.3

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  $a_1, \dots, a_n \in I$  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.  $\square$

## 4.2 Nakayama's Lemma

### Lemma 4.2.1: 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.  $\square$

### Lemma 4.2.2: 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  $M = r^{-1}rM = 0$ .  $\square$

### Corollary 4.2.3

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  $M = N$ .  $\square$

### Corollary 4.2.4

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

*Proof.* For the first part, we already know that  $M/mM$  is an  $R$ -module. We notice that for any  $k \in m$  and  $t + mM \in M/mM$  we have that  $k(t + mM) = kt + kmM$ . But  $kt \in m$  means that  $kt + kmM = mM$ . Hence  $M/mM$  is well defined as an  $R/m$ -module. Now suppose that  $M$  is finitely generated by the elements  $a_1, \dots, a_n$ . Let  $x + mM \in M/mM$ . Then there exists  $r_k \in R$  such that  $x = r_1 a_1 + \dots + r_n a_n$ . But this means that

$$x + mM = r_1(a_1 + mM) + \dots + r_n(a_n + mM)$$

This means that  $M/mM$  is generated by  $a_1 + mM, \dots, a_n + mM$ . We conclude that  $M/mM$  is finite dimensional.

Suppose that  $a_1, \dots, a_n \in M$  generates  $M$  as an  $R$ -module. By the same argument as above, we can see that  $a_1 + mM, \dots, a_n + mM$  is a set of generators for  $M/mM$ . 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.  $\square$

### 4.3 Change of Rings

#### Definition 4.3.1: 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 4.3.2: 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 4.3.3

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

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

## 5 Algebra Over a Commutative Ring

### 5.1 Commutative Algebras

#### Definition 5.1.1: Commutative Algebras

Let  $R$  be a commutative ring. A commutative  $R$ -algebra is an  $R$ -algebra  $A$  that is commutative.

#### Proposition 5.1.2

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.  $\square$

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.

### 5.2 Finitely Generated Algebra

#### Definition 5.2.1: Finitely Generated Algebra

Let  $A$  be a commutative algebra over a ring  $R$ . We say that  $A$  is a finitely generated algebra if there exists a finite set of elements  $a_1, \dots, a_n$  such that  $A$  is generated by  $a_1, \dots, a_n$ . Explicitly, this means that for all  $a \in A$ , there exists  $c_{i_1, \dots, i_n} \in R$  for  $i_1, \dots, i_n \in \mathbb{N}$  such that

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

Finitely generated algebras are also called algebra of finite type.

#### Theorem 5.2.2

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 5.2.3: 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 5.2.4**

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. □

## 6 Localization

### 6.1 Localization of a Ring

#### Definition 6.1.1: 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 6.1.2: Localization of a Ring

Let  $R$  be a commutative ring and  $S \subseteq R$  be a multiplicative set. Define the ring of fractions of  $R$  with respect to  $S$  by

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

where  $\sim$  is defined by

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

If  $S = \{1, f, f^2, \dots\}$  then we write  $S^{-1}R = R_f = R[1/f]$ .

#### Proposition 6.1.3

Let  $S^{-1}R$  be a ring of fractions.

- $\sim$  as defined in the ring of fractions is an equivalence relation
- $(S^{-1}R, +, \times)$  is a ring
- The map  $\phi : R \rightarrow S^{-1}R$  defined by  $\phi(r) \rightarrow \frac{r}{1}$  is a ring homomorphism

*Proof.*

- Trivial
- 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  $\frac{1}{1}$ .
- We have that  $\phi(r + s) = \frac{r+s}{1} = \frac{r}{1} + \frac{s}{1} = \phi(r) + \phi(s)$  and  $\phi(rs) = \frac{rs}{1} = \frac{r}{1} \cdot \frac{s}{1} = \phi(r) \cdot \phi(s)$  for any  $r, s \in R$ .

□

#### Theorem 6.1.4: Universal Property

Let  $g : A \rightarrow B$  be a ring homomorphism such that  $g(s)$  is a unit in  $B$  for all  $s \in S$ . Then there exists a unique ring homomorphism  $h : S^{-1}A \rightarrow B$  such that  $g = h \circ \phi$ . In other words, the following diagram commutes:

$$\begin{array}{ccc} A & \xrightarrow{\phi} & S^{-1}A \\ & \searrow g & \downarrow \exists! h \\ & & B \end{array}$$

## 6.2 Localization at a Prime Ideal

### Lemma 6.2.1

Let  $R$  be a 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  $xy \notin P$ .  $\square$

### Definition 6.2.2: Localization on Prime Ideals

Let  $R$  be a commutative ring. Let  $P$  be a prime ideal. Denote

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

the localization of  $R$  at  $P$ .

### Lemma 6.2.3

Let  $R$  be an integral domain. Then the localization

$$(R \setminus (0))^{-1}R$$

is exactly the field of fractions of  $R$ .

### Proposition 6.2.4

Let  $R$  be a ring and let  $p$  be a prime ideal of  $R$ . Then  $R_p$  is a local ring.

*Proof.* Let  $I$  be the set of all non-units of  $R_p$ . It is sufficient to show that  $I$  is an ideal by the above lemma. Clearly if  $i \in I$  then  $r \cdot i$  is also not invertible. Explicitly, we have

$$I = \left\{ \frac{r}{s} \in R_p \mid r \in p \right\}$$

Let  $\frac{r_1}{s_1}, \frac{r_2}{s_2} \in I$ , then  $\frac{r_1}{s_1} + \frac{r_2}{s_2} = \frac{r_1 s_2 + r_2 s_1}{s_1 s_2}$  is in  $I$  since  $r_1, r_2 \in p$  and  $p$  being an ideal implies  $r_1 s_2 + r_2 s_1 \in p$ .  $\square$

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.

## 6.3 Properties of Localization

### Proposition 6.3.1

Localization commutes with direct sum of modules and quotient modules.

## 6.4 Localization of a Module

### Definition 6.4.1: 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

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

If  $S = \{1, f, f^2, \dots\}$  then we write  $S^{-1}M = M_f = M[1/f]$ .

### Proposition 6.4.2

Let  $S$  be a multiplicative set of a ring  $R$ . Then localization at  $S$  preserves exact sequences.

### Proposition 6.4.3

Let  $M$  be an  $A$ -module. Then the  $S^{-1}A$  modules  $S^{-1}M$  is isomorphic to  $S^{-1}A \otimes_A M$ . More precisely, there exists a unique isomorphism  $f : S^{-1}A \otimes_A M \rightarrow S^{-1}M$  such that

$$f((a/s) \otimes m) = am/s$$

## 7 Primary Decomposition

### 7.1 Support of a Module

#### Definition 7.1.1: Support of a Module

Let  $A$  be a commutative ring. Let  $M$  be an  $A$ -module. The support of  $M$  is the subset

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

### 7.2 Associated Prime

#### Definition 7.2.1: Associated Prime

Let  $M$  be an  $A$ -module. An associated prime  $P$  of  $M$  is a prime ideal of  $A$  such that there exists some  $m \in M$  such that  $P = \text{Ann}(m)$ .

### 7.3 Primary Ideals

#### Definition 7.3.1: 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 7.3.2

Let  $A$  be a commutative ring. Let  $Q$  be a primary ideal of  $A$ . Then  $\sqrt{Q}$  is the smallest prime ideal containing  $Q$ .

#### Lemma 7.3.3

Let  $R$  be a Noetherian ring and  $I$  be a proper ideal that is not primary. Then

$$I = J_1 \cap J_2$$

for some ideals  $J_1, J_2 \neq I$ .

#### Definition 7.3.4: P-Primary Ideals

Let  $A$  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  $A$  if

$$Q = \sqrt{P}$$

#### Theorem 7.3.5

Let  $A$  be a Noetherian ring and  $Q$  an ideal of  $A$ . Then  $Q$  is  $P$ -primary if and only if  $\text{Ann}(A/Q) = \{P\}$ .

### 7.4 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 7.4.1: 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

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

**Definition 7.4.2: 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 7.4.3**

Every proper ideal in a Noetherian ring has a primary decomposition.

**Lemma 7.4.4**

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



## 8 Integral Dependence

### 8.1 Integral Extensions

#### Definition 8.1.1: Integral Elements

Let  $B$  be a 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  $p(b) = 0$ .

#### Proposition 8.1.2

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

- $b$  is integral over  $A$
- The subring  $A[b] \subseteq B$  is finite over  $A$
- There exists an  $A$  sub-algebra  $A' \subseteq B$  such that  $A[b] \subseteq A'$  and  $A'$  is finite over  $A$ .

#### Proposition 8.1.3

Let  $B$  be a 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  $b_1 b_2$  are both integral over  $A$ .

#### Definition 8.1.4: Integral Extensions

Let  $B$  be a ring and let  $A \subseteq B$  be a subring. We say that  $B$  is integral over  $A$  if all elements of  $B$  are integral over  $A$ .

#### Lemma 8.1.5

Let  $A \subseteq B \subseteq C$  be rings. If  $C$  is integral over  $B$  and  $B$  is integral over  $A$ , then  $C$  is integral over  $A$ .

#### Definition 8.1.6: Integral Closure

Let  $B$  be an  $A$ -algebra. Define the subring

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

to be the integral closure of  $A$  in  $B$ . If  $\overline{A} = A$ , then we say that  $A$  is integrally closed in  $B$ .

#### Lemma 8.1.7

Let  $B$  be a ring and let  $A \subseteq B$  be a subring. Then  $\overline{A}$  is an integral extension of  $A$ .

#### Definition 8.1.8: Normal Domains

Let  $R$  be a domain. We say that  $R$  is normal (integrally closed) if  $R$  is integrally closed in its field of fractions.

The integral closure of  $R$  in  $\text{Frac}(R)$  is called the normalization of  $R$ .

## 8.2 The Going-Up and Going-Down Theorems

## 8.3 Dedekind Domains

### Definition 8.3.1: Dedekind Domains

Let  $R$  be a ring. We say that  $R$  is a dedekind domain if the following are true.

- $R$  is an integral domain
- $R$  is an integrally closed
- $R$  is Noetherian
- Every non-zero prime ideal of  $R$  is maximal

## 9 Discrete Valuation Rings

### 9.1 Discrete Valuation Rings

#### Definition 9.1.1: Totally Ordered Group

A totally ordered group is a group  $G$  with a total order " $\leq$ " such that it is

- a left ordered group:  $a \leq b$  implies  $ca \leq cb$  for all  $a, b, c \in G$
- a right ordered group:  $a \leq b$  implies  $ac \leq bc$  for all  $a, b, c \in G$

#### Definition 9.1.2: 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  $v : K \setminus \{0\} \rightarrow G$  such that for all  $x, y \in K^*$ , we have

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

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

$v$  is said to be a discrete valuation if  $G = \mathbb{Z}$ .

#### Proposition 9.1.3

Let  $K$  be a field and  $v : K \rightarrow \mathbb{Z}$  a discrete valuation. Then

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

is a subring of  $K$ .

#### Definition 9.1.4: Discrete Valuation Rings

The discrete valuation ring of a discrete valuation  $v : K \rightarrow \mathbb{Z}$  is the subset

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

Alternatively, any ring isomorphic to a discrete valuation ring of some discrete valuation is also called a discrete valuation.

#### Proposition 9.1.5

Let  $R$  be a discrete valuation ring with respect to the valuation  $v$ . Let  $t \in R$  be such that  $v(t) = 1$ . Then the following are true.

- A nonzero element  $u \in R$  is a unit if and only if  $v(u) = 0$
- Every non-zero ideal of  $R$  is a principal ideal of the form  $(t^n)$  for some  $n \geq 0$
- Every  $r \in R \setminus \{0\}$  can be written in the form  $r = ut^n$  for some unit  $u$  and  $n \geq 0$ .

*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.

- Let  $t \in R$  such that  $v(t) = 1$ . Let  $x \in m$  where  $v(x) = n > 0$ . Then  $v(x) = nv(t) = v(t^n)$  means that every  $x \in m$  is of the form  $t^n$ . Thus  $m = (t)$ . Since every ideal  $I$  is a subset of this maximal ideal, any ideal is of the form  $I = (t^n)$  for some  $n > 0$ .
- Follows from the fact that  $(t^n)$  is the unique maximal ideal.



### Proposition 9.1.6

Let  $R$  be an integral domain. Then the following are equivalent.

- $R$  is a discrete valuation ring
- $R$  is a UFD with a unique irreducible element up to multiplication of a unit
- $R$  is a Noetherian local ring with a principal maximal ideal

*Proof.*

- (1)  $\implies$  (3): We have seen that the set of non-units is precisely the set  $m = \{x \in R \mid v(x) > 0\}$ . We show that this is an ideal. Clearly  $x, y \in m$  implies  $v(x + y) = \min\{v(x), v(y)\} > 0$ . Let  $u \in R$ . Then  $v(ux) = v(u) + v(x) > 0$  since  $v(x) > 0$  and  $v(u) \geq 0$ .

We have seen that every ideal is of the form  $(t^n)$  for some  $n > 0$ . Thus every ascending chains of ideal must be of the form

$$(t^{n_1}) \subset (t^{n_2}) \subset \dots$$

for  $n_1 > n_2 > \dots$ . Since  $n_1, n_2, \dots$  is strictly decreasing, the chain must eventually stabilizes. This proves that  $R$  is Noetherian and has principal maximal ideal.

- (1)  $\implies$  (3):



## 10 Dimension Theory for Rings

### 10.1 Dimension and Height

#### Definition 10.1.1: Krull Dimension

Let  $R$  be a commutative ring. Define the Krull dimension of  $R$  to be

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

#### Definition 10.1.2: Height of a Prime Ideal

Let  $p$  be a prime ideal in a ring  $R$ . Define the height of  $p$  to be

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

#### Lemma 10.1.3

Let  $p$  be a prime ideal in a ring  $R$ . Then

$$\text{ht}(p) = \dim(R_p)$$

#### Theorem 10.1.4: 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

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

### 10.2 Length of a Module

#### Definition 10.2.1: Length of a Module

Let  $R$  be a ring and let  $M$  be an  $R$ -module. Define the length of  $M$  to be

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

#### Lemma 10.2.2

Let  $R$  be a ring. Let  $0 \rightarrow M' \rightarrow M \rightarrow M'' \rightarrow 0$  be a short exact sequence of  $R$ -modules. Then

$$l_R(M) = l_R(M') + l_R(M'')$$

#### Lemma 10.2.3

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

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

#### Proposition 10.2.4

Let  $R$  be a ring and let  $M$  be an  $R$ -module. Then the following are equivalent.

- $M$  is simple
- $l_R(M) = 1$
- $M \cong A/m$  for some maximal ideal  $m$  of  $A$

### 10.3 The Hilbert Polynomial

#### Definition 10.3.1: The Hilbert Polynomial

Let  $R = \bigoplus_{k=0}^{\infty} R_k$  be a Noetherian graded ring. Let  $M = \bigoplus_{k=0}^{\infty} M_k$  be a graded  $R$ -module. Define the Hilbert function  $H_M : \mathbb{N} \rightarrow \mathbb{N}$  of  $R$  to be the function defined by

$$H_M(n) = l_{R_0}(M_n)$$

#### Definition 10.3.2: The Hilbert Series

Let  $R = \bigoplus_{k=0}^{\infty} R_k$  be a Noetherian graded ring. Let  $M = \bigoplus_{k=0}^{\infty} M_k$  be a graded  $R$ -module. Define the Hilbert series  $HS_M \in \mathbb{Z}[[t]]$  of  $M$  to be the formal series

$$HS_M(t) = \sum_{k=0}^{\infty} H_M(k)t^k = \sum_{k=0}^{\infty} l_{R_0}(M_k)t^k$$

#### Theorem 10.3.3

Let  $R = \bigoplus_{k=0}^{\infty} R_k$  be a Noetherian graded ring such that  $R_0$  is Artinian. Let  $M = \bigoplus_{k=0}^{\infty} M_k$  be a graded  $R$ -module. Let  $\lambda : \{M_i \mid i \in I\} \rightarrow \mathbb{Z}$  be an additive function. Then the function

$$g(t) = \sum_{k=0}^{\infty} \lambda(M_k)t^k$$

is a rational function and can be written in the form

$$g(t) = \frac{f(t)}{\prod_{i=1}^r (1 - t^{d_i})}$$

for some  $f(t) \in \mathbb{Z}[t]$  and  $d_i \in \mathbb{N}$ .

#### Theorem 10.3.4: The Fundamental Theorem of Dimension Theory

Let  $(R, m)$  be a local Noetherian ring. Let  $I$  be an  $m$ -primary ideal. Then the following numbers are equal.

- Let  $J = \bigoplus_{k=0}^{\infty} \frac{I^k}{I^{k+1}}$ . The order of the pole at 1 of the rational function  $HS_J$ .
- The minimum number of elements of  $R$  that can generate an  $m$ -primary ideal of  $R$
- The dimension  $\dim_{R/m}(R)$

The following is a generalization of Krull's principal ideal theorem. Both of the theorems can actually be deduced directly from the fundamental theorem.

#### Theorem 10.3.5: Krull's Height Theorem

Let  $R$  be a Noetherian ring. Let  $I$  be a proper ideal generated by  $n$  elements. Let  $p$  be the smallest prime ideal containing  $I$ . Then

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

#### Theorem 10.3.6

Let  $(R, m)$  be a Noetherian local ring and let  $k = R/m$  be the residue field. Then

$$\dim(R) \leq \dim_k(m/m^2)$$

## 10.4 Global Dimension of a Ring