Commutative Algebra 1

Labix

December 4, 2024

Abstract

Contents

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 nth 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 $k[[x]]$. □

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

1.2 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.

Theorem 1.2.1: Hilbert's Basis Theorem

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

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

is a Noetherian ring.

Proposition 1.2.2

Let $R = \bigoplus_{i=0}^{n} R_i$ 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 Artinian Commutative Rings

We recall some facts about Artinian 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 Artinian if and only if M_1 and M_3 are Artinian.
- If M and N are R-modules, then $M \oplus N$ is Artinian if and only if M and N are Artinian.

- If M is an R-module and N is an R-submodule of M, then M is Artinian if and only if N and M/N are Artinian.
- If R is Artinian and I is an ideal of R, then R/I is Artinian.

Proposition 1.3.1

Let R be an integral domain. Then R is Artinian if and only if R is a field.

Proposition 1.3.2

Let R be a commutative ring. If R is Artinian, then the following are true.
- Every prime ideal of R is maximal
- There is an equality $N(R) = J(R)$
- R has only a finite number of maximal ideals

Theorem 1.3.3: (Hopkins)

Let R be a commutative ring. If R is Artinian then R is Noetherian.

1.4 Spectra of a Ring

Definition 1.4.1: 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 1.4.2: 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 1.4.3

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 1.4.4

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

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

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 P 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 $f_1 : R \times S \to R$ 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 $\overline{J}$ denote the ideal of R/I corresponding to J under the correspondence theorem. Then there is an isomorphism

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

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

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 quotieting by the ideal (3) gives the field $\mathbb{Z}/3\mathbb{Z}$. □

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

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

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 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.

□

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 $x \in \sqrt{IJ}$.

□

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:

$$\begin{matrix}\text{Maximal} \\ \text{ideals}\end{matrix} \subset \begin{matrix}\text{Prime} \\ \text{ideals}\end{matrix} \subset \begin{matrix}\text{Radical} \\ \text{ideals}\end{matrix}$$

Theorem 2.2.7

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

$$\left\{\begin{matrix}\text{Ideals of } R \\ \text{containing } I\end{matrix}\right\} \overset{1:1}{\longleftrightarrow} \{\text{Ideals of } R/I\}$$

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:

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

and

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

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

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

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. □

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. □

2.4 Extensions and Contractions of Ideals

Definition 2.4.1: Extension of Ideals

Let R, S be commutative rings. Let $f : R \to S$ 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 $f : R \to S$ 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 $f : R \to S$ 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 $f : R \to S$ 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 $f : R \to S$ 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. □

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 $R[x_1, \ldots, x_n]$ 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 $x^{(a_1,\ldots,a_n)}$.

Definition 3.1.1: Monomial Ordering

A monomial ordering on a polynomial ring $k[x_1, \ldots, x_n]$ 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 $a = (a_1, \ldots, a_n)$ and $b = (b_1, \ldots, b_n)$ 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 $a = (a_1, \ldots, a_n)$ and $b = (b_1, \ldots, b_n)$ 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 $a = (a_1, \ldots, a_n)$ and $b = (b_1, \ldots, b_n)$ 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 $k[x_1, \ldots, x_n]$.

Definition 3.1.6: Multidegree

Let $f \in k[x_1, \ldots, x_n]$ 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 $k[x_1, \ldots, x_n]$.

Definition 3.1.7: Leading Objects

Let $f \in k[x_1, \ldots, x_n]$ 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 $\text{LM}(f) = c_{\text{multideg(f)}} \in k$
- Define the leading term of f to be $\text{LT} = \text{LC}(f) \cdot \text{LM}(f)$

Proposition 3.1.8: Division Algorithm in $k[x_1, \ldots, x_n]$

3.2 Monomial Ideals

Definition 3.2.1: Monomial Ideals

An ideal $I \subset k[x_1, \ldots, x_n]$ 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 $k[x_1, \ldots, x_n]$. Then a monomial x^w lies in I if and only if $x^v | x^w$ for some $v \in A$. Moreover, if $f = \sum_{w \in \mathbb{N}^n} c_w x^w \in k[x_1, \ldots, x_n]$ 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

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

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

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 $\cdot : R \times M \to M$ 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 $\varphi \in \mathrm{End}_R(M)$. If $\varphi(M) \subseteq IM$, then there exists $a_1, \ldots, a_n \in I$ such that

$$\varphi^n + a_1\varphi^{n-1} + \cdots + a_{n-1}\varphi + \mathrm{id}_M = 0 : M \to M$$

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

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

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 ρ 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. □

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 $\varphi = \mathrm{id}_M$. Then φ is surjective so that $M = \varphi(M) \subseteq IM$. By crl 4.1.3, there exists $r_1, \ldots, r_n \in I$ such that $(1 + r_1 + \cdots + r_n)M = 0$. By choosing $r = 1 + r_1 + \cdots + r_n$, we see that $rM = 0$ and $r - 1 \in I$ so that we conclude. □

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 $M = r^{-1}rM = 0$. □

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

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

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 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.
- $a_1, \ldots, a_n \in M$ generates M as an R-module if and only if $a_1 + mM, \ldots, a_n + mM$

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 $a_1, \ldots, a_n$. Let $x + mM \in M/mM$. Then there exists $r_k \in R$ such that $x = r_1 a_1 + \cdots + r_n a_n$. But this means that

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

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

Suppose that $a_1, \ldots, a_n \in M$ generates M as an R-module. By the same argument as above, we can see that $a_1 + mM, \ldots, a_n + mM$ is a set of generators for M/mM. For the other direction, suppose that $a_1 + mM, \ldots, a_n + mM$ generates M/mM as an R/m-vector space. Define $N = Ra_1 + \cdots + Ra_n \leq M$. 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 $x + mM = r_1(a_1 + mM) + \cdots + r_n(a_n + M)$. 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 $M = N = Ra_1 + \cdots + Ra_n$ so that M is generated by $a_1, \ldots, a_n$. And so we are done. □

4.3 Change of Rings

Definition 4.3.1: Extension of Scalars

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

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

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

- For $f \in \mathrm{Hom}_S(S \otimes_R M, N)$, define the map $f^+ \in \mathrm{Hom}_R(M, N)$ by
$$f^+(m) = f(1 \otimes m)$$
- For $g \in \mathrm{Hom}_R(M, N)$, define the map $g^- \in \mathrm{Hom}_S(S \otimes_R M, N)$ by
$$g^-(s \otimes m) = s \cdot g(m)$$

4.4 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 4.4.1

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

In particular, it is an abelian group.

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 ϕ

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 4.4.2

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 4.4.3: Induced Map of Hom

Let R be a commutative ring. Let M_1, M_2, N be R-modules. Let $f : M_1 \to M_2$ be an R-module homomorphism. Define the induced map

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

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

Lemma 4.4.4

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

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

is an R-module homomorphism.

4.5 Applying Hom and Tensor to Exact Sequences

Proposition 4.5.1

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 sequence

$$0 \longrightarrow \text{Hom}_R(M_3.N) \xrightarrow{g^*} \text{Hom}_R(M_2, N) \xrightarrow{f^*} \text{Hom}_R(M_1, N)$$

is 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 $k \in \text{im}(f)$, ϕ descends to a map $\overline{\phi} : \frac{B}{\text{im}(f)} \to G$. But $\text{im}(f) = \ker(g)$ hence this is equivalent to a map $\overline{\phi} : \frac{B}{\ker(g)} \to G$. But by the first isomorphism theorem and the fact that g is surjective, we conclude that $\overline{g} : \frac{B}{\ker(g)} \overset{g}{\cong} C$, where $b + \ker(g) \mapsto g(b)$. Thus we have constructed a map $\overline{\phi} \circ \overline{g}^{-1} : C \to G$ given by $g(b) \mapsto b + \ker(g) \mapsto \phi(b)$. But now $g^*(\overline{\phi} \circ \overline{g}^{-1})$ is the map defined by
$$b \mapsto g(b) \mapsto b + \ker(g) \mapsto \phi(b)$$
and so this map is exactly ϕ. Thus $\phi \in \text{im}(g^*)$.

□

Proposition 4.5.2

Let R be a 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

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

is exact.

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

5 Localization

5.1 Localization of a Ring

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 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

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

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 5.1.3

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 $k : R \to S^{-1}R$ defined by $r \mapsto r/1$ is a ring homomorphism, called the localization map.

Proof.

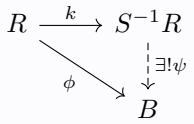
- Trivial
- Define addition by $\frac{r}{s} + \frac{r'}{s'} = \frac{rs'+r's}{ss'}$ and multiplication by $\frac{r}{s} \cdot \frac{r'}{s'} = \frac{rr'}{ss'}$. Clearly addition is abelian, and has identity $\frac{0}{1}$ and inverse $\frac{-r}{s}$ for any $\frac{r}{s} \in S^{-1}R$. Multiplication also has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

□

Proposition 5.1.4: Universal Property

Let R be a commutative ring. Let S be a multiplicative subset of R. Let $k : R \to S^{-1}R$ be localization map. Then the following is true.

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



Lemma 5.1.5

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.

5.2 Localization at a Prime Ideal

Lemma 5.2.1

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 $xy \notin P$. □

Definition 5.2.2: 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 5.2.3

Let R be an integral domain. Then we have

$$\text{Frac}(R) = R_{(0)}$$

Proposition 5.2.4

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. 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

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

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 $r_1 s_2 + r_2 s_1 \in P$. □

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.

5.3 Localization of a Module

Definition 5.3.1: 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

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

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

$$S^{-1}M = M_f = M[1/f]$$

Lemma 5.3.2

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 an $S^{-1}R$-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 5.3.3: 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 $\phi : M \to N$ be an R-module homomorphism. Define the induced map

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

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

Lemma 5.3.4

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

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

is a well defined ring homomorphism.

Proposition 5.3.5

Let R be a commutative ring. Let $S \subseteq R$ be a multiplicative subset. 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 the following is an exact sequence of $S^{-1}R$-modules.

$$0 \longrightarrow S^{-1}M_1 \xrightarrow{S^{-1}f} S^{-1}M_2 \xrightarrow{S^{-1}g} S^{-1}M_3 \longrightarrow 0$$

Corollary 5.3.6

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.

- If N_1, N_2 are R-submodules of M, then
$$S^{-1}(N_1 + N_2) = S^{-1}N_1 + S^{-1}N_2$$
as $S^{-1}R$-submodules of $S^{-1}M$.
- 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 $S^{-1}M$.
- 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.
- If N is an R-module, then
$$S^{-1}(M \oplus N) \cong S^{-1}M \oplus S^{-1}N$$
as $S^{-1}R$-modules.

Proposition 5.3.7

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

Lemma 5.3.8

Let R be a commutative ring. Let $S \subseteq R$ be a multiplicative subset. Let M, N be R-modules. Let $\phi : M \to N$ 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 images:
$$S^{-1}(\operatorname{im}\phi) \cong \operatorname{im}(S^{-1}\phi)$$
- Localization commutes with cokernels:
$$S^{-1}\frac{N}{\operatorname{im}(\phi)} \cong \frac{S^{-1}N}{\operatorname{im}(S^{-1}\phi)}$$

5.4 Local Properties

Definition 5.4.1: Local Properties

Let R be a commutative ring. Let M be an R-module.

- A property of R-modules is local if the following is true. M has the property if and only if M_P has the property for all prime ideals P.
- 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.

More local properties: zero, nilpotent, injective, surjective, isomorphic
Non-local properties: freeness, domain

Proposition 5.4.2: Exactness is Local

Let R be a commutative ring. Let M_1, M_2, M_3 be R-modules. Let $f : M_1 \to M_2$ and $g : M_2 \to M_3$ be R-module homomorphisms. Then the following conditions are equivalent.

- The following sequence is exact:

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

- The following sequence is exact:

$$0 \longrightarrow (M_1)_P \xrightarrow{f_P} (M_2)_P \xrightarrow{g_P} (M_3)_P \longrightarrow 0$$

  for all prime ideals P of R.
- The following sequence is exact:

$$0 \longrightarrow (M_1)_m \xrightarrow{f_m} (M_2)_m \xrightarrow{g_m} (M_3)_m \longrightarrow 0$$

  for all maximal ideals m of R.

5.5 Ideals of a Localization

Definition 5.5.1: 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 5.5.2: L

t R be a commutative ring. Let I be an ideal of R. Let $S \subseteq R$ be a multiplicative subset. Let $\iota : R \hookrightarrow S^{-1}R$ be the inclusion homomorphism. Then we have

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

Theorem 5.5.3

Let R be a commutative ring. Let I be an ideal of R. Let $S \subseteq R$ be a multiplicative subset. Let $\iota : R \hookrightarrow S^{-1}R$ be the inclusion homomorphism. Then there is a one-to-one bijection

$$\{J \mid J \text{ is an ideal of } S^{-1}R\} \xleftrightarrow{1:1} \left\{I \mid \begin{smallmatrix} I \text{ is an ideal of } R \text{ and} \\ I \text{ is closed under division by } S \end{smallmatrix}\right\}$$

given by $J \mapsto J^c$.

Proposition 5.5.4

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

$$\{J \mid J \text{ is a prime ideal of } S^{-1}R\} \xleftrightarrow{1:1} \left\{ I \;\middle|\; \begin{smallmatrix} I \text{ is a prime ideal of } R \text{ and} \\ I \cap S = \emptyset \end{smallmatrix} \right\}$$

6 Primary Decomposition

6.1 Support of a Module

Definition 6.1.1: Support of a Module

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

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

6.2 Associated Prime

Definition 6.2.1: 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 $P = \text{Ann}(m)$.

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

Lemma 6.3.3

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 6.3.4: 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 6.3.5

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

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 $P_1, \ldots, P_n$. 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 $Q_1, \ldots, Q_r$ of A such that

$$I = Q_1 \cap \cdots \cap Q_r$$

Definition 6.4.2: Minimal Primary Decompositions

Let A be a commutative ring. Let I be an ideal of A. Let

$$I = Q_1 \cap \cdots \cap Q_r$$

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 6.4.3

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

Lemma 6.4.4

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

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.

Proposition 7.1.4

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 $b_1 b_2$ are both integral over A.

7.2 Integral Extensions

Definition 7.2.1: 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 all elements of B are integral over A.

Lemma 7.2.2

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

Proposition 7.2.3

Let A, B be commutative rings such that $A \subset B$ is an integral extension. Let J be an ideal of B. Then $\frac{B}{J}$ is integral over $\frac{A}{J \cap A}$.

Proposition 7.2.4

Let A, B be commutative rings such that $A \subset B$ is an integral extension. Let S be a multiplicative subset of B. Then $S^{-1}B$ is integral over $S^{-1}A$.

Lemma 7.2.5

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.

Definition 7.2.6: 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. If $\overline{A} = A$, then we say that A is integrally closed in B.

Lemma 7.2.7

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

7.3 The Going-Up and Going-Down Theorems

We want to compare prime ideals between integral extensions.

Proposition 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.

Proposition 7.3.2

Let A, B be rings such that $A \subset B$ is an integral extension. Let P be a prime ideal of A. Then the following are true.

- There exists a prime ideal Q of B such that $P = Q \cap A$
- 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 $Q_1 = Q_2$.

Theorem 7.3.3: The Going-Up Theorem

Let A, B be rings such that $A \subset B$ is an integral extension. Let $0 \leq m < n$. Consider the following situation

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

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

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

7.4 Normal Domains

Definition 7.4.1: Normal Domains

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

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

7.5 Dedekind Domains

Definition 7.5.1: 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

8 Algebra Over a Commutative Ring

8.1 Commutative Algebras

Definition 8.1.1: Commutative Algebras

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

Proposition 8.1.2

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 $f : R \to A$

Proof. Suppose that A is an R-algebra. Then define a map $f : R \to A$ 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 $f : R \to A$. Define an action $\cdot : R \times A \to A$ 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.

$$\left\{ (A, R) \;\middle|\; \begin{array}{c} A \text{ is a commutative} \\ R\text{-algebra} \end{array} \right\} \overset{1:1}{\longleftrightarrow} \left\{ \phi : R \to A \;\middle|\; \begin{array}{c} \phi \text{ is a ring homomorphism} \\ \text{such that } f(R) \subseteq Z(A) = A \end{array} \right\}$$

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

Proposition 8.1.3

Let B be an A-algebra. Let S be a multiplicative set of B. Let M be an $S^{-1}(B)$-module. Then for any A-derivation $d : B \to M$, there exists one unique way of extending the derivation to $d : S^{-1}B \to M$, defined by the formula:

$$d\left(\frac{b}{s}\right) = \frac{sd(b) - bd(s)}{s^2}$$

Proof. Temporarily denote a derivation from $S^{-1}B$ to M by D. Suppose that $b \in B$ and $s \in S$. Notice that D has to satisfy the following:

$$d(b) = D(b) = D\left(s\frac{b}{s}\right) = \frac{b}{s}D(s) + sD\left(\frac{b}{s}\right)$$

Now multiply both sides by s^{-1} to obtain

$$D\left(\frac{b}{s}\right) = \frac{sD(b) - bD(s)}{s^2}$$

Thus any A-derivation $S^{-1}B$ to M must satisfy the above formula. This shows that there can only be one unique way of extending it.

For existence, we just have to show that it is a well defined map. Suppose that $\frac{a}{r} = \frac{b}{s}$. This means that there exists $q \in S$ such that $q(sa - rb) = 0$. The goal is to show that

$$\frac{rd(a) - ad(r)}{r^2} = \frac{sd(b) - bd(s)}{s^2}$$

or in other words, there exists $p \in S$ such that $p\left(s^2(rd(a) - ad(r)) - r^2sd(b) - bd(s)\right) = 0$. I claim that $p = q^2$ does the job. Indeed we have that

$$\begin{aligned} q^2\left(s^2(rd(a) - ad(r)) - r^2sd(b) - bd(s)\right) &= q^2(sad(rs) - rsd(as) - rbd(rs) + rsd(br)) \\ &= q^2((sa - rb)d(rs) + rs(d(br - as))) \\ &= rsq^2d(br - as) \end{aligned}$$

Now in fact, $q^2d(br - as) = 0$ because

$$\begin{aligned} q^2d(br - as) &= q(qd(br - as)) \\ &= q(d(q(br - as)) - (br - as)d(q)) \\ &= 0 \end{aligned}$$

Thus we conclude. □

8.2 Finitely Generated Algebra

Definition 8.2.1: Finitely Generated Algebras

Let R be a commutative ring. Let A be an R-algebra. We say that A is finitely generated if there exists $a_1, \ldots, a_n \in A$ such that every element $a \in A$ can be written as a polynomial in $a_1, \ldots, a_n$. This means that

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

Finitely generated algebras are also called algebra of finite type.

Theorem 8.2.2

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 $a_1, \ldots, a_n \in A$ such that the evaluation homomorphism

  $$\phi : R[x_1, \ldots, x_n] \to A$$

  given by $\phi(f) = f(a_1, \ldots, a_n)$ is a surjection
- There is an isomorphism

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

  for some ideal I

Definition 8.2.3: Finitely Presented Algebra

Let R be a ring. Let $A = R[x_1, \ldots, x_n]/I$ be a finitely generated algebra over R for some ideal I. We say that A is finitely presented if I is finitely generated.

Lemma 8.2.4

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. □

8.3 Finite Algebras

Definition 8.3.1: 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 8.3.2

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

8.4 Zariski's Lemma

Lemma 8.4.1

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

Theorem 8.4.2: Zariski's Lemma

Let F be a field. Let K be a field that is also a finitely generated algebra over F. Then K is a finite algebra. In particular, K is a finitely generated vector space over F.

Corollary 8.4.3

Let F be an algebraically closed field. Let K be a field that is also a finitely generated algebra over F. Then the inclusion homomorphism $F \hookrightarrow K$ is an F-algebra isomorphism.

Corollary 8.4.4

Let F be an algebraically closed field. Then every maximal ideal of $F[x_1, \ldots, x_n]$ is of the form $(x_1 - a_1, \ldots, x_n - a_n)$ for some $a_1, \ldots, a_n \in F$.

9 Introduction to Dimension Theory for Rings

9.1 Krull Dimension

Definition 9.1.1: Krull Dimension

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

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

9.2 Structure Theorem for Artinian Rings

Lemma 9.2.1

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 $\dim(R) = 0$

Proposition 9.2.2

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

Theorem 9.2.3: Structure Theorem for Commutative Artinian Rings

Let R be an Artinian commutative ring. Then there exists Artinian local rings $A_1, \ldots, A_k$ such that

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

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

9.3 Height of Prime Ideals

Definition 9.3.1: Height of a Prime Ideal

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

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

Lemma 9.3.2

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

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

Theorem 9.3.3: 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

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

9.4 Length of a Module

Definition 9.4.1: 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 9.4.2

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

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

Lemma 9.4.3

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 9.4.4

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

9.5 The Hilbert Polynomial

Definition 9.5.1: 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 $H_M : \mathbb{N} \to \mathbb{N}$ of R to be the function defined by

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

Definition 9.5.2: 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 9.5.3

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 $\lambda : \{M_i \mid i \in I\} \to \mathbb{Z}$ 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 9.5.4: 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 9.5.5: 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 9.5.6

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 Valuation and Valuation Rings

10.1 Valuation Rings

Definition 10.1.1: 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 10.1.2

Let R be a valuation ring. Then the following are true.
- R is a local ring
- R is integrally closed

10.2 Valuations on a Field

Definition 10.2.1: 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 10.2.2: 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 group homomorphism $v : K^\times \to G$ 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 $v(0) = \infty$.

Definition 10.2.3: Associated Valuation Ring

Let K be a field and $v : K \to \mathbb{Z}$ 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 10.2.4

Let K be a field. Let v be a discrete valuation on K. Then R_v is a valuation ring.

10.3 Discrete Valuations and Normalizations

Definition 10.3.1: Discrete Valuations

Let K be a field. A discrete valuation on K is a valuation $v : K^\times \to \mathbb{Z}$.

Definition 10.3.2: Normalized Discrete Valuations

Let (K, v) be a discrete valuation ring. We say that it is normalized if v is surjective.

Lemma 10.3.3

Let K be a field with a discrete valuation v. Then $v(K^\times) = n\mathbb{Z}$ for some $n \in \mathbb{N}$.

Lemma 10.3.4: 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 $v_N : K^\times \to \mathbb{Z}$ defined by

$$v_N(k) = \frac{1}{n} v(k)$$

for all $k \in K^\times$.

Therefore we always work on normalized discrete valuation rings.

10.4 Discrete Valuation Rings

Definition 10.4.1: 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.

Proposition 10.4.2

Let R be a discrete valuation ring with 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 $v(u) = 0$
- $\dim(R) = 1$

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.

□

Definition 10.4.3: 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 10.4.4

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 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 $t \in R$ 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 10.4.5

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 $m = \{x \in K | v(x) > 0\}$. 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):

□

Proposition 10.4.6

Let R be a Noetherian local integral domain such that $\dim(R) = 1$. Let m be its unique maximal ideal. Then the following are equivalent.
- R is a discrete valuation ring.
- R is integrally closed
- m is a principal ideal
- $\dim_{R/m}(m/m^2) = 1$
- For ideal $I \neq 0$ of R, $I = m^k$ for some $k \in \mathbb{N}$
- There exists $t \in R$ such that every ideal $I \neq 0$ of R is of the form $I = (t^n)$ for some $n \in \mathbb{N}$.

11 Four Important Rings

In this section we will investigate four particular types of Noetherian local rings. Therefore it is important to revise on what we know about Noetherian local rings as of now.

- Noetherian means that the supremum of the set of all ascending chains of terminate at a largest ideal.
- Locality means that the ring has a unique maximal ideal.

Noetherian local rings enjoy the fundamental theorem of dimension theory, which says that the different definitions of dimensions coincide. The definitions of the four types of rings depends heavily on the notion of dimension.

11.1 Regular Local Rings

Regularity is an important concept in algebraic geometry to detecting singularities. We motivate the definition by the following proposition.

Definition 11.1.1: Regular Local Rings

A Noetherian local ring (R, m) is said to be regular if

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

for $k = R/m$ the residue field of R.

Theorem 11.1.2

Let (R, m) be a Noetherian local ring. Let n be the minimal number of elements needed to generate m. Then R is regular if and only if $n = \dim(R)$.

Theorem 11.1.3

Let A be a Noetherian local ring of dimension 1 with maximal ideal m. Then the following are equivalent:

- A is regular
- m is principal
- A is an integral domain, and all ideals are of the form m^n for $n \geq 0$ or (0)
- A is a principal ideal domain

11.2 Complete Intersection Rings

Definition 11.2.1: Complete Intersection Rings

Let (R, m) be a Noetherian local ring. We say that R is a complete intersection ring if there exists a regular local ring (A, q) and an ideal I generated by a regular sequence such that

$$\hat{R} \cong \frac{A}{I}$$

11.3 Gorenstein Rings

Definition 11.3.1: Gorenstein Rings

Definition 11.3.2: Injective Dimension

11.4 Cohen-Macauley Rings

$$\begin{matrix}\text{Regular}\\ \text{Local Rings}\end{matrix} \subset \begin{matrix}\text{Complete}\\ \text{Intersection Rings}\end{matrix} \subset \begin{matrix}\text{Gorenstein}\\ \text{Rings}\end{matrix} \subset \begin{matrix}\text{Cohen-Macauley}\\ \text{Rings}\end{matrix}$$

12 Kähler Differentials

The goal of this section is to define the derivations and the module of Kähler differentials, as well as seeing some first consequences such as the two exact sequences. To show existence of the module of Kähler differentials, we will see two different constructions of the module.

12.1 Kähler Differentials

We now define the module of Kähler Differentials which is the main object of study. For each A-derivation d from an A-algebra B to a B-module M, d factors through a universal object no matter what d we choose. This is the content of the following definition.

Definition 12.1.1: Kähler Differentials

A B-module $\Omega^1_{B/A}$ together with an A-derivation $d : B \to \Omega^1_{B/A}$ is said to be a module Kähler Differentials of B over A if it satisfies the following universal property:

For any B-module M, and for any A-derivation $d' : B \to M$, there exists a unique B-module homomorphism $f : \Omega^1_{B/A} \to M$ such that $d' = f \circ d$. In other words, the following diagram commutes:

$$\begin{array}{ccc} B & \xrightarrow{d} & \Omega^1_{B/A} \\ & \searrow^{d'} & \downarrow{\scriptstyle \exists! f} \\ & & M \end{array}$$

The above definition merely shows what properties we would like a module of Kähler differentials to satisfy. Notice that we have yet to show its existence. The above construction is also universal in the following sense.

Lemma 12.1.2

Let A be a ring and B an A-algebra. Let M be a B-module. Then there is a canonical B-module isomorphism

$$\mathrm{Hom}_B(\Omega^1_{B/A}, M) \cong \mathrm{Der}_A(B, M)$$

Proof. Fix M a B-module. Let $d' \in \mathrm{Der}_A(B, M)$. By the universal property of $\Omega^1_{B/A}(M)$, there exists a unique B-module homomorphism $f : \Omega^1_{B/A} \to M$ such that $d' = f \circ d$. This gives a map $\phi : \mathrm{Der}_A(B, M) \to \mathrm{Hom}_B(\Omega^1_{B/A}, M)$ defined by $\phi(d') = f$.

Conversely, given a map $g \in \mathrm{Hom}_B(\Omega^1_{B/A}, M)$, pre-composition with d gives a pull back map $d^* : \mathrm{Hom}_B(\Omega^1_{B/A}, M) \to \mathrm{Der}_A(B, M)$ defined by $d^*(g) = g \circ d$. These map are inverses of each other:

$$\begin{aligned} (d^* \circ \phi)(d') &= d^*(f) \\ &= f \circ d \\ &= d' && \text{(By universal property)} \end{aligned}$$

and $(\phi \circ d^*)(g) = \phi(g \circ d) = g$. Thus these map is a bijective map of sets.

It remains to show that d^* is a B-module homomorphism. Let $f, g \in \mathrm{Hom}_B(\Omega^1_{B/A}, M)$.

- $d^*(f + g) = (f + g) \circ d$ is a map

$$b \overset{d}{\mapsto} d(b) \overset{f+g}{\mapsto} f(d(b)) + g(d(b))$$

for $b \in B$. $d^*(f) + d^*(g) = f \circ d + g \circ d$ is a map

$$b \mapsto f(d(b)) + g(d(b))$$

thus addition is preserved by d^*.

- Let $u \in B$. We want to show that $d^*(u \cdot f) = u \cdot d^*(f)$. The left hand side sends an element $b \in B$ by

$$b \overset{d}{\mapsto} d(b) \overset{u \cdot f}{\mapsto} u \cdot f(d(b))$$

The right hand side sends $b \mapsto u \cdot f(d(b))$. Thus proving they are the same.

And so we have reached the conclusion. □

The definition of the module and the above lemma shows the following: The functor $M \mapsto \text{Der}_A(B, M)$ between the category of B-modules is representable. Indeed, one may recall that a functor is said to be representable if it is naturally isomorphic to the Hom functor together with a fixed object, which is precisely the content of the above lemma.

Let us now see an explicit construction of the module to prove the existence of the module of Kähler Differentials.

Proposition 12.1.3

Let A be a ring and B be an A-algebra. Let F be the free B-module generated by the symbols $\{d(b) \mid b \in B\}$. Let R be the submodule of F generated by the following relations:

- $d(a_1b_1 + a_2b_2) - a_1d(b_1) - a_2d(b_2)$ for all $b_1, b_2 \in B$ and $a_1, a_2 \in A$
- $d(b_1b_2) - b_1d(b_2) - b_2d(b_1)$ for all $b_1, b_2 \in B$

Then F/R is a module of Kähler Differentials for B over A.

Proof. Clearly F/R is a B-module. Moreover, define $d : B \to F/R$ by $b \mapsto d(b) + R$. This map is an A-derivation since the following are satisfied:

- d is an A-module homomorphism: Let $b_1, b_2 \in B$ and $a_1, a_2 \in A$. Then $a_1b_1 + a_2b_2$ is mapped to $d(a_1b_1 + a_2b_2) + R$. We know from the relations that $d(a_1b_1 + a_2b_2) + R = a_1d(b_1) + a_2d(b_2) + R$. Thus d is A-linear.
- d satisfies the Leibniz rule: Let $b_1, b_2 \in B$. Then b_1b_2 is mapped to $d(b_1b_2) + R$. Since $d(b_1b_2) + R = b_1d(b_2) + d(b_1)b_2$, we have that b_1b_2 is mapped to $b_1d(b_2) + d(b_1)b_2 + R$.

This shows that $d : B \to F/R$ is an A derivation.

It remains to show that $(F/R, d)$ has the universal property. Let M be a B-module and $d' : B \to M$ an A-derivation. Define a map $f : F \to M$ on generators by $d(b) \mapsto d'(b)$ and extending from generators to the entire module. This is a B-module homomorphism by definition. Clearly $f \circ d = d'$. It also unique since f is defined on the generators of F.

Finally we want to show that f projects to a map $\bar{f} : F/R \to M$. This requires us to check that $f(d(a_1b_1 + a_2b_2)) = f(a_1d(b_1) + a_2d(b_2))$ and $f(d(b_1b_2)) = f(b_1d(b_2) + d(b_1)b_2)$. But this is clear. Since $f : F \to R$ is a B-module homomorphism, we have

$$f(d(a_1b_1 + a_2b_2)) - f(a_1d(b_1) + a_2d(b_2)) = 0$$

and

$$f(d(b_1b_2)) - f(b_1d(b_2) + d(b_1)b_2) = 0$$

implying f sends $d(a_1b_1 + a_2b_2) - a_1d(b_1) - a_2d(b_2)$ and $d(b_1b_2) - b_1d(b_2) - d(b_1)b_2$ to 0. Since we checked them on generators of R this result extends to all of R. Thus we are done. □

Aside from the construction through quotients, we can also express the module explicitly via the kernel of a diagonal morphism. Using the universal property, we see that all these constructions are the same.

Proposition 12.1.4

Let A be a ring and B be an A-algebra. Let $f : B \otimes_A B \to B$ be a function defined to be $f(b_1 \otimes_A b_2) = b_1 b_2$. Let I be the kernel of f. Then $(I/I^2, d)$ is a module of Kähler Differentials of B over A, where the derivation is the homomorphism $d : B \to I/I^2$ defined by $db = 1 \otimes b - b \otimes 1 \pmod{I^2}$.

Proof. We break down the proof in 3 main steps.

Step 1: Show that $\ker(f) = \langle 1 \otimes b - b \otimes 1 \mid b \in B \rangle$.
Write $I = \langle 1 \otimes b - b \otimes 1 \mid b \in B \rangle$. For any generator $1 \otimes b - b \otimes 1$ of I, we see that

$$f(1 \otimes b - b \otimes 1) = 0$$

Thus $I \subseteq \ker(f)$. Now suppose that $\sum_{i,j} b_i \otimes b_j \in \ker(f)$. Then using the identity

$$b_i \otimes b_j = b_i b_j \otimes 1 + (b_i \otimes 1)(1 \otimes b_j - b_j \otimes 1)$$

and the fact that $b_i b_j = 0$ (because $0 = f(b_i \otimes b_j) = b_i b_j$) we see that

$$\sum_{i,j} b_i \otimes b_j = \sum_{i,j} (b_i \otimes 1)(1 \otimes b_j - b_j \otimes 1)$$

Since each $1 \otimes b_j - b_j \otimes 1$ lies in $\ker(f)$, we conclude that $\sum_{i,j} b_i \otimes b_j$ so that $I = \ker(f)$.

Step 2: Check that $d : B \to I/I^2$ is an A-derivation.

- $d : B \to I/I^2$ is an A-module homomorphism: Let $a_1 a_2 \in A$ and $b_1, b_2 \in B$. Then we have

$$\begin{aligned} d(a_1 b_1 + a_2 b_2) &= 1 \otimes (a_1 b_2 + a_2 b_2) - (a_1 b_2 + a_2 b_2) \otimes 1 + I^2 \\ &= a_1(1 \otimes b_1) + a_2(1 \otimes b_2) - a_1(b_1 \otimes 1) - a_2(b_2 \otimes 1) + I^2 \\ &= a_1 d(b_1 b_2) + a_2 d(b_1 b_2) + I^2 \end{aligned}$$

  Thus we are done. (Notice that we did not use the fact that all the expressions are taken modulo I^2)
- d satisfies the Leibniz rule: Let $b_1, b_2 \in B$. Then we have
  $d(b_1 b_2) = 1 \otimes b_1 b_2 - b_1 b_2 \otimes 1 + I^2$ on one hand. On the other hand we have

$$b_1 d(b_2) + b_2 d(b_1) = b_1(1 \otimes b_2 - b_2 \otimes 1) + b_2(1 \otimes b_1 - b_1 \otimes 1) + I^2$$

  Subtracting them gives

$$\begin{aligned} d(b_1 b_2) - b_1 d(b_2) - b_2 d(b_1) &= 1 \otimes b_1 b_2 - b_1 \otimes b_2 - b_2 \otimes b_1 + b_2 b_1 \otimes 1 \\ &= (1 \otimes b_1 - b_1 \otimes 1)(1 \otimes b_2 - b_2 \otimes 1) + I^2 \end{aligned}$$

  But $(1 \otimes b_1 - b_1 \otimes 1)(1 \otimes b_2 - b_2 \otimes 1)$ lies in I^2 thus subtraction gives 0.

Thus d is an A-derivation.

Step 3: Show that the universal property is satisfied.
Let M be a B-module and $d' : B \to M$ an A-derivation. We want to find a unique $\tilde{\phi} : B \to M$ such that $d' = \tilde{\phi} \circ d$.

Step 3.1: Construct a homomorphism of A-algebra from $B \otimes B$ to $B \ltimes M$
Define $\phi : B \otimes B \to B \ltimes M$ (Refer to **??** for definition of $B \ltimes M$) by

$$\phi(b_1 \otimes b_2) = (b_1 b_2, b_1 d'(b_2))$$

and extend it linearly so that $\phi(b_1 \otimes b_2 + b_3 \otimes b_4) = \phi(b_1 \otimes b_2) + \phi(b_3 \otimes b_4)$. This is a homomorphism of A-algebra since

- Addition is preserved: This is by definition.
- $\phi(ab_1 \otimes b_2) = \phi(b_1 \otimes ab_2) = a\phi(b_1 \otimes b_2)$: Let $a \in A$ and $b_1 \otimes b_2 \in B \otimes_A B$. Then

$$\begin{aligned}\phi(ab_1 \otimes b_2) &= (ab_1b_2, ab_1d'(b_2)) \\ &= a \cdot \phi(b_1 \otimes b_2) \\ \phi(b_1 \otimes ab_2) &= (ab_1b_2, b_1d'(ab_2)) \\ &= (ab_1b_2, ab_1d'(b_2))\end{aligned}$$

  Thus we are done.
- Product is preserved: For $u_1, u_2, v_1, v_2 \in B$, we have

$$\begin{aligned}\phi((u_1 \otimes u_2) \cdot \phi(v_1 \otimes v_2)) &= (u_1u_2, u_1d'(u_2)) \cdot (v_1v_2, v_1d'(v_2)) \\ &= (u_1u_2v_1v_2, u_1u_2v_1d'(v_2) + v_1v_2u_1d'(u_2)) \\ &= (u_1v_1u_2v_2, u_1v_1d'(u_2v_2) \\ &= \phi(u_1v_1 \otimes u_2v_2)\end{aligned}$$

Thus ϕ is a homomorphism of A-algebra.

Step 3.2: Construct $\tilde{\phi}$ from ϕ.
Since ϕ is a map $B \otimes B$ to $B \ltimes M$, we can restrict this map to I a result in a new map $\bar{\phi} : I \to B \ltimes M$. Notice that for $1 \otimes b - b \otimes 1$ a generator of I, we have

$$\begin{aligned}\bar{\phi}(1 \otimes b - b \otimes 1) &= \bar{\phi}(1 \otimes b) - \bar{\phi}(b \otimes 1) \\ &= (b, d'(b)) - (b, d'(1)) \\ &= (b, d'(b)) - (b, 0) \\ &= (0, d'(b))\end{aligned}$$

Thus we actually have a map $\bar{\phi} : I \to M$. Finally, notice that for $(1 \otimes u - u \otimes 1)(1 \otimes v - v \otimes 1)$ a generator of I^2, we have

$$\begin{aligned}\bar{\phi}(x) &= \phi(1 \otimes u - u \otimes 1)\phi(1 \otimes v - v \otimes 1) \\ &= \sum (0, d'(u))(0, d'(v)) \\ &= \sum (0, 0) && \text{(Mult. in Trivial Extension)} \\ &= (0, 0)\end{aligned}$$

which shows $\bar{\phi}$ kills of I^2 and thus $\bar{\phi}$ factors through I/I^2 so that we get a map $\tilde{\phi} : I/I^2 \to M$.

Step 3.3: Show that $\tilde{\phi}$ satisfies all the required properties.
For $b \in B$, we have that

$$\tilde{\phi}(d(b)) = \tilde{\phi}(1 \otimes b - b \otimes 1 + I^2) = d'(b)$$

and thus $d' = \tilde{\phi} \circ d$. Moreover, this map is unique since it is defined on the generators of I, namely the $d(b)$ for $b \in B$.

This concludes the proof.
Materials referenced: [**?**], [**?**], [**?**] □

This version of the module of Kähler Differentials generalizes well to the theory of schemes. Interested readers are referred to [**?**].

Our first step towards computing the module of Kähler Differentials for coordinate rings comes from a computation of the polynomial ring.

Lemma 12.1.5

Let A be a ring and $B = A[x_1, \ldots, x_n]$ so that B is an A-algebra. Then

$$\Omega^1_{B/A} = \bigoplus_{i=1}^{n} Bd(x_i)$$

is a finitely generated B-module.

Proof. I claim that $\Omega^1_{B/A}$ has basis $d(x_1), \ldots, d(x_n)$. We proceed by induction.

When $n = 1$, a general polynomial in $A[x]$ is of the form

$$f(x) = \sum_{i=0}^{n} c_i x^i$$

for $c_i \in A$. Applying d subject to the conditions of quotienting gives

$$d(f) = \sum_{i=0}^{n} c_i d(x^i)$$

But $d(x^i) = xd(x^{i-1}) + x^{i-1}d(x)$. Repeating this allows us to reduce $d(x^i) = g_i(x)d(x)$. Doing this for each x^i in the sum in fact gives us $f(x) = \frac{df}{dx}d(x)$. Thus we see that $\Omega^1_{A[x]/A}$ is a $A[x]$ module with basis $d(x)$.

Now suppose that $\Omega^1_{A[x_1,\ldots,x_{n-1}]/A} = \bigoplus_{i=1}^{n-1} Bd(x_i)$. Then for every $f \in A[x_1, \ldots, x_n]$, we can write the function as

$$f(x_1, \ldots, x_n) = \sum_{i=0}^{s} g_i(x_1, \ldots, x_{n-1})x_n^i$$

and then we can apply the same process again:

$$d(f) = \sum_{i=0}^{s} (x_n^i d(g_i) + g_i d(x_n^i))$$

except that now $d(g_i)$ by induction hypothesis can be written in terms of the basis $d(x_1), \ldots, d(x_{n-1})$. As a side note: by doing some multiplication, one can easily see that

$$d(f) = \sum_{i=0}^{s} \frac{\partial f}{\partial x_i} d(x_i)$$

By **??**, since $\Omega^1_{B/A}$ is a B-module, there exists a free B module $\bigoplus_{i=1}^{m} B$ such that the map $\psi : \bigoplus_{i=1}^{m} B$ is surjective. In fact, by choosing $m = n$ and mapping each basis e_i of $\bigoplus_{i=1}^{n} B$ to $d(x_i)$, we obtain a surjective map.

Now consider the map $\partial : B \to \bigoplus_{i=1}^{n} B$ (No calculus involved, just notation!) defined by

$$f \mapsto \left(\frac{\partial f}{\partial x_1}, \ldots, \frac{\partial f}{\partial x_n} \right)$$

It is clear that this map is an A-derivation. By the universal property of $\Omega^1_{B/A}$, the derivation factors through $d : A \to \Omega^1_{B/A}$. This leaves us with a B-module homomorphism $\phi : \Omega^1_{B/A} \to \bigoplus_{i=1}^{n} B$ defined by

$$d(f) \mapsto \left(\frac{\partial f}{\partial x_1}, \ldots, \frac{\partial f}{\partial x_n} \right)$$

This map is surjective. Notice that for each monomial x_i in B, we have $\partial(x_i) = e_i$. Since $\partial = \phi \circ d$, $d(x_i) \in \Omega^1_{A/k}$ maps to e_i and thus ϕ is surjective.

It is clear that ϕ and ψ are inverses of each other since the basis elements that they map to and from are the same. □

12.2 Transfering the System of Differentials

This section aims to develop the necessary machinery in order to compute the module of Kähler Differentials for coordinate rings. We will see explicit calculation of the cuspidal cubic, an ellipse and the double cone to demonstrate how the two exact sequences can be used along with the Jacobian of the defining equations of the variety to compute the module of Kähler Differentials.

Theorem 12.2.1: First Exact Sequence

Let B, C be A-algebras and let $\phi : B \to C$ be an A-algebra homomorphism. Then the following sequence is an exact sequence of C-modules:

$$\Omega^1_{B/A} \otimes_B C \xrightarrow{f} \Omega^1_{C/A} \xrightarrow{g} \Omega^1_{C/B} \longrightarrow 0$$

where f and g is defined respectively as

$$f(d_{B/A}(b) \otimes c) = c \cdot d_{C/A}(\phi(b))$$

and

$$g(d_{C/A}(c)) = d_{C/B}(c)$$

and extended linearly.

Proof. Denote $d_{B/A}, d_{C/A}, d_{C/B}$ the derivations for $\Omega^1_{B/A}, \Omega^1_{C/A}, \Omega^1_{C/B}$ respectively. Clearly g is surjective since for any $c_1 d_{C/B}(c_2) \in \Omega^1_{C/B}$, just choose $c_1 d_{C/A}(c_2) \in \Omega^1_{C/A}$. We just have to show that $\ker(g) = \operatorname{im}(f)$. It is enough to show that

$$0 \longrightarrow \operatorname{Hom}_C(\Omega^1_{C/B}, N) \longrightarrow \operatorname{Hom}_C(\Omega^1_{C/A}, N) \longrightarrow \operatorname{Hom}_C(\Omega^1_{B/A} \otimes_B C, N)$$

is exact by **??**. Using the fact that $\operatorname{Hom}_C(\Omega^1_{B/A} \otimes_B C, N) = \operatorname{Hom}_B(\Omega^1_{B/A}, N)$ (**??**) and the fact that $\operatorname{Hom}(\Omega^1_{B/A}, N) \cong \operatorname{Der}_A(B, N)$, we can transform the sequence into

$$0 \longrightarrow \operatorname{Der}_B(C, N) \xrightarrow{u} \operatorname{Der}_A(C, N) \xrightarrow{v} \operatorname{Der}_A(B, N)$$

Notice that u is just the inclusion map and v is just the restriction map. In particular, an A-derivation is a B-derivation if and only if its restriction to B is trivial. Hence we conclude that $\operatorname{im}(u) = \ker(v)$. Materials Referenced: [**?**], [**?**] □

Theorem 12.2.2: Second Exact Sequence

Let A be a ring and B an A-algebra. Let I be an ideal of B and $C = B/I$. Then the following sequence is an exact sequence of C-modules:

$$I/I^2 \longrightarrow \Omega^1_{B/A} \otimes_B C \xrightarrow{\delta} \Omega^1_{C/A} \xrightarrow{f} 0$$

where δ and f is defined respectively as

$$\delta(i + I^2) = d(i) \otimes 1$$

and

$$f(d(b)\otimes c) = c\cdot d(\phi(b))$$

and then extended linearly.

Proof. Notice that δ is well defined. Indeed, if $i+I^2 = j+I^2$, then there exists $h_1, h_2 \in I$ such that $i-j = h_1h_2$. Now we have that

$$\begin{aligned}\delta(i-j) &= d(h_1h_2)\otimes 1\\ &= h_1d(h_2)\otimes 1 + h_2d(h_1)\otimes 1\\ &= d(h_2)\otimes h_1 + I + d(h_1)\otimes h_2 + I\\ &= d(h_2)\otimes 0 + d(h_1)\otimes 0\\ &= 0\end{aligned}$$

We can see that f is surjective. Indeed for any $d(b+I)\in\Omega^1_{C/A}$, just choose $d(b)\otimes 1 \in \Omega^1_{B/A}\otimes_B C$. Then $f(d(b)\otimes 1) = d(b+I)$.

It remains to show that $\mathrm{im}(\delta) = \ker(f)$. Notice that to prove the exactness of the sequence in question, we just have to show the exactness of the following sequence (by **??**):

$$0 \longrightarrow \mathrm{Hom}_C(\Omega^1_{C/A}, N) \longrightarrow \mathrm{Hom}_C(\Omega^1_{B/A}\otimes_B \tfrac{B}{I}) \longrightarrow \mathrm{Hom}_C(I/I^2, N)$$

Using the fact that $I/I^2 \cong I\otimes_B \frac{B}{I}$ (by **??**) and $\mathrm{Hom}_C(\Omega^1_{B/A}\otimes_B B/I, N) = \mathrm{Hom}_B(\Omega^1_{B/A}, N)$ (by **??**) we can transform this sequence into

$$0 \longrightarrow \mathrm{Hom}_C(\Omega^1_{C/A}, N) \longrightarrow \mathrm{Hom}_B(\Omega^1_{B/A}, N) \longrightarrow \mathrm{Hom}_B(I, N)$$

and further using $\mathrm{Der}_A(B,N)\cong \mathrm{Hom}_B(\Omega^1_{B/A}, N)$ (by 12.1.2), transform into

$$0 \longrightarrow \mathrm{Der}_A(B/I, N) \xrightarrow{f_*} \mathrm{Der}_A(B,N) \xrightarrow{\delta_*} \mathrm{Hom}_B(I,N)$$

There is no need to prove the second arrow to be injective. We need to show exactness between the second and third arrow.

Notice that any $\phi\in\mathrm{Der}_A(B/I,N)$ can be extended naturally to an A-linear derivation from B to N: just pre-compose it with the projection map $p: B\to B/I$. This map is A-linear hence $\phi\circ p$ is A-linear. Moreover, p is B-linear and ϕ is a derivation so that it satisfies the Leibniz rule. Also, a natural map from $\mathrm{Der}_A(B,N)$ to $\mathrm{Hom}_B(I,N)$ is given just by restricting $\psi\in\mathrm{Der}_A(B,N)$ to I. The new map under restriction will naturally become a homomorphism from I to N. The kernel of the third arrow is just any derivation in $\mathrm{Der}_A(B,N)$ that is identically 0 on I.

But these derivations are precisely those of $\mathrm{Der}_A(B/I,N)$! □

A very nice application towards computing the module of differential forms is given by the second exact sequence. For $B = A[x_1,\ldots,x_n]$ and $C = \frac{B}{I=(f_1,\ldots,f_r)}$, we can use **??** to see that $\Omega^1_{B/A}\otimes C \cong \bigoplus_{i=1}^n C dx_i$. By the second exact sequence 12.2.2, we see that

$$\Omega^1_{C/A} \cong \mathrm{coker}\left(\frac{I}{I^2}\to \bigoplus_{i=1}^n C dx_i\right)$$

Since I/I^2 is a C-module, by **??** there exists a surjective map $\bigoplus_{i=1}^m C de_i \twoheadrightarrow I/I^2$. In fact $m=r$ since I is finitely generated by $f_1,\ldots,f_r$ and thus the map sends e_i to f_i for $1\le i\le r$.

Now consider the map

$$J : \bigoplus_{i=1}^{r} C de_i \twoheadrightarrow \frac{I}{I^2} \to \bigoplus_{i=1}^{n} C dx_i$$

This is a map from a free module of rank r to a free module of rank n. So we can write this in an $n \times r$ matrix. Since the map $I/I^2 \to \bigoplus_{i=1}^{n} C dx_i$ sends f_i to $d(f_i) = \sum_{k=1}^{n} \frac{\partial f_i}{\partial x_k} dx_k$ (by second exact sequence 12.2.2) and e_i is sent f_i, we have that J is the matrix

$$\begin{pmatrix} \frac{\partial f_1}{\partial x_1} & \cdots & \frac{\partial f_r}{\partial x_1} \\ \vdots & \ddots & \vdots \\ \frac{\partial f_1}{\partial x_n} & \cdots & \frac{\partial f_r}{\partial x_n} \end{pmatrix}$$

Finally, since $\operatorname{im}(A \twoheadrightarrow B \to C) = \operatorname{im}(B \to C)$, we thus have

$$\operatorname{coker}(J) \cong \Omega^1_{C/A}$$

which means that $\Omega^1_{C/A}$ is just the cokernel of the matrix. This exposition can be found in [**?**].

12.3 Characterization for Separability

The module of Kähler differentials give a necessary and sufficient condition for a finite extension to be separable. Before the main proposition, we will need a lemma.

Lemma 12.3.1

Let L/K be a finite field extension and $\Omega^1_{L/K}$ the module of Kähler Differentials. Let $f(b) = c_0 + c_1 b + \cdots + c_n b^n \in L$ for $c_0, \ldots, c_n \in K$ and $b \in L$. Then $d(f(b)) = f'(b)d(b)$ where $f'(b)$ is the derivative of $f(b)$ with respect to b in the sense of calculus.

Proof. Since $f(b)$ is a finite sum, we apply linearity and Leibniz rule of d to get

$$f'(b) = d(c_0) + bd(c_1) + c_1 d(b) + \cdots + b^n d(c_n) + c_n d(b^n)$$

Since each $c_0, \ldots, c_n \in K$, we obtain $f'(b) = c_1 d(b) + \cdots + c_n \cdot n b^{n-1} d(b)$. Thus factoring out $d(b)$ in the sum, we obtain precisely the standard derivative in calculus, and that $d(f(b)) = f'(b)d(b)$ □

Proposition 12.3.2

Let K be a field and L/K a finite field extension. Then L/K is separable if and only if $\Omega^1_{L/K} = 0$.

Proof. Suppose that L/K is separable. Suppose that $b \in L$ has minimal polynomial $f \in K[x]$. f is separable since L/K is separable. By 12.3.1, we have that $d(f(b)) = f'(b)d(b)$. But the fact that f is separable implies that $f'(b) \neq 0$. At the same time we have $f(b) = 0$ since f is the minimal polynomial of b. This implies that $d(f(b)) = 0$ in $\Omega^1_{L/K} = 0$. Since L is a field, and $f'(b) \neq 0$, we must have $d(b) = 0$ for all $b \in L$. This means that $\Omega^1_{L/K} = 0$.

If L/K is inseparable, then there exists an intermediate field E such that L/E is a simple inseparable extension. Since L/K is finite, L/E is finite and thus is algebraic which means that there exists some polynomial $p \in E[t]$ for which $L = \frac{E[t]}{(p(t))}$. In this case, we have already seen that

$$\Omega^1_{L/E} \cong \frac{L dt}{(p'(t)dt)} \cong \frac{L}{(p'(t))}$$

Since $p'(t) = 0$, we have that $\Omega^1_{L/E} \cong L \neq 0$. By the first exact sequence 12.2.1, we have that $\Omega^1_{L/K}$ maps surjectively onto $\Omega^1_{L/E} \neq 0$ which proves that $\Omega^1_{L/K}$ is non-zero.
Materials referenced: [**?**], [**?**] □

This gives a very nice characterization of separability. Readers can find more in [**?**] and [**?**]. To extend this equivalence under the assumption that L/K is algebraic instead of finite, one can show that Ω^1 preserves colimits in the sense in [**?**]. Namely that the functor $F : \text{Algebra}_R \to \text{Mod}_T$ from the category of R-algebra to the category of T-modules where T is a colimit of a diagram in the category of R-algerba preserves colimits. Then observe that an algebraic extension is the colimit of the finite subextensions.

Analogous to the above result, there is a similar proposition for $\text{Der}_K(L)$ for when L/K is algebraic and separable. This is given by [**?**].

Proposition 12.3.3

Let L/K be an algebraic field extension that is separable. Then $\text{Der}_K(L) = 0$.

Proof. Suppose that $D \in \text{Der}_K(L)$. If $a \in L$, let p be the minimal polynomial of a. Then

$$0 = D(p(a)) = p'(a)D(a)$$

by 12.3.1. Since p is separable over K, $p'(a) \neq 0$. Thus $D(a) = 0$ and so we are done.
Materials referenced: [**?**] □

This proposition will be of use at **??**.