Commutative Algebra 2

Labix

February 14, 2025

Abstract

Contents

1 Filtrations

1.1 Filtrations and Stable Filtrations

Definition 1.1.1: Descending Filtrations

Let R be a commutative ring. Let M be an R-module. A descending filtration of M consists of a sequence of R-submodules M_n for $n \in \mathbb{N}$ such that

$$M_0 \supseteq M_1 \supseteq \cdots \supseteq M_n \supseteq \cdots$$

Definition 1.1.2: Stable Filtrations

Let R be a commutative ring. Let I be an ideal of R. Let M be an R-module. Let

$$M_0 \supseteq \cdots \supseteq M_n \supseteq \cdots$$

be a descending filtration. We say that the filtration is stable with respect to I if there exists $k \in \mathbb{N}$ such that

$$IM_n = M_{n+1}$$

for all $n \geq k$.

Definition 1.1.3: Graded Module Associated to a Filtration

Let R be a commutative ring. Let M be an R-module. Let $I_0 \supseteq I_1 \supseteq \cdots \supseteq I_n \supseteq \cdots$ be a filtration of R. Define the graded ring associated to the filtration to be

$$\text{gr}(R) = \bigoplus_{n=0}^{\infty} \frac{I_n M}{I_{n+1} M}$$

with multiplication given by $(x + I_{n+1}M) \cdot (y + I_{m+1}M) = xy + I_{n+m+1}M$

We have seen in Rings and Modules that the graded ring associated to the filtrartion

$$R \supseteq I \supseteq I^2 \supseteq \cdots \supseteq I^n \supseteq \cdots$$

is precisely the graded ring

$$\text{gr}_I(M) = \bigoplus_{n=0}^{\infty} \frac{I^n}{I^{n+1}}$$

associated to the commutative ring R.

1.2 Filtrations by Powers of Ideals

Theorem 1.2.1: Artin-Rees Lemma

Let R be a Noetherian commutative ring. Let I be an ideal of A. Let M be a finitely generated R-module. Let $N \leq M$ be an R-submodule. Then there exists $c \in \mathbb{N}$ such that

$$I^n M \cap N = I^{n-c}(I^c M \cap N)$$

for all $n > c$.

Proof. $\square$

Theorem 1.2.2: Krull's Intersection Theorem

Let (R, m) be a Noetherian local ring. Then

$$\bigcap_{i=0}^{\infty} m^i = \{0\}$$

Proof. Let $N = \bigcap_{i=0}^{\infty} m^i$. Then $N = I^n M = I^n M \cap N$ for some $n \in \mathbb{N}$. By the Artin-Rees lemma, we have

$$N = I^n M \cap N = I^{n-c}(I^c M \cap N) \subseteq IN$$

for some $c \in \mathbb{N}$. Hence $N = IN$. By Nakayama's lemma, we conclude that $N = 0$. □

2 Completions

2.1 General Completion Methods

Definition 2.1.1: Completion of a Module

Let R be a commutative ring and let M be an R-module. Let $M_0 \supset M_1 \supset \cdots \supset M_n \supset \cdots$ be a descending filtration of R-submodules of M. Define the completion of M with respect to the filtration to be the inverse limit

$$\widehat{M} = \varprojlim_i \frac{M}{M_i}$$

2.2 I-Adic Completion

Definition 2.2.1: I-Adic Completion

Let R be a commutative ring. Let M be an R-module. Let I be an ideal of R. Define the I-adic completion of M to be the completion of M with respect to the filtration

$$I^0M \supset I^1M \supset \cdots I^nM \supset \cdots$$

Explicitly, it is given by the inverse limit

$$\widehat{M}_I = \varprojlim_{n\in\mathbb{N}} \frac{M}{I^nM}$$

Let R be a commutative ring. Let M be an R-module and N an R-submodule of M. The most important consequence of the Artin-Rees lemma is that the sub-filtration $I^n(M\cap N)$ coming from M and the natural filtration I^nN induces that same completion.

Proposition 2.2.2

Let R be a Noetherian commutative ring. Let M be a finitely generated R-module. Let N be an R-submodule of M. Consider the following two filtrations on N.

- The induced sub-filtration $I^nM \cap N$ from M.
- The natural filtration I^nN.

The completion of N with respect to the two filtrations are equal.

Proof. Let $k \in \mathbb{N}$ and $x \in I^kN$. Then $x \in I^kM$ and since N is a submodule, we have $x \in N$ so that $x \in I^kM \cap N$ (The converse is not true unless for large enough k. We will prove it using the Artin-Rees lemma).

By the Artin-Rees lemma, there exists $c \in \mathbb{N}$ such that

$$I^nM \cap N = I^n(I^{n-c}M \cap N)$$

for all $n > c$. Let $x \in I^nM \cap N$. The Artin-Rees lemma give $x \in I^n(I^{n-c}M \cap N)$. Then

$$x = \sum_{i=1}^{r} y_it_i$$

where $y_i \in I^n$ and $t_i \in I^{n-c}M \cap N$. In particular, $t_i \in N$ and N is a submodule implies that $x \in I^nN$.

Hence for all $n > c$, we have an equality

$$I^nN = I^nM \cap N$$

By definition of inverse limits (I think by cofinality of (co)limits), we conclude that their completions give the same R-module. $\square$

Let $\mathcal{A}$ be an abelian category (for example **Ab**, **Ring**, ${}_R$**Mod**, **Vect**$_k$). Fix $\mathcal{J}$ a diagram. Recall that as long as all diagrams $\mathcal{J} \to \mathcal{C}$ admits a limits, then the assignment

$$\lim_{\mathcal{J}} : \mathcal{C}^{\mathcal{J}} \to \mathcal{C}$$

is a well defined functor. Moreover, it is left exact. In particular, generally speaking completions would give a left exact. However, when we complete I-adically, the Artin-Rees lemma give right exactness (under some finiteness conditions).

Proposition 2.2.3

Let R be a Noetherian commutative ring. Let M_1, M_2, M_3 be finitely generated R-modules such that the following

$$0 \longrightarrow M_1 \longrightarrow M_2 \longrightarrow M_3 \longrightarrow 0$$

Then for any ideal I of R, completion with respect to I gives an exact sequence

$$0 \longrightarrow \widehat{M_1}_I \longrightarrow \widehat{M_2}_I \longrightarrow \widehat{M_3}_I \longrightarrow 0$$

where the maps are induced by the universal property of inverse limits.

Proposition 2.2.4

Let R be a Noetherian commutative ring. Let M be a finitely generated R-module. Let I be an ideal of R. Then there is an R-module isomorphism

$$\widehat{M}_I \cong M \otimes_R \widehat{R}_I$$

given by the universal property.

Definition 2.2.5: I-Adicly Complete

Let R be a commutative ring. Let M be an R-module. Let I be an ideal of R. We say that M is I-adicly complete if the induced map of inverse limits

$$M \to \widehat{M}_I$$

is an R-module isomorphism.

2.3 Completion of a Ring

Proposition 2.3.1

Let R be a commutative ring. Let I be an ideal of R. If R is Noetherian, then the following are true.
- $\widehat{R}_I$ is Noetherian.
- $\widehat{R}_I$ is a flat R-module.

Proposition 2.3.2

Let R be a commutative ring. Let m be a maximal ideal. Then $\widehat{R}$ is a local ring with unique maximal ideal $\widehat{m}_m \widehat{R}_m$.

Definition 2.3.3: Complete Local Rings

Let (R, m) be a local ring. We say that R is a complete local ring if R is m-adicly complete.

2.4 Hensel's Lemma

Theorem 2.4.1: Hensel's Lemma

Let (R, m) be a complete local ring. Let $\overline{(-)} : R[x] \to (R/m)[x]$ be the projection map. Let $f \in R[x]$ be monic. If $g, h \in (R/m)[x]$ are monic and $\overline{f} = gh$ and $\gcd(g, h) = 1$, then there exists unique polynomials $u, v \in R[x]$ such that $f = uv$ and $\overline{u} = g$ and $\overline{v} = h$.

3 More on Dimension Theory

3.1 The Hilbert Series

Definition 3.1.1: The Hilbert Function

Let R be commutative ring such that $R = \bigoplus_{i=0}^{\infty} R_i$ is graded. Let $M = \bigoplus_{i=0}^{\infty} M_i$ be a graded R-module. Define the Hilbert function of M to be

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

Definition 3.1.2: The Hilbert Series

Let R be commutative ring such that $R = \bigoplus_{i=0}^{\infty} R_i$ is graded. Let $M = \bigoplus_{i=0}^{\infty} M_i$ be a graded R-module. Define the Hilbert-Samuel series of M to be the infinite series $HS_M \in \mathbb{Z}[[t]]$ given by

$$HS_M(t) = \sum_{i=0}^{\infty} HF_M(i)t^i = \sum_{i=0}^{\infty} l_{R_0}(M_i)t^i$$

Proposition 3.1.3

Let $R = \bigoplus_{i=0}^{\infty} R_i$ be a commutative, Noetherian and graded ring. Let $M = \bigoplus_{k=0}^{\infty} M_k$ be a finitely generated graded R-module. Then there exists $f \in \mathbb{Z}[t]$ such that the Hilbert series is given

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

as a rational function for some $d_i \in \mathbb{N}$.

Proof. Since R is Noetherian, R is finitely generated as an R_0-module. Let n be the number of generators. We induct on n.

If $n = 0$, then $R_0 = R$ so that M is a finitely generated R_0-module. This means there exists $k \in \mathbb{N}$ such that $M_k = M_{k+1} = \cdots = 0$. In this case $HS_M(t)$ is a polynomial.

Assume it is true for all numbers less than n. Let $x \in R_i$. Then $x \cdot M_k \subseteq M_{i+k}$ for each k. Consider multiplication as a map $\phi_k : M_k \to M_{i+k}$. Then define $K_k = \ker(\phi_k)$ and $L_{i+k} = \text{coker}(\phi_k)$. Define

$$K = \bigoplus_{i=0}^{\infty} K_i \quad \text{and} \quad L = \bigoplus_{i=0}^{\infty} L_i$$

They are R-submodules of M and quotient of M respectively and hence are finitely generated. The exact sequence

$$0 \longrightarrow K_k \longrightarrow M_k \xrightarrow{\phi_k} M_{i+k} \longrightarrow L_{i+k} \longrightarrow 0$$

Recall that we can split this four term long exact sequence into two short exact sequences given by

$$0 \longrightarrow K_k \longrightarrow M_k \twoheadrightarrow \text{im}(\phi_k) \longrightarrow 0$$

$$0 \longrightarrow \text{im}(\phi_k) \hookrightarrow M_{i+k} \longrightarrow L_{i+k} \longrightarrow 0$$

From Rings and Modules we know that $l_{R_0}(M_k) = l_{R_0}(K_k) + l_{R_0}(\text{im}(\phi_k))$ and

$l_{R_0}(M_{i+k}) = l_{R_0}(\text{im}(\phi_k)) + l_{R_0}(L_{i+k})$. Combining the both gives

$$\begin{aligned} l_{R_0}(K_k) - l_{R_0}(M_k) + l_{R_0}(M_{i+k}) - l_{R_0}(L_{i+k}) &= 0 \\ t^{i+k}l_{R_0}(K_k) - t^{i+k}l_{R_0}(M_k) + t^{i+k}l_{R_0}(M_{i+k}) - t^{i+k}l_{R_0}(L_{i+k}) &= 0 \\ \sum_{k=-\infty}^{\infty} t^{i+k}l_{R_0}(K_k) - \sum_{k=-\infty}^{\infty} t^{i+k}l_{R_0}(M_k) + \sum_{k=-\infty}^{\infty} t^{i+k}l_{R_0}(M_{i+k}) - \sum_{k=-\infty}^{\infty} t^{i+k}l_{R_0}(L_{i+k}) &= 0 \\ \sum_{k=0}^{\infty} t^{i+k}l_{R_0}(K_k) - \sum_{k=0}^{\infty} t^{i+k}l_{R_0}(M_k) + \sum_{k=-i}^{\infty} t^{i+k}l_{R_0}(M_{i+k}) - \sum_{k=-i}^{\infty} t^{i+k}l_{R_0}(L_{i+k}) &= 0 \\ t^iHS_K(t) - t^iHS_M(t) + HS_M(t) - HS_L(t) &= 0 \end{aligned}$$

Rewriting gives the expression

$$(1-t^i)HS_M(t) = HS_L(t) - t^iHS_K(t)$$

Now notice that K is a direct sum of the kernel of multiplication by x. Hence K is annihilated by x. Similarly, L is a direct sum of the cokernel of multiplication by x. Hence

$$x \cdot L_n \in \ker(\phi_n) = 0 \in L_{i+n}$$

□

Corollary 3.1.4

Let $R = \bigoplus_{i=0}^{\infty} R_i$ be a commutative, Noetherian and graded ring. Let $M = \bigoplus_{k=0}^{\infty} M_k$ be a finitely generated graded R-module. Suppose that the Hilbert series of M is given by

$$HS_M(t) = \frac{f(t)}{(1-t)^r}$$

for some $f \in \mathbb{Z}[t]$ and $r \in \mathbb{N}$. Then there exists a polynomial $\varphi \in \mathbb{Q}[t]$ such that the following are true.

- The smallest number $d \in \mathbb{N}$ such that
$$\lim_{t\to 1}(1-t)^dHS_M(t) < \infty$$
is $\deg(\varphi)$.
- $\varphi(n) = l_{R_0}(M_n)$ for all $n \geq \deg(f) + 1 - \deg(\varphi)$. (In other words, the length function can be given as a rational polynomial)

Proof. I claim that

$$\frac{1}{(1-t)^r} = \sum_{k=0}^{\infty} \binom{r+k-1}{r-1} t^k$$

We proceed by induction. When $r = 1$ this is just the geometric series. Suppose that it is true $< r$. Then we have

$$\begin{aligned}\frac{1}{(1-t)^r} &= \frac{d}{dt}\int \frac{1}{(1-t)^r}\,dt \\ &= \frac{1}{r-1}\frac{d}{dt}\left(\frac{1}{(1-t)^{r-1}}\right) \\ &= \frac{1}{r-1}\frac{d}{dt}\left(\sum_{k=0}^{\infty}\binom{r+k-2}{r-2}t^k\right) \\ &= \frac{1}{r-1}\sum_{k=1}^{\infty}\frac{(r+k-2)!}{(r-2)!k!}kt^{k-1} \\ &= \sum_{k=1}^{\infty}\frac{(r+k-2)!}{(r-1)!(k-1)!}t^{k-1} \\ &= \sum_{k=1}^{\infty}\binom{r+k-2}{r-1}t^{k-1} \\ &= \sum_{k=0}^{\infty}\binom{r+k-1}{r-1}t^k\end{aligned}$$

which completes the induction step. After cancelling factors of $(1-t)$ in $f(t)$ with the denominator, we may suppose that $f(t)$ is now given coprime with $1-t$ and the denominator has power $= d$.

Suppose $f(t)$ is given by $\sum_{i=0}^{N} a_i t^i$. Then we have

$$HS_M(t) = \frac{f(t)}{(1-t)^d} = \sum_{i=0}^{N} a_i t^i \sum_{k=0}^{\infty}\binom{d+k-1}{d-1}t^k$$

The coefficient of t^n in this product is given by $\sum_{j=0}^{N} a_j\binom{d+n-j-1}{d-1}$. Set $\varphi(n)$ to be this sum. But the coefficient of $HS_M(t)$ is also $l_{R_0}(M_n)$ by definition. Hence we deduce that

$$l_{R_0}(n) = \varphi(n) = \sum_{j=0}^{N} a_j\binom{d+n-j-1}{d-1}$$

which is non-zero when $n \geq N+1-d = \deg(f)+1-d$. In particular, expanding the binomial gives a polynomial in n whose largest power of n is d. Hence $d = \deg(\varphi)$ and we are done. □

3.2 The Hilbert-Samuel Function

In the following we use the convention $I^0 = R$ for I an ideal of the commutative ring R.

Definition 3.2.1: Hilbert-Samuel Function

Let R be a commutative ring. Let I be an ideal of R. Let M be a finitely generated R-module. Define the Hilbert-Samuel function of M with respect to I to be

$$\chi_M^I(n) = l_R\left(\frac{M}{I^n M}\right)$$

Proposition 3.2.2

Let R be a commutative ring. Let I be an ideal of R. Let M be a finitely generated R-module. Then we have

$$\chi_M^I(n) = \sum_{i=0}^n HF_{\text{gr}_I(M)}(i) = \sum_{i=0}^n l_R\left(\frac{I^iM}{I^{i+1}M}\right)$$

3.3 Minimal Number of Generators of m-Primary Ideals

Let R be a commutative ring. Let P be a prime ideal of P. Recall that an ideal I is said to be P-primary if the following are true.

- I is primary. This means that $ab \in I$ implies $a \in I$ or $b^n \in I$ for some $n \in \mathbb{N}$.
- $P = \sqrt{I}$

Definition 3.3.1: Minimal Number of Generators of an m-Primary Ideal

Let R be a commutative ring. Let m be a maximal ideal of R. Let I be an m-primary ideal of R. Define

$$\delta_I(R) = \min\{n \in \mathbb{N} \mid x_1, \dots, x_n \in R \text{ generates } I\}$$

Proposition 3.3.2

Let (R, m) be a local ring. Let I be an m-primary ideal of R. Then

$$\delta_I(R) = \delta_m(R)$$

In particular, δ_I is invariant of the choice of the m-primary ideal.

Proposition 3.3.3

Let (R, m) be a Noetherian local ring. Then

$$\delta_m(R) = \dim_{R/m}(m/m^2) < \infty$$

Proof. We have seen this as a consequence of Nakayama's lemma in Commutative Algebra 1. ☐

3.4 The Fundamental Theorem of Dimension Theory

Theorem 3.4.1: The Fundamental Theorem of Dimension Theory

Let (R, m) be a local Noetherian ring. Then the following numbers are equal.

- The Krull dimension $\dim(R)$.
- The smallest number $d \in \mathbb{N}$ such that

$$\lim_{t \to 1}(1-t)^d HS_{\text{gr}_m(R)}(t) < \infty$$

  (Called the order of the pole at 1, equivalently the number r so that $HS_{\text{gr}(R)} = \frac{f(t)}{(1-t)^r}$ and f and $(1-t)$ are coprime.
- The minimal number of generators

$$\delta_m(R) = \min\{n \in \mathbb{N} \mid x_1, \dots, x_n \in R \text{ generates } m\}$$

(which is the same number as the minimal number of generators of any m-primary ideals).

Theorem 3.4.2: Krull's Height Theorem

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

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

Proposition 3.4.3

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

$$\dim(R) \leq \dim_{R/m}\left(\frac{m}{m^2}\right) < \infty$$

Proof. We have seen in Commutative Algebra 1 that $\dim(R) = \dim(R_m) = \text{ht}_R(m)$. By Krull's height theorem, $\text{ht}_R(m) \leq \delta_m(R)$. Finally, by prp3.2.3 we have $\delta_m(R) = \dim_{R/m}(m/m^2)$ so we are done. □

Proposition 3.4.4

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

$$\dim(R) = \dim(\widehat{R})$$

4 Regular Sequences

4.1 Regular Sequences

Definition 4.1.1: Regular Elements

Let R be a commutative ring. Let M be an R-module. Let $x \in R$. We say that x is an M-regular element if x is not a zero divisor.

Note that this is the same as saying the multiplication map $\phi_x : M \to M$ is injective.

Definition 4.1.2: Regular Sequences

Let R be a commutative ring and let M be an R-module. Let $x_1, \dots, x_n \in R$ be an ordered sequence in R. We say that the sequence is M-regular if x_k is a regular element of $\frac{M}{(x_1,\dots,x_{k-1})M}$ for $1 \leq k \leq n$.

It is important to note that M-regularity depends on the order of the elements in the sequence.

4.2 Relation to the Koszul Complex

Let R be a commutative ring. Let $x_1, \dots, x_n \in R$. Recall that the Koszul complex $K(x_1, \dots, x_n)$ is the chain complex given explicitly as

$$0 \longrightarrow \bigwedge_{i=1}^n R^n \xrightarrow{d_n} \bigwedge_{i=1}^{n-1} R^n \longrightarrow \cdots \longrightarrow R^n \xrightarrow{d_1} R \longrightarrow 0$$

where the differential $d_k : \bigwedge_{i=1}^k R^n \to \bigwedge_{i=1}^{k-1} R^n$ is given on basis elements by

$$d(e_{i_1} \wedge \cdots \wedge e_{i_k}) = \sum_{j=1}^k (-1)^{j+1} x_{i_j} e_{i_0} \wedge \cdots \wedge \hat{e}_{i_j} \wedge \cdots \wedge e_{i_k}$$

where each $e_{i_j} \in \mathbb{R}^n$.

For an example, let R be a commutative ring. Let $x, y \in R$. Then the Koszul complex $K(x, y)$ is given by

$$0 \longrightarrow R \longrightarrow R^2 \longrightarrow R \longrightarrow 0$$

The differentials are given as follows.

- The first differential $R^2 \to R$ is given by $(r, s) \mapsto rx + sy$. It can also be given as a 1×2 matrix as $\begin{pmatrix} x & y \end{pmatrix}$. Also alternatively, we can write an R-basis for R^2 with $(1, 0)$ and $(0, 1)$. Then define the map $R^2 \to R$ by $(1, 0) \mapsto x$ and $(0, 1) \mapsto y$.
- The second differential $R \to R^2$ is given by $1 \mapsto (x, -y)$.

Proposition 4.2.1

Let R be a commutative ring and let M be an R-module. Let $x_1, \dots, x_n \in R$ be an ordered sequence in R. If $x_1, \dots, x_n$ is M-regular, then

$$H_p^{\text{Kos}}(x_1, \dots, x_n; M) = 0$$

for all $p \geq 1$.

Corollary 4.2.2

Let R be a commutative ring and let $x_1, \dots, x_n \in R$. If $x_1, \dots, x_n$ is a regular sequence, then the Koszul complex $K(x_1, \dots, x_n)$ is a free resolution of $R/(x_1, \dots, x_n)$.

Proposition 4.2.3

Let R be a commutative ring. Let M be an R-module. Let $x, y \in R$. If x is a regular element and $H_1^{\text{Kos}}(x, y; M) = 0$, then x, y is a regular sequence.

Proposition 4.2.4

Let (R, m) be a Noetherian local ring. Let M be a finitely generated R-module. Let $x, y \in m$. Then x, y is an M-regular sequence if and only if y, x is an M-regular sequence.

4.3 Depth of an Ideal

5 Homological Dimension Theory

5.1 Projective Dimension

Definition 5.1.1: Projective Dimension

Let R be a commutative ring. Let M be an R-module. Define the projective dimension of M to be

$$\text{pd}_R(M) = \min\{n \in \mathbb{N} \mid \text{there is a projective resolution of } M \text{ with } n \text{ terms}\}$$

5.2 Depth of a Module

Definition 5.2.1: I-Depth of a Module

Let R be a commutative ring. Let I be an ideal of R. Let M be a finitely generated R-module. Define the I-depth of M to be

$$\text{depth}_I(M) = \min\{n \in \mathbb{N} \mid \text{Ext}_R^n(R/I, M) \neq 0\}$$

Proposition 5.2.2

Let (R, m) be a Noetherian local ring. Let M be a finitely generated R-module. Then we have

$$\text{depth}_m(M) = \sup\{n \in \mathbb{N} \mid x_1, \dots, x_n \in m \text{ is an } M\text{-regular sequence }\}$$

Proposition 5.2.3

Let (R, m) be a Noetherian local ring. Then $\text{depth}_m(R) = 0$ if and only if m is an associated prime.

Theorem 5.2.4: Auslander–Buchsbaum formula

Let (R, m) be a Noetherian local ring. Let M be a finitely generated R-module. If $\text{pd}_R(M)$ is finite, then we have

$$\text{pd}_R(M) + \text{depth}_m(M) = \text{depth}_m(R)$$

5.3 Global Dimensions

Definition 5.3.1: Global Dimension

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

$$\text{gl dim}(R) = \sup\{\text{pd}(M) \mid M \text{ is an } R\text{-module }\}$$

Theorem 5.3.2: Hilbert's Syzygy Theorem

Let k be a field. Let M be a finitely generated module over $k[x_1, \dots, x_n]$. Then M has a free resolution of length at most $n + 1$.

6 Regular Local Rings

6.1 Basic Properties

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

Definition 6.1.1: Regular Local Rings

Let (R, m) be a Noetherian local ring. We say that R is a regular local ring if

$$\dim(R) \leq \dim_{R/m}\left(\frac{m}{m^2}\right)$$

Lemma 6.1.2

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 6.1.3

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

6.2 Homological Methods

7 Two Important Rings Through the Koszul Complex

In this section we will investigate two 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.

7.1 Gorenstein Rings

Definition 7.1.1: Gorenstein Rings

Definition 7.1.2: Injective Dimension

7.2 Cohen-Macauley Rings

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

8 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.

8.1 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 8.1.1: 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:

$$\begin{tikzcd} B \arrow[r, "d"] \arrow[dr, "d'"'] & \Omega^1_{B/A} \arrow[d, dashed, "\exists! f"] \\ & M \end{tikzcd}$$

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 8.1.2

Let A be a ring and B an A-algebra. Let M be a B-module. Then there is a canonical B-module isomorphism
$$\text{Hom}_B(\Omega^1_{B/A}, M) \cong \text{Der}_A(B, M)$$

Proof. Fix M a B-module. Let $d' \in \text{Der}_A(B, M)$. 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 $\phi : \text{Der}_A(B, M) \to \text{Hom}_B(\Omega^1_{B/A}, M)$ defined by $\phi(d') = f$.

Conversely, given a map $g \in \text{Hom}_B(\Omega^1_{B/A}, M)$, pre-composition with d gives a pull back map $d^* : \text{Hom}_B(\Omega^1_{B/A}, M) \to \text{Der}_A(B, M)$ 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 $f, g \in \text{Hom}_B(\Omega^1_{B/A}, M)$.

- $d^*(f + g) = (f + g) \circ d$ 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 8.1.3

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 8.1.4

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 8.1.5

Let A be a ring and $B = A[x_1, \dots, x_n]$ 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 $d(x_1), \dots, d(x_n)$. 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 $\Omega^1_{A[x_1,\dots,x_{n-1}]/A} = \bigoplus_{i=1}^{n-1} Bd(x_i)$. Then for every $f \in A[x_1, \dots, x_n]$, we can write the function as

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

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 $d(x_1), \dots, d(x_{n-1})$. 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

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

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

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

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. □

8.2 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 8.2.1: 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 8.2.2: 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 $i - j = h_1 h_2$. Now we have that

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

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 8.1.2), 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 $B = A[x_1, \dots, x_n]$ and $C = \frac{B}{I = (f_1, \dots, f_r)}$, 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 8.2.2, 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 $f_1, \dots, f_r$ and thus the map sends e_i to f_i for $1 \leq i \leq r$.

Now consider the map

$$J : \bigoplus_{i=1}^{r} Cde_i \twoheadrightarrow \frac{I}{I^2} \to \bigoplus_{i=1}^{n} Cdx_i$$

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 $I/I^2 \to \bigoplus_{i=1}^{n} Cdx_i$ sends f_i to $d(f_i) = \sum_{k=1}^{n} \frac{\partial f_i}{\partial x_k} dx_k$ (by second exact sequence 8.2.2) 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 $\text{im}(A \twoheadrightarrow B \to C) = \text{im}(B \to C)$, we thus have

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

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

8.3 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 8.3.1

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 $c_0, \dots, c_n \in K$ 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 $c_0, \dots, c_n \in K$, we obtain $f'(b) = c_1 d(b) + \cdots + c_n \cdot nb^{n-1} d(b)$. 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 8.3.2

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 8.3.1, 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

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

Since $p'(t) = 0$, we have that $\Omega^1_{L/E} \cong L \neq 0$. By the first exact sequence 8.2.1, 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 8.3.3

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 8.3.1. 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 **??**.

9 The Picard Group of an Integral Domain

9.1 The Picard Group

Definition 9.1.1: The Picard Group of a Ring

Let R be an integral domain. Define the picard group of R to be the set

$$\text{Pic}(R) = \{I \subseteq R \mid I \text{ is invertible}\}/\sim$$

where $I \sim J$ if I and J are isomorphic as R-modules, together with binary operation given by tensor products.

Lemma 9.1.2

Let R be a ring. If R is a UFD, then $\text{Pic}(R)$ is trivial.