Commutative Algebra 2

Labix

May 13, 2025

Abstract

Contents

1 Results from Homological Algebra

1.1 Inverse Systems

Definition 1.1.1: Inverse Systems

Definition 1.1.2: Short Exact Sequence of Inverse Systems

Proposition 1.1.3

Left Exactness of the Inverse Limit Functor

Definition 1.1.4: The Mittag-Leffler Condition

Lemma 1.1.5

Surjective maps imply Mittag-Leffler

Proposition 1.1.6

Exactness of the inverse limit functor with Mittag-Leffler

1.2 Projective and Injective Modules

Let R be a commutative ring. Let P be an R-module. Recall that P is projective if one of the following equivalent conditions hold.

- $\text{Hom}(P, -)$ is an exact functor (it sends exact sequences to exact sequences).
- For every surjective homomorphism $f : N \twoheadrightarrow M$ and every R-module homomorphism $g : P \to M$, there exists a module homomorphism $h : P \to N$ such that the following diagram commutes:

$$\begin{tikzcd} & N \arrow[d, two heads, "f"] \\ P \arrow[ur, dashed, "\exists h"] \arrow[r, "g"'] & M \end{tikzcd}$$

- $P \oplus Q$ is a free R-module for some R-module Q.

In particular, the following are projective modules.

- Free modules are projective.
- $\bigoplus_{i \in I} P_i$ is projective if and only if each P_i is projective.

Proposition 1.2.1

Let R be a commutative ring. Let P be a finitely generated R-module. Suppose that one of the following conditions hold.

- R is a local ring.
- R is graded and P is graded.

If P is projective, then P is free.

Proposition 1.2.2

Let R be a Dedekind domain. Then every ideal of R is projective.

Let R be a commutative ring. Let I be an R-module. Recall that I is injective if one of the following equivalent conditions hold.

- $\mathrm{Hom}(-, I)$ is an exact functor (it sends exact sequences to exact sequences).
- For every injective homomorphism $f : N \rightarrowtail M$ and every module homomorphism $g : N \to I$, there exists a module homomorphism $h : M \to I$ such that the following diagram commutes:

$$\begin{tikzcd} N \arrow[d, tail, "f"'] \arrow[dr, "g"] & \\ M \arrow[r, dashed, "\exists h"'] & I \end{tikzcd}$$

1.3 Flat Modules

Let R be a commutative ring. Let M be an R-module. Recall that M is a flat R-module if the functor $- \otimes_R M$ is exact. Equivalently, the functor sends injective maps to injective maps. Moreover, we have the following properties:

- If M, N are flat R-modules, then $M \otimes_R N$ is flat.
- If S is an R-algebra and M is a flat R-module, then $M \otimes_R S$ is a flat S-module.
- If S is an R-algebra and M is a flat S-module, then M is a flat R-module.

Moreover, we have the following relations between different homological notions of modules

$$\text{Free Modules} \subset \text{Projective Modules} \subset \text{Flat Modules} \subset \text{Torsion Free Modules}$$

Proposition 1.3.1

Let R be a commutative ring. Let S be a multiplicative subset of R. Then $S^{-1}R$ is a flat R-module.

Definition 1.3.2: Faithfully Flat

Let R be a commutative ring. Let M be an R-module. We say that M is faithfully flat if for any sequence of R-modules:

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

The sequence is short exact if and only if the sequence

$$0 \longrightarrow M_1 \otimes_R M \xrightarrow{f \otimes_R \mathrm{id}_M} M_2 \otimes_R M \xrightarrow{g \otimes_R \mathrm{id}_M} M_3 \otimes_R M \longrightarrow 0$$

is exact.

Definition 1.3.3: Flat Homomorphism

Let R, S be rings. Let $\varphi : R \to S$ be a ring homomorphism. We say that φ is flat if S is flat as an R-module.

Proposition 1.3.4

Let R be a commutative ring. Let M be an R-module. Then the following are equivalent.

- M is flat.
- For every R-module N, we have $\text{Tor}_1^R(M, N) = 0$.
- For every finitely generated ideal I, we have $\text{Tor}_1^R(M, A/I) = 0$.

Proposition 1.3.5

Let R be a commutative ring. Let the following be an exact sequence of R-modules.

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

If M_1 and M_3 are flat, then M_2 is flat.

1.4 Finitely Presented Modules

Let R be commutative ring. Recall that an R-module M if finitely presented if there exists an exact sequence of the form

$$R^m \longrightarrow R^n \longrightarrow M \longrightarrow 0$$

Lemma 1.4.1

Let R be a commutative ring. Let M be an R-module. Then M is finitely presented if and only if M is finitely generated.

2 Filtrations

2.1 Filtrations and Stable Filtrations

Definition 2.1.1: 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 2.1.2: 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 2.1.3: 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

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

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.

2.2 Filtrations by Powers of Ideals

Theorem 2.2.1: 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 2.2.2: 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 $N = 0$. □

3 Completions

3.1 General Completion Methods

Definition 3.1.1: 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

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

The maps defining the inverse limit is given by the projection maps $M \to \frac{M}{M_i}$, which descends to a well defined map $\frac{M}{M_{i+1}} \to \frac{M}{M_i}$.

Lemma 3.1.2

Let R be a commutative ring. Let M be an R-module. Let $\{M_i \mid i \in \mathbb{N}\}$ and $\{N_j \mid j \in \mathbb{N}\}$ be two filtrations of M. Suppose that for all $i \in \mathbb{N}$, there exists $j \in \mathbb{N}$ such that $M_i \subseteq N_j$, and that for all $j \in \mathbb{N}$, there exists $i \in \mathbb{N}$ such that $N_j \subseteq M_i$. Then there is a natural isomorphism

$$\varprojlim_i \frac{M}{M_i} \cong \varprojlim_j \frac{M}{N_j}$$

given by the universal property of inverse limits.

Lemma 3.1.3

Let R be a commutative ring. Let M be an R-module. The map $M \to \widehat{M}$ induced by the universal property is injective if and only if $\bigcap_{i=0}^{\infty} M_i = \{0\}$.

For instance, the assumption of the lemma holds true when (R, m) is a Noetherian local ring and we take the R-module as the maximal ideal m.

3.2 I-Adic Completion of a Module

Definition 3.2.1: 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 3.2.2

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 $I^n N$.

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

Proof. Let $k \in \mathbb{N}$ and $x \in I^k N$. Then $x \in I^k M$ and since N is a submodule, we have $x \in N$ so that $x \in I^k M \cap N$ (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

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

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

$$x = \sum_{i=1}^{r} y_i t_i$$

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

Hence for all $n > c$, we have an equality $I^n N = I^n M \cap N$. By lemma 2.1.2, we conclude that the completion with respect to the two filtrations are isomorphic. $\square$

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 3.2.3

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 3.2.4

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 3.2.5: 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.

3.3 I-Adic Completion of a Ring

Example 3.3.1

Let k be a field. Then the following are true.

- The completion of $k[x]$ with respect to the maximal ideal $(x-a)$ is $k[[x-a]]$. Moreover, any element $f \in k[x]$ has image given by $(f \bmod (x-a)^n)_{n\in\mathbb{N}}$.
- The element $1/1-x \in k[[x]]$ is represented by the sequence $(1, 1+t, 1+t+t^2, \dots)$.
- The completion of $k[x_1, \dots, x_n]$ with respect to the maximal ideal $(x_1 - a_1, \dots, x_n - a_n)$ is $k[[x_1, \dots, x_n]]$.

Proposition 3.3.2

Let R be a Noetherian commutative ring. Let I be an ideal of R. Then the following are true.

- If I is finitely generated by $a_1, \dots, a_n \in I$, then there is an isomorphism

$$\widehat{R} \cong \frac{R[[x_1, \dots, x_n]]}{(x_1 - a_1, \dots, x_n - a_n)}$$

- $\widehat{R}_I$ is Noetherian.
- $\widehat{R}_I$ is a flat R-module.

Proposition 3.3.3

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 3.3.4: 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.

Lemma 3.3.5

Let (R, m) be a local ring. If R is Artinian, then R is complete.

3.4 Hensel's Lemma

Theorem 3.4.1: 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 $\overline{v} = h$.

4 More on Dimension Theory

4.1 The Hilbert Series of a General Graded Module

Definition 4.1.1: 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 4.1.2: 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 4.1.3

Let R be commutative ring such that $R = \bigoplus_{i=0}^\infty R_i$ is graded. Let the following be an exact sequence of graded R-modules.

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

Then we have

$$HS_{M_2}(t) = HS_{M_1}(t) + HS_{M_3}(t)$$

Example 4.1.4

Let R be a commutative ring. Let $A_d = R[x_1, \dots, x_d]$ be graded with $\deg(x_i) = 1$. Then we have

$$HS_{A_d}(t) = l_R(R)\sum_{n=0}^\infty \binom{d+n-1}{d-1}t^n$$

Proof. We induct on d. When $d = 1$, then $HF_{R[x]}(n) = l_R(R \cdot x^n) = l_R(R)$. Hence $HS_{R[x]}(t) = l_R(R)\sum_{n=0}^\infty t^n$. Suppose that the result is true for $\leq d-1$. Consider the exact sequence

$$0 \longrightarrow R[x_1, \dots, x_d](-1) \xrightarrow{\times x_d} R[x_1, \dots, x_d] \twoheadrightarrow R[x_1, \dots, x_{d-1}] \longrightarrow 0$$

Then we have

$$HF_{A_d}(n) = HF_{A_d(-1)}(n) + HF_{A_{d-1}}(n) = HF_{A_d}(n-1) + \binom{d+n-2}{d-2}l_R(R)$$

Now fix d and induct on n ($n = 0$ is clear) to deduce that

$$HF_{A_d}(n) = l_R(R)\left(\binom{d+n-2}{d-1} + \binom{d+n-2}{d-2}\right) = l_R(R)\binom{d+n-1}{d-1}$$

and so induction is complete. The result on the Hilbert series then follows. □

Example 4.1.5

Let k be a field. Let $n \geq 2$. Let $f \in k[x_1, \dots, x_d]$ be a homogeneous polynomial of degree s. Let $A = \frac{k[x_1,\dots,x_n]}{(f)}$. Then we have

$$HF_A(n) = \binom{d+n-1}{d-1} - \binom{d+n-1-s}{d-1}$$

Proof. Consider the short exact sequence

$$0 \longrightarrow k[x_1, \dots, x_d](-s) \xrightarrow{\times f} k[x_1, \dots, x_d] \twoheadrightarrow \frac{k[x_1,\dots,x_d]}{(f)} \longrightarrow 0$$

We have that

$$HF_A(n) = HF_{k[x_1,\dots,x_d]}(n) - HF_{k[x_1,\dots,x_d](-s)}(n) = \binom{d+n-1}{d-1} - \binom{d+n-1-s}{d-1}$$

□

Proposition 4.1.6

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

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

□

Proposition 4.1.7

Let k be a field. Let $M = \bigoplus_{k=0}^{\infty} M_k$ be a finitely generated graded k-module. If M is generated by r homogeneous elements of degrees $d_1, \dots, d_r$, then the Hilbert-series of M is given by

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

for some $f \in \mathbb{Z}[t]$.

Example 4.1.8

Let k be a field. Let $A = k[x_1, \dots, x_d]$. Then the Hilbert series of A is given by

$$HS_A(t) = \frac{1}{(1-t)^d}$$

Definition 4.1.9: The Hilbert Polynomial

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 $f(t) = \sum_{j=0}^{s} a_j t^j \in \mathbb{Z}[t]$. Define the Hilbert polynomial of M to be

$$HP_M(t) = \sum_{j=0}^{s} \binom{r+n-1-j}{r-1} a_j$$

Lemma 4.1.10

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 $f \in \mathbb{Z}[t]$. Then the following are true.

- The smallest $d \in \mathbb{N}$ such that
$$\lim_{t\to 1} HS_M(t) < \infty$$
is $\deg(HP_M) + 1$.
- $HP_M(n) = HF_M(n)$ for all $n \geq \deg(f) - \deg(HP_M)$

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

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

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. ∎

Example 4.1.11

Let k be a field. Let $A = k[x_1, \dots, x_d]$. Let $f \in A$ be homogeneous of degree s. Then the following are true.

- $HP_A(t) = \frac{1}{(d+1)!}(t+d-1)(t+d)\cdots(t+1)$.
- If $d \geq 2$, then $\deg(HP_{A/(f)}) = d-2$.

Proof. Recall that $HF_A(n) = \binom{d+n-1}{d-1} = \frac{(d+n-1)!}{(d-1)!n!} = \frac{1}{(d-1)!}(d+n-1)\cdots(n+1)$.

As for the second example, we have

$$\begin{aligned} HF_{A/(f)}(n) &= \binom{d+n-1}{d-1} - \binom{d+n-1-s}{d-1} \\ &= \frac{1}{(d-1)!}\left((d+n-1)\cdots(n+1) - (d+n-1-s)\cdots(n-s+1)\right) \end{aligned}$$

when $n \geq s$. Notice that there is no n^{d-1} since the first and second terms with n^{d-1} cancel each other out. Hence the degree of the Hilbert function is $d-2$. $\square$

4.2 The Hilbert Series of the Associated Graded Module

Let R be a commutative ring. Let I be an ideal of R. Let M be an R-module. Under these assumptions we can associate to M a graded R-module

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

and then apply the above theorem to the associated graded ring. First thing of note is that $HS_{\text{gr}_I(M)}(t)$ is of the form in 3.1.4.

Proposition 4.2.1

Let R be a commutative ring. Let I be an ideal of R. Let M be a finitely generated R-module. Then the Hilbert series of $\text{gr}_I(M)$ is given by

$$HS_{\text{gr}_I(M)}(t) = \frac{f(t)}{(1-t)^d}$$

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

Definition 4.2.2: The Hilbert Series Degree

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 degree to be

$$d_I(M) = \min\{d \in \mathbb{N} \mid \lim_{t\to 1}(1-t)^d HS_{\text{gr}_I(M)}(t) < \infty\}$$

This is the same as saying that

$$HS_{\text{gr}_I(M)}(t) = \frac{f(t)}{(1-t)^{d_I(M)}}$$

for f and $1-t$ coprime.

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

Definition 4.2.3: 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

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

We should think χ_M^I as a function $\mathbb{N} \to \mathbb{N}$. If we restrict the domain to $n > \deg(f)$ where $\text{HS}_{\text{gr}_I(M)}(t) = \frac{f(t)}{(1-t)^{d_I(M)}}$ then χ_M^I is a polynomial in n.

Proposition 4.2.4

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

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

Proof. We consider the collection of short exact sequences of the form

$$0 \longrightarrow I^k M \longrightarrow I^{k-1}M \longrightarrow \frac{I^{k-1}M}{I^k M} \longrightarrow 0$$

For $1 \leq k \leq n$. Using the fact that $l_R(I^{k-1}M/I^k M) = l_R(I^{k-1}M) - l_R(I^k M)$, we deduce that

$$\sum_{k=1}^n l_R\left(\frac{I^{k-1}M}{I^k M}\right) = l_R(M) - l_R\left(\frac{M}{I^n M}\right) = l\left(\frac{M}{I^n M}\right)$$

$\square$

We can think of the Hilbert-Samuel function as the partial sum of the coefficients of the Hilbert series of $\text{gr}_I(M)$. Indeed, the Hilbert series of the associated graded ring is given by

$$HS_{\text{gr}_I(M)}(t) = l_R\left(\frac{M}{IM}\right) + l_R\left(\frac{IM}{I^2M}\right)t + l_R\left(\frac{I^2M}{I^3M}\right)t^2 + \dots$$

Proposition 4.2.5

Let R be a commutative ring. Let I be an ideal of R. Let M be a finitely generated R-module. Then the Hilbert polynomial of $\text{gr}_I(M)$ is equal to the Hilbert Samuel function. In other words, we have

$$HP_{\text{gr}_I(M)} = \chi_M^I$$

Proposition 4.2.6

Let (R, m) be a Noetherian local ring. Let I be an m-primary ideal. Let M be a finitely generated R-module. Then

$$d_I(M) = d_m(M)$$

In particular, the Hilbert series degree is invariant under the choice of m-primary ideal.

Proof. Since I is m-primary in a Noetherian local ring, we have $m^n \subseteq I \subseteq m$ for some n.

Then we have $m^{nr} \subseteq I^r \subseteq m^r$. Hence we have

$$l_R\left(\frac{M}{m^n M}\right) \leq l_R\left(\frac{M}{I^n M}\right) \leq l_R\left(\frac{M}{m^{rn} M}\right)$$

since $N \leq M$ implies that $l_R(M) = l_R(N) + l_R(M/N) \geq l_R(N)$. Hence for large n we have

$$\chi_M^m(n) \leq \chi_M^I(n) \leq \chi_M^m(rn)$$

Since the first and last polynomial in the inequality have the same degree, we conclude that χ_M^I has the same degree as χ_M^m. □

Proposition 4.2.7

Let (R, m) be a Noetherian local ring. Let I be an m-primary ideal of R. Let the following be an exact sequence of finitely generated R-modules.

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

Then we have

$$d_I(M_2) = \max\{d_I(M_1), d_I(M_3)\}$$

Moreover, if $d_I(M_1) = d_I(M_2) = d_I(M_3)$ then the leading coefficient of $\chi_{M_2}^I$ is equal to the sum of the leading coefficients of $\chi_{M_1}^I$ and $\chi_{M_3}^I$.

Corollary 4.2.8

Let (R, m) be a local ring that is an integral domain. Let I be an m-primary ideal. Let $x \in R$ be non-zero. Then we have

$$d_I\left(\frac{R}{(x)}\right) \leq d_I(R) - 1$$

Proof. The multiplication by x map is injective in this case, and so we obtain an exact sequence

$$0 \longrightarrow R \xrightarrow{\cdot x} R \longrightarrow \frac{R}{(x)} \longrightarrow 0$$

Applying the above prp gives $d_I(R) = \max\{d_I(R), d_I(R/(x))\}$. Assume for a contradiction that $d_I(R/(x)) = d_I(R)$. Then the leading coefficient of χ_R^I is equal to the leading coefficients of χ_R^I and $\chi_{R/(x)}^I$ by the above prp. But this implies that the leading coefficient of $\chi_{R/(x)}^I$ is 0, a contradiction. Hence $d_I(R/(x))$ is strictly less than $d_I(R)$, and so $d_I(R/(x)) \leq d_I(R) - 1$. □

4.3 System of Parameters and Its Minimal Size

Definition 4.3.1: System of Parameters of a Module

Let (R, m) be a Noetherian local ring. Let M be an R-module, Let $x_1, \dots, x_r \in R$. We say that the sequence is a system of parameters for M if

$$l(M/(x_1, \dots, x_r)M) < \infty$$

Lemma 4.3.2

Let (R, m) be a Noetherian local ring. Let $x_1, \dots, x_r \in m$. Then the sequence is a system of parameters of R if and only if $(x_1, \dots, x_r)$ generate an m-primary ideal.

Lemma 4.3.3

Let R be a Noetherian local ring. Then R has a system of parameters.

Proposition 4.3.4

Let (R, m) be a Noetherian local ring of dimension $\dim(R) = d$. Let $x_1, \dots, x_d$ be a system of parameters of R. Then the following are true.

- $\dim(R/(x_1, \dots, x_i)) = d - i$ for all $1 \leq i \leq d$.
- $R/(x_1, \dots, x_d)$ is Artinian.

Lemma 4.3.5

Let (R, m) be a Noetherian local ring of dimension d. Let $x_1, \dots, x_d$ be a system of parameters of R. Then $x_1, \dots, x_d$ are algebraically independent over R/m.

Definition 4.3.6: Minimal Elements for Finite Length

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

$$\delta(M) = \min\{n \in \mathbb{N} \mid x_1, \dots, x_n \in R \text{ such that } l_R(M/x_1M + \cdots + M/x_nM) < \infty\}$$

Proposition 4.3.7

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

$$\delta(R) = \min\{d \in \mathbb{N} \mid x_1, \dots, x_n \in m \text{ is a system of parameters }\}$$

Proposition 4.3.8

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

$$\delta(R) \leq \dim_{R/m}(m/m^2) < \infty$$

Proof. We have that $\delta(R) \leq$ minimal number of generators of $m = \dim_{R/m}(m/m^2)$. □

4.4 The Fundamental Theorem of Dimension Theory

Theorem 4.4.1: The Fundamental Theorem of Dimension Theory

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

- The Krull dimension
$$\dim(M) = \dim(R/\text{Ann}_R(M))$$
- The Hilbert-Samuel degree
$$d_I(M) = \min\{d \in \mathbb{N} \mid \lim_{t \to 1}(1-t)^d HS_{\text{gr}_I(M)}(t) < \infty\}$$

- The minimal number of generators

$$\delta_I(M) = \min\{n \in \mathbb{N} \mid x_1, \dots, x_n \in m \mid l_R(M/(x_1, \dots, x_n)M) < \infty\}$$

Proof.

- $\dim(R) \leq d_I(R)$
We induct on d. When $d_I(R) = 0$, then $l\left(\frac{R}{m^n}\right)$ is eventually constant by 3.2.3. Then $m^n = m^{n+1}$ for some n. By Nakayama's lemma we conclude that $m^n = 0$. Then R is a Noetherian commutative ring that has a nilpotent maximal ideal. From Commutative Algebra 1 2.3.5 we conclude that R is Artinian, and $\dim(R) = 0$.

  When $d \neq 0$, let $P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_r$ be a chain of prime ideals of R. Let $x \in P_1 \setminus P_0$. Then the image $[x]$ of x under the quotient map $R \to \frac{R}{P_0}$ is non-zero. Moreover, $\frac{R}{P_0}$ is an integral domain. Let $A = \frac{R/P_0}{([x])} \cong \frac{R}{P_0+xR}$. We can apply 3.2.5 to deduce that $d_m(A) \leq d_m(R/P_0) - 1$. By inductive hypothesis we deduce that $\dim(A) \leq d_m(A) \leq d_m(R/P_0) - 1$.

  Write $p : R \to A$ the quotient map. It descends to a map $p : \frac{R}{P_i} \to \frac{A}{p(P_i)}$ for $1 \leq i \leq r$. Since $A \cong \frac{R}{P_0+xR}$ we deduce that $\frac{A}{P_i} \cong \frac{R}{P_0+xR+P_i} \cong \frac{R}{P_i}$ since $x \in P_1$. Hence $p : \frac{R}{P_i} \to \frac{A}{p(P_i)}$ is an isomorphism. Since P_i is prime, $\frac{R}{P_i}$ is an integral domain and so $\frac{A}{p(P_i)}$ is an integral domain and $p(P_i)$ is prime. This means that we now have a chain of prime ideals $p(P_1) \subset \cdots \subset p(P_r)$ in A. It is a strict chain since $\frac{R}{P_i}$ is strictly biggerthan $\frac{R}{P_{i+1}}$ implies that $\frac{A}{p(P_i)}$ is strictly bigger than $\frac{A}{p(P_{i+1})}$. Then we have

$$r - 1 \leq \dim(A) \leq d_m(A) \leq d_m(R/P_0) - 1$$

  Finally, under the surjective map p, R/m^n is sent to $A/p(m)^n$. Hence $l(R/m^n) \geq l(A/p(m)^n)$ so that $d_m(R) \geq d_m(R/P_0)$. Then combining with the above inequality we deduce that $r - 1 \leq d_m(R/P_0) - 1 \leq d_m(R) - 1$ so that $r \leq d_m(R)$. Since this is true for all chains of prime ideals of R, we deduce that $\dim(R) \leq d_m(R)$.

- $d_m(R) \leq \delta_m(R)$. Suppose that $x_1, \dots, x_r$ generate m.

□

Theorem 4.4.2: Krull's Principal Ideal Theorem

Let R be a Noetherian commutative ring. Let I be a principal ideal of R. Let P be a smallest prime ideal containing I. Then we have

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

Proof. Suppose that $I = (x)$. I claim that $(x)_P$ is PR_P-primary ideal. Since R is Noetherian, R_P is Noetherian and this means that $(PR_P)^n = 0$ for some n. Then $0 \subset (x)_P \subseteq PR_P$ implies that $(x)_P$ is PR_P-primary. By the fundamental theorem of dimension theory, we have

$$\text{ht}_R(P) = \dim(R_P) = \delta_{R_P}((x)_P) \leq 1$$

and so we are done. □

Theorem 4.4.3: 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 4.4.4

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, $\text{ht}_R(m) \leq \delta(R)$. Finally, by prp3.2.3 we have $\delta(R) \leq \dim_{R/m}(m/m^2)$ so we are done. $\square$

Proposition 4.4.5

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

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

Proposition 4.4.6

Let R be a Noetherian commutative ring. Let P be a prime ideal of R. Then P satisfies the descending chain condition.

5 Regular Sequences

5.1 Regular Sequences

Definition 5.1.1: 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 5.1.2: Regular Sequences

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

Lemma 5.1.3

Let R be a commutative ring. Let M be an R-module. If $x_1, \dots, x_n$ is an M-regular sequence, then $x_1^r, \dots, x_n^r$ is an M-regular sequence for all $r \in \mathbb{N} \setminus \{0\}$.

Lemma 5.1.4

Let (R, m) be a local ring. If $x_1, \dots, x_n \in m$ is a regular sequence, then it is always extendable to a system of parameters.

Definition 5.1.5: Maximal Regular Sequences

Let R be a commutative ring. Let M be an R-module. Let $x_1, \dots, x_n \in I$ be a regular sequence. We say that the sequence is maximal if for any $y \in I$, $x_1, \dots, x_n, y$ is not a regular sequence.

5.2 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 5.2.1

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 an M-regular sequence, then

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

for all $p \geq 1$.

Corollary 5.2.2

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 5.2.3

Let R be a commutative ring. Let $M \neq \{0\}$ be an R-module. Suppose that one of the following conditions hold.
- R is a local ring with unique maximal ideal m, $x_1, \dots, x_n \in m$ and M is a finitely generated R-module.
- R is an $\mathbb{N}$-graded ring, M is an $\mathbb{N}$ graded R-module and $x_1, \dots, x_n$ are homogeneous elements of degree > 0.

If moreover $H_1^{\text{Kos}}(x_1, \dots, x_n; M) = 0$, then $x_1, \dots, x_n$ is an M-regular sequence.

5.3 The Depth of a Module

Definition 5.3.1: 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

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

If (R, m) is a local ring then we write $\text{depth}(M) = \text{depth}_m(M)$.

Lemma 5.3.2

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

Proof. The depth is equal to the maximal M-regular sequence in m. It is 0 if and only if there is no regular sequences at all, which is true if and only if every element of m is a zero divisor. Since the union of associated primes is precisely the set of non-zero zero divisors, every element of m is a zero divisor if and only if m is contained in the union of associated primes. By plenty of primes, m is contained in one of the associated primes. Then by maximality of m, m is an associated prime of M. $\square$

Example 5.3.3

he following are true.
- We have $\text{depth}_{(x,y)}\left(\frac{k[x,y]}{(xy,y^2)}\right) = 0$.
- Let $R = \frac{k[x,y,z,t]}{(xz,xt,yz,yt)}$. Let $m = (x, y, z, t)$. Then $\text{depth}_m(R) = 1$.

Proof. Consider the element $y+(xy,y^2)$ in the ring. Notice that (x,y) annihilates the element. By maximality of (x,y), we have $(x,y)=\text{Ann}_{k[x,y]/(xy,y^2)}([y])$ and so $(x,y)\in\text{Ass}(k[x,y]/(xy,y^2))$. Since Ass is the union of all non-zero zero divisors, we conclude that every element of m is a zero divisor. Thus the (x,y)-depth is 0.

Clearly $y+t$ is a non-zero divisor because the ideal in the quotient does not contain linear polynomials, and so the m-depth of R is greater than or equal to 1. However, notice that we have $m=\text{Ann}_{R/(y+t)}([y])$. Hence the every element of m is a zero divisor of $R/(y+t)$, and so $\text{depth}_m(R)=1$. □

Proposition 5.3.4: Depth Sensitivity of the Koszul Complex

Let R be a Noetherian commutative ring. Let $I=(x_1,\dots,x_n)$ be an ideal of R. Let M be a finitely generated R-module such that $IM\neq M$. Then we have

$$\text{depth}_I(M)=n-\sup\{i\in\mathbb{N}\mid H_i^{\text{Kos}}(x_1,\dots,x_n,M)\neq 0\}$$

Corollary 5.3.5

Let R be a Noetherian commutative ring. Let $I=(x_1,\dots,x_n)$ be an ideal of R. Let M be a finitely generated R-module such that $IM\neq M$. Then $x_1,\dots,x_n$ is an M-regular sequence if and only if $\text{depth}_I(M)=n$.

5.4 Depth and the Vanishing of Ext

Proposition 5.4.1

Let R be a Noetherian commutative ring. Let I be an ideal of R. Let M be a finitely generated R-module such that $IM\neq M$. Let $n\in\mathbb{N}$. Then the following are equivalent.

- For all $i<n$,
  $$\text{Ext}_R^i(N,M)=0$$
  for all finitely generated R-module N such that $\text{Supp}(N)\subseteq\{P\in\text{Spec}(R)\mid I\subseteq P\}$.
- For all $i<n$,
  $$\text{Ext}_R^i(N,M)=0$$
  for some finitely generated R-module N such that $\text{Supp}(N)=\{P\in\text{Spec}(R)\mid I\subseteq P\}$.
- For all $i<n$,
  $$\text{Ext}_R^i(R/I,M)=0$$

As an immediate corollary, we see that

$$\begin{aligned}\text{depth}_I(M)&=\min\{n\in\mathbb{N}\mid\text{Ext}_R^n(N,M)\neq 0\text{ for all finitely generated }R\text{-module }N\}\\&=\min\left\{n\in\mathbb{N}\;\middle|\;\substack{\text{Ext}_R^n(N,M)\neq 0\text{ for some finitely generated }R\text{-module }N\text{ such that}\\ \text{Supp}(N)\subseteq\{P\in\text{Spec}(R)\mid I\subseteq P\}}\right\}\end{aligned}$$

and the most important one:

Corollary 5.4.2

Let R be a Noetherian commutative ring. Let I be an ideal of R. Let M be a finitely generated R-module such that $IM\neq M$. Then we have

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

Lemma 5.4.3

Let (R, m) be a Noetherian local ring. Let the following be an exact sequence of finitely generated R-modules.

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

Then the following are true.

- $\text{depth}(M_2) \geq \min\{\text{depth}(M_1), \text{depth}(M_3)\}$.
- $\text{depth}(M_3) \geq \min\{\text{depth}(M_1) - 1, \text{depth}(M_2)\}$.
- $\text{depth}(M_1) \geq \min\{\text{depth}(M_2), \text{depth}(M_3) + 1\}$.

Lemma 5.4.4

Let (R, m) be a Noetherian local ring. Let $M \neq \{0\}$ be a finitely generated R-module. Let $x \in R$ be an M-regular element. Then we have

$$\text{depth}(M/xM) = \text{depth}(M) - 1$$

Corollary 5.4.5

Let (R, m) be a Noetherian local ring. Let $M \neq \{0\}$ be a finitely generated R-module. Let $x_1, \dots, x_r$ be an M-regular sequence of length $r < \text{depth}(M)$. Then $x_1, \dots, x_r$ can be extended to an M-regular sequence of length $\text{depth}(M)$.

5.5 Further Results on Depth

Theorem 5.5.1: Serre's Criterion for Normality

Let R be a Noetherian integral domain. Suppose that for every $P \in \text{Spec}(R)$ such that $\text{ht}(P) = 1$, R_P is a DVR. Then R is normal if and only if for every $P \in \text{Spec}(R)$ such that $\text{ht}(P) \geq 2$, $\text{depth}(R_P) \geq 2$.

6 Homological Dimension Theory

6.1 Injective and Projective Dimension

Definition 6.1.1: Injective Dimension

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

$$\text{id}_R(M) = \min\{n \in \mathbb{N} \mid \text{there is an injective resolution of } M \text{ with } n \text{ terms}\}$$

Proposition 6.1.2

Let R be a commutative ring. Let M be an R-module. Then the following are equivalent.

- M has an injective resolution of length $\leq d \in \mathbb{N}$.
- $\text{Ext}_R^{d+1}(N, M) = 0$ for all R-modules N.
- $\text{Ext}_R^{d+1}(R/P, M) = 0$ for all $P \in \text{Spec}(R)$.

It follows that

$$\begin{aligned} \text{id}_R(M) &= \min\{d \in \mathbb{N} \mid \text{Ext}_R^{d+1}(N, M) = 0 \text{ for all } R\text{-modules } N\} \\ &= \min\{d \in \mathbb{N} \mid \text{Ext}_R^{d+1}(R/P, M) = 0 \text{ for all } P \in \text{Spec}(R)\} \end{aligned}$$

Definition 6.1.3: Projective Dimension

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

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

Proposition 6.1.4

Let R be a commutative ring. Let M be an R-module. Then M has a projective resolution of length $\leq d \in \mathbb{N}$ if and only if $\text{Ext}_R^{d+1}(M, N) = 0$ for all R-modules N.

It follows that

$$\text{pd}_R(M) = \min\{d \in \mathbb{N} \mid \text{Ext}_R^{d+1}(M, N) = 0 \text{ for all } R\text{-modules } N\}$$

6.2 Global Dimensions

Definition 6.2.1: Global Dimension

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

$$\text{gl dim}(R) = \sup\{\text{pd}(M) \mid M \in {}_R\mathbf{Mod}\}$$

Proposition 6.2.2

Let R be a commutative ring. Then the following numbers are equal.

- $\text{gl dim}(R) = \sup\{\text{pd}(M) \mid M \in {}_R\mathbf{Mod}\}$.
- $\sup\{\text{id}(M) \mid M \in {}_R\mathbf{Mod}\}$
- $\sup\{\text{pd}(R/I) \mid I \text{ is an ideal of } R\}$
- $\sup\{d \in \mathbb{N} \mid \text{Ext}_R^{d+1}(M, N) = 0 \text{ for some } M, N \in {}_R\mathbf{Mod}\}$

6.3 The Auslander-Buchsbaum Formula

Theorem 6.3.1: 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
$$\text{pd}_R(M) + \text{depth}_m(M) = \text{depth}_m(R)$$

Theorem 6.3.2: Ischebeck's Theorem

Let (R, m) be a Noetherian local ring. Let M, N be non-zero finitely generated R-modules. Then we have
$$\text{Ext}^i_R(N, M) = 0$$
for all $0 \leq i \leq \text{depth}_m(M) - \dim(N)$.

Proposition 6.3.3

Let (R, m) be a Noetherian local ring. Let M be a finitely generated R-module. Let $P \in \text{Ass}(M)$. Then we have
$$\text{depth}_m(M) \leq \dim\left(\frac{R}{P}\right)$$

Proposition 6.3.4

Let (R, m) be a Noetherian local ring. Then we have
$$\text{depth}_m(R) = \text{depth}_{\widehat{m}}(\widehat{R})$$

6.4 Hilbert's Syzygy Theorem

Lemma 6.4.1: Hyperplane Section Principle

Let R be a commutative ring. Let M be a finitely generated R-module. Let $x \in R$. Denote $\pi : M \to M/xM$ the quotient map. Suppose that one of the following conditions hold.

- R is a graded ring, M is a graded R-module and $x \in R$ has homogeneous degree > 0.
- R is a local ring with unique maximal ideal m and $x \in m$.

Let $Q_\bullet \to M/xM$ be a free resolution. Then there exists a free resolution $P_\bullet \to M$ of M together with a chain map $P_\bullet \to Q_\bullet$ such that $\text{rank}(H_k(P_\bullet)) = \text{rank}(H_k(Q_\bullet))$. In the graded case, the graded pieces of the resolutions have the same degrees.

Theorem 6.4.2: Hilbert's Syzygy Theorem

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

7 Regular Local Rings

7.1 Basic Definitions

Definition 7.1.1: Regular Local Rings

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

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

Proposition 7.1.2

Let (R,m) be a Noetherian local ring of dimension d. Then the following are equivalent.
- R is a regular local ring.
- $\text{gr}_m(R)$ is isomorphic to $k[x_1,\dots,x_d]$ as a graded ring.
- m is generated by d elements.

Lemma 7.1.3

Let R be regular local ring. Then R is an integral domain.

Lemma 7.1.4

Let R be commutative ring. Then R is a regular local ring of dimension 1 if and only if R is a DVR.

Proof. We have seen that if R is a DVR, then R is a regular local ring of dimension 1. $\square$

Lemma 7.1.5

Let R be a Noetherian commutative ring. Then the following are true.
- R is a regular local ring if and only if $R[x]$ is a regular local ring.
- Suppose that R is local. Then R is a regular local ring if and only if $\widehat{R}$ is a regular local ring.

7.2 Regular System of Parameters

Definition 7.2.1: Regular System of Parameters

Let (R,m) be a regular local ring. A regular system of parameters is a system of parameters of R that generate m.

Proposition 7.2.2

Let (R,m) be a regular local ring. Then any regular system of parameters is a regular sequence.

Proposition 7.2.3

Let (R,m) be a regular local ring of dimension $\dim(R) = d$. Let $x_1,\dots,x_i \in m$ be elements in m. Then the following are equivalent.
- The sequence $x_1,\dots,x_i$ can be extended to a regular system of parameters for R.
- $[x_1],\dots,[x_i]$ are linearly independent in $\frac{m}{m^2}$.

- $\frac{R}{(x_1,\dots,x_i)}$ is a regular local ring of dimension $d-i$.

Proposition 7.2.4

Let (R,m) be a regular local ring of dimension n. Suppose that $x_1,\dots,x_n$ is a regular sequence of parameters for R. Then the set

$$\{x_1^{k_1}\cdots x_n^{k_n} \mid k_1+\cdots+k_n=d\}$$

forms a basis for the vector space m^d/m^{d+1} over R/m. In particular, we have

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

Corollary 7.2.5

Let (R,m) be a regular local ring of dimension n. Then the set

$$\{x_1^{k_1}\cdots x_n^{k_n} \mid k_1+\cdots+k_n\leq d\}$$

forms a basis for the vector space R/m^{d+1} over R/m. In particular, we have

$$l_{R/m}\left(\frac{R}{m^{d+1}}\right)=\binom{d+n}{d}$$

7.3 Characterization Using Homological Dimensions

Proposition 7.3.1

Let R be a local ring. Then R is a regular local ring if and only if $\text{gl}\dim(R)<\infty$.

Corollary 7.3.2

Let R be a regular local ring. Let $P\in\text{Spec}(R)$. Then R_P is a regular local ring.

Theorem 7.3.3: Auslander–Buchsbaum Theorem

Let R be a regular local ring. Then R is a UFD.

7.4 Regular Rings

8 Two Important Rings Through the Koszul Complex

8.1 Cohen-Macaulay for Noetherian Local Rings

Let R be a Noetherian local ring. Recall that R is a regular local ring if its maximal ideal is generated by $\dim(R)$ elements. IN this case, the sequence of elements generating the maximal ideal is called a regular system of parameters. It is in general not true that they form a m-regular sequence.

Recall that $\dim(M) = \dim(R/\text{Ann}(M))$.

Definition 8.1.1: Cohen-Macaulay Modules over Noetherain Local Rings

Let (R, m) be a Noetherian local ring. Let M be a non-zero finitely generated R-module. We say that M is Cohen-Macaulay if

$$\dim(M) = \text{depth}(M)$$

By convention $M = 0$ is also a Cohen-Macaulay module.

In the case that $M = R$, we say that R is a Cohen-Macaulay ring if

$$\dim(R) = \text{depth}(R)$$

In general, we know that $\text{depth}(R) \leq \dim(R)$ because every regular sequence can be extended to a system of parameters, but there is no guarantee that the extended sequence is then a regular sequence. The condition that $\dim(R) = \text{depth}(R)$ then refers to the existence of a regular sequence that is also a system of parameters.

Proposition 8.1.2

Let (R, m) be a Cohen-Macaulay ring. Then every system of parameters of R is a regular sequence.

This means that system of parameters in a Cohen-Macaulay ring coincides with maximal regular sequences.

Proposition 8.1.3

Let (R, m) be a Noetherian local ring. Let M be Cohen-Macaulay R-module. Let $P \in \text{Ass}(M)$. Then we have

$$\dim(M) = \text{depth}(M) = \dim\left(\frac{R}{P}\right)$$

Moreover, M has no embedded associated primes (every associated prime is minimal).

Proposition 8.1.4

Let (R, m) be a Noetherian local ring. Let M be a finitely generated R-module. Let $x_1, \dots, x_r$ be an M-regular sequence. Then M is Cohen-Macaulay if and only if $M/(x_1, \dots, x_r)M$ is Cohen-Macaulay.

Proposition 8.1.5

Let (R, m) be a Noetherian local ring. Let M be a Cohen-Macaulay R-module. Let $P \in \text{Spec}(R)$. Then the following are true.

- M_P is a Cohen-Macaulay R_P-module.
- $\text{depth}_P(M) = \text{depth}_{PR_P}(M_P)$.

Lemma 8.1.6

Let R be a regular local ring. Then R is a Cohen-Macaulay ring.

Proposition 8.1.7

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

- R is Cohen-Macaulay if and only if $\widehat{R}$ is Cohen-Macaulay.
- R is Cohen-Macaulay if and only if $R[x]$ is Cohen-Macaulay.

8.2 Cohen-Macaulay for General Noetherian Rings

Definition 8.2.1: Cohen-Macaulay Modules

Let R be a Noetherian commutative ring. Let M be an R-module. We say that M is a Cohen-Macaulay if for all maximal ideals $m \in \text{Supp}(M)$, M_m is Cohen-Macaulay.

Proposition 8.2.2

Let R be a commutative ring. Then the following are true.

- R is Cohen-Macaulay if and only if $\widehat{R}$ is Cohen-Macaulay.
- R is Cohen-Macaulay if and only if $R[x]$ is Cohen-Macaulay.

Definition 8.2.3: Unmixed Ideals

Let R be a Noetherian commutative ring. Let $I \subseteq R$ be a proper ideal. We say that I is unmixed if for any prime divisor $P \in \text{Spec}(R)$ of I, the height $\text{ht}(P)$ is constant.

Lemma 8.2.4

Let R be a Noetherian commutative ring. Let $I \subseteq R$ be a proper ideal. Then I is unmixed if and only if I has no embedded associated primes.

Theorem 8.2.5: The Unmixedness Theorem

Let R be a Noetherian commutative ring. Then R is Cohen-Macaulay if and only if for every $r \geq 0$, every ideal I generated by r elements such that $\text{ht}(I) = r$ is unmixed.

8.3 Gorenstein Rings

Definition 8.3.1: Gorenstein Rings

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

9 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.

9.1 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 9.1.1: 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 9.1.2

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 9.1.3

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 9.1.4

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 9.1.5

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. □

9.2 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 9.2.1: 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 $\ker(g) = \mathrm{im}(f)$. It is enough to show that

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

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

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

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 $\mathrm{im}(u) = \ker(v)$. Materials Referenced: [**?**], [**?**] □

Theorem 9.2.2: 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 $\operatorname{im}(\delta) = \ker(f)$. Notice that to prove the exactness of the sequence in question, we just have to show the exactness of the following sequence (by **??**):

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

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

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

and further using $\text{Der}_A(B, N) \cong \operatorname{Hom}_B(\Omega^1_{B/A}, N)$ (by 9.1.2), transform into

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

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 $\phi \in \text{Der}_A(B/I, N)$ 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 $\text{Der}_A(B, N)$ to $\operatorname{Hom}_B(I, N)$ is given just by restricting $\psi \in \text{Der}_A(B, N)$ 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 $\text{Der}_A(B, N)$ that is identically 0 on I.

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

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 9.2.2, we see that

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

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 $1 \le i \le r$.

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 9.2.2) 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 $\mathrm{im}(A \twoheadrightarrow B \to C) = \mathrm{im}(B \to C)$, 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 [**?**].

9.3 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 9.3.1

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 9.3.2

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 9.3.1, 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 9.2.1, 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 9.3.3

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 9.3.1. 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 **??**.

10 The Picard Group of an Integral Domain

10.1 The Picard Group

Definition 10.1.1: 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 10.1.2

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