

Commutative Algebra 2

Labix

May 15, 2025

Abstract

Contents

1	Results from Homological Algebra	3
1.1	Inverse Systems	3
1.2	Projective and Injective Modules	3
1.3	Flat Modules	4
1.4	Finitely Presented Modules	4
1.5	Socle of a Module	5
2	Filtrations	6
2.1	Filtrations and Stable Filtrations	6
2.2	The I-Adic Filtration	6
3	Completions	8
3.1	General Completion Methods	8
3.2	A Topology on Completion	8
3.3	I-Adic Completion of a Module	9
3.4	I-Adic Completion of a Ring	10
3.5	Hensel's Lemma	11
4	More on Dimension Theory	12
4.1	The Hilbert Series of a General Graded Module	12
4.2	The Hilbert Series of the Associated Graded Module	16
4.3	System of Parameters and Its Minimal Size	17
4.4	The Fundamental Theorem of Dimension Theory	18
5	Regular Sequences	21
5.1	Regular Sequences	21
5.2	Relation to the Koszul Complex	21
5.3	The Depth of a Module	22
5.4	Depth and the Vanishing of Ext	23
5.5	Further Results on Depth	24
6	Homological Dimension Theory	25
6.1	Injective and Projective Dimension	25
6.2	Global Dimensions	25
6.3	The Auslander-Buchsbaum Formula	25
6.4	Hilbert's Syzygy Theorem	26
7	Regular Local Rings	27
7.1	Basic Definitions	27
7.2	Regular System of Parameters	27
7.3	Characterization Using Homological Dimensions	28
7.4	Regular Rings	28
8	Three Important Rings	29
8.1	Cohen-Macaulay for Noetherian Local Rings	29
8.2	Cohen-Macaulay for General Noetherian Rings	30
8.3	Gorenstein Rings	30
8.4	Complete Intersection Rings	30
9	Kähler Differentials	31
9.1	Kähler Differentials	31
9.2	Characterization for Separability	37
10	The Picard Group of an Integral Domain	39
10.1	The Picard Group	39

1 Results from Homological Algebra

1.1 Inverse Systems

Proposition 1.1.1 Left Exactness of the Inverse Limit Functor

Definition 1.1.2 (The Mittag-Leffler Condition)

Lemma 1.1.3 Surjective maps imply Mittag-Leffler

Proposition 1.1.4 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 $g : P \rightarrow M$, there exists a module homomorphism $h : P \rightarrow N$ such that the following diagram commutes:

$$\begin{array}{ccc} & N & \\ \nearrow \exists h & \downarrow f & \\ P & \xrightarrow{g} & M \end{array}$$

- $P \oplus Q$ 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.

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

$$\begin{array}{ccc} N & & \\ \downarrow f & \searrow g & \\ M & \dashrightarrow \exists h & I \end{array}$$

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

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

is exact.

Definition 1.3.3 (Flat Homomorphism) Let R, S be rings. Let $\varphi : R \rightarrow S$ 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 is 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.

1.5 Socle of a Module

Definition 1.5.1 (Socle)

Let (R, m) be a local ring. Let M be an R -module. Define the socle of M to be

$$\text{Socle}(M) = \{x \in M \mid mx = 0\}$$

Lemma 1.5.2

Let (R, m) be a local ring. Let M be an R -module. Then there is an isomorphism of R -modules

$$\text{Socle}(M) = \text{Hom}_R(R/m, M)$$

given by $f \mapsto f(1)$.

Proposition 1.5.3

Let (R, m) be an Artinian local ring. Then $\text{Socle}(R) = R/m$ if and only if R is an injective R -module.

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 filtration

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

is precisely the graded ring

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

associated to the commutative ring R .

2.2 The I-Adic Filtration

Definition 2.2.1 (I-Adic Filtration) Let R be a commutative ring. Let I be an ideal of R . Define the I -adic filtration of R to be the filtration

$$M \supseteq IM \supseteq I^2 M \supseteq \cdots \supseteq I^n M \supseteq \cdots$$

Theorem 2.2.2 (Artin-Rees Lemma)

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

Let $x \in I^{n-c}(I^c M \cap N)$. Then clearly $x \in I^c M \cap N \subseteq N$ and $x \in I^{n-c} I^c M = I^n M$. Thus $I^{n-c}(I^c M \cap N) \subseteq I^n M \cap N$.

Now suppose that $I = (a_1, \dots, a_r)$ and $M = (m_1, \dots, m_s)$. Then I^n is generated by $\{a_1^{n_1} \cdots a_r^{n_r} \mid n_1 + \cdots + n_r = n\}$, and for any $m \in M$, there exists $f_i \in R[x_1, \dots, x_r]$ homoge-

neous such that $m = \sum_{i=1}^s f_i(a_1, \dots, a_r)m_i$. Define

$$J_n = \left\{ (f_1, \dots, f_s) \in k[x_1, \dots, x_r]^s \mid f_i \text{ homogeneous of degree } n \text{ and } \sum_{i=1}^s f_i(a_1, \dots, a_r)m_i \in N \right\}$$

Let $J = \sum_{i=0}^{\infty} J_i$. Since R is Noetherian, $R[x_1, \dots, x_r]$ is Noetherian and so the $R[x_1, \dots, x_r]$ -module J is finitely generated by say u_1, \dots, u_t . Suppose that u_j is homogeneous of degree d_j .

For any $x \in I^M \cap N$, write $x = \sum_{i=1}^s f_i(a_1, \dots, a_r)m_i$ for some $f_i \in R[x_1, \dots, x_r]$ homogeneous of degree n . Then $(f_1, \dots, f_s) \in J_n$. Since u_1, \dots, u_t generates J , we have that

$$(f_1, \dots, f_s) = \sum_{j=1}^t p_j u_j$$

for some $p_j \in R[x_1, \dots, x_r]$. For each $1 \leq i \leq r$, f_i is homogeneous of degree n . Hence $\sum_{j=1}^t p_j u_{j,i}$ is also homogeneous of degree n . Hence p_j must be homogeneous of degree $n - d_j$. Now we have

$$\begin{aligned} x &= \sum_{i=1}^s f_i(a_1, \dots, a_r)m_i \\ &= \sum_{i=1}^s p_j(a_1, \dots, a_r) \sum_{j=1}^t u_{j,i}(a_1, \dots, a_r)m_i \\ &= \sum_{j=1}^t p_j(a_1, \dots, a_r) \sum_{i=1}^s u_{j,i}(a_1, \dots, a_r)m_i \end{aligned}$$

and $\sum_{i=1}^s u_{j,i}(a_1, \dots, a_r)m_i \in I^{d_j}M \cap N$. When $n > c = \max\{d_j \mid 1 \leq j \leq t\}$, we have $p_j(a_1, \dots, a_r) \in I^{n-d_j} = I^{n-c}I^{c-d_j}$, and so $x \in I^{n-c}(I^cM \cap N)$. ■

Theorem 2.2.3 (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 $N = m^n \cap N$ for some $n \in \mathbb{N}$. By the Artin-Rees lemma, we have

$$N = m^n \cap N = m^{n-c}(m^c \cap N) \subseteq mN$$

for some $c \in \mathbb{N}$. Hence $N = mN$. 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 $M \rightarrow \frac{M}{M_i}$, which descends to a well defined map $\frac{M}{M_{i+1}} \rightarrow \frac{M}{M_i}$.

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 $M \rightarrow \widehat{M}$ 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 .

Proposition 3.1.4

Let R be a commutative ring. Let M be an R -module. Let $\{M_n \mid n \in \mathbb{N}\}$ be a descending filtration of R -submodules of M . Denote $\widehat{M_n}$ the completion of M_n with respect to the filtration $\{M_k \mid k \geq n\}$. Then induced map by the universal property induces an isomorphism

$$\frac{M}{M_n} \cong \frac{\widehat{M}}{\widehat{M_n}}$$

Definition 3.1.5 (Complete Modules)

Let R be a commutative ring. Let M be an R -module. Let $\{M_n \mid n \in \mathbb{N}\}$ be a descending filtration of R -submodules of M . We say that M is complete with respect to the filtration if there is an isomorphism

$$M \cong \widehat{M}$$

induced by the universal property of completion.

Proposition 3.1.6

Let R be a commutative ring. Let M be an R -module. Let $\{M_n \mid n \in \mathbb{N}\}$ be a descending filtration of R -submodules of M . Then \widehat{M} is complete with respect to the filtration $\{\widehat{M_n} \mid n \in \mathbb{N}\}$.

3.2 A Topology on Completion

Definition 3.2.1 (Convergent Sequences)

Let R be a commutative ring. Let M be an R -module. Let $\{M_n \mid n \in \mathbb{N}\}$ be a descending filtration of R -submodules of M . Let $(x_n \in M_n)_{n \in \mathbb{N}}$ be a sequence of elements. We say that the sequence

converges to $x \in M$ if for all $n \in \mathbb{N}$, there exists $N \in \mathbb{N}$ such that

$$x_i - x \in M_n$$

for all $i \geq N$.

Definition 3.2.2 (Cauchy Sequences)

Let R be a commutative ring. Let M be an R -module. Let $\{M_n \mid n \in \mathbb{N}\}$ be a descending filtration of R -submodules of M . Let $(x_n \in M_n)_{n \in \mathbb{N}}$ be a sequence of elements. We say that the sequence converges to $x \in M$ if for all $n \in \mathbb{N}$, there exists $N \in \mathbb{N}$ such that

$$x_i - x_j \in M_n$$

for all $i, j \geq N$.

Lemma 3.2.3 Let R be a commutative ring. Let M be an R -module. Let $\{M_n \mid n \in \mathbb{N}\}$ be a descending filtration of R -submodules of M . Let $(x_n \in M_n)_{n \in \mathbb{N}}$ be a sequence of elements. If the sequence converges, then the sequence is Cauchy.

Proposition 3.2.4

Let R be a commutative ring. Let M be an R -module. Let $\{M_n \mid n \in \mathbb{N}\}$ be a descending filtration of R -submodules of M . Then M is complete with respect to the filtration if and only if every Cauchy sequence converges.

Definition 3.2.5 (Linear Topology)

3.3 I-Adic Completion of a Module

Definition 3.3.1 (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 I -adic filtration. Explicitly, it is given by the inverse limit

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

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 $I^n N$ induces that same completion.

Proposition 3.3.2 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 $I^n M \cap N$ 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. ■

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

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

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 3.3.3 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

$$0 \longrightarrow \widehat{M}_{1I} \longrightarrow \widehat{M}_{2I} \longrightarrow \widehat{M}_{3I} \longrightarrow 0$$

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

Proposition 3.3.4 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 3.3.5 (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 -adically complete if the induced map of inverse limits

$$M \rightarrow \widehat{M}_I$$

is an R -module isomorphism.

3.4 I-Adic Completion of a Ring

Example 3.4.1 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 3.4.2 Let R be a Noetherian commutative ring. Let I be an ideal of R . Then the following are true.

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

Proposition 3.4.3 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 3.4.4 (Complete Local Rings) Let (R, m) be a local ring. We say that R is a complete local ring if R is m -adically complete.

Lemma 3.4.5

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

Proof

Since R is Artinian, the descending chain $m \supseteq m^2 \supseteq \dots$ eventually terminates at $m^n = 0$ for some $n \in \mathbb{N}$. By definition of inverse limits, we have $\widehat{A} = A$. ■

Theorem 3.4.6 (Cohen Structure Theorem)

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

- If R contains a field $k \subset R$, there is an isomorphism

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

induced by the universal property of completion for some ideal $I \subseteq R$ and $n \in \mathbb{N}$.

- Otherwise, there exists a DVR D such that there is an isomorphism

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

for some ideal $I \subseteq R$ and $n \in \mathbb{N}$.

3.5 Hensel's Lemma

Theorem 3.5.1 (Hensel's Lemma)

Let (R, m) be a complete local ring. Let $\overline{(-)} : R[x] \rightarrow (R/m)[x]$ 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 $\overline{v} = h$.

Proof

Since g and h are coprime, by Bezout's lemma there exists $a, b \in R/m[x]$ such that $af + bg = 1$ where $\deg(a) < \deg(h)$ and $\deg(b) < \deg(g)$.

We induct on n . ■

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 $f \in k[x_1, \dots, x_n]$ 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 be a Noetherian commutative graded ring. Let R be generated by x_1, \dots, x_r where $\deg(x_i) = d_i$. Let M be a finitely generated graded R -module. Then there exists $f \in \mathbb{Z}[t]$ such that

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

Proof

We proceed by induction on r . When $r = 0$, then M is finitely generated R -module, and so for large enough $N \in \mathbb{N}$ we have $M_n = 0$ for $n > N$. In this case, $HS_M(t)$ is already in our desired form.

Suppose the result is true for $\leq r-1$. Consider multiplication by x_r and the induced exact sequence is gives:

$$0 \longrightarrow K_n \longrightarrow M_n \xrightarrow{x_r} M_{n+d_r} \longrightarrow L_{n+d_r} \longrightarrow 0$$

Here $K_n = \ker(x_r)$ and $L_{n+d_r} = \text{coker}(x_r)$. Notice that $K = \bigoplus_{n=0}^{\infty} K_n$ is a submodule of M and $L = \bigoplus_{n=0}^{\infty} L_n$ is a quotient of M , and so both are finitely generated R -modules. Moreover, since x_r annihilates, both K and L , they are $R_0[x_1, \dots, x_{r-1}]$ -modules. Hence the inductive hypothesis applies to both of them. Now by a property of length, we obtain

$$HF_K(n) - HF_M(n) + HF_M(n + d_r) - HF_L(n + d_r) = 0$$

Multiplying by t^{n+d_r} on both sides and summing over n , we obtain

$$t^{d_r} HS_K(t) - t^{d_r} HS_M(t) + HS_M(t) - \sum_{n=0}^{d_r-1} HF_M(n)t^n - HS_L(t) + \sum_{n=0}^{d_r-1} HF_L(n)t^n = 0$$

Write $g \in \mathbb{Z}[t]$ the polynomial $g(t) = \sum_{n=0}^{d_r-1} HF_M(n)t^n - \sum_{n=0}^{d_r-1} HF_L(n)t^n$. Then we simplify the above result into

$$(1 - t^{d_r})HS_M(t) + t^{d_r}HS_K(t) - HS_L(t) = g(t)$$

and hence

$$HS_M(t) = \frac{1}{1 - t^{d_r}} \left(g(t) - \frac{t^{d_r}k(t)}{\prod_{i=1}^{r-1} (1 - t^{d_i})} + \frac{l(t)}{\prod_{i=1}^{r-1} (1 - t^{d_i})} \right) = \frac{(1 - t^{d_r})g(t) - t^{d_r}k(t) + l(t)}{\prod_{i=1}^r (1 - t^{d_i})}$$

■

Example 4.1.7

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

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

Example 4.1.8

Let k be a field. Let $f \in k[x_1, \dots, x_d]$ be irreducible and homogeneous of degree r . Then the Hilbert series of $R = k[x_1, \dots, x_d]/(f)$ is given by

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

Proof

Consider the short exact sequence

$$0 \longrightarrow k[x_1, \dots, x_d]_{n-r} \xrightarrow{\times f} k[x_1, \dots, x_d]_n \longrightarrow R_n \longrightarrow 0$$

The Hilbert function of R is given by

$$HF_R(n) = HF_{k[x_1, \dots, x_d]}(n) - HF_{k[x_1, \dots, x_d]}(n - r)$$

Then we have that

$$t^{n-r} HF_R(n) = t^{-r} (t^n HF_{k[x_1, \dots, x_d]}(n)) + t^{n-r} HF_{k[x_1, \dots, x_d]}(n - r)$$

and summing over n gives

$$t^{-r} HS_R(t) = (t^{-r} + 1) HS_{k[x_1, \dots, x_d]}(t)$$

and simplifying gives our desired result. ■

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

$$\lim_{t \rightarrow 1} HS_M(t) < \infty$$

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

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

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 $d - 2$. ■

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

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

In fact, it is a graded $\mathrm{gr}_I(R)$ -module. When R is Noetherian, I is finitely generated, and so $\mathrm{gr}_I(R)$ is finitely generated by degree 1 elements (the images of the generators of I in I/I^2). Hence the Hilbert series for $\mathrm{gr}_I(M)$ as a $\mathrm{gr}_I(R)$ is in the form

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

by 4.1.6.

Definition 4.2.1 (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

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

This is the same as saying that

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

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 4.2.2 (Hilbert-Samuel Function) Let R be a Noetherian 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 $\mathbb{N} \rightarrow \mathbb{N}$. If we restrict the domain to $n > \deg(f)$ where $HS_{\mathrm{gr}_I(M)}(t) = \frac{f(t)}{(1-t)^{d_I(M)}}$ then χ_M^I is a polynomial in n .

Proposition 4.2.3 Let R be a commutative ring. Let I be an ideal of R . Let M be a finitely generated R -module. Then we have

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

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

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

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 4.2.4 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 4.2.5 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 4.2.6 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 $\chi_{M_3}^I$.

4.3 System of Parameters and Its Minimal Size

Definition 4.3.1 (Size of minimal Generators)

Let (R, m) be a Noetherian local ring. Let M be an R -module. Define

$$\delta(M) = \min\{r \in \mathbb{N} \mid l_R(M/(x_1, \dots, x_r)M) < \infty\}$$

Definition 4.3.2 (System of Parameters of a Module)

Let (R, m) be a Noetherian local ring. Let M be an R -module. A system of parameters is a sequence of $\delta(M)$ elements of $x_1, \dots, x_{\delta(M)} \in m$ that realizes the lower bound of $\delta(M)$, meaning that

$$l_R(M/(x_1, \dots, x_{\delta(M)})M) < \infty$$

Lemma 4.3.3 Let (R, m) be a Noetherian local ring such that $\delta(R) = r$. Then the following are true.

- 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.
- We have

$$\delta(R) = \min\{d \in \mathbb{N} \mid (x_1, \dots, x_r) \text{ is an } m \text{ primary ideal}\}$$

Lemma 4.3.4 Let R be a Noetherian local ring. Then R has a system of parameters.

Proposition 4.3.5 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

Lemma 4.4.1

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

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

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 $d(R) = \max\{d(R), d(R/(x))\}$. Assume for a contradiction that $d(R/(x)) = d(R)$. Then the leading coefficient of χ_R is equal to the leading coefficients of χ_R and $\chi_{R/(x)}$ by 4.2.6. But this implies that the leading coefficient of $\chi_{R/(x)}$ is 0, a contradiction. Hence $d(R/(x))$ is strictly less than $d(R)$, and so $d(R/(x)) \leq d(R) - 1$. ■

Theorem 4.4.2 (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

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

- 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

- $\dim(M) \leq d(M)$:

We induct on d . When $d(R) = 0$, then the Hilbert series is a polynomial which means that the Hilbert function is 0 for large enough n . By 4.2.3, we have that $\chi_M(n) = \chi_M(n+1)$ for large enough n , which means that $m^{n+1} = m^n$. By Nakayama's lemma, we have $m^n = 0$. Then R is Noetherian commutative ring with nilpotent maximal ideal. Hence R is Artinian and $\dim(R) = 0$.

Now suppose that $d(R) > 0$. If $\dim(R) = 0$ then we are done. If not, then let $P_0 \subset \cdots \subset P_r$ be a chain of prime ideals in R . Let $x \in P_1 \setminus P_0$. Then $[x] \in R/P_0$ is non-zero. Since R/P_0 is an integral domain, we can apply 4.4.1 to deduce that $d(R/(P_0 + (x))) \leq d(R/P_0) - 1$. By induction hypothesis, we have that

$$\dim(R/(P_0 + (x))) \leq d(R/(P_0 + (x))) \leq d(R/P_0) - 1$$

Also, by 4.2.6 we have that $d(R/P_0) \leq d(R)$ and so we now have $\dim(R/(P_0 + (x))) \leq d(R)$. Now $P_1 \subset \cdots \subset P_r$ is a strictly increasing chain of prime ideals containing P_0 and so by the correspondence theorem we have a strictly increasing chain of prime ideals of length $r - 1$ in $R/(P_0 + (x))$. Hence we have

$$r - 1 \leq \dim(R/(P_0 + (x))) \leq d(R/P_0) - 1 \leq d(R) - 1$$

Since this is true for all $r \leq \dim(R)$, we thus have $\dim(R) \leq d(R)$. For general R -modules, first note that since M is finitely generated, M has a disassembly. Let $0 = M_0 \subset \cdots \subset M_n = M$ be the disassembly of M . For each $1 \leq i \leq n$, consider the exact sequences

$$0 \longrightarrow M_{i-1} \longrightarrow M_i \longrightarrow \frac{M_i}{M_{i-1}} \cong \frac{R}{P_i} \longrightarrow 0$$

where $P_{i+1} \in \text{Spec}(R)$. By 4.2.6 we have that $d(M_i) = \max\{d(M_{i-1}), d(R/P_i) = \dim(R/P_i)\}$. Hence inductively we have that $d(M) = \max\{d(R/P) \mid P \in \text{Spec}(R)\}$. Together with 8.1.7 in Commutative Algebra 1 we conclude that

$$\dim(M) = \max\{\dim(R/P) \mid P \in \text{Ass}(M)\} \leq \max\{d(R/P) \mid P \in \{P_1, \dots, P_n\}\} = d(M)$$

since minimal primes over $\text{Ass}(M)$ is the same as minimal primes in the set $\{P_1, \dots, P_n\}$.

- $d(R) \leq \delta(R)$:

Let $I = (a_1, \dots, a_{\delta(R)})$ be an m -primary ideal of R . We have seen that R/I is an Artinian ring by 6.3.12 in Commutative Algebra 1. Since R/I is Noetherian and Artinian, it has a composition series and hence $l_{R/I}(R/I)$ has finite length. Now we know that $\text{gr}_I(R) = \frac{R/I[a_1, \dots, a_{\delta(R)}]}{J}$ where each generator has degree 1 and J is the relations between the generators. Then using the exact sequence

$$0 \longrightarrow J \longrightarrow R/I[a_1, \dots, a_n] \longrightarrow \text{gr}_I(R) \longrightarrow 0$$

and 4.2.6, we have that $d(R) \leq d(R/I[a_1, \dots, a_{\delta(R)}])$. By a slight generalization of 4.1.11, we have that the degree of the Hilbert polynomial of $R/I[a_1, \dots, a_n]$ is given by $\delta(R) - 1$ and so $d(R/I[a_1, \dots, a_{\delta(R)}]) = \delta(R)$. Hence $d(R) \leq \delta(R)$.

- $\delta(R) \leq \dim(R)$:

We induct on $\dim(R)$. If $\dim(R) = 0$, then R is Artinian and so m is nilpotent. Then we have $\sqrt{(0)} = \sqrt{m^n} = m$ and so (0) is m -primary. Hence $\delta(R) = 0$. So suppose that $\dim(R) > 0$. By 2.1.3 in Commutative Algebra 1, R has only finitely many minimal prime ideals. Let P_1, \dots, P_n be the list of all distinct minimal prime ideals of R . Since R is local and $\dim(R) > 0$, we have $P_i \subset m$ is a strict inclusion. I claim that $\bigcup_{i=1}^n P_i \subset m$ is a strict subset. Indeed if not, then $m \subseteq \bigcup_{i=1}^n P_i$ and prime avoidance implies that $m \subseteq P_i$, a contradiction. Hence there exists $0 \neq x \in m \setminus \bigcup_{i=1}^n P_i$.

Let $Q_0 \subset \cdots \subset Q_k$ be a strictly increasing chain of prime ideals in $R/(x)$. By the correspondence Q_0 corresponds to a prime ideal containing (x) . This means that the corresponding prime ideal of Q_0 in R cannot be any of the P_1, \dots, P_n and so is not a minimal prime ideal of R . This proves that $\dim(R/(x)) \leq \dim(R) - 1$. By induction hypothesis, we have that $\delta(R/(x)) \leq \dim(R/(x)) \leq \dim(R) - 1$. Then this means that there exists an $m/(x)$ -primary ideal $([x], \dots, [x_{\dim(R)-1}])$ of $R/(x)$. Then $(x_1, \dots, x_{\dim(R)-1}, x)$ is an m -primary ideal of R . Hence $\delta(R) \leq \dim(R)$. ■

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

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

Proof

The ideal IR_P in R_P is a subset of PR_P , and so is a primary ideal with $\sqrt{IR_P} = PR_P$. By the fundamental theorem of dimension theory, we have

$$\text{ht}_R(P) = \dim(R_P) = \delta(I) \leq n$$

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. ■

Proposition 4.4.5

Let (R, m) be a Noetherian local ring of dimension $\dim(R) = d$. Let $x_1, \dots, x_d \in m$ 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.

Proof

Let $P_0 \subset \dots \subset P_r$ be a maximal chain of prime ideals in $R/(x_1, \dots, x_i)$ lifted into R by the correspondence theorem. Then P_0 is a minimal prime over (x_1, \dots, x_i) since the chain is maximal. By Krull's height theorem, we have $\text{ht}_R(P_0) \leq i$. This means that we can extend the chain of prime ideals $P_0 \subset \dots \subset P_r$ downwards of at most i steps to obtain a chain of prime ideals in R . Since it may not be a maximal chain, we have

$$\text{ht}_R(P) + r \leq i + r = i + \dim(R/(x_1, \dots, x_i)) \leq \dim(R)$$

Hence $\dim(R/(x_1, \dots, x_i)) \leq \dim(R) - i$. On the other hand, let $P_0 \subset \dots \subset P_d$ be a maximal chain of prime ideals in R . Since R is a local ring with unique maximal ideal m , $(x_1, \dots, x_i) \subseteq m$. Hence there exists a smallest prime P_k in the maximal chain such that $(x_1, \dots, x_i) \subseteq P_k$. It is a minimal prime since the chain is maximal. Then again since the chain is maximal, we have $\text{ht}(P_k) = k$. By Krull's height theorem, we have $k \leq i$. The $P_k \subset \dots \subset P_d$ is a maximal chain but may not be the biggest of the chains in $R/(x_1, \dots, x_i)$. Hence $\dim(R/(x_1, \dots, x_i)) \geq \dim(R) - k \geq \dim(R) - i$. Combining the two inequalities gives the desired result.

Following the above, we have that $\dim(R/(x_1, \dots, x_d)) = 0$. Thus we have that $R/(x_1, \dots, x_d)$ is a Noetherian ring and has dimension 0. Hence $R/(x_1, \dots, x_r)$ is an Artinian ring. ■

Proposition 4.4.6 Let (R, m) be a local ring. Then we have

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

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 for all $0 \neq m \in M$, $xm \neq 0$.

Note that this is the same as saying the multiplication map $\phi_x : M \rightarrow M$ is injective, and in the case that $M = R$, that x is not a zero divisor.

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.

Corollary 5.1.5

Let (R, m) be a Noetherian local ring. If $x_1, \dots, x_n \in m$ is a regular sequence, then we have

$$\dim \left(\frac{R}{(x_1, \dots, x_n)} \right) = \dim(R) - n$$

Proof

By the above lemma, the regular sequence can be extended to a system of parameters, then by 4.4.5 we are done. ■

Idea: both system of parameters and regular sequences cuts down a variety by dimension, but regular sequences are doing more...

Definition 5.1.6 (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

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

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

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

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 $R^2 \rightarrow R$ 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 $R^2 \rightarrow R$ by $(1, 0) \mapsto x$ and $(0, 1) \mapsto y$.
- The second differential $R \rightarrow R^2$ 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 $p \geq 1$.

Proof

We induct on n . When $n = 1$, then x_1 being a non-zero divisor means that the multiplication by x_1 map is injective. Hence $H_1(x_1; M) = 0$. ■

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 . ■

Example 5.3.3 the 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 $i < n$,

$$\text{Ext}_R^i(R/I, M) = 0$$

Proposition 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

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

Proof ■

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 $\text{depth}(M)$.

Theorem 5.4.6 (Ischebeck's Theorem) Let (R, m) be a Noetherian local ring. Let M, N be non-zero finitely generated R -modules. Then we have

$$\text{Ext}_R^i(N, M) = 0$$

for all $0 \leq i \leq \text{depth}_m(M) - \dim(N)$.

Proposition 5.4.7 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 5.4.8 Let (R, m) be a Noetherian local ring. Then we have

$$\text{depth}_m(R) = \text{depth}_{\hat{m}}(\hat{R})$$

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

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

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 $\leq d \in \mathbb{N}$.
- $\mathrm{Ext}_R^{d+1}(N, M) = 0$ for all R -modules N .
- $\mathrm{Ext}_R^{d+1}(R/P, M) = 0$ for all $P \in \mathrm{Spec}(R)$.

It follows that

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

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

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

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 $\mathrm{Ext}_R^{d+1}(M, N) = 0$ for all R -modules N .

It follows that

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

6.2 Global Dimensions

Definition 6.2.1 (Global Dimension) Let R be a commutative ring. Define the global dimension of R to be

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

Proposition 6.2.2 Let R be a commutative ring. Then the following numbers are equal.

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

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 $\mathrm{pd}_R(M)$ is finite, then we have

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

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 $\pi : M \rightarrow M/xM$ 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 $Q_\bullet \rightarrow M/xM$ be a free resolution. Then there exists a free resolution $P_\bullet \rightarrow M$ of M together with a chain map $P_\bullet \rightarrow Q_\bullet$ 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. ■

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 \hat{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 Three Important Rings

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 Noetherian 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.

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

Proposition 8.1.2 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 8.1.3 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 8.1.4 Let (R, m) be a Noetherian local ring. Let M be a finitely generated R -module. Then every system of parameters is a maximal M -regular sequence.

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.
- $\text{depth}_P(M) = \text{depth}_{R_P}(M_P)$.

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 \hat{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 \hat{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)

Let R be a Noetherian local ring. We say that R is a Gorenstein ring if

$$\text{id}_R(R) < \infty$$

Proposition 8.3.2

Let R be a Noetherian local ring. Then the following are equivalent.

- R is Gorenstein.
- For all $i \neq \dim(R)$, $\text{Ext}_R^i(R/m, R) = 0$ and $\text{Ext}_R^{\dim(R)}(R/m, R) = R/m$.
- R is Cohen Macaulay and $\text{Ext}_R^{\dim(R)}(R/m, R) = R/m$.
- R is Cohen Macaulay and $\dim(\text{Socle}(R/(x_1, \dots, x_n))) = 1$ for any system of parameters x_1, \dots, x_n .
- R is Cohen Macaulay and $R/(x_1, \dots, x_n)$ is an injective $R/(x_1, \dots, x_n)$ -module.

Corollary 8.3.3 Let R be a regular local ring. Then R is Gorenstein.

8.4 Complete Intersection Rings

$$\text{Regular Local Rings} \subset \text{Complete Intersection Rings} \subset \text{Gorenstein Rings} \subset \text{Cohen-Macaulay Rings}$$

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)

Let A be a commutative ring. Let B be an A -algebra. The module of Kähler differentials is an B -module $\Omega_{B/A}^1$ together with an A -module homomorphism $d_{B/A} : B \rightarrow \Omega_{B/A}^1$ called the universal derivation such that the following universal property is satisfied: For any B -module M and any A -derivation $d : B \rightarrow M$, there exists a unique B -module homomorphism $\Omega_{B/A}^1 \rightarrow M$ such that the following diagram commutes:

$$\begin{array}{ccc} B & \xrightarrow{d_u} & \Omega_{B/A}^1 \\ & \searrow d & \downarrow \exists! \\ & & M \end{array}$$

Proposition 9.1.2

Let A be a commutative ring. Let 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 we have $F/R \cong \Omega_{B/A}^1$.

Proof

Clearly F/R is a B -module. Moreover, define $d : B \rightarrow F/R$ 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 $d(b_1b_2) + R = b_1d(b_2) + d(b_1)b_2 + R$, we have that b_1b_2 is mapped to $b_1d(b_2) + d(b_1)b_2 + R$.

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

It remains to show that $(F/R, d)$ has the universal property. Let M be a B -module and $d' : B \rightarrow M$ an A -derivation. Define a map $f : F \rightarrow M$ 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 is also unique since f is defined on the generators of F .

Finally we want to show that f projects to a map $\bar{f} : F/R \rightarrow M$. 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 $f : F \rightarrow M$ 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. ■

Proposition 9.1.3 Let A be a commutative ring. Let B be an A -algebra. Let $f : B \otimes_A B \rightarrow B$ denote the B -module homomorphism defined on generators by $b_1 \otimes b_2 \mapsto b_1b_2$. Then we have an isomorphism

$$\Omega_{B/A}^1 \cong \frac{\ker(f)}{\ker(f)^2}$$

Moreover, the universal derivation $d_{B/A} : B \rightarrow \frac{\ker(f)}{\ker(f)^2}$ in this case is given by

$$d_{B/A}(b) = 1 \otimes b - b \otimes 1 + I^2$$

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 $d : B \rightarrow I/I^2$ is an A -derivation.

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

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

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 $d' : B \rightarrow M$ an A -derivation. We want to find a unique $\tilde{\phi} : B \rightarrow M$ 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 $\phi : B \otimes B \rightarrow B \ltimes M$ (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

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

Thus we are done.

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

$$\begin{aligned} \phi((u_1 \otimes u_2) \cdot \phi(v_1 \otimes v_2)) &= (u_1 u_2, u_1 d'(u_2)) \cdot (v_1 v_2, v_1 d'(v_2)) \\ &= (u_1 u_2 v_1 v_2, u_1 u_2 v_1 d'(v_2) + v_1 v_2 u_1 d'(u_2)) \\ &= (u_1 v_1 u_2 v_2, u_1 v_1 d'(u_2 v_2)) \\ &= \phi(u_1 v_1 \otimes u_2 v_2) \end{aligned}$$

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

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

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

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: [?], [?], [?]

Lemma 9.1.4 Let A be a commutative ring. Let B be an A -algebra. Let M be a B -module. Then there is an isomorphism of B -modules

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

induced by the universal property of the module of Kähler differentials.

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

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

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

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

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

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

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

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

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

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.

Example 9.1.5 Let A be a commutative ring. Let $B = A[x_1, \dots, x_n]$. Then there is an isomorphism

$$\Omega_{B/A}^1 \cong \bigoplus_{i=1}^n B d(x_i)$$

Proof

Theorem 9.1.6 (First Exact Sequence)

Let A be a commutative ring. Let B, C be A -algebras and let $\varphi : B \rightarrow C$ be an A -algebra homomorphism. Then there is an exact sequence of C -modules:

$$\Omega_{B/A}^1 \otimes_B C \xrightarrow{d_{B/A}(b) \otimes c \mapsto cd_{C/A}(\varphi(b))} \Omega_{C/A}^1 \longrightarrow \Omega_{C/B}^1 \longrightarrow 0$$

where the second map is induced by the universal property.

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

$$0 \longrightarrow \text{Hom}_C(\Omega_{C/B}^1, N) \longrightarrow \text{Hom}_C(\Omega_{C/A}^1, N) \longrightarrow \text{Hom}_C(\Omega_{B/A}^1 \otimes_B C, N)$$

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

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

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 $\text{im}(u) = \ker(v)$. Materials Referenced: [?], [?] ■

Theorem 9.1.7 (Second Exact Sequence)

Let A be a commutative ring. Let B be an A -algebra. Let I be an ideal of B . Then there is an exact sequence of B/I -modules:

$$\frac{I}{I^2} \xrightarrow{b \mapsto d(b) \otimes 1} \Omega_{B/A}^1 \otimes_B \frac{B}{I} \longrightarrow \Omega_{(B/I)/A}^1 \longrightarrow 0$$

where the second map is given in the first exact sequence.

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 $d(b + I) \in \Omega_{C/A}^1$, just choose $d(b) \otimes 1 \in \Omega_{B/A}^1 \otimes_B C$. Then $f(d(b) \otimes 1) = d(b + I)$.

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

$$0 \longrightarrow \text{Hom}_C(\Omega_{C/A}^1, N) \longrightarrow \text{Hom}_C(\Omega_{B/A}^1 \otimes_B \frac{B}{I}, N) \longrightarrow \text{Hom}_C(I/I^2, N)$$

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

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

and further using $\operatorname{Der}_A(B, N) \cong \operatorname{Hom}_B(\Omega_{B/A}^1, N)$ (by 9.1.4), transform into

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

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 $\phi \in \operatorname{Der}_A(B/I, N)$ can be extended naturally to an A -linear derivation from B to N : just pre-compose it with the projection map $p : B \rightarrow B/I$. 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 $\operatorname{Der}_A(B, N)$ to $\operatorname{Hom}_B(I, N)$ is given just by restricting $\psi \in \operatorname{Der}_A(B, N)$ 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 $\operatorname{Der}_A(B, N)$ that is identically 0 on I .

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

Example 9.1.8 Let A be a commutative ring. Let $B = \frac{A[x_1, \dots, x_n]}{(f_1, \dots, f_r)}$. Then we have

$$\Omega_{B/A}^1 \cong \operatorname{coker}(J)$$

where J is the Jacobian matrix of f_1, \dots, f_r .

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 $\Omega_{B/A}^1 \otimes C \cong \bigoplus_{i=1}^n C dx_i$. By the second exact sequence 9.1.7, we see that

$$\Omega_{C/A}^1 \cong \operatorname{coker} \left(\frac{I}{I^2} \rightarrow \bigoplus_{i=1}^n C dx_i \right)$$

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

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

This is a map from a free module of rank r to a free module of rank n . So we can write this in an $n \times r$ matrix. Since the map $I/I^2 \rightarrow \bigoplus_{i=1}^n C dx_i$ sends f_i to $d(f_i) = \sum_{k=1}^n \frac{\partial f_i}{\partial x_k} dx_k$ (by second exact sequence 9.1.7) and e_i is sent f_i , we have that J is the matrix

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

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

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

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

Proposition 9.1.9

Let A be a commutative ring. Let B be an A -algebra. Then the following are true.

- Let S be a multiplicative subset of A . Then there is an isomorphism of B -modules

$$S^{-1}\Omega_{B/A}^1 \cong \Omega_{S^{-1}B/A}^1$$

induced by the universal property of the module.

- Let C be an A -algebra. Then there is an isomorphism of B -modules

$$\Omega_{B/A}^1 \otimes_A C \cong \Omega_{B \otimes_A C/A}^1$$

induced by the universal property of the module.

9.2 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 9.2.1 Let L/K be a finite field extension and $\Omega_{L/K}^1$ the module of Kähler Differentials. Let $f(b) = c_0 + c_1b + \cdots + c_nb^n \in L$ 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

$$f'(b) = d(c_0) + bd(c_1) + c_1d(b) + \cdots + b^nd(c_n) + c_nd(b^n)$$

Since each $c_0, \dots, c_n \in K$, we obtain $f'(b) = c_1d(b) + \cdots + c_n \cdot nb^{n-1}d(b)$. 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 9.2.2 Let K be a field and L/K a finite field extension. Then L/K is separable if and only if $\Omega_{L/K}^1 = 0$.

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 9.2.1, 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 $\Omega_{L/K}^1 = 0$. Since L is a field, and $f'(b) \neq 0$, we must have $d(b) = 0$ for all $b \in L$. This means that $\Omega_{L/K}^1 = 0$.

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

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

Since $p'(t) = 0$, we have that $\Omega_{L/E}^1 \cong L \neq 0$. By the first exact sequence 9.1.6, we have that $\Omega_{L/K}^1$ maps surjectively onto $\Omega_{L/E}^1 \neq 0$ which proves that $\Omega_{L/K}^1$ 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 $F : \text{Algebra}_R \rightarrow \text{Mod}_T$ 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 -algebra 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 9.2.3 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 9.2.1. 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.