

Review basic notions

- radical, reduced ring
- prime ideal, primary ideal = $R/\mathfrak{q}$ i.e. $x \notin \mathfrak{q}, xy \in \mathfrak{q} \Rightarrow y^n \in \mathfrak{q}$ for some n
all zero divisors in $R/\mathfrak{q}$ are nilpotent
- $\text{Spec}(R)$, $\text{Max}(R) = \Omega(R)$ maximal spectrum with Zariski topology
- localization
- finite R -modules, finite R -algebras, finitely generated R -algebras

Lemma: $P_1, P_2, P_3, \dots, P_m$ ideals of R , $m \geq 2$, $P_3, \dots, P_m$ prime ideals
 I = an ideal of R

Then $I \subseteq \bigcup_{i=1}^m P_i \Leftrightarrow I \subseteq P_i$ for some i

Pf: $m=2$. Suppose $I \not\subseteq P_1$ and $I \not\subseteq P_2 \Rightarrow \exists x_1, x_2 \in I, x_1 \notin P_1, x_2 \notin P_2$
 $\Rightarrow x_1 + x_2 \notin P_1$ and $x_1 + x_2 \notin P_2$, contradiction $\Rightarrow x_1 \in P_2, x_2 \in P_1$

Induction: True for $m=r$. Suppose: $I \subseteq P_1 \cup P_2 \cup \dots \cup P_r \cup P_{r+1}$, $I \not\subseteq P_i \forall i$
no inclusion relation $P_i \subseteq P_j \forall i \neq j$.

Know $I \cdot P_1 \dots P_r \not\subseteq P_{r+1}$ (since P_{r+1} is prime)

Take $x \in I \cdot P_1 \dots P_r, x \notin P_{r+1}$

May assume: $I \not\subseteq P_1 \cup \dots \cup P_r$, by induction.

$\Rightarrow \exists y \in I \cdot (P_1 \cup \dots \cup P_r) \Rightarrow y \in P_{r+1}$

Consider $x+y$: $x+y \notin (P_1 \cup \dots \cup P_r) \Rightarrow x+y \in P_{r+1}$

However $x \notin P_{r+1}$ and $y \in P_{r+1} \Rightarrow x+y \notin P_{r+1}$. Contradiction!

QED.

Lemma: $I_1, \dots, I_r$ ideals of R s.t. $I_i + I_j = R \forall i \neq j$

Then $I_1 \cap \dots \cap I_r = I_1 \dots I_r$ and $R/\bigcap I_j \cong (R/I_1) \times \dots \times (R/I_r)$

Proof: Induction: suffices to show: $(I_1 \cap \dots \cap I_{r-1}) + I_r = R$
for $r \geq 3$

$r=2$:
 $I_1 + I_2 = R$

Write $1 = x_i + y_i, x_i \in I_i, y_i \in I_r, i=1, \dots, r-1$

easy. $1 = \prod_{i=1}^{r-1} (x_i + y_i) \equiv \prod_{i=1}^{r-1} x_i \pmod{I_r} \Rightarrow (I_1 \cap \dots \cap I_{r-1}) + I_r = R$

Notation: $M_{\mathfrak{p}}$ = localization of an R -module at a prime ideal $\mathfrak{p}$ of R

- exactness property of localization $M \mapsto S^{-1}M = M \otimes_R S^{-1}R$
- M : R -module $\rightsquigarrow M = (0) \Leftrightarrow M_{\mathfrak{p}} = (0) \quad \forall \mathfrak{p} \in \text{Spec}(R)$
- finitely presented modules
- R -algebras of finite presentation

Elementary properties of finitely presented modules

Prop: M : fin. pres. R -module $0 \rightarrow K \rightarrow N \rightarrow M \rightarrow 0$ short exact

N : fin. generated R -module

Then K is fin. gen.

Pf:
$$\begin{array}{ccccccc} 0 \rightarrow K' & \rightarrow & L_1 & \rightarrow & M & \rightarrow & 0 \\ & & \downarrow \beta & & \downarrow \alpha & & \parallel \\ 0 \rightarrow K & \rightarrow & N & \rightarrow & M & \rightarrow & 0 \end{array}$$

$\nwarrow$ finite free

$K' = \text{fin. } R\text{-module}$

$$\rightsquigarrow 0 \rightarrow \text{coker}(\beta) \xrightarrow{\sim} \text{coker}(\alpha) \rightsquigarrow 0 \rightarrow K' \rightarrow K \rightarrow K/K' \rightarrow 0$$

$\uparrow$ finite R -module $\uparrow$ finite R -module $\uparrow$ finite R -module

QED

Prop: M, N : R -modules. S : flat R -alg

$$\rightsquigarrow \text{Hom}_R(M, N) \otimes_R S \xrightarrow{\lambda} \text{Hom}_S(M \otimes_R S, N \otimes_R S)$$

Then 1) α is injective if M is a finite R -module

2) α is an isom. if M is a fin. presented R -module

Pf: $L_1 \rightarrow L_0 \rightarrow M$ exact, L_0 : finite free R -module, L_1 : free R -module

finite free if M is of fin. pres

$$\rightsquigarrow 0 \rightarrow \text{Hom}_R(M, N) \otimes_R S \rightarrow \text{Hom}_R(L_0, N) \otimes_R S \rightarrow \text{Hom}_R(L_1, N) \otimes_R S$$

$$\downarrow \lambda \quad \downarrow \sim \quad \downarrow \lambda'$$

$$0 \rightarrow \text{Hom}_S(M \otimes_R S, N \otimes_R S) \rightarrow \text{Hom}_S(L_0 \otimes_R S, N \otimes_R S) \rightarrow \text{Hom}_S(L_1 \otimes_R S, N \otimes_R S)$$

+ λ' is an isom when M is of finite presentation.

QED

- Krull dimension
- Noetherian rings, Noetherian modules over a commutative ring
- Artinian rings

↪ "if" part trivial

Prop: A commutative ring R is Artinian iff $\text{length}_A(A) < \infty$

Proof 1) A has only a finite number of max. ideals $\xrightarrow{\text{length as an } A\text{-module}}$

Otherwise: Say $P_1, \dots, P_n, \dots$ is an infinite sequence of distinct max. ideals

$$\leadsto P_1 \not\supseteq P_1 \cdot P_2 \not\supseteq P_1 \cdot P_2 \cdot P_3 \not\supseteq \dots \quad \text{contradiction}$$

2) Let $P_1, \dots, P_n$ be the max. ideals of R

$$\text{Let } I = P_1 \cdot \dots \cdot P_n \quad I \supseteq I^2 \supseteq \dots \supseteq I^m \supseteq \dots \text{ stops}$$

$$\leadsto \exists N \text{ s.t. } I^N = I^{N+1} = \dots$$

$$\text{Let } J := (0 : I^N) \leadsto (J : I) = ((0 : I^N) : I) = (0 : I^{N+1}) = J$$

Claim: $J = R$

Otherwise, let J' be a minimal element of $\{J_i : J_i \text{ ideal of } R, J_i \not\supseteq J\}$

$$\Rightarrow J' = J + Rx \quad \forall x \in J' \setminus J$$

Note $J + Ix \neq J'$ by Nakayama's lemma, because $I \subseteq \text{rad}(R)$

minimality of $J' \Rightarrow J + Ix = J \quad \forall x \in J' \setminus J$

$$\text{i.e. } J' \cdot I \subseteq J \Rightarrow J' \subseteq (J : I) = J$$

Conclusion: $I^N = 0$

3) Use $I^N = 0$ to get a descending finite filtration of R ,
s.t. each graded piece is $\cong R/P_i$

QED

Lemma: $I \subseteq R$ an ideal, $b \in R$. If both $I + bR$ and $(I : bR)$ are finitely generated ideals, so is I .

Sublemma: Let $I' \subseteq I$ be ideals of R , $b \in R$. If $I' + bR = I + bR$, then $I = I' + (bR) \cap I$

Proof of Lemma: Take a f.g. ideal $I' \subseteq I$ s.t. $I' + bR = I + bR$

Sublemma $\Rightarrow I = I' + (bR) \cap I$, $(bR \cap I) = (I : bR) \cdot b$ and I' are both fin. gen. QED.

Thm (Cohen) A commutative ring R is Noetherian iff every prime ideal is finitely generated

Assume R is not Noetherian

Pf: Zorn's Lemma $\Rightarrow$ The family of ideals in R which are not finitely generated is $\neq \emptyset$, and has a maximal element I .
 I : not a prime ideal $\leadsto \exists a, b \in R$, $a, b \notin I$ and $ab \in I$

$\leadsto$ Both $I + bR$ and $(I : bR)$ are finitely generated

Lemma $\Rightarrow I$ is finitely generated, a contradiction

Nakayama's Lemma:

M : finite R -module, I : ideal of R

Assume: $IM = M$ and $\text{Ker}(M \xrightarrow{x} M) = 0 \quad \forall x \in 1 + I$

then $M = (0)$.

Remark: If $I \subseteq \text{rad}(A)$, then $1 + I \subseteq R^\times$

Cor: M : R -module $N, N' \subseteq M$ R -submodule, $I \subseteq R$ an ideal

Suppose that $M = N + IN'$, and

either (a) I is nilpotent,

or (b) $I \subseteq \text{rad}(A)$,

then $M = N$

Flatness

Prop: The following properties of an R -module M is equivalent

- (1) M is R -flat
- (2) $0 \rightarrow N' \rightarrow N$ exact sequence of R -modules $\Rightarrow 0 \rightarrow N' \otimes_R M \rightarrow N \otimes_R M$ is exact
- (3) $I \otimes_R M \xrightarrow{\sim} IM$ $\forall$ finitely generated ideal $I \in R$
- (4) $\text{Tor}_1^R(M, A/I) = 0$ $\forall$ finitely generated ideal $I \in R$
- (5) $\text{Tor}_1^R(M, N) = 0$ $\forall$ finite R -module N
- (6) $\forall$ sequence $a_1, \dots, a_r \in A$ s.t. $\sum_{i=1}^r a_i x_i = 0$
 $\exists y_1, \dots, y_s \in M$ $x_1, \dots, x_r \in M$
 $\exists (b_{ij}) \in A$ s.t. $\sum_{i=1}^r a_i b_{ij} = 0 \quad \forall j$ and $x_i = \sum_{j=1}^s b_{ij} y_j \quad \forall i=1, \dots, r$

Pf: (1) — (5) are equivalent: well known (use $\text{Tor}_i^R(?, N)$ commutes with direct limit)

Meaning of (6):

$$0 \rightarrow K \xrightarrow{\beta} A^r \xrightarrow{\alpha} A$$

$$K \otimes_R M \xrightarrow{\beta \otimes_R M} M^r \xrightarrow{\alpha \otimes_R M} M$$

(6) means: $\text{Ker}(\alpha \otimes_R M) = \text{Im}(\beta \otimes_R M)$ so (1) $\Rightarrow$ (6)

(6) $\Rightarrow$ (3)

Given $\sum_i a_i \otimes x_i \in I \otimes_R M$ s.t. $\sum a_i x_i = 0$ $a_i \in I, x_i \in M$

$$(6) \leadsto \sum_i a_i \otimes x_i = \sum_{i,j} a_i \otimes b_{ij} y_j = \sum_j \sum_i a_i b_{ij} \otimes y_j = 0$$

$$\text{i.e. } I \otimes_R M \xrightarrow{\sim} I \cdot M \quad \text{QED}$$

Lemma (i) $R \rightarrow R'$ ring homom. M = flat R -module $\Rightarrow M \otimes_R R'$ is R' -flat

(ii) R, S : multiplicative subset in $R \leadsto S^{-1}R$ is flat over R

(iii) $R \rightarrow R'$: flat ring homom $\Rightarrow \text{Tor}_R^i(M, N) \otimes_R R' \xrightarrow{\sim} \text{Tor}_{R'}^i(M \otimes_R R', N \otimes_R R')$

(iv) $R \rightarrow R'$: flat ring homom. M, N : R -module

Assume: M admit a resolution by finite free R -modules

$$\Rightarrow \text{Ext}_R^i(M \otimes_R R', N \otimes_R R') \xleftarrow{\sim} \text{Ext}_R^i(M, N) \otimes_R R'$$

Prop: $(R, \mathfrak{m}, k)$ local ring (not nec. Noetherian), M : R -module

Suppose either $\mathfrak{m}$ is nilpotent
or M is finite over A .

Then M is free $\Leftrightarrow M$ is proj $\Leftrightarrow M$ is flat

Assume M flat over R

Proof: Choose $\{x_i\}_{i \in I}$ s.t. $(\bar{x}_i \in M/\mathfrak{m}M)_{i \in I}$ is a k -basis of $\bar{M}$

Nakayama: $M = \sum a_i x_i$

Claim: $x_1, \dots, x_n$ are linearly indep over R $\forall$ subset $\{x_1, \dots, x_n\} \subseteq \{x_i\}$

$$\sum_{i=1}^n a_i x_i = 0 \Rightarrow \exists y_j \in M \text{ s.t. } \sum_{i=1}^n a_i b_{ij} = 0$$

$$b_{ij} \in R \quad x_i = \sum_{j=1}^m b_{ij} y_j$$

May assume: $b_{n1} \in R^\times$ (look at $x_n = \sum_{j=1}^m b_{nj} y_j$)

$$\wedge \Rightarrow a_n = \sum_{i=1}^{n-1} a_i \underbrace{(-b_{n1}^{-1} \cdot b_{ni})}_{c_i}$$

$$0 = a_1 x_1 + \dots + a_n x_n = a_1 x_1 + \dots + a_{n-1} x_{n-1} + (a_1 c_1 + \dots + a_{n-1} c_{n-1}) x_n$$

$$= a_1 (x_1 + c_1 x_n) + \dots + a_{n-1} (x_{n-1} + c_{n-1} x_n) = 0$$

Induction on n , for the statement:

$x_1, \dots, x_n \in M$ s.t. $\bar{x}_1, \dots, \bar{x}_n \in \bar{M}$ are linearly indep over k

$\Rightarrow x_1, \dots, x_n$ are linearly indep over R

QED.

Prop: $R \rightarrow S$ ring homom. The following are equiv.

(1) S is flat over R

(2) S_P is flat over $R_{P \cap R} \forall P \in \text{Spec}(S)$

(3) $S_{\mathfrak{m}}$ is flat over $R_{\mathfrak{m} \cap R} \forall \mathfrak{m} \in \text{Max}(S)$

$$(3) \Rightarrow (1) \quad \text{Tor}_i^R(S, N)_{\mathfrak{m}} = \text{Tor}_i^{R_{\mathfrak{m} \cap R}}(S_{\mathfrak{m}}, M_{\mathfrak{m} \cap R}) \quad N: R\text{-module}$$

$$\forall \mathfrak{m} \in \text{Max}(S)$$

Lemma

M : A -module

The following are equivalent

(1) M is faithfully flat over A

(2) M is flat over A and $M \otimes_A N \neq (0) \quad \forall$ non-zero A -module N

(3) M is flat over A and $M/\mathfrak{m}M \neq 0 \quad \forall \mathfrak{m} \in \text{Max}(A)$

(1) $\Rightarrow$ (2) $\Rightarrow$ (3) obvious

(2) $\Rightarrow$ (1) Apply (2) to $N = \text{Coker} \begin{pmatrix} \text{Ker} \\ \text{(a module homom)} \end{pmatrix}$ and $N = H. \text{(a complex)}$

(3) $\Rightarrow$ (2): $0 \rightarrow A/I \rightarrow N$

$$0 \rightarrow (A/I) \otimes_A M \rightarrow N \otimes_A M$$

$\nwarrow$
 $\neq (0)$ by (3)

Base change: M : f.flat over A
 $\Rightarrow M \otimes_A B$ is f.flat over B

Consequence of $A \rightarrow B$ faithfully flat

(a) $A \xrightarrow{\phi} B$ is injective

$a \in \text{Ker}(\phi) \leadsto$ Consider $A \xrightarrow{a} A$

(b) $\forall$ ideal $I \subseteq A$, have $IB \cap A = I \quad \because A/I \rightarrow B/IB$ is faithfully flat

(c) $\text{Spec}(B) \rightarrow \text{Spec}(A)$ is surjective

$$\because \forall \mathfrak{p} \in \text{Spec}(A) \quad \mathfrak{p}B \neq B$$

Faithfully flat ring homom

Lemma $A \rightarrow B$ ring homomorphism

- (1) B is faithfully flat over A
 $\Leftrightarrow$ (2) B_P is flat over $A_P \cap A \ \forall P \in \text{Spec}(B)$ and $\text{Spec}(B) \rightarrow \text{Spec}(A)$ is surj
 (3) B is flat over A and $\forall \mathfrak{m} \in \text{Max}(A), \exists$ a max. ideal $\tilde{\mathfrak{m}} \in \text{Max}(B)$ st.

(1) $\Rightarrow$ (2) $A_{\mathfrak{f}} \rightarrow B \otimes_A A_{\mathfrak{f}} =: B_{\mathfrak{f}}$ is faithfully flat $\forall \mathfrak{f} \in \text{Spec}(A) \ \tilde{\mathfrak{m}} \cap A = \mathfrak{f}$
 $\Rightarrow (A_{\mathfrak{f}}/\mathfrak{f}A_{\mathfrak{f}}) \otimes_{A_{\mathfrak{f}}} B_{\mathfrak{f}} \neq 0 \Rightarrow B_{\mathfrak{f}}/\mathfrak{f}B_{\mathfrak{f}} \neq (0)$.

descent property 1) $\begin{array}{c} B \\ \uparrow \\ A \end{array} \begin{array}{c} N \\ \swarrow \\ \end{array}$ N faithfully flat B -module
 and also faithfully flat over A
 $\Rightarrow B$ is faithfully flat over A

pf:

$M_1 \rightarrow M_2 \rightarrow M_3$: A -module homom

$\Rightarrow (M_i \otimes_A B) \otimes_B N = M_i \otimes_A N$ q.e.d.

descent property 2) $\begin{array}{c} B \\ \uparrow \text{f.f. flat} \\ A \end{array} \begin{array}{c} M \\ \swarrow \\ \end{array}$

(2a) M is A -flat $\Leftrightarrow M \otimes_A B$ is B -flat

$N_1 \rightarrow N_2 \rightarrow N_3$: A -module homom $\Rightarrow (N_i \otimes_A B) \otimes_B (M \otimes_A B) = (N_i \otimes_A M) \otimes_A B$

(2b) M is a finite A -module $\Leftrightarrow M \otimes_A B$ is a finite B -module

$\Leftarrow \exists y_1, \dots, y_m \in M \otimes_A B$ st. $M \otimes_A B = \sum_{i=1}^m B y_i$

$\exists x_1, \dots, x_n \in M$ st. $y_i \in \sum_{j=1}^n B \cdot (x_j \otimes 1) \Rightarrow (M / \sum_{j=1}^n A x_j) \otimes_A B = (0)$

(3b) M is finitely presented over $A \Leftrightarrow M \otimes_A B$ is finitely presented over B

§

Going up and Going down

- These are properties of order-preserving maps between posets

1. GD holds for $A \rightarrow B$ flatPf: Given $P \in \text{Spec}(B)$

$$\mathfrak{p} = A \cap P \quad \text{and} \quad \mathfrak{p} \geq \mathfrak{p}' \in \text{Spec}(A)$$

Consider $A_{\mathfrak{p}} \rightarrow B_{\mathfrak{p}} \otimes_A A_{\mathfrak{p}}$ faithfully flat $\circ \circ P: (B_{\mathfrak{p}} \otimes_A A_{\mathfrak{p}}) \cap A_{\mathfrak{p}} = \mathfrak{p} A_{\mathfrak{p}}$ $\Rightarrow \text{Spec}(B_{\mathfrak{p}} \otimes_A A_{\mathfrak{p}}) \rightarrow \text{Spec}(A_{\mathfrak{p}})$ is surjective. q.e.d.

2. GU holds for integral ring extensions

Lemma 1 $\mathfrak{m} \in \text{Max}(A)$, $A \hookrightarrow B$ integral, $P \in \text{Spec}(B)$, if $P \cap A = \mathfrak{m}$ then P is a maximal idealPf $A/\mathfrak{m} \hookrightarrow B/P$

$$\forall \bar{y} \in B/P \quad \exists \text{ relation } \bar{y}^n + a_{n-1} \bar{y}^{n-1} + \dots + a_0 = 0 \quad \text{with } a_i \in A/\mathfrak{m} \quad n \geq 1$$

$$\Rightarrow \bar{y}^{-1} = -a_0^{-1} (\bar{y}^{n-1} + a_{n-1} \bar{y}^{n-2} + \dots + a_2 \bar{y} + a_1)$$

So B/P is a field. q.e.d.Lemma 2 $A \hookrightarrow B$ integral, $M \in \text{Max}(B) \Rightarrow M \cap A \in \text{Max}(A)$ Pf: $\forall \bar{x} \in A/M \cap A$, $\exists$ relation

$$\bar{x}^{-n} + b_{n-1} \bar{x}^{-n+1} + \dots + b_1 \bar{x}^{-1} + b_0 = 0 \quad \Rightarrow \bar{x}^{-1} \in A/M \cap A \quad \text{q.e.d.}$$

Lying over

Lemma 3 $A \hookrightarrow B$ integral(a) $\text{Spec}(B) \rightarrow \text{Spec}(A)$ is surjective(b) If $P_1 \subseteq P_2$ are prime ideals of B s.t. $P_1 \cap A = P_2 \cap A$, then $P_1 = P_2$ Pf: (a) $\forall \mathfrak{p} \in \text{Spec}(A)$, $A_{\mathfrak{p}} \hookrightarrow B_{\mathfrak{p}} \otimes_A A_{\mathfrak{p}}$ every maximal ideal of $B_{\mathfrak{p}} \otimes_A A_{\mathfrak{p}}$ contracts to $\mathfrak{p} A_{\mathfrak{p}}$ by Lemma 2(b) Suppose $P_1 \cap A = P_2 \cap A = \mathfrak{p}$ Consider $A_{\mathfrak{p}} \rightarrow B_{\mathfrak{p}} \otimes_A A_{\mathfrak{p}}$
 $\Rightarrow P_1 A_{\mathfrak{p}} = P_2 A_{\mathfrak{p}}$ by Lemma 1

Prop 1 $A \rightarrow B$ integral $\Rightarrow$ GU holds

pf: $\mathfrak{P} = \bigcap_{\mathfrak{P}' \in \text{Spec}(B)} \mathfrak{P}' \cap A$ $\mathfrak{P} \in \mathfrak{P}'$ in $\text{Spec}(A)$

$$A/\mathfrak{P} \hookrightarrow B/\mathfrak{P}$$

$$\cap \quad \cap$$

$$(A/\mathfrak{P})_{\mathfrak{P}'/\mathfrak{P}} \hookrightarrow (B/\mathfrak{P}) \otimes_{A/\mathfrak{P}} (A/\mathfrak{P})_{\mathfrak{P}'/\mathfrak{P}}$$

Every maximal ideal of $(B/\mathfrak{P}) \otimes_{A/\mathfrak{P}} (A/\mathfrak{P})_{\mathfrak{P}'/\mathfrak{P}}$ contracts to $(\mathfrak{P}'/\mathfrak{P}) \cdot (A/\mathfrak{P})_{\mathfrak{P}'/\mathfrak{P}}$ q.e.d.

Prop 2 $A \hookrightarrow B$ integral domains, and A is integrally closed in $\frac{\text{frac}(A)}{K}$

(a) GD holds

(b) If B is the integral closure of A in $\text{frac}(B)=L$, and L/K normal field extⁿ, then for any two prime ideals $\mathfrak{P}, \mathfrak{P}' \in \text{Spec } B$ s.t. $\mathfrak{P}' \cap A = \mathfrak{P} \cap A$,

$$\exists \sigma \in \text{Aut}(L/K) \text{ s.t. } \sigma(\mathfrak{P}) = \mathfrak{P}'$$

pf: (b) $\Rightarrow$ (a): Take a normal extⁿ L of K containing $\text{frac}(B)$
By Lemma 3 (Lying over)

Given

$$\mathfrak{P} \neq \mathfrak{P}'$$

May assume: $\text{frac}(B)$ is a normal field extⁿ of K
and $B = \mathcal{O}_L =$ integral closure of A in L

Lying over: $\exists \mathfrak{P}'$ s.t. $\mathfrak{P}' \cap A = \mathfrak{P} \cap A$. Pick $\mathfrak{P}_1 \equiv \mathfrak{P}'$ lying above $\mathfrak{P}$

Apply (b) to $\mathfrak{P}$ and $\mathfrak{P}_1$.

(a) Assume first that $[L:K] < \infty$. Let $\text{Aut}(L/K) = \{\sigma_1, \dots, \sigma_n\}$

Suppose $\mathfrak{P}_i = \sigma_i(\mathfrak{P}) \neq \mathfrak{P}' \forall i$. By Lemma 3: $\mathfrak{P}' \not\subseteq \mathfrak{P}_i \forall i$

$$\Rightarrow \mathfrak{P}' \not\subseteq \mathfrak{P}_1 \cup \dots \cup \mathfrak{P}_n$$

$$\Rightarrow \exists x \in \mathfrak{P}' \setminus (\mathfrak{P}_1 \cup \dots \cup \mathfrak{P}_n)$$

$$\text{Let } y = \left(\prod_{i=1}^n \sigma_i^{-1}(x) \right)^m \in K$$

$m=1$ if L/K separable
otherwise: $m \in \mathbb{p}\mathbb{N}$

$$\Rightarrow y \in A \cap \mathfrak{P}' = A \cap \mathfrak{P}$$

However $\Rightarrow \sigma_i^{-1}(x) \in \mathfrak{P}$ for some $i \Rightarrow x \in \sigma_i \mathfrak{P}$ for some i ,
contradiction

General case

$$\text{Let } K' = L \underset{K}{\overset{\text{Aut}(L/K)}{\text{p.insep}}} \underset{\text{Spec}(\mathcal{O}_{K'})}{\overset{\text{radicial}}{\rightarrow}} \text{Spec}(\mathcal{O}_K)$$

May assume: L/K is Galois Let $G = \text{Gal}(L/K)$

$\Rightarrow \forall$ finite Galois subextⁿ $L'/K \subset L/K$

Consider $S(L') = \left\{ \sigma \in \text{Gal}(L'/K) \mid \sigma(P \cap \mathcal{O}_{L'}) = P' \cap \mathcal{O}_{L'} \right\}$

$\leftarrow$ have proved

ϕ

$$\Rightarrow \bigcap_{L'/K \text{ finite Galois}} S(L') \neq \phi \quad \Rightarrow \text{QED.}$$

§ Noetherian spaces and irreducible spaces

ref. EGA 0 §2

Defⁿ: A topological space X is irreducible if it is not the union of two closed subspaces Z_1, Z_2 with $Z_i \neq X$ for $i=1,2$

Defⁿ: A point x of an irreducible topological space X is a generic point of X if $\overline{\{x\}} = X$

An example of an irreducible topological space without a generic pt:

$\text{Max}(\mathbb{C}[x])$

Def: A maximal element in $\{\text{irred. subsets of } X\}$ is called an irreducible component of X (nec. closed)

Def: A topological space X is Noetherian if the set of all open subsets of X has the maximum property.

i.e. every non-empty family of open subsets of X has a maximal element.

Equivalently: every ascending chain of open subsets of X stops

Equivalently: every descending chain of closed subsets of X stops

Noetherian induction: (Applied to the poset of closed subsets of a Noetherian top. space)

$(E, \leq)$ a poset s.t. the minimum property holds

Suppose $P: E \rightarrow \{T, F\}$ is a function s.t. $(*)_a$ holds $\forall a \in E$.

$(*)_a$: If $P(x) = T \ \forall x \not\leq a$, then $P(a) = T$

Then $P(x) = T \ \forall x \in E$

- Lemma: (1) Every subspace of a Noetherian top. space is Noetherian
- (2) If X is a topological space, and $Z_1, \dots, Z_n =$ subsets of X such that $X = Z_1 \cup \dots \cup Z_n$ and Z_i with induced topology is Noetherian for $i=1, \dots, n$. Then X is Noetherian
- (3) Every Noetherian space X is quasi-compact
(Clear $\because$ the family of open subsets of X has the maximum property)
- $\leadsto$ Every open subset of a Noetherian top. space is quasi-compact
- (4) If X is a topological space st. every open subset of X is quasi-compact, then X is Noetherian.
($\forall (U_i)$ increasing chain of open subsets of X)
 $\bigcup_i U_i$ is quasi-compact w/ of open subsets of X)
- (5) Every Noetherian topological space is the union of a finite number of irreducible components

Pf. Noetherian induction: Every closed subset Z of X is a finite union of irreducible components of Z

induction hypothesis = Every closed subset Z of X st. $Z \subsetneq X$ is a union of a finite number of irreducible components

Either X is irred $\leadsto$ OK

or $X = Z_1 \cup Z_2$, Z_1, Z_2 closed and $Z_i \subsetneq X$ for $i=1, 2$

Apply induction hypothesis. q.e.d.

Exer 1. Give an example of irred. topological space which is not noetherian

2. $\text{Spec}(R)$ is Noetherian if and only if
 $\forall$ ideal $I \subseteq R \quad \exists$ a finite number of elements $x_1, \dots, x_n \in I$
 s.t. $I \subseteq \text{rad}(x_1, \dots, x_n)$

pf of the "if" part

3. $I_1 \subseteq I_2 \subseteq \dots$ increasing sequence of ideals s.t.
 $\text{rad}(I_i) = I_i \quad \forall_i$

$$\text{Let } I = \bigcup I_i \rightarrow I = \text{rad}(I)$$

$$\exists \overset{\wedge}{x_1, \dots, x_n} \in I_{i_0} \text{ s.t. } \text{rad}(x_1, \dots, x_n) \overset{||}{=} I \overset{\cap}{=} \text{rad}(x_1, \dots, x_n)$$

irreducible p.e.d.

$$\text{rad}(I) \supseteq \text{rad}(x_1, \dots, x_n)$$

3. Given an example of an Noetherian topological space
 without a generic point
ex $\text{Max}(\mathbb{Q}[x])$

Def (a) A continuous map $X \xrightarrow{f} Y$ of top. space ref EGA O_{III} §1.8 is quasi-compact if $\forall$ quasi-compact open subset $U \subseteq Y$, $f^{-1}(U)$ is quasi-compact

morphisms between

Note = This notion is not every useful for locally compact Hausdorff spaces: If Y is connected, then the only quasi-cpt open subsets of Y are Y and $\emptyset$. Thus suppose that X, Y are both locally compact Hausdorff, $f: X \rightarrow Y$ is quasi-compact and Y is connected, then f is quasi-cpt iff either Y is non-compact, or both X and Y are compact

The only situation I know of where this definition is useful is when both X and Y are locally isomorphic to a profinite set with pro-finite topology

composition of quasi-cpt maps are quasi-cpt, but unclear whether base change of a quasi-cpt map is quasi-cpt

Perhaps: For $X \xrightarrow{f} Y$ continuous, X, Y locally compact Hausdorff, a more useful notion is to require that $\forall$ compact subset $Z \subseteq Y$, $f^{-1}(Z)$ is compact

ie compact closed subset

Remark: In Bourbaki's definition, compact $\Rightarrow$ Hausdorff

Def: A subset Z of a topological space X is retrocompact if $Z \rightarrow X$ is quasi-compact.

Equiv: $\forall$ quasi-compact open subset U of X , $Z \cap U$ is quasi-compact.

Note: Every closed subset is retrocompact

Remark: a) If X is locally Noetherian, every quasi-compact open subset is Noetherian, hence every subset is retrocompact

b) If X is compact Hausdorff and connected, every retrocompact subset is closed

c) If X is connect Hausdorff and non-compact, every subset of X is retrocompact

const. 2

Properties (1) A finite union of retrocompact subsets is retrocompact

(2) A finite union of quasi-compact subsets is quasi-compact

(3) Every finite intersection of retrocompact open subsets

Exer $\nearrow$ is (open and) retrocompact

$\Rightarrow$ (4) If X is locally noetherian, then every quasi-compact subspace of X is Noetherian; consequently:

every subset of a locally Noetherian space is retro-compact
($\because$ every subset of a Noetherian space is Noetherian, therefore quasi-cpt.)

Definition A subset $Z \subseteq X$ is constructible iff

$Z \in$ The smallest Boolean subalg of 2^X which contains all retrocompact open subsets of X

Cor. A subset of a locally Noetherian space is constructible iff it is a finite union of locally closed subsets

Prop/Exer: A subset $Z \subseteq X$ is constructible iff

$\exists$ retrocompact open subsets U_i, V_i of X st.

$$Z = \bigcup_{i=1}^n (U_i \cap (X \setminus V_i))$$

Cor.

Cor 2 Every constructible subset is retro-compact

pf: U, V retro compact open subsets, $W = \text{cpt open}$

$$\leadsto U \cap (X \setminus V) \cap W = \underbrace{(U \cap W)}_{\text{quasi-cpt}} \cap (X \setminus V) = \text{a closed subset of the quasi-cpt open subset } (U \cap W) = \text{quasi-cpt g.e.d}$$

Cor 3 (a) An open subset U of X is constructible $\Leftrightarrow U$ is retrocompact

(b) A closed subset C of X is constructible $\Leftrightarrow X \setminus C$ is retrocompact

pf: Clearly (a) $\Rightarrow$ (b)

For (a) " $\Rightarrow$ " follows from Cor 2

" $\Leftarrow$ " obvious.

g.e.d.

Constructible 3

Prop 4 $T \subseteq X$ constructible, $U \subseteq X$ open

(a) $T \cap U$ is constructible in U

(b) If U is retrocompact in X and $T \subseteq X$,

then T is constructible in $X \iff T$ is constructible in U

pf: (a) Exercise

(b): " $\Rightarrow$ " follows from (a)

" $\Leftarrow$ ": Suffices to show that if V, W are retrocompact open subsets in U , then $V \cap (U \setminus W)$ is constructible in X

$$\begin{array}{c} V \hookrightarrow U \hookrightarrow X \\ \text{quasi-compact} \quad \text{quasi-compact} \end{array} \Rightarrow V \text{ is retrocompact in } X$$

Similarly W is retrocompact in X

$\Rightarrow V \cap (U \setminus W) = V \cap (X \setminus W)$ is constructible in X . q.e.d.

Cor 5 Let X be a topological space and let $(U_i)_{i \in I}$ be a finite family of

Remark (a) A subset of a Noetherian space is constructible if and only if it is a finite union of locally closed subsets

(b) Suppose X is locally Noetherian. Recall that every pt x of X has a neighborhood U which is Noetherian and hence quasi-compact. Also every quasi-compact open subset of X is Noetherian. Therefore every subset of a locally Noetherian space is retrocompact

$\Rightarrow Z \subseteq X$ is constructible

$$\iff Z = \bigcup_{i=1}^n (U_i \cap (X \setminus V_i))$$

U_i, V_i open subsets of X

constr 4

Cor 6: Let X be a quasi-compact topological space such that there exists a basis $(U_i)_{i \in I}$ of open subsets with each U_i retrocompact.

Then a subset $Z \subseteq X$ is constructible iff Z is locally constructible.

Ex: If X is (the topological space underlying) a quasi-cpt quasi-separated scheme, then the assumption on X in Cor 6 is satisfied.

Reformulation

Cor 6': (a) Every constructible subset Z of X is locally constructible.

(b) If X is quasi-cpt and the topology of X admits a basis consisting of retrocompact open subsets, then every locally constructible subset of X is constructible.

Cor 7 Suppose X admits a basis of retrocompact open subsets. Every loc. constructible subset T of X is retrocompact.

($\because T \cap (a \text{ quasi-cpt open subset } U)$ is constructible in U)
hence retrocompact in U , hence quasi-cpt

Constructible subsets of a Noetherian space

Lemma 8 $E \subseteq X$ constructible, X noetherian

E is dense in $X \iff X$ contains a dense open subset

Prop 9. X noetherian. A subset $E \subseteq X$ is constructible
iff $\forall$ irreducible closed subset Y of X , $E \cap Y$ is either nowhere
nowhere dense in Y or contain a dense open subset of Y

PF of if: Noetherian induction on: the family of closed
subsets Z of X s.t. $Z \cap E$ is constructible

Cor. 10 X noetherian. $(E_\alpha)_{\alpha \in I}$ a filtering increasing
family of constructible subsets s.t. (i) $X = \bigcup E_\alpha$

(ii) Every irreducible closed subset of X is contained in
 $\overline{E_\alpha}$ for some α

Then $\exists \alpha \in I$ s.t. $E_\alpha = X$ (condition ii) is redundant
(if every irred closed subset contains a generic pt.)

PF: Noetherian induction on:
the family of all closed subsets of X contained in
one of the E_α 's.

Exer: Define irreducible topological space X :

if $\emptyset \neq U_1 \cap \dots \cap U_n$ each U_i open, then $U_i = \emptyset$
for some i

Exer Prove, using Zorn's lemma, that every irreducible subset of X is contained in a maximal irreducible subset of X (necessarily closed)

$\Rightarrow$ For every commutative ring R , any ideal I and a prime ideal $P \supseteq I$, $\exists$ exists a prime ideal $\mathfrak{p} \subseteq P$ which is minimal among prime ideals containing I .

Exer $\text{Spec } R$ is irred. iff $\text{rad}(0) = \text{a prime ideal}$

i.e. R is

§ Chevalley's theorem

Constr 6

Lemma: Let $Z \subseteq \text{Spec}(A)$ be a constructible subset.

There exists an A -algebra B of finite presentation

$$\text{s.t. } Z = \text{Image}(\text{Spec}(B) \rightarrow \text{Spec}(A))$$

(Chevalley)

Theorem: Let B be an A -algebra of finite presentation.

Let $Z \subseteq \text{Spec}(B)$ be a constructible subset

Then the image of Z under the map $\text{Spec}(B) \rightarrow \text{Spec}(A)$ is a constructible subset of $\text{Spec}(A)$

EGA IV Thm 1.8.4

Lemma: Every constructible subset of $\text{Spec}(A)$ is of the form

$$\bigcup_{i=1}^n \left(U_i \cap (\text{Spec}(A) \setminus \text{Spec}(V_i)) \right),$$

where U_i and V_i are retro-compact open subsets of $\text{Spec}(A)$ for each $i=1, \dots, n$

$\Rightarrow$ Chevalley's theorem is reduced to the special case when $Z = \text{Spec}(B)$:

$\exists$ i) a $\mathbb{Z}$ -algebra of finite type A'

ii) a finitely presented A' -algebra B'

iii) a ring homomorphism $\varphi: A' \rightarrow A$

iv) an A -linear isomorphism $B' \otimes_{A'} A \xrightarrow{\beta} B$

$$\begin{array}{ccc} \text{Spec } B & \xrightarrow{u} & \text{Spec}(B') \\ w \downarrow & & \downarrow v \\ \text{Spec } A & \xrightarrow{a_\varphi} & \text{Spec}(A') \end{array}$$

$$w(\text{Spec}(B)) = (a_\varphi)^{-1}(v(\text{Spec}(B')))$$

Constr. 7

Proof of Chevalley's theorem when $Z = \text{Spec}(B)$ and A is Noetherian

Noetherian induction:

Reduce to: A = noetherian domain $A \subseteq B \leftarrow$ f.g. A -alg.

$${}^a\phi = \text{Spec}(B) \rightarrow \text{Spec}(A)$$

Then $\exists 0 \neq a \in A$ s.t. $\text{Spec}(A[\frac{1}{a}]) \subseteq {}^a\phi(\text{Spec}(B))$

$\leadsto$ May assume B = integral domain

$$B = A[\underbrace{x_1, \dots, x_r}_{\text{alg. indep}}, \underbrace{x_{r+1}, \dots, x_n}_{\text{algebraic over } A[x_1, \dots, x_r]}]$$

$$\begin{array}{ccc} B[\frac{1}{a}] & \leftarrow & B \\ \uparrow \xi & & \uparrow \phi \\ A[\frac{1}{a}] & \leftarrow & A \end{array}$$

$\leadsto \exists a \in A$ s.t. $B[\frac{1}{a}]$ is integral over $A[\frac{1}{a}, x_1, \dots, x_r]$

$$\begin{aligned} \leadsto {}^a\phi(\text{Spec } B[\frac{1}{a}]) &= {}^a\gamma({}^a\xi(\text{Spec } A[\frac{1}{a}])) \\ &= {}^a\gamma(\text{Spec } A[\frac{1}{a}, x_1, \dots, x_r]) \\ &= \text{Spec } A[\frac{1}{a}]. \end{aligned}$$

q.e.d.

§ Primary decomposition

Defⁿ: M : A -module. $\text{Ass}_A(M) = \text{Ass}(M) = \left\{ \mathfrak{p} \in \text{Spec}(A) \mid \exists x \in M \text{ s.t. } \mathfrak{p} = \text{Ann}(a) \right\}$

Lemma¹: Every maximal element of $\{ \text{Ann}(x) \mid x \in M \}$ is a prime ideal of A

Cor² A noetherian, M : A -module. then $\text{Ass}(M) \neq \emptyset \iff M \neq 0$

Cor³ A noetherian, $a \in A$. M : A -module

$[a]_M: M \rightarrow M$ is injective $\iff a \notin \bigcup_{\mathfrak{p} \in \text{Ass}(M)} \mathfrak{p}$

(If $ax \neq 0$, $x \neq 0$, then $\text{Ass}(Ax) \ni \mathfrak{p} = \text{Ann}_A(bx) \ni a$)

Lemma⁴ 1) $0 \rightarrow M' \rightarrow M \rightarrow M'' \rightarrow 0$

$\Rightarrow \text{Ass}(M) \subseteq \text{Ass}(M') \cup \text{Ass}(M'')$

2) $\text{Ass}\left(\bigoplus_{j \in J} M_j\right) = \bigcup_j \text{Ass}(M_j)$

Cor⁵: $(Q_j)_{j \in J}$ $|J| < \infty$ If $\bigcap_j Q_j = (0)$, then

$Q_j \subseteq M$ A -submodules

$\text{Ass}(M) \subseteq \bigcup_j \text{Ass}(M/Q_j)$

$\left(M \hookrightarrow \bigoplus_j (M/Q_j) \right)$

Prop⁶ $\forall$ subset $\Phi \subseteq \text{Ass}(M)$

$\exists$ an A -submodule $N \subseteq M$ s.t. $\text{Ass}(N) = \text{Ass}(M) \setminus \Phi$

Pf $\{ P \subseteq M \mid \text{Ass}(P) \subseteq \text{Ass}(M) \setminus \Phi \} = \mathcal{F}$ and $\text{Ass}(M/N) = \Phi$

has a maximal element N , by Zorn's lemma

$\Rightarrow \text{Ass}(N) \subseteq \text{Ass}(M) \setminus \Phi$ Claim: $\text{Ass}(M/N) \cap \Phi = \emptyset$, for $\forall \mathfrak{p} \in \text{Ass}(M/N)$,

$\forall \mathfrak{p} \in \text{Ass}(M/N) \rightsquigarrow \exists \text{ exact } 0 \rightarrow N \rightarrow \tilde{M} \rightarrow A/\mathfrak{p} \rightarrow 0$ N maximal in $\mathcal{F}$ $\Rightarrow \mathfrak{p} \notin \Phi$ QED

Lemma 7: M : A -module S : multiplicatively closed $\bar{S} = \{s^{-1} | s \in S\}$

$$(a) \quad \text{Ass}_A(M) \cap \text{Spec}(\bar{S}^{-1}A) \longleftrightarrow \text{Ass}_{\bar{S}^{-1}A}(\bar{S}^{-1}M)$$

(b) If $\mathfrak{p} \in \text{Spec}(A)$ is finitely generated, $\mathfrak{p} \cap S = \emptyset$ and $\bar{S}^{-1}\mathfrak{p} \in \text{Ass}_{\bar{S}^{-1}A}(\bar{S}^{-1}M)$, then $\mathfrak{p} \in \text{Ass}_A(M)$

Proposition 8 A Noetherian M : A -module.

$$\Psi = \{ \mathfrak{p} \in \text{Spec}(A) \mid \mathfrak{p} \cap S = \emptyset \}$$

Then $\exists!$ submodule $N \subseteq M$ s.t.

$$\text{Ass}(N) = \text{Ass}(M) \cap \Psi \quad \text{and} \quad \text{Ass}(M/N) = \Psi$$

This submodule N is $N = \text{Ker}(M \rightarrow \bar{S}^{-1}M)$; it is the largest sub-module among all submodules $N' \subseteq M$ s.t. $\text{Ass}(N') \cap S \neq \emptyset$

Lemma 9: (a) $\mathfrak{p} \in \text{Ass}(M)$, $\mathfrak{p}' \supseteq \mathfrak{p} \Rightarrow \mathfrak{p}' \in \text{Supp}(M)$

(b) If A is Noetherian, then $\text{Supp}(M) = \{ \mathfrak{p}' \in \text{Spec}(A) \mid \exists \mathfrak{p} \in \text{Ass}(M) \text{ s.t. } \mathfrak{p}' \supseteq \mathfrak{p} \}$

A : Noetherian, M : finite A -module

$\Rightarrow \exists$ a composition series

$$(0) = M_0 \subsetneq M_1 \subsetneq \dots \subsetneq M_m = M \text{ s.t. } M_i/M_{i-1} \cong A/\mathfrak{p}_i \quad \mathfrak{p}_i \in \text{Spec}(A)$$

$$\Rightarrow \text{Ass}(M) \subseteq \{ \mathfrak{p}_1, \dots, \mathfrak{p}_r \} \subseteq \text{Supp}(M)$$

primary 3

Definition: Let A be a ring and M be an A -module.

We say that M is co-primary if $\forall a \in A$, $[a]_M$ is either injective or almost nilpotent in the sense that $\forall x \in M \exists n \in \mathbb{N}$ s.t. $a^n x = 0$.

Note: If M is co-primary, then $\{a \in A \mid [a] \text{ is almost nilpotent}\}$ is a prime ideal.

Lemma 10: If A is noetherian, then an A -module M is co-primary iff $\text{Ass}(M)$ is a singleton $\{p\}$.

Defⁿ: A : noetherian M : A -module N : a submodule of M

A primary decomposition of N in M is

a finite family $(Q_i)_{i \in I}$ of A -submodules s.t. $\bigcap_{i \in I} Q_i = N$ and each Q_i is co-primary.

Thm 11: Assume M/N is a finite A -module, A Noetherian.

Ex 4: $\exists$ a primary decomposition of N in M .

This follows from Prop. 6.

primary 4

25

(primary decomposition and extension of scalars)
ring homomom

Theorem: $A \rightarrow B$ M : A -module N : B -module

Assume: N is flat over A

Then (1) $\text{Ass}_B(M \otimes_A N) \supseteq \bigcup_{\mathfrak{p} \in \text{Ass}_A(M)} \text{Ass}_B(N/\mathfrak{p}N)$

(2) If A is Noetherian, then

$$\text{Ass}_B(M \otimes_A N) = \bigcup_{\mathfrak{p} \in \text{Ass}_A(M)} \text{Ass}_B(N/\mathfrak{p}N)$$

reference: Bourbaki, Alg Comm. IV §2 n°6

Pf (1): $A/\mathfrak{p} \hookrightarrow M \Rightarrow N/\mathfrak{p}N \subseteq M \otimes_A N$
 $\Rightarrow \text{Ass}_B(N/\mathfrak{p}N) \subseteq \text{Ass}_B(M \otimes_A N)$ (1) is proved

(2): Assume now that A is Noetherian

Lemma: Suppose that M' is an A -module s.t. $\text{Ass}_A(M') = \{\mathfrak{p}\}$,
 and N is flat as an A -module

Then $P \cap A = \mathfrak{p} \quad \forall P \in \text{Ass}_B(M' \otimes_A N)$

pf of Lemma:

Choose $n \in \mathbb{N}$ s.t. $\mathfrak{p}^n M' = 0$ Given $P \in \text{Ass}_B(M' \otimes_A N) \rightsquigarrow B/P \hookrightarrow M' \otimes_A N$

Elements of $A/\mathfrak{p}$ act injectively on $M' \rightsquigarrow P \cap A \subseteq \mathfrak{p}$ Lemma proved

Proof of (2)

Assume first that $\text{Ass}_A(M) = \{\mathfrak{p}\}$, a singleton

Lemma $\Rightarrow \forall P \in \text{Ass}_B(M \otimes_A N)$ have $P \cap A = \mathfrak{p}$

Have filtration

$(0) \subseteq M_1 \subsetneq \dots \subsetneq M_m = M$ s.t. $M_i/M_{i+1} \cong A/\mathfrak{p}_i$ $\mathfrak{p}_i$: prime ideal

$\exists n$ s.t. $\mathfrak{p}^n M = 0$

$$\Rightarrow \text{Ass}_B(M \otimes_A N) \subseteq \bigcup_{i=1}^m \text{Ass}_B(N/\mathfrak{p}_i N) \cap \varphi^{-1}(\{\mathfrak{p}\})$$

$$N \text{ flat over } A \leadsto \forall Q \in \text{Ass}_B(N/\mathfrak{p}_i N), \text{ have } Q \cap A = \mathfrak{p}_i$$

$$\Rightarrow \text{Ass}_B(M \otimes_A N) \subseteq \text{Ass}_B(N/\mathfrak{p}_i N)$$

General case

Devissage using a primary decomposition of M $\Rightarrow$ statement (2) holds for every finite A -module M $\Rightarrow$ Statement (2) holds for every A -module M .

QED.

Corollary $A \xrightarrow{\text{flat}} B$ A, B Noetherian $Q \subseteq M$ $\mathfrak{p}$ -primary A -sub-module $P \in \text{Spec}(B), \mathfrak{p} = P \cap A$ Then $Q \otimes_A B$ is a P -primary submodule of $M \otimes_A B$ $\Leftrightarrow \mathfrak{p}B$ is a P -primary ideal of B

graded 1

- defⁿ: $(\mathbb{N})$ graded ring $A = \bigoplus_{i=0}^{\infty} A_i$ $(\mathbb{N})$ graded $(\bigoplus_{i \in \mathbb{N}} A_i)$ -module $M = \bigoplus_{i \in \mathbb{N}} M_i$

$$A_i \cdot M_j \subseteq M_{i+j}$$

(or. $M = \bigoplus_{i \in \mathbb{Z}} M_i$) $(\mathbb{N})$ -Filtered ring $A = A^0 \supseteq A^1 \supseteq \dots$ $(\mathbb{N})$ -Filtered A -module $M = M^0 \supseteq M^1 \supseteq \dots$ decreasing filtration

$$A^i \cdot M^j \subseteq M^{i+j}$$

ex I -adic filtration of a ring A
module M def: I -good filtration of a filtered A -module compatible with the I -adic filtration of A
 $\exists n_0 \in \mathbb{N}$ st. $I^i \cdot M^j = M^{i+j} \quad \forall j \geq n_0$ defⁿ: Rees ring of I : $A \oplus I \oplus I^2 \oplus \dots =: \text{Rees}_I(A)$

$$= \sum_{i \in \mathbb{N}} I^i t$$

Rees module of (M_i) :

$$\text{Rees}(M) = \sum_{i \geq 0} M^i t$$

Lemma A : commutative ring $I \subseteq A$ M : fg. A -module, with filtration M^i

$$\text{st. } I^i \cdot M^j \subseteq M^{i+j}$$

Then the filtration (M_i) is I -goodie compatible with the I -adic filtration of A

$$\Leftrightarrow R(M) = \bigoplus_{i \in \mathbb{N}} M^i \text{ is a finitely generated } \text{Rees}_I(A)\text{-module}$$

Lemma A : noetherian $\Rightarrow \text{Rees}_I(A)$ is a finitely generated A -alg.
hence Noetherian(Artin-Rees) Prop: A : noetherian, $I \subseteq A$ ideal. M fin. gen A -module N_1, N_2 : A -submodules of M

$$\Rightarrow \exists n_0 \in \mathbb{N} \text{ st } I^{n-n_0}(I^{n_0} N_1 \cap N_2) = I^n N_1 \cap N_2 \quad \forall n \geq n_0$$

graded 2

pf: $\bigoplus_{n \geq 0} (I^n N_1 \cap N_2)$ is a graded $\text{Rees}_I(A)$ -submodule of the Noetherian $\text{Rees}_I(A)$ -module $\text{Rees}_I M$.

$\Rightarrow \bigoplus_{n \geq 0} I^n N_1 \cap N_2$ is fin. gen. over $\text{Rees}_I(A)$

$\Leftrightarrow$ The filtration $(I^n N_1 \cap N_2)_{n \in \mathbb{N}}$ of $N_1 \cap N_2$ is I -good. q.e.d.

(Krull intersection thm)

A : noetherian, $I \subseteq A$ f.g. ideal, M : fin. gen A -module

$$\Rightarrow I \left(\bigcap_{n=0}^{\infty} I^n M \right) = \bigcap_{n=0}^{\infty} I^{n+1} M$$

pf: $\exists r \in \mathbb{N}$ s.t.

$$I^n (I^r M \cap N) = I^{n+r} M \cap N \quad \forall n \geq r$$

$\parallel$
 $I \cap N$

$\parallel$
 N

q.e.d.

Cor: A : Noetherian semi-local

$\pi = \text{rad}(A)$

M : f.g. A -module

$$\Rightarrow \bigcap_{i=0}^{\infty} \pi^i M = 0$$

Hilbert-Samuel 0

N -graded ring module

Lemma: A noetherian, $I \subseteq A$ an ideal $\Rightarrow \text{gr}_I(A) = \bigoplus_n I^n/I^{n+1}$ is noetherian

Prop: A : Artinian $M = \bigoplus_{n=0}^{\infty} M_n$: finitely generated graded module over $A[x_1, \dots, x_m]$
 $\Rightarrow \exists$ polynomial $f_M(x) \in \mathbb{Q}(x)$ poly ring graded by total degree
 s.t. $f_M(n) = \text{length}_A(M_n)$

pf: Prove this statement $H(M)$ by induction.

- $H(M/M)$ holds trivially

- Suppose N is a submodule of M s.t. $H(M/N')$ holds $\forall$ graded submodule $N' \neq N$

Want to prove $H(M/N)$

If $N = N_1 \cap N_2$ N_1, N_2 : graded $H(M/N_1)$ $H(M/N_2)$

$$0 \rightarrow N_2/N_1 \cap N_2 \rightarrow M/N_1 \cap N_2 \rightarrow M/N_2 \rightarrow 0$$

$\uparrow \cong$

$$0 \rightarrow N_1 + N_2/N_1 \rightarrow M/N_1 \rightarrow M/N_1 + N_2 \rightarrow 0$$

$$\leadsto H(M/N_2) + H(M/N_1) + H(M/N_1 + N_2) \Rightarrow H(N_2 + N_1/N_1) + H(N_2/N_1 \cap N_2) + H(N)$$

- Suppose N is an irreducible submodule of M

$\leadsto N$ is a primary submodule

Hilb-Samuel 1

Def $\text{Num} F = \left\{ f: \mathbb{N} \rightarrow \mathbb{Z} \mid \exists g(x) \in \mathbb{Q}[x] \text{ and } \exists n_0 \in \mathbb{N} \text{ st } \begin{matrix} f(n) = g(n) \\ \forall n \geq n_0 \end{matrix} \right\}$

(V)

Lemma $\text{Num} P = \left\{ f \in \mathbb{Q}[x] \mid \exists n_0(f) \in \mathbb{N} \text{ st } f(n) \in \mathbb{Z} \forall n \geq n_0 \right\}$

$$= \bigoplus_{i \in \mathbb{N}} \mathbb{Z} \cdot \binom{x}{i}$$

$$\binom{x}{i} := \frac{x(x-1)\cdots(x-i+1)}{i!}$$

$\uparrow$
= 1 when $i=0$

$$= \left\{ f \in \mathbb{Q}[x] \mid f(n) \in \mathbb{Z} \forall n \in \mathbb{N} \right\}$$

Pf: induction on $\deg(f)$ of a given $f(x) \in \text{Num}(P)$

Given $f(x) \in \text{Num} P$

$$(\Delta f)(x) \stackrel{\text{def}}{=} f(x+1) - f(x) = \sum_{i=1}^d a_i \binom{x}{i-1}$$

Use. $\binom{x+1}{i} - \binom{x}{i} = \binom{x}{i-1}$

Prop: A = noetherian M : f.g. A -module. The following are equiv:

(1) $\ell(M) < \infty$

(2) $\text{supp}(M) \subseteq \text{Spm}(A)$ (necessarily finitely many)

(3) $\text{Ass}(M) \subseteq \text{Spm}(A)$

Pf (1) $\Rightarrow$ (2) $M = M_1 \supsetneq M_2 \supsetneq \cdots \supsetneq M_m \supsetneq (0)$ $M_i \cong A/P_i$

$\leadsto \text{Supp}(M) = \bigcup \text{supp}(M_i/M_{i+1}) = \{P_1, \dots, P_m\}$ $\nearrow$ max ideal
all max ideals

(2) $\Rightarrow$ (3) Obvious - $\text{Ass}(M) \subseteq \text{supp}(M)$

(3) $\Rightarrow$ (2) $\text{Ass}(M)$ and $\text{supp}(M)$ have the same minimal element

(2) $\Rightarrow$ (1) $M = M_1 \supsetneq M_2 \supsetneq \cdots \supsetneq M_m = (0)$ $M_i/M_{i+1} = A/P_i$ P_i prime

$\leadsto$ Each P_i is a max ideal

Hilb-Samuel 2

Lemma/fact A : Noeth. M : A -module

$$0 \rightarrow M' \rightarrow M \rightarrow M'' \rightarrow 0 \text{ short exact}$$

$$\Rightarrow \begin{cases} l(M) < \infty \Leftrightarrow l(M'), l(M'') < \infty \\ l(M) = l(M') + l(M'') \end{cases}$$

Lemma A : Noeth. M : f.g. A -module

$$J: \text{ideal} \quad l(M/JM) < \infty \Rightarrow l(M/J^n M) < \infty \quad \forall n \in \mathbb{N}$$

$$(\circ) \quad \text{supp}(M/JM) = \text{supp}(M) \cap \text{Spec}(A/JA)$$

Thm (Hilbert) $A = A_0 \oplus A_1 \oplus \dots$ graded, Noetherian

A_0 : artinian, A = generated by $A_0 \otimes A_1$

Assume: A_1 can be generated by r elements as a module over A_0

$M = M_0 \oplus M_1 \oplus \dots$ f.g. graded A -module

Then 1) M_i is a f.g. A_0 -module $\forall i \in \mathbb{N}$

2) $n \mapsto l(M_n)$ is a numerical polynomial for $n \gg 0$
of degree $\leq r-1$

Pf: Induction on r

case $r=0$: easy $x_1, \dots, x_r$ - generators of A_1

$$0 \rightarrow K \rightarrow M \xrightarrow{x_i} M \rightarrow C \rightarrow 0$$

K, C : graded $(A/x_i A)$ -modules $\leadsto$ Can apply induction

$$\Delta l(M_n) = l(M_{n+1}) - l(M_n) = l(C_{n+1}) - l(K_n)$$

q.e.d.

Hilbert-Samuel 3

Prop: A_0 : artinian. $A = A_0[x_1, \dots, x_r]$ polynomial ring
 $M = M_0 \oplus M_1 \oplus \dots$ f.g. graded A -module

Suppose:
$$\ell(M_n) = \sum_{i=0}^{r-1} a_i \binom{n}{i}$$

$$H_0[x_1, \dots, x_n] \otimes_{A_0} M_0 \xrightarrow{\varphi} M \quad \text{the natural map}$$

Assume: φ is surjective i.e. M_0 generates M over A .

Then 1) $a_{r-1} \leq \ell(M_0)$

2) $a_{r-1} = \ell(M_0)$ iff φ is an isomorphism

pf: 1): obvious

2) Suppose $a_{r-1} = \ell(M_0)$

Look at a composition series of M_0

$$M_0 = M_0^0 \supsetneq M_0^1 \supsetneq \dots \supsetneq M_0^r \supsetneq (0)$$

$$M_0^i / M_0^{i+1} \cong k_i \quad k_i = A / \mathfrak{m}_i$$

$$0 \rightarrow K \rightarrow H_0[x_1, \dots, x_n] \otimes_{A_0} M_0 \xrightarrow{\varphi} M \rightarrow 0$$

↓
devisaged into = $k_i[x_1, \dots, x_n]$

If $K \neq 0 \implies$ get a non-trivial A -submodule
of some $k_i[x_1, \dots, x_n]$
corresponding to K .

q.e.d.

Thm (Samuel) A : Noetherian M : f.g. A -module $Q \subseteq A$ ideal
 s.t. $\ell(M/QM) < \infty$. $M = M_0 \supseteq M_1 \supseteq M_2 \supseteq \dots$ Q -good filtration
 Then $n \mapsto \ell(M/M_n)$ is a polynomial for $n \gg 0$, and has the same leading terms as $n \mapsto \ell(M/Q^n M)$

pf: (1) Consider $gr_Q(A) = \bigoplus_{i \geq 0} Q^i / Q^{i+1}$ graded ring
 $gr_*(M) = \bigoplus_{i \geq 0} M_i / M_{i+1}$

Let $\alpha = \text{Ann}_A(M) \sim \text{Supp}(A/Q + \alpha) = \text{Spec}(A/Q + \alpha) = \text{Supp}(M/QM)$

$gr_*(M)$ = fin. gen. $gr_Q(A/\alpha) = \bigoplus_{i \geq 0} (Q^i + \alpha) / (Q^{i+1} + \alpha) \Rightarrow A/(Q + \alpha)$ is Artinian
 - module

$\Rightarrow$ Hilbert $n \mapsto \text{length}(M_n / M_{n+1})$ is a polynomial for $n \gg 0$
 of degree $\leq r-1$ if Q/Q^2 is generated by r elements

Let $g(i) = \text{length}(M/M_i)$

$\Rightarrow (\Delta g)(n) = f(n) \Rightarrow f(n)$ is a polynomial of degree $\leq r$

(2) Consider $g(n) = \ell(M/M_n)$ and $h(n) = \ell(M/Q^n M)$

$\exists n_0$ s.t. $Q^n M \subseteq M_n \subseteq Q^{n-n_0} M \quad \forall n \geq n_0$

$\Rightarrow h(n) \leq g(n) \leq h(n-n_0) \quad \forall n \geq n_0$
 polynomial in n_0 with the same leading term as $h(n)$

QED

Cor. A : Noetherian M : f.g. A -module Q : ideal of A s.t. $\ell(M/QM) < \infty$

$0 \rightarrow M' \rightarrow M \rightarrow M'' \rightarrow 0$ short exact

$\Rightarrow h_Q(M) - h_Q(M') - h_Q(M'') = \text{a poly of degree} < \deg$
 (Here $h_Q(M)(n) = \ell(M/Q^n M) \quad \forall n \gg 0$)

pf: $0 \rightarrow M'/Q^n M \cap M' \rightarrow M/Q^n M \rightarrow M''/Q^n M'' \rightarrow 0$

$(Q^n M \cap M')_{n \in \mathbb{N}}$ is a Q -good filtration on M'

S

q.e.d.

$$(2) \quad d(M) \leq c(M)$$

Suppose $x_1, \dots, x_r \in \mathcal{R}$ and $\ell(M/\sum x_i M) < \infty$, must show $d(M) \leq r$

$$\text{Easy: } d(M) = \deg_{\mathcal{R}} h_{\mathcal{R}}(M) \leq r$$

$$Q = x_1 A + \dots + x_r A$$

$$(M/QM)[x_1, \dots, x_r] \twoheadrightarrow \bigoplus_{i \in \mathbb{N}} Q^i M / Q^{i+1} M$$

$$(3) \quad c(M) \leq \dim(M) \quad \text{induction on } \dim(M) \quad \left((1) \text{ shows: } \dim(M) < \infty \right)$$

Case $\dim(M) = 0$ obvious. Let $P_0 \subsetneq P_1 \subsetneq \dots \subsetneq P_r$ $r = \dim(M)$

chain of prime ideals in $\text{supp}(M)$

Choose $x \in P_1 \setminus \bigcup (\text{minimal elements of } \text{Ass}(M))$

$$\Rightarrow \dim \text{supp}(M/xM) \leq r-1 \quad \text{by construction}$$

$$\text{induction} \Rightarrow c(M/xM) \leq \dim \text{supp}(M/xM) \leq r-1$$

$$\circ \quad c(M) \leq c(M/xM) + 1 \quad \text{by def}^n \text{ of } c(M)$$

$$\Rightarrow c(M) \leq r. \quad \text{q.e.d of (3)}$$

QED

Def: $(A, \mathcal{R})$ noetherian semi-local. M : finite A -module

A system of parameters of M is a sequence of elements

$$x_1, \dots, x_{\dim(M)} \text{ s.t. } \text{length}(M/x_1 M + \dots + x_{\dim(M)} M) < \infty$$

Cor/Exer:

$(A, \mathcal{R})$ semi-local M : finite A -module

$$x_1, \dots, x_r \in \mathcal{R}$$

$$(a) \quad \dim(M/x_1 M + \dots + x_r M) \geq \dim(M) - r$$

(b) $x_1, \dots, x_r$ can be enlarged to a system of parameters of M

$$\iff \dim(M/x_1 M + \dots + x_r M) = \dim(M) - r$$

Hilb-Sam 5

Prop A -noeth. M : f.g. A -module

Q, Q' : ideals of A st. $\text{supp}(M) \cap \text{Spec}(A/Q) = \text{supp}(M) \cap \text{Spec}(A/Q') \subseteq \text{Spm}(A)$

Then $\deg h_Q(M) = \deg h_{Q'}(M)$

Pf: $\exists n_0 \in \mathbb{N}$ st. for $\mathcal{O}_M := \text{Ann}_A(M)$

$$(\mathcal{O}_M + Q)^{n_0} \subseteq (\mathcal{O}_M + Q') \quad \text{and} \quad (\mathcal{O}_M + Q')^{n_0} \subseteq \mathcal{O}_M + Q$$

$$\Rightarrow h_{Q'}(M)(n) \leq h_Q(M)(n \cdot n_0) \quad \forall n \gg 0$$

$$h_Q(M)(n) \leq h_{Q'}(M)(n \cdot n_0)$$

q.e.d.

Def: $(A, \mathfrak{m})$: semi-local Noetherian

M : f.g. A -module

1) $d(M) := \deg h_Q(n) \quad n \gg 0 \quad \text{for any/every ideal } Q \text{ st. } \sqrt{Q} = \mathfrak{m}$

2) $c(M) := \min \{ r \in \mathbb{N} \mid \exists x_1, \dots, x_r \in M \text{ st. } \ell(M/(x_1 M + \dots + x_r M)) < \infty \}$

3) $\dim(M) = \dim(A/\text{Ann}(M)) = \dim(\text{supp}(M)) = \sup_{\mathfrak{p} \in \text{Ass}(M)} \dim(A/\mathfrak{p})$

Thm: $(A, \mathfrak{m})$ semi-local. Then $\dim(M) = d(M) = c(M)$

Pf: (1) $\dim(M) \leq d(M)$ (2) $d(M) \leq c(M)$ (3) $c(M) \leq \dim(M)$

(1) $\dim(M) \leq d(M)$ induction on $d(M)$, case $d(M)=0$ obvious

Must show: $\forall$ minimal element $\mathfrak{p}$ in $\text{Ass}(M)$, $\dim(A/\mathfrak{p}) \leq d(M)$

Since $A/\mathfrak{p} \hookrightarrow M$ suffices to show $\dim(A/\mathfrak{p}) \leq \dim(A/\mathfrak{p})$

Must show: $\forall \mathfrak{p} = \mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \dots \subsetneq \mathfrak{p}_r$ chain of prime ideals $\mathfrak{p} = \text{minimal elt in } \text{Ass}(M)$

have $r \leq d(A/\mathfrak{p})$ Pick $x \in \mathfrak{p}_1 \setminus \mathfrak{p}_0 = \mathfrak{p}$

$$\text{clearly } r-1 \leq \dim \text{supp}(A/\mathfrak{p}_0 + Ax)$$

$$\begin{cases} 0 \rightarrow A/\mathfrak{p} \xrightarrow{x} A/\mathfrak{p} \rightarrow A/\mathfrak{p} + Ax \rightarrow 0 \end{cases} \quad \text{So cor on HS 4} \Rightarrow d(A/\mathfrak{p} + Ax) \leq d(A/\mathfrak{p}) - 1$$

$\hookrightarrow$ induction: $\dim \text{supp}(A/\mathfrak{p}_0 + Ax) \leq d(A/\mathfrak{p}_0) - 1$

$$\Rightarrow r \leq d(A/\mathfrak{p}) \quad \text{q.e.d. for (1)}$$

Cor

(Generalized principal ideal theorem):

A = noetherian $a_1, \dots, a_n \in A$, $I = (a_1, \dots, a_n)$

Then $\text{ht}(P) \leq n$ for every minimal elt of $\text{supp}(A/I)$

In particular: $\text{ht}(I) \leq n$

$$\text{pf: } \underset{\substack{\uparrow \\ \text{for } A_{\mathfrak{p}}}}{C(A_{\mathfrak{p}}/(a_1 A_{\mathfrak{p}} + \dots + a_n A_{\mathfrak{p}}))} = 0 \quad \text{dim}^{\parallel}(A_{\mathfrak{p}}/a_1 A_{\mathfrak{p}} + \dots + a_n A_{\mathfrak{p}})$$

Cor (principal ideal thm) case: $n=1$ above

In particular, for every non-zero divisor $a \in A$, every min. elt of $\text{Spec}(A/aA)$ is a ht one prime.

Note For an ideal J of A ,

$$\text{ht}(J) = \text{Min} \{ \text{ht}(P) \mid P \text{ is a minimal elt of } \text{Spec}(A/J) \}$$

Thus $\text{ht}(J) \leq n$ is weaker than: $\text{ht}(P) \leq n \quad \forall \text{ minimal elt } P \text{ of } \text{Spec}(A/J)$

Prop: A = noetherian ring

$$\Rightarrow \dim A[x] = \dim(A) + 1$$

pf: - May assume: $\dim(A) < \infty$.

[- May assume: A is local, $\mathfrak{m} = \text{max ideal of } A$]

- $\dim A[x] \geq \dim A + 1$ obvious

- To show: $\dim(A[x]) \leq \dim A + 1$.

Given $P \in \text{Spec } A[x]$, let $\mathfrak{p} = P \cap A$: $A[x]_{\mathfrak{p}} = A_{\mathfrak{p}}[x]_{\mathfrak{p}A[x]}$

$\Rightarrow$ May assume: A local with maximal ideal $\mathfrak{m}$ and $P \cap A = \mathfrak{m}$

$$A[x]_{\mathfrak{p}} / \mathfrak{m} A[x]_{\mathfrak{p}} = (A/\mathfrak{m})[x], \quad \exists f \in P \text{ st. } P = \mathfrak{m} A[x] + f A[x]$$

Let $a_1, \dots, a_{\dim(A)}$ be a system of parameters of A

$\Rightarrow a_1, \dots, a_{\dim(A)}, f$ is a system of parameters of $A[x]_{\mathfrak{p}}$

Hilb-Sam 8

Prop/
Exer

$(A, \mathfrak{m})$ noetherian local $x_1, \dots, x_d$ a system of parameters in $\mathfrak{m}$

Then

$$1) \alpha = (A/\mathfrak{m})[x_1, \dots, x_d] \xrightarrow{\sim} \bigoplus_{n \geq 0} \frac{I^n}{I^n \mathfrak{m}} = \left(\bigoplus_{n \geq 0} \frac{I^n}{I^{n+1}} \right) \otimes_{A/I} A/\mathfrak{m}$$

$$x_i \mapsto x_i + I \mathfrak{m} \quad I = (x_1, \dots, x_d)$$

$\uparrow$
in degree 1

is a graded ring isom.

2) If $k \hookrightarrow A$, k is a field, then $x_1, \dots, x_d$ are alg. indep. over k

3) Suppose k is a field, K is a field extⁿ of k st. $\text{tr.deg}(K/k) = d < \infty$,
and $k \subset A \subset K$ (ie. A is a k -subalg. of K)

Then $\dim(A) \leq d$ (Not assuming A to be noetherian)

pf: Suppose $P_0 \subsetneq \dots \subsetneq P_{d+1}$

Pick $x_1 \in P_1 \setminus P_0, \dots, x_{d+1} \in P_{d+1} \setminus P_d$ Consider $B := k[x_1, \dots, x_{d+1}]$

and $\mathfrak{p}_i = P_i \cap B$ $i=0, \dots, d+1$, Then $x_i \in \mathfrak{p}_i \setminus \mathfrak{p}_{i-1}$ $\forall i=1, \dots, d+1$

$\Rightarrow \mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \dots \subsetneq \mathfrak{p}_{d+1}$ prime ideals of B $\leftarrow$ Noetherian.

Definition For $(A, \mathfrak{m})$ Noetherian semi-local $M =$ finite A -module

$$\mathfrak{Q} \subseteq \mathfrak{m} \quad \sqrt{\mathfrak{Q}} = \mathfrak{m}$$

$$d = \dim(M)$$

Define the multiplicity $e(\mathfrak{Q}, M)$ M wr.t $\mathfrak{Q}$ by

$$h_{\mathfrak{Q}}(M)(x) = e(\mathfrak{Q}, M) \cdot \frac{x^d}{d!} + (\text{poly. of degree} \leq d-1)$$

$$\text{i.e. } l(M/\mathfrak{Q}^n M) = e(\mathfrak{Q}, M) \cdot \frac{n^d}{d!} + (\text{poly in } n \text{ of degree} \leq d-1)$$

for $n \gg 0$

Hilb-Sam 9

Lemma $(A, \mathfrak{r})$ semi-local Noetherian $\mathcal{Q}$ ideal st. $\text{rad}(\mathcal{Q}) = \mathfrak{r}$,
 Then $M \mapsto e_{\mathcal{Q}}(M)$ is an additive function on the abel.
 category of f.g. A -modules

Lemma $(A, \mathfrak{r})$ semi-local Noeth, $\mathcal{Q}$ = an ideal of def^n , i.e. $\text{rad}(\mathcal{Q}) = \mathfrak{r}$

1) M = f.g. A -module Let $d = \dim(M)$

Then

$$e(\mathcal{Q}, M) = \sum_{\substack{P \in \text{Ass}(M) \\ \dim(A/P) = d}} e_{A/P}(\mathcal{Q} + P/P, A/P) \cdot \text{length}_{A/P}(M_P)$$

↑
 multiplicity of the
 (A/P) -module A/P
 w.r.t $\mathcal{Q} + P/P \subseteq A/P$

General def^n of ideal of $\text{def}^n \mathcal{Q}$
 of a ring A = ideal ring $(A, \mathfrak{r})$:

- 1) $\mathcal{Q} \subseteq \text{rad}(A)$
- 2) $\exists n \in \mathbb{N}$ st $\text{rad}(A)^n \subseteq \mathcal{Q}$

Poincaré series: $\mathbb{Z}[[T]][\frac{1}{T}]$

Lemma 1: $A = A_0[X_1, \dots, X_n]$ graded, $\deg(X_i) = d_i$, A_0 = Artinian

$$M = \text{graded } A\text{-module of finite type} \\ = \bigoplus_{n \in \mathbb{Z}} M_n$$

$$\leadsto P_M(T) = \sum_{m \in \mathbb{Z}} \text{length}_{A_0}(M_m) \cdot T^m \in \mathbb{Z}[T, T^{-1}, (1-T^{d_1})^{-1}, \dots, (1-T^{d_n})^{-1}] \subseteq \mathbb{Z}[[T]][\frac{1}{T}]$$

Poincaré series for M

$\in \mathbb{Z}[T, (1-T^{d_1})^{-1}, \dots, (1-T^{d_n})^{-1}]$
if $M_m = 0 \quad \forall m < 0$

Will focus (mostly) on the case $d_1 = \dots = d_n = 1$.

O_X

Lemma 2: $F(T) \in \mathbb{Z}[T, T^{-1}, (1-T)^{-1}]$ $F(T) \geq 0$ in the sense that $a_i \geq 0 \quad \forall i$

$$\sum_{n \geq n_0} a_n T^n$$

Write $F(T) = (1-T)^{-d} \cdot Q(T) \quad Q(T) \in \mathbb{Z}[T, T^{-1}], \quad Q(1) \neq 0$

$d \geq 0$

Note d is uniquely determined by $F(T)$.

$$d = \min \{ r \in \mathbb{N} \mid (1-T)^r F(T) \in \mathbb{Z}[T, T^{-1}] \}$$

If $F(T) \geq 0$ in the sense that $a_i \geq 0 \quad \forall i \in \mathbb{Z}$, then $Q(1) > 0$

Write $Q(T) = \sum_{j \in \mathbb{Z}} b_j T^j$ $b_j \neq 0$ for only finitely many j 's

$$(1-T)^{-d} = \sum_{m \geq 0} \binom{m+d-1}{d-1} T^m \leadsto F(T) = (1-T)^{-d} Q(T) \\ = \sum_n \left(\sum_{j \leq n} b_j \binom{n-j+d-1}{d-1} \right) \cdot T^n$$

polynomial of degree $\leq d-1$

coeff of T^{d-1} is $\frac{1}{(d-1)!} \sum_j b_j = \frac{1}{(d-1)!} Q(1)$

Lemma 3 $F_1(T), F_2(T) \in \mathbb{Z}[T, T^{-1}, (1-T)^{-1}]$ $F_1(T) - F_2(T) \geq 0$
 $\begin{matrix} 0 & & 0 \end{matrix}$
 i.e. all coeff. of $F_1(T) - F_2(T)$ are ≥ 0

$$F_i = (1-T)^{-d_i} Q_i(T), \quad Q_i(T) \in \mathbb{Z}[T, T^{-1}], \quad Q_i(1) \neq 0$$

Then: either $d_1 > d_2$, or $d_1 = d_2$ and $Q_1(1) > Q_2(1)$

Lemma 4 (Trivial estimate 1) the HS-series of a quotient filtered module

$M = A$ -module

$(P_n)_{n \in \mathbb{Z}}$ decreasing filtration of M $P_n \supseteq P_{n+1} \quad \forall n$ $Q_n = M$ for some $n \in \mathbb{Z}$
 $(Q_n)_{n \in \mathbb{Z}}$

$$l_A(P_n/Q_n) < \infty \quad \forall n \quad \left[\text{look at } Q_n \subseteq P_{n+1} \cap Q_n \subseteq P_{n+1} \right]$$

Then

$$\sum_n l((P_{n+1} \cap Q_n)/Q_{n+1}) \cdot T^n \leq \sum_n l(P_{n+1}/Q_{n+1}) T^n \leq (1-T) \sum_n l((P_{n+1} \cap Q_n)/Q_{n+1}) T^n$$

① ②

pf ①: obvious

$$\textcircled{2} \Leftrightarrow l(P_{n+1}/Q_{n+1}) \leq \sum_{i \leq n} l((P_{i+1} \cap Q_i)/Q_{i+1})$$

$$\sum_{i \leq n} (P_{n+1} \cap Q_i) / (P_{n+1} \cap Q_{i+1}) \quad \hookrightarrow \quad (P_{i+1} \cap Q_i) / Q_{i+1}$$

Lemma 5 (Trivial estimate 2) $M = A$ -module (F_n) decreasing filtration on M $\forall i \leq n$
 $\exists \delta \in \mathbb{Z} \delta = M \Rightarrow M$ endom. s.t. $f(M_i) \subseteq M_{i+\delta} \quad \forall i$ $\exists i_0$ s.t. $F_{i_0} = M$ $l(F_i/F_{i+1}) < \infty \quad \forall i$

$$H_M = \sum_n l(F_n/F_{n+1}) \cdot T^n \quad \text{HS-series for } M \quad M' = \text{Ker}(f), \quad M'' = M/M'$$

$$H_{M'} = \sum_n l((F_n \cap M')/(F_{n+1} \cap M')) \cdot T^n \quad \varphi: \text{gr}(M) \rightarrow \text{gr}(M) \text{ induced by } f$$

$$M_i/M_{i+1} \rightarrow M_{i+\delta}/M_{i+\delta+1}$$

$$H_{M''} = \sum_n l((F_n + M')/(F_{n+1} + M')) \cdot T^n$$

$$0 \rightarrow (F_n \cap M') \rightarrow F_n/F_{n+1} \rightarrow F_n + M' / F_{n+1} + M' \rightarrow 0$$

Let $P_{\text{Ker}(\varphi)} = \sum_n l(\text{Ker}(\varphi_n)) \cdot T^n$ Poincaré series for $\text{Ker}(\varphi_n) \subseteq \text{gr}_n M$ exact

(1) $H_{M''} \leq P_{\text{Ker}(\varphi)}$

(2) $(1-T^\delta) \cdot (1-T)^{-1} H_M + T^\delta \cdot P_{\text{Ker}(\varphi)} \leq (1-T)^{-1} H_{M''} \leq (1-T^\delta)(1-T)^{-1} H_M + T^\delta(1-T)^{-1} P_{\text{Ker}(\varphi)}$
 (a) (b)

HS12

$$\text{Let } G_n = f^{-1}(F_{n+\delta})$$

$$\text{pf. (1)} \quad P_{\text{Ker}(\varphi)} = \sum_n \ell((G_{n+1} \cap F_n)/F_{n+1}) T^n$$

$$H_{M'} = \sum \ell((M' \cap F_n)/(M' \cap F_{n+1})) T^n$$

$$M' \cap F^n / M' \cap F_{n+1} \hookrightarrow G_n \cap F^n / F_{n+1} \Rightarrow (1) \text{ proved}$$

(2) Apply Lemma 4 to $G_n \cap F_n \supseteq M' \cap F_n$

$$\leadsto P_{\text{Ker}(\varphi)} \leq \sum_n \ell((G_{n+1} \cap F_n)/F_{n+1}) \cdot T^n \leq (1-T)^{-1} P_{\text{Ker}(\varphi)} \quad (2a)$$

From

$$0 \rightarrow G_{n+1}/F_{n+1} \rightarrow M/F_{n+1} \xrightarrow{f_n} M/F_{n+1+\delta} \rightarrow M/(M' \cap F_{n+1+\delta}) \rightarrow 0$$

$\downarrow \text{is}$
 $M''/F''_{n+1+\delta}$

$$T^{n+\delta} \cdot \ell(M''/F''_{n+1+\delta}) = \ell(M/F_{n+1+\delta}) - \ell(M/F_{n+1}) + \ell(G_{n+1}/F_{n+1})$$

$$\Rightarrow \sum_n \sum_{i \leq n} \ell(F''_{i+\delta}/F''_{i+1+\delta}) T^{n+\delta} = (1-T^\delta) \cdot (1-T)^{-1} H_M + T^\delta \sum_n \ell(G_{n+1}/F_{n+1}) T^n$$

$(1-T)^{-1} H_{M''}$ (2c)

(2a)+(2b)

$$\Rightarrow (1-T^\delta)(1-T)^{-1} H_M + T^\delta P_{\text{Ker}(\varphi)} \leq (1-T)^{-1} H_{M''} \leq (1-T^\delta)(1-T)^{-1} H_M + T^\delta (1-T)^{-1} P_{\text{Ker}(\varphi)}$$

q.e.d.

Corollary 6 (a) $(1-T)^{-1} H_{M''} \geq \frac{(1-T^\delta)}{(1-T)} H_M$

(b) $(1-T)^{-1} H_{M'} = \frac{(1-T^\delta)}{(1-T)} H_M$ iff $\text{Ker}(\varphi) = 0$

If --- holds, then $M' = \text{Ker}(f) \subseteq \bigcap_n F_n$, and

$$0 \rightarrow \text{gr}(M) \xrightarrow{\varphi} \text{gr}(M) \rightarrow \text{gr}(M'') \rightarrow 0 \text{ is exact}$$

Lemma 5. M : A -module $F_\bullet$: decreasing filtration s.t. $\ell_A(F_i/F_{i+1}) < \infty \forall i$
 $f: M \rightarrow M$ $f(M_i) \subseteq f(M_{i+5}) \forall i \in \mathbb{Z}$ and $F_{i_0} = M$ for some $i_0 \in \mathbb{Z}$

$\varphi: \text{gr}(M) \rightarrow \text{gr}(M)$ induced by f , homog. of degree 5

Let $M' = \text{Ker}(M)$, $M'' = M/M' = \text{co-image of } f$

Give M' , M'' the induced filtration $(M' \cap F_i)_{i \in \mathbb{Z}}$, $(F_i + M'/M')_{i \in \mathbb{Z}}$

$$\text{Let } H_M = \sum_n \ell(F_n/F_{n+1}) T^n$$

associated Poincaré series

$$H_{M'} = \sum_n \ell((F_n \cap M')/(F_{n+1} \cap M')) T^n$$

$$H_{M''} = \sum_n \ell((F_n + M')/(F_{n+1} + M')) T^n$$

$$\text{Let } G_n = f^{-1}(F_{n+5})$$

$\text{Ker}(\varphi) \subseteq \text{gr}(M)$, graded submodule

$$\text{Ker}(\varphi)_n = \text{Ker}(\varphi)_n = G_{n+1} \cap F_n / F_{n+1} \subseteq F_n / F_{n+1}$$

$$\text{Let } P_{\text{Ker}(\varphi)} = \sum_n \ell(\text{Ker}(\varphi)_n) T^n = \sum_n \ell((G_{n+1} \cap F_n)/F_{n+1}) T^n$$

Then

$$(1) H_{M''} \leq P_{\text{Ker}(\varphi)}$$

$$(2) \begin{aligned} (1-T)^5 \cdot (1-T)^{-1} \cdot H_M + T^5 P_{\text{Ker}(\varphi)} &\stackrel{(a)}{\leq} (1-T)^{-1} H_{M''} \\ &\stackrel{(b)}{\leq} (1-T)^5 (1-T)^{-1} H_M + T^5 (1-T)^{-1} P_{\text{Ker}(\varphi)} \end{aligned}$$

Pf: (1) means: $\ell((F_n \cap M')/(F_{n+1} \cap M')) \leq \ell(G_{n+1} \cap F_n / F_{n+1}) \quad \forall n$

o.o The map $F_n \cap M' / F_{n+1} \cap M' \longrightarrow G_{n+1} \cap F_n / F_{n+1}$ induced by $M' \hookrightarrow G_{n+1}$ is an injection $\forall n$

Have exact sequence

$$(2) \quad 0 \rightarrow G_{n+1}/F_{n+1} \rightarrow M/F_{n+1} \xrightarrow{f_n} M/F_{n+1+\delta} \rightarrow M/M' + F_{n+1+\delta} \rightarrow 0$$

$$\Rightarrow \ell(M''/F''_{n+\delta}) = \ell(M/F_{n+1+\delta}) - \ell(M/F_{n+1}) + \ell(G_{n+1}/F_{n+1}) \quad \text{--- (c)}$$

$$\sum_n T^{n+\delta} \cdot \text{--- (c)} \\ \sum_n \sum_{i \leq n} \ell(F_{i+\delta}/F''_{i+\delta}) T^{n+\delta} = \sum_n \sum_{i \leq n} \ell(F_{i+\delta}/F_{i+1+\delta}) T^{n+\delta} - \sum_n \sum_{i \leq n} \ell(F_i/F_{i+1}) T^{n+\delta} \\ (1-T)^{-1} \cdot H_{M''} \quad (1-T)^{-1} H_M \quad (1-T)^{-1} \cdot T^\delta \cdot H_M \\ + T^\delta \sum_n \ell(G_{n+1}/F_{n+1}) T^n$$

$$\Rightarrow (1-T)^{-1} H_{M''} = (1-T)^{-1} \cdot (1-T^\delta) H_M + T^\delta \sum_n \ell(G_{n+1}/F_{n+1}) T^n \quad \text{--- (c)'}$$

$$(2) \Leftrightarrow \text{--- (b)} \quad P_{\text{Ker}(\varphi)} \leq \sum_n \ell(G_{n+1}/F_{n+1}) T^n \stackrel{(b)}{\leq} (1-T)^{-1} P_{\text{Ker} \varphi} \\ \sum_n \ell((G_{n+1} \cap F_n)/F_{n+1}) T^n$$

(a) means: $\ell(G_{n+1} \cap F_n / F_{n+1}) \leq \ell(G_{n+1}/F_{n+1})$, which is obvious $\because G_{n+1} \cap F_n \subseteq G_{n+1}$

(b) means $\ell(G_{n+1}/F_{n+1}) \leq \sum_{i \leq n} \ell((G_{i+1} \cap F_i)/F_{i+1}) \quad \forall n \quad \text{--- (b)'}$

Recall $G_n = f^{-1}(F_{n+\delta})$

Filter G_{n+1}/F_{n+1} by: $(G_{i+1} \cap F_i / F_{i+1})_{i \leq n+1}$

$$\Rightarrow \ell(G_{n+1}/F_{n+1}) = \sum_{i \leq n} \ell((G_{i+1} \cap F_i)/(G_{n+1} \cap F_{i+1})) \quad \text{--- (d)}$$

Have $(G_{n+1} \cap F_i)/(G_{n+1} \cap F_{i+1}) \hookrightarrow (G_{i+1} \cap F_i)/F_{i+1} \quad \forall i \leq n$

So (d) $\Rightarrow \ell(G_{n+1}/F_{n+1}) \leq \sum_{i \leq n} \ell((G_{i+1} \cap F_i)/F_{i+1})$, which is (b)'.

QED

HS 13

Prop 7: A = Noetherian $\mathfrak{a}$ ideal M = finite A -module $e(M/\mathfrak{a}M) < \infty$

$$gr(A) = \bigoplus_{n \geq 0} \mathfrak{a}^n / \mathfrak{a}^{n+1}$$

$$x_1, \dots, x_s \in \mathfrak{a} \quad x_i \in \mathfrak{a}^{\delta_i} \text{ for } i=1, \dots, s$$

$$\xi_i = x_i \bmod \mathfrak{a}^{\delta_i+1} \in \mathfrak{a}^{\delta_i} / \mathfrak{a}^{\delta_i+1}$$

Let $\bar{M} = M / x_1 M + \dots + x_s M$ with $\mathfrak{a}$ -adic filtration $\leftarrow \bar{F}$

$$(a) \quad H_{\bar{M}, \bar{F}} \geq \prod_{i=1}^s \left(\frac{1-T^{\delta_i}}{1-T} \right) \cdot H_{M, F}$$

M with $\mathfrak{a}$ -adic filtration F

$$(b) \quad H_{\bar{M}, \bar{F}} = \prod_{i=1}^s \left(\frac{1-T^{\delta_i}}{1-T} \right) H_{M, F} \text{ iff}$$

$$\forall i = 0, \dots, s-1$$

$$\left(gr(M) / \left(\xi_1 gr(M) + \dots + \xi_{s-1} gr(M) \right) \xrightarrow{\xi_s} gr(M) / \left(\xi_1 gr(M) + \dots + \xi_s gr(M) \right) \right)$$

is injective

" $(\xi_1, \dots, \xi_s)$ is a regular sequence for $gr(M)$ "
as a $gr(A)$ -module

Prop 8 $(A, \mathfrak{m})$ Noetherian local $x_1, \dots, x_s \in \mathfrak{m}$, $x_i \in \mathfrak{m}^{\delta_i}$ $\xi_i = x_i \bmod \mathfrak{m}^{\delta_i+1} \in \mathfrak{m}^{\delta_i} / \mathfrak{m}^{\delta_i+1}$

Then

$$(a) \quad e(A/x_1 A + \dots + x_s A) \geq \delta_1 \cdots \delta_s \cdot e(A)$$

$$(b) \quad e(A/x_1 A + \dots + x_s A) = \delta_1 \cdots \delta_s \cdot e(A) \text{ if}$$

$\xi_1, \dots, \xi_s$ is a regular sequence for $\bigoplus_{n \geq 0} \mathfrak{m}^n / \mathfrak{m}^{n+1} = gr(A)$

$$Pf \quad (1-T)^{-s} \cdot H_B \geq \prod_{i=1}^s \left(\frac{1-T^{\delta_i}}{1-T} \right) H_A \text{ and equality holds if } \xi_1, \dots, \xi_s$$

is a regular sequence for $gr(A)$

$$l(M/\mathfrak{o}_\alpha M) < \infty$$

Prop 9 $(A, \mathfrak{o}_\alpha)$: Noetherian

M : finite A -module

$$x \in \mathfrak{o}_\alpha^\delta, \quad \xi = x \bmod \mathfrak{o}_\alpha^{\delta+1} \in \mathfrak{o}_\alpha^\delta / \mathfrak{o}_\alpha^{\delta+1} \in \text{gr}_\alpha(A) \quad \varphi = (\text{gr}_\alpha(M) \xrightarrow{\xi} \text{gr}_\alpha(M))$$

(a) $\dim(M/xM) = \text{either } \dim(M) \text{ or } \dim(M)-1$,

and if $\dim(M/xM) = \dim(M)-1$, then $e_\alpha(M/xM) \geq \delta \cdot e_\alpha(M)$

(b) Suppose $\dim(M) \geq 1$ and $l(\text{Ker}(\varphi)) < \infty$, then

$$\dim(M/xM) = \dim(M)-1. \quad \text{Moreover}$$

(b1) If $\dim(M) > 1$, then $e_\alpha(M/xM) = \delta e_\alpha(M)$

(b2) If $\dim(M) = 1$, then

$$n \delta e_\alpha(M) \leq \text{length}_A(M/x^n M) \leq n \delta \cdot e_\alpha(M) + \text{length}_A(\text{Ker } \varphi^n) \quad \forall n$$

therefore

$$\delta \cdot e_\alpha(M) = e_{xA}(M) \leq \text{length}_{M/xM}(M/x^n M) \text{ increasing submodules of } \text{gr}_\alpha(M) \text{ of finite length, hence stabilize as } n \rightarrow \infty$$

Pf: Let $P(T) = \sum_{A/\mathfrak{o}_\alpha} l(\text{Ker}(\varphi_n)) T^n$.

Have

$$T^\delta \cdot P + \frac{1-T^\delta}{1-T} H_M \leq (1-T)^{-1} H_{M/xM} \leq \frac{1-T^\delta}{1-T} H_M + T^\delta \cdot (1-T)^{-1} P$$

(a) and (b1) follow from this estimate

The inequality (b2)

$$\delta \cdot e_\alpha(M) \leq \text{length}(M/xM) \leq \delta \cdot e_\alpha(M) + \text{length}(\text{Ker}(\varphi))$$

$$n \delta e_\alpha(M) \leq \text{length}(M/x^n M) \leq n \cdot \delta e_\alpha(M) + \text{length}(\text{Ker } \varphi^n)$$

Also follows from the inequality of HS poly in (b1): $x \mapsto x^n$

[and remember that $H_{M/xM} \in \mathbb{Z}[T]$, $H_{M/x^n M}(1) = l(M/x^n M)$ evaluate $\forall n$]

Observe that $\text{Ker}(\varphi^n)$ stabilizes as $n \rightarrow \infty$
to a fixed submodule of finite length in $\text{gr}_\alpha(M)$

Thm $(A, \mathfrak{m})$ Noetherian semi-local, M : finite A -module, $\mathfrak{o}_2 \subseteq \mathfrak{m}$
 $x_1, \dots, x_r \in \mathfrak{o}_2$ Let $J = x_1 A + \dots + x_r A$ $\ell(M/\mathfrak{o}_2 M) < \infty$

(a) $\dim(M/JM) \geq \dim(M) - r$

(b) If $\dim(M/JM) = \dim(M) - r$, then $e_{\mathfrak{o}_2}(M/JM) \geq e_{\mathfrak{o}_2}(M)$

(c) If $r < \dim(M)$ and $\forall i=1, \dots, r$, the element x_i is superficial for $M/(x_1 M + \dots + x_{i-1} M)$, then

$\dim(M/JM) = \dim(M) - r$ and $e_{\mathfrak{o}_2}(M/JM) = e_{\mathfrak{o}_2}(M)$

(d) If $r = \dim(M)$ and for $i=1, \dots, r$ the elt x_i is superficial for $M/(x_1 M + \dots + x_{i-1} M)$, then

$e_{\mathfrak{o}_2}(M) = e_J(M) \leq \ell(M/JM) < \infty$

Pf (a), (b), (c) follow from Prop 9 by induction

(d): Let $N = M/(x_1 M + \dots + x_{r-1} M)$ Have $e_{\mathfrak{o}_2}(N) = e_{\mathfrak{o}_2}(M)$

Prop 9 $\Rightarrow$ $e_{\mathfrak{o}_2}(N) = e_{x_r A}(N) \leq \text{length}(N/x_r N) = \ell(M/JM)$

Note $e_{x_r A}(N) = e_J(N)$ by defⁿ

Have $e_J(N) \geq e_J(M)$ by (c)

$\Rightarrow e_J(M) \leq e_J(N) = e_{x_r A}(N) \overset{\text{from Prop 9}}{=} e_{\mathfrak{o}_2}(N) \overset{(c)}{=} e_{\mathfrak{o}_2}(M) \leq e_J(M)$

$\mathfrak{o}_2 \subseteq J$

QED

Zar. 1

Def linear topology, etc.

Terminology in EGA.

Note: Obvious generalization to modules

- 1) linear topology on a commutative ring: $\exists$ a fund system of open nbd of 0 consisting of ideals
- 2) an ideal of defⁿ I of a ring with a linear topology: I is open and $\forall$ open nbd V of 0, $\exists n \in \mathbb{N}$ s.t. $I^n \subseteq V$ (ie. $I^n \rightarrow 0$)
- 3) preadmissible linear topology on A : $\exists$ an ideal of defⁿ
- 4) admissible = pre-admissible and complete separated

Note I = an ideal of defⁿ. I^n may not be open

Fact: A Noetherian & pre-admissible $\Rightarrow \exists$ largest ideal of defⁿ

- 5) A is pre-adic if $\exists$ an ideal of defⁿ I s.t. $(I^n)_{n \in \mathbb{N}}$ form a fund system of neighborhoods of 0
 $(\Leftrightarrow I^n \text{ is open } \forall n \in \mathbb{N})$

- 6) A is adic if it is pre-adic + complete and separated

- completion w.r.t. a linearly topologized ring/module

Lemma A : Noetherian $0 \rightarrow M' \rightarrow M \rightarrow M'' \rightarrow 0$ exact, finite A -modules
 $\Rightarrow 0 \rightarrow \hat{M}' \rightarrow \hat{M} \rightarrow \hat{M}'' \rightarrow 0$ exact I -adic

Cor A : Noetherian, M : finite A -module
 $\Rightarrow \hat{M} \cong M \otimes_A \hat{A}$

Cor $A \rightarrow \hat{A} = I$ -adic completion is flat

Cor: A : I -adically complete $\Rightarrow$ Every submodule $N \subseteq M$
 M : finite A -module is closed

Zar2

Def: Zariski ring = a Noetherian ring with adic topology s.t. every ideal is closed (in the I -adic topology)

Prop: (A, I) is Zariski

$$\Leftrightarrow (ii) I \subseteq \text{rad}(A)$$

$$\Leftrightarrow (iii) \text{ Every finite } A\text{-module is } I\text{-adically separated}$$

$$\Leftrightarrow (iv) \forall \text{ finite } A\text{-module } M, \text{ every submodule is } I\text{-adically closed}$$

$$\Leftrightarrow (v) A \rightarrow \hat{A} \text{ is faithfully flat}$$

show: $(i) \Rightarrow (ii) \Rightarrow (iii) \Rightarrow (iv) \Rightarrow (i)$

Artin-Rees

trivial

$$(i) \Rightarrow (ii)$$

$$N \subseteq M, (iii) \Rightarrow M/N \text{ is separated}$$

If $\mathfrak{m} \subseteq I \Rightarrow \mathfrak{m} + I^n = A \forall n \Rightarrow \mathfrak{m} \text{ is not closed in } A, \text{ Contradiction}$

$$(ii) \Rightarrow (v) \text{ follows from Artin-Rees + NAK}$$

$$(v) \Rightarrow (ii) \text{ Given } \mathfrak{m} = \text{maximal ideal} \text{ Need to show: } I \subseteq \mathfrak{m}$$

$$\hat{A} \xrightarrow{f} A \rightarrow \hat{A} \text{ f.flat} \Rightarrow \exists \overline{M} \subseteq \hat{A} \text{ maximal ideal}$$

$$\text{s.t. } M \cap A = \mathfrak{m}$$

$$1 + I\hat{A} \in \text{rad}(\hat{A}) \Rightarrow I\hat{A} \subseteq M \Rightarrow I \subseteq M \cap A = \mathfrak{m}$$

Ex of Zar. rings: Noeth. semi-local rings, completion of a Noeth. ring w.r.t. an adic topology

Prop: (A, I) = Zariski ring $\hat{A}$ = I -adic completion

(a) $\mathfrak{o} \subseteq A$ ideal. $\mathfrak{o}\hat{A}$ is a principal ideal $\Rightarrow \mathfrak{o}$ is a principal ideal

(b) $\hat{A}$ is normal $\Rightarrow A$ is normal

pf: (b) is a consequence of faithful flatness of $A \rightarrow \hat{A}$

(a): $\mathfrak{o}\hat{A}$ principal $\Rightarrow$ choose α s.t. $\mathfrak{o}\hat{A} \cap I^n \hat{A} \subseteq I\alpha\hat{A}$

$$\alpha \in \hat{A}$$

Write $\alpha = \sum a_i \xi_i$ $a_i \in \mathfrak{o}, \xi_i \in \hat{A}$ approximate ξ_i by elements of A

$$\leadsto \text{Let } a = \sum a_i x_i$$

$$\xi_i \equiv x_i \pmod{I^n \hat{A}}$$

$$\leadsto \alpha = a + \beta \quad \beta \in \mathfrak{o}\hat{A} \cap I^n \hat{A} \subseteq I\alpha\hat{A}$$

$$\Rightarrow \alpha\hat{A} \subseteq \mathfrak{o}\hat{A} + I\alpha\hat{A} \Rightarrow \alpha\hat{A} = \mathfrak{o}\hat{A} \text{ q.e.d.}$$

W1

p : prime

$$\Phi_n(X_0, X_1, \dots, X_n) = X_0^{p^n} + pX_1^{p^{n-1}} + p^2X_2^{p^{n-2}} + \dots + p^{n-1}X_{n-1}^p + p^nX_n$$

$$\Phi_0(X_0) = X_0$$

$$\Phi_1(X_0, X_1) = X_0^p + pX_1$$

$$\Phi_{n-1}(X_0, \dots, X_{n-1}) = X_0^{p^{n-1}} + pX_1^{p^{n-2}} + \dots + p^{n-1}X_{n-1}$$

$$\Phi_2(X_0, X_1, X_2) = X_0^{p^2} + pX_1^p + p^2X_2$$

$$\begin{aligned} \leadsto \Phi_n(X_0, X_1, \dots, X_n) &= \Phi_{n-1}(X_0^p, X_1^p, \dots, X_{n-1}^p) + p^nX_n \\ &= X_0^{p^n} + p\Phi_{n-1}(X_1, \dots, X_n) \end{aligned}$$

Lemma 1 $A = J_0 \supseteq J_1 \supseteq J_2 \supseteq \dots$ decreasing sequence of ideals, $p \in J_1$

$$J_n \cdot J_m \subseteq J_{n+m} \quad \forall m, n \in \mathbb{N}$$

$$(1) \quad a_i \equiv b_i \pmod{J_m} \quad \text{for } i=0, 1, \dots, n$$

$$\Rightarrow \Phi_i(a_0, \dots, a_n) \equiv \Phi_i(b_0, \dots, b_n) \pmod{J_{m+i}} \quad \text{for } i=0, 1, \dots, n$$

$$(2) \quad \text{If } [p] = \bigoplus_{m \geq 0} J_m/J_{m+1} \xrightarrow{\text{w.t. homom.}} \bigoplus_{m \geq 0} J_m/J_{m+1} \text{ is } \underline{\text{injective}}$$

$$\underline{\text{then}}: \quad \text{If } \Phi_i(a_0, \dots, a_n) \equiv \Phi_i(b_0, b_1, \dots, b_n) \pmod{J_{m+i}} \quad \text{for } i=0, 1, \dots, n$$

$$\text{then } a_i \equiv b_i \pmod{J_m} \quad \text{for } i=0, 1, \dots, n$$

pf of (1) Induction on n .

pf of (2) Induction on n .

W2

Lemma 2 A = ring, with p -adic filtration

$\sigma: A \rightarrow A$ ring homom. s.t. $\sigma(a) \equiv a^p \pmod{p} \quad \forall a \in A$

$a_0, \dots, a_{n-1} \in A$

Let $u_i = \Phi_i(a_0, \dots, a_i)$ for $i=0, 1, \dots, n$

Given an element " u_n " $\in A$

$\exists a_n \in A$ s.t. $\Phi_n(a_0, \dots, a_{n-1}, a_n) = u_n$

$$\Leftrightarrow u_n \equiv \sigma(u_{n-1}) \pmod{p^n A}$$

Prop 3: A : ring $\sigma: A \rightarrow A$ lifting of Frobenius

$$\Phi: A^{\mathbb{N}} \rightarrow A^{\mathbb{N}} \\ (a_i)_{i \in \mathbb{N}} \mapsto (\Phi_i(a_0, \dots, a_i))_{i \in \mathbb{N}}$$

$$(u_0, u_1, \dots) = (u_i)_{i \in \mathbb{N}} \in \text{Im}(\Phi)$$

$$\Leftrightarrow u_n \equiv \sigma(u_{n-1}) \pmod{p^n} \quad \forall n.$$

$$f: A^{\mathbb{N}} \rightarrow A^{\mathbb{N}} \quad (b_0, b_1, b_2, \dots) \mapsto (b_1, b_2, \dots)$$

$$v: A^{\mathbb{N}} \rightarrow A^{\mathbb{N}} \quad (b_0, b_1, b_2, \dots) \mapsto (0, pa_0, pa_1, \dots)$$

Properties of Witt vectors

Prop 4 $\Phi: W(\cdot) \rightarrow \mathbb{A}^{\mathbb{N}}$ $a = (a_0, a_1, \dots, a_m, \dots) \mapsto (\Phi_0(a), \Phi_1(a), \Phi_2(a), \dots)$

Have: $S: W(\cdot) \times W(\cdot) \rightarrow W(\cdot)$ functorial maps

$$P: W(\cdot) \times W(\cdot) \rightarrow W(\cdot)$$

$$I: W(\cdot) \times W(\cdot) \rightarrow W(\cdot)$$

$$\text{st. } \Phi(S(a, b)) = \Phi(a) + \Phi(b)$$

$$\Phi(P(a, b)) = \Phi(a) \cdot \Phi(b) \quad \forall a, b$$

$$\Phi(I(a)) = -\Phi(a)$$

so that (W, S, P, I) defines a functor from (Comm. Alg.) to (Rings)

and $\Phi: W \rightarrow \mathbb{A}^{\mathbb{N}}$ is a natural transformation

In addition:

Prop 5 $\Phi \circ F = f \circ \Phi \quad F: W(\cdot) \rightarrow W(\cdot) \text{ ring endomorphisms}$

$$\Phi \circ V = v \circ \Phi \quad V: W(\cdot) \rightarrow W(\cdot) \text{ endom of } (W(\cdot), +)$$

Prop 5: (a) $F_A(V_A(a)) = p \cdot a \quad \forall a \in W(A) \quad \forall \text{ comm. ring } A$

$$(b) \quad V_A(a \cdot F_A(b)) = V_A(a) \cdot b \quad \forall a, b \in W(A)$$

$$(c) \quad V_A(a) \cdot V_A(b) = p \cdot V_A(a \cdot b) \quad \forall a, b \in W(A)$$

$$(d) \quad V_A(F_A(b)) = V_A(1) \cdot b \quad \begin{matrix} 1 = (1, 0, 0, \dots) \in W(A) \\ V_A(1) = (0, 1, 0, 0, \dots) \in W(A) \end{matrix} \quad \forall b \in W(A)$$

$$(e) \quad F_A(a) \equiv a^p \pmod{p} W(A) \quad \forall a \in W(A)$$

Note: (e) is different from: The images of $F_A(a)$ and $(a_0^p, a_1^p, a_2^p, \dots)$ in $W(A/pA)$ are equal.

Pf (b) check $v_B(\xi f_B(\eta)) = v_B(\xi) \cdot \eta \quad \forall \xi, \eta \in \mathbb{A}^{\mathbb{N}} (\mathbb{Z}[x_0, x_1, x_2, \dots; y_0, y_1, y_2, \dots])$

$$\parallel$$

$$v_B(\xi_0 \eta_1, \xi_1 \eta_2, \dots) \stackrel{?}{=} (0, p \xi_0 \eta_1, p \xi_1 \eta_2, \dots)$$

yes

W4

Pf of (c): $V(a) \cdot V(b) = \underset{\substack{\uparrow \\ \text{by (b)}}}{V_A(a \cdot FV(b))} = \underset{\substack{\uparrow \\ \text{by (a)}}}{V_A(a \cdot pb)} = p \cdot V_A(a \cdot b)$

(d) $V_A(F_A(b)) = V_A(1 \cdot F_A(b)) = V_A(1) \cdot b$, $V_A(1) = (0, 1, 0, 0, \dots) \in W(A)$

(e) Suffices to check:

$$f_B(\xi) \equiv \xi^p \pmod{p \Phi_B(W(B))} \quad \forall \xi \in \Phi_B(W(B))$$

Have $\xi = (\xi_0, \xi_1, \dots) \in B^{\mathbb{N}}$, $\sigma(\xi_n) \equiv \xi_{n+1} \pmod{p^{n+1}B} \quad \forall n$

$$f_B(\xi) = (\xi_1, \xi_2, \dots)$$

$$f_B(\xi) \equiv \xi^p \pmod{p \Phi_B(W(B))} \text{ means:}$$

$$\sigma(\xi_{n+1} - \xi_n^p) - (\xi_{n+2} - \xi_{n+1}^p) \equiv 0 \pmod{p^{n+2}B} \quad \forall n$$

This congruence follows from the condition that $\sigma(\xi_n) - \xi_{n+1} \equiv 0 \pmod{p^{n+1}B} \quad \forall n$
QED

Defⁿ: $\tau_A: A \rightarrow W(A) \quad a \mapsto (a, 0, 0, 0, \dots) \quad \forall a \in A$
(Teichmüller map)

Prop 6: (a) $\tau(ab) = \tau(a) \cdot \tau(b) \quad \forall a, b \in A$ ($\tau_A: A \rightarrow W(A)$ is "multiplicative")

(b) $\tau(a) \cdot x = (a^{p^n} x_n) \quad \forall a \in A, \forall x = (x_0, x_1, x_2, \dots) \in W(A)$

(c) $(a_0, a_1, \dots) = \sum_{n \geq 0} V^n(\tau(a_n)) \quad \forall a_0, a_1, \dots \in A$
(Exercise)

Defⁿ a) $\forall$ commutative ring A , $\forall n \in \mathbb{N}$

define the V -adic filtration $(V_m(A))_{m \geq 0}$ on $W(A)$ by:

$$V_m(A) := V^m(W(A))$$

Note: $V_m(a) \cdot b = V_m(a \cdot F^m(b)) \quad \forall a, b \in W(A)$

$\Rightarrow V_m(A)$ is an ideal of $W(A)$

This filtration defines a topology on $W(A)$, called the V -adic topology

b) Define $\forall m \in \mathbb{N}_{\geq 1}$, $W_m(A) := W(A)/V^m(W(A))$

$$\{ [a_0, \dots, a_{m-1}] = a_0, a_1, \dots, a_{m-1} \in A \}$$

$W_m(A)$ is a commutative ring.

Defⁿ a) Define $V_m^n: W_m(A) \longrightarrow W_{m+n}(A)$ $\forall m \geq 1, \forall n \geq 0$

$$\begin{array}{ccc} W(A) & \xrightarrow{V^n} & W(A) \\ \downarrow \pi_m & & \downarrow \pi_{m+n} \\ W_m(A) & \xrightarrow{V_m^n} & W_{m+n}(A) \end{array}$$

b) Define $F_m^n: W_{m+n}(A) \longrightarrow W_m(A)$ $\forall m \geq 1, \forall n \geq 0$

$$\begin{array}{ccc} W(A) & \xrightarrow{F^n} & W(A) \\ \downarrow \pi_{m+n} & & \downarrow \pi_m \\ W_{m+n}(A) & \xrightarrow{F_m^n} & W_m(A) \end{array}$$

Note $F(V_{m+1}(A)) \subseteq V_m(A)$
 $\circ \circ F(V^{n+1}(\underline{a})) = p \cdot V^m(\underline{a})$
 $\forall \underline{a} \in W(A)$

Lemma: $V_1(A)^k = p^{k-1} V_1(A) \subseteq V^k(W(A))$ $\forall k \geq 1$

($V(\underline{a}) \cdot V(\underline{b}) = p V(\underline{a} \cdot \underline{b}) \quad \forall \underline{a}, \underline{b} \in W(A)$, by Prop 5 (c), plus induction)

Prop 7. Suppose that $p \cdot 1_A = 0$ in A

(a) $F\underline{a} = (a_n^p)_{n \in \mathbb{Z}}$ $\forall \underline{a} \in W(A)$

(b) $p \cdot \underline{a} = VF(\underline{a}) = FV(\underline{a}) = (0, a_0^p, a_1^p, \dots)$ $\forall \underline{a} = (a_0, a_1, a_2, \dots) \in W(A)$

(c) $V^m(\underline{a}) \cdot V^n(\underline{b}) = V^{m+n}(F^n(\underline{a}) \cdot F^m(\underline{b}))$ $\forall \underline{a}, \underline{b} \in W(A)$

Pf. (a) $\Leftrightarrow F_n(\underline{x}) \equiv x_n^p \pmod{p}$ in $\mathbb{Z}[x_0, x_1, \dots]$ $\forall n$ $F(\underline{x}) = (F_0(\underline{x}), F_1(\underline{x}), F_2(\underline{x}), \dots) \in W(\mathbb{Z}[x_0, x_1, x_2, \dots])$

This congruence is equivalent to:

$$\Phi_m(F(\underline{x})) \equiv \Phi_m(x_0^p, x_1^p, x_2^p, \dots) \pmod{p^{m+1} \mathbb{Z}[x_0, x_1, x_2, \dots]} \quad \forall m$$

//

$$\Phi_{m+1}(\underline{x}) = \Phi_m(x_0^p, x_1^p, \dots, x_m^p) + p^{m+1} x_{m+1}$$

(b) follows from (a).

$$\begin{aligned} \text{(c)} \quad V^m(\underline{a}) \cdot V^n(\underline{b}) &= V^m(\underline{a} \cdot F^n V^n(\underline{b})) \xrightarrow{FV=VF} V^m(\underline{a} \cdot V^n F^n(\underline{b})) = V^m(V^n(F^n(\underline{a}) \cdot F^m(\underline{b}))) \\ &= V^{m+n}(F^n(\underline{a}) \cdot F^m(\underline{b})) \end{aligned}$$

Prop 8 (1) The $V_1(A)$ -adic topology on $W(A)$ is finer than the p -adic topology on $W(A)$ ($\cap_{k=1}^{\infty} V_1(A)^k \subseteq p^{k-1} W(A) \quad \forall k \geq 1$)

(2) Suppose that $p \cdot 1_A = 0$ in A .

(2a) The $V_1(A)$ -adic topology on $W(A)$ coincides with the p -adic topology

(2b) The p -adic topology on $W(A)$ is finer than the V -adic topology on $W(A)$

(2c) $W(A)$ is complete and separated w.r.t. the p -adic topology

pf (2a): $p^k W(A) \subseteq V_1(A)^k \subseteq p^{k-1} W(A)$

(2b): $p^m W(A) \subseteq V^m(W(A))$

Prop 9. Suppose that A is perfect of characteristic $p > 0$, i.e. $p \cdot 1_A = 0$ and $F_p: A \xrightarrow{\sim} A$.

(a) $\forall a = (a_0, a_1, \dots, a_n, \dots) \in W(A), \quad a = \sum_{n \geq 0} p^n \zeta(a_n^{p^n})$

(b) The three topologies on $W(A)$: p -adic, V -adic, $V_1(A)$ -adic coincide

In particular, $V_n(A) = p^n W(A) = (V_1(A))^n \quad \forall n \geq 1$

(c) $W(A)/p W(A) \xrightarrow{\sim} A$

Prop 10 Suppose that A is a perfect field of characteristic $p > 0$.

Then $W(A)$ is a discrete valuation ring with maximal ideal $p \cdot W(A)$ and residue field A .

(Exer)

Cohen 1

p-ring

Def 1 A p-ring is a commutative ring C such that $p \cdot C$ is a maximal ideal of C and C is complete and separated for the p -adic topology.

Prop 1 Let C be a p-ring (0) Every element of C is of the form $p^n \cdot u$, with $n \in \mathbb{N}$, $u \in C^\times$.

(1) C is a local ring with maximal ideal pC

(2) Suppose $p \cdot 1_C$ is nilpotent. Let $d =$ the smallest natural number s.t. $p^d \cdot 1_C = 0$

Then every ideal of C is of the form $p^k C$ for some k with $0 \leq k \leq d$.

Moreover $p^k C \neq p^l C \quad \forall k \neq l, 1 \leq k, l \leq d$, and $\text{length}_C(C) = d$

(3) Suppose $p \cdot 1_C$ is not unipotent. Then C is a DVR of mixed characteristics $(0, p)$.

The ideals of C are of the form $p^n C$, $n \in \mathbb{N}$: $p^n C \neq p^m C$ if $n \neq m$, $\text{length}_C(C) = \infty$

pf: (0), (1): exercise $\circ \circ \bigcap_{n \in \mathbb{N}} p^n C = (0)$

(2) $C \supseteq pC \supseteq \dots \supseteq p^{d-1}C \supseteq p^d C = (0)$

Note: $p^i C \not\subseteq p^{i+1} C$ for $i=0, 1, \dots, d-1$. If $p^i C = p^{i+1} C \quad i \leq d-1 \Rightarrow p^{d-1} C = p^{d-1-i} \cdot p^i C = p^{d-i} \cdot p^i C = p^d C = (0)$

Let I be an ideal of C , and let k be the smallest natural number s.t. $I \supseteq p^k C$.

Claim: $I = p^k C$: Given any $x \in I$, write $x = p^m u$, $u \in C^\times \Rightarrow p^m C \subseteq I \Rightarrow m \geq k \Rightarrow x \in p^k C$

$\text{length}_C(C) = d \quad \circ \circ \quad p^i C / p^{i+1} C \cong C / pC$ as C -modules.

(3) Immediate from defⁿ of DVR.

Remark: Prop 1 shows: p-rings which are domains = absolutely unramified complete dvrs

Will see: p-rings which are not domains = quotient rings of abs. unramified complete dvrs by (p^d) , $d \in \mathbb{N}_{\geq 1}$

Prop 2 Let $u: C \rightarrow C'$ be a ring homom. of p-rings, $\kappa_C = C/pC$, $\kappa_{C'} = C'/pC'$

(a) $\ell(C) \geq \ell(C')$; $\ell(C) = \ell(C')$ iff u is injective $v: \kappa_C \rightarrow \kappa_{C'}$ induced by u .

(b) u is surjective iff $v: \kappa_C \xrightarrow{\sim} \kappa_{C'}$

(c) u is an isom iff $v: \kappa_C \xrightarrow{\sim} \kappa_{C'}$ and $\ell(C) = \ell(C')$

Note (a) + (b) $\Rightarrow$ (c) trivially.

Cohen 2

Pf (a)
$$\left. \begin{array}{l} p^{n+1}1_{C'} \neq 0 \Rightarrow p^{n+1}1_C \neq 0 \\ \Leftrightarrow u \text{ is injective} \end{array} \right\} \Rightarrow l(C') \leq l(C) \text{ and } l(C') = l(C) \text{ if } u \text{ is injective}$$

(b) : dévissage, $(p^n C)_{0 \leq n \leq d} \rightarrow (p^m C')_{0 \leq m \leq d'} \quad d' = l(C') \leq l(C) = d$

Prop 3 $(C_m, \pi_{n,m}: C_m \rightarrow C_n)$ a projective system of p-rings indexed by $\mathbb{N}$

s.t. $\pi_{n,m}: C_m \twoheadrightarrow C_n \quad \forall m \geq n$

Then $C := \varprojlim_{\leftarrow m} C_m$ is a p-ring, and $\pi_n: C \twoheadrightarrow C_n \quad \forall n$
(exer.) inducing an isom $\kappa_C \xrightarrow{\sim} \kappa_{C_m}$

Defⁿ Let $(A, \mathfrak{m}_A)$ be a complete separated local ring (not nec. Noetherian) such that $\kappa_A := A/\mathfrak{m}_A$ is a field of characteristic $p > 0$.

A Cohen subring of A is a ^{local} subring $C \subseteq A$ which is a p-ring such that $A = \mathfrak{m}_A + C$; i.e. $C/\mathfrak{m}_A \cap C \stackrel{\kappa_C}{=} C/pC \xrightarrow{\sim} A/\mathfrak{m}_A \stackrel{\kappa_A}{=}$

Example: C : a p-ring $\Rightarrow C$ is a Cohen subring of $C[[X_1, \dots, X_n]]$

Theorem 4 (Existence of Cohen subring in complete local rings)

Let $(A, \mathfrak{m}_A)$ be a complete separated local ring s.t. $\kappa = A/\mathfrak{m}_A \cong \mathbb{F}_p$.

Let $S \subseteq A$ be a subset of A s.t. $\pi: A \rightarrow \kappa$ induces a bijection $S \xrightarrow{\sim} \pi(S) \subseteq \kappa$ and $\pi(S)$ is a p-basis of κ .

(a) $\exists!$ Cohen subring $C \subseteq A$ containing S

(b) C is closed in A , and the $\mathfrak{m}_A$ -adic topology of A induces the p-adic topology on C

(c) Every closed subring $A' \subseteq A$ such that $A' \supseteq S$ and $A' + \mathfrak{m}_A = A$ contains C

Will first prove Thm 4 when $\mathfrak{m}_A$ is nilpotent. Then deduce the general case from this special case

Cohen 3

Pf of Thm 4

Part I. Case when $\pi_A^{n+1} = (0)$, $n \in \mathbb{N}$

Let $B_n = \text{Im} \left(\Phi_n: W_{n+1}(A) \rightarrow A \right) \subseteq A$
 $[a_0, a_1, \dots, a_n] \mapsto \sum_{i=0}^n p^i a_i^{p^{n-i}}$

Define $C_n :=$ the subring generated by $S \cup B_n$

Lemma 1 Let $A' \subseteq A$ be a subring of A s.t. $A' \geq S$. Then $A' \geq C_n \iff A' + \pi_A^n = A$

pf of Lemma 1: " $\Rightarrow$ ": $\pi(B_n) = \kappa^{p^n} \rightsquigarrow \pi(C_n) = \kappa^{p^n}[\pi(S)] = \kappa$

" $\Leftarrow$ ": Suppose $A' + \pi_A^n = A \quad \forall a_0, a_1, \dots, a_n \in A$, pick $a'_0, a'_1, \dots, a'_n \in A'$ s.t. $a'_i \equiv a_i \pmod{\pi_A^n}$ $\forall i=0,1,\dots,n$
 $\rightsquigarrow \Phi_n(a_0, a_1, \dots, a_n) \equiv \Phi_n(a'_0, a'_1, \dots, a'_n) \pmod{\pi_A^n} \in A' \Rightarrow A' \geq B_n$ q.e.d.
 $\because$ they are $\equiv \pmod{\pi_A^{n+1}}$

Let $\mathcal{C} = \{ \text{subrings } A' \subseteq A \text{ s.t. } A' \geq S \text{ and } A' + \pi_A^n = A \}$

$\uparrow$ $\{ \text{subrings } A' \subseteq A \text{ s.t. } A' \geq S \cup B_n \} \ni C_n = \text{the unique minimal element in } \mathcal{C}$
Lemma 1 !!

Must show: pC is a maximal ideal of A

Lemma 2 $C \cap \pi_A^n = pC$ (must show " $\subseteq$ ")

pf of Lemma 2: $C_n = C_{n+1} = C$ Consider monomials $Z_\alpha := \prod_{s \in S} s^{\alpha_s}$

Since $\Phi_{n+1}(a_0, a_1, \dots, a_{n+1}) = a_0^{p^{n+1}} + p \Phi_n(a_1, \dots, a_{n+1})$ $\alpha = (\alpha_s)_{s \in S}$
 $0 \leq \alpha_s < p^{n+1} \quad \forall s$

$\rightsquigarrow$ Every element of B_{n+1} is of the form $a^{p^{n+1}} + p \cdot b$ with $a \in A$
 $b \in B_n$

$\rightsquigarrow$ Every element $x \in C_{n+1}$ is of the form

$$x = \sum_{\alpha \in \Lambda} c_\alpha^{p^{n+1}} Z_\alpha + p y, \quad \alpha \in A \quad \forall \alpha \in \Lambda, \text{ and } y \in C_n = C$$

$\alpha \in \Lambda \leftarrow$ the set of all $(\alpha_s)_{s \in S}$ s.t. $0 \leq \alpha_s < p^{n+1} \quad \forall s$

$\Rightarrow$ If $x \in C \cap \pi_A^n$, then $c_\alpha \in \pi_A^n \quad \forall \alpha \in \Lambda$, hence $c_\alpha^{p^{n+1}} = 0 \quad \forall \alpha \in \Lambda$

In other words $x = p y$ for some $y \in C$ q.e.d.

Back to Thm 4, under the assumption that $\pi_A^{n+1} = (0)$

(b) = trivial; (c) follows from Lemma 1.

For (a), suppose $C' \subseteq A$, $C' \geq S$, C' : Cohen subring. Lemma 1 $\Rightarrow C' \geq C$. inclusion of p-rings with the same residue field
 $\Rightarrow C' = C$.

Cohen 4

Proof of Thm 4, Part 2 = general case

$$\pi_n: A \twoheadrightarrow A_n$$

Let $A_n = A/\mathfrak{m}_A^{n+1} \quad \forall n \in \mathbb{N}$. Let C_n = the Cohen subring of A_n containing $\pi_n(S)$.

Let $\pi_{n,m}: A_m \twoheadrightarrow A_n \quad \forall m \geq n \rightsquigarrow \pi_{n,m}(C_m) = C_n \quad \forall m \geq n$ by Part 1.

$$\text{Let } C = \varprojlim_n C_n \subseteq A = \varprojlim_n A_n$$

Easy to see: C is a Cohen subring of A

Check C is closed in A : Let $J_n = C \cap \mathfrak{m}_A^n \quad \bigcap_{n \geq 1} J_n = (0) \quad \circ \circ \quad \bigcap_{n \in \mathbb{N}} \mathfrak{m}_A^n = (0)$

Since every ideal of C is of the form $\mathfrak{p}^n C$, there is a function $t: \mathbb{N} \rightarrow \mathbb{N}$ s.t. $J_n = \mathfrak{p}^{t(n)} C$

Assertion (b) follows easily.

Assertion (c): Given $A' \subseteq A$, $A' \supseteq S$, and $A' + \mathfrak{m}_A = A$
closed subring

$$\text{Part 1} \Rightarrow \pi_n(A') \supseteq C_n \quad \forall n \quad A' = \bigcap_{n \geq 1} \pi_n^{-1}(\pi_n(A')) \quad \text{since } A' \text{ is closed}$$

$$\Rightarrow A' \supseteq \bigcap_{n \geq 1} \pi_n^{-1}(C_n) = C$$

QED

Prop 5. (Uniqueness of p-rings)

Let C and C' be p-rings with residue fields κ_C and $\kappa_{C'}$.

$$\pi_C: C \twoheadrightarrow \kappa_C, \quad \pi_{C'}: C' \twoheadrightarrow \kappa_{C'}. \quad \text{Let } \nu: \kappa_C \xrightarrow{\sim} \kappa_{C'}$$

Let $(x_s)_{s \in S}$ be a family of elements of C s.t. $(\pi_C(x_s))_{s \in S}$ is a p-basis of κ_C

Let $(x'_s)_{s \in S}$ be a family of elements of C' s.t. $(\pi_{C'}(x'_s))_{s \in S}$ is a p-basis of $\kappa_{C'}$

Suppose that $\nu(\pi_C(x_s)) = \pi_{C'}(x'_s) \quad \forall s \in S$ and $\ell(C) \geq \ell(C')$

$\exists!$ homomorphism $u: C \rightarrow C'$ such that $u(x_s) = x'_s \quad \forall s$ and $\pi_{C'} \circ u = \nu \circ \pi_C$.

This homomorphism u is surjective; u is an isomorphism if $\ell(C) = \ell(C')$.

pf: Let $\tilde{A} = C \times_{\kappa} C' = \{(a, a') \mid a \in C, a' \in C', \nu(\pi_C(a)) = \pi_{C'}(a')\}$, a complete local ring
 $\bigcup \{(x_s, x'_s) \mid s \in S\}$

Apply Thm 5 $\rightsquigarrow$ get a Cohen subring $\tilde{C} \subseteq \tilde{A}$

Have $\ell(\tilde{C}) = \max(\ell(C), \ell(C'))$ (consider $\mathfrak{p}^n \nmid \tilde{A}$)

$\rightsquigarrow \text{pr}_1|_{\tilde{C}} \xrightarrow{\sim} C$ is an isom. $\rightsquigarrow$ define $u := \text{pr}_2 \circ (\text{pr}_1|_{\tilde{C}})^{-1}: C \rightarrow C'$

q.e.d.

Cohen 5

Prop 6 (Existence of p-rings)

Let $\kappa \cong \mathbb{F}_p$ be a field. Let $n \in \mathbb{N} \cup \{\infty\}$. There exists a p-ring whose residue field is isomorphic to κ .

Pf: A Cohen subring C of $W(\kappa)$ is p-ring with $\ell(C) = \infty$.

(Recall that $(W(\kappa), \pi = V(W(\kappa)))$ is a complete separated local ring. q.e.d.)

Corollary 7 Let C be a p-ring with $\ell(C) =: n < \infty$. There exists a p-ring C' and an isomorphism $C'/p^n C' \cong C$.

(Immediate from Prop 6 and Prop 5)

Proposition 7 Let $\kappa \cong \mathbb{F}_p$ be a perfect field of characteristic $p > 0$.

Let C be a p-ring with $C/pC \xrightarrow{\alpha} \kappa$. Let $n = \ell(C) \in \mathbb{N} \cup \{\infty\}$.

There exists a isomorphism $C \rightarrow W_n(\kappa)$ which induces the isom. $C/pC \xrightarrow{\alpha} \kappa$.

Prop 8 Let A be a complete separated local ring whose residue field k is perfect of characteristic $p > 0$. $\pi: A \twoheadrightarrow k$

(a) $\exists!$ ring homom $u: W(k) \rightarrow A$ such that $\pi(u(\underline{a})) = a_0$

(b) The homom u in (a) is continuous for $\forall \underline{a} = (a_0, a_1, \dots) \in W(k)$
the $pW(k)$ -adic topology on $W(k)$, and $\text{Im}(u) =$ the unique Cohen subring of A .

Prop 9 Let A be a complete separated local ring with perfect residue field $k \cong \mathbb{F}_p$.

(a) There exists a unique multiplicative subset $S \subseteq A$ such that $\pi: A \twoheadrightarrow k$ induces a bijection $S \xrightarrow{\sim} k$

(b) An element $a \in A$ is in S iff $\forall n \in \mathbb{N}, \exists a_n \in A$ st. $a_n^{p^n} = a$.

(c) $S = \{u(y, 0, 0, \dots) \mid y \in k\}$, where $u: W(k) \rightarrow A$ is the ring homom in Prop 8.

Cohen 6

Proof of Prop 9: Let $T = \{x \in A \mid \forall n \in \mathbb{N}, \exists x_n \in A \text{ s.t. } x_n^{p^n} = x\}$

Uniqueness part of (a): $\forall$ multiplicative (=multiplicatively closed) subset $S \subseteq A$ s.t.

$$\pi|_S: S \xrightarrow{\sim} k \text{ clearly } S \subseteq T$$

Must show: $\pi|_T: T \rightarrow k$ is injective

Otherwise $\exists x, y \in T$ s.t. $x \neq y$ and $\pi(x) = \pi(y)$. $\forall n \in \mathbb{N}$, pick $x_n, y_n \in A$ $x_n^{p^n} = x$, $y_n^{p^n} = y$

$$\Rightarrow x_n \equiv y_n \pmod{m_A} \Rightarrow x_n^{p^n} \equiv y_n^{p^n} \pmod{m_A^{n+1}} \quad \forall n \Rightarrow x = y$$

existence: Have $u: W(k) \rightarrow A$

$S := \{u(y, 0, 0, \dots) \mid y \in k\}$ is a multiplicative subset of A

and $\pi|_S: S \xrightarrow{\sim} k$. We have proved (a) - (c). QED

Theorem 10 Let (A, m) be a complete Noetherian local ring with $k = A/m_A \cong \mathbb{F}_p$, $p > 0$.

Let C be a p-ring with $C/pC = k$ and $\ell(C) = \infty$. Let $m = \dim_k(m_A / (m_A^2 + pA))$

(1) $\exists$ an ideal $\alpha \subseteq C[[T_1, \dots, T_m]]$ and a local isomorphism $C[[T_1, \dots, T_m]]/\alpha \xrightarrow{\sim} A$

(2) Let $d := \dim(A)$. Suppose that $p \cdot 1_A$ is not a zero divisor of A .

Then $\exists$ a subring $B \subseteq A$ such that $B \cong C[[T_1, \dots, T_{d-1}]]$ and A is a finite A' -algebra

Pf: ⁽¹⁾ Let C' be a Cohen subring of A . Know: $\exists$ surjective local homom $C \xrightarrow{u} C' \hookrightarrow A$

Let $\bar{T}_1, \dots, \bar{T}_m$ be a k -basis of $m_A / (m_A^2 + pA)$, and pick $t_1, \dots, t_m \in m$ s.t. $t_i \mapsto \bar{T}_i$

$\Rightarrow \exists$ a surjective ring homom $C[[T_1, \dots, T_m]] \xrightarrow{v} A$ extending u s.t. $v(T_i) = \frac{v_i}{v_i}$

(2) Assume: $p \cdot 1_A$ is not a zero divisor of A

$\Rightarrow \exists$ elements $y_1, \dots, y_{d-1} \in m$ such that $\dim(A/(p, y_1, \dots, y_{d-1})) = 0$

$\Rightarrow$ get a ring homom $\alpha: C[[T_1, \dots, T_{d-1}]] \rightarrow A$ α is finite by Nagayama's Lemma
 $T_i \mapsto y_i$

$\Rightarrow \alpha$ is injective (Consider $\text{gr}_\bullet(C[[T_1, \dots, T_{d-1}]]) \cong k[\omega, T_1, \dots, T_{d-1}]$)

QED

Remark: Thm 10 is the case of mixed characteristics $(0, p)$ of Cohen's structure theorem.

(Existence of coeff. fields) Cohen 7

Prop. 11 Let $(A, \mathfrak{m})$ be a complete separated local ring, and assume A contains a subfield k_0 .

- (a) Suppose that $\text{char}(k_0) = 0$. $\exists!$ subfield $k \subseteq A$ containing k_0 st. the composition $k \hookrightarrow A \twoheadrightarrow A/\mathfrak{m}$ is an isomorphism
- (b) Suppose that $\text{char}(k_0) = p > 0$. There is a subfield $K \subseteq A$ (i.e. K is a subring of A and K is a field) such that the composition $K \hookrightarrow A \twoheadrightarrow A/\mathfrak{m}$ is an isomorphism

Pf (a): Follows easily from Hensel's Lemma

(b) Will prove a strong statement (b)':

(b)': If $(x_\lambda)_{\lambda \in \Lambda}$ is a p -basis of $\kappa_A = A/\mathfrak{m}_A$. Then $\exists!$ a unique subfield K containing all x_λ 's such that $K \hookrightarrow A \twoheadrightarrow A/\mathfrak{m} \xrightarrow{\cong}$

This subfield K is a Cohen subring of A

(Consequence of Thm. 4)

QED

Theorem 12 Let A be a complete Noetherian local ring which contains a field. Let $d = \dim(A)$, and let K be a coefficient field of A .

Let $m = \dim_K(\mathfrak{m}_A/\mathfrak{m}_A^2)$

(a) $\exists$ an ideal $\mathcal{O} \subseteq K[[T_1, \dots, T_m]]$ and an isom. $K[[T_1, \dots, T_m]]/\mathcal{O} \xrightarrow{\cong} A$

(b) $\exists$ a K -subalgebra $A' \subseteq A$ such that A is a finite A' -algebra and $A' \cong K[[X_1, \dots, X_d]]$

(c) If the local ring $(A, \mathfrak{m}_A)$ is regular, i.e. $\dim_K(\mathfrak{m}_A/\mathfrak{m}_A^2) = \dim(A)$, then $\exists$ a K -isom. $K[[X_1, \dots, X_d]] \xrightarrow{\cong} A$

(This follows from Prop. 12)

Remark: Cohen's structure theorem(s) is a deep/landmark theorem and has many applications, including the finiteness of derived normal models of complete Noetherian local rings and analytic unramifiedness of Nagata rings.

Groeb 1

§1 Term order on monomials

$x_1, \dots, x_n$ variables $\underline{x}^\alpha = x_1^{\alpha_1} \dots x_n^{\alpha_n}$, $\alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{N}^n$

Def 1 A term order on $\underline{x}^{\mathbb{N}^n} = \{\underline{x}^\alpha : \alpha \in \mathbb{N}^n\}$ = monomials in $x_1, \dots, x_n$ is a linear order $<$ on $\underline{x}^{\mathbb{N}^n}$ which satisfies conditions (i) and (ii) below

(i) $1 < \underline{x}^\beta \quad \forall \beta \in \mathbb{N}^n \setminus \{0\}$

(ii) If $\underline{x}^\alpha < \underline{x}^\beta$, then $\underline{x}^\alpha \cdot \underline{x}^\gamma < \underline{x}^\beta \cdot \underline{x}^\gamma \quad \forall \gamma \in \mathbb{N}^n$

Example 1 The lexicographic order on $\underline{x}^{\mathbb{N}^n}$ with $x_1 > x_2 > \dots > x_n$:

$$\underline{x}^\alpha <_{\text{lex}} \underline{x}^\beta \iff \exists i \text{ with } 1 \leq i \leq n \text{ s.t. } \alpha_j = \beta_j \quad \forall j = 1, \dots, i-1, \text{ and } \alpha_i < \beta_i$$

i.e. $\beta - \alpha = (\underbrace{0, 0, \dots, 0}_{i-1}, >0, * \dots *)$

Example 2 The degree lexicographic order on $\underline{x}^{\mathbb{N}^n}$ with $x_1 > x_2 > \dots > x_n$:

$$\underline{x}^\alpha <_{\text{deglex}} \underline{x}^\beta \iff \text{either } \alpha_1 + \dots + \alpha_n < \beta_1 + \dots + \beta_n, \\ \text{or } \alpha_1 + \dots + \alpha_n = \beta_1 + \dots + \beta_n \text{ and } \underline{x}^\alpha <_{\text{lex}} \underline{x}^\beta$$

Example The reverse lexicographic order on $\underline{x}^{\mathbb{N}^n}$ with $x_1 > x_2 > \dots > x_n$:

$$\underline{x}^\alpha <_{\text{revlex}} \underline{x}^\beta \iff \text{either } \alpha_1 + \dots + \alpha_n < \beta_1 + \dots + \beta_n, \\ \text{or } \alpha_1 + \dots + \alpha_n = \beta_1 + \dots + \beta_n, \text{ and } \exists i \text{ with } 1 \leq i \leq n \text{ s.t.} \\ \alpha_i > \beta_i \text{ and } \alpha_j = \beta_j \quad \forall j \geq i+1. \text{ i.e. } \beta - \alpha = (* \dots *, \underbrace{<0}_{i}, 0, \dots, 0)$$

Lemma 1 Let $<$ be a term order on $\underline{x}^{\mathbb{N}^n}$.

1) If $\underline{x}^\alpha \mid \underline{x}^\beta$, then $\underline{x}^\alpha \leq \underline{x}^\beta$

2) The linear order $<$ on $\underline{x}^{\mathbb{N}^n}$ is a well-ordering.

Let $<$ be a term order on $\underline{x}^{\mathbb{N}^n}$

Def Let k be a field, and write $k[\underline{x}] = k[x_1, \dots, x_n]$. Let $f \in k[\underline{x}]$

$$f = a_1 \underline{x}^{\alpha_1} + \dots + a_r \underline{x}^{\alpha_r} \quad r \geq 1, a_1, \dots, a_r \neq 0, \underline{x}^{\alpha_1} > \underline{x}^{\alpha_2} > \dots > \underline{x}^{\alpha_r}$$

(1) $\text{lm}(f) = \underline{x}^{\alpha_1}$ = the leading monomial of f

(2) $\text{lc}(f) = a_1$ = the leading coefficient of f

(3) $\text{lt}(f) = a_1 \underline{x}^{\alpha_1}$ = the leading term of f

Groeb 2

Def 2 Let $A = k[x_1, \dots, x_n]$, $k = \text{a field}$. Let $A^m = A^{\oplus m} = A \cdot e_1 \oplus \dots \oplus A e_m$
a free A -module of rank m

(1) A monomial in A^m is an element of the form $X \cdot e_i$, $X = x^\alpha$ a monomial in A , $1 \leq i \leq m$

(2) A term order on A^m is a linear order on the set of all monomials in A^m which satisfies (i) + (ii) below

(i) If $T = X \cdot e_i$ is a monomial in A^m and $Z \neq 1$ is a monomial in A , then $T < ZT$

(ii) If T, U are monomials in A^m , $T < U$, and Z is a monomial in A , then $ZT < ZU$

(3) For an element $f = a_1 T_1 + \dots + a_n T_n$, $a_1, \dots, a_n \in k$, $T_i = \text{monomial in } A^m$
 $T_1 > T_2 > \dots > T_n$

(a) $l_m(f) = T_1$

(b) $l_c(f) = a_1$

(c) $l_t(f) = a_1 T_1$

Example. Let $<$ be a term order on A . Have two term orders on A^m

(i) TOP (term over position) X, Y monomials in A

$$X e_i <_{\text{TOP}} Y e_j \iff \text{either } X < Y, \text{ or } X = Y \text{ and } i < j$$

$$(\leadsto e_1 <_{\text{TOP}} e_2 <_{\text{TOP}} \dots <_{\text{TOP}} e_m)$$

(ii) POT (position over term)

$$X e_i <_{\text{POT}} Y e_j \iff \text{either } i < j, \text{ or } i = j \text{ and } X < Y$$

$$(\text{again } e_1 <_{\text{POT}} e_2 <_{\text{POT}} \dots <_{\text{POT}} e_m)$$

Def 3 Let $x_1, \dots, x_n$ and $y_1, \dots, y_m$ be two sets of variables. Let $<_x$ be a term order on $x^{\mathbb{N}^n}$, and let $<_y$ be a term order on $y^{\mathbb{N}^m}$.

(a) An elimination order $<$ on $x^{\mathbb{N}^n} \cdot y^{\mathbb{N}^m}$ with the x -variables larger than the y -variables is a linear order on $x^{\mathbb{N}^n} \cdot y^{\mathbb{N}^m}$ such that

$$y^\beta > x^\alpha \cdot y^{\beta'} \implies \alpha = 0$$

$$\forall \alpha \in \mathbb{N}^n, \forall \beta, \beta' \in \mathbb{N}^m$$

Groeb 3

(b) The elimination order on $x^{\mathbb{N}^n} \cdot y^{\mathbb{N}^m}$ attached to $<_x$ and $<_y$ with the x -variables larger than the y -variables is defined by:

$$x^\alpha \cdot y^\beta < x^{\alpha'} \cdot y^{\beta'} \iff \text{either } x^\alpha <_x x^{\alpha'}, \text{ or } x^\alpha = x^{\alpha'} \text{ and } y^\beta <_y y^{\beta'}.$$

Remark: One uses an elimination order with the x -variables larger than the y -variables to "eliminate the x -variables" in elimination theory.

This means: given an ideal $I \subseteq k[x_1, \dots, x_n; y_1, \dots, y_m]$, compute the ideal $I \cap k[y_1, \dots, y_m] \subseteq k[y_1, \dots, y_m]$.

Remark on term orders on A^m : Both the TOP and POT are compatible with the given term order $<_A$ on A , in the following sense:

$$X <_A Y \implies X \cdot T < Y \cdot T \quad \forall X, Y \in x^{\mathbb{N}^n}, \forall \text{ monomial } T \text{ in } A^m$$

Remark A property of $<_{\text{revlex}}$ on $x^{\mathbb{N}^n}$

$$x^\alpha > x^\beta \text{ and } \alpha_r + \alpha_{r+1} + \dots + \alpha_n \geq 1 \implies \beta_r + \dots + \beta_n \geq 1 \quad \forall \alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{N}^n \quad \forall r, k \leq n$$

$$\beta = (\beta_1, \dots, \beta_n)$$

In other words, if $x^\alpha > x^\beta$ and $x^\alpha \in (x_r, x_{r+1}, \dots, x_n) \cdot k[x]$, then $x^\beta \in (x_r, x_{r+1}, \dots, x_n) \cdot k[x]$.

Lemma 2 Every term order on monomials in A^m is a well-ordering (on the set of all monomials of A^m)

Hint of a direct proof of Lemma 1: The semi-group $\mathbb{N}^n$ satisfies the following finiteness property: Let $S \subseteq \mathbb{N}^n$ be a subset of $\mathbb{N}^n$ such that $S + \mathbb{N}^n = S$. Then $\exists$ elements $s_1, \dots, s_r \in S$ s.t. $S = \bigcup_{i=1}^r (s_i + \mathbb{N}^n)$

Remark Let $x_1, x_2, \dots, x_n$ be the variables of A .

Groeb 3a

Def: Let $x_1, \dots, x_n; y_1, \dots, y_m$ be two groups variables. Let $A = k[x_1, \dots, x_n]$

$$B = k[x_1, \dots, x_n; y_1, \dots, y_m] = A[y_1, \dots, y_m]$$

$$\text{Let } F = B e_1 \oplus \dots \oplus B e_\ell$$

(a) An elimination term order for F is a term order for (monomials in) F with the x -variables larger than the y -variable is a term order for F such that $y^\beta e_i > x^\alpha y^{\beta'} e_j \Rightarrow \alpha = 0 \quad \forall \alpha \in \mathbb{N}^n, \forall \beta, \beta' \in \mathbb{N}^m, \forall i, j \in \{1, \dots, \ell\}$

Remark. Let $<$ be an elimination order on $x^{\mathbb{N}^n} \cdot y^{\mathbb{N}^m}$ with the x -variables larger than the y -variables. Then the TOP order $<_{\text{TOP}}$ for F is an elimination order for F with the x -variables larger than the y -variables.

Groeb 4

§2 The division algorithm

First, on $k[x_1, \dots, x_n]$, with a given term order $<$

Description of the algorithm:

Input: $\vec{f} = (f_1, \dots, f_s) \in k[x]^s$, $f_i \neq 0 \forall i$ and $f \in k[x]$

Output: $\vec{u} = (u_1, \dots, u_s) \in k[x]^s$ and $r \in k[x]$ such that

$$f = u_1 f_1 + \dots + u_s f_s + r \quad r = \text{remainder}$$

$$\text{Max}(\text{lm}(u_1) \text{lm}(f_1), \dots, \text{lm}(u_s) \text{lm}(f_s), r) = \text{lm}(f)$$

r is reduced w.r.t. $\vec{f}$ in the sense that: with $r \neq 0$,
or $r = a_1 x^{\alpha_1} + \dots + a_m x^{\alpha_m}$
 $\alpha_1 > \dots > \alpha_m$ $a_i \neq 0 \forall i$
and $\text{lm}(f_i) \nmid x^{\alpha_j} \quad \forall i=1, \dots, s, \forall j=1, \dots, m$

Initialize: $u_1 = \dots = u_s = 0$, $r := 0$, $h := f$ h : variable to hold the polynomial to be divided by $\vec{f}$

Do ① unless $h=0$
If $\exists i$ s.t. $\text{lm}(f_i) \mid \text{lm}(h)$, let $j = \text{Min}\{i : \text{lm}(f_i) \mid \text{lm}(h)\}$ Variation here:
Pick $j \in \{i : \text{lm}(f_i) \mid \text{lm}(h)\}$
reassign values of $u_j \rightsquigarrow u_j + \frac{\text{lt}(h)}{\text{lt}(f_j)}$
 $h \rightsquigarrow h - \frac{\text{lt}(h)}{\text{lt}(f_j)} f_j$; go back to ①

Otherwise $\text{lp}(f_j) \nmid \text{lp}(h) \quad \forall j=1, \dots, s$,

reassign $r \rightsquigarrow r + \text{lt}(h)$

$h \rightsquigarrow h - \text{lt}(h)$; go back to ①

(The effect is: test the next highest term of the old value of h)

Remark. 1) The output, $\vec{u}$ and $\vec{r}$, of the division algorithm generally depends on the order of the f_j 's.

2) Will see: The output is independent of the order of the f_j 's if $\{f_j\}$ is a Groebner basis of the ideal $\sum f_j k[x_1, \dots, x_n]$

Notation: $f \xrightarrow{\vec{f}} r$ " f is reduced to $\vec{r}$ after division by $\vec{f}$ "

Groeb 5

§3 Groebner basis of ideals

Let $<$ be a term order on $A = k[x_1, \dots, x_n]$.

$\Rightarrow$ an increasing filtration of A by finite $\dim^k$ k -vector subspaces indexed by $\mathbb{N}^n$: $\text{Fil}_{\leq x^\alpha} = \{0\} \cup \{f \in A \mid \text{lm}(f) \leq x^\alpha\}$

Defⁿ 1 Let $I \subseteq k[x_1, \dots, x_n]$ be an ideal, with the filtration $(I \cap \text{Fil}_{\leq x^\alpha})_{\alpha \in \mathbb{N}^n}$

Let $gr_{\leq}(I) := \bigoplus_{\alpha \in \mathbb{N}^n} (I \cap \text{Fil}_{\leq x^\alpha}) / (I \cap \text{Fil}_{< x^\alpha})$

a graded ideal of $k[x_1, \dots, x_n]$

Defⁿ 2 Let $G = \{g_1, \dots, g_t\}$ be a finite subset of an ideal $I \subseteq k[x]$ s.t. $g_i \neq 0 \forall_i$.

We say that G is a Groebner basis of I if

(*) $\bigcup_i \text{lm}(g_i) \cdot k[x] = gr_{\leq}(I)$ Equivalently, $\forall_{\substack{f \in I \\ f \neq 0}} \exists i \in \{1, \dots, t\} \text{ s.t. } \text{lm}(g_i) \mid \text{lm}(f)$

(Exercise: Show that the two conditions are equivalent, and $I = \sum_{i=1}^t g_i \cdot k[x]$.)

Theorem 3 Let $I \subseteq k[x_1, \dots, x_n]$ be a non-zero ideal of $k[x]$, and let

$\vec{g} = (g_1, \dots, g_t)$, $g_i \in I \forall_i$. The following conditions are equivalent

(1) (**) $\forall_{\substack{f \in I \\ f \neq 0}} \exists i \in \{1, \dots, t\} \text{ s.t. } \text{lm}(g_i) \mid \text{lm}(f)$

(2) $f \in I \iff f \xrightarrow{\vec{g}}_+ 0 \quad \forall_{\substack{f \in k[x] \\ f \neq 0}}$

(3) $f \in I \iff \exists h_1, \dots, h_t \in k[x] \text{ s.t. } f = \sum_{i=1}^t h_i \cdot g_i \text{ and } \text{lm}(f) = \max_{1 \leq i \leq t} (\text{lm}(h_i) \cdot \text{lm}(g_i))$
 $\forall_{\substack{f \in k[x] \\ f \neq 0}}$

(Note: We allow some (but not all) of the h_i 's to be zero.)

(4) (*) $\bigcup_{i=1}^t \text{lm}(g_i) \cdot k[x] = gr_{\leq}(I)$

(The equivalence of these conditions are not difficult.)

Groeb 6

Prop. Let $B = \{g_1, \dots, g_t\}$ be a finite set of non-zero elements of $k[x_1, \dots, x_n]$. Let $<$ be a term order on $x^{\mathbb{N}^n}$. Then G is a Groebner basis if and only if the remainder of division of f by G is uniquely determined by f , $\forall f \in k[x]$.
 i.e. in any expression $f = \sum_{i=1}^t h_i g_i + r$ with $lp(f) = \max(lp(h_i) \cdot lp(g_i), r)$ and r reduced w.r.t G , r is uniquely determined by f .

Pf. (a) Assume that G is a Groebner basis, and r_1, r_2 are two remainders
 i.e. $f = \sum_i h_i g_i + r = \sum_i h'_i g_i + r'$ $lp(f) = \max(lp(h_i) \cdot lp(g_i), r)$
 and r, r' both reduced w.r.t. G $= \max(lp(h_i) \cdot lp(g'_i), r')$
 i.e. no term of r, r' is divisible by $lp(g_i) \forall i$ $\leftarrow$ This is the key
 $\Rightarrow r - r' \in I = \sum_i g_i k[x]$. If $r - r' \neq 0$, then $lp(r - r')$ is not divisible by $lp(g_i) \forall i$ contradiction.

(b) Assume that the remainder of division of f by G is unique determined by f , $\forall f$;
 write $f \xrightarrow{G} r$ for "f reduces to r".

Claim: This assumption implies: $\forall c \in k \forall \text{monomial } x^\alpha, \forall g_i, g - c x^\alpha g_i \xrightarrow{G} r$ if $g \xrightarrow{G} r$.

It is easy to see that (b) follows from the claim, $\because$ every element $f \in I$ can be written as $f = \sum_{i=1}^t \sum_a x^{\alpha_{i,a}} g_i$ (finite sum), so $f \xrightarrow{G} 0 \forall f \in I$.

It remains to prove the claim.

Separate two cases: (a) The monomial $x^\alpha \cdot lm(g_i)$ appears in a term of f

(b) The monomial $x^\alpha \cdot lm(g_i)$ does not appear in any term of f

Let's illustrate the argument in case (b):

Then do: $g - c \cdot x^\alpha \cdot g_i \xrightarrow{g_i} (g - c \cdot x^\alpha \cdot g_i) + c \cdot x^\alpha \cdot g_i \quad \checkmark$

Groeb 7

§4 Buchberger's algorithm

Def 1 For $0 \neq f, g \in k[x_1, \dots, x_n]$, define $S(f, g) \in k[x_1, \dots, x_n]$ by $k = \text{a field}$

$$S(f, g) = \frac{\text{LCM}(\text{lm}(f), \text{lm}(g))}{\text{lt}(f)} \cdot f - \frac{\text{LCM}(\text{lm}(f), \text{lm}(g))}{\text{lt}(g)} \cdot g$$

called the S-polynomial of f and g .

^(Buchberger)
Theorem 2 Let $G = \{g_1, \dots, g_t\}$ be a finite set of non-zero elements of $k[x_1, \dots, x_n]$.
Then G is Groebner basis of $\sum_i g_i k[x_1, \dots, x_n]$ iff
 $S(g_i, g_j) \xrightarrow{G} 0 \quad \forall i \neq j$

Lemma Let $f_1, \dots, f_s \in k[x_1, \dots, x_n]$ be non-zero polynomials s.t. $\text{lm}(f_i) = x^\alpha \quad \forall i=1, \dots, s$.

Suppose that $c_1, \dots, c_s \in k$ s.t. $f \stackrel{\text{def}}{=} \sum_{i=1}^s c_i f_i$ has $\text{lm}(f) < x^\alpha$.

i.e. $\sum_{i=1}^s c_i \cdot \text{lc}(f_i) = 0$. Then $f \in \sum_{i=1}^{s-1} k \cdot S(f_i, f_{i+1})$

pf: Let $a_i = \text{lc}(f_i)$

$$f = c_1 f_1 + \dots + c_s f_s$$

$$= c_1 a_1 \left(\frac{f_1}{a_1}\right) + \dots + c_s a_s \left(\frac{f_s}{a_s}\right)$$

$$= c_1 a_1 \left(\frac{f_1}{a_1} - \frac{f_2}{a_2}\right) + (c_1 a_1 + c_2 a_2) \left(\frac{f_2}{a_2} - \frac{f_3}{a_3}\right) + \dots + (c_{s-1} a_{s-1} + c_s a_s) \left(\frac{f_s}{a_s} - \frac{f_{s+1}}{a_{s+1}}\right)$$

$$= \sum_{i=1}^{s-1} \left(\sum_{j=i}^s c_j a_j \right) \cdot S(f_i, f_{i+1}) \quad \text{q.e.d.}$$

Proof of Thm 2 "only if" is trivial, $\because S(g_i, g_j) \in \sum_{i=1}^t g_i k[x_1, \dots, x_n]$

"if": Given $f \in I = \sum_{i=1}^t g_i k[x]$
Pick $h_1, \dots, h_t \in k[x]$ s.t. $f = \sum_{i=1}^t h_i g_i$ and

$$x^\alpha = \max_{1 \leq i \leq t} (\text{lm}(h_i) \cdot \text{lp}(g_i)) \leq \max_{1 \leq i \leq t} (\text{lm}(h'_i) \cdot \text{lm}(g_i)) \quad \forall h'_1, \dots, h'_t \in k[x] \text{ s.t. } f = \sum_{i=1}^t h'_i g_i$$

Claim: $x^\alpha = \text{lp}(f)$ (claim $\Rightarrow f \xrightarrow{G} 0 \quad \forall f \in I$, so G is a Groebner basis)

Suppose that $x^\alpha > \text{lp}(f)$. Will find a better representation of f with a smaller x^α .

Let $S = \{ i \mid \text{lm}(h_i) \cdot \text{lm}(g_i) = x^\alpha \}$

$$\text{Consider } g := \sum_{i \in S} \text{lt}(h_i) \cdot g_i = \sum_{i \in S} \text{lc}(h_i) \cdot \text{lm}(h_i) \cdot g_i$$

Lemma $\Rightarrow g \in \sum_{i \in S} k \cdot S(\text{lm}(h_i) g_i, \text{lm}(h_j) g_j)$

Groeb 8

$$\begin{aligned} S(\text{lm}(h_i) \cdot g_i, \text{lm}(h_j) \cdot g_j) &= \frac{x^\alpha}{\text{lt}(\text{lm}(h_i) \cdot g_i)} \text{lm}(h_i) \cdot g_i - \frac{x^\alpha}{\text{lt}(\text{lm}(h_j) \cdot g_j)} \text{lm}(h_j) \cdot g_j \\ &= \frac{x^\alpha}{\text{lt}(g_i)} g_i - \frac{x^\alpha}{\text{lt}(g_j)} g_j = \frac{x^\alpha}{\text{LCM}(\text{lt}(g_i), \text{lt}(g_j))} \cdot S(g_i, g_j) \end{aligned}$$

Since $S(g_i, g_j) \xrightarrow{G} 0$, it follows that $\frac{x^\alpha}{\text{LCM}(\text{lt}(g_i), \text{lt}(g_j))} \cdot S(g_i, g_j) \xrightarrow{G} 0$

$$\Rightarrow \forall i, j \in S, \quad S(\text{lm}(h_i) g_i, \text{lm}(h_j) g_j) = \sum_{\mu=1}^t h_{i,j,\mu} \cdot g_\mu \quad \text{with } \text{lm}(h_{i,j,\mu}) \cdot \text{lt}(g_\mu) < x^\alpha$$

$\exists h_{i,j,\mu} \in k[x_1, \dots, x_n] \quad \mu=1, \dots, t \text{ s.t.}$

$$\circ \circ \text{lt}(S(g_i, g_j)) < \text{LCM}(\text{lt}(g_i), \text{lt}(g_j))$$

This gives us another expression

$$\begin{aligned} f &= \sum_{i,j \in S} \sum_{\mu} c_{i,j,\mu} \cdot h_{i,j,\mu} \cdot g_\mu + \sum_{i \in S} h_i \cdot g_i \quad c_{i,j,\mu} \in k \\ \text{s.t. } \text{Max} \left(\left\{ \text{lt}(h_{i,j,\mu}) \cdot \text{lt}(g_\mu) \mid \substack{i,j \in S \\ 1 \leq \mu \leq t} \right\} \cup \left\{ \text{lt}(h_i) \cdot \text{lt}(g_i) \mid i \in S \right\} \right) &< x^\alpha \end{aligned}$$

This is a contradiction. QED

Buchberger's theorem gives an effective criterion on whether a given set of generators of an ideal $I \subseteq k[x_1, \dots, x_n]$ is a Groebner basis. It also leads to an algorithm for constructing a Groebner basis of a given ideal I , starting with a set of generators of I :

Begin with a set $\{f_1, \dots, f_s\}$ of generators of an ideal $I \subseteq k[x]$ and a term order of x^N

Compute $S(f_i, f_j)$ and $S(f_i, f_j) \xrightarrow{F} r_{ij}$
 $\vec{f} = (f_1, \dots, f_s)$

If $r_{ij} = 0 \quad \forall i \neq j$, $(f_1, \dots, f_s)$ is a Groebner basis

Otherwise, expand $f_1, \dots, f_s$ include the first non-zero r_{ij} one encounters and repeat this.

Prop: The above algorithm stops eventually:

At the i -th run, we get a finite set of generators G_n . If G_n is not a Groebner basis, we get an element $r_n \in I$, reduced w.r.t. G_n . So

$\text{lt}(r_n) \notin \sum_{f \in G_n} \text{lt}(f) \cdot k[x] = J_n$ Thus $J_n \subsetneq J_{n+1}$. Such an ascending chain must stop. QED.

Groeb 9

§5

Uniqueness of reduced Groebner basis

(analog of: row reduced echelon form in linear algebra)

Def 1. a) A Groebner basis $G = \{g_1, \dots, g_t\}$ for an ideal $I \subseteq k[x_1, \dots, x_n]$ is minimal if $lc(g_i) = 1 \ \forall i=1, \dots, t$ and $lt(g_i) \nmid lt(g_j) \ \forall i \neq j$

b) A Groebner basis $G = \{g_1, \dots, g_t\}$ of I is reduced if $lc(g_i) = 1 \ \forall i=1, \dots, t$ and $lt(g_i)$ does not divide any term of $g_j \ \forall i \neq j$.
(Clearly every reduced Groebner basis is minimal)

Prop 2. Let $G = \{g_1, \dots, g_t\}$ and $G' = \{g'_1, \dots, g'_s\}$ be Groebner bases of the same ideal $I \subseteq k[x_1, \dots, x_n]$. Then $s = t$, and $\exists! \sigma \in S_t$ s.t.
 $lt(g_i) = lt(g'_{\sigma(i)}) \ \forall i=1, \dots, t$

(Exer.) Note that $\{lt(g_1), \dots, lt(g_t)\}$ is the set of extremal points of $\{\alpha \in \mathbb{N}^n \mid x^\alpha \in gr_{\leq}(I)\}$

Theorem 3 Fix a term order on $x^{\mathbb{N}^n}$. Every non-zero ideal I of $k[x_1, \dots, x_n]$ has a unique reduced Groebner basis

Pf: Existence easy.

Uniqueness: Let $\{g_1, \dots, g_t\}$ and $\{g'_1, \dots, g'_t\}$ be minimal Groebner bases of I s.t. $lt(g_i) = lt(g'_i) \ \forall i=1, \dots, t$

Show: $g_i = g'_i$. If $g_i - g'_i \neq 0$, $lm(g_i - g'_i)$ is divisible by $lm(g_i)$ for some i . But $i \notin \{2, 3, \dots, t\}$ by assumption, so $lm(g_i)$

$lm(g_i) \mid lm(g_i - g'_i)$, hence $lm(g_i) = lm(g'_i) < lm(g_i - g'_i)$, a contradiction. q.e.d.

§6. Generalization to free modules of finite rank over $k[x_1, \dots, x_n]$, $k = \text{a field}$

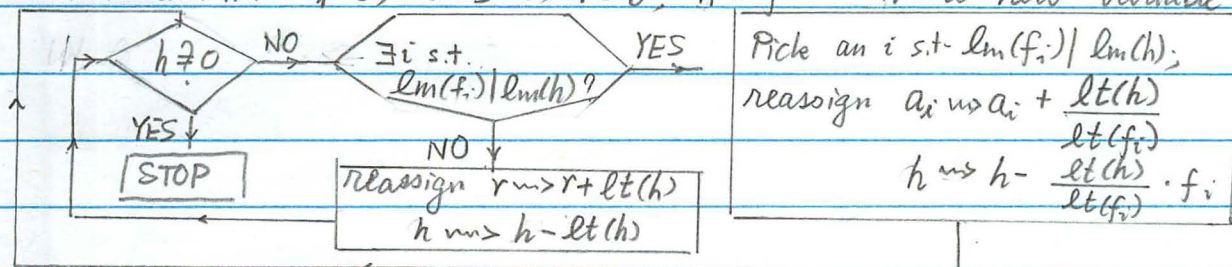
Division algorithm on A^m , $A = k[x_1, \dots, x_n]$, w.r.t. a term order $<$ on A^n

Input: $f, f_1, \dots, f_s \in A^m$ $f_i \neq 0$ for $i=1, \dots, s$

Output: $a_1, \dots, a_s \in A$, $r \in A^m$ with $f = a_1 f_1 + \dots + a_s f_s + r$

and $\bullet$ r is reduced w.r.t. $\{f_1, \dots, f_s\}$, i.e. either $r=0$ or
 $\bullet \max_{1 \leq i \leq s} (\text{lm}(a_i f_i), \text{lm}(r)) = \text{lm}(f)$ $r \neq 0$ and no term of r is divisible by $\text{lm}(f_i) \forall i=1, \dots, s$

Initialization: $a_i=0, \dots, a_s=0, r=0, h=f$ h : a new variable



- The above division algorithm allows "some randomness" in the step which involves picking an element of $\{i: \text{lm}(f_i) | \text{lm}(h)\}$
- When the algorithm stops, the values in the registers $a_1, \dots, a_s, r$ are the required output. Notation: $f \xrightarrow{\{f_1, \dots, f_s\}} r$

Defⁿ 1 Let ${}^{0*}M \subseteq A^m$ be an A -submodule. A subset $G = \{g_1, \dots, g_t\} \subseteq M$ with $g_i \neq 0 \forall i=1, \dots, t$ is a Groebner basis of M w.r.t. a given term order $<$ on A^m if $\forall f \in A^m, \exists i \in \{1, \dots, t\}$ s.t. $\text{lm}(g_i) | \text{lm}(f)$.

Thm 2 Let ${}^{0*}M \subseteq A^m$ be an A -submodule, and $G = \{g_1, \dots, g_t\}$ $g_i \neq 0 \forall i$, $< = \text{a term order on } A^m$. The following are equivalent ${}^{0*}f \in M$

(i) G is a Groebner basis of M

(ii) $f \in M \iff f \xrightarrow{G} 0$

(iii) $f \in M \iff \exists h_1, \dots, h_t \in A$ s.t. $f = h_1 g_1 + \dots + h_t g_t$ and $\text{lm}(f) = \max_{1 \leq i \leq t} (\text{lm}(h_i) \cdot \text{lm}(g_i))$

(iv) $\forall f \in A^m$, if $f \xrightarrow{G} r_1$ and $f \xrightarrow{G} r_2$ and r_1, r_2 are reduced mod G , then $r_1 = r_2$

(v) $\sum A \cdot \text{lm}(g_i) = \text{gr}_<(M)$

Groeb 11

Def 3 For $f, g \in A^m$, define $S(f, g) \in A^m$ by

$$S(f, g) = \frac{\text{LCM}(\text{lm}(f), \text{lm}(g))}{\text{lt}(f)} f - \frac{\text{LCM}(\text{lm}(f), \text{lm}(g))}{\text{lt}(g)} g$$

Note: If $\text{lm}(f) = x^\alpha \cdot e_i$, $\text{lm}(g) = x^\beta \cdot e_j$ and $i \neq j$, then $\text{LCM}(\text{lm}(f), \text{lm}(g)) = 0$ by definition, and $S(f, g) = 0$

Theorem 4 Let M be a non-zero A -submodule of A^m , $G = \{g_1, \dots, g_r\} \subseteq M$.
Then G is a Groebner basis of M iff $g_i \neq 0 \ \forall i$

$$S(g_i, g_j) \xrightarrow{G} 0 \quad \forall i, j \text{ with } i \neq j$$

Algorithm to enhance a set of generators of M to a Groebner basis:
At each stage, compute $S(f_i, f_j) \xrightarrow{G} r_{ij}$. Whenever one gets a non-zero remainder r_{ij} , add r_{ij} to the set of generators and repeat. After a finite number of steps, all remainders are zero, and we have a Groebner basis of M .

Proposition 5

§7. First Applications of Groebner bases

(1) The ideal membership problem: determine where a given element $f \in k[x_1, \dots, x_n]$ lies in an ideal I , I defined by a set of generators.

First compute a Groebner basis of I using Buchberger's algorithm, then perform a division to see whether $f \xrightarrow{G} 0$

(2) Solve polynomial equations: Given $f_1, \dots, f_m \in k[x_1, \dots, x_n]$, say $m \geq n$.
Use $<_{\text{lex}}$ with $x_1 > x_2 > \dots > x_n$ Find common zeros of $\sum_i f_i \cdot k[x]$

Key: $<_{\text{lex}}$ is an elimination order

$\Rightarrow$ Let $G = \{g_1, \dots, g_t\}$ be a Groebner basis of $\sum_i f_i \cdot k[x_1, \dots, x_n] = I$

Then $G \cap k[x_n]$ is a Groebner basis of $I \cap k[x_n]$

$G \cap k[x_{n-1}, x_n]$ is a Groebner basis of $I \cap k[x_{n-1}, x_n]$

$G \cap k[x_i, x_{i+1}, \dots, x_n]$ is a Groebner basis of $I \cap k[x_i, x_{i+1}, \dots, x_n]$

(3) Elimination: $I = (f_1, \dots, f_e) \subseteq k[x_1, \dots, x_n, y_1, \dots, y_m]$

$<$: an elimination order on $x^{N^n} \cdot y^{N^m}$ with the x -variables larger than the y -var.

Let $G = \{g_1, \dots, g_t\}$ be a Groebner basis for I

$\Rightarrow G \cap k[y_1, \dots, y_m]$ is a Groebner basis for $I \cap k[y_1, \dots, y_m]$

("eliminate the x -variables")

(4) Intersection of ideals

Lemma: Let $I, J \subseteq k[x_1, \dots, x_n]$ be ideals. Let w be a new variable.

Then $I \cap J = (w \cdot I \cdot k[x_1, \dots, x_n, w] + (1-w) \cdot J \cdot k[x_1, \dots, x_n, w]) \cap k[x_1, \dots, x_n]$

(Exer.)

This Lemma + elimination gives a method to compute $I \cap J$

- (5) Compute the lcm of two non-zero elements $f, g \in k[x_1, \dots, x_n]$
 (Recall that $k[x_1, \dots, x_n]$ is a UFD)

$$\text{lcm}(f, g) \cdot k[x_1, \dots, x_n] = f k[x_1, \dots, x_n] \cap g k[x_1, \dots, x_n]$$

$$\text{gcd}(f, g) = f \cdot g / \text{lcm}(f, g)$$

- (6) Compute $(I : J)$, I, J ideals of $k[x_1, \dots, x_n]$

$$\text{Let } J = \sum_{i=1}^l f_i \cdot k[x_1, \dots, x_n] \quad f_i \neq 0 \quad \forall i$$

$$(a) (I : J) = \bigcap_{i=1}^l (I : f_i)$$

$$(b) (I : f_i) = \frac{1}{f_i} \cdot (I \cap f_i)$$

- (7) Find an explicit k -basis of $k[x_1, \dots, x_n]/I$, $I = \sum_{i=1}^l f_i k[x_1, \dots, x_n]$

or more generally, find an explicit k -basis of $k[x_1, \dots, x_n]^{\oplus m}/M$,
 where M is a $k[x_1, \dots, x_n]$ -submodule of $k[x_1, \dots, x_n]^{\oplus m}$.

Let $<$ be a term order on $k[x_1, \dots, x_n]^{\oplus m}$, and let $G = \{g_1, \dots, g_t\}$
 be a reduced Groebner basis of M . Then the image in $k[x_1, \dots, x_n]^{\oplus m}/M$
 of

$\{ \underline{x}^\alpha \cdot e_i \mid \underline{x}^\alpha \cdot e_i \text{ is not divisible by } \text{lm}(g_j) \quad \forall j=1, \dots, t \}$
 is a k -basis of $k[x_1, \dots, x_n]^{\oplus m}/M$

- (8) Compute $\text{Ker}(\psi: k[y_1, \dots, y_m] \rightarrow k[z_1, \dots, z_n])$ ψ : a k -linear ring homom.

Let $f_i \stackrel{\text{def}}{=} \psi(y_i)$, $i=1, \dots, m$

Consider the ideal $\sum_{i=1}^m (y_i - f_i(x_1, \dots, x_n)) k[x_1, \dots, x_n, y_1, \dots, y_m] =: J$

Then $\text{Ker}(\psi) = J \cap k[y_1, \dots, y_m]$

§8 Syzygies (= linear relations)

Def 1. Let M be a (left) R -module and let $u_1, \dots, u_n \in M$ be elements of M .

Define the relation module, or the syzygy module $\text{Syz}(u_1, \dots, u_n)$ by

$$\text{Syz}(u_1, \dots, u_n) = \{ (a_1, \dots, a_n) \in R^n \mid \sum_{i=1}^n a_i u_i = 0 \},$$

i.e.
$$0 \rightarrow \text{Syz}(u_1, \dots, u_n) \rightarrow R^n \rightarrow M$$

$$(a_1, \dots, a_n) \mapsto \sum_{i=1}^n a_i u_i$$

Lemma 2 Let M be an R -module, let P and Q be projective R -modules.

Let $p: P \rightarrow M$ and $q: Q \rightarrow M$ be R -linear surjections, $R := \text{Ker}(p)$, $S := \text{Ker}(q)$

Let $f: P \rightarrow Q$ and $g: Q \rightarrow P$ be R -linear maps st. $p = q \circ f$ and $q = p \circ g$

$$S \hookrightarrow Q \xrightarrow{q} M$$

$$R \hookrightarrow P \xrightarrow{p} M$$

$$\text{Then: } R = \text{Im}(\text{id}_P - g \circ f) + g(S)$$

Rmk: In the case P, Q are both free modules of finite rank, Lemma 2 tells us how to express the syzygy module module R of a set $(u_1, \dots, u_s)$ of generators of M in terms of the syzygy module S of another set $(v_1, \dots, v_t)$ of generators of M

Pf of Lemma 2 $p = q \circ f = p \circ g \circ f \Rightarrow \text{Im}(\text{id}_P - g \circ f) \subseteq R$, clearly $g(S) \subseteq R$

$$\text{clearly } g \circ f \circ g = g \circ p \circ g = g \circ q = 0$$

$$\Rightarrow f \circ x \in S$$

$$x \in R \Rightarrow x = \underbrace{x - g(f(x))}_{\in \text{Im}(\text{id}_P - g \circ f)} + \underbrace{g(f(x))}_{\in g(S)}$$

$$\text{Im}(\text{id}_P - g \circ f) + g(S)$$

q.e.d.

Prop 3 Let $Y_1, \dots, Y_s$ be non-zero monomials in $A^m = k[x_1, \dots, x_n]^m$

$$\text{Syz}(Y_1, \dots, Y_s) \subseteq A \vec{v}_1 \oplus \dots \oplus A \vec{v}_s = A^s$$

$$\text{Then } \text{Syz}(Y_1, \dots, Y_s) = \sum_{0 \leq i, j \leq s} A \cdot \left(\frac{\text{lcm}(Y_i, Y_j)}{Y_i} \vec{v}_i - \frac{\text{lcm}(Y_i, Y_j)}{Y_j} \vec{v}_j \right)$$

Pf. $\text{Syz}(Y_1, \dots, Y_s) = A$ -span of monomials in $\text{Syz}(Y_1, \dots, Y_s) \subseteq A \vec{v}_1 \oplus \dots \oplus A \vec{v}_s = A^s$

because $Y_1, \dots, Y_s$ are monomials in A^m

Groeb 15

Let $h_1, \dots, h_s$ be terms in A s.t. $h_1 Y_1 + \dots + h_s Y_s = 0$, i.e. $\sum_j h_j \vec{v}_j \in \text{SyZ}(Y_1, \dots, Y_s)$

Must show: $\sum_j h_j \vec{v}_j \in \sum_{i,j} A \left(\frac{\text{lcm}(Y_i, Y_j)}{Y_i} \vec{v}_i - \frac{\text{lcm}(Y_i, Y_j)}{Y_j} \vec{v}_j \right)$

$\forall i=1, \dots, n$, let $S_i = \{j \mid Y_j \in A \cdot \vec{e}_i\} \leadsto \sum_{j \in S_i} h_j Y_j = 0$. Write $Y_j = z_j \cdot e_i$
 $z_j \in A \quad \forall j \in S_i$

Sufficed to show:

$$\sum_{j \in S_i} h_j \vec{v}_j \in \sum_{j, j' \in S_i} A \left(\frac{\text{lcm}(Y_j, Y_{j'})}{Y_j} \vec{v}_j - \frac{\text{lcm}(Y_j, Y_{j'})}{Y_{j'}} \vec{v}_{j'} \right)$$

Write $S_i = \{j_1, j_2, \dots, j_a\}$, $h_{j_\mu} = c_\mu \cdot X_\mu$ $c_\mu \in k$, X_μ : monomial in A

$$\begin{matrix} \text{distinct} \\ \vec{z}_{j_\mu} = d_\mu W_\mu \end{matrix}$$

May assume $\begin{cases} c_a \neq 0 \\ X_\mu \cdot W_\mu = X, \forall \mu=1, \dots, a \end{cases}$ (Otherwise, decompose S_i into a disjoint union of subsets)
 Know: $c_1 d_1 + \dots + c_a d_a = 0$

$$\begin{aligned} \leadsto \sum_{j \in S_i} h_j \vec{v}_j &= c_1 X_1 \vec{v}_{j_1} + \dots + c_a X_a \vec{v}_{j_a} \\ &= c_1 d_1 \frac{X}{d_1 W_1} \vec{v}_{j_1} + \dots + c_a d_a \frac{X}{d_a W_a} \vec{v}_{j_a} \end{aligned}$$

Write as a telescoping sum

$$= c_1 d_1 \frac{X}{\text{lcm}(W_1, W_2)} \left(\frac{\text{lcm}(W_1, W_2)}{d_1 W_1} \vec{v}_{j_1} - \frac{\text{lcm}(W_1, W_2)}{d_2 W_2} \vec{v}_{j_2} \right)$$

$$+ (c_1 d_1 + c_2 d_2) \frac{X}{\text{lcm}(W_2, W_3)} \left(\frac{\text{lcm}(W_2, W_3)}{d_2 W_2} \vec{v}_{j_2} - \frac{\text{lcm}(W_2, W_3)}{d_3 W_3} \vec{v}_{j_3} \right)$$

+ ...

$$+ (c_1 d_1 + \dots + c_{a-1} d_{a-1}) \frac{X}{\text{lcm}(W_{a-1}, W_a)} \left(\frac{\text{lcm}(W_{a-1}, W_a)}{d_{a-1} W_{a-1}} \vec{v}_{j_{a-1}} - \frac{\text{lcm}(W_{a-1}, W_a)}{d_a W_a} \vec{v}_{j_a} \right)$$

$$+ \underbrace{(c_1 d_1 + \dots + c_a d_a)}_0 \frac{X}{c_a d_a}$$

QED.

Note: This proof is similar to the Lemma in §2, before Buchberger's theorem.

Theorem 4 Let $(g_1, \dots, g_t)$ be a finite sequence of non-zero elements in A^m which is a Groebner basis of $\sum_{j=1}^t A g_j$ w.r.t a term order $<$ on $A^{\oplus m}$.

Define, for each $i \neq j$,

$$S(g_i, g_j) := \frac{\text{lcm}(\text{lm}(g_i), \text{lm}(g_j))}{\text{lm}(g_i)} g_i - \frac{\text{lcm}(\text{lm}(g_i), \text{lm}(g_j))}{\text{lm}(g_j)} g_j$$

and write $S(g_i, g_j)$ as

$$S(g_i, g_j) = \sum_{\nu=1}^t h_{ij\nu} g_\nu \quad h_{ij\nu} \in A$$

$$\max_{\nu} (\text{lm}(h_{ij\nu}) \cdot \text{lm}(g_\nu)) = \text{lm} S(g_i, g_j)$$

Then

$$(*) \quad \text{Syz}(g_1, \dots, g_t) = \sum_{i,j} A \cdot \left(\underbrace{\frac{\text{lcm}(\text{lm}(g_i), \text{lm}(g_j))}{\text{lm}(g_i)} \vec{v}_i - \frac{\text{lcm}(\text{lm}(g_i), \text{lm}(g_j))}{\text{lm}(g_j)} \vec{v}_j}_{\substack{!! \\ S(g_i, g_j) \in A\vec{v}_1 + \dots + A\vec{v}_t}} - \sum_{\nu=1}^t h_{ij\nu} \vec{v}_\nu \right)$$

Pf: Suppose that $\text{Syz}(g_1, \dots, g_t) \not\subseteq \text{r.h.s. of } (*)$

Let $X = \min_{\sum_j u_j \vec{v}_j \in \text{Syz}(g_1, \dots, g_t) \setminus \text{r.h.s. of } (*)} \max_{1 \leq j \leq t} (\text{lm}(u_j) \cdot \text{lm}(g_j))$, a monomial in $A\vec{v}_1 + \dots + A\vec{v}_t$

W.l.o.g. Have $u_1 \vec{v}_1 + \dots + u_t \vec{v}_t \in \text{Syz}(g_1, \dots, g_t) \setminus \text{r.h.s. of } (*)$

$$\text{s.t. } \max_{1 \leq j \leq t} (\text{lm}(u_j) \cdot \text{lm}(g_j)) = X$$

Will produce an element $u'_1 \vec{v}_1 + \dots + u'_t \vec{v}_t \equiv u_1 \vec{v}_1 + \dots + u_t \vec{v}_t \pmod{\text{r.h.s. of } (*)}$

with $\max_{1 \leq j \leq t} (\text{lm}(u'_j) \cdot \text{lm}(g_j)) < X$, which is a contradiction.

Define

$$\bullet \quad S := \{j \in \{1, 2, \dots, t\} \mid \text{lm}(u_j) \cdot \text{lm}(g_j) = X\}$$

$$\bullet \quad w_j = \begin{cases} u_j & \text{if } j \notin S \\ u_j - \text{lt}(u_j) & \text{if } j \in S \end{cases}$$

$$\text{Have: } \sum_{j \in S} \text{lt}(w_j) \cdot \text{lm}(g_j) = 0, \text{ i.e. } \sum_{j \in S} \text{lt}(w_j) \vec{v}_j \in \text{Syz}(\text{lm}(g_1), \dots, \text{lm}(g_t))$$

$$\text{Prop 3} \Rightarrow \exists (a_{ij})_{i,j \in S} \text{ s.t. } \sum_{j \in S} \text{lt}(w_j) \vec{v}_j = \sum_{i,j \in S} a_{ij} \left(\frac{\text{lcm}(\text{lm}(g_i), \text{lm}(g_j))}{\text{lm}(g_i)} \vec{v}_i - \frac{\text{lcm}(\text{lm}(g_i), \text{lm}(g_j))}{\text{lm}(g_j)} \vec{v}_j \right)$$

$$\text{lm}(a_{ij}) \cdot \text{lcm}(\text{lm}(g_i), \text{lm}(g_j)) = X$$

$$\text{if } a_{ij} \cdot \text{lcm}(\text{lm}(g_i), \text{lm}(g_j)) \neq 0$$

Groeb 17

$$\Rightarrow \sum_{j=1}^t u_j \vec{v}_j - \sum_{i,j \in S} a_{ij} s(q_i, g_j) \in \text{Syz}(g_1, \dots, g_t)$$

$$\sum_{j=1}^t u'_j \vec{v}_j \quad \text{and} \quad \max_{1 \leq j \leq t} (\text{lm}(u'_j) \cdot \text{lm}(g_j)) < X. \quad \text{QED}$$

How to compute the syzygy module $\text{Syz}(u_1, \dots, u_s)$ of a set $(u_1, \dots, u_s)$ of generators $u_1, \dots, u_s$ of a submodule $M \subseteq A^m$, $A = k[x_1, \dots, x_n]$:

- 1) Expand the given set of generators $u_1, \dots, u_s$ to a Groebner basis $(g_1, \dots, g_t)$ of M w.r.t. a chosen term order on A^m (Buchberger's algorithm).
- 2) By Theorem 4, the process of computing $(g_1, \dots, g_t)$ during the execution of the Buchberger's algorithm also furnishes a set of generators of $\text{Syz}(g_1, \dots, g_t)$.
- 3) Use Lemma 2 to get a set of generators of $\text{Syz}(u_1, \dots, u_s)$.

Remark: Here we need to find $(a_{ij}) \in M_{s \times t}(A)$ such that

$g_j = \sum_{i=1}^s a_{ij} u_i$, which one obtains by tracking the computation of the Groebner basis $(g_1, \dots, g_t)$.

Groeb 18

§9 Applications of syzygies

(1) Compute the intersection of two ideals $I, J \subseteq R[x_1, \dots, x_n] = A$

$$\text{Let } I = \sum_{i=1}^s f_i A, \quad J = \sum_{j=1}^t g_j A.$$

Consider the Syzygy module $\text{Syz} \left(\begin{matrix} [1] \\ [1] \end{matrix}, \begin{matrix} [f_1] \\ [0] \end{matrix}, \dots, \begin{matrix} [f_s] \\ [0] \end{matrix}, \begin{matrix} [0] \\ [g_1] \end{matrix}, \dots, \begin{matrix} [0] \\ [g_t] \end{matrix} \right)$ of $u_i \in A^2 \quad \forall i$

Let $\left(\sum_{\mu=0}^{s+t} h_{e\mu} \vec{v}_\mu \right)_{1 \leq l \leq r}$ be a set of generators of $\text{Syz}(u_0, u_1, \dots, u_s, u_{s+1}, \dots, u_{s+t})$

$$\text{Then } I \cap J = \sum_{l=1}^r h_{e0} A$$

↑
the first coord of the syzygy $h_{e0} \vec{v}_0 + h_{e1} \vec{v}_1 + \dots + h_{e,s+t} \vec{v}_{s+t}$

(2) compute the intersection $M \cap N$ of two A -submodules of A^m , $A = k[x_1, \dots, x_n]$

(3) Let $I = f_1 A + f_2 A + f_3 A$, $J = g_1 A + g_2 A$, compute $(I : J)$ "ideal quotient"

$$\text{Consider } \text{Syz} \left(\begin{matrix} [f_1] \\ [f_2] \\ [f_3] \end{matrix}, \begin{matrix} [g_1] \\ [0] \\ [0] \end{matrix}, \begin{matrix} [g_2] \\ [0] \\ [0] \end{matrix}, \begin{matrix} [0] \\ [g_1] \\ [0] \end{matrix}, \begin{matrix} [0] \\ [g_2] \\ [0] \end{matrix}, \begin{matrix} [0] \\ [0] \\ [g_1] \end{matrix}, \begin{matrix} [0] \\ [0] \\ [g_2] \end{matrix} \right) \quad A = k[x_1, \dots, x_n]$$

The ideal of A generated by the first coordinates $(h_{e0})_{1 \leq l \leq r}$ of a set $\left(\sum_{\mu=0}^6 h_{e\mu} \vec{v}_\mu \right)_{1 \leq l \leq r}$ of generators of $\text{Syz}(u_0, u_1, \dots, u_6)$ is equal to $(I : J)$

(4) Let $M \subseteq A^m$ be an A -submodule of A^m , compute $\text{Ann}_A(A/M)$

(5) Let M, N be finitely generated A -modules, $A = k[x_1, \dots, x_n]$.

Compute (a) A free resolution of M

(b) $\text{Ext}_A^i(M, N)$, $\text{Tor}_i^A(M, N)$

Hilbert syzygy theorem =

Let M be a finitely generated graded A -module, $A = k[x_1, \dots, x_n]$, $k =$ a field.

There exists a finite minimal resolution

$$0 \rightarrow F_s \xrightarrow{\partial_s} \dots \rightarrow F_1 \xrightarrow{\partial_1} F_0 \xrightarrow{\partial_0} M \rightarrow 0 \quad \text{with } s \leq n \quad F_i = \text{finite free graded } A\text{-module}$$

That this resolution is minimal means:

$$\forall i \text{ with } 0 \leq i \leq s-1, \quad \dim_k \left(\frac{\text{Im}(\partial_i)}{(x_1, \dots, x_n) \cdot \text{Im}(\partial_i)} \right) = \text{rank}_A(F_i)$$

||
minimal number of generators of $\text{Im}(\partial_i)$

Corollary Let M be a finite A -module, $A = k[x_1, \dots, x_n]$, $k =$ a field.

There exists a finite free resolution

$$0 \rightarrow F_s \xrightarrow{\partial_s} \dots \rightarrow F_2 \xrightarrow{\partial_2} F_1 \xrightarrow{\partial_1} F_0 \xrightarrow{\partial_0} M \rightarrow 0 \quad \text{with } s \leq n+1$$

$$(M \cong \tilde{M} \otimes_{k[x_0, x_1, \dots, x_n]} k[x_0, x_1, \dots, x_n] / (1-x_0))$$

Remark ¹⁾ It is a deep result that every finitely generated projective $k[x_1, \dots, x_n]$ is free (Serre's conjecture, Theorem of Quillen - Suslin).
^a k field

$\Rightarrow$ Every finite A -module admits a finite free resolution of length $\leq n$.

2) There is a constructive proof of the above result, using method involving Groebner basis. See Theorem 3.10.4, p. 197 of "An Introduction to Gröbner Bases" by Adams and Loustaunau

Depth

Depth

Def 1 A : comm. ring M : A -module $a_1, \dots, a_r \in A$

$(a_1, \dots, a_r)$ is an M -regular sequence if

(1) $M \neq a_1 M + \dots + a_r M$

(2) a_i is not a zero divisor of $M/a_1 M + \dots + a_{i-1} M$.

(This notion depends on the order of the elements $a_1, \dots, a_r$.)

Def 2 M : A -module, $a_1, \dots, a_r \in A$, $I = a_1 A + \dots + a_r A$
 $(a_1, \dots, a_r)$ is an M -quasi-regular

sequence if the map

$$\psi: (M/IM) \otimes_A (A/I)[x_1, \dots, x_r] \xrightarrow{\sim} \text{gr}_I(M) \quad \text{as graded } (A/I)\text{-modules}$$

$$(M/IM^n)[x_1, \dots, x_r]$$

Prop 3 Suppose that $(a_1, \dots, a_r)$ is an M -regular sequence in an A -module M .

Then $(a_1^{n_1}, \dots, a_r^{n_r})$ is an M -regular sequence $\forall n_1, \dots, n_r \in \mathbb{N}_{\geq 1}$

pf Lemma If $\xi_1, \dots, \xi_r \in M$ and $a_1 \xi_1 + \dots + a_r \xi_r = 0$, then $\xi_i \in (a_1, \dots, a_r)M$
 $\forall i=1, \dots, r$

pf of Lemma: Induction on r . Obvious if $r=1$

$r \geq 2$: $\exists \eta_1, \dots, \eta_{r-1} \in M$ s.t. $\xi_r = a_1 \eta_1 + \dots + a_{r-1} \eta_{r-1}$

$0 = a_1 \xi_1 + \dots + a_r \xi_r = a_1 (\xi_1 + a_r \eta_1) + \dots + a_{r-1} (\xi_{r-1} + a_{r-1} \eta_{r-1})$

induction $\xi_i + a_r \eta_i \in (a_1, \dots, a_{r-1})M$ for $i=1, \dots, r-1$. q.e.d.

pf of Thm 3. Suffices to show: $a_1^n, a_2, \dots, a_r$ is M -regular $\forall n \in \mathbb{N}_{\geq 1}$

Induction on $n \geq 2$. $\xRightarrow{\text{induction}}$ $(a_1^{n-1}, a_2, \dots, a_r)$ is M -regular

Show inductively that $(a_1^n, a_2, \dots, a_i)$ is M -regular $\forall i=2, \dots, r-1$

$\xRightarrow{\text{induction}}$ $(a_1^n, a_2, \dots, a_{i-1})$ is M -regular.

Suppose $a_i \cdot x = a_1^n \xi_1 + \dots + a_{i-1} \xi_{i-1}$, $x, \xi_1, \dots, \xi_{i-1} \in M$

induction $x = a_1^{n-1} \eta_1 + a_2 \eta_2 + \dots + a_{i-1} \eta_{i-1}$ $\eta_1, \dots, \eta_{i-1} \in M$

hyp. for $n-1 \Rightarrow a_1^{n-1} (a_1 \xi_1 - a_i \eta_1) + a_2 (\xi_2 - a_i \eta_2) + \dots + a_{i-1} (\xi_{i-1} - a_i \eta_{i-1}) = 0$

$\xRightarrow{\text{Lemma}} a_1 \xi_1 - a_i \eta_1 \in (a_1^{n-1}, a_2, \dots, a_{i-1})M \Rightarrow a_i \eta_1 \in (a_1, \dots, a_{i-1})M \Rightarrow \eta_1 \in (a_1, \dots, a_{i-1})M$

QED $\Rightarrow x \in (a_1^n, a_2, \dots, a_{i-1})M$

Depth 2

Prop. 4 Let $(a_1, \dots, a_n)$ be an M -regular sequence, $a_1, \dots, a_n \in A$, $M = A$ -module
Then $(a_1, \dots, a_n)$ is M -quasi-regular

Lemma 5 Let $(b_1, \dots, b_m)$ be an M -quasi-regular sequence. Let $J = \sum_{j=1}^m b_j A$.

Suppose that $x \in A$, and $(JM : x) = JM$ (i.e. $M/JM \xrightarrow{x} M/JM$)

Then $(J^v M : x) = J^v M \quad \forall v \in \mathbb{N}_{\geq 1}$

Pf. Induction on $v \geq 1$. Suppose true for $v-1$, and $\xi \in M$, $x \cdot \xi \in J^v M$.

Want to show: $\xi \in J^v M$. Induction hypoth. $\Rightarrow \xi \in J^{v-1} M$

$\Rightarrow \exists$ homog. poly $F(Y_1, \dots, Y_m) \in M[Y_1, \dots, Y_m]$ of degree $v-1$ s.t. $\xi = F(b_1, \dots, b_m)$

$$x \cdot \xi = (x \cdot F(b_1, \dots, b_m)) \in J^v M$$

$$\in M[Y_1, \dots, Y_m]$$

$$\Rightarrow x \cdot F(Y_1, \dots, Y_m) \in JM[Y_1, \dots, Y_m]$$

$$\Rightarrow \text{all coef. of } x \cdot F(Y_1, \dots, Y_m) \text{ are in } JM \text{ q.e.d.}$$

Pf of Prop 4: Induction on n ; case $n=1$ trivial.

Suffices to show: If $F(X_1, \dots, X_n) \in M[X_1, \dots, X_n]$ homog. of degree v s.t.

s.t. $F(a_1, \dots, a_n) = 0$, then $F \in IM[X_1, \dots, X_n]$, i.e. all coef. of F are in IM .

Prove this statement by induction on v : suppose statement holds for $v-1$

Write $F(X_1, \dots, X_n) = G(X_1, \dots, X_{n-1}) + X_n \cdot H(X_1, \dots, X_n)$ $G(X_1, \dots, X_{n-1})$ homog, deg = v

$\Rightarrow a_n \cdot H(a_1, \dots, a_n) = -G(a_1, \dots, a_{n-1}) \in (a_1 A + \dots + a_{n-1} A) \cdot M$ $H(X_1, \dots, X_n)$ homog, deg = $v-1$

Lemma 5 $\Rightarrow H(a_1, \dots, a_n) \in (a_1 A + \dots + a_{n-1} A) \cdot M \subseteq (a_1 A + \dots + a_{n-1} A + a_n A) \cdot A$

$\Rightarrow$ (a) (Since H is homog of deg $v-1$) $\xRightarrow{\text{induction on } v} H(X_1, \dots, X_n) \in IM[X_1, \dots, X_n]$

(b) $\exists f(X_1, \dots, X_{n-1}) \in M[X_1, \dots, X_{n-1}]$, homog. of degree v , s.t. $f(a_1, \dots, a_{n-1}) = H(a_1, \dots, a_n)$

Let $g(X_1, \dots, X_{n-1}) = G(X_1, \dots, X_{n-1}) + a_n \cdot f(X_1, \dots, X_{n-1}) \in M[X_1, \dots, X_{n-1}]$, homog. of deg. v

We have: $g(a_1, \dots, a_{n-1}) = 0$

induction on $n \Rightarrow g(X_1, \dots, X_{n-1}) \in IM[X_1, \dots, X_{n-1}]$

$\Rightarrow G(X_1, \dots, X_{n-1}) = g(X_1, \dots, X_{n-1}) - a_n f(X_1, \dots, X_{n-1}) \in IM[X_1, \dots, X_{n-1}]$

$\Rightarrow F(X_1, \dots, X_n) = G + X_n H \in IM[X_1, \dots, X_n]$.

q.e.d.

Depth 3

$$a_i \in A$$

$$M \neq 0,$$

Prop 6 Suppose that $(a_1, \dots, a_n)$ is M -quasi-regular, $M/(a_1, \dots, a_n)M \neq 0$, and $M, M/a_1M, M/(a_1, a_2)M, \dots, M/(a_1, \dots, a_{n-1})M$ are I -adically separated, where $I = a_1A + a_2A + \dots + a_nA$. Then $(a_1, \dots, a_n)$ is M -regular.

Rank: The separation condition holds if ^(a) A is Noetherian, M f.g. A -module, $I \subseteq \text{rad}(A)$ or if ^(b) M is $\mathbb{N}$ -graded A -module, $a_1, \dots, a_n$ homog. $\deg > 0$.

Pf: Induction on n .

Case $n=1$: Suppose $x \in M$ and $a_1 x = 0 \Rightarrow$ show inductively that $x \in I^i M \forall i \in \mathbb{N}$

General n : Elementary argument $\Rightarrow$

$(a_2, \dots, a_n)$ is (M/a_1M) -quasi-regular

Example k : a field $A = k[X, Y, Z]$, $a_1 = XY-1$, $a_2 = Y-1$, $a_3 = YZ$

Claim 1 (a_1, a_2, a_3) is A -regular

$$k[X, Y, Z]/(XY, Y-1) \cong k[X, Z]/(X) \quad \sim \text{clear}$$

Claim 2 (a_1, a_3, a_2) is not A -regular

In fact, a_1, a_3 is not A -regular: $k[X, Y, Z]/(XY) \ni x \stackrel{\neq 0}{=} x \pmod{XY}$ and $a_3 x = 0$ in $k[X, Y, Z]/(XY)$

Conclusion: In favorable situations (such as those in the Rank after Prop 6), $(a_{\sigma(1)}, a_{\sigma(2)}, \dots, a_{\sigma(n)})$ is M -regular $\forall \sigma \in S_n$ if $(a_1, \dots, a_n)$ is M -regular.

But this is false in general.

Exer. Let A be a local ring and M a f.g. A -module. Let $a_1, \dots, a_n \in A$

Show that if $a_1, \dots, a_n$ is M -regular, then $a_{\sigma(1)}, \dots, a_{\sigma(n)}$ is M -regular

$\forall \sigma \in S_n$. Explain why localization argument does not prove that this statement holds for a general commutative ring.

Depth 4

Theorem 7. Let A be a Noetherian ring, M be a finite A -module.

$I \subseteq A$ be an ideal s.t. $IM \neq M$. Let $n \in \mathbb{N}_{\geq 1}$. The following are equivalent

(1) $\text{Ext}_A^i(N, M) = 0$ for $i=0, 1, \dots, n-1$ $\forall$ finite A -module N with $\text{supp}(N) \subseteq \text{Spec}(A/I)$

(2) $\text{Ext}_A^i(A/I, M) = 0$ for $i=0, 1, \dots, n-1$

(3) $\exists$ a finite A -module N with $\text{supp}(N) = \text{Spec}(A/I)$ s.t.

$\text{Ext}_A^i(N, M) = 0$ for $i=0, 1, \dots, n-1$

(4) $\exists$ an M -regular sequence $a_1, \dots, a_n$ with $a_j \in I \ \forall j=1, \dots, n$

Pf. (1) $\Rightarrow$ (2) $\Rightarrow$ (3) obvious

(3) $\Rightarrow$ (4): Show first that $\exists$ a non-zer-divisor in I .

Otherwise, $I \subseteq \bigcup_{\mathfrak{p} \in \text{Ass}_A(M)} \mathfrak{p} \Rightarrow \exists \mathfrak{p} \in \text{Ass}_A(M)$ s.t. $I \subseteq \mathfrak{p}$

$A/\mathfrak{p} \hookrightarrow M \Rightarrow 0 \neq \text{Hom}_{A/\mathfrak{p}}(A/\mathfrak{p}/\mathfrak{p}A/\mathfrak{p}, M/\mathfrak{p}M) \Rightarrow \text{Hom}_{A/\mathfrak{p}}(N/\mathfrak{p}N, M/\mathfrak{p}M) \neq 0$,
 $\uparrow$ a field
 $\text{Hom}_A(N, M) \otimes_A A/\mathfrak{p}$, contradiction

Pick $a_1 \in I$, $0 \rightarrow M \xrightarrow{a_1} M \rightarrow M_1 \rightarrow 0$

$\leadsto \text{Ext}_A^i(N, M_1) = 0$ for $i=0, 1, \dots, n-2 \xRightarrow{\text{induction}} \exists a_2, \dots, a_n \in I$ s.t. $(a_2, \dots, a_n)$ is M_1 -regular.

(4) $\Rightarrow$ (1) $0 \rightarrow M \xrightarrow{a_1} M \rightarrow M_1 = M/a_1M \rightarrow 0$

$\xRightarrow{\text{induction on } n} \exists \text{Ext}_A^i(N, M_1) = 0$ for $i=0, 1, \dots, n-2 \ \forall$ finite A -module N with $\text{supp}(N) \subseteq \text{Spec}(A/I)$

long exact sequence: (*) $0 \rightarrow \text{Ext}_A^i(N, M) \xrightarrow{a_1} \text{Ext}_A^i(N, M)$ for $i=0, 1, \dots, n-1$

$I \subseteq \text{rad}(\text{Ann}_A(N))$ i.e. $\exists r \in \mathbb{N}$ s.t. $a_1^r \cdot N = 0$

So (*) $\Rightarrow a_1^r \cdot \text{Ext}_A^i(N, M) \neq 0 \ \forall i \in \mathbb{N}$

$\text{Ext}_A^i(N, M) = 0$ for $i=0, 1, \dots, n-1 \ \forall$ finite A -module N with $\text{supp}(N) \subseteq \text{Spec}(A/I)$

QED

Depth 5

Defⁿ 8 Let M be a finite A -module, A Noetherian. Let $I \subseteq A$ be an ideal

1) The I -depth of M is

$$\text{depth}_I(M) = \min \{ i \in \mathbb{N} \mid \text{Ext}_A^i(A/I, M) \neq 0 \} \in \mathbb{N} \cup \{\infty\}$$

($\text{depth}_I(M) = \infty$ if $M = 0$)

2) The grade of M is

$$\text{grade}(M) = \min \{ i \in \mathbb{N} \mid \text{Ext}_A^i(M, A) \neq 0 \}$$

$$\begin{aligned} & \text{Thm 7} \quad \text{grade}(M) = \text{depth}_{\text{Ann}_A(M)}(A) \quad \leadsto \text{grade}(A/I) = \text{depth}_I(A) \end{aligned}$$

Lemma 9 A : Noetherian, M : finite A -module as before, $\text{grade}^k(M) < \infty$

$$\text{Ext}_A^i(M, N) = 0 \quad \forall i = 0, 1, \dots, \text{grade}(M) - \text{proj.dim}(N) - 1$$

$\text{proj.dim}(N)$ $\text{grade}(M)$

pf: Induction on l . Case $l=0$ immediate from defⁿ of $\text{grade}(M)$

$$0 \rightarrow N' \rightarrow F \rightarrow N \rightarrow 0 \quad \text{proj.dim}(N') = l-1$$

$\uparrow$
free

$$i \leq k-l-1 \Rightarrow \text{Ext}_A^i(M, F) \rightarrow \text{Ext}_A^i(M, N) \rightarrow \text{Ext}_A^{i+1}(M, N')$$

$\parallel$ $\circledast$ $i+1 \leq k-(l-1)-1$
0 and induction hypth. q.e.d.

Lemma 10 $(A, \mathfrak{m})$ Noeth. local, N, M : finite A -modules

Then

$$\text{Ext}_A^i(N, M) = 0 \quad \text{for } i = 0, 1, \dots, \text{depth}_{\mathfrak{m}}(M) - \dim(N) - 1$$

pf: Induction on $l = \dim(N)$, case $l=0$: clear by Thm 7

Assume $l > 0$. Dévissage on $N \leadsto$ May assume: $N \cong A/\mathfrak{p}$, $\mathfrak{p}$ = a prime ideal

Pick $x \in \mathfrak{m} \setminus \mathfrak{p} \leadsto$ have $0 \rightarrow N \xrightarrow{x} N \rightarrow N/xN \rightarrow 0$

$$A/(\mathfrak{p} + Ax) \quad \dim(N/xN) = l-1$$

$$i \leq \text{depth}(M) - \dim(N) - 1 \Rightarrow \text{Ext}_A^i(N, M) \xrightarrow{x} \text{Ext}_A^i(N, M) \rightarrow \text{Ext}_A^{i+1}(N/xN, M)$$

$\parallel \leftarrow$ induction

By Nakayama: $\text{Ext}_A^i(N, M) = 0$

q.e.d.

Depth 6

Theorem 11 $(A, \mathfrak{m})$ Noeth. local, M finite A -module

Then $\text{depth}(M) \leq \dim(A/\mathfrak{p}) \quad \forall \mathfrak{p} \in \text{Ass}_A(M)$

Pf. $\mathfrak{p} \in \text{Ass}_A(M) \Rightarrow \text{Hom}_A(A/\mathfrak{p}, M) \neq 0$

Lemma 10 $\Rightarrow \text{depth}(M) \leq \dim(A/\mathfrak{p}) \quad \text{q.e.d.}$

Lemma 12 $(A, \mathfrak{m})$ Noetherian local, M : finite A -module

$(a_1, \dots, a_r)$: M -regular sequence. Then

$$\dim(M/(a_1, \dots, a_r)M) = \dim(M) - r$$

Pf. $\geq$ obvious

$\leq$: May assume $r=1$. a_1 is M -reg $\Leftrightarrow a_1 \notin$ any minimal element of $\text{supp}(M)$. q.e.d.

Prop 13 A Noetherian, M : finite A -module, $I \subseteq A$ ideal

Then $\text{depth}_I(M) = \inf \{ \text{depth}(M_{\mathfrak{p}}) \mid \mathfrak{p} \in \text{Spec}(A/I) \}$

Pf. Either induction on r.h.s. of the above, (using Lemma 12), or use the Thm 7, plus

$$\text{Ext}_A^i(N, M)_{\mathfrak{p}} \cong \text{Ext}_{A_{\mathfrak{p}}}^i(N \otimes_A A_{\mathfrak{p}}, M \otimes_A A_{\mathfrak{p}}) \quad \forall \mathfrak{p} \in \text{Spec}(A) \quad \text{q.e.d.}$$

(a) A finite module M

Def 14 over a Noeth. local ring $(A, \mathfrak{m})$ is Macaulay, or Cohen-Macaulay, if either $M=0$, or if $\text{depth}_{\mathfrak{m}}(M) = \dim(M)$

(b) A Noeth. local ring $(A, \mathfrak{m})$ is CM if A is a CM A -module

Prop 14 $(A, \mathfrak{m})$ Noeth. local ring, M : finite A -module

(a) If M is CM and $\mathfrak{p} \in \text{Ass}(M)$, then $\text{depth}(M) = \dim(A/\mathfrak{p})$.

(unmixedness)

In particular M has no associated primes, and $\text{supp}(M)$ is equi-dim^l

(b) Let $(a_1, \dots, a_r)$ be an M -reg. sequence, and let $M' \stackrel{\text{def}}{=} M/(a_1, \dots, a_r)M$.

Then M is CM $\Leftrightarrow M'$ is CM

(c) Suppose M is CM. Then $M_{\mathfrak{p}}$ is a CM $A_{\mathfrak{p}}$ module $\forall \mathfrak{p} \in \text{supp}(M)$
and $\text{depth}_{\mathfrak{p}}(M) = \text{depth}_{A_{\mathfrak{p}}}(M_{\mathfrak{p}}) \quad \forall \mathfrak{p} \in \text{supp}(M)$

Depth 7

Pf (a) Given $\mathfrak{p} \in \text{Ass}(M) \Rightarrow M_{\mathfrak{p}} \neq 0 \leadsto \text{depth}(M) = \dim(M) \geq \dim(A/\mathfrak{p})$

Combined with the general inequality $\text{depth}(M) \leq \dim(A/\mathfrak{p})$ gives = (Thm 11).

(b) Note first that $M=0 \Leftrightarrow M' = M/(a_1 \dots a_r)M$ (Nakayama). Assume $M \neq 0$.

Have $\dim(M') = \dim(M) - r$ and $\text{depth}(M') = \text{depth}(M) - r$ (Thm 7).

(c). May assume $M_{\mathfrak{p}} \neq 0$.

Clearly: $\dim(M_{\mathfrak{p}}) \geq \text{depth}_{A_{\mathfrak{p}}}(M_{\mathfrak{p}}) \geq \text{depth}_{\mathfrak{p}}(M)$.

Prove $\text{depth}_{A_{\mathfrak{p}}}(M_{\mathfrak{p}}) = \text{depth}_{\mathfrak{p}}(M)$ by induction on $\text{depth}_{\mathfrak{p}}(M)$.
 $\because \text{Ext}_A^i(A/\mathfrak{p}, M) = 0 \Rightarrow \text{Ext}_{A_{\mathfrak{p}}}^i(A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}}, M_{\mathfrak{p}}) = 0$

Key case: when $\text{depth}_{\mathfrak{p}}(M) = 0$ i.e. $\exists \mathfrak{q} \in \text{Ass}_A(M)$ s.t. $\mathfrak{p} \subseteq \mathfrak{q}$. $\overset{\text{Ann}_A(M)}{\mathfrak{p} \subseteq \mathfrak{q}} \Rightarrow \mathfrak{p} = \mathfrak{q}$ by (a)

case when $\text{depth}_{\mathfrak{p}}(M) > 0$. Pick $x \in \mathfrak{p}$ which is M -regular $\Rightarrow \dim M_{\mathfrak{p}} = 0 \Rightarrow \text{depth}_{A_{\mathfrak{p}}}(M_{\mathfrak{p}}) = 0$

$\leadsto \text{depth}_{\mathfrak{p}}(M) = 1 + \text{depth}_{\mathfrak{p}}(M/xM) \stackrel{\text{induction}}{=} 1 + \text{depth}_{A_{\mathfrak{p}}}(M_{\mathfrak{p}}/xM_{\mathfrak{p}}) = \text{depth}_{A_{\mathfrak{p}}}(M_{\mathfrak{p}})$

$\because M/xM$ is CM by (b)

QED

Theorem 15. Let $(A, \mathfrak{m})$ be a CM Noth local ring

(a) $\text{ht}(I) = \text{depth}_I(A) = \text{grade}(A/I)$ $I \subseteq \mathfrak{m}$ an ideal

$\text{ht}(I) + \dim(A/I) = \dim(A)$

(b) A is catenary, i.e. $\forall \mathfrak{p} \subseteq \mathfrak{q} \in \text{Spec}(A)$, all maximal chains of prime ideals between $\mathfrak{p}$ and $\mathfrak{q}$ have the same length

(c) $\forall a_1, \dots, a_r \in \mathfrak{m}$, the following are equivalent

(i) $a_1, \dots, a_r$ is A -regular

(ii) $\text{ht}(a_1, \dots, a_i) = i \quad \forall i = 1, \dots, r$

(iii) $\text{ht}(a_1, \dots, a_r) = r$

(iv) $\exists a_{r+1}, \dots, a_n$ with $n = \dim(A)$ s.t. $(a_1, \dots, a_n)$ is a system of parameters of A

Pf. (c): (i) $\Rightarrow$ (ii) $\Rightarrow$ (iii) $\Rightarrow$ (iv) easy.

(iv) $\Rightarrow$ (i): must show: every system of parameters is a regular sequence

Depth 8

Given a system of parameters $x_1, \dots, x_n$ of A . $\leadsto x_1$ is not a zero-divisor
 $\Rightarrow A/x_1A$ is CM. Conclude by induction on $\dim(A)$

(a) Let $a_1, \dots, a_r \in I$, an A -reg. sequence, $r = \text{depth}_I(A)$

$$(c) \Rightarrow \text{ht}(a_1, \dots, a_r) = r \leq \text{ht}(I) \quad \because a_1A + \dots + a_rA \subseteq I$$

$$= \text{depth}_I(A)$$

Conversely, pick $b_1, \dots, b_s \in I$ s.t. $\text{ht}(b_1, \dots, b_i) = i \quad \forall i=1, \dots, s$
 $s = \text{ht}(I)$

(c) $\Rightarrow b_1, \dots, b_s$ is an A -reg. sequence $\Rightarrow s \leq \text{depth}_I(A)$
 $\text{ht}(I)$

Have shown:

$$\text{ht}(I) = \text{depth}_I(A) = \text{grade}(A/I)$$

Must show $\dim(A/I) + \text{ht}(I) = \dim(A)$ (Note: $\leq$ holds always)

Suffices to show:

$$\dim \text{ht}(\mathfrak{f}) = \dim(A) + \dim(A/\mathfrak{f}) \quad (\text{Exer.})$$

$$\forall \mathfrak{f} \in \text{Spec}(A)$$

Given $\mathfrak{f} \in \text{Spec}(A)$.

Know $A_{\mathfrak{f}}$ is CM (Prop 14) $\leadsto \text{ht}(\mathfrak{f}) = \dim(A_{\mathfrak{f}}) = \text{depth}(A_{\mathfrak{f}}) = \text{depth}_{\mathfrak{f}}(A)$

$\Rightarrow \exists$ an A -regular sequence $a_1, \dots, a_r \in \mathfrak{f}$ $r = \text{depth}_{\mathfrak{f}}(A)$

$\leadsto A/(a_1A + \dots + a_rA)$ is CM, of dim $\dim(A) - r$

and $\mathfrak{f}$ is a minimal element in $\text{Ass}(A/(a_1A + \dots + a_rA))$

$$\text{and } \dim(A/\mathfrak{f}) = \text{depth}(A/(a_1A + \dots + a_rA)) = \dim(A) - r$$

$$= \dim(A) - \text{ht}(\mathfrak{f})$$

(b) $\mathfrak{f} \supseteq \mathfrak{q}_{\mathfrak{f}} \quad A_{\mathfrak{f}}$ is CM.

$$(a) \Rightarrow \dim(A_{\mathfrak{f}}) = \text{ht}_{A_{\mathfrak{f}}}(\mathfrak{q}_{\mathfrak{f}}A_{\mathfrak{f}}) + \dim(A_{\mathfrak{f}}/\mathfrak{q}_{\mathfrak{f}}A_{\mathfrak{f}}) \quad \text{QED.}$$

Def 15 A commutative Noetherian $I \subseteq A$ ideal

(a) We say A is CM if $A_{\mathfrak{f}}$ is CM $\forall \mathfrak{f} \in \text{Spec}(A)$
 (or equiv. $A_{\mathfrak{m}}$ is CM $\forall \mathfrak{m} \in \text{Spm}(A)$)

(b) We say I is unmixed if $\text{ht}(\mathfrak{f}) = \text{ht}(I) \quad \forall \mathfrak{f} \in \text{Ass}(A/I)$

Depth 9

Def 6 (c): We say that "the unmixedness theorem holds for A " if every ideal I generated by $\text{ht}(I)$ elements is unmixed

Note: If $r = \text{ht}(I)$, $a_1, \dots, a_r \in I$ and $I = a_1 A + \dots + a_r A$, then $\text{ht}(\mathfrak{p}) \geq r \quad \forall \mathfrak{p} \in \text{Ass}_A(A/I)$. So the condition cond^n for I means: A/I has no embedded prime

Prop 17 A Noetherian commutative ring is Cohen-Macaulay iff the unmixedness theorem holds for A .

Theorem 18 Let A be a CM Noetherian ring. Then $A[X_1, \dots, X_n]$ is CM.

Cor. A CM $\Rightarrow$ every f.g. A -algebra is catenary

Pf of Thm 18. May assume $n=1$. $B = A[X]$, $P \in \text{Spec}(B)$, $\mathfrak{p} = P \cap A$

Must show: $B_{\mathfrak{p}}$ is CM. May assume: A is local $\mathfrak{p} = \text{max ideal of } A$

$\Rightarrow B/\mathfrak{p}B = k[X]$ k : a field

$\Rightarrow$ either $P = \mathfrak{p}B$, or $P = \mathfrak{p}B + fB$, $f \in B[X]$ monic and $\deg(f) > 0$

Let $a_1, \dots, a_d$ be an A -regular sequence in $\mathfrak{p}$, $d = \dim(A)$

Case $P = \mathfrak{p}B \Rightarrow \dim(B_{\mathfrak{p}}) = \dim A$ Note: $a_1, \dots, a_d$ is also a B -regular sequence in $B \because B/A$ is flat
 $\Rightarrow \text{depth}_{\mathfrak{p}}(B_{\mathfrak{p}}) = d = \dim(B_{\mathfrak{p}})$ O.K.

Case $P = \mathfrak{p}B + fB \Rightarrow \dim(B_{\mathfrak{p}}) = \dim(A) + 1$

$\Rightarrow (a_1, \dots, a_d, f)$ is a regular sequence in P

$\because f$ is a non-zero divisor in $A/(a_1 A + \dots + a_d A)[X]$
 $\nwarrow$ monic.

$\Rightarrow \text{depth}_{\mathfrak{p}}(B_{\mathfrak{p}}) = d+1$ O.K.

Q.E.D.

Reg 1

Def 1 A commutative ring A is normal if $A_{\mathfrak{p}}$ is an integral domain which is integrally closed in $\text{frac}(A_{\mathfrak{p}})$ $\forall \mathfrak{p} \in \text{Spec}(A)$

Def 2(a) Let $A \subseteq B$ be commutative rings, and let $u \in B$

We say that u is integral over A if $\exists$ a monic polynomial $f(X) \in A[X]$ s.t. $f(u) = 0$, or equivalently, $\exists$ a finite A -submodule $M \subseteq B$ such that $u \cdot M \subseteq M$

Def 2(b) Let A be a commutative ring, and let $B = \text{frac}(A) = \text{total ring of fractions of } A$. An element $u \in B$ is almost integral over A if $\exists$ a non-zero divisor $a \in A$ s.t. $a \cdot A[u] \subseteq A$. In other words $(A : A[u])$ contains a non-zero divisor of A

Note: (i) $u \in \text{frac}(A)$ is integral $\Rightarrow u$ is almost integral

(ii) A Noetherian $\Rightarrow$ (almost integral $\Rightarrow$ integral)

Def 2(c) (i) A commutative ring is normal if $A_{\mathfrak{p}}$ is a local domain integrally closed in $\text{frac}(A_{\mathfrak{p}})$ $\forall \mathfrak{p} \in \text{Spec}(A)$.

(ii) A commutative ring A is completely normal if A contains every element $u \in \text{frac}(A)$ which is almost integral over A

Prop 3 (1) A completely normal domain $\Rightarrow$ so are $A[x_1, \dots, x_n]$ and $A[[x_1, \dots, x_n]]$

(2) A normal domain $\Rightarrow$ so is $A[x_1, \dots, x_n]$.

Pf (1) A completely normal domain. Consider $A[X]$. Let $K = \text{frac}(A)$.

$u \in K(x)$ almost integral over $A[x] \Rightarrow u \in K[x]$, and the leading coeff of u is almost integral over A

The same argument works for $A[[X]] \Rightarrow$ The leading coeff of u is in A , etc.

Reg 2

(2) Suppose that A is a normal domain. Given $u \in K(X)$, integral over $A[X]$.
Write $u = \frac{f(X)}{g(X)}$ and let $A_0 =$ the subring of A generated by coefficients of $f(X)$ and $g(X)$.
 $f(X), g(X) \in A[X]$ $\uparrow$ Noetherian

The argument in (1) shows that :

• $u \in K[x]$, and all coefficients b_j of u are almost integral over A_0 .
 $\Rightarrow b_d x^d + \dots + b_0$, $b_j \in K$ A_0 Noetherian $\Rightarrow b_j$ is integral over $A_0 \forall j$
 $\Rightarrow b_j \in A \quad \forall j = 0, 1, \dots, d$ QED

Recall / Defⁿ:

Recall / Defⁿ: A comm. ring
 $\forall$ ideal $J \subseteq A$, Consider the family $\{I \mid \begin{matrix} I \subseteq A \text{ ideal} \\ I \subseteq Z(A/J) = \text{zero divisors of } A/J \end{matrix}\} =: \mathcal{I}_{A/J}$
 $\Rightarrow Z(A/J) = \bigcup \text{maximal elements } P \text{ in } \mathcal{I}$
 and every maximal element of $\mathcal{I}$ is a prime ideal of A

Prp 4 Let A be a commutative ring.

Then $A = \left\{ y \in \text{frac}(A) \mid \begin{array}{l} \text{the image of } y \text{ in } \text{frac}(A_S) \text{ lies in } A_S \\ \forall \text{ max. element } S \text{ contained in } Z(A_S/A) \\ S = \text{a non-zero divisor in } A \end{array} \right\}$

Symbolically -

$A = \bigcap_{\mathfrak{p}} A_{\mathfrak{p}}$, $\mathfrak{p}$ runs through all prime ideals st. $\exists s \in A$, s not a zero divisor and $\mathfrak{p}$ is a maximal element of the family $\mathcal{F}_{A/sA}$

Pf. Suppose that $y = \frac{a}{s} \in \bigcap_{\mathfrak{p}} A_{\mathfrak{p}}$, $0 \neq a \in A$, $s = \text{not a zero divisor of } A$

Let $I := (sA : aA)$. Suppose that $y \notin A$, i.e. $I \neq A \Leftrightarrow a \notin sA$

$\Rightarrow I \subseteq Z(A/A)$. Let $\mathfrak{p}$ be a maximal element

among the family of ideals I' s.t. $I \subseteq I' \subseteq Z(A/sA)$

Know: The image of y in $\text{fibre}(A_j)$ is in A_j , i.e. $\exists t \notin \emptyset, b \in A$

∴ $ta = sb \Rightarrow t \in I \Rightarrow t \in J$, a contradiction

q.e.d.

Reg 3

Rmk: (a) Prop 4 is often statement in the case when A is a domain (and also Noetherian)

(b) There are two generalizations of the notion of associated primes to non-Noetherian case. In prop 4 we used the maximal prime ideals contained in $Z(A/sA)$, s : non-zero-divisor in A . Nagata's approach/defⁿ of "prime divisors", denoted by $\text{Ass}_d(A/IA)$ in Exercise set 3, is based on this consideration.

(Recall) Prop 5. Let $(A, \mathfrak{m})$ be a Noetherian local ring. Then A is a regular local ring iff it is normal

Lemma 6 ^{A Noetherian domain} $A \ni a \neq 0$, $\mathfrak{P} \in \text{Ass}_A(A/aA)$. Then $\mathfrak{P}^{-1} \stackrel{\text{def}}{=} \{x \in \text{frac}(A) : x \cdot \mathfrak{P} \subseteq A\} \neq A$
 pf: $\exists b \in A, aA$ s.t. $(aA : bA) = \mathfrak{P} \leadsto \frac{b}{a} \in \mathfrak{P}^{-1}$ q.e.d.

Lemma 7 $(A, \mathfrak{m})$: Noeth local domain. Assume that $\mathfrak{m} \mathfrak{m}^{-1} = A$ (b)
 Then A is regular of $\dim = 1$; i.e. A is a DVR

pf: Pick $a \in \mathfrak{m} \setminus \mathfrak{m}^2$, Consider $a \cdot \mathfrak{P}^{-1} \subseteq A \leadsto a \cdot \mathfrak{P}^{-1} \not\subseteq \mathfrak{P}$, for otherwise
 i.e. $a \cdot \mathfrak{P}^{-1} = A \Rightarrow aA = \mathfrak{P}$ q.e.d. $a \cdot \mathfrak{P}^{-1} \cdot \mathfrak{P} \subseteq \mathfrak{P}^2$
 $a \cdot A \subseteq \mathfrak{P}^2$

Prop 8 Let A be a Noetherian normal domain. Then every non-zero principal ideal is unmixed, (b) $A = \bigcap_{\text{ht}(\mathfrak{P})=1} A_{\mathfrak{P}}$. (c) $A_{\mathfrak{P}}$ is CM $\forall \mathfrak{P}$ with $\text{ht}(\mathfrak{P}) \leq 2$

pf: Consider $\mathfrak{P} \in \text{Ass}(A/aA)$, $a \neq 0$. May and do assume: A is local

By Lemma 6, $\mathfrak{P}^{-1} \neq A$ Claim: $\mathfrak{P} \mathfrak{P}^{-1} = A$. Otherwise $\mathfrak{P} \mathfrak{P}^{-1} = \mathfrak{P}$
 $\Rightarrow \mathfrak{P} (\mathfrak{P}^{-1})^n = \mathfrak{P} \quad \forall n \Rightarrow$ Every element of $\mathfrak{P}^{-1}$ is integral over A
 $\Rightarrow \mathfrak{P}^{-1} \subseteq A$, contradiction Claim proved

Lemma 7 $\Rightarrow \text{ht}(\mathfrak{P}) = 1$, $\forall \mathfrak{P} \in \text{Ass}(A/aA)$. Have proved (a)

(b) Follows from (a) and Prop 4

(c) also follows.

QED.

Reg 4

Def 9 Conditions (S_i) and (R_i) for a commutative ring A $i \in \mathbb{N}$

$$(S_i) = \text{depth}(A_{\mathfrak{p}}) \geq \inf(i, \text{ht}(\mathfrak{p})) \quad \forall \mathfrak{p} \in \text{Spec}(A)$$

$$(R_i) = A_{\mathfrak{p}} \text{ is regular } \quad \forall \mathfrak{p} \in \text{Spec}(A) \text{ with } \text{ht}(\mathfrak{p}) \leq i$$

Remark: (S_0) holds always, (S_1) means: $\text{Ass}_A(0) = \{\text{minimal ideals of } A\}$

(S_2) means: $\text{Ass}_A(0)$ has no embedded primes and $\text{Ass}_A(A/aA)$ has no embedded primes for every non-zero-divisor a in A

$$(S_0) + (R_0) \Leftrightarrow A \text{ is reduced}$$

Thm 10 A Noetherian ring A is normal iff it satisfies (S_2) and (R_1)

Pf "only if": Prop 5 $\Rightarrow (R_1)$ Prop 8 $\Rightarrow (S_2)$

"if": Let $\text{frac}(A) = \text{total ring of fractions of } A \cong K_1 \times \dots \times K_m$ $K_i = \text{fields}$

Let $\mathfrak{p}_1, \dots, \mathfrak{p}_m$ be the minimal ideals of A $\because A$ is reduced

$$(0) = \mathfrak{p}_1 \cap \dots \cap \mathfrak{p}_m \quad A \hookrightarrow (A/\mathfrak{p}_1) \times \dots \times (A/\mathfrak{p}_m) \quad K_i = \text{frac}(A/\mathfrak{p}_i)$$

Claim: A is integrally closed in $K_1 \times \dots \times K_m$

$$\text{Claim} \Rightarrow e_i \in A \quad \forall i$$

$$e_i = i\text{-th idempotents} \\ \sum_i e_i = 1, \quad e_i \cdot e_j = \begin{cases} 0 & i \neq j \\ 1 & i = j \end{cases}$$

$$\leadsto A_i := A \cdot e_i \subseteq A \quad \forall i \text{ and } A = A_1 \times \dots \times A_m$$

Suppose $\frac{a}{b} \in \text{frac}(A)$, $a, b \in A$, b is a non-zero-divisor

$$\left(\frac{a}{b}\right)^n + c_{n-1} \left(\frac{a}{b}\right)^{n-1} + \dots + c_1 \left(\frac{a}{b}\right) + c_0 = 0 \quad c_{n-1}, \dots, c_0 \in A$$

$$\text{i.e. } a^n + c_{n-1} a^{n-1} b + \dots + c_1 a b^{n-1} + c_0 b^n = 0$$

$$A \text{ is } S_2, \quad A = \bigcap_{\text{ht}(\mathfrak{p})=1} A_{\mathfrak{p}}$$

Suffices to show: $a \in b A_{\mathfrak{p}} \quad \forall \mathfrak{p} \in \text{Spec}(A)$. But $A_{\mathfrak{p}}$ is a DVR by (R_2) .

QED.

Reg 5

Prop 11 Let A be a Noetherian regular ring, i.e. $A_{\mathfrak{p}}$ is a regular local ring $\forall \mathfrak{p} \in \text{Spec}(A)$. Then $A[X_1, \dots, X_n]$ is regular $\forall n \in \mathbb{N}$

pf May assume A is local with max ideal $\mathfrak{m}$

$P =$ a prime ideal of $A[X]_{\mathfrak{B}}$ $P \cap A = \mathfrak{m}$ $\mathfrak{m} = x_1 A + \dots + x_d A$, $x_i \in \mathfrak{m} \setminus \mathfrak{m}^2$

Must show: B_P is regular

Two cases (a) $P = \mathfrak{m}B$ (b) $P = \mathfrak{m}B + f(X)B$, $f(X)$ monic in $B = A[X]$

Case (a): $P = x_1 B + \dots + x_d B$ $\dim B_P = d$

Case (b): $P = x_1 B + \dots + x_d B + f \cdot B$ $\dim B_P = d+1$ q.e.d.

Recall: $M = A$ -module

$\text{proj. dim}_A(M) =$ the length of a shortest projective resolution of M

$\text{inj. dim}_A(M) =$ the length of a shortest injective resolution of M

Lemma/Fact 12. (a) M is projective $\Leftrightarrow \text{Ext}_A^1(M, N) = 0 \quad \forall A$ -module N

(b) M is injective $\Leftrightarrow \text{Ext}_A^1(A/I, M) = 0 \quad \forall$ ideal $I \subseteq A$

Lemma/Fact 13 The following statements for a commutative ring A and an integer $n \in \mathbb{N} \cup \{\infty\}$ are equivalent

(i) $\text{proj. dim}_A(M) \leq n \quad \forall A$ -module M

(ii) $\text{proj. dim}_A(M) \leq n \quad \forall$ finite A -module M

(iii) $\text{inj. dim}_A(M) \leq n \quad \forall A$ -module M

(iv) $\text{Ext}_A^{n+1}(M, N) = 0 \quad \forall A$ -modules M, N

Defⁿ: The global dimension of A is

$$\text{gl. dim}(A) = \sup_{\substack{M \\ \uparrow \\ A\text{-module}}} (\text{proj. dim}(M)) = \sup_M (\text{inj. dim}(M))$$

Cor / Fact 14 A finite module M over a Noetherian ring A is projective iff $\text{Ext}_A^1(M, N) = 0 \quad \forall$ finite A -module N

Reg 6

Lemma / Fact 15 $(A, \mathfrak{m})$ Noetherian local, $k = A/\mathfrak{m}$

M : finite A -module. Then

$$\text{proj. dim}_A(M) \leq n \iff \text{Tor}_{n+1}^A(M, \kappa) = 0$$

pf. " $\Rightarrow$ ": obvious

" $\Leftarrow$ " Key case: $n=0$. So assume $\text{Tor}_1^A(M, \kappa) = 0$. ^{Consider} $0 \rightarrow M_1 \rightarrow L \xrightarrow{u} M \rightarrow 0$

$$\Rightarrow \begin{array}{ccccccc} \text{Tor}_1^A(M, \kappa) & \rightarrow & M \otimes_A \kappa & \rightarrow & L \otimes_A \kappa & \xrightarrow[\sim]{\bar{u}} & M \otimes_A \kappa \rightarrow 0 \\ \parallel & & & & & & \uparrow \\ 0 & \Rightarrow & M \otimes_A \kappa = 0 & \Rightarrow & M_1 = 0 & & \text{finite free s.t.} \\ & & & & & & L/\text{nr} L \xrightarrow[\sim]{\bar{u}} M/\text{nr} \cdot M \end{array}$$

Cor / Exer. 16 A Noetherian

(1) $\text{proj. dim}_A(M) \leq n \iff \text{Tor}_{n+1}^A(M, A/\mathfrak{p}) = 0 \quad \forall \mathfrak{p} \in \text{Spec}(A), M: A\text{-module}$

(2) The following are equivalent

(i) $\text{gl. dim } (A) \leq n$

(ii) $\text{proj. dim}_A(N) \leq n \quad \forall \text{ finite } A\text{-module } N$

(iii) $\text{inj dim}_A(N) \leq n \quad \forall \text{ finite } A\text{-module } N$

(iv) $\text{Ext}_A^{n+1}(N, N') = 0 \quad \forall \text{ finite } A\text{-modules } N, N'$

(v) $\text{Tor}_A^{n+1}(N, N') = 0 \quad \forall \text{ finite } A\text{-modules } N, N'$

$$(3) \quad \text{gl. dim}(A) = \sup_{P \in \text{Spec}(A)} \text{gl. dim}(A_P)$$

Prop. 17 (A, m) Noetherian local, $n = A/m$. Then, $n \in \mathbb{N}$

$$\text{gl. dim}(A) \leq n \iff \text{Tor}_{n+1}^A(\kappa, \kappa) = 0$$

pf. " $\Leftarrow$ ": $\text{Tor}_{n+1}^A(\kappa, \kappa) = 0 \Rightarrow \text{proj. dim}_A(\kappa) \leq n \Rightarrow \text{Tor}_{n+1}^A(M, \kappa) = 0$ $\forall A$ -module M

$\text{gl. dim}(A) \leq n \Leftarrow \text{proj. dim}_A(M) \leq n$ $\swarrow \text{Lemma 15}$

Cor 16 $\forall$ finite A -module M

Lemma 18 $(A, \mathfrak{m})$ Noeth. local, $\kappa = A/\mathfrak{m}$, M : finite A -module

If $\text{proj. dim}(M) = m < \infty$, and $x \in R$ is M -regular, then $\text{proj. dim}_A(M/xM) = m+1$

pf. $0 \rightarrow M \xrightarrow{x} M \rightarrow M/xM \rightarrow 0 \rightsquigarrow \text{Tor}_{m+1}^A(M/xM, K) \cong \text{Tor}_m^A(M, K) \neq 0$
and $\text{Tor}_i^A(M/xM, K) = 0 \quad \forall i \geq m+2$. q.e.d.

Reg 7

Prop. 19 (Auslander-Buchsbaum) $(A, \mathfrak{m})$ Noetherian local ring, $\kappa = A/\mathfrak{m}$

M : finite A -module. Assume $\text{proj dim}_A(M) < \infty$. Then
 $\text{proj dim}(M) + \text{depth}(M) = \text{depth}(A)$

pf: Induction on $h = \text{proj dim}(M)$

Case $h=0$ obvious

Key case: $h=1$. $\Rightarrow$ Have a minimal free resolution $L_1 \cong A^r, L_2 \cong A^s$
 $0 \rightarrow L_1 \xrightarrow{\alpha} L_0 \xrightarrow{u} M \rightarrow 0$ st. $\alpha \in \mathfrak{m} \cdot \text{Hom}_A(L_1, L_0)$

$$\begin{aligned} \Rightarrow 0 \rightarrow \text{Hom}_A(\kappa, L_1) \xrightarrow{0} \text{Hom}_A(\kappa, L_0) &\rightarrow \text{Hom}_A(\kappa, M) \xrightarrow{\text{and } u \otimes \kappa} L_0 \otimes_A \kappa \xrightarrow{\sim} L_1 \otimes_A \kappa \\ \rightarrow \text{Ext}_A^1(\kappa, L_1) \xrightarrow{0} \text{Ext}_A^1(\kappa, L_0) &\rightarrow \text{Ext}_A^1(\kappa, M) \rightarrow \text{Ext}_A^1(\kappa, L_0) \rightarrow \dots \end{aligned}$$

$$\Rightarrow \text{Hom}_A(\kappa, L_1) = 0, \text{ i.e. } \text{Hom}_A(\kappa, A) = 0,$$

$$\text{and } 0 \rightarrow \text{Ext}_A^i(\kappa, A)^s \rightarrow \text{Ext}_A^i(\kappa, M) \rightarrow \text{Ext}_A^{i+1}(\kappa, A)^r \rightarrow 0$$

$\forall i \geq 0$.

$\Rightarrow \text{depth}(A) = \text{depth}(M) + 1$. This is the equality when $\text{proj dim}(M)=1$ ^{asserted}

Case $h \geq 2$: Take a minimal resolution of M , and reduce to the

case when $\text{proj dim}(N)$

$$= \text{proj dim}(M) - 1 \geq 1$$

$$0 \rightarrow N \rightarrow L_0 \rightarrow M \rightarrow 0$$

$\uparrow$
finite free

$$\Rightarrow \text{depth}(N) = \text{depth}(A) - \text{proj dim}(N)$$

$$\Rightarrow \text{depth}(N) = \text{depth}(M) + 1$$

QED.

Reg 8

Prop. 20 (A, m, κ) Noetherian reg. local ring of dimension d . Then $\text{gl. dim}(A) = d$

Pf. Lemma 18 $\Rightarrow \text{proj dim}_A(\kappa) = d \xRightarrow{\text{Prop 17}} \text{gl. dim}(A) = d$. q.e.d.

Cor²¹ (Hilbert syzygy theorem, homological proof)

k : field $\leadsto$ gl. dim $k[x_1, \dots, x_n] = n$

(Immediate from Prop. 11, Cor 16 and Prop 20)

The converse of Prop. 20 holds (Serre's Theorem): If $(A, \mathfrak{m})$ is a Noeth. local ring with finite global dim, then $(A, \mathfrak{m})$ is regular.

Def 22 (Koszul complex) Let A be a commutative ring. $x_1, \dots, x_n \in A$

(i) $K_*(x_i) \stackrel{\text{def}}{=} \left(0 \rightarrow A \cdot e_i \xrightarrow{x_i} A \rightarrow 0 \right)$ a complex of length 1 chain

(ii) $K_*(X) \stackrel{\text{def}}{=} K_*(X_1, \dots, X_n) = K_*(X_1) \otimes_A \dots \otimes_A K_*(X_n)$ tensor product of chain complexes

(iii) $K_*(\underline{X}, M) \stackrel{\text{def}}{=} K_*(\underline{X}) \otimes_A M$
 $\quad \quad \quad \swarrow$ thought of as a chain complex of length 0 concentrated at degree 0

(iv) Notation: $L = A \cdot e_1 \oplus \dots \oplus A \cdot e_n$ free A -module with basis $e_1, \dots, e_n$

$$K_p(x_1, \dots, x_n) = \bigwedge_A^p (L) = \bigoplus_{\substack{\alpha = (i_1, \dots, i_p) \\ 1 \leq i_1 < i_2 < \dots < i_p \leq n}} A \cdot e_{\alpha_1} \wedge \dots \wedge e_{\alpha_p}$$

$$d(e_{\alpha_1} \wedge \dots \wedge e_{\alpha_p}) = \sum_{r=1}^p (-1)^{r-1} x_{\alpha_r} e_{\alpha_1} \wedge \dots \wedge e_{\alpha_{r-1}} \wedge e_{\alpha_{r+1}} \wedge \dots \wedge e_{\alpha_p}$$

Lemma 23 C : a chain complex of A -modules, $x \in A$. $K(x) = (0 \rightarrow A \xrightarrow{\deg 1} A \xrightarrow{\deg 0} 0)$

(1) We have a long exact sequence

$$\cdots \rightarrow H_{i+1}(C_*) \rightarrow H_{i+1}(C_* \otimes_A K(x)) \rightarrow H_i(C_*) \xrightarrow{(1)_x} H_i(C_*) \rightarrow H_i(C_* \otimes_A K(x)) \rightarrow$$

$$\cdots \rightarrow H_1(C_\bullet) \rightarrow H_1(C_\bullet \otimes K(x)) \rightarrow H_0(C_\bullet) \xrightarrow{x} H_0(C_\bullet) \rightarrow H_0(C_\bullet \otimes K(x)) \rightarrow 0$$

Reg 9

Lemma 23

(2) If $C.$ is acyclic, i.e. $H_i(C.) = 0 \forall i \geq 1$, then $H_i(C. \otimes_A K(x)) = 0 \forall i \geq 2$, and we have a 4-term exact sequence

$$0 \rightarrow H_1(C. \otimes_A K(x)) \rightarrow H_0(C.) \xrightarrow{x} H_0(C.) \rightarrow H_0(C. \otimes_A K(x)) \rightarrow 0$$

In particular, if x is $H_0(C.)$ -regular, then $C. \otimes_A K(x)$ is acyclic.

Pf.

$$0 \rightarrow C. \rightarrow C.(x) \rightarrow C.[1] \rightarrow 0$$

$$\text{where } (C.[1])_i = \begin{cases} C_{i-1} & \text{if } i \geq 0 \\ 0 & \text{if } i = -1 \end{cases}$$

$$\text{and } d_i^{C.[1]} = d_{i-1}^{C.} \quad \forall i \geq 1 \quad \text{q.e.d.}$$

Prop. 24 If $(x_1, \dots, x_n)$ is an M -regular sequence of an A -module M .
Then $H_i(K(x) \otimes_A M) = 0 \forall i \geq 1$ and $H_0(K(x) \otimes_A M) = M / (x_1 M + \dots + x_n M)$.
 $x_i \in A \forall i = 1, \dots, n$

Lemma 25 Let $L. \rightarrow M = (\dots \rightarrow L_i \xrightarrow{d_i} L_{i-1} \rightarrow \dots \rightarrow L_1 \xrightarrow{d_1} L_0 \xrightarrow{\varepsilon} M)$ be a minimal resolution of a finite module M over a Noetherian local ring $(A, \mathfrak{m})$.
 $K = A/\mathfrak{m}$

Let $F. = (\dots \rightarrow F_i \xrightarrow{d'_i} F_{i-1} \rightarrow \dots \rightarrow F_1 \xrightarrow{d'_1} F_0)$ be an augmented complex
 $\downarrow \varepsilon'$
 M

s.t. (a) F_i is finite free $\forall i$

(b) $\varepsilon'_0 \otimes \kappa: F_0 \otimes_A \kappa \rightarrow M \otimes_A \kappa$ is injective

(c) $d'_i(F_i) \subseteq \mathfrak{m} F_{i-1} \forall i \geq 1$, and d'_i induces an injection

$$F_i \otimes_A \kappa \rightarrow (\mathfrak{m}/\mathfrak{m}^2) \otimes_A F_{i-1} \quad \forall i \geq 1$$

Then $\exists$ a homomorphism of augmented complexes $F. \xrightarrow{\alpha_i} L.$

$$\begin{array}{ccc} \downarrow \varepsilon' & & \downarrow \varepsilon \\ M & = & M \end{array}$$

such that α_i is injective and $\alpha_i(F_i)$ is an A -direct summand of L_i $\forall i \geq 0$. In particular

$$\text{rank}_A(F_i) \leq \text{rank}_A(L_i) = \dim_K(\text{Tor}_i^A(M, K)) \quad \forall i \geq 0$$

Reg 10

Pf of Lemma 25. The existence of α follows from the exactness of $F \xrightarrow{\varepsilon} M \rightarrow 0$.

The assumptions (b), (c) + easy induction shows that

$$f_i \otimes_A \kappa: F_i \otimes_A \kappa \rightarrow L_i \otimes_A \kappa$$

is injective $\forall i \geq 0$.

q.e.d.

Prop. 26 $(A, \mathfrak{m}, \kappa)$ Noetherian local ring. $d = \dim_{\kappa}(\mathfrak{m}/\mathfrak{m}^2)$

Then $\dim_{\kappa} \operatorname{Tor}_i^A(\kappa, \kappa) \geq \binom{d}{i} \quad \forall i = 0, 1, \dots, d$

Pf: Apply Lemma 25, with $F = K(x_1, \dots, x_d)$,

where $x_1, \dots, x_d \in \mathfrak{m}$ s.t. $(x_i \bmod \mathfrak{m}^2)_{1 \leq i \leq d}$ form a κ -basis of $\mathfrak{m}/\mathfrak{m}^2$.

q.e.d.

Theorem 27 (Serre) A Noetherian local ring $(A, \mathfrak{m}, \kappa)$ is regular

iff $\operatorname{gl. dim}(A) < \infty$. (And if so, $\operatorname{gl. dim}(A) = \dim(A) = \dim_{\kappa}(\mathfrak{m}/\mathfrak{m}^2)$)

Pf: Only need to prove "if" Let $d = \dim_{\kappa}(\mathfrak{m}/\mathfrak{m}^2)$.

Prop 26 $\Rightarrow \operatorname{Tor}_d^A(\kappa, \kappa) \neq 0 \Rightarrow \operatorname{gl. dim}(A) \geq d$

Auslander-Buchsbaum $\Rightarrow \operatorname{gl. dim}(A) = \operatorname{proj. dim}_A(\kappa) = \operatorname{depth}(A)$

+ Prop. 17

$\Rightarrow \dim(A) \leq \dim_{\kappa}(\mathfrak{m}/\mathfrak{m}^2) \leq \operatorname{gl. dim}(A) = \operatorname{depth}(A) \leq \dim(A)$ QED

Cor. $(A, \mathfrak{m}, \kappa)$ Noeth. regular local $\Rightarrow A_{\mathfrak{f}}$ is a regular local ring $\forall \mathfrak{f} \in \operatorname{Spec}(A)$

§1. Associated primes and prime divisors

(1.1) **Definition (Bourbaki, *Alg. Comm.* Ch. IV, §1, Exer. 17)** Let M be a module over a commutative ring A . The set $\text{Ass}_w(M)$ of prime ideals weakly associated to M is the subset of $\text{Spec}(A)$ consisting of all prime ideals $\mathfrak{p}$ such that there exists an element $x \in M$ such that $\text{Ann}_A(x) \subseteq \mathfrak{p}$, and $\mathfrak{p}$ is a minimal element of the set of all prime ideals containing $\text{Ann}_A(x)$.

(1.2) **Definition (Nagata, *Local Rings*, Ch. 1, §7)** (a) Let M be a module over a commutative ring A . The set $\text{Ass}_N(M)$ is the subset of $\text{Spec}(A)$ consisting of all prime ideals $\mathfrak{p}$ of A such that there exists a multiplicatively closed subset S of $A \setminus \mathfrak{p}$ and $\mathfrak{p} \cdot S^{-1}A$ is a maximal element of the family consisting of all ideals of $S^{-1}A$ contained in the set $\mathcal{Z}(S^{-1}M)$ of all zero divisors of $S^{-1}M$.

(b) Let I be an ideal of A . Nagata called $\text{Ass}_N(A/I)$ the set of *prime divisors* of I .

(1.3) **Lemma** Let M be a module over a commutative ring A .

- (i) $\text{Ass}_w(M) = \emptyset$ if and only if $M = 0$.
- (ii) $\bigcup_{\mathfrak{p} \in \text{Ass}_w(M)} \mathfrak{p} = \mathcal{Z}(M)$, the set of all zero divisors of M .
- (iii) If $0 \rightarrow M' \rightarrow M \rightarrow M'' \rightarrow 0$ is a short exact sequence of A -modules, then

$$\text{Ass}_w(M') \subseteq \text{Ass}_w(M) \subseteq \text{Ass}_w(M') \cup \text{Ass}_w(M'').$$

(1.4) **Lemma** Let M be a module over a commutative ring A .

- (i) $\text{Ass}(M) \subseteq \text{Ass}_w(M) \subseteq \text{Ass}_N(M)$.
- (ii) $\bigcup_{\mathfrak{p} \in \text{Ass}_w(M)} \mathfrak{p} = \bigcup_{\mathfrak{p} \in \text{Ass}_N(M)} \mathfrak{p} = \mathcal{Z}(M)$.
- (iii) If A is Noetherian, then $\text{Ass}_w(M) = \text{Ass}(M) = \text{Ass}_N(M)$.

(1.5) **Example** We produce a commutative ring A with $\text{Ass}_w(A) \subsetneq \text{Ass}_N(A)$.

Let k be a field, and let $(x_i)_{i \geq 1}$ be a countable set of variables. Let

$$u_1 = x_1, \quad u_2 = x_1^{1/2} x_2, \quad u_3 = x_1^{1/4} x_2^{1/4} x_3, \dots, \quad u_i = (x_1 x_2 \cdots x_{i-1})^{2^{-i+1}} x_i, \dots$$

and let

$$A = \bigcup_{n \in \mathbb{N}} k[x_1^{2^{-n}}, \dots, x_n^{2^{-n}}] / (u_1, \dots, u_n).$$

Let $\mathfrak{m}$ be the maximal ideal of A generated by all elements of the form $x_i^{2^{-j}}$, $i, j \geq 1$. Then $\mathfrak{m} \subset \mathcal{Z}(A)$, i.e. every element of $\mathfrak{m}$ is a zero divisor. So $\mathfrak{m}$ is a prime divisor of 0 in the sense of Nagata, i.e. $\mathfrak{m} \in \text{Ass}_N(A)$.

Claim. For every non-zero element $y \in A$, there exists an $n_0 \in \mathbb{N}$ such that

$$\text{Ann}(y) \subseteq \bigcup_{n \geq 1} \left(\sum_{1 \leq i \leq n_0} x_i^{2^{-n}} A \right) =: \mathfrak{q}_{n_0}$$

The proof of this claim is omitted here. This claim implies that $\mathfrak{m} \notin \text{Ann}_w(A)$.