∫(͡° ͜ʖ ͡°)dx

MA 526

Commutative Algebra

Notes By: Aryaman Maithani

Spring 2020-21

Lecture 1 (07-01-2021)

07 January 2021 08:07

Noetherian Rings and Modules

Defn. (Poset) A set S with a relation $\leq$ which is
(i) Reflexive
(ii) Anti-symmetric
(iii) Transitive

A total order is a poset in which any two elements are comparable.
A subset of a poset is called a chain if it is totally ordered.

Propn. Let S be a poset.
TFAE
(1) $x_1 \leq x_2 \leq x_3 \leq \cdots \Rightarrow \exists N \in \mathbb{N}$ s.t. $x_n = x_{n+1}$ $\forall n \geq N$
(2) $T \subset S$, $T \neq \phi \Rightarrow T$ has a maximal element.

Proof. (1) $\Rightarrow$ (2)
Let $\phi \subsetneq T \subsetneq S$. Suppose, for the sake of contradiction, that T has no maximal element.

Pick any $x_1 \in T$. x_1 not maximal. $\therefore \exists x_2 \in T$ s.t. $x_2 > x_1$.
x_2 not maximal. $\exists x_3 \in T$ with $x_3 > x_2$. ...
We get a chain $x_1 < x_2 < \cdots$ which does not stabilise.

(2) $\Rightarrow$ (1) Let $x_1 \leq x_2 \leq x_3 \leq \cdots$ be a chain.
Consider $T = \{x_i : i \in \mathbb{N}\}$. This has a maximal element.
Let $N \in \mathbb{N}$ be s.t. x_N is maximal.
By assumption, $x_N \leq x_{N+1}$ but also maximal.
$\therefore x_N = x_{N+1}$.
In fact, for any $M > N$, the above argument holds. ∎

(1) is called the ascending chain condition. (a.c.c.)
(2) — " — maximal condition.

Def^n. Let R be a commutative ring with 1.
Let M be an R-module.
Let P be the poset of submodules of M (w.r.t. inclusion).
M is said to be Noetherian if P satisfies a.c.c.

(Equivalently, P satisfies maximal condition.)

If R is a Noetherian R-module, R is called a Noetherian ring.

There are the dual properties: descending chain condition (d.c.c.)
minimal condition.

Def^n. If submodules of an R-module M satisfy d.c.c., M is called an Artinian module.
Similarly, if R is Artinian as an R-module, it is called an Artinian ring.

Note that R-submodules of R are precisely ideals.
Thus, the Art./Noe. conditions are a.c.c./d.c.c. on ideals.

We shall soon see that Noe. rings are Art. but converse not true.

Examples.

(1) R PID. $R = \mathbb{Z}$ or $\mathbb{K}[x]$, for example.
Let us consider $\mathbb{Z}$.

$$0 \subsetneq (n_1) \subsetneq (n_2) \subsetneq \cdots$$

$n_2 \mid n_1$ with $n_2 \neq \pm n_1$, ...

At each stage, at least one prime is exhausted

Similar argument works in $\mathbb{k}[x]$ or any PID.

$\mathbb{Z}$ is NOT Noetherian. $(2) \supsetneq (2^2) \supsetneq (2^3) \supsetneq \cdots$

Can do the same in any PID which is not a field.

(2) $\mathbb{k}$ a field. $\mathbb{k}$ is both. } have only finitely many ideals. Satisfy acc & dcc trivially.

(3) $\mathbb{Z}/n\mathbb{Z} \leftarrow$ both
$n > 1$

(4) Any finite abelian group G is a $\mathbb{Z}$-module.
Only finitely many subgroups ($\mathbb{Z}$-submodules) and hence, both.

(5) $\mathbb{Q}/\mathbb{Z}$. $\quad 0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$.

$$\mathbb{Q}/\mathbb{Z} = \left\{ \frac{r}{s} + \mathbb{Z} \;\middle|\; r, s \in \mathbb{Z} \text{ with } s \neq 0 \right\}$$

is an infinite abelian group.

Fix a prime $p > 0$. Define $G_n \subset \mathbb{Q}/\mathbb{Z}$ as

$$G_n := \left\{ \frac{a}{p^n} + \mathbb{Z} \;\middle|\; a \in \mathbb{Z} \right\}.$$

$$G_0 = 0 \subsetneq G_1 \subsetneq G_2 \subsetneq \cdots$$

$$\left(\frac{1}{p^n} + \mathbb{Z} \in G_n \setminus G_{n-1} \right)$$

Thus, $\mathbb{Q}/\mathbb{Z}$ is not Noetherian. (as a $\mathbb{Z}$-module)

Moreover, $G = \bigcup_{n=1}^{\infty} G_n \leq \mathbb{Q}/\mathbb{Z}$. This subgroup is also not a Noetherian $\mathbb{Z}$-module.

However, G does satisfy d.c.c.
(Ex. Every subgroup of G is of the form G_n.)

Thus, G is Artinian but not Noetherian!

(6) Hilbert Basis Theorem. $\mathbb{k}[x_1, \ldots, x_n]$ is Noe. ($n=1$ done above)

However, $\mathbb{k}[x_1, \ldots]$ is not Noetherian.
$(x_1) \subsetneq (x_1, x_2) \subsetneq \cdots$

Not Artinian either. $R \supsetneq (x_1, x_2, \ldots) \supsetneq (x_2, \ldots) \supsetneq (x_3, \ldots) \supsetneq \cdots$
$(x_1) \supsetneq (x_1^2) \supsetneq (x_1^3) \supsetneq \cdots$

(7) $0 \to \mathbb{Z} \to H \stackrel{\mathbb{Q}}{\leq} \to G \to 0$

$H = \left\{ \frac{m}{p^n} : m \in \mathbb{Z}, n \in \mathbb{N} \cup \{0\} \right\}$ (p fixed prime)

Then H is not Art because $\mathbb{Z}$ is not.
H is not Noe. because G is not.

Lecture 2 (12-01-2021)

12 January 2021 14:02

Thm. Suppose R is a ring and M an R-module. Then M is Noetherian iff every submodule of M is f.g.

Proof ($\Rightarrow$) Suppose M is Noetherian and $N \leq M$ a submodule.
To show: N is not f.g.
Suppose not.
Then, $N \neq \{0\}$. ($\because \langle \phi \rangle = \{0\}$)
$\Rightarrow \exists\, x_1 \in N$ s.t. $x_1 \neq 0$.
$N_1 = Rx_1 \subsetneq N$. Thus, $\exists\, x_2 \in N \setminus N_1$.
$N_1 \subsetneq N_2 = Rx_1 + Rx_2 \subsetneq N$.

Similarly, we can construct $x_3, \ldots$

Thus, $0 \subsetneq N_1 \subsetneq N_2 \subsetneq N_3 \subsetneq \cdots \subseteq N \subseteq M$.
$\rightarrow\leftarrow$

Thus, N is f.g.. As N was arbitrary every submodule of M is f.g.

($\Leftarrow$) Suppose every submodule of M is f.g.
We show that a.c.c. holds

Let $M_1 \subseteq M_2 \subseteq M_3 \subseteq \cdots \subseteq M$ be a seq. of submodules.

Put $N := \bigcup_{i=1}^{\infty} M_i$. $\leftarrow$ This is a submodule of M since $\{M_i\}_{i=1}^{\infty}$ is a chain.

Thus, N is f.g. Then, $R = \langle x_1, \ldots, x_g \rangle$ for some $x_1, \ldots, x_g \in N$.

$\therefore N = \bigcup_{i=1}^{\infty} M_i$, for some x_j, $\exists\, M_j$ s.t. $x_j \in M_j$.

$\therefore \quad N = \bigcup_{i=1}^{\infty} M_i$, for some x_j, $\exists M_j$ s.t. $x_j \in M_j$.

However, note that $\{M_i\}$ is a chain and $\exists t \in \mathbb{N}$ s.t.

$$x_1, \ldots, x_g \in M_t.$$

Thus, $x_1, \ldots, x_g \in M_T \quad \forall T \geq t$.

$$\Rightarrow \quad M_t = M = M_T \quad \forall T \geq t.$$

Thus, M is Noetherian.

<u>Cor.</u> A ring is Noetherian iff every ideal of R is f.g.

<u>Prop^n.</u> Suppose $0 \to N \xrightarrow{f} M \xrightarrow{g} P \to 0$ is an exact sequence. (That is, $\ker f = 0$, $\operatorname{im} f = \ker g$, $\operatorname{im} f = P$.)

(i) M is Noetherian $\Leftrightarrow$ N and P are Noetherian
(ii) M is Artinian $\Leftrightarrow$ N and P are Artinian

<u>Proof.</u> We prove (i). (ii) is similar.

($\Rightarrow$) $N \simeq f(N)$ as f is injective.
Enough to prove $f(N)$ is Noetherian. But $f(N) \leq M$.
Thus, any chain in $f(N)$ is also in M. Thus, $f(N)$ is Noetherian because M is so.

$P \simeq M/\ker g$. Note any submodule of $M/\ker g$ is of the form $L/\ker g$ for some $L \leq M$ with $\ker g \leq L$.
↑ sufficient to show this is Noetherian
Conclude.

($\Leftarrow$) Let N and P be Noetherian modules.

Let $M_0 \leq M_1 \leq \cdots \leq M$ be an icreasing sequence.

$\Rightarrow$ $f^{-1}(M_0) \leq f^{-1}(M_1) \leq \cdots \leq N$.

N is Noe., thus $\exists n \in \mathbb{N}$ s.t. $f^{-1}(M_{n+i}) = f^{-1}(M_n)$ $\forall i \geq 0$.

Similarly,

$$g(M_0) \leq g(M_1) \leq \cdots \leq P$$

$\Rightarrow$ $\exists m \in \mathbb{N}$ with $m \geq n$ s.t. $g(M_m) = g(M_{m+i})$ $\forall i \geq 0$

Then,
$$\left.\begin{aligned} f^{-1}(M_m) &= f^{-1}(M_{m+i}) \\ g(M_m) &= g(M_{m+i}) \end{aligned}\right\} \forall i \geq 0$$

Claim. $M_m = M_{m+i}$ $\forall i \geq 0$.

($\subseteq$) is given

($\supseteq$) Let $x \in M_{m+i}$. $g(x) \in g(M_{m+i}) = g(M_m)$

$\Rightarrow$ $g(x) = g(y)$ for some $y \in M_m$

$\Rightarrow$ $x - y \in \ker g = \operatorname{im} f \cap M_{n+i}$

$\Rightarrow$ $x - y = f(z)$ for some $z \in N$

$\Rightarrow$ $z \in f^{-1}(M_{n+i}) = f^{-1}(M_n)$

$\Rightarrow$ $\underset{x-y}{\overset{\shortparallel}{f(z)}} \in M_n$

$\Rightarrow$ $x - y \in M_n$ but $y \in M_n$

$\therefore$ $x \in M_n$, as desired.

Cor. Let $M_1, \ldots, M_n$ be R-modules.
Then
$$\bigoplus_{i=1}^n M_i \text{ is Noe} \iff M_i \text{ is Noe } \forall i.$$

Similar statetement holds for Artinian.

Proof. $(\Rightarrow)$ $\pi_i : \bigoplus_{j=1}^n M_j \twoheadrightarrow M_i$ is onto.

$$0 \to \ker \pi_i \xrightarrow{\text{incl}} \bigoplus_{j=1}^n M_j \xrightarrow{\pi} M_i \to 0$$

shows M_i is Noe. (or Art).

$(\Leftarrow)$ Induction on n. $n=1$ true. Assume for n. Then,

$$0 \to \underset{\substack{\uparrow \\ \text{Noetherian} \\ \text{(assumption)}}}{M_{n+1}} \xrightarrow{\text{ind}} \bigoplus_{i=1}^{n+1} M_i \twoheadrightarrow \underset{\substack{\uparrow \\ \text{Noetherian} \\ \text{(induction)}}}{\bigoplus_{i=1}^{n} M_i} \to 0$$

$\therefore \bigoplus_{i=1}^{n+1} M_i$ is Noe. $\boxtimes$

Cor. Let R be a Noetherian (resp Artinian) ring and M a f.g. R-module. Then, M is Noetherian (resp. Artinian).

Proof. Since M is f.g., we can write M as a quotient of $R^{\oplus n}$. (*)
But $R^{\oplus n}$ is Noe. (resp Art.) since R is.
Thus, so is M.

(*) Let $M = Rm_1 + \cdots + Rm_n$ for $m_1, \ldots, m_n \in M$

$$0 \to \ker f \to \bigoplus_{i=1}^n Re_i \xrightarrow{f} M \to 0$$ is an exact sequence.

$$e_i \mapsto m_i$$

[Note that for Noe., it is necessary that M be f.g. Thus, it is necessary & suff. if R is Noetherian.
However, for Art., M need not be f.g.]

Remark Subrings of Noetherian rings need not be Noetherian.

$R = \mathbb{k}[x, y]$ $\qquad$ $\mathbb{k}$ field ; $\quad x, y$ indeterminate

R is Noetherian. (Hilbert's basis theorem)

$S = \mathbb{k}[x, xy, xy^2, \dots]$ is a subring of R.

Note that

$$\langle x \rangle \subsetneq \langle x, xy \rangle \subsetneq \langle x, xy, xy^2 \rangle \subsetneq \cdots$$

are strictly increasing ideals in $\underline{\underline{S}}$.

Note that in R, $\langle x \rangle = \langle x, xy \rangle$ since $y \in R$.

Thus, S is not Noetherian even though R is.

EXAMPLE. Let $X = [0, 1]$. $\quad \mathcal{C}(X) = \{ f : X \to \mathbb{R} \mid f \text{ is continuous} \}$ is a comm. ring with 1. (Pointwise operations.)

$\mathcal{C}(X)$ is not Noetherian.

Define $F_n := \left[0, \frac{1}{n}\right]$ for $n \in \mathbb{N}$.

$$F_1 \supset F_2 \supset F_3 \supset \cdots$$

Define

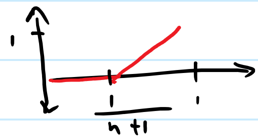
$$I_n = \{ f \in \mathcal{C}(X) : f(F_n) = 0 \}.$$

Note I_n is an ideal. Moreover

$$I_1 \subsetneq I_2 \subsetneq I_3 \subsetneq \cdots$$

($\subset$) is clear because $f_{n+1} \subset f_n$

($\neq$) because



Thus, R is not Noetherian.

R : Noetherian ring, I is an ideal

$\Rightarrow R/I$ is Noetherian (as a ring)

(What NOT to do: $0 \to I \to R \to R/I \to 0$

This only shows R/I is a Noe. R-module, not as ring.)

(However, this can be improved.)

See note.

Proof

$\Rightarrow$ let $K \trianglelefteq R/I$ be an ideal. Then, $K = J/I$ for some $I \subseteq J \trianglelefteq R$.

R is Noe $\Rightarrow J$ is f.g. $\Rightarrow I$ is f.g. $\boxtimes$

NOTE. Let M be an R-module.

$\operatorname{ann} M := \{ r \in R : rm = 0 \ \forall m \in M \}$.

(E.g. R/I is an R-module and $\operatorname{ann}(R/I) = I$.)

M is also an $R/\operatorname{ann} M$ - module with operation

$$(r + \operatorname{ann} M)\, m = rm. \qquad \text{(well-defined)}$$

Then, the module structure is the "same". This shows that the previous argument actually works.

Thm. (Hilbert Basis Theorem) (Hilbert's Basis Theorem)
Let R be a Noetherian ring and X an indeterminate.
Then $R[X]$ is Noetherian.

Remark. Note the converse is trivial since $R \cong \frac{R[X]}{\langle X \rangle}$.

$(x = X.)$

Proof. Suppose $R[x]$ is not Noetherian.
Then, $\exists\, I \trianglelefteq R[x]$ s.t. I is not f.g.
In particular, $I \neq 0$. $\exists f_1 \in I \setminus \{0\}$

Pick f_1 of least degree. (May be many such f_1. Does not matter.)

$f_1 = a_1 x^{d_1} + (\text{smaller terms})$

$(d_1 = \deg f_1)$

$I \neq (f_1)$. Choose $f_2 \in I \setminus (f_1)$ of least degree. (d_2)

$f_2 = a_2 x^{d_2} + (\text{smaller terms})$

$I \neq (f_1, f_2)$. Continue picking $f_3, f_4, \ldots$ similarly

Note $a_1 \neq 0$, $a_2 \neq 0$, ...

Consider the following ideals of R:

$$(a_1) \subseteq (a_1, a_2) \subseteq (a_1, a_2, a_3) \subseteq \cdots$$

R is Noetherian. Thus, the above chain stabilises

$$\Rightarrow (a_1, \ldots, a_k) = (a_1, \ldots, a_k, \ldots, a_{k+i}) \quad \forall i \geq 0$$

$$a_{k+1} = b_1 a_1 + \cdots + b_k a_k \quad \text{for some } b_1, \ldots, b_k \in R.$$

$$f_1 = a_1 x^{d_1} + (\cdots)$$
$$\vdots$$
$$f_k = a_k x^{d_k} + (\cdots)$$
$$f_{k+1} = a_k x^{d_{k+1}} + (\cdots)$$

Note $d_1 \leq d_2 \leq \cdots$

Thus, $d_{k+1} \geq d_k \geq \cdots$

Now, look at
$$g = b_1 f_1 x^{d_{k+1} - d_1} + \cdots + b_k a_k f x^{d_{k+1} - d_k} - f_{k+1}$$

Note : $\deg g < \underset{\deg f_{k+1}}{\overset{\shortparallel}{d_{k+1}}}$ but $g \notin (f_1, \ldots, f_k)$.

else $f_{k+1} \in (f_1, \ldots, f_k)$ $\rightarrow\leftarrow$

Thus, $R[x]$ is Noetherian.

Cor. R Noetherian $\Rightarrow$ $R[x_1, \ldots, x_n]$ is Noetherian.
Moreover, quotients are also Noetherian.

Cor. R Noetherian $\Rightarrow$ any f.g. R-alg is Noetherian.

$$S = R[s_1, \ldots, s_n] \simeq \frac{R[x_1, \ldots, x_n]}{I}.$$

Remark. Analogous result NOT true for Artinian. $\mathbb{k}$ & $\mathbb{k}[x]$.

Lecture 3 (15-01-2021)

15 January 2021 14:03

Lemma. Let $I \trianglelefteq R$ be an ideal and $b \in R$ be s.t.

$$I : b = \{ r \in R \mid rb \in I \}$$ and

$\langle I, b \rangle$ are finitely generated. Then, I is also f.g.

Proof.

$$\begin{tikzcd} I:b \arrow[dr, dash] & & \langle I, b\rangle \arrow[dl, dash] \\ & I & \end{tikzcd}$$

$$\langle I, b \rangle = \{ x + yb \mid x \in I, y \in R \}$$

Generators of $\langle I, b \rangle$ can be of the form $a_1, \dots, a_r \in I$, b.

$$\langle I, b \rangle = \langle a_1, \dots, a_r, b \rangle.$$

$$(I:b) = (c_1, \dots, c_s) \Rightarrow c_i b \in I \quad \forall i$$

Put $J = \langle a_1, \dots, a_r, c_1 b, \dots, c_s b \rangle \subseteq I$.

We show $I \subseteq J$ and conclude. ($\because J$ is f.g.)

Let $a \in I \subseteq \langle I, b \rangle = \langle J, b \rangle$. Then, $a = c + rb$, $c \in J, r \in R$

$$\Rightarrow rb = a - c \in I$$

$$\Rightarrow r \in I : b$$

Thus, $r = d_1 c_1 + \cdots + d_s c_s$ $\quad (I : b = \langle c_1, \dots, c_s \rangle)$

$$\Rightarrow a = c + rb = \underbrace{c}_{\in J} + d_1 \underbrace{bc_1}_{\in J} + \cdots + d_s \underbrace{bc_s}_{\in J}$$

$\therefore a \in J$. $\blacksquare$

Thm. (Cohen's Theorem)

If prime ideals of a commutative ring are f.g., then the ring is Noetherian.

Proof. We show that all ideals are f.g.
Suppose not. Define

$$\Sigma = \{ I \mid I \trianglelefteq R \text{ s.t. } I \text{ is not f.g.} \}$$

$\Sigma \neq \emptyset$ by hypothesis. Σ is a poset, under $\subseteq$.

Suppose $\{I_\alpha\}_{\alpha \in \Lambda}$ is a chain of ideals in Σ.
We show that

$$I = \bigcup_{\alpha \in \Lambda} I_\alpha \quad \text{is not f.g.}$$

(That it is an ideal is clear.)

This is simple for if $I = \langle x_1, \ldots, x_r \rangle$, then one can find a suitable $\alpha \in \Lambda$ s.t. $I_\alpha \ni x_1, \ldots, x_r$. ($\because \{I_\alpha\}$ is a chain)
In that case

$$I = \langle x_1, \ldots, x_r \rangle \subseteq I_\alpha \subseteq I.$$

Thus, $I_\alpha = \langle x_1, \ldots, x_r \rangle$ is f.g. $\rightarrow\leftarrow$

Thus, Σ has a maximal element, by Zorn's Lemma.
Let J be a maximal element of Σ.
Since $J \in \Sigma$, J is not f.g and hence, not prime.

$\therefore \exists a, b \in R$ s.t. $a \notin J$, $b \notin J$ but $ab \in J$.

$$ab \in J \Rightarrow a \in J : b \supsetneq J \quad \text{since } a \notin J$$

Also, $\langle J, b \rangle \supsetneq J$ since $b \notin J$.

Since J is maximal, $(J : b)$, $\langle J, b \rangle \notin \Sigma$.
Thus, both are f.g. By the earlier lemma,

so is J.

Thus, we have a contradiction.

Thus, all ideals are f.g. and hence, R is Noetherian. $\blacksquare$

Cor. R is Noetherian $\Rightarrow R[\![x_1, \dots, x_n]\!]$ is Noetherian.

Proof. Enough to prove for $n=1$.
Using Cohen's, it is sufficient to show that prime ideals in $R[\![x]\!]$ are f.g.

Consider the evaluation map
$$\phi : R[\![x]\!] \longrightarrow R$$
$$f(x) \mapsto f(0)$$

Let $\mathfrak{p} \in \operatorname{Spec}(R[\![x]\!])$. Then, $\phi(\mathfrak{p})$ is an ideal of R (ϕ is onto) and hence, $\phi(\mathfrak{p})$ is f.g. (since R is Noetherian)

$\phi(\mathfrak{p}) = \langle a_1, \dots, a_r \rangle$ ← ideal of all constant terms in $\mathfrak{p}$.

Case 1. $x \in \mathfrak{p}$.
Let $f(x) \in \mathfrak{p}$ be arbitrary

Write $f(x) = b_0 + b_1 x + \cdots = b_0 + x(b_1 + b_2 x + \cdots)$ ← $\langle b_0, x \rangle$
Then, $b_0 \in \phi(\mathfrak{p})$.
$$b_0 = c_1 a_1 + \cdots + c_r a_r$$

$$f(x) \in \langle a_0, \dots, a_r, x \rangle \subset \mathfrak{p}$$

$$\therefore \mathfrak{p} = \langle a_0, \dots, a_r, x \rangle \text{ is f.g.}$$

Case 2. $x \notin \mathfrak{p}$

$\phi(\mathfrak{p}) = \langle a_1, \ldots, a_r \rangle$

For each $i = 1, \ldots, r$, we have $f_i(x) \in \mathfrak{p}$

s.t.

$$f_i(x) = a_i + x g_i(x) \quad ; \quad g_i(x) \in R[[x]].$$

Claim. $\mathfrak{p} = \langle f_1, \ldots, f_r \rangle$. (2) is obvious.

Proof. Let $g(x) \in \mathfrak{p}$.

Write $g(x) = b + x h(x)$, $h(x) \in R[[x]]$.

$$b = \sum_{i=1}^{r} b_i a_i$$

$$g - \sum b_i f_i = [b + x h(x)] - \sum b_i (a_i + x g_i(x))$$

$$\underbrace{\underset{\mathfrak{p} \ni}{g} - \sum \underset{\in \mathfrak{p}}{b_i f_i}}_{\in \mathfrak{p}} = \underset{\notin \mathfrak{p}}{x} \underbrace{\left[h(x) - \sum_{i=1}^{r} b_i g_i(x) \right]}_{\therefore \in \mathfrak{p}}$$

call this $h_1(x)$

$$g(x) = \sum b_i f_i + x h_1(x)$$

Can repeat the process on $h_1(x) \in \mathfrak{p}$ to give

$$h_1(x) = \sum c_i f_i + x h_2(x) \quad \text{for } h_2(x) \in R[[x]].$$

$$g(x) = \sum b_i f_i + x \sum c_i f_i + x^2 h_2(x)$$

Can continue so on to get $g(x) \in \langle f_1, \ldots, f_r \rangle$.

$$g(x) = f_1 (b_1 + x c_1 + x^2 d_1 + \cdots)$$

$+ \cdot$

$\vdots$

$$+ f_r \left(b_r + x\, c_r + x^2 d_r + \cdots \right)$$

Lecture 4 (19-01-2021)

19 January 2021 13:52

Chapter 2: Associated primes of ideals and modules

$R \to$ commutative ring with 1. $I, J \trianglelefteq R$ are ideals.

Recall the colon of two ideals I, J is the ideal

(colon)

$$I :_R J := \{ r \in R \mid rJ \subset I \}.$$

(Analog of division.)

Suppose M, N are R-submodules of some R-module M'.
We define

$$M :_R N := \{ r \in R \mid rN \subseteq M \}.$$

$M :_R N$ is an ideal of R.

$$\text{ann } M = 0 :_R M = \{ r \in R \mid rM = 0 \}.$$

(ann M or annihilator of M)

Example $R = \mathbb{Z}$, $M = \mathbb{Z}/n\mathbb{Z}$ is a R-module

Suppose $n = p^a q^b$ p, q primes

$$(n : p^a q^{b-1}) = (q) \qquad (n : p^{a-1} q^b) = (p)$$

Note $I : J \supseteq I$ in general. Thus, can go modulo n.

$$\frac{(n : p^a q^{b-1})}{(n)} = \frac{(q)}{(n)} \qquad \frac{(n : p^{a-1} q^b)}{(n)} = \frac{(p)}{(n)}$$

prime ideal in $\mathbb{Z}/n\mathbb{Z}$

ideal in $\mathbb{Z}$

$$(q) = 0 :_{\mathbb{Z}} x \qquad (p) = 0 :_{\mathbb{Z}} y$$

element of $\mathbb{Z}/n\mathbb{Z}$

$$(q) = 0 :_{\mathbb{Z}} x \quad \text{element of } \mathbb{Z}/n\mathbb{Z} \qquad\qquad (p) = 0 :_{\mathbb{Z}} y$$

$$x = p^a b^{q-1} + (n) \qquad\qquad y = p^{a-1} q^b + (n)$$

Defn Let M be an R-module and $0 \neq x \in M$.
If $0 :_R x = \mathfrak{p}$ is a prime ideal in R, then we say that $\mathfrak{p}$ is an associated prime of M.

(Associated primes)

$$\mathrm{Ass}_R(M) := \{ \mathfrak{p} \in \mathrm{Spec}(R) \mid \mathfrak{p} = 0 : x \text{ for some } x \in M \setminus \{0\} \}$$

$$\mathrm{Ass}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}) = \{ (p), (q) \}.$$

($\supseteq$) by earlier

($\subseteq$) $\mathrm{Spec}(\mathbb{Z}/n\mathbb{Z}) = \{(p), (q)\}$.

$$\mu_x : R \xrightarrow{x} M, \quad r \longmapsto rx \qquad \mu_x = \text{the homothety by } x$$

μ_x is an R-linear map.

$$\ker \mu_x = \{ r \in R : rx = 0 \} = \mathrm{ann}_R(x) = (0 : x)$$

If $(0 : x) = \mathfrak{p}$ is prime, then

$$\frac{R}{\ker \mu_x} = \frac{R}{\mathfrak{p}} \hookrightarrow M, \qquad \frac{R}{\mathfrak{p}} \simeq Rx$$

(That is, $R/\mathfrak{p}$ injects into M.)

Conversely, if $R/\mathfrak{p} \overset{\varphi}{\hookrightarrow} M$ (R-linear), then $\mathfrak{p} = 0 : x$ for some $0 \neq x \in M$.

If $\varphi(1 + \mathfrak{p}) = x$, then
$\varphi(r + \mathfrak{p}) = rx$. $\quad \therefore\ \tilde{\varphi} : R \to M$ is μ_x
and $\mathfrak{p} = \ker \mu_x$.

Thus, alternate defn :

$$\mathrm{Ass}\ M = \{ \mathfrak{p} \in \mathrm{Spec}\ R \mid R/\mathfrak{p} \hookrightarrow M \}.$$

(Associated primes are those $\mathfrak{p}$ s.t. $R/\mathfrak{p}$ injects into M as a submodule.)

Def^n. $a \in R$ is a zero divisor on M if $ax = 0$ for some $0 \neq x \in M$.

(Zero divisors)

$Z(M)$ = set of zero divisors. ($Z(M) \subseteq R$) not necessarily an ideal

Note that a is a zero divisor $\Leftrightarrow$ μ_a is not injective.

If μ_a is injective, then μ_a is called a non zero divisor on M, or M-regular.

(Non zero divisors or M-regular)

Note $\mathfrak{p} \in \mathrm{Ass}\ M \Rightarrow \mathfrak{p} = 0 : x$ for some $x \in M \setminus \{0\}$

$\Rightarrow \mathfrak{p} \subseteq Z(M)$

Prop^n. (Existence of associated primes)

Let R be a Noetherian ring and $M \neq 0$ a f.g. R-module.

Then,

(a) Maximal elements among $\{(0:x) \mid x \in M\}$ are prime ideals.

Hence, $\mathrm{Ass}\ M \neq \phi$.

(b) $Z(M) = \bigcup_{\mathfrak{p} \in \mathrm{Ass}\ M} \mathfrak{p}$.

Proof. (a) $\mathcal{F} := \{ (0:x) \mid x \in M \setminus \{0\} \}$.

Note that $\mathcal{F}$ is non empty ($M \neq 0$) and contains only proper ideals. ($1 \notin (0:x)$ if $x \neq 0$)

As R is Noetherian, $\mathcal{F}$ has a maximal element (w.r.t. $\subseteq$).

<u>Claim</u>. Any maximal member of $\mathcal{F}$ is prime. Hence, Ass $M \neq \phi$.

<u>Proof</u>. Let $0:x$ be a maximal member.

Let $a, b \in R$ be s.t. $ab \in 0:x$, $a \notin 0:x$.

To show: $b \in 0:x$. That is, $bx = 0$.

$abx = 0$ $\quad (\because ab \in 0:x)$

$\Rightarrow b \in \underbrace{0:ax}_{\in \mathcal{F} \text{ since } ax \neq 0 \text{ since } a \notin 0:x} \supseteq 0:x$

By maximality, $0:x = 0:ax \ni b$.

$\therefore b \in 0:x$. Thus, $(0:x)$ is prime. ✓

(Didn't use M f.g. here. We usually keep the blanket assumption anyway.)

(b) We saw $\mathcal{Z}(M) \supseteq \bigcup_{p \in \operatorname{Ass} M} p$ already.

$(\subseteq)$ Let $b \in \mathcal{Z}(M)^{\subseteq R}$. Thus, $bx = 0$ for some $x \in M \setminus \{0\}$.

That is, $b \in 0:x$.

Since $\mathcal{F}$ has maximal members, $0:x \subseteq 0:y$ for some maximal member $0:y$. (use a.c.c.) But that is prime.

Thus, $b \in 0:y \subset \bigcup_{p \in \operatorname{Ass} M} p$. ∎

Ex. $\mathbb{Z}/n\mathbb{Z}$, $n = p^a q^b$, then $\mathcal{Z}(\mathbb{Z}/n\mathbb{Z}) = (p) \cup (q)$.

Ex. Let $\Bbbk$ be a field. $R = \Bbbk[x, y]$. (UFD)

Consider $I = (x^2, xy) = (x) \cap (x^2, y)$ (Ex 1)

$I : x \ni x, y$. But $\dfrac{R}{(x, y)} \simeq \Bbbk \to$ field.

$(x, y) \subseteq I : x$

Thus, (x, y) is maximal.

However, $x \notin I$. Thus, $I : x \neq R$. $\therefore (x, y) \subseteq I \subsetneq R$

Thus, $I : x = (x, y) = \mathfrak{m}$.

$M = R/I$, $0 : \bar{x} = \mathfrak{m}$. $\Rightarrow \mathfrak{m} \in \mathrm{Ass}(R/I)$.

($\supseteq$) is clear

$=$ by maximality ($\bar{x} \neq 0$)

$I : y \underset{\text{prove!}}{=} (x) = \mathfrak{p}$ prime

(Ex 2.)

$\therefore \mathfrak{p} \in \mathrm{Ass}\,(R/I)$. $\mathfrak{p} \subset \mathfrak{m}$.

We will see later: $\mathrm{Ass}\,(R/I) = \{\mathfrak{p}, \mathfrak{m}\}$.

both primes but $\mathfrak{p}$ is not maximal!

Behaviour of associated primes under localisation

Let R be a Noetherian ring and $M \neq 0$ an R-module.
Let $S \subseteq R$ be an m.c.s. of R.

$$R \longrightarrow S^{-1}R \qquad\qquad M \longrightarrow S^{-1}M \cong S^{-1}R \otimes_R M$$

$$r \longmapsto \frac{r}{1} \qquad\qquad x \longmapsto \frac{x}{1}$$

$$S^{-1}M = \left\{ \frac{m}{s} \;\middle|\; \begin{array}{l} m \in M \\ s \in S \end{array} \right\}$$

$$\frac{m}{s} = \frac{m'}{s'} \Leftrightarrow \exists\, t \in S \text{ s.t. } t(ms' - sm') = 0.$$

(We will assume $1 \in S$.)

What is the connection $\mathrm{Ass}_R M \longleftrightarrow \mathrm{Ass}_{S^{-1}R} S^{-1}M$?

Recall: $\mathrm{Spec}\,(S^{-1}R) = \{ S^{-1}\mathfrak{p} : \mathfrak{p} \cap S = \emptyset \}$

What we will show is:

$$\mathrm{Ass}\ M \longleftrightarrow \mathrm{Ass}_{S^{-1}R}\ S^{-1}M$$
$$\{\mathfrak{p}_1, \dots, \mathfrak{p}_r\} \longleftrightarrow \{S^{-1}\mathfrak{p}_i \mid \mathfrak{p}_i \cap S = \phi\}$$

Prop^n. ① $\mathrm{Ass}_{S^{-1}R}(S^{-1}M) = \{S^{-1}\mathfrak{p} \mid \mathfrak{p} \in \mathrm{Ass}\ M,\ \mathfrak{p} \cap S = \phi\}$

② $\mathfrak{p} \in \mathrm{Ass}_R\ M \iff \mathfrak{p}R_\mathfrak{p} \in \mathrm{Ass}_{R_\mathfrak{p}}\ M_\mathfrak{p}$ → Reduces the problem to solving over local rings.

Proof. ①(⊇) Let $\mathfrak{p} \in \mathrm{Ass}\ M$, $\mathfrak{p} \cap S = \phi$.

Thus, $R/\mathfrak{p} \hookrightarrow M$.

(Recall that localisation preserves exactness)

$$0 \to R/\mathfrak{p} \to M \to \mathrm{coker} \to 0$$

localise

(S^{-1} commutes with this quotienting)

$$0 \to S^{-1}R/S^{-1}\mathfrak{p} \to S^{-1}M \to S^{-1}\mathrm{coker} \to 0$$

$$\Rightarrow S^{-1}\mathfrak{p} \in \mathrm{Ass}_{S^{-1}R}\ S^{-1}M$$

Why does localisation commute with quotienting? Because exactness.

$0 \to \mathfrak{p} \to R \to R/\mathfrak{p} \to 0$

⇝

$0 \to S^{-1}\mathfrak{p} \to S^{-1}R \to S^{-1}(R/\mathfrak{p}) \to 0$

$R \longrightarrow S^{-1}R$ $\quad S^{-1}M$ is an $S^{-1}R$ module,

$r \longmapsto \frac{r}{1}$ $\quad$ also an R module (restriction of scalars)

Ex. $\mathrm{Ass}_R\ S^{-1}M = \{\mathfrak{p} \in \mathrm{Ass}\ M \mid \mathfrak{p} \cap S = \phi\}$

(⊆) Let $S^{-1}\mathfrak{p} \in \mathrm{Ann}_{S^{-1}R}\ S^{-1}M$ where $\mathfrak{p} \in \mathrm{Spec}\ R$ and $\mathfrak{p} \cap S = \phi$.

↳ we know primes of $S^{-1}R$ are of this form

$$S^{-1}P = 0 :_{S^{-1}R} \frac{x}{s} = \left\{\frac{a}{t} \;\middle|\; \frac{a}{t} \cdot \frac{x}{s} = \frac{0}{1}\right\}$$

for some $\frac{x}{s}$

$$= \left\{\frac{a}{t} \;\middle|\; \frac{ax}{1} = \frac{0}{1}\right\}$$

$$= \left\{\frac{a}{t} \mid \exists u \in S \text{ s.t. } uax = 0\right\}$$

Write $\mathfrak{p} = (a_1, \dots, a_s)$.

Then, $S^{-1}\mathfrak{p}$ kills $\frac{x}{s}$.

That is, $\frac{a_i}{1} \frac{x}{s} = 0 \quad \forall i$

$\Rightarrow \exists s_i \in S$ s.t. $s_i a_i x = 0 \quad \forall i$

Put $s = s_1 \cdots s_n$. Then, $s a_i x = 0 \quad \forall i$.

$\Rightarrow a_i \in 0 : sx \quad \forall i$

$\Rightarrow \mathfrak{p} \subseteq (0 : sx)$.

We now show $\supseteq$.

Let $b \in (0 : sx)$. Then, $bsx = 0$.

$\Rightarrow \frac{b}{1} \cdot \frac{x}{1} = 0$ in $S^{-1}M$

$\Rightarrow \frac{b}{1} \cdot \frac{x}{s} = 0$

$\Rightarrow \frac{b}{1} \in 0 : \frac{x}{s} = S^{-1}\mathfrak{p}$

$\Rightarrow \frac{b}{1} = \frac{a}{t}$; $a \in \mathfrak{p}$, $t \in S$

$\Rightarrow \exists u \in S$, $u(bt - a) = 0$

$\Updownarrow$

$\underset{\notin \mathfrak{p}}{u}\, b\underset{\notin \mathfrak{p}}{t} = \underbrace{ua}_{\in \mathfrak{p}}$

$\Rightarrow b \in \mathfrak{p}$ ☒

(b) Take $S = R \setminus \mathfrak{p}$. $\mathfrak{p} \in \operatorname{Ass} M \Leftrightarrow \underset{\mathfrak{p}R_\mathfrak{p}}{\underset{\shortparallel}{S^{-1}\mathfrak{p}}} \in \operatorname{Ass}_{R_\mathfrak{p}} \underset{M_\mathfrak{p}}{\underbrace{S^{-1}M}}$

Properties of supp M

Recall: $\operatorname{Supp} M = \{\mathfrak{p} \in \operatorname{Spec}(R) \mid M_\mathfrak{p} \neq 0\}$.

If M is f.g., the $\operatorname{Supp} M = V(\operatorname{ann} M)$.

In particular, $\operatorname{Supp} M$ is a closed subset of $\operatorname{Spec} R$.

in Zariski topology

Note that the complement is open.

Prop^n. Let $0 \to N \to M \to L \to 0$ be an exact sequence of R-modules. Then,

$$\operatorname{supp} M = \operatorname{supp} N \cup \operatorname{supp} L.$$

Proof. ($\subseteq$) Let $\mathfrak{p} \in \operatorname{Supp} M$ and suppose $\mathfrak{p} \notin \operatorname{supp} N$. That is, $M_\mathfrak{p} \neq 0$ and $N_\mathfrak{p} = 0$. We show $L_\mathfrak{p} \neq 0$.

Note that $0 \to N \to M \to L \to 0$ is exact.

$\Rightarrow$ $0 \to N_\mathfrak{p} \to M_\mathfrak{p} \to L_\mathfrak{p} \to 0$ is exact

$\Rightarrow$ $0 \to M_\mathfrak{p} \to L_\mathfrak{p} \to 0$ is exact

$\Rightarrow$ $\underset{\neq 0}{M_\mathfrak{p}} \simeq L_\mathfrak{p}$

$\therefore L_\mathfrak{p} \neq 0$ or $\mathfrak{p} \in \operatorname{Supp} L$.

($\supseteq$) Suppose $\mathfrak{p} \in \operatorname{Supp} N$.

$\underset{\text{exact}}{0 \to N \to M}$ $\Rightarrow$ $0 \to \underset{\neq 0}{N_\mathfrak{p}} \xrightarrow[\text{1-1}]{} M_\mathfrak{p}$ exact

$\therefore M_\mathfrak{p} \neq 0$

$\Rightarrow \mathfrak{p} \in \operatorname{Supp} M$

Similarly, let $\mathfrak{p} \in \operatorname{Supp} L$. $M \to L \to 0$ exact

$\Rightarrow M_\mathfrak{p} \to L_\mathfrak{p}$ is surjective

and $L_\mathfrak{p} \neq 0$.

Thus, $M_\mathfrak{p} \neq 0$ or $\mathfrak{p} \in \operatorname{Supp} M$. ∎

Prop^n. Let L, K be f.g R-modules
Then,

$$\mathrm{Supp}\,(L \otimes_R K) = \mathrm{Supp}\, L \cap \mathrm{Supp}\, K.$$

In particular, $\mathrm{Supp}\, M/IM = \mathrm{Supp}\, M \cap V(I)$

Proof. ($\subseteq$) Let $\mathfrak{p} \in \mathrm{Supp}\,(L \otimes K)$.

Note $(L \otimes_R K)_\mathfrak{p} \simeq L_\mathfrak{p} \otimes_{R_\mathfrak{p}} K_\mathfrak{p}$.

(As $R_\mathfrak{p}$ - modules.)

Thus, $L_\mathfrak{p}, K_\mathfrak{p} \neq 0$. Thus, $\mathfrak{p} \in \mathrm{Supp}\, L \cap \mathrm{Supp} K$.

($\supseteq$) Let $\mathfrak{p} \in \mathrm{Supp}\, L \cap \mathrm{Supp}\, K$.

To show: $(L \otimes_R K)_\mathfrak{p} \neq 0$.

Note

$$(L \otimes_R K)_\mathfrak{p} \simeq L_\mathfrak{p} \otimes_{R_\mathfrak{p}} K_\mathfrak{p}$$

$R_\mathfrak{p}$ is a local ring with maximal ideal $\mathfrak{p}R_\mathfrak{p}$.
Moreover, $L_\mathfrak{p}, K_\mathfrak{p}$ are f.g. $R_\mathfrak{p}$-modules
Suffices to prove the following:

Prop^n. Let $(R, \mathfrak{m})$ be local and L, K f.g. R-modules.
Then, $L \otimes_R K \neq 0$.

Proof. Look at $\dfrac{L}{\mathfrak{m}L} \otimes_{R/\mathfrak{m}} \dfrac{K}{\mathfrak{m}K}$. $L/\mathfrak{m}L$ & $K/\mathfrak{m}K$ are fin dim $R/\mathfrak{m}$ v. spaces.

Note $\dim_k (V_1 \otimes_k V_2) = \dim_k V_1 \, \dim_k V_2$

Thus, $\dfrac{L}{\mathfrak{m}L} \otimes_{R/\mathfrak{m}} \dfrac{K}{\mathfrak{m}K} \neq 0$. In turn, $L \otimes_R K \neq 0$. ∎

Connection between Ass M and Supp M

Thm. $\mathrm{Ass}\, M \subset \mathrm{Supp}\, M$.

Proof. $\mathfrak{p} \in \mathrm{Ass}\ M \Rightarrow R/\mathfrak{p} \hookrightarrow M$

localisation preserves exactness and commutes with quotients

$$\Downarrow$$

field $\rightarrow \dfrac{R_\mathfrak{p}}{\mathfrak{p}R_\mathfrak{p}} \hookrightarrow M_\mathfrak{p}$

$\neq 0$

$\therefore\ M_\mathfrak{p} \neq 0$

Thus, $\mathrm{Ass}\ M \subset \mathrm{Supp}\ M$.

Converse not true. Take $\Bbbk$ as an inf. field.

$$(x) \subseteq k[x, y] = R$$

$$\mathrm{Supp}\left(R/(x)\right) = \mathcal{V}((x)) \ni \underbrace{(x, y-\alpha)}_{\text{maximal ideals}}{}_{\alpha \in k}$$

$$\mathrm{Ass}_R\left(R/(x)\right) = \{(0 : \bar{f})\ \text{prime} \mid x \nmid f\}$$

$$gf \in (x)$$

$x \mid gf$ but $x \nmid f$

$\Rightarrow x \mid g$

$\Rightarrow (g) \subseteq (x)$

Ex. $\mathrm{Ass}_R(R/\mathfrak{p}) = \{\mathfrak{p}\}$

Thus, $\mathrm{Ass}_R(R/(x))$ is a singleton, whereas Supp is infinite.

Lecture 5 (22-01-2021)

22 January 2021 13:59

Recall: R Noetherian, M a f.g. R-module

(1) $\text{Ass } M = \{ \mathfrak{p} \in \text{Spec } R : R/\mathfrak{p} \hookrightarrow M \} \subseteq \text{Supp } M = \mathcal{V}(\text{ann } M)$

(2) Maximal element among $0 : x$, $0 \neq x \in M$ are prime ideals and hence, $\in \text{Ass } M$.
(Converse not true, had seen example.)

(3) $\mathcal{Z}(M) = \bigcup_{\mathfrak{p} \in \text{Ass } M} \mathfrak{p}$

(4) If $0 \to M \to N \to P \to 0$ is an exact sequence,
then: (1) $\text{Ass } N \subseteq \text{Ass } M \cup \text{Ass } P$
(2) $\text{Ass } M \oplus N = \text{Ass } M \cup \text{Ass } N$
(3) $\text{Supp } M \otimes_R N = \text{Supp } M \cap \text{Supp } N$
(4) $\text{Supp } M/IM = \text{Supp } M \cap \mathcal{V}(I)$

R - Noetherian ring
M - f.g. R-module

$\text{Ass } M \subseteq \text{Supp } M$

Prop^n $\text{Ass } M$, $\text{Supp } M$ have same set of minimal primes.

Proof. Let $\mathfrak{p} \in \text{Supp } M = \mathcal{V}(\text{ann } M)$ be minimal.
TST: $\mathfrak{p} \in \text{Ass } M$. (Since $\text{Ass } M \subset \text{Supp } M$, it will show that $\mathfrak{p}$ is minimal in $\text{Ass } M$.)

Note $\mathfrak{p} \in \mathrm{Ass}_R M \iff \mathfrak{p}R_\mathfrak{p} \in \mathrm{Ass}_{R_\mathfrak{p}} M_\mathfrak{p}$.

Recall the $(R_\mathfrak{p}, \mathfrak{p}R_\mathfrak{p})$ is local. Thus, $\mathfrak{p}R_\mathfrak{p}$ is the only prime ideal (since $\mathfrak{p}$ was minimal) in support.
Thus,
$$\underset{\substack{\neq\\ 0}}{\mathrm{Supp}_{R_\mathfrak{p}} M_\mathfrak{p}} = \{\mathfrak{p}R_\mathfrak{p}\}.$$
$(\supseteq)$ in general
$(\subseteq)$ by minimality

Moreover, $\emptyset \neq \mathrm{Ass}_{R_\mathfrak{p}} M_\mathfrak{p} \subseteq \mathrm{Supp}_{R_\mathfrak{p}} M_\mathfrak{p}$.

Thus, $\mathfrak{p}R_\mathfrak{p} \in \mathrm{Ass}_{R_\mathfrak{p}} M_\mathfrak{p}$ and hence, $\mathfrak{p} \in \mathrm{Ass}_R M$.

Let $I \trianglelefteq R$ be an ideal. Then, $\mathrm{Ass}(R/I) \subseteq \mathrm{Supp}(R/I) = V(I)$.
Thus, if $\mathfrak{p}$ is minimal in I, then $\mathfrak{p} \in \mathrm{Ass}(R/I)$ and thus,
$$R/\mathfrak{p} \underset{1 \mapsto \bar{x}}{\hookrightarrow} R/I.$$

$$\mathfrak{p} = (\bar{0} : \bar{x}) \qquad x \in R/I$$
$$\Rightarrow \mathfrak{p} = I : x$$

Other direc.: $\mathfrak{p} \in \mathrm{Ass}(M)$ minimal
$\Rightarrow \mathfrak{p}$ is minimal in $\mathrm{Supp}(M)$ (We know it is in Supp)

Suppose not. Then, $\exists$ minimal $\mathfrak{q} \in \mathrm{Supp}\, M$ s.t.
$\mathfrak{q} \subsetneq \mathfrak{p}$. (Primes satisfy d.c.c.)

But then, by the previous part, $\mathfrak{q} \in \mathrm{Ann}\, M$ and $\mathfrak{q} \subsetneq \mathfrak{p}$, contradicting minimality. ∎

Example. $R = \mathbb{k}[X, Y]$, $I = (x^2, xy)$

$\mathfrak{p} = (x) \subseteq (x, y) = \mathfrak{m} \in \mathrm{Ass}(R/I)$

$\underbrace{\mathfrak{p} = (x)}_{\text{minimal prime}} \subseteq \underbrace{(x, y) = \mathfrak{m}}_{\text{embedded associated prime}} \in \operatorname{Ass}(R/I)$

If $\mathfrak{q} \supseteq I = (x^2, xy)$

$\Rightarrow x \in \mathfrak{q} \Rightarrow (x) \subset \mathfrak{q}$ $\quad \therefore$ unique minimal prime

$\mathfrak{m} = I : x \quad \Rightarrow \quad \mathfrak{m} = 0 : \bar{x} \quad \in \operatorname{Ass} R/I$

$\Rightarrow \dfrac{\mathfrak{m}}{I} = \dfrac{I : x}{I}$

Thm. R Noe., M f.g. Rmodule.

(1) $\exists$ a sequence of submodules

$$(0) \subset M_1 \subset \cdots \subset M_{n-2} \subset M_{n-1} \subset M \qquad (*)$$

s.t.

$$M/M_{n-1} \simeq R/\mathfrak{p}_n, \ \ldots, \ M_2/M_1 \simeq R/\mathfrak{p}_2, \ M_1/(0) = M_1 \simeq R/\mathfrak{p}_1$$

for primes $\mathfrak{p}_1, \ldots, \mathfrak{p}_n \in \operatorname{Spec}(R)$.

Recall that $\operatorname{Ass} R/\mathfrak{p} = \{\mathfrak{p}\}$.

Using short exact sequences, we can get the Ass of big module.

(2) If M has a sequence of type $(*)$, then

$$\operatorname{Ass} M \subset \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\} \in \operatorname{Supp} M.$$

In particular, $\operatorname{Ass} M$ is finite.

Proof. We may assume $M \neq 0$.

Proof. We may assume $M \neq 0$.

(1) We know $\operatorname{Ass} M \neq \phi$.

Pick $p_1 \in \operatorname{Ass} M$. $\quad R/p_1 \xrightarrow[\sim]{\mu_x} \underset{M_1}{\overset{\wr\wr}{Rx}} \subseteq M$

$0 \subset M_1 \subset M, \qquad M_1/0 \simeq R/p_1$

- If $M = M_1 = Rx$, $\operatorname{Ass}(M) = \operatorname{Ass}(R/p_1) = \{p_1\}$ and both parts are true.

Thus, assume $M \neq M_1$ and hence, $M/M_1 \neq 0$

Then, $\operatorname{Ass} M/M_1 \neq \phi$.

Pick $p_2 \in \operatorname{Ass}(M/M_1)$. Thus,

$$R/p_2 \simeq M_2/M_1 \quad \text{where} \quad \underset{M_1}{\overset{\cup\!\shortmid}{M_2}} \subseteq M$$

a typical submodule of M/M_1

$0 \subset M_1 \subset M_2 \subset M.$

- If $M = M_2$, we stop and conclude first part.

Can repeat the process. We get an ascending chain of submodules

$$0 \subset M_1 \subset M_2 \subset \cdots \subset M.$$

But M is Noetherian; thus, the above terminates. Moreover, the eventual termination must be at M, else we could continue.

Thus, we get

$$0 \subset M_1 \subset M_2 \subset \cdots \subset M_{n-1} \subset M \quad \text{where}$$

$$M_{i+1}/M_i \simeq R/p_i \quad \text{for each } i.$$

(2) To show $\operatorname{Ass} M \subseteq \{p_1, \dots, p_n\} \subseteq \operatorname{Supp} M$.

Had seen it true when $n=1$.

Suppose $n=2$. We have

$$0 \subsetneq M_1 \subsetneq M_2 \subseteq M$$

We have

$$0 \longrightarrow M_1 \longrightarrow M \longrightarrow M/M_1 \longrightarrow 0$$

$$\Rightarrow \operatorname{Ass} M \subset \underbrace{\operatorname{Ass} M_1}_{= \{p_1\}} \cup \underbrace{\operatorname{Ass} M/M_1}_{= \{p_2\}} \quad \text{(Ex 1.)}$$

$$\Rightarrow \operatorname{Ass} M \subset \{p_1, p_2\}$$

Note $\operatorname{Supp} M = \operatorname{Supp} M_1 \cup \operatorname{Supp} M/M_1$

$$\supseteq \operatorname{Ass} M \cup \operatorname{Ass} M/M_1$$

$$\supseteq \{p_1, p_2\}.$$

Continue by induction

$$0 \longrightarrow M_{n-1} \longrightarrow M_n = M \longrightarrow M/M_{n-1} \longrightarrow 0.$$

$$\operatorname{Ass}(M_n) \subseteq \underbrace{\operatorname{Ass}(M_{n-1})}_{\overset{\text{ind}}{\subseteq} \{p_1, \dots, p_{n-1}\}} \cup \underbrace{\operatorname{Ass}(M/M_{n-1})}_{= \{p_n\}}$$

Thus, $\operatorname{Ass}(M) \subseteq \{p_1, \dots, p_{n-1}\}$.

By induction, $\{p_1, \dots, p_{n-1}\} \subseteq \operatorname{Supp} M_{n-1} \subseteq \operatorname{Supp} M$.

Moreover, $p_n \in \operatorname{Supp}(M/M_{n-1}) \subset \operatorname{Supp}(M)$.

Thus,

$$\operatorname{Ass} M \subseteq \{p_1, \dots, p_n\} \subseteq \operatorname{Supp}(M). \qquad \blacksquare$$

Note for (2), it works for any filtration (*), however constructed.

$R = \mathbb{k}[x,y]$, $\quad I = (x^2, xy)$

Example Let us prove $\quad \mathrm{Ass}(R/I) = \{\overset{(x)}{\overset{\shortparallel}{\mathfrak{p}}}, \overset{(x,y)}{\overset{\shortparallel}{\mathfrak{m}}}\}$.

(⊇) Shown already

$$I : y = (x^2, xy) : (y) = (x) = \mathfrak{p} \qquad \text{(Ex 2.)}$$

Let $\bar{y} = y + I \in R/I$

$$0 :_R \bar{y} = \{r \in R : r\bar{y} = 0\}$$
$$= \{r \in R : ry \in I\}$$
$$= I :_R y$$

$\varphi : R/I \xrightarrow{\bar{y}} R/I$

$\mathrm{im}\,\varphi = \bar{y}(R/I) \cong \dfrac{R/I}{\ker\varphi} \cong \dfrac{R}{I:y}$

$R \twoheadrightarrow R/I \twoheadrightarrow \mathrm{im}\,\varphi$

$$R/I \xrightarrow{\bar{y}} \bar{y}(R/I) \cong \frac{R}{I:y} = \frac{R}{\mathfrak{p}} \hookrightarrow \frac{R}{I}$$

it is isomorphic to a submodule of R/I, namely $\langle \bar{y} \rangle$

knew this already

$$\therefore \mathfrak{p} \in \mathrm{Ass}(R/I)$$

$$\bar{y}(R/I) \subseteq R/I$$

$$\frac{R/I}{\bar{y}(R/I)} = \frac{R/I}{\frac{y+I}{I}} \cong \frac{R}{(y, I)}$$
$$= \frac{R}{(y, x^2, xy)} = \frac{R}{(y, x^2)} \neq 0$$

So far: $\quad 0 \subset \underset{\overset{\shortparallel}{M_1}}{\bar{y}R/I} \subset \underbrace{R/I.}_{R/(y,x^2)}$

Thus, now we look at $\mathrm{Ass}(M/M_1)$.

$$\phi \neq \mathrm{Ass}(M/M_1) = \mathrm{Ass}\left(R/(y,x^2)\right) \subseteq V\left((y,x^2)\right)$$
$$\overset{\shortparallel}{\{\mathfrak{m}\}} = \{(x,y)\}$$

if $\mathfrak{p}' \supset (y, x^2)$,
then $\mathfrak{p}' \ni y, x^2$
$\Rightarrow \mathfrak{p}' \ni y, x$
$\Rightarrow \mathfrak{p}' \supset (x,y) = \mathfrak{m}$

$\therefore \mathrm{Ass}(M/M_1) = \{\mathfrak{m}\}$.

(Check) $\quad \mathfrak{m} = (y, x^2) : x$. $\qquad x\left(\dfrac{R}{(y,x^2)}\right) = \dfrac{(x,y)}{(y,x^2)} = M_2$

Def^n. (p-primary and p-coprimary)

Let M be a module such that $\mathrm{Ass}\, M = \{\mathfrak{p}\}$.
Then, M is called p-coprimary.
If $N \subseteq M$ and $\mathrm{Ass}(M/N) = \{\mathfrak{p}\}$, then N is called p-primary.

Example. $\underset{\{(p)\}}{\mathrm{Ass}_{\mathbb{Z}}(\mathbb{Z}/p^n\mathbb{Z})} \subseteq \mathrm{Supp}(\mathbb{Z}/p^n\mathbb{Z}) = V(p^n\mathbb{Z}) = \{(p)\}$.

$\therefore$ $p^n\mathbb{Z}$ is $p\mathbb{Z}$-primary submodule of $\mathbb{Z}$.

In general, if $\mathfrak{m}$ is a maximal ideal of R,

$\mathrm{Ass}(R/\mathfrak{m}^n R) \subseteq \mathrm{Supp}(R/\mathfrak{m}^n R) = V(\mathfrak{m}^n R) = \{\mathfrak{m}\}$

$\cup\!\!\mid$ $\quad \mathfrak{m} = 0 : \overline{\mathfrak{m}^{n-1}}$

$\{\mathfrak{m}\}$

$\therefore$ $\mathfrak{m}^n$ is an $\mathfrak{m}$-primary ideal. (Converse not true.)

$\underset{\mathfrak{m}^2}{\underset{\|}{(x^2, y^2, xy)}} \subseteq \underset{I}{\underset{\|}{(x^2, y)}} \subseteq \underset{\mathfrak{m}}{\underset{\|}{(x, y)}}$

$\underset{\neq \phi}{\mathrm{Ass}(R/I)} \subseteq \mathrm{supp}(R/I) = V(I) = \{\mathfrak{m}\}$

$\Rightarrow \mathrm{Ass}\, R/I = \{\mathfrak{m}\}$

The above works for any I s.t. $\mathfrak{m}^2 \subset I \subset \mathfrak{m}$.

Example. If $\mathfrak{p} \in \mathrm{Spec}\, R$, then $\mathfrak{p}^n$ need not be $\mathfrak{p}$-primary.

$R = \mathbb{k}[x, y, z]$, $\quad F = z^2 - xy$, $\quad S = R/(F)$.

Is (F) a prime ideal? By Eisenstein, F is irred in $\mathbb{k}[X, Y][Z]$.

$\therefore$ $R/(F)$ is an integral domain.

$$V((F)) \supseteq \{(F), (X, Y, Z), (X, Z), (Y, Z)\}$$

$x = X + (F)$, $y = Y + (F)$, $z = Z + (F)$.

$z^2 = xy$ in S.

Consider $\mathfrak{p} = \frac{(X, Z)}{(F)} = (x, z)$.

Then, $\mathfrak{p}^2 = (x^2, xz, z^2)$
$= (x^2, xz, xy)$
$= (x)\underbrace{(x, y, z)}_{\text{maximal, say } \mathfrak{m}}$

Note $\mathfrak{m} = \mathfrak{p}^2 : x$.

Thus, $\mathfrak{m} \in \mathrm{Ass}(S/\mathfrak{p}^2)$. Moreover, $\overset{\text{minimal prime}}{\mathfrak{p}} \in \mathrm{Ass}(S/\mathfrak{p}^2)$.

Thus, $\mathfrak{p}^2$ is not primary.

Lecture 6 (26-01-2021)

26 January 2021 13:59

R Noetherian, $M \to$ finite R module

f.g., not saying M, as a set, is finite

Suppose $\mathrm{Ass}\ M = \{p\}$. $\mathrm{Ass}\ M \subseteq \mathrm{Supp}\ M$

same set of minimal elements

$$\mathrm{Supp}\ M = V(\mathrm{ann}\ M)$$

$\exists$ only one minimal prime $\supseteq \mathrm{ann}\ M$

$$\therefore \sqrt{\mathrm{ann}\ M} = \mathfrak{p} \qquad \left(\sqrt{I} = \bigcap V(\mathrm{ann}\ I)\right)$$

$$Z(M) = \bigcup_{q \in \mathrm{Ass}\ M} q = \mathfrak{p} = \sqrt{\mathrm{ann}\ M}$$

$V(\mathfrak{p}) = V(\mathrm{ann}\ M)$

$a \in \mathfrak{p} \Rightarrow \exists n$ s.t. $a^n \in \mathrm{ann}\ M$.

$\Rightarrow a^n M = 0$

$\mu_a : M \longrightarrow M$ with $\underbrace{\mu_a \circ \cdots \circ \mu_a}_{n} = 0$

Thus, μ_a is a nilpotent endomorphism.

$$\begin{aligned} \mathrm{nil}(M) &= \{ a \in R \mid \mu_a \text{ is nilpotent} \} \\ &= \{ a \in R \mid a^n M = 0 \} \\ &= \sqrt{\mathrm{ann}\ M} \end{aligned}$$

(Nilpotents of M)

Thus, $Z(M) = \mathrm{nil}(M) = \sqrt{\mathrm{ann} M}$

($\supseteq$) in general

($\subseteq$) if $\mathrm{Ass}\ M = \{\mathfrak{p}\}$

Thus, $\mathrm{Ass}\ M = \{p\} \Rightarrow Z(M) = \mathrm{nil}(M)$

Thus, $\operatorname{Ass} M = \{\mathfrak{p}\} \Rightarrow Z(M) = \operatorname{nil}(M)$

μ_a not 1-1 $\qquad$ μ_a is nilpotent

$(\Leftarrow)$ also true.

Proof: Suppose $Z(M) = \operatorname{nil}(M)$. Then we show that $\operatorname{Ass}(M)$ is singleton. Claim $\operatorname{Ass}(M) = \{\mathfrak{p}\}$ for $\mathfrak{p} = \sqrt{\operatorname{ann} M}$.
(That is, M is coprimary or that 0 is primary.)

Let $\mathfrak{p} \in \operatorname{Ass}(M)$. Thus, $\mathfrak{p} \subseteq Z(M) = \operatorname{nil}(M)$ $\qquad$ $\left(Z(M) = \bigcup \operatorname{Ass} M\right)$

$\left(a \in Z(M) \Rightarrow a \in \operatorname{nil}(M)\right)$

If $a \in \mathfrak{p}$, then $a^n M = 0$, thus $a \in \sqrt{\operatorname{ann} M}$.

Thus, $\mathfrak{p} \subset \sqrt{\operatorname{ann} M}$.

OTOH, $\mathfrak{p} \in \operatorname{Supp}(M) = V(\operatorname{ann} M)$

Thus, $\mathfrak{p} \supset \operatorname{ann} M \Rightarrow \mathfrak{p} \supset \sqrt{\operatorname{ann} M}$.

Thus, $\operatorname{Ass} M \subset \{\sqrt{\operatorname{ann} M}\}$. Since $\operatorname{Ass} M \neq \emptyset$, we are done. ☒

$N \subseteq M$ and N is $\mathfrak{p}$-primary

$\Leftrightarrow \operatorname{Ass}(M/N) = \{\mathfrak{p}\}$

$\Leftrightarrow Z(M/N) = \operatorname{nil}(M/N) = \sqrt{\operatorname{ann} \frac{M}{N}}$

$\Rightarrow \mathfrak{p} = \sqrt{\operatorname{ann}(M/N)} \in \operatorname{Spec} R$

$a \in \sqrt{\operatorname{ann} M/N} \Leftrightarrow a^n \in \operatorname{ann} M/N \Leftrightarrow a^n M \subseteq N$

$\mathfrak{p} = \{a \in R \mid a^n M \subseteq N \text{ for some } n \in \mathbb{N}\}$

$M = R/I$, I an ideal

I is $\mathfrak{p}$-primary $\Rightarrow \mathfrak{p} = \sqrt{\operatorname{ann} R/I}$

$\Leftrightarrow \mathfrak{p} = \sqrt{I}$

$$\Updownarrow$$

$$Z(R/I) = \operatorname{nil}(R/I) = \sqrt{I}$$
$$= \bigcup_{\mathfrak{p} \in \operatorname{Ass}(R/I)}$$

Prop^n. Let $N_1, N_2 \subseteq M$, $\mathfrak{p}$-primary.
Then, $N_1 \cap N_2$ is $\mathfrak{p}$-primary. (Not necessary for sums or colons.)

Proof. Need to prove $\operatorname{Ass}\left(M/N_1 \cap N_2\right) = \{\mathfrak{p}\}$.

Know: $\operatorname{Ass}(M/N_1) = \operatorname{Ass}(M/N_2) = \{\mathfrak{p}\}$.

$$M \xrightarrow{\varphi} M/N_1 \oplus M/N_2$$
$$m \longmapsto (m+N_1, m+N_2)$$

$$\ker \varphi = N_1 \cap N_2$$

Then,
$$0 \longrightarrow \frac{M}{N_1 \cap N_2} \xrightarrow{\bar{\varphi}} \frac{M}{N_1} \oplus \frac{M}{N_2} \xrightarrow{\psi} \frac{M}{N_1 + N_2} \longrightarrow 0$$
$$(m_1+N_1, m_2+N_2) \longmapsto \overline{m_1 - m_2}$$

is a short exact sequence.

since it's a submodule now

direct sum

$$\operatorname{Ass}\left(M/N_1 \cap N_2\right) \subseteq \operatorname{Ass}\left(\frac{M}{N_1} \oplus \frac{M}{N_2}\right) = \operatorname{Ass}\left(\frac{M}{N_1}\right) \cup \operatorname{Ass}\left(\frac{M}{N_2}\right)$$
$$= \{\mathfrak{p}\}$$

Since $M/N_1 \cap N_2 \neq 0$, $\operatorname{Ass}\left(M/N_1 \cap N_2\right) = \{\mathfrak{p}\}$. $\blacksquare$

Q. What is the source of primary submodules?

Def^n. Suppose $N \subseteq M$ and $N = N_2 \cap N_1$ with $N \subsetneq N_1, N_2 \subseteq M$.
Then, N is called reducible, else it is called irreducible.

(Irreducible submodules, reducible submodules)

Example ① $\mathfrak{p} \in \operatorname{Spec}(R)$. Then $\mathfrak{p}$ is irreducible.

Proof. Suppose $\mathfrak{p} = I \cap J \supseteq IJ$.

Then, $IJ \subseteq \mathfrak{p}$ and thus, $I \subseteq \mathfrak{p}$ or $J \subseteq \mathfrak{p}$.

But $\mathfrak{p} \subseteq I, J$ given.

Thus, $I = \mathfrak{p}$ or $J = \mathfrak{p}$.

② Let $p > 0$ be prime. Then, $I = p^n \mathbb{Z}$ is irreducible.

Proof. Suppose $p^n \mathbb{Z} = m_1 \mathbb{Z} \cap m_2 \mathbb{Z}$ ← $\mathbb{Z}$ is a PID

$= \operatorname{lcm}(m_1, m_2)\, \mathbb{Z}$

$\Rightarrow m_1 = \pm p^r, \quad m_2 = \pm p^s$ with $\max(r, s) = n$.

$\Rightarrow \pm p^n = m_1$ or m_2

Note that $\operatorname{Ass}(R/\mathfrak{p}) = \{\mathfrak{p}\}$ and $\operatorname{Ass}(\mathbb{Z}/p^n\mathbb{Z}) = \{p\mathbb{Z}\}$.

Thus, $\mathfrak{p}$ and $p^n \mathbb{Z}$ are primary and irreducible submodules.

Thm. Any submodule of M (finite over Noe.) is an intersection of finitely many submodules which are irreducible submodules.

Proof. Let $\mathcal{F} = \{N \leq M \mid N \neq \text{finite intersection of irreducibles}\}$.

Suppose $\mathcal{F} \neq \emptyset$. Then, $\exists L \in \mathcal{F}$ maximal. (Noetherian)

Thus, $L = L_1 \cap L_2$ with $L \subsetneq L_1, L_2 \leq M$.

Thus, $L_1, L_2 \notin \mathcal{F}$.

Thus, L_1 and L_2 are finite intersections of irred submodules.

Thus, so is $L_1 \cap L_2 = L$ →←

Thus, $\mathcal{F} = \emptyset$. ∎

Prop^n. Irreducible proper submodules are primary. (Converse not true.)

Proof. Let N be irreducible. To show: $|\mathrm{Ass}(M/N)| = 1$.
Suppose it is not primary. Then, $\mathrm{Ass}(M/N) \ni \mathfrak{p}, \mathfrak{q}$
where $\mathfrak{p} \neq \mathfrak{q} \in \operatorname{Spec} R$.

$$\Rightarrow \quad \mathfrak{p} = 0 : \bar{x} \qquad x \in M \setminus N$$

exclusion

$$\mathfrak{q} = 0 : \bar{y} \qquad y \in M \setminus N$$

$$\mathfrak{p} = 0 : \bar{x} \qquad\qquad \mathfrak{q} = N :_R yR$$

$$= N :_R xR$$

$(xR = \langle x \rangle = \{rx : r \in R\} \subseteq M)$

Note $R/\mathfrak{p} \simeq \bar{x}R = \dfrac{xR + N}{N}$ → only one ass prime $\mathfrak{p}$

submodules of M/N

$R/\mathfrak{q} \simeq \bar{y}R = \dfrac{yR + N}{N}$ → only one ass prime $\mathfrak{q}$

(Note that if $0 \neq \bar{z} \in R/\mathfrak{p}$, then $0 : \bar{z} = \{a \in R \mid az \in \mathfrak{p}\}$ ($\bar{z} \notin \mathfrak{p}$)

$= \mathfrak{p}$

III^{ly} if $0 \neq \bar{z} \in R/\mathfrak{q}$, then $0 : \bar{z} = \mathfrak{q}$.)

$$\bar{x}R \cap \bar{y}R = \left(\frac{xR+N}{N}\right) \cap \left(\frac{yR+N}{N}\right)$$

any non-zero element would have ann $= \mathfrak{p}$ and $= \mathfrak{q}$
but $\mathfrak{p} \neq \mathfrak{q}$. ∴ intersection $= 0$

$$\therefore \bar{x}R \cap \bar{y}R = 0$$

$$\Rightarrow N = (xR + N) \cap (yR + N)$$

$$\underset{N}{\supsetneq} \qquad \underset{N}{\supsetneq}$$

→ N is reducible →←

Thus N is primary ⊡

$\to$ N is reducible $\to\leftarrow$

Thus, N is primary. ☒

A corollary of above:

Thm. Any submodule N of M can be written as

$$N = N_1 \cap \cdots \cap N_r, \qquad (*)$$

where $N_1, \ldots, N_r$ are primary submodules, i.e.,

$\mathrm{Ass}(M/N_i) = \{p_i\}$ where $p_i = \sqrt{\mathrm{Ass}\, M/N_i}$.

$(*)$ is called a primary decomposition of N.

(Primary decomposition)

Note that if $p_i = p_j$, then $N_i \cap N_j$ is also $p_i = p_j$ primary. Thus, we can combine them. Thus, we can make sure that $p_i \neq p_j$ for $i \neq j$. This decomposition is called a minimal primary decomposition.

A decomposition $N_1 \cap N_2 \cap \cdots \cap N_r$ is called irredundant if no N_i can be dropped.

(Minimal primary decomposition, irredundant primary decomposition)

Thm. If $N = N_1 \cap \cdots \cap N_r$, irredundant and $\mathrm{Ass}(M/N_i) = \{p_i\}$, then

$$\mathrm{Ass}(M/N) = \{p_1, \ldots, p_r\}$$

$$p_i = \sqrt{\mathrm{ann}\; M/N_i} = \sqrt{N_i : M}.$$

(Macaulay2 is a website that does this decomposition.)

Proof. By passing to a quotient, we may assume $N = 0$.

$0 = N_1 \cap \cdots \cap N_r$, N_i are p_i-primary

$$M \xrightarrow{\varphi} \frac{M}{N_1} \oplus \cdots \oplus \frac{M}{N_r}.$$

$$M \xrightarrow{\varphi} \frac{M}{N_1} \oplus \cdots \oplus \frac{M}{N_r}.$$

$\ker \varphi = N_1 \cap \cdots \cap N_r = 0$. Thus, φ is 1-1 and hence,

$$\operatorname{Ass} M \subseteq \{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\} = \bigcup_{i=1}^{r} \operatorname{Ass}(M/N_i).$$

($\supseteq$) We show $\mathfrak{p} = \mathfrak{p}_1$ is an associated prime of M.

Pick $x \in N_2 \cap \cdots \cap N_r \setminus N_1$ $\quad \neq \emptyset$ since irredundant

$$\mathfrak{p}_1 = \sqrt{\operatorname{ann} M/N_1}$$

$0 \neq \bar{x} \in M/N_1$. $\exists n \in \mathbb{N}$ s.t. $\mathfrak{p}_1^n x \subseteq N_1$

but $x \notin N_1$.

Then, $\underset{\substack{\cap\!\!\!| \\ N_1}}{\mathfrak{p}_1^n x} \subseteq \cdots \subseteq \mathfrak{p}_1^2 x \subseteq \mathfrak{p}_1 x \subseteq (x) \not\subseteq N_1$

Let n be minimal s.t. $\mathfrak{p}_1^n x \subseteq N_1$ but $\mathfrak{p}_1^{n-1} x \subseteq N_1$.

($n = 1$ allowed)

Pick $y \in \mathfrak{p}_1^{n-1} x$ s.t. $y \notin N_1$.

$$\underbrace{\mathfrak{p}_1 y}_{\subseteq \mathfrak{p}_1^n x^{(1)}} \subseteq N_1.$$

Note that $x \in N_2 \cap \cdots \cap N_r$ and thus,

$\mathfrak{p}^n x \subset N_2 \cap \cdots \cap N_r$ and $\mathfrak{p}^n x \subset N_1$.

Thus, $\mathfrak{p} y \subset \mathfrak{p}^n x \subset N_1 \cap \cdots \cap N_r = 0$.

$\Rightarrow \quad \mathfrak{p} \subset (0 : y)$.

<u>Claim</u>. $\mathfrak{p} = (0 : y)$

<u>Proof</u>. ($\supseteq$) Let $a \in (0 : y)$.

We already know $a y \in \mathfrak{p}^{n-1} x \subset N_2 \cap \cdots \cap N_r$.

$ay = 0 \Rightarrow a\bar{y} = 0$ in M/N_1 and $\bar{y} \neq 0$

$\Rightarrow a \in Z(M/N_1) = \mathfrak{p}$

Thus, $\mathfrak{p} = (0 : y) \in \operatorname{Ass} M$. ∎

Lecture 7 (02-02-2021)

02 February 2021 13:58

Chapter 3: Artinian rings and Artinian modules

Artinian rings : d.c.c. on ideals
$\equiv$ minimal condition of any nonempty set of ideals

Artinian modules : "submodules" instead of "ideals" above.

Will see interesting results such as:

Thm. (1) Artinian rings are Noetherian.
A Noetherian ring R is Artinian
$\Leftrightarrow \operatorname{Spec} R = \operatorname{mSpec}(R) = \{\mathfrak{p} \in \operatorname{Spec} R : \mathfrak{p} \text{ is maximal}\}$.

(2) Artinian modules need not be Noetherian modules.

(3) If M is finite over an Artinian ring, then M is both Noetherian and Artinian.

(4) If M is both Noetherian and Artinian:
then any strict chain of submodules will terminate on both sides. Moreover, the length of all maximal chains is the same, called the length $\ell(M)$ of the module.
$\to$ Analog of dimension

Examples. (1) Any field is both Artinian and Noetherian.
More generally, if a ring R has finitely many ideals, then R is both.

$(n>0)$ $\mathbb{Z}/n\mathbb{Z} \longrightarrow$ ideals of the form $(m)/(n)$ where $m|n$.
Thus $\#$ ideals in $\mathbb{Z}/n\mathbb{Z}$ $=$ $\#$ positive disiors of n.

(2) Similarly, $R = \frac{\mathbb{k}[x]}{(f(x))}$ is both Art and Noe. for $\deg(f(x)) \geq 1$.

Note that $\operatorname{Spec} \mathbb{Z}/n\mathbb{Z} = \operatorname{mSpec}(\mathbb{Z}/n\mathbb{Z})$
$= \left\{ \frac{p\mathbb{Z}}{n\mathbb{Z}} : p \mid n,\ p \text{ prime} \right\}$

$\operatorname{Spec} \frac{\mathbb{k}[x]}{f(x)} = \operatorname{mSpec} \frac{\mathbb{k}[x]}{f(x)}$ (will see this is true in all Art. rings.)

(3) $\mathbb{Z}$ is Noetherian (PID) but $\mathbb{Z}$ is not Artinian.
$(2) \supsetneq (2^2) \supsetneq (2^3) \supsetneq \cdots$ never terminates.

(4) Artinian rings need not have finitely many ideals.
assume infinite
$S = \mathbb{k}[x, y]$; consider $\mathfrak{m} = (x, y)$ and $\mathfrak{m}^2 = (x^2, xy, y^2)$.

Put $R = S/\mathfrak{m}^2$. $\operatorname{Spec}(R) = \{ \mathfrak{m}/\mathfrak{m}^2 \}$

Claim 1. R is Artinian.

Proof. Note that R is a $\mathbb{k}$-vector space.
$x = X + \mathfrak{m}^2$, $y = Y + \mathfrak{m}^2$
Then, $x^2 = xy = y^2 = 0$ in R.
Elements of R:
$$\sum a_{ij} x^i y^j$$
But $x^i y^j = 0$ whenever $i+j \geq 2$ or $i \geq 2, j \geq 2, (i, j \geq 1)$

Thus, the only elements are $\mathbb{k}$-linear combinations of
$1, x, y$.
Moreover, $\{1, x, y\}$ is a basis of R as a $\mathbb{k}$-vector space.
Moreover, ideals are $\mathbb{k}$-vector subspaces.

Moreover, ideals are $\mathbb{k}$-vector subspaces.
If $I_1 \supsetneq I_2 \supsetneq \cdots$, then it is a decreasing chain of subspaces. Thus, it must terminate. $\square$

Claim 2. R has infinitely many ideals.

Proof. $I_\alpha = (x+\alpha y)$; $\alpha \in \mathbb{k}$

Suppose $I_\alpha = I_\beta$ and $\alpha \neq \beta$.

Then, $\langle x+\alpha y \rangle = \langle x+\beta y \rangle = J$.

$$\Rightarrow (x+\alpha y) - (x+\beta y) \in J$$

maximal

$(x,y) = (x+\alpha y)$

$\dim_{\mathbb{k}} = 2$ $\quad$ $\dim_{\mathbb{k}} = 1$

$$\Rightarrow (\alpha - \beta) y \in J \qquad (\because \alpha - \beta \text{ is invertible})$$

$$\Rightarrow y \in J$$

$$\Rightarrow x \in J \qquad (\because x + \alpha y \in J)$$

$\rightarrow\leftarrow$

$\therefore \{I_\alpha\}_{\alpha \in \mathbb{k}}$ are distinct and infinitely many.

Basic properties of Artinian Rings

R is an Artinian ring:

(1) If I is an R-ideal, then R/I is Artinian.

(Ideals of R/I are of the form J/I for $I \subseteq J \trianglelefteq R$.
Thus, (J_n/I) descending $\Rightarrow (J_n)$ desc $\Rightarrow (J_n)$ stabilises $\Rightarrow (J_n/I)$ stab.)

(2) Suppose R is an Artinian integral domain. Then R is a field.

Let $0 \neq x \in R$. Then, $(x) \supseteq (x^2) \supseteq \cdots$ and hence,
$(x^n) = (x^{n+1})$ for some n.

$\therefore x^n = r x^{n+1}$ for some $r \in R$.

$\Rightarrow 1 = rx$ (since $0 \neq x \in R \leftarrow$ integral domain)

$\Rightarrow x$ is invertible. $\therefore R$ is a field.

The proof also tells us: Any non-zero divisor in an Artinian ring is invertible.

(3) Let $\mathfrak{p} \in \operatorname{Spec} R$ and R Artinian. Then, $\mathfrak{p}$ is maximal.

$R/\mathfrak{p}$ is a domain. It is Artinian, by (1). It is a field, by (2).

(4) Let R be Artinian. Then, it has finitely many maximal ideals.

Suppose not. Take a countable collection and label them $\mathfrak{m}_1, \mathfrak{m}_2, \ldots$ of distinct max ideals.

Then, $\mathfrak{m}_1 \supsetneq \mathfrak{m}_1 \cap \mathfrak{m}_2 \supseteq \cdots$

$$\therefore \quad \underset{\mathfrak{m}_1 \cdots \mathfrak{m}_n}{\overset{\cup\!|}{\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_n}} = \underset{\mathfrak{m}_{n+1}}{\overset{\cap\!|}{\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_{n+1}}} \quad \text{for some } n.$$

$\mathfrak{m}_{n+1} \to$ prime

$\Downarrow$

$\mathfrak{m}_1 \cdots \mathfrak{m}_n \subseteq \mathfrak{m}_{n+1}$

$\therefore \exists i \in \{1, \ldots, n\}$ s.t. $\mathfrak{m}_i \subseteq \mathfrak{m}_{n+1}$. $\rightarrow\leftarrow$

In particular, $\operatorname{Spec}(R) = \operatorname{mSpec}(R)$ is a finite set.

Thus, $\underbrace{J(R)}_{\text{Jacobson radical}} = \underbrace{N(R)}_{\text{nilradical}}$.

$\mathcal{N}(R) = \sqrt{0} = \mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_n$ is the primary decomposition of $\sqrt{0}$.

we'll see later that this can be dropped

Suppose $I \trianglelefteq R$, R is Artinian and Noetherian.

Then, $\operatorname{Ass}(R/I) = \underbrace{\operatorname{Supp}(R/I)}_{} = V(I)$

all ideals are maximal here (using Art.)
thus, they are minimal elements
hence, they are in Ass. (Noe)

(5) $\mathcal{N}(R) = N = \{x \in R : x^n = 0 \text{ for some } n\}$ is a nilpotent ideal, i.e., $N^k = 0$ for some k.

Proof. We have $N \supseteq N^2 \supseteq N^3 \supseteq \cdots$.

Thus $N^n = N^{n+1}$ for some n. can't use NAK

Proof. We have $N \supset N^2 \supset N^3 \supset \cdots$.

Thus, $N^n = N^{n+1} = \cdots$ for some n.

can't use NAK here. Dunno if I is f.g.

Claim. $N^n = 0$.

Proof. Put $I = N^n$. $N^n = N^{2n}$ and thus, $I = I^2$.

Suppose, for the sake of contradiction, that $I \neq 0$

$$\Sigma = \{ K \subseteq R : K \text{ is an ideal of } R,\ KI \neq 0 \}.$$

Note $I, R \in \Sigma$. In particular $\Sigma \neq \emptyset$ and hence, it has a minimal element, say L.

Then, $L \in \Sigma$ and $LI \neq 0$. Clearly $L \neq 0$.

Pick $a \in L \setminus \{0\}$ s.t. $(a)I \neq 0$. $\therefore (a) \in \Sigma$.

Moreover, $(a) \subseteq L$. By minimality, $L = (a)$.

Also,

$$0 \neq (a)I = (a)I^2 = (aI)I$$

Thus, $(aI) \subset (a) = L$ and $(aI) \in \Sigma$.

Again, $\boxed{(a)I = (a) = L.}$

Also, $I = N^n \subseteq N = J(R)$.

By Nakayama, $I(a) = (a) \Rightarrow (a) = 0$. $\rightarrow\leftarrow$

(a) is f.g.!

Thus, $N^n = I = 0$, as desired. ☒

Artinian Modules

Examples Fix a prime p.

$0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$ is an exact sequence of $\mathbb{Z}$-modules.

Localise the above at $S = \{1, p, p^2, \ldots\}$.

$\mathbb{Z} \subseteq S^{-1}\mathbb{Z} = \mathbb{Z}[\frac{1}{p}] = \mathbb{Z}$-algebra generated by $\frac{1}{p}$

$$= \left\{ \frac{n}{p^t} : n \in \mathbb{Z}, \ t \geq 0 \right\} \subseteq \mathbb{Q}.$$

$$0 \to \mathbb{Z} \to \mathbb{Z}[\tfrac{1}{p}] \to \frac{\mathbb{Z}[\frac{1}{p}]}{\mathbb{Z}} \to 0$$

$\dfrac{\mathbb{Z}[\frac{1}{p}]}{\mathbb{Z}}$ is a ($\mathbb{Z}$-algebra and a) $\mathbb{Z}$-module.

$$= E(p) = \left\{ \frac{r}{p^n} + \mathbb{Z} : \underset{n \geq 0}{(r,p) = 1}, \ r \in \mathbb{Z} \right\}$$

Fix some $n \geq 1$. Consider $x = \left[\frac{1}{p^n}\right]$.

$$\mathbb{Z} \xrightarrow[\mu_x]{} \mathbb{Z}x \subseteq E[p]$$

$$\ker \mu_x = \left\{ m \in \mathbb{Z} : mx = \left[\tfrac{0}{1}\right] \right\}$$
$$= \{ m \in \mathbb{Z} : p^n \mid m \}$$
$$= p^n \mathbb{Z}$$

$\therefore \dfrac{\mathbb{Z}}{p^n\mathbb{Z}} \simeq \mathbb{Z}x \subseteq E(p)$

cyclic group of order p^n

$\therefore E(p)$ contains cyclic groups of order p^n; $n = 1, 2, \ldots$

Call these groups $G_1, G_2, \ldots$

$$G_1 \subsetneq G_2 \subsetneq G_3 \subsetneq \cdots$$

(strict because $p^n < p^{n+1}$ $\forall n$.)

$$\left[\frac{1}{p^n}\right] = p \cdot \left[\frac{1}{p^{n+1}}\right] \in G_{n+1}.$$

$\therefore E(p)$ is not a Noetherian $\mathbb{Z}$-module.

$$E(p) = \frac{\mathbb{Z}[\frac{1}{p}]}{\mathbb{Z}}$$

Thus, $\mathbb{Z}[\frac{1}{p}]$ is also not a Noetherian $\mathbb{Z}$-module.

Claim. $E(p) = \frac{\mathbb{Z}[1/p]}{\mathbb{Z}}$ is an Artinian $\mathbb{Z}$-module

Lecture 8 (05-02-2021)

05 February 2021 13:59

We show that any proper $\mathbb{Z}$-submodule of $E(p)$ is of the form $G_t = \left\langle \left[\frac{1}{p^t}\right] \right\rangle$ for some t.

Since G_t is finite, we would have shown that $E(p)$ is Artinian.

Proof. Assume $0 \subsetneq H \subsetneq E(p)$.

$\exists \underset{\neq 0}{\frac{r}{p^t} + \mathbb{Z}} \in H$ with $(r, p^t) = 1$.

$\exists a, b \in \mathbb{Z}$ s.t. $ar + bp^t = 1$

$$\Rightarrow \frac{ar}{p^t} - \frac{1}{p^t} = b \in \mathbb{Z}.$$

$$\therefore \left[\frac{ar}{p^t}\right] = \left[\frac{1}{p^t}\right]$$

$\therefore H \supseteq G_t$

Moreover, the argument shows $E(p) = \bigcup_{t=0}^{\infty} G_t$.

Now, since $H \neq E(p)$, $\exists t$ s.t. $G_{t+1} \not\subset H$.

Pick the smallest such t.

Thus, $G_0 \subset G_1 \subset \cdots \subset G_t \subset H \not\supset G_{t+1}$.

Claim. $G_t = H$.

Proof. $(\subseteq)$ is by def^n.

$(\supseteq)$ Suppose not. Pick $\left[\frac{r}{p^x}\right] \in H \setminus G_t$ with $(r, p^x) = 1$.

$\Rightarrow \left[\frac{1}{p^x}\right] \in H$ (same argument as earlier)

(else $\left[\frac{r}{p^x}\right] \subseteq G_t$)

$\left\lfloor p^x \right\rfloor$

(but $x \geq t+1$) $\quad \left(\text{else } \left[\frac{r}{p^x}\right] \subseteq G_t \right)$

$\Rightarrow \left[\frac{1}{p^{t+1}}\right] \subseteq H$

$\Rightarrow G_{t+1} \subseteq H \qquad \rightarrow\leftarrow$

Thus, $E(p)$ is an Artinian $\mathbb{Z}$-module which is not Noetherian.

Q. When is V a Noetherian $\mathbb{k}$-module?

Ans. Precisely when V has finite dim.

If not finite, $\exists \{x_1, x_2, \ldots\} \subseteq V$ L.I.

Then, $\langle x_1 \rangle \subsetneq \langle x_1, x_2 \rangle \subsetneq \cdots$. $\therefore$ Not Noetherian.

If V finite, then increasing chain $\Rightarrow$ increasing dimension.

Same answer for "Artinian" instead of "Noetherian".

Some more basic properties of Artinian modules:

(1) $N \subset M$ R-modules.

$$0 \longrightarrow N \xhookrightarrow{i} M \xrightarrow{\pi} M/N \longrightarrow 0.$$

Then, M is Artinian $\Leftrightarrow$ N and M/N are Artinian.

The proof is identical as to what we did for Noetherian.

(2) $0 \rightarrow N \rightarrow M \rightarrow L \rightarrow 0$ exact.

M is Art $\Leftrightarrow$ N and L are Art.

(3) Let $M_1, \ldots, M_n$ be R-modules.

Then, $\bigoplus_{i=1}^{n} M_i$ is Artinian $\Leftrightarrow$ $M_1, \ldots, M_n$ are Artinian.

For $n \geq 2$, note $0 \to \bigoplus_{i=1}^{n-1} M_i \to \bigoplus_{i=1}^{n} M_i \to M_n \to 0$

is exact. Use induction.

$\Rightarrow \bigoplus_{i=1}^{n} R$ is Artinian (as an R-mod) if R is an Artinian ring

free module of rank n.

$\prod_{i=1}^{\infty} \mathbb{Z}/2\mathbb{Z}$ is not Artinian $\mathbb{Z}$-module although $\mathbb{Z}/2\mathbb{Z}$ is an Artinian $\mathbb{Z}$-module.

Prop^n. Let M be a f.g. R module, where R is Artinian. Then, M is also Artinian.

Proof. Let $M = \langle x_1, \ldots, x_n \rangle$.

Define $\varphi: \bigoplus_{i=1}^{n} R \twoheadrightarrow M$ by $e_i \mapsto x_i$.

Then, $0 \to \ker \varphi \to \bigoplus R \to M \to 0$ is exact. ∎

Art $\therefore$ this is Art.

Note. As opposed to Noetherian modules, Artinian modules need not be f.g. (Recall $E(p) = \mathbb{Z}[1/p]/\mathbb{Z}$.)

Prop^n. Let M be a f.g. Artinian module. Then, $R/\operatorname{ann} M$ is also Artinian.

Proof. $M = Rm_1 + \cdots + Rm_t$ for $m_1, \ldots, m_t \in M$.

Define $\varphi: R \to M \oplus \cdots \oplus M$ by

$r \mapsto (rm_1, \ldots, rm_t)$.

Then, φ is R-linear with $\ker \varphi = \operatorname{ann} M$.

$$\therefore \quad \frac{R}{\operatorname{ann} M} \hookrightarrow \underbrace{M \oplus \cdots \oplus M}_{\text{Artinian}}$$

$\therefore$ $R/\operatorname{ann} M$ also Artinian

Thus, $R/\operatorname{ann} M$ is Artinian as an $\underline{\underline{R\text{-module}}}$.

The action of R on $R/\operatorname{ann} M$ factors through $R/\operatorname{ann} M$ and hence, $R/\operatorname{ann} M$ is an Artinian ring as well. ∎

Lemma. Let M be an R-module and $\mathfrak{m}_1, \ldots, \mathfrak{m}_n \subseteq R$ are maximal ideals such that $\mathfrak{m}_1 \cdots \mathfrak{m}_n M = 0$.
(That is, $\mathfrak{m}_1 \cdots \mathfrak{m}_n \subseteq \operatorname{ann} M$.)
Then, M is Noetherian $\Leftrightarrow$ M is Artinian.

Proof. Induction on n.

$n = 1$: $\mathfrak{m}_1 = \mathfrak{m}$. $\mathfrak{m} M = 0$.

Basic principle : If M is an R-module and $I \subseteq \operatorname{ann} M$, then M is R/I-module.

$M \simeq M/\mathfrak{m}M$ is an $R/\mathfrak{m}$-vector space.

Thus, M is Noetherian as $R/\mathfrak{m}$ module
$\Leftrightarrow$ M is fin. dim over $R/\mathfrak{m}$
$\Leftrightarrow$ M is Artinian as $R/\mathfrak{m}$ module

But the structure of M as R or $R/\mathfrak{m}$ module is the "same". Thus, $\Leftrightarrow$ is true for R-modules.

Assume true for $n-1$.

$$0 \longrightarrow \underbrace{\mathfrak{m}_n M}_{\text{killed by } \mathfrak{m}_1 \cdots \mathfrak{m}_{n-1}} \longrightarrow M \longrightarrow \underbrace{M/\mathfrak{m}_n M}_{\text{killed by } \mathfrak{m}_n} \longrightarrow 0$$

$\underbrace{\mathfrak{m}_n \cdots}$ killed by $\mathfrak{m}_1 \cdots \mathfrak{m}_{n-1}$
by induction: Noe $\Leftrightarrow$ Art

$\underbrace{/\mathfrak{m}_n M}$ killed by $\mathfrak{m}_n$
$\therefore$ v-space over $R/\mathfrak{m}_n$
$\therefore$ Noe $\Leftrightarrow$ Art

M Noe $\Leftrightarrow$ $\mathfrak{m}_n M$ & $M/\mathfrak{m}_n M$ are Noe

$\Updownarrow$

M Art $\Leftrightarrow$ $\mathfrak{m}_n M$ & $M/\mathfrak{m}_n M$ are Art

---

Thm. Let R be an Artinian ring. Then, R is Noetherian.

Proof. R Artinian $\Rightarrow$ $\operatorname{Spec} R = \operatorname{mSpec} R$ has only finitely many ideals
$$\operatorname{Spec} R = \{\mathfrak{m}_1, \dots, \mathfrak{m}_n\}$$

Then, $\mathcal{N}(R) = \mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_n$ is nilpotent.
$$\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_n = \mathfrak{m}_1 \cdots \mathfrak{m}_n \quad \text{pairwise comaximal}$$

$\exists r \in (\mathfrak{m}_1 \cdots \mathfrak{m}_n)^k \subseteq \mathfrak{m}_1 \cdots \mathfrak{m}_n$ s.t. $r \cdot 1 = 0$

$\therefore$ $\exists k$ s.t. $(\mathfrak{m}_1 \cdots \mathfrak{m}_n)^k = 0$.

$\therefore$ $\mathfrak{m}_1 \cdots \mathfrak{m}_n M = 0$ is satisfied by $M = R$.

R is Art $\Rightarrow$ R is Noetherian, by above. ∎

Thm. Let R be an Artinian ring.
Then, $\exists$ uniquely determined Artinian local rings $R_1, \dots, R_n$ s.t.
$$R \simeq R_1 \times \cdots \times R_n.$$

Proof. Let $\mathfrak{m}_1, \dots, \mathfrak{m}_n$ be the (finitely many) distinct maximal ideals.
Then, $\forall t \gg 0$,

$$\mathfrak{m}_1^t \, \mathfrak{m}_2^t \cdots \mathfrak{m}_n^t = 0.$$

But $\mathfrak{m}_1^t, \ldots, \mathfrak{m}_n^t$ are p-wise comaximal. Thus,

$$\mathfrak{m}_1^t \cap \cdots \cap \mathfrak{m}_n^t = \mathfrak{m}_1^t \cdots \mathfrak{m}_n^t = 0$$

Note that $R/\mathfrak{m}_i^t$ is local and Artinian.

↳ unique maximal $\mathfrak{m}_i/\mathfrak{m}_i^t$

By CRT, $R \xrightarrow{\sim} R/\mathfrak{m}_1^t \times \cdots \times R/\mathfrak{m}_n^t$.

$\therefore$ R Artinian $\Rightarrow$ R is a direct product of <u>some</u> Artinian local rings.

Lecture 9 (09-02-2021)

09 February 2021 14:00

Had shown: If R is Artinian, then $R \simeq \prod_{i=1}^{n} R_i$ where R_i are Artinian local rings.

(Recall Proof.) · $\operatorname{Spec} R = \operatorname{mSpec} R$ ← finite
$= \{m_1, \dots, m_n\}$

· $\operatorname{Jac}(R) = \mathcal{N}(R) = m_1 \cap \dots \cap m_n = \prod_{i=1}^{n} m_i$ ← nilpotent

· $\exists\, k \geq 1$ $N^k = 0$

$\therefore$ $m_1^k \cap \dots \cap m_n^k = \prod_{i=1}^{n} m_i^k = 0$ and

$$R \xrightarrow{\varphi} R/m_1^k \times \dots \times R/m_n^k$$

φ is an isomorphism, by Chinese Remainder Theorem ∎

Conversely, let $R \simeq R_1 \times \dots \times R_n$ where $R_1, R_2, \dots, R_n$ are Artinian local rings ($R_i \neq 0$ $\forall i$)

TST. R is Artinian and $\{R_1, \dots, R_n\}$ is uniquely determined set of local rings.

Proof. WLOG, $R = R_1 \times \dots \times R_n$.

Consider $\pi_i : R \longrightarrow R_i$, $(a_1, \dots, a_n) \mapsto a_i$.

$I_i := \ker \pi_i = R_1 \times \dots \times R_{i-1} \times 0 \times R_{i+1} \times \dots \times R_n$ and

$R_i = R/I_i$.

$I_i + I_j = R$ if $i \neq j$ and $(0) = I_1 \cap \dots \cap I_n$.

R_i is Artinian local. Lift the maximal ideal to get m_i.
$\simeq R/I_i$ (That is $\operatorname{Spec}(R/I_i) = \{m_i/I_i\}$. (Primes are maximal : Artin.))

$\cong R/I_i$ (That is $\mathrm{Spec}(R/I_i) = \{m_i/I_i\}$. (Primes are maximal Artin.))

$\Rightarrow \sqrt{I_i} = m_i$ (I_i is m_i-primary)

Thus, $0 = I_1 \cap \cdots \cap I_n$ is a primary decomposition of (0) in R. Moreover, $m_1, \ldots, m_n$ are the minimal primes of 0. (*) $\therefore$ I_is are uniquely determined. ($\to$ distinct $\{I_i\}$ because co-maximal pairwise)

$\therefore R/I_i$s are uniquely determined.

(*) Note that $0 = I_1 \cap \cdots \cap I_n = I_1 \cdots I_n$

Thus, if $0 \subseteq p \subseteq m_1$, then $I_i \subset p$ for some i.

But $\sqrt{I_i} = m_i$ and thus, $m_i \subset p$.

Thus, $p = m_i$ and $m_i = m_1$.

Thus, $i=1$. $\therefore m_1$ is minimal. (Similar for rest.)

$R_i \cong R/I_i$ Artinian ring

$\therefore R_i$ is Artinian R-module

$\Rightarrow \prod R_i = R$ is Artinian R-module

$\Rightarrow R$ is Artinian ring.

Modules which are both Artinian and Noetherian

Examples (1) Fin. dim. v. spaces over fields.

(2) Rings which are Artinian.

(3) Direct sum of modules which are both.

(4) If $m_1, \ldots, m_n$ are maximal ideals and

$$m_1 \cdots m_n M = 0.$$

Then, M is Noe $\Leftrightarrow M$ is Art.

Q. R is Artinian and M is Artinian R-module. Is M Noetherian R-module?

A. Yes!

Proof Let $\{m_1, \dots, m_n\} = \operatorname{Spec} R = \operatorname{mSpec} R$.

Note $\exists k \geq 1$ $m_1^k \cdots m_n^k = 0$

$$\Rightarrow \underbrace{m_1^k \cdots m_n^k}_{\text{product of maximal ideals}} M = 0$$

$\therefore$ M is Art $\iff$ M is Noe.

↳ we know this!

Thus, if R is Artinian and M an R-module, TFAE:

(i) M is Artinian

(ii) M is Noetherian

(iii) M is f.g.

Defn. (Simple) $R \to$ commutative ring

An R-module M is called simple if $M \neq 0$ and the only submodules of M are 0 and M.

Example (1) Field $\mathbb{k}$ is a simple $\mathbb{k}$-module.

(2) 1-dim v. space over a field.

Let M be a simple R-module, $M \neq 0$.

$\exists\, m \in M \setminus \{0\}$. Then $Rm = M$.

$$\varphi : R \to M, \quad \varphi(r) := rm.$$

$$\ker \varphi = I, \qquad M \simeq R/I \quad \text{as } R\text{-module}.$$

Then, I has to be maximal, else M won't be simple.

(If $I \subsetneq J \subsetneq R$, then J/I is (isomorphic to) a non-zero proper submodule of M.)

$\therefore$ $\{\text{Simple } R\text{-modules}\} \underset{\text{up to isomorphism classes}}{\approx} \{R/m : m \in \operatorname{mSpec}(R)\}$

Let M be a f.g. module over an Artinian ring R.
$\therefore$ M is Noe. and Art.

Suppose $M^{\neq 0}$ is not simple.
Then, $\exists$ maximal submodule $M_1^{\neq 0}$ among proper submodules.
Thus, $\underbrace{M_1 \subsetneq M}_{\text{nothing in between}}$.

Thus, M/M_1 is simple.

Similarly, we can continue as long as we don't get 0:

$$\cdots \subsetneq M_2 \subsetneq M_1 \subsetneq M$$

$\left(M_i/M_{i+1} \text{ simple} \right)$

By Artinian-ness, it must terminate. Moreover, termination at 0. That is:

$$(0) = M_n \subsetneq M_{n-1} \subsetneq \cdots \subsetneq M_1 \subsetneq M_0 = M$$

$$\frac{M_{n-1}}{M_n} \simeq R/\mathfrak{m}_{n-1}, \dots, \frac{M_0}{M_1} \simeq R/\mathfrak{m}_0$$

Composition series (Composition series)

The length of the above series is $\underline{\underline{n}}$.

If V is n-dim $\mathbb{k}$ vec. space and $\mathcal{B} = \{x_1, \dots, x_n\}$ is a basis, define $V_i = \langle x_1, \dots, x_i \rangle$ and then,

$$(0) \subset V_1 \subset V_2 \subset \cdots \subset V_n = V \text{ is a composition series.}$$

$\left(\dim\left(\frac{V_i}{V_{i-1}}\right) = 1 \text{ and hence, } V_i/V_{i-1} \text{ is simple.} \right)$

Note that all comp. series of V have same length. We prove the same for modules.

Example. ① $\mathbb{Z}/6\mathbb{Z} \rightarrow$ Artinian ring

$\mathrm{Spec}(\mathbb{Z}/6\mathbb{Z}) = \{ (2)/(6),\ (3)/(6) \}$.

$$(0) \subseteq \frac{2\mathbb{Z}}{6\mathbb{Z}} \subseteq \frac{\mathbb{Z}}{6\mathbb{Z}}$$

$$(0) \subseteq \frac{3\mathbb{Z}}{6\mathbb{Z}} \subseteq \frac{\mathbb{Z}}{6\mathbb{Z}}$$

both are composition series!

$$\frac{\mathbb{Z}/6\mathbb{Z}}{3\mathbb{Z}/6\mathbb{Z}} \qquad \frac{\mathbb{Z}/6\mathbb{Z}}{2\mathbb{Z}/6\mathbb{Z}}$$

$\leftarrow$ same quotients appear above, in diff order

② Let $p > 0$ be prime. $\underbrace{\mathbb{Z}/p^4\mathbb{Z}}_{=R} \leftarrow$ Artinian

$$0 = \frac{p^4\mathbb{Z}}{p^4\mathbb{Z}} \subseteq \frac{p^3\mathbb{Z}}{p^4\mathbb{Z}} \subseteq \frac{p^2\mathbb{Z}}{p^4\mathbb{Z}} \subseteq \frac{p\mathbb{Z}}{p^4\mathbb{Z}} \subset \frac{\mathbb{Z}}{p^4\mathbb{Z}} = R$$

All quotients are $\dfrac{\mathbb{Z}/p^4\mathbb{Z}}{p\mathbb{Z}/p^4\mathbb{Z}}$.

Thm. $R \to$ any comm ring. $M \to$ R-module

M is Noetherian and Artinian $\Leftrightarrow$ M has a comp. series.

Proof. ($\Rightarrow$) done earlier. (We did not use R Artin there.)

($\Leftarrow$) Let $(0) \subset M_1 \subset \cdots \subset M_n = M$ be a composition series.

- $n = 1$. Then, M is simple. Thus, it is Artinian and Noe. both.

Induct on n. Suppose $n \geq 2$. We have

By induction, $M_1, \ldots, M_{n-1}$ are both Noe. & Art.

Go both M_1:

$$\frac{M_1}{M_1} \subset \underbrace{\frac{M_2}{M_1}}_{\text{simple}} \subset \underbrace{\frac{M_3}{M_1}}_{\text{simple}} \subset \cdots \subset \frac{M_{n-1}}{M_1} \subset \underbrace{\frac{M_n}{M_1}}_{\text{simple}}$$

$$\underbrace{\overbrace{M_1 \quad \overline{M_1} \quad M_1}^{}}_{}$$ simple, simple, ..., simple

length $n-1$

$\therefore$ M_n/M_1 is both Noe and Art.

But

$$0 \to M_1 \to M_n \to M_n/M_1 \to 0$$ is

exact.

both

$\therefore$ M_n is both. $\blacksquare$

Def^n Let $M^{\neq 0}$ be an R-module.

Define $\ell_R(M) = \min\{n \mid M \text{ has a composition of length } n\}$.

$(\min \phi = \infty.)$

This is called the *length* of the module M over R.

(Length of a module)

Prop^n Let $M^{\neq 0}$ have a composition series.

Suppose $0 \lneq N \lneq M$. Then,

$$\ell(N) < \ell(M).$$

(M comp series $\Rightarrow$ M both Noe & Art $\Downarrow$ N has a c.s. $\Leftarrow$ N both Noe & Art)

Proof. Let us take a minimal composition series of M.

$$(0) \subset M_1 \subset M_2 \subset \cdots \subset M_{n-1} \subset M_n = M$$

Then,

$$(0) \subseteq \overset{N_1}{\overset{\shortparallel}{M_1 \cap N}} \subset \overset{N_2}{\overset{\shortparallel}{M_2 \cap N}} \subset \cdots \subset \overset{N_{n-1}}{\overset{\shortparallel}{M_{n-1} \cap N}} \subset \overset{N_n}{\overset{\shortparallel}{M_n \cap N}} = N$$

We now look at the quotients.

$$M_2 \cap N \xrightarrow{\iota} M_2 \xrightarrow{\pi} M_2/M_1.$$

$$\ker(\pi \circ \iota) = M_1 \cap N.$$

$$\therefore \quad \frac{M_2 \cap N}{M_1 \cap N} \hookrightarrow \frac{M_2}{M_1} \to \text{simple}$$

$$\therefore \frac{M_2 \cap N}{M_1 \cap N} = 0 \quad \text{or} \quad \text{simple}$$

$$\therefore \quad \frac{M_2 \cap N}{M_1 \cap N} = 0 \quad \text{or} \quad \text{simple}$$

$$M_1 \cap N = M_2 \cap N \qquad\qquad M_1 \cap N \subsetneq M_2 \cap N$$

Similarly, we see that

$$0 \subseteq N_1 \subseteq \cdots \subseteq N_{n-1} \subseteq N_n = N$$ with each quotient either 0 or simple.

→ inclusion is equality

Case 1. At least one quotient is zero.

Then, we can remove the duplicates and get a strictly smaller c.s.

Case 2. $N_i \neq N_{i+1} \quad \forall i$.

$$0 \subsetneq M_1 \subsetneq M_2 \subsetneq \cdots \subsetneq M_{n-1} \subsetneq M_n = M$$

$$0 \subsetneq N_1 = N \cap M_1 \subsetneq \cdots \subsetneq N_{n-1} = M_{n-1} \cap N \subsetneq N_n = N$$

$$0 \subsetneq N_1 \subseteq M_1 \Rightarrow N_1 = M_1.$$

$$0 \subsetneq \frac{N_2}{N_1} \hookrightarrow \frac{M_2}{M_1} \Rightarrow \frac{N_2}{N_1} = \frac{M_2}{M_1} \quad \text{but} \quad N_1 = M_1.$$

$$\therefore N_2 = M_2.$$

Inductively, $\underset{N}{\overset{}{\underset{\shortparallel}{N_n}}} = M$. $\rightarrow\leftarrow$

Thus, $N_i = N_{i+1}$ for some i and hence, $l_R(N) < l_R(M)$. ∎

Lecture 10 (12-02-2021)

12 February 2021 14:00

$M \to$ Art and Noe $\to$ has c.s.

$$0 = M_0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_n = M.$$

$$M_i/M_{i-1} \simeq R/\mathfrak{m}_i \quad \text{for } \mathfrak{m}_i \in \operatorname{mSpec} R.$$

$\therefore$ $\operatorname{Ass} M \subseteq \{\mathfrak{m}_1, \ldots, \mathfrak{m}_n\} \subseteq \operatorname{supp} M.$

$\ell(M) = \min\{n : M \text{ has a c.s. of length } n\}.$

Had shown: If $N \subsetneq M$, then $\ell(N) < \ell(M)$.

Prop^n. Any two composition series of a finite length module have equal length.

Proof. Suppose $0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_k \subseteq M$ such that each quotient is simple. Let $n := \ell(M)$.

Then, $0 < \ell(M_1) < \cdots < \ell(M_k) \le n.$

Thus, $k \le n$.

Now, if $0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_k = M$ is a c.s., then

$n = \min\{\text{lengths of c.s.}\} \le k.$

$\therefore$ $n = k$.

That is, any c.s. has length n. ∎

Prop^n Now, suppose we have a chain

$0 = N_0 \subsetneq N_1 \subsetneq N_2 \subsetneq \cdots \subsetneq N_n = M$. Then, it must be a c.s., i.e., $\frac{N_i}{N_{i-1}}$ must be simple.

Proof. If $\frac{N_i}{N_{i-1}}$ is not simple for some i, then we can insert a module in between. This contradicts the $k \leq n$ inequality of earlier.

Prop^n. Suppose $0 \to N \to M \to L \to 0$ is exact sequence of finite length R-modules. Then, $\ell(M) = \ell(N) + \ell(L)$.

Proof. We may assume $N \subset M$ and $L = M/N$.
Let $0 \subset N_1 \subseteq \cdots \subset N_n = N$ be a composition series of N. Let $0 \subset \frac{M_1}{N} \subset \cdots \subset \frac{M_\ell}{N} = M/N$ be

a composition series of $L = M/N$.
Lift it back in M to get
$$N = M_0 \subset M_1 \subset \cdots \subset M_\ell = M.$$

Putting together the two series, we get:
$$0 \subset N_1 \subset \cdots \subset N_N = M_0 \subset M_1 \subset \cdots \subset M_\ell = M.$$
Note that $\frac{M_i}{M_{i-1}} \simeq \frac{M_i/N}{M_{i-1}/N}$ is simple.

All the quotients are simple and thus, it is a c.s. for M giving
$$\ell(M) = n + \ell = \ell(N) + \ell(L).$$ ☒

Lecture 11 (16-02-2021)

16 February 2021 14:01

Chapter 4: Integral Extension of Rings

Algebraic extensions of fields

$$\begin{array}{c} L \\ | \\ K \end{array}$$

$x \in L$ is called algebraic if it satisfies an equation of the form

$$x^n + a_1 x^{n-1} + \cdots + a_n = 0$$

where $a_1, \ldots, a_n \in K$.

Def^n. Let $R \subset S$ be commutative rings with $1 \neq 0$. $s \in S$ is called integral over R if there exists a monic polynomial $f(x) \in R[x]$ s.t. $f(s) = 0$.

Let $T = \{ s \in S \mid s \text{ is integral over } R \}$.

Note

↳ $x - r$

Thm. T is a subring of S. That is, it is closed under addition, inverses and multiplication.

Def^n. We say that T is the integral closure of R in S. In case R is a domain and S = field of fracs, then T is called the normalisation of R. R is called normal or integrally closed if $T = R$.

(integral closure, normalisation, normal, integrally closed)

(1) → look at elements integral over R

$$\begin{array}{c} | \text{ alg.} \\ K = \text{frac. field of } R \end{array}$$

e.g.

$$\begin{array}{c} L \\ | \text{ Galois} \\ \mathbb{Q} \\ | \end{array}$$

$$\begin{array}{c} \mid \text{alg.} \\ K = \text{frac. field of } R \\ \mid \\ R \end{array} \qquad \text{e.g.} \quad \begin{array}{c} \mathbb{Q} \\ \mid \\ \mathbb{Z} \end{array}$$

The integral closure, denoted $\mathcal{O}_L$ is called the ring of integers.

Thm. If R is a UFD, then R is integrally closed (normal domain).
(E.g., $\mathbb{Z}$, $k[x_1, \dots, x_n]$.)

Proof. Let $K = \left\{ \frac{a}{b} \mid a, b \in R, \ b \neq 0 \right\}$.

Let $\frac{a}{b} \in K$ be integral over R.

We show that $\frac{a}{b} \in R$.

WLOG, $\gcd(a, b) = 1$.
no common primes in factorisation

Since it is integral, $\exists r_1, \dots, r_n \in R$ s.t.

$$\left(\frac{a}{b}\right)^n + r_1 \left(\frac{a}{b}\right)^{n-1} + \dots + r_n = 0.$$

Multiply with b^n to get

$a^n = -b(\dots)$ and thus, every prime fac. of b is of a as well. Thus, b is a unit and hence, $\frac{a}{b} \in R$. $\blacksquare$

Example of non-normal: Let $R = \dfrac{k[x, y]}{(y^2 - x^3)}$

Ex. $y^2 - x^3$ is irreducible. $\therefore (y^2 - x^3)$ is a prime ideal.

Thus, R is an integral domain.
Define $\varphi : k[x, y] \longrightarrow k[t]$
$x \longmapsto t^2$

$$Y \mapsto t^3$$
$$\varphi|_{\mathbb{k}} = id$$

Then, $\ker\varphi \supseteq (Y^2 - X^3)$. In fact $\ker\varphi = (Y^2 - X^3)$.

$$\therefore \frac{\mathbb{k}[X,Y]}{(Y^2-X^3)} \simeq im\,\varphi = \mathbb{k}[t^2, t^3]$$

↳ subring of $\mathbb{k}[t]$ generated by t^2 and t^3

$$\begin{array}{c} \mathbb{k}[t] \ni t \text{ is integral over } \mathbb{k}[t^2, t^3] \\ | \\ R \simeq \mathbb{k}[t^2, t^3] \end{array}$$

$$R = \frac{\mathbb{k}[X,Y]}{(X^3 - Y^2)}.$$

Let $x = X + (X^3 - Y^2)$, $y = Y + (X^3 - Y^2) \in R$.

$x^3 = y^2$ in R and hence,

$x = \left(\frac{y}{x}\right)^2 \in Q(R) \to$ quotient field of R.

Thus, $\frac{y}{x} \in Q(R) \setminus R$ and is integral. (satisfies $z^2 - x \in R[z]$)

Later, we see that

$$\begin{array}{c} Q(R) \\ | \\ \mathbb{k}[x, y, \frac{y}{x}] = \text{integral closure of } R \text{ in } Q(R) \\ | \\ \mathbb{k} \end{array}$$

Cayley-Hamilton Theorem

$T: V \to V$, $\dim V = n$, V is a $\mathbb{k}$-vector space.

$\det(xI_n - T) = \chi_T(x)$.

Then, $\chi_T(T): V \to V$ is the zero-map.

How to generalise to modules?

(Cayley-Hamilton theorem for modules)

Thm. Let R be a commutative ring.

I an R-ideal and M a f.g. R module.
Let $\varphi: M \to M$ be an R-endomorphism such that
$$\varphi(M) \subset IM.$$

Then, $\exists$ a monic polynomial $f(x) \in R[x]$ s.t.
$$f(x) = x^n + a_1 x^{n-1} + \cdots + a_n$$
with $a_1, \ldots, a_n \in I$
and $f(\varphi) = 0$.

Proof. M is an R-module, $\varphi: M \to M$ is an endomorphism.
M can be thought of as an $R[X]$-module with

$$X \cdot m = \varphi(m) \quad \text{extended as}$$
$$(r_0 + r_1 X + \cdots + r_n X^n) m = r_0 \cdot m + r_1 \cdot \varphi(m) + \cdots + r_n \varphi^n(m).$$

(Can check that is actually defines an $R[X]$-module.)

Write $M = Rm_1 + \cdots + Rm_n$ with $m_1, \ldots, m_n \in M$.
$\varphi(M) \subset IM$ and thus,
$$X \cdot m_1 = \varphi(m_1) = a_{11} m_1 + \cdots + a_{1n} m_n, \quad a_{1i} \in I \ \forall i$$
$$\vdots$$
$$X \cdot m_n = \varphi(m_n) = a_{n1} m_1 + \cdots + a_{nn} m_n, \quad a_{ni} \in I \ \forall i.$$

Thus,
$$(X - a_{11}) m_1 - a_{12} m_2 - \cdots - a_{1n} m_n = 0$$
$$-a_{21} m_1 + (X - a_{22}) m_2 - \cdots - a_{2n} m_n = 0$$
$$\vdots$$
$$-a_{n1} m_1 - a_{n2} m_2 - \cdots + (X - a_{nn}) m_n = 0$$

The above are n linear equations in $m_1, \ldots, m_n$ with co-efficients in $R[X]$. In matrix form:

$$(X I_n - A) \begin{bmatrix} m_1 \\ \vdots \end{bmatrix} = 0 \quad \text{with} \quad A = (a_{ij}).$$

$$(XI_n - A)\begin{bmatrix} m_1 \\ \vdots \\ m_n \end{bmatrix} = 0 \qquad \text{with} \qquad A = (a_{ij}).$$

Multiplying with adjoint:

$$\det(XI_n - A)\cdot I_n \begin{bmatrix} m_1 \\ \vdots \\ m_n \end{bmatrix} = 0 \Rightarrow \det(xI_n - A)\, m_i = 0 \ \forall i.$$

$$\rightarrow \quad \det(XI_n - A) \in \operatorname{ann}_{R[x]} M.$$

Note that $\det(XI_n - A) = X^n + a_1 X^{n-1} + \cdots + a_n$
for $a_1, \dots, a_n \in I$.

By our definition of $R[x]$-module, substituting $X = \varphi$ above shows that
$\varphi^n + a_1\varphi^{n-1} + \cdots + a_n$ is the zero endomorphism. ∎

Cor. (Nakayama lemma) Suppose $M = IM$. (M is f.g. over R.)
Then, $\exists\, a \in I$ s.t. $(1+a)M = 0$. If $a \in J(R)$, then $M = 0$.

Proof. Consider $\varphi = \mathrm{id}_M : M \rightarrow M$. This is an endomorphism. Let I be as given.
Then, $\varphi(M) = M = IM \subset IM$. Thus, CH applies and

$$\varphi^n + a_1\varphi^{n-1} + \cdots + a_n\varphi^0 = 0 \quad \text{for } a_1, \dots, a_n \in R.$$

Note that $\varphi^0 = \cdots = \varphi^n = \mathrm{id}$.

$$\therefore \quad 1 + \underbrace{(a_1 + \cdots + a_n)}_{=: a \,\in I} \in \operatorname{ann}_R(M)$$

In particular, if $I \subset J(R)$, then $1 + a$ is a unit. ∎

Cor. Let $\varphi : M \to M$ be a surjective endomorphism. (M is a f.g. R-module)
Then, φ is an isomorphism.

Proof. M is an $R[x]$-module via φ.
Then, φ is also an $R[x]$-endomorphism of M. Then, take
$I = (x) \subseteq R[x]$.

We have $M = \varphi(M) = (x) M$.

By NAK, $\exists a \in (x)$ s.t.

$$(1+a) M = 0.$$

Thus, $$(1 + x f(x)) M = 0.$$

We now show $\varphi : M \to M$ is injective.

Let $\varphi(m) = 0$. Then, $(1 + x f(x)) m = 0$

$$\underset{\displaystyle m + \varphi f(\varphi)(m) = m + 0}{\overset{\|}{(1+xf(x))\,m}}$$

Thus, $m = 0$. ∎

A free R module is of the form $\bigoplus_{i \in \Lambda} R$.

Finite rank : $\bigoplus_{i=1}^{n} R$. $n \to$ rank of this free module

$R^n \simeq R^m \iff m = n$ $\leftarrow$ Thus, rank is well-defined (Not true if R non-comm.)

Another consequence of CH.

Recall. Linear independence of $m_1, \dots, m_n \in M$ over R:

$$a_1 m_1 + \cdots + a_n m_n = 0 \iff a_i = 0 \ \forall i$$

Thm $M \simeq R^n$, then any set of n generators are linearly independent. In particular, $R^n \simeq R^m \iff n = m$

Proof. Let $M = Rm_1 + \cdots + Rm_n \simeq R^n$.

We know $M \simeq R^n$, let $\alpha : M \xrightarrow{\sim} R^n$.

Define $\beta : R^n \longrightarrow M$ by $e_i \longmapsto m_i$.

That is, $\beta(r_1, \ldots, r_n) = r_1 m_1 + \cdots + r_n m_n$.

To show $m_1, \ldots, m_n$ are R-lin. indep., it suffices to show that β is injective.

Now, note that $\beta\alpha : M \longrightarrow M$ is a surjective endomorphism.

Thus, $\beta\alpha$ is an isomorphism. Moreover,

$$\beta = (\beta\alpha)\alpha^{-1} \text{ and hence, } \beta \text{ is an iso.}$$

$\therefore$ $m_1, \ldots, m_n$ are R-linearly independent.

Now, suppose $R^n \cong R^m$ with $m < n$.

Let $\varphi : R^m \xrightarrow{\sim} R^n$.

Then, $\varphi(e_1), \ldots, \varphi(e_m)$ generate R^n.

But, so do $\varphi(e_1), \ldots, \varphi(e_m), \underbrace{0, \ldots, 0}_{n-m}$ and hence, must be R-lin indep. $\rightarrow\leftarrow$ ∎

We now prove Thm 1

$$\begin{array}{c} S \\ | \\ T \\ | \\ R \end{array} \quad T = \{ s \in S : s \text{ is integral over } R\} \text{ is a subring of } S.$$

Thm. $R \subset S$ ring extension. $s \in S$.

TFAE:

(i) s is integral over R

(ii) $R[s] = R$-alg generated by s is a f.g. R-module

(iii) $\exists$ a subring T s.t. $R \subset R[s] \subset T \subset S$ s.t.

T is a f.g. R-module.

Proof. (i) $\Rightarrow$ (ii)

$\exists\, r_1, \dots, r_n \in R$ s.t. $s^n = r_1 s^{n-1} + \dots + r_n$.

Thus, $s^{n+i} \in R\langle 1, s, \dots, s^{n-1} \rangle$ for all $i \geq 0$.

Thus, $R[s] = R + Rs + \dots + Rs^{n-1}$.

(ii) $\Rightarrow$ (iii) Take $T = R[s]$.

(iii) $\Rightarrow$ (i)

$$\begin{tikzcd} R \arrow[r, dash, bend left, "\text{finite}"] & T \arrow[r, dash] & S \\ & s \arrow[u, phantom, "\rotatebox{90}{$\in$}"] & \end{tikzcd}$$

Consider
$$\mu_s : T \longrightarrow T \quad \text{given by}$$
$$t \longmapsto ts.$$

This is an R-linear map. By CH, we have

$$\mu_s^n + b_1 \mu_s^{n-1} + \dots + b_n = 0 \quad \text{for some } b_1, \dots, b_n \in R$$

Apply the above endomorphism on $t = 1$ to get

$$s^n + b_1 s^{n-1} + \dots + b_n = 0.$$ ∎

Lecture 12 (19-02-2021)

19 February 2021 13:59

Let $R \subset S$ be a ring extension and
$$T = \{ s \in S : s \text{ is integral over } R \}.$$

We have proved (using NAK) that

s is int $/R$ $\iff^{\exists T'}$ $s \in T'$ where $R \subset T' \subset S$ and T' is a f.g. R-module

To show: If $a, b \in T$ then $a-b$, $ab \in T$. ($0 \in T$ is clear.)

Proof. Let $a, b \in T$. Then, $R \subset R[a] \subset S$.

Now, b is integral over $R[a]$ as well.
$$\underbrace{R \subset R[a]}_{\text{finite}} \subset \underbrace{R[a]}_{}\!\!\underbrace{[b]}_{\text{finite}} \subset S$$

$\therefore R[a][b]$ is a finite R-module.

Now, $a-b$, $ab \in R[a,b] = R[a][b]$.

Thus, $a-b$, $ab \in T$. ∎

$$\begin{tikzcd}
\mathbb{Q} \arrow[r, dash, "alg"] \arrow[d, dash] & K \arrow[d, dash] \\
\mathbb{Z} \arrow[r, dash] & \overline{\mathbb{Z}}^K
\end{tikzcd}$$

$$\overline{\mathbb{Z}}^K = \{ x \in K : x \text{ is int } /\mathbb{Z} \}$$
$$= \text{The ring of integers in } K$$
$$= \mathcal{O}_K$$

Thm. $\mathcal{O}_K$ is a Noetherian ring. (Will prove this later.)

Transitivity of integral extensions

Prop^n. Suppose $R \subset S \subset T$ and S/R and T/S are integral extensions. Then, T/R is also an integral extension.

Proof. Let $t \in T$. t is integral$/S$.

$\therefore \exists\, s_1, \ldots, s_n \in S$ s.t.

$$t^n + s_1 t^{n-1} + \cdots + s_n = 0.$$

$$\begin{tikzcd} T \arrow[d, dash] & \\ S \arrow[d, dash] \arrow[r, dash] & R[s_1, \ldots, s_n] = R' \\ R \arrow[ur, dash] & \end{tikzcd}$$

R' is a f.g. R-module.

Moreover, t is integral$/R'$.

Thus, $R'[t] = R[s_1, \ldots, s_n, t]$ is a f.g. R module.

$\therefore$ t is integral over R.

$\therefore$ T/R is an integral extension. ∎

Thus, if we consider

$$\begin{tikzcd} S \arrow[d, dash] \arrow[r, dash] & T = \bar{R}^S \\ R \arrow[ur, dash] & \end{tikzcd}$$

and $s \in S$ is integral over T, then s is int$/R$.

$\therefore$ $s \in T$.

In other words, T is integrally closed in S.

Behaviour of integral dependence under quotient rings and localisation

$$\begin{tikzcd} S \trianglerighteq I \arrow[r, "\pi"] & S/I \\ R \arrow[u, "i", "\text{integral}"'] \arrow[ur, dashed] & \end{tikzcd}$$

$\pi \circ i : R \to S/I$ is a ring homomorphism

$\ker \pi \circ i = I \cap R = I^c \to$ contraction of I in R.

Thus, $R/I^c \hookrightarrow S/I$ is an injection.

Identify R/I^c with its image in S/I.

Prop^n. $R/I^c \hookrightarrow S/I$ is also an integral extension. (If $R \subset S$ is.)

Proof Let $s' = s + I \in S/I$ where $s \in S$.

Then $s^n + r_1 s^{n-1} + \cdots + r_n = 0$ for $r_1, \ldots, r_n \in R$.

Going mod I gives

$$s'^n + r_1' s'^{n-1} + \cdots + r_n' = 0 \quad \text{in } S/I.$$

But $r_1' \in R/I^c$ under the identification.

Thus, S/I is integral over R/I^c. ∎

Def^n Suppose $\varphi : R \to S$ is a ring homomorphism.
Then, φ is called *integral* if $S/\varphi(R)$ is an integral extension.

Thus, we have shown that $R/I^c \hookrightarrow S/I$ is an integral homomorphism.

Localisation:

Let $U \subset R$ be a mult. closed subset and S/R be an int. ext. $U \subset S$ is also m.c.s.
$U^{-1}R \hookrightarrow U^{-1}S$ is an injection.

Prop^n $U^{-1}S / U^{-1}R$ is an integral extension.

Proof. Let $\frac{s}{u} \in U^{-1}S$.

Let $r_1, \ldots, r_n \in R$ be so that

$$s^n + r_1 s^{n-1} + \cdots + r_n = 0 \quad \text{in } S.$$

Multiply with $\left(\frac{1}{u}\right)^n$ in $U^{-1}S$:

$$\left(\frac{s}{u}\right)^n + \left(\frac{r_1}{u}\right) \cdot \left(\frac{s}{u}\right)^{n-1} + \frac{r_2}{u^2} \cdot \left(\frac{s}{u}\right)^{n-2} + \cdots + \frac{r_n}{u^n} = 0$$

in $U^{-1}S$.

But $(r_1/u), r_2/u^2, \ldots, r_n/u^n \in U^{-1}R$.

But $(r_1/u), r_2/u^2, \dots, r_n/u^n \in U^{-1}R$.

Thus, $\frac{s}{u}$ is int / $U^{-1}R$. $\boxed{}$

Prop^n. Let R be an integral domain. TFAE:

(1) R is integrally closed (normal).

(2) R_p is integrally closed $\forall p \in \operatorname{Spec} R$.

(3) R_m is integrally closed $\forall m \in \operatorname{mSpec} R$.

(Note R_p and R_m have the same field of fracs as R.)

Thus, the property of being "integrally closed" is a local property.

Proof. $0 \to R \to \bar{R} \to \bar{R}/R \to 0$ is an exact seq. of R-mods.

Localise at $p \in \operatorname{Spec} R$ to get

$$0 \to R_p \to (\bar{R})_p \to (\bar{R}/R)_p \to 0$$

integral since localisation preserves

Ex. $\left(\bar{R}^S\right)_p = \overline{R_p}^{S_p}$

$$\therefore \quad 0 \to R_p \to \overline{R_p} \to (\bar{R}/R)_p \to 0$$

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

(ii) $\Rightarrow$ (iii) obvious

(iii) $\Rightarrow$ (i) R_m is int. closed $\forall m$

TST R is int. closed

$$0 \to R \to \bar{R} \to R/R \to 0$$

$$0 \to R_m \to (\bar{R})_m \to (\bar{R}/R)_m \to 0$$

$$(\bar{R})_m = \overline{R_m}$$

...

$\overline{R_m}$

R is int closed $\iff \overline{R}/R = 0$ vanishing is local

$\iff (\overline{R}/R)_m = 0 \ \forall m$

$\iff (\overline{R})_m / R_m = 0 \quad \forall m$

this is true since R_m is assumed to be int closed $\forall m$

Thus, we are done. ☒

Chains of prime ideals in integral extensions

I.S. Cohen and A. Seidenberg (1946)

- Lying over
- Incomparability
- Going up theorem
- Going down theorem

Q. $A \xrightarrow{\varphi} B$ ring maps

$\varphi^{-1}(q) \qquad q \triangleleft B$

Induces : $\varphi^* : \operatorname{Spec} B \longrightarrow \operatorname{Spec} A$

- When is φ^* a closed map?
- When is φ^* an open map?

Can be answered using above theorems

Lemma Let $R \subset S$ be an int. ext. of domains.
Then, R is a field $\iff S$ is a field.

$\therefore \mathcal{O}_K$ cannot be a field

$\mathbb{Q} \hookrightarrow K$, $\mathbb{Z} \to \mathcal{O}_K$

Proof ($\Rightarrow$) Let R be a field.

Let $s \in S \setminus \{0\}$. We show s is invertible.

Pick $f(x) \in R[x]$ monic s.t. $f(s) = 0$ with smallest degree.

Let the dependence be

$$s^n + r_1 s^{n-1} + \cdots + r_n = 0.$$

If $r_n = 0$, then $s(s^{n-1} + \cdots + r_{n-1}) = 0$

but $s \neq 0$ and thus, $\underbrace{s^{n-1} + \cdots + r_{n-1} = 0}$. (lower degree)

$\therefore$ $r_n \neq 0$

$$r_n = -s\left(s^{n-1} + r_1 s^{n-2} + \cdots + r_{n-1}\right).$$

Since r_n is non-zero and R is a field, we multiply by r_n^{-1} to get

$$1 = (s)\left[\underbrace{(-r_n^{-1})\left(s^{n-1} + \cdots + r_{n-1}\right)}_{\in S}\right]$$

Thus, s is invertible in S and hence, S is a field.

($\Leftarrow$) S is a field. To show R is a field.

Let $0 \neq r \in R$.

We know r has an inverse $s \in S$.

$\exists r_1, \ldots, r_n \in R$ s.t.

$$s^n + r_1 s^{n-1} + \cdots + r_n = 0 \quad \text{in } S.$$

Multiply with r^n and use $rs = 1$:

$$1 + r r_1 + r^2 r_2 + \cdots + r^n r_n = 0$$

$$\Rightarrow \quad 1 = r\,\underbrace{\left(-r_1 - r r_2 - \cdots - r^{n-1} r_n\right)}_{\in R}$$

$\therefore$ r is invertible in R. ∎

Cor. Let $R \subset S$ be rings (not nec. domains).

Let $\mathfrak{q} \in \operatorname{Spec} S$ and $\mathfrak{p} = R \cap \mathfrak{q}$.

Then, $\mathfrak{q} \in \operatorname{mSpec} S \iff \mathfrak{p} \in \operatorname{mSpec} R$.

Then, $\mathfrak{q} \in \operatorname{mSpec} S \iff \mathfrak{p} \in \operatorname{mSpec} R$.

$\mathfrak{q}$ lies over $\mathfrak{p}$

Thus, primes over maximal ideals are maximal.

Thm. (Lying over theorem)

Let $R \subset S$ be an integral extension of rings and $P \in \operatorname{Spec} R$. Then, $\exists$ a prime ideal of Q of S s.t. $Q \cap R = P$.

Proof. $R \setminus P = U$ is a m.c.s. of R.

If $Q \in \operatorname{Spec} S$ and $Q \cap R = P$, then $Q \cap U = \phi$.

$$\begin{tikzcd}
Q \arrow[d, bend right] & S \arrow[r] & U^{-1}S & U^{-1}Q \arrow[lll, bend right] \arrow[d, bend left] \\
P & R \arrow[u] \arrow[r] \arrow[ur, phantom, "\circlearrowright"] & U^{-1}R \arrow[u] & U^{-1}P \arrow[lll, bend left]
\end{tikzcd}$$

Since the diagram commutes, it suffices to show $\exists\, U^{-1}Q$, $Q \in \operatorname{Spec} S$, $Q \cap U = \phi$ and $U^{-1}Q \cap R_P = P R_P$.

Thus, we may assume R is a local ring and show that $\exists\, Q \in \operatorname{Spec} S$ s.t. $Q \cap R = \mathfrak{m}$

$\mathfrak{m}$ = unique maximal ideal of R.

$$\begin{array}{l} S \\ \big|\, \text{int} \\ (R, \mathfrak{m}) \leftarrow \text{local} \end{array}$$

Now, take any maximal ideal of S. By earlier corollary, the contraction is maximal and hence, $\mathfrak{m}$. ∎

Thm. (Going up Theorem)

$$\begin{array}{cccccccccc} S & & Q_1 & \subset Q_2 \subset \cdots & \subset & Q_m & \subset & \exists Q_{m+1} \\ \text{int}\ \big| & & \big| & \big| & & \big| & & \big| \end{array}$$

$$\begin{tikzcd}[column sep=small] S & Q_1 \arrow[r, phantom, "\subset"] \arrow[d, dash] & Q_2 \arrow[r, phantom, "\subset"] \arrow[d, dash] & \cdots \arrow[r, phantom, "\subset"] & Q_m \arrow[r, phantom, "\subset"] \arrow[d, dash] & Q_{m+1} \arrow[d, dash] \\ R \arrow[u, dash, "\text{int}"] & P_1 \arrow[r, phantom, "\subset"] & P_2 \arrow[r, phantom, "\subset"] & \cdots \arrow[r, phantom, "\subset"] & P_m \arrow[r, phantom, "\subset"] & P_{m+1} \end{tikzcd}$$

Let $P_1, P_2 \in \operatorname{Spec} R$ and $Q_1 \subset \operatorname{Spec} S$ be s.t. $Q_1 \cap R = P_1 \subset P_2$. Then, $\exists\, Q_2 \in \operatorname{Spec} S$ s.t. $Q_2 \cap R = P_2$ and $Q_2 \supset Q_1$.

Proof.

$$\begin{tikzcd} Q_1 \arrow[r, phantom, "\subset"] \arrow[d, dash] & \overset{\exists}{Q_2} \arrow[d, dash] \\ P_1 \arrow[r, phantom, "\subsetneq"] & P_2 \end{tikzcd}$$

$$\begin{tikzcd} S \arrow[r] & S/Q_1 \\ R \arrow[u, dash] \arrow[r] & R/P_1 \arrow[u, "\text{int}"] \end{tikzcd} \quad \supset \underbrace{\frac{P_2}{P_1}}_{\neq 0} \text{ prime in } R/P_1$$

$\exists\, Q_2/Q_1$ contracting to P_2/P_1 by lying over ?

$$\begin{tikzcd} Q_2 & S \arrow[r, two heads, "f"] & S/Q_1 & Q_2/Q_1 \arrow[d, dash] \\ Q_2 \cap R = P_2 & R \arrow[u, "i"] \arrow[r, two heads, "g"] \arrow[ur, phantom, "\circlearrowright"] & R \arrow[u, "i_2"] & \supset \dfrac{P_2}{P_1} \end{tikzcd}$$

Thus, $P_2 = Q_2 \cap R$ and $Q_2 \supset Q_1$. ∎

Lecture 13 (23-02-2021)

23 February 2021 14:00

Going Down Theorem for Integral Extensions

Prop^n (Incompatibility (INC)) Let $R \subset S$ be an integral extension of rings.

$$\begin{tikzcd} S \arrow[d, dash] & Q_1 \arrow[dr, dash] & & Q_2 \arrow[dl, dash] \\ R & & P & \end{tikzcd}$$

Let $Q_1, Q_2 \in \operatorname{Spec} S$ which lie over P.

$Q_1^c = P = Q_2^c$.

If $Q_1 \neq Q_2$, then $Q_1 \not\subset Q_2$ and $Q_2 \not\subset Q_1$.

Thus, the fiber $\{Q \in \operatorname{Spec} S : Q^c = P\}$ is an anti-chain.

Proof.

$$\begin{tikzcd} S/Q_1 \arrow[d, dash] \\ R/P \end{tikzcd}$$

is also an integral extension. It is of domains.

We want to show $Q_2(S/Q_1) \neq 0$. (i.e., $Q_2 \not\subset Q_1$)

Let $A \subset B$ be an integral extension of domains.

Let $I \trianglelefteq B$ be a non-zero ideal.

To show: $I \cap A = I^c \neq 0$.

Proof

Let $a \in I$ with $a \neq 0$. a is integral. Write

$(r_1, \dots, r_n \in A)$ $a^n + r_1 a^{n-1} + \dots + r_n = 0$ of smallest degree.

Then, $r_n \neq 0$. We have

$$\underset{A}{\underset{\nearrow}{r_n}} = -(a^n + \dots + r_{n-1} a) \in I$$

$\therefore r_n \in I \cap A \neq 0$. ∎

$$\begin{tikzcd} S \arrow[d, dash, "\text{int}"'] & Q_1 \arrow[dr, dash] & & Q_2 \arrow[dl, dash] \\ R & & P & \end{tikzcd}$$

Let $Q_2 \subsetneq Q_1$. (we get a contradiction)

$$\begin{tikzcd} S \arrow[r] & S/Q_2 \\ R \arrow[u, dash] \arrow[r] \arrow[ur, phantom, "\circlearrowright"] & R/P \arrow[u, dash] \end{tikzcd}$$

Then, $\dfrac{Q_1}{Q_2} \neq 0$

contraction

$P/P = 0$

Thus, $\frac{Q_1}{Q_2}$ contracts to 0, a contradiction. ■

Lemma. Let $f: R \longrightarrow S$ be a ring homomorphism and $p \in \operatorname{Spec} R$.
Then,

$$\exists\, Q \in \operatorname{Spec} S \quad \text{s.t.} \quad Q^c = f^{-1}(Q) = P$$
$$\Leftrightarrow \quad \underbrace{f^{-1}(f(p)S)}_{= p^{ec}} = P$$

(This is a general fact. No assumption of integral extension.)

Proof. $(\Rightarrow)$ Let $Q \in \operatorname{Spec} S$ be s.t. $Q^c = P$.

To show: $P^{ec} = P$

That is, $f^{-1}(f(P)S) = P$.

$$P = Q^c = f^{-1}(Q) \Rightarrow f(P) \subset Q \Rightarrow f(P)S \subset Q$$
$$\Rightarrow f^{-1}(f(P)S) \subset f^{-1}(Q) = P$$

$\therefore \underbrace{f^{-1}(f(p)s)}_{= p^{ec}} \subset P.$ $\qquad P \subset \underbrace{f^{-1}(f(P)S)}_{= p^{ec}}$ is always true.

$(\Leftarrow)$ Let $P = p^{ec}$.

TS: $\exists Q \in \operatorname{Spec} S$ s.t. $Q^c = P$.

Take $W = R \setminus P$ and localise at W.

$$\begin{array}{ccc} S & \longrightarrow & f(W)^{-1}S \cong W^{-1}S \\ {\scriptstyle f}\uparrow & & \uparrow{\scriptstyle f} \\ R & \longrightarrow & W^{-1}R \end{array}$$

think of S as R-mod.

$p^e \cap f(W) = \phi$ since $p^{ec} = P$.

$p^e(f(W)^{-1}S) = p^e(W^{-1}S)$ is a proper ideal

Then, $p^e(W^{-1}S) \subseteq m$ for some maximal ideal $\mathfrak{m}$.

$$\therefore \quad \underbrace{\mathfrak{m} \cap R_p}_{\left(\frac{f}{1}\right)^{-1}(\mathfrak{m})} = pR_p$$

has to be prime

$pR_p \subset f^{-1}(f(P)S) \cap f^{-1}(\mathfrak{m})$

Now, $\mathfrak{m}$ is of the form $f(\omega)^{-1}Q$ for some $Q \in \operatorname{Spec} S$.

$$\begin{tikzcd}
Q \arrow[dd, bend right] & S \arrow[r] & f(\omega)^{-1}S & \mathfrak{m} \arrow[lll, bend right] \arrow[dd, bend left] \\
& R \arrow[u, "f"] \arrow[r] \arrow[ur, phantom, "\circlearrowleft"] & R_p \arrow[u, "\frac{f}{1}"'] & \\
P & & & pR_p \arrow[lll, bend left]
\end{tikzcd}$$

Then, by commutativity of diagram, $Q^c = P$. ∎

Going down theorem: GDT

Applicable to normal domains.

Thm. (Going down theorem)

Let R be a normal domain $R \subset S$ an integral extension. (int. domain)

Given $P_0, P_1 \in \operatorname{Spec} R$ and $Q_0 \subset \operatorname{Spec} S$ with $P_0 \supset P_1$ and $Q_0^c = P_0$, $\exists Q_1 \in \operatorname{Spec} S$ s.t. $Q_0 \supset Q_1$ and $Q_1^c = P_1$.

$$\begin{array}{ccccc}
S & & Q_0 & \supset & \exists\, Q_1 \\
| & & | & & \vdots \\
R & & P_0 & \supset & P_1
\end{array}$$

Lemma.

$$\begin{array}{lcl}
PS \quad S & — & Q(S) = L \\
\quad\ \ \uparrow \text{ incl.} & & \quad | \text{ alg.} \\
P \subseteq R & — & Q(R) = K
\end{array}$$

Let $\alpha \in PS \subset L$.

Let $\operatorname{irr}(\alpha, K)$ be the min. poly of α / K. Then, all the non-leading coefficients $\in P$. (Leading co-eff $= 1$.)

Proof. Let $f(x) = \operatorname{irr}(\alpha, K)$.

Construct a splitting field of $f(x)$ and let the roots of $\alpha = \alpha_1, \dots, \alpha_n$.

$$f(x) = \prod_{i=1}^{n} (x - \alpha_i).$$

The co-efficients are elementary symmetric functions of $\alpha_1, \dots, \alpha_n$.

Let $M = L(\alpha_2, \dots, \alpha_n)$ = splitting field of $f(x)$ over L.

Replace L with M and S with its int. closure in $L = M$.

$f(x)$ is irred $\Rightarrow$ $Gal(L/K)$ acts transitively on $\{\alpha_1, \dots, \alpha_n\}$.

Let $\sigma_i \in Gal(L/K)$ be s.t. $\sigma_i(\alpha_1) = \alpha_i$.

$$\sigma_i(PS) = P\sigma_i(S).$$

$$\begin{array}{ccc} S & \xrightarrow{\sigma_i} & S \\ {\scriptstyle \text{int}}\Big| & & \\ R & & \end{array}$$

σ_i is a K-fixing automorphism

Given $s \in S$, $s^m + r_1 s^{m-1} + \dots + r_m = 0 \rightsquigarrow (\sigma_i(s))^m + r_1(\sigma_i(s))^{m-1} + \dots + r_m = 0$

$$\Downarrow$$

$$\sigma_i(S) = \bar{S} = S.$$

Thus, each $\alpha_i \in PS$.

Thus, each elementary sym. f^n of α_i is in PS.

$\therefore$ Non-leading coefficients of $f(x)$ are in

$$PS \cap K = (PS \cap S) \cap K$$

elements of K int. over S ⊆ $S \cap K$ = R

$$= PS \cap (S \cap K)$$

$$= PS \cap R$$

using laying over thm. & first lemma

$$= P^{ec}$$

$$= P \qquad ☒$$

Thm Let R be a normal domain and $K = Q(R)$ and L/K is an alg. extension. $irr(\alpha, K) \in R[x]$ $\Leftrightarrow$ $\alpha \in \bar{R}^L$.

$$\begin{array}{cc} & \alpha \in L \\ \bar{R}^L & \Big| \text{alg.} \end{array}$$

$$\begin{tikzcd} & {} \arrow[d, dash, "\text{alg.}"] \\ \boxed{\bar{R}^L} \arrow[ur, dash] \arrow[d, dash] & K \\ R \arrow[ur, dash] & \end{tikzcd}$$

Reading exercise. B

Going Down Theorem

$$\begin{tikzcd} S \leftarrow \text{int domain} & Q_0 \arrow[d, dash] & \supset \exists Q_1 \arrow[d, dash] \\ R \leftarrow \text{normal domain} \arrow[u, hook, "\text{int}"] & P_0 & \supset P_1 \end{tikzcd}$$

Proof. $\exists Q_1 \in \operatorname{Spec} S$ contracting to P_1 iff $P_1^{ec} = P_1$

But to get $Q_1 \subset Q_0$, we go to localisation.

Thus, it is equivalent to proving

$$R \cap P_1 S_{Q_0} = P_1.$$

(2) always true

$$\begin{tikzcd} S_{Q_0} \\ S \arrow[u, hook, "\text{(incl. since } S \text{ is dom.)}"] \\ R \arrow[u, hook] \end{tikzcd}$$

($\subseteq$) Now, let $0 \neq x \in R \cap P_1 S_{Q_0}$.

Then, $x = \dfrac{y}{s} \in R$ where $y \in P_1 S$, $s \in S \setminus Q_0$.

$\therefore \quad y = xs \in P_1 S.$

$\operatorname{irr}(y, K)$ has non-leading co-efficients in P_1.

$$y^n + a_1 y^{n-1} + \cdots + a_n = 0 \quad \text{for} \quad a_1, \ldots, a_n \in P_1$$

$$\Rightarrow \left(\frac{y}{x}\right)^n + \frac{a_1}{x}\left(\frac{y}{x}\right)^{n-1} + \cdots + \frac{a_n}{x^n} = 0$$

$\Rightarrow \quad \operatorname{irr}\left(\frac{y}{x}, K\right)$ has degree n.

$\Rightarrow \quad a' \quad \ldots \quad \in R$

$$\Rightarrow \frac{a_i}{x^i} = b_i \in R$$

$$\Rightarrow a_i = x^i b_i \in P_1 \quad \forall i$$

If $x \notin P_1$, then $b_i \in P_1$ $\forall i$.

$$s^n + \underbrace{b_1 s^{n-1} + \cdots + b_n}_{\in P_1} = 0$$

$\therefore s^n \in P_1$ $\therefore s \in P_1$ $\rightarrow\leftarrow$

$\because s \notin Q_1$

Thus, $x \in P_1$, as desired. $\therefore R \cap P_1 S_{Q_0} = P_1$. ∎

Example. GDT need not hold if R is not a normal domain.

Let K be a field and $\operatorname{char} K = 0$.

Consider $f(X,Y) = Y^2 - X^2(X+1) = Y^2 - (X^2 + X^3)$.

$f(X,Y)$ is irr. in $K[X,Y]$ by Eisenstein.

Put $P = (f(X,Y))$.

$$R = \frac{K[X,Y]}{P} = K[x,y] \quad \text{where } x = X + P,\ y = Y + P.$$

$$\begin{array}{c} K[x,y] \\ | \\ K[x] \end{array}$$

$$y^2 = x^2 + x^3$$

$$\Rightarrow \left(\frac{y}{x}\right)^2 = 1 + x$$

$\frac{y}{x} \notin R$ (Prove this) but $\frac{y}{x} \in Q(R)$ and is integral over R.

$\therefore R$ is not normal.

$S = R\left[\frac{y}{x}\right]$ happens to be a normal domain.

GDT holds for $R \subset S$.

(only primes are 0 and maximal)

$S[z] = k[x, \frac{y}{x}, y][z]$ This does not satisfy GDT.

$R[z] = k[x, y, z]$

Lecture 14 (05-03-2021)

05 March 2021 14:01

Integral closure of normal domains
Rings of integers in number fields are free abelian groups of finite rank

$$\begin{tikzcd} & K \arrow[dl, dash, "\text{finite}"'] \arrow[d, dash] \\ \mathbb{Q} \arrow[d, dash] & \mathbb{Z}^K \\ \mathbb{Z} \arrow[ur, dash] & \end{tikzcd}$$

$K \longrightarrow$ number field

$\mathbb{Z}^K$ = integral closure of $\mathbb{Z}$ in K $= \mathcal{O}_K$

Thm $\mathcal{O}_K$ is a free abelian group of finite rank.

More general result:
Let R be a Noetherian normal domain with quotient field K.
Let $K \subset L$ be a finite separable extension.
Consider $\overline{R}^L$.

Q.
- Is $\overline{R}^L$ a Noetherian ring?
- Is $\overline{R}^L$ a finite R-module?

Thm. $\overline{R}^L$ is a finite R-module.
Thus, it is a Noetherian ring.

This uses facts about bilinear forms and norm/trace.

Recall:
(1) Norm and trace functions
Suppose $K \subset L$ is a finite alg. sep. extension.

$$\begin{tikzcd} L \arrow[r, "\sigma"] \arrow[d, dash] & \overline{K} \arrow[d, dash] \\ K \arrow[r, dash] & K \end{tikzcd}$$

$\overline{K}$ = alg. closure of K

$\# \{\sigma : L \to \overline{K} \mid K \text{ embedding}\} = [L:K] = s.$

Let $\sigma_1, \ldots, \sigma_s$ be the K embeddings.
Pick $x \in L$. Then,

$$tr(x) = \sum_{i=1}^{s} \sigma_i(x)$$

$$N(x) = \prod_{i=1}^{s} \sigma_i(x).$$

It follows that $tr: L \to K$ is a linear functional
and $N: L^\times \to K^\times$ is a group homomorphism.

Alternate def^n of $N(x)$, $tr(x)$.

Define $\mu_x : L \longrightarrow L$ by $\mu_x(a) = ax$.
This is a K-linear map.
Fix a K-basis $B = \{e_1, \ldots, e_n\}$ of L.
Let $[\mu_x]$ denote μ_x w.r.t. B.
Then, $tr(x) := tr\,[\mu_x]$ and $N(x) = \det[\mu_x]$.
Here, it's clear that $tr(x), N(x) \in K$ and that
$tr: L \to K$ functional, $N: L^\times \to K^\times$ homomorphism.

(2) Bilinear form using trace

$$\begin{array}{c} L \\ \text{alg} \Big| \\ K \end{array} \qquad \begin{aligned} L \times L &\longrightarrow K \\ (x, y) &\longmapsto tr(xy) \end{aligned}$$

This is a symmetric bilinear form.
Called the trace form.

Example. $\mathbb{Q}(\sqrt{d})$ assume d square free
$\Big|$
$\mathbb{Q}$ $\quad u \overset{\in \mathbb{Q}(\sqrt{d})}{=} a + b\sqrt{d}$; $\quad a, b \in \mathbb{Q}$

$|\mathrm{Gal}(\mathbb{Q}(\sqrt{d})/\mathbb{Q})| = 2$, id and $\sqrt{d} \mapsto -\sqrt{d}$ are the elements

$$tr(u) = (a + b\sqrt{d}) + (a - b\sqrt{d}) = 2a$$
$$N(u) = (a + b\sqrt{d})(a - b\sqrt{d}) = a^2 - b^2 d$$

Prop^n. Suppose E/K is a degree n algebraic extension. Let $u \in E$. Then,

$$\begin{array}{c} E \\ | \\ E(u) \\ | \\ K \end{array}$$

$$tr(u) = [E : K(u)] \sum_{i=1}^{s} u_i$$

and

$$N(u) = \left(\prod_{i=1}^{s} u_i\right)^{[E:K(u)]},$$

where $u_1, \ldots, u_s$ are roots of $\mathrm{irr}(\alpha, K)$ in $\bar{K}$.

Proof. Exercise. $\square$

Non degenerate Bilinear form

Let V be f.d. v.s. over K.
Let $f : V \times V \to K$ be a bilinear form.

Define $L_f(u) : V \to K$ defined as
$$w \mapsto f(u, w).$$

$L_f(u)$ is a linear functional.

Similarly, $R_f(w) : V \to K$ is defined as
$$u \mapsto f(u, w).$$

left and right functionals induced by the bilinear form

Fix a basis $B = \{e_1, \ldots, e_n\}$ of V.
Let $f : V \times V \to K$ be a bilinear form. To f, we associate the matrix

$$[f]_B = [f(e_i, e_j)]_{ij}.$$

Conversely, given an $n \times n$ matrix, we get a bilinear form.

Ex. TFAE:

(1) $[f]_B$ is non-singular.

(2) $\forall v \in V \setminus \{0\}$, $\exists u \in V$ s.t. $f(u, v) \neq 0$.

(3) $\forall u \in V \setminus \{0\}$, $\exists v \in V$ s.t. $f(u, v) \neq 0$.

If any of the above (equivalent) conditions are satisfied, f is said to be a non-degenerate bilinear form.

Note $L_f(u) : V \to K$ is linear. Thus, $L_f(u) \in V^*$.

Hence, L_f is a map from V to V^*. (Check it is linear.)

$L_f : V \to V^*$ is injective

$\Leftrightarrow (u \neq 0 \Rightarrow L_f(u) \neq 0)$

$\Leftrightarrow (u \neq 0 \Rightarrow \exists v \in V$ s.t. $L_f(u)(v) \neq 0)$

$\Leftrightarrow f$ is non-degenerate.

Prop^n. V is n-dim v. space $/K$.

Let $B = \{e_1, \dots, e_n\}$ be a basis of V/K.

$f : V \times V \to K$ non degenerate bilinear form.

Then, $\exists\, b_1, \dots, b_n$ basis of V s.t.

$$f(e_i, b_j) = \delta_{ij}, \qquad \forall\, i, j.$$

$\{b_1, \dots, b_n\}$ is called a dual basis.

Proof.

$$\begin{tikzcd} V \times V \arrow[r, "f"] \arrow[d, "\varphi"] & K \\ V \times (V^*) \arrow[ur, "e_V"'] & \end{tikzcd}$$

$(x, y) \mapsto (x, R_f(y))$

$(x, f) \mapsto f(x)$

Claim: The diagram commutes, i.e, $f = e_V \circ \varphi$.

Proof. $(e_v \circ \varphi)(x,y) = e_v(x, R_f(y))$
$= R_f(y)(x) = f(x,y)$. ⊠

f is non-degenerate $\Rightarrow$ $R_f : V \to V^*$ is an isomorphism.

Any $v \in V$ can be written as $v = \sum x_i e_i$

$$[v]_B = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = \text{co-ordinate vector}$$

We have the coordinate function(als) $g_i : V \to K$ as
$v \mapsto x_i$.

Note that $g_i \in V^*$ and $R_f : V \to V^*$ is an iso.

Thus, $\exists b_1, \dots, b_n \in V$ s.t. $R_f(b_i) = g_i$.

$$\begin{tikzcd} V \times V \arrow[r] \arrow[d] & K \\ V \times (V^*) \arrow[ur] & \end{tikzcd}$$

$$f(e_i, b_j) = (e_v \circ \varphi)(e_i, b_j)$$
$$= e_v(e_i, R_f(b_j)) = e_v(e_i, g_j)$$
$$= g_j(e_i) = \delta_{i,j}$$ ⊠

Thm. Let L/K be a finite separable normal extension.
$\mathrm{Gal}(L/K) = \{\sigma_1, \dots, \sigma_n\}$.
$\mathrm{Tr} : L \times L \to K$ is defined as $(x,y) \mapsto \mathrm{tr}(xy)$.
Then, Tr is a sym. non-deg. bilin. form.

Proof. Only need to check that it is non-deg.
Let $A = [f(e_i, e_j)]_{ij} = [\mathrm{tr}(e_i e_j)]_{ij}$.
We show $\det A \neq 0$.

$$\mathrm{tr}(e_i e_j) = \sum_{\ell=1}^{n} \sigma_\ell(e_i e_j) = \sum_{\ell=1}^{n} \sigma_\ell(e_i)\sigma_\ell(e_j).$$

Define $M = [\sigma_\ell(e_j)]_{\ell, j}$

$$N = [\sigma_\ell(e_i)]_{i,\ell} \qquad \text{(note the switch).}$$

Then, $N = M^t$.

Moreover, $\det(A) = (\det M)(\det N) = (\det N)^2$.

Suffices to prove N is non-singular.

If $[\sigma_\ell(e_i)]_{i,\ell}$ is singular, then

$\exists\, (c_1, \dots, c_n) \in L^n$ not zero s.t.

$$[c_1 \cdots c_n]\,[\sigma_\ell(e_i)] = 0$$

Thus, $c_1\sigma_1(e_j) + \cdots + c_n\sigma_n(e_j) = 0 \quad \forall j$

$\Rightarrow c_1\sigma_1 + \cdots + c_n\sigma_n = 0$ map

Invoke Dedekind's thm about independence of characters to get a contradiction.

Thus, the trace form is non-degenerate. ∎

Main Theorem. Let R be a Noetherian normal domain.

$K = Q(R)$, quotient field.

E/K is a finite separable extension.

$$\begin{tikzcd} & E \arrow[d, dash] \\ K \arrow[ur, dash] \arrow[d, dash] & \overline{R}^E =: S \\ R \arrow[ur, dash] & \end{tikzcd}$$

Then, S is a f.g. R-module.

In particular, R is a Noetherian ring.

Not true if R not normal or not sep.

Proof. Let L be the smallest Galois extension of L containing E.

$\overline{R}^E \subset \overline{R}^L$.

If $\overline{R}^L$ is a finite R-submodule, we are done, since R is Noetherian.

Thus, we may assume E/K is itself a Galois extension.

Then, $E \times E \longrightarrow K$ is non-degenerate.

Let $\{e_1, \dots, e_n\}$ be a basis of E/K.

$E = Ke_1 \oplus \cdots \oplus Ke_n$.

Normality of $R \Rightarrow \exists r_1, \dots, r_n \in R \setminus \{0\}$ s.t. $r_1 e_1, \dots, r_n e_n \in S$.

$e_1 \to$ alg. over K Thus, $e_1^n + \frac{r_1}{s_1} e_1^{n-1} + \cdots + \frac{r_n}{s_n} = 0$; $r_i \in R$, $s_i \in R \setminus \{0\}$

Can assume $s_1 = \cdots = s_n = s^n$ for some $s \in R \setminus \{0\}$.

Then, $(s_1 e_1)^n + t_1 (se_1)^{n-1} + \cdots + t_n = 0$.

$\Rightarrow s_1 e_1 \in S$.

Thus, we may assume $e_1, \dots, e_n \in S$.

Non-degeneracy of trace form gives a basis $\{f_1, \dots, f_n\}$ of E/K s.t.

$$tr(e_i f_j) = \delta_{ij}.$$

To show: $S \subset$ f.g. R module.

Take $\alpha \in S \subseteq E$. Then,

$$\alpha = \sum_{j=1} c_j f_j \quad \text{where } c_j \in K.$$

$$\Rightarrow e_i \alpha = \sum_{j=1}^{n} c_j e_i f_j$$

$$\Rightarrow \underbrace{tr(e_i \alpha)}_{} = \sum_{j=1}^{n} c_j \, tr(e_i f_j) = c_i$$

$e_i \alpha \in S$. Thus, it is fixed by every $\sigma \in Gal$

Thus, $tr(e_i \alpha) \in S$

$\Rightarrow c_i = tr(e_i \alpha) \in S \cap K = R$.

$\therefore \alpha = \sum c_i f_i \in Rf_1 + \cdots + Rf_n$.

R is Noe. $\Rightarrow$ S is a f.g. R-module

$\Rightarrow$ Noe R-module ∎

Lecture 15 (09-03-2021)

09 March 2021 14:01

Chapter 5: Dimension Theory of Affine Algebra over Fields

Results to be proven:

1. Artin - Tate Lemma
   (टेट)

2. Hilbert's Nullstellensatz
   Zero Point theorem

Solutions of polynomial equations

$$(*) \quad \begin{aligned} f_0(x_1, \dots, x_n) &= 0 \\ &\vdots \\ f_s(x_1, \dots, x_n) &= 0 \end{aligned} \qquad f_i \in K[x_1, \dots, x_n]$$

(a) Does $(*)$ have a solution in K^n?

$I = (f_1, \dots, f_s) \subset S = K[x_1, \dots, x_n]$.

$Z(I) = \{a \in K^n : g(a) = 0 \ \forall g \in I\}$

$\hookrightarrow$ algebraic subset of K^n

Assume K is alg. closed.

Nullstellensatz gives:

(1) $Z(I) \neq \phi \iff I \subsetneq S$

$\Uparrow$

(2) Structure of maximal ideals in $K[x_1, \dots, x_n]$

$$K^n \longleftrightarrow \text{mSpec } S$$

$$a = (a_1, \dots, a_n) \longmapsto m_a = (x_1 - a_1, \dots, x_n - a_n).$$

$\Uparrow$

Artin- Tate Lemma

Noether normalisation Lemma:

$Z(I) = X \subseteq K^n = \mathbb{A}^n$ = Affine n-space over K.

$X \longrightarrow K$

$f(x_1, \dots, x_n) \rightsquigarrow (a \mapsto f(a))$

If K is infinite, then $f \equiv g$ as functions
$\Updownarrow$ $f \equiv g$ as polynomials

$f, g : X \to K$

$(f-g)(a) = 0 \quad \forall a \in X = Z(I)$

$f - g \in \mathcal{I}(X) = \{ h : h(b) = 0 \ \forall b \in X \}$

$S / \mathcal{I}(X) \cong$ Ring of poly functions $X \to K$

$\parallel$

Coordinate ring of X

$X \rightsquigarrow S/\mathcal{I}(X)$ affine K-algebra

$\mathcal{I}(X)$ is a radical ideal.

Lemma (Artin-Tate Lemma) Let $R \subset S \subset T$ be rings.

① R is Noetherian.

② T is a f.g. S module.

③ T is a f.g. R algebra.

T/S is integral

$T = R[c_1, \dots, c_m] = Sb_1 + \cdots + Sb_n$

T | S | R Noetherian

Then, S is a f.g. R algebra.

Thus, $S = R[s_1, \dots, s_t]$ for some $s_i \in S$.

In particular, S is Noetherian.

(Non) Example.

$K[x, y]$
|
$S = K[x, xy, xy^2, \dots]$ ← Not Noetherian

$$\begin{array}{c} | \\ S = K[x, xy, xy^2, \dots] \\ | \\ K \end{array}$$

$\leftarrow$ Not Noetherian

Proof. $T = R[c_1, \dots, c_m] = Sb_1 + \dots + Sb_n$.

Write $c_i = \sum_{j=1}^{n} s_{ij} b_j, \quad i = 1, \dots, m.$ $\quad s_{ij} \in S$

$$\sum_\alpha \beta_\alpha c_1^{\alpha_1} \cdots c_m^{\alpha_m} \in T, \quad \beta_\alpha \in R \quad \forall \alpha$$

$\uparrow$ typical element of T

$$c_i b_j = \sum_{k=1}^{n} s_{ijk} b_k \quad \forall i, j \qquad s_{ijk} \in S$$

$$\begin{array}{l} T = R[c_1, \dots, c_m] = Sb_1 + \dots + Sb_n \\ | \text{ integral extension} \\ S \\ \quad \diagdown \\ \qquad S_0 := R[s_{ij}, s_{ijk} \mid \forall i, j, k] \\ \quad \diagup \\ R \end{array}$$

Noetherian ring

$$t = \sum \beta_\alpha c_1^{\alpha_1} \cdots c_m^{\alpha_m} \in T = R[c_1, \dots, c_m]$$

Use formulae for b_i and $c_i b_j$ to get an expression for t:

$$t = u_1 b_1 + \cdots + u_n b_n + u_{n+1}, \quad u_i \in S_0$$

$\Rightarrow$ T is a f.g. S_0 module.

$\Rightarrow$ T is a Noetherian S_0-module.

$\Rightarrow$ S ——————— .

$\Rightarrow$ S is a f.g. R-algebra ▢

Lemma (Zariski) K is any field.
R is an affine K-algebra, i.e., $R = \underbrace{k[x_1, \dots, x_n]}_{S} / I$.

Let R be a field (that is, I is maximal in S).
S/I is an algebraic extension of K.

$$\begin{array}{ccc} S & \twoheadrightarrow & S/I \\ | & \nearrow & \\ K & & \end{array}$$

Proof. $K[r_1, \dots, r_n]$ over K

We need to show that each r_i is algebraic.
Relabel and suppose $r_1, \dots, r_m$ are alg. indep. s.t.

$$\begin{array}{c} K[r_1, \dots, r_n] \\ \big|\ \text{alg.} \\ K(r_1, \dots, r_m) \\ \big|\ \text{transc.} \\ K \end{array}$$

If $m = 0$, then done.
Let $m > 0$.

Note that alg. extension is integral. Thus, A-T applies.

$\Rightarrow$ $K(r_1, \dots, r_m)$ is a f.g. K-algebra.
$\Rightarrow$ $K(X_1, \dots, X_m)$ is a f.g. K-algebra.

$$\Rightarrow \quad K(X_1, \dots, X_m) = K\left[\frac{f_1}{g_1}, \dots, \frac{f_t}{g_t}\right]$$

We may assume $\gcd(f_i, g_i) = 1 \quad \forall i$.

Now, look at $\dfrac{1}{g_1 \cdots g_t + 1}$.

Suppose

Suppose

$$\frac{1}{g_1 \cdots g_t + 1} = \Phi\left(\frac{f_1}{g_1}, \dots, \frac{f_t}{g_t}\right)$$

polynomial with total degree d

$$\Rightarrow \frac{1}{g_1 \cdots g_t + 1} = \frac{f}{(g_1 \cdots g_t)^d}$$

$$\Rightarrow (g_1 \cdots g_t)^d = (g_1 \cdots g_t + 1) f$$

Thus, $g_1 \cdots g_t + 1$ has no irred factor.
$\Rightarrow$ $g_1 \cdots g_t + 1$ is a unit and hence, each g_i is a constant. But then $\frac{1}{x_1} \notin K[f_1, \dots, f_n]$.

Thus, $m = 0$. ☒

Thus, if $K = \bar{K}$ (alg. closed), then

$$K \hookrightarrow \frac{K[x_1, \dots, x_n]}{\mathfrak{m}} \text{ is an isomorphism.}$$

φ (inverse)

$$\Rightarrow \varphi(x_i + \mathfrak{m}) = a_i \in K \quad \forall i$$
$$\Rightarrow x_i + \mathfrak{m} = a_i + \mathfrak{m} \quad \forall i$$
$$\Rightarrow x_i - a_i \in \mathfrak{m} \quad \forall i$$

$$\Rightarrow \mathfrak{m}_a = (x_1 - a_1, \dots, x_n - a_n) \subset \mathfrak{m}.$$

Note that $\mathfrak{m}_a$ is the kernel of $ev_a : K[x_1, \dots, x_n] \twoheadrightarrow K$
$$ev_a(f) = f(a).$$

Thus, $\mathfrak{m}_a$ is maximal and hence, $\mathfrak{m} = \mathfrak{m}_a$.

Thus, if $K = \bar{K}$, then
$$K^n \longleftrightarrow m\mathrm{Spec}\, K[x_1, \dots, x_n]$$
$$a \longleftrightarrow \mathfrak{m}_a$$

Thus, if $K = \bar{K}$, then $K^n \leftrightarrow \text{mSpec } K[x_1, \dots, x_n]$

$$a \longleftrightarrow m_a$$

bijection

Thm. (Weak Nullstellensatz)

If $K = \bar{K}$, then any $m \in \text{mSpec } K[x_1, \dots, x_n]$ is of the form $(x_1 - a_1, \dots, x_n - a_n)$.

(Non) Example. $x^2 + 1 \in \mathbb{R}[x]$ generates a maximal ideal.

If K is any field, then every maximal ideal in $K[x_1, \dots, x_n]$ requires n generators: $(f_1(x_1), f_2(x_1, x_2), \dots, f_n(x_1, \dots, x_n))$.

↳ irred

Criterion for solubility:

Thm.

$$(*) \quad \begin{cases} f_1(x_1, \dots, x_n) = 0 \\ \vdots \\ f_s(x_1, \dots, x_n) = 0 \end{cases} \qquad K = \bar{K}$$

$(*)$ has a sol^n $\iff$ $I = (f_1, \dots, f_s) \neq S$

$(\iff 1 \notin I)$

Proof. $(\Rightarrow)$ Let $a = (a_1, \dots, a_n)$ be a sol^n of $(*)$.

$f_i(a) = 0 \quad \forall i$

$\Rightarrow f_i \in (x_1 - a_1, \dots, x_n - a_n) = m_a$ ⊃ consider the Taylor expansion about a

$\Rightarrow I = (f_1, \dots, f_s) \subseteq m_a \subsetneq S.$

$(\Leftarrow)$ Let $a \in K^n$ be s.t. $I = (f_1, \dots, f_n) \subset m_a$.

Then, $f_i(a) = 0 \quad \forall i.$ $\blacksquare$

Remark No need to assume $s < \infty$.

Hilbert's Strong Nullstellensatz (HSN) $(k = \bar{k})$

$$X \overset{\subseteq k^n}{} \longmapsto \mathcal{I}(X)^{\subseteq S} = \text{ideal of } X$$
$$= \{ f \in S : f(a) = 0 \ \forall a \in X \}$$

$$\mathcal{Z}(I)^{\subseteq k^n} \longleftarrow I^{\subseteq S}$$
$$\|$$
$$\{ a \in k^n : f(a) = 0 \ \forall f \in I \}.$$

HSN: $\mathcal{I}(\mathcal{Z}(I)) = \sqrt{I}$.

If $I = \sqrt{I}$, then $\mathcal{I}(\mathcal{Z}(I)) = I$.

$\Rightarrow \exists$ 1-1 correspondence between alg. subsets of k^n and radical ideals of $S = k[x_1, \dots, x_n]$.

Lecture 16 (12-03-2021)

12 March 2021 14:03

Recall Strong Nullstellensatz :

$\overline{K} = K$ alg. closed (in particular, K is infinite)

$\mathbb{A}^n_K$ = Affine n-space over K

$= K^n$

along with ring of polynomial functions $K^n \longrightarrow K$

Let $I \subseteq S = K[x_1, \dots, x_n]$ be an ideal.

$Z(I) = \{ a \in \mathbb{A}^n_K : f(a) = 0 \ \forall f \in I \}$.

= zero set of I

= the algebraic subset of $\mathbb{A}^n_K$

$= Z(\sqrt{I})$.

$$S = K[x_1, \dots, x_n] \qquad\qquad \mathbb{A}^n_K$$

$$I \longmapsto Z(I)$$

$$S \supseteq \mathcal{I}(X) \longleftarrow\!\shortmid \ X \subseteq \mathbb{A}^n_K$$

$\mathcal{I}(X)$ = ideal of $X = \{ f \in S : f(a) = 0 \ \forall a \in X \}$.

$g^n(a) = 0 \ \forall a \in X \iff g(a) = 0 \ \forall a \in X$.

$\therefore \ \mathcal{I}(x)$ is a radical ideal of S.

<u>Hilbert's Strong Nullstellensatz</u> (HSN)

$$\mathcal{I}(Z(I)) = \sqrt{I}.$$

In particular, there is a bijection between

$$\{\text{radical ideals in } S\} \longleftrightarrow \{\text{algebraic subsets in } \mathbb{A}^n_K\}.$$

$$\begin{tikzcd} I \arrow[r, mapsto] & Z(I) \arrow[dl, bend left] \\ I = g(Z(I)) & \end{tikzcd}$$

($Z(g(X)) = X$ is easy to show)

Example Take $k = \mathbb{R}$ ← not alg. closed.
Note (x^2+1) and (1) are distinct radical ideals.
But $Z(x^2+1) = \phi = Z(1)$.
Thus, no 1-1 correspondence.

Proof. To show: $\sqrt{I} = g(Z(I))$.

($\subseteq$) Note that $I \subseteq g(Z(I))$ is clear.
Since $g(Z(I))$ is a radical ideal, $\sqrt{I} \subseteq g(Z(I))$.

($\supseteq$) Let $f \in g(Z(I))$.
Thus, $f(b) = 0 \quad \forall\, b \in Z(I)$.
Assume $f \neq 0$.

$$\begin{tikzcd}[arrows=dash] S[x_{n+1}] = T \supseteq (I,\ x_{n+1}f - 1) \\ k[x_1, \ldots, x_n] = S \arrow[u] \end{tikzcd}$$

Claim. $(I,\ x_{n+1} f - 1) = T$.
Proof. Suppose not. $(I,\ x_{n+1} f - 1) \subset m \in m\operatorname{Spec} T$.
But $T = k[x_1, \ldots, x_n]$.
Thus, by Weak Nullstellensatz, $m = (x_1 - a_1, \ldots, x_{n+1} - a_{n+1})$
for $(a_1, \ldots, a_{n+1}) \in \mathbb{A}^{n+1}_k$.
Easy to see that $Z(m_a) = \{a\}$.

Let us call $(I,\ x_{n+1} f - 1) = J$.
Then, $Z(J) \supseteq Z(m_a) = \{a\}$ or $a \in Z(J)$.

Then, $Z(J) \supseteq Z(m_a) = \{a\}$ or $a \in Z(J)$.

$\therefore$ if $g \in I$, then $g(a_1, \ldots, a_n) = 0$. Thus, $(a_1, \ldots, a_n) \in Z(I)$.

Moreover, $a_{n+1} f(a_1, \ldots, a_n) - 1 = 0$.

But $(a_1, \ldots, a_n) \in Z(I)$ gives $f(a_1, \ldots, a_n) = 0$.

$\therefore$ $a_{n+1} \cdot 0 - 1 = 0$ or $1 = 0$. $\rightarrow\leftarrow$

Thus, $J = T$. ■

This gives us that $1 = f_1 g_1 + \cdots + f_n g_n + p \cdot (x_{n+1} f - 1)$ — $(*)$

where $f_1, \ldots, f_n \in I$ and $g_1, \ldots, g_n, p \in T$.

Define $\Phi : K[x_1, \ldots, x_n, x_{n+1}] \longrightarrow K(x_1, \ldots, x_n)$

$$\Phi(k) = k \quad \forall\, k \in K$$
$$\Phi(x_i) = x_i \quad \forall\, i = 1, \ldots, n$$

(Note $f \neq 0$ by assumption.) $$\Phi(x_{n+1}) = \frac{1}{f} \in K(x_1, \ldots, x_n).$$

Apply Φ to $(*)$:

$$1 = \sum_{i=1}^{n} f_i(x_1, \ldots, x_n)\, g_i\left(x_1, \ldots, x_n, \frac{1}{f}\right) + 0$$

$\nwarrow$ no x_{n+1} now

$\exists\, d \in \mathbb{N}$ so that f^d is a common denominator of RHS. Cross-multiply to get $f^d \in I$ and thus, $f \in \sqrt{I}$. ■

Noetherian Normalisation Theorem

Prop^n. Let K be any field. Let $f \in S = K[x_1, \ldots, x_n]$ be a non-constant polynomial.

|| $f = \sum_{\alpha \in \mathbb{N}^n} a_\alpha x^\alpha$; if $a_\alpha \neq 0$, x^α is called a term of f.

$$f = \sum_{\alpha \in \mathbb{N}^n} a_\alpha x^\alpha \quad ; \quad \text{if } a_\alpha \neq 0, \ x^\alpha \text{ is called a term of } f.$$
($a_\alpha = 0$ for all but finitely many α.)

Let $N > \max\{\alpha_i : \forall i \ \forall \alpha \text{ s.t. } x^\alpha \text{ is a term of } f\}$.

Wlog, assume x_n appears non-trivially in f.

$$\phi : S \longrightarrow S$$
$$k \longmapsto k \quad \forall k \in K$$
$$x_i \longmapsto x_i - x_n^{N^i} \quad i = 1, \dots, n-1$$
$$x_n \longmapsto x_n$$

Ex: Show that ϕ is an automorphism. (Easy to see onto.)

$$f = x_n^r g_r + x_n^{r-1} g_{r-1} + \cdots + g_r$$
$$g_1, \dots, g_r \in K[x_1, \dots, x_{n-1}]$$

Claim. $\phi(f)$ is a "monic" polynomial in x_n. (co-efficient is non-zero and in K.)

Proof. $f = \sum c_\alpha x^\alpha$.

$$\phi(f) = \sum c_\alpha \phi(x^\alpha).$$

Let us now analyse $\phi(x^\alpha)$.

$$\phi(x_1^{a_1} \cdots x_n^{a_n}) = x_n^{a_n} (\phi(x_1))^{a_1} \cdots (\phi(x_{n-1}))^{a_{n-1}}$$

$$= x_n^{a_n} (x_1 - x_n^N)^{a_1} (x_2 - x_n^{N^2})^{a_2} \cdots (x_{n-1} - x_n^{N^{n-1}})^{a_n}$$

exponent of x_n

$$a_n + a_1 N + a_2 N^2 + \cdots + a_{n-1} N^{n-1} =: \psi(a)$$
$$a = (a_1, \dots, a_n).$$

Now, $\phi(f) = \sum c_\alpha \phi(x^\alpha)$

power of x_n

$$\alpha \neq \beta \Rightarrow \psi(\alpha) \neq \psi(\beta) \quad \text{(N-adic expansion.)}$$

Thus, the largest of $\psi(a)$ will not get cancelled and thus, $\phi(f)$ looks like

$$c_\alpha x_n^{\psi(\alpha)} + \underbrace{\cdots}_{\text{lower powers}} \quad \text{with } 0 \neq c_\alpha \in K$$

of x_n and other x_i

Thus, we are done. ☒

If $|K| = \infty$, then ϕ can be chosen to be a linear change of coordinates.

Thm. (Noetherian Normalisation Theorem)
$R = K[\theta_1, \ldots, \theta_n]$ is an affine K-algebra.
Then, $\exists$ alg. indep. elements $z_1, \ldots, z_d \in R$ s.t.

$$\begin{array}{c} R \\ \Big| \ \text{integral extension} \\ K[z_1, \ldots, z_d] = S \end{array}$$

In particular, R is a finite S-module.

Thus, any finite affine K-alg is an int. extension of a polynomial ring.

Proof. Induct on n. $n = 0$: $R = K$, take $S = K$.
Let $n \geq 1$. Assume result true for $< n$.

$R = K[\theta_1, \ldots, \theta_n]$.

If $\theta_1, \ldots, \theta_n$ are alg. indep., take $z_i = \theta_i$. Done.
Assume not.
Then, $\exists F(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n]$ s.t. $F(\theta_1, \ldots, \theta_n) = 0$.

By previous result, $\exists \phi \in \mathrm{Aut}\, K[x_1, \ldots, x_n]$ s.t.

$$\phi(F) = aX_n^r + g_1 X_n^{r-1} + \cdots + g_r$$

$a \in K \setminus \{0\}$ and $g_1, \ldots, g_r \in K[x_1, \ldots, x_{n-1}]$.

$$F(\theta_1, \ldots, \theta_n) = 0 \Rightarrow \phi(F(\theta_1, \ldots, \theta_n)) = 0$$

$$\parallel$$

$$F(\underbrace{\phi(\theta_1)}_{\theta_1'}, \ldots, \underbrace{\phi(\theta_{n-1})}_{\theta_{n-1}'}, \underbrace{\phi(\theta_n)}_{=\theta_n})$$

$$0 = a\theta_n^r + g_1 \theta_r^{r-1} + \cdots + g_r.$$

Divide by a to get θ_n is int/ $K[\theta_1', \ldots, \theta_{n-1}']$.

By induction,

$$\begin{array}{c} K[\theta_1, \ldots, \theta_n] \\ \Big| \text{ int} \\ K[\theta_1', \ldots, \theta_{n-1}'] \\ \Big| \text{ int} \\ K[z_1, \ldots, z_d]. \end{array} \Bigg) \text{ int}$$

Lecture 17 (16-03-2021)

16 March 2021 14:01

Recall:

(1) HSN. $k = \bar{k}$. $\mathcal{I}(\mathcal{Z}(I)) = \sqrt{I}$.

$\{$ radical ideals of $K[x_1, \ldots, x_n]\} \longleftrightarrow \{$alg. subsets of $\mathbb{A}^n_K\}$.

(2) NNL. Let K be any field.

$R = K[r_1, \ldots, r_n]$.

$\exists$ alg indep $z_1, \ldots, z_d \in R$ s.t.

$$\begin{array}{c} R \\ \Big| \text{ int. ext.} \\ K[z_1, \ldots, z_d] \end{array}$$

(3) Zariski's lemma: $R = \dfrac{\overbrace{K[x_1, \ldots, x_n]}^{=S}}{m}$, where $m \in \operatorname{mSpec} S$.

$$0 \longrightarrow K \xhookrightarrow{i} K[x_1, \ldots, x_n] \xrightarrow{\pi} S/m \longrightarrow 0.$$

$\ker \pi \circ i \neq K$. Thus, $\ker(\pi \circ i) = 0$.

$K \subset S/m$ is an alg. ext. $\longleftarrow$ ZL

We had proven the above before HWN. Now, we prove it again using NNL.

Proof. $R = S/m$ is an affine k-alg.

By NNL, $\exists z_1, \ldots, z_d \in R$: $\underbrace{K[z_1, \ldots, z_d]}_{\text{poly ring}} \underbrace{\subset}_{\text{int extension}} \underbrace{R}_{\text{field}}$

By our earlier result, $k[z_1, \ldots, z_d]$ must be a field.

Thus, $d = 0$ and R/K is an integral and hence, Thus, $d = 0$ and R/K is an integral and hence, alg. extension. ∎

Cor. Let $\varphi : R \longrightarrow S$, (ring homo.) R and S are affine K-alg.
Let $\mathfrak{m} \in \operatorname{mSpec} S$. Then, $\varphi^{-1}(\mathfrak{m})$ is also maximal.

Proof. $K \hookrightarrow R \xrightarrow{\varphi} S \xrightarrow{\pi} S/\mathfrak{m} \longrightarrow 0$

$\varphi^{-1}(\mathfrak{m}) = \ker(\pi \circ \varphi)$

$$\begin{tikzcd}
K \arrow[r, hook] \arrow[d] & R/\varphi^{-1}(\mathfrak{m}) \arrow[r, hook] \arrow[d] & S/\mathfrak{m} \arrow[d] \\
\text{field} & \text{domain} & \text{field}
\end{tikzcd}$$

$$\underbrace{\text{field} \qquad\qquad \text{field}}_{\text{alg. extension by ZL}}$$

An integral domain between alg. extension of fields has to be a field. Thus, $\varphi^{-1}(\mathfrak{m})$ is a maximal ideal. ∎

Cor. Let R be an affine K-algebra and $I \trianglelefteq R$ an ideal.
Then,

$$\sqrt{I} = \bigcap_{I \subseteq \mathfrak{m} \in \operatorname{mSpec} R} \mathfrak{m}.$$

(In general, $\sqrt{I} = \bigcap_{I \subseteq \mathfrak{p} \in \operatorname{Spec} R} \mathfrak{p}$.)

In particular $(I = 0)$, $\mathcal{N}(R) = \operatorname{Jac}(R)$.

Proof. $(\subseteq)$ is clear.

$(\supseteq)$ If $g \notin \sqrt{I}$, then $\exists$ a maximal ideal
$\mathfrak{m} \supseteq I$ s.t. $g \notin \mathfrak{m}$. $(*)$

Thus, $g \notin \bigcap_{\substack{I \subseteq \mathfrak{m} \\ \mathfrak{m} \text{ max}}} \mathfrak{m}$.

(*) $g \notin \sqrt{I} \Rightarrow g^n \notin I \quad \forall n \in \mathbb{N}$

Let $W = \{1, g, g^2, \ldots\}$.

Then, $I \cap W = \phi$.

Thus, IR_g is a proper ideal of R_g.

$\therefore \exists$ a maximal ideal of R_g, say PR_g s.t.

$IR_g \subset PR_g$.

Note $R_g = R[\frac{1}{g}]$ is an affine K-algebra. (Since R was.)

$$\begin{array}{c} R_g \\ | \\ R \end{array}$$

The contraction of PR_g to R is a maximal ideal.

But $P = PR_g \cap R$. Thus, $I \subset P \leftarrow$ maximal

and $PR_g \neq R_g \Rightarrow g \notin P$. ∎

(Elementary) Dimension Theory of Affine K-algebras

Krull dimension of a commutative ring

Def^n. A saturated chain of prime ideals is a chain $p_0 \subset p_1 \subset \cdots \subset p_n$ such that

$\nexists\, q \in \mathrm{Spec}(R)$ s.t. $p_i \subsetneq q \subsetneq p_{i+1}$ for some $i \in \{0, \ldots, n-1\}$.

The length of the above chain is n.

$$\dim(R) := \sup \{ n : \exists \text{ a saturated chain of prime ideals of length } n \}.$$

Remark $\dim(R) = \infty$ is possible even if R is Noetherian

We shall (much) later that if R is Noe. and $\mathfrak{p} = \langle r_1, \dots, r_n \rangle$ is prime, then $\dim (R_{\mathfrak{p}}) \leq n$.

Thus, $\mathrm{spec}(R)$ satisfies d.c.c.

Ex. ① If R is Artinian, then all primes are maximal.

Thus, $\dim R = 0$.

$\dim \text{field} = 0$.

② $\dim \mathbb{Z} = 1$. (Only saturated chains are $0 \subset p\mathbb{Z}$ for p prime.)

(3) Same reasoning as above shows $\dim K[x] = 1$. (K field)

(4) If R is a PID which is not a field, then $\dim(R) = 1$.

Propⁿ. $R \subset S$ integral extension.

(1) $\dim R = \dim S$.

(2) if $I \subsetneq S$, then $\dim(S/I) = \dim(R/I \cap R)$.

(3) Suppose S is integral and R normal.

Let $Q \in \mathrm{Spec}\, S$.

Then, $\underset{\text{height of } Q}{\underset{\|}{\dim S_Q}} = \dim R_{Q \cap R}$.

(Proof. We did in tutorial.)

Thm. Let R be an affine domain over a field K.

Let $z_1, \dots, z_d \in R$ be alg. indep. and $\underset{S}{\underset{\|}{K[z_1, \dots, z_d]}} \subset R$ be an integral extension. (Exists by NNL.)

$K[z_1, \dots, z_d]$: UFD, normal

Then,

(1) $\dim R = d = \dim K[z_1, \dots, z_d]$.

(2) any maximal saturated chain of prime ideals in R has length d.

(The above shows uniqueness of d.)

Proof. Since $S \subset R$ is an int. ext, $\dim(S) = \dim(R)$.

Thus, we only need to show $\dim(S) = d$.

We prove this via induction on d.

Note the chain

$$(0) \subset (z_1) \subset (z_1, z_2) \subset \cdots \subset (z_1, \ldots, z_d)$$

is saturated. Thus, $\dim(S) \geq d$.

$d = 1$: $\dim K[z_1] = 1$. ✓

$d \geq 2$: Let

$$0 \subset P_1 \subset \cdots \subset P_n \quad \text{be a saturated}$$

chain of prime ideals in S.

The above implies that $P_1 = \langle f \rangle$ for $f \in S$ irreducible.

$$S/P_1 = S/\langle f \rangle \quad ; \quad f \in K[z_1, \ldots, z_d].$$

$\exists$ change of variable s.t. we can assume

$$f = a z_d^n + g_1 z_d^{n-1} + \cdots + g_n,$$

$$K \ni a \neq 0, \quad g_1, \ldots, g_n \in K[z_1, \ldots, z_{d-1}].$$

Note $\langle f \rangle = \langle f/a \rangle$. Thus, we may assume $a = 1$.

$$\frac{K[z_1, \ldots, z_d]}{\langle f \rangle} \quad \leftarrow \text{affine domain}$$

$$\Big| \quad \text{int ext}$$

$$K[z_1, \ldots, z_{d-1}]$$

By induction, $\dim K[z_1, \ldots, z_{d-1}] = d-1$.

Thus, $\dim(S/P_1) = \dim(S/(f)) = d-1$.

By induction, we may also assume that all sat. chain in $k[z_1, \ldots, z_{d-1}]$ have length $d-1$.

(*) $0 \subset P_1 \subset \cdots \subset P_n$ mod (f)

$0 \subset P_2/(f) \subset \cdots \subset P_n/(f)$ → saturated

Thus, if (*) was saturated, so is the below one and thus, $n-1 = d-1$ or $n = d$. ∎

Lecture 18 (23-03-2021)

23 March 2021 13:58

Graded Rings and Graded Modules

Preparation for Dimension Theory of Modules over local rings and graded modules over graded rings

Goals: (i) Artin – Rees lemma

- R Noetherian, M f.g. R module, $I \subsetneq R$ an ideal.

$N \leq M$ submodule.

We have the submodules $\{I^n M\}$.

This gives a filtration $\{I^n M \cap N\}$ of submodules of N.

Then, $\exists\, n \in \mathbb{N}$ s.t.

$$(I^{n+1} M) \cap N = I(I^n M \cap N).$$

(2) Krull's Intersection Theorem.

(i) Let (R, m) be Noetherian local and $I \subseteq m$ and ideal.

Then $\bigcap_{n=1}^{\infty} I^n = (0)$.

(ii) If R is a Noetherian domain.

If $I \neq R$ is an ideal, then $\bigcap_{n=1}^{\infty} I^n = (0)$.

Prototype: Let K be a field and $X_1, \dots, X_n$ be indeterminates.

Let $g_1, \dots, g_n$ be homogeneous polynomials in $R = K[X_1, \dots, X_n]$.

$I = (g_1, \dots, g_n)$. Then, $S = R/I$ is an example of a graded ring.

More general:

Let R be any commutative ring. Let $\{R_n : n = 0, 1, \dots\}$ be a sequence of additive subgroups s.t.

$$R = \bigoplus_{n=0}^{\infty} R_n \quad \text{and} \quad R_n R_m \subseteq R_{n+m} \quad \forall n, m.$$

Then, R is called a graded ring. Any $x \in R_n$ is called homogeneous of degree n.

In the earlier case, let $R = K[X_1, \dots, X_r]$ and

R_n = K vector space generated by monomials of degree n in $X_1, \dots, X_r$.

$$\dim_K (R_n) = \binom{n+r-1}{n} \quad \text{and} \quad R = \bigoplus_{n=0}^{\infty} R_n.$$

Note that $R_n R_m \subseteq R_{n+m}$ $\forall n, m$ implies $R_0 R_0 \subseteq R_0$.
Thus, R_0 is a subring of R. (Check $1_R \in R_0$.)
Moreover, $R_0 R_n \subseteq R_n$ $\Rightarrow$ each R_n is an R_0 - module.

Take $I \subseteq K[X_1, \dots, X_n]$.
$\hookrightarrow$ homogenous poly. generate this. (Diff. degrees allowed.)
Then, R/I is also a graded ring. (Will show in a while.)

Will show: $I = \bigoplus_{n=0}^{\infty} (I \cap R_n)$,

$$R/I = \frac{\bigoplus R_n}{\bigoplus I \cap R_n} = \bigoplus_{n=0}^{\infty} R_n / I \cap R_n.$$

Def^n. An $\overset{\text{graded}}{R}$-module M is called graded if

$$M = \bigoplus_{n \in \mathbb{Z}} M_n, \qquad M_n \to \text{additive subgroup}$$

$$\text{and} \quad R_m M_n \subseteq M_{n+m} \quad \forall n, m.$$

(M is called a graded $R = \bigoplus_{n \geq 0} R_n$ - module.)

Remark. Here we have said $n \in \mathbb{Z}$. Can be $\mathbb{N}$ or $\mathbb{N}_0$ also.

When is a submodule N of M called a graded submodule?
N is called graded if it is generated by homogeneous elements of M.

An aside:
$K[x_1, \dots, x_n]$
$$\deg(x_1^{a_1} \cdots x_n^{a_n}) := \underset{\overset{\shortparallel}{a}}{(a_1, \dots, a_n)} \in \mathbb{N}_0^n.$$

$$R_a := K x_1^{a_1} \cdots x_n^{a_n}$$

$R = \bigoplus_{a \in \mathbb{N}_0^n} R_a$. Here, R is $\mathbb{N}_0^n$ - graded.

(Grading can be done over semigroups, et cetera)

Characterisation of graded submodules.

Thm. Consider $R = \bigoplus_{n \geq 0} R_n$, $M = \bigoplus_{n \geq 0} M_n \longrightarrow$ graded R-module.

$N \leq M$ submodule. TFAE:

(1) N is a graded R-submodule of M.

(2) $N = \bigoplus_{n=0}^{\infty} (N \cap M_n)$. (So it is a graded module with this grading)

(3) If $y \in N$ and $y = y_0 + \cdots + y_n$, where $y_i \in M_i$, then $y_i \in N$ $\forall i$.

Proof (2) $\Rightarrow$ (1). $N = \bigoplus_{n=0}^{\infty} (N \cap M_n)$.

To show: N is generated by homogeneous elements.

Let $y \in N$. Then, $y = y_0 + \cdots + y_d$, where $y_i \in M_i \cap N$.

If N has y as a generator, then y can be replaced where y_i. (These are in N by assumption.)

(1) $\Rightarrow$ (3) Let N be generated by homogeneous elements $y \in N$.

$N = \sum_{i \in \Lambda} n_i$, $n_i \in M_{d_i}$.

Suppose $y = y_0 + y_1 + \cdots + y_d \in N$.

TST: each $y_i \in N$.

$$y = \sum n_i a_i \qquad a_i \in R$$
$$= y_0 + y_1 + \cdots + y_d$$

The above eq^n is in M. But M is direct sum of M_n.
Thus every element is a unique sum of homogeneous elts.

Write $a_i = \sum a_{i_k}$; $a_{i_k} \in R_k$.

Thus, $y_j = \sum n_i \, a_{i_{j-1}} \in N$.

(3) $\Rightarrow$ (2) Let $n \in N \subset M = \bigoplus_{n \geq 0} M_n$

$n = n_0 + n_1 + \cdots + n_r$; $n_i \in M_i$.

But $n_i \in N$. Thus, $N = \bigoplus_{n \geq 0} (N \cap M_n)$. $\boxtimes$

Characterisation of Noetherian graded rings.

Thm. $R = \bigoplus_{n \geq 0} R_n$ is Noetherian $\Leftrightarrow$ R_0 is a Noetherian ring and R is a f.g. R_0-algebra, i.e., $R = R_0[r_1, \ldots, r_n]$.

Proof. ($\Rightarrow$) $R = \bigoplus_{n=0}^{\infty} R_n$ Noetherian.

Let $\pi_0 : R \twoheadrightarrow R_0$ be the projection map.
π_0 is a ring homomorphism.

$\ker(\pi_0) = R_1 \oplus R_2 \oplus \cdots = R^+$
$=$ ideal gen. by elements of +ve degree.

Thus, $R_0 \simeq R/R_+$. $\therefore$ R_0 is a Noetherian ring.

R_+ is a f.g. ideal. (Since R is Noe.)

$R_+ = (f_1, f_2, \ldots, f_r)$; $f_i \in R_{d_i}$, $d_i \geq 1$.
(If f_i not homog., replace with homog. gen.)

Claim. $R = R_0[f_1, \ldots, f_r] =: S$.

Proof. Apply induction on n to show $R_n \subset S$.
$R_0 \subset S$. ✓
Assume $R_0, \ldots, R_n \subseteq S$.
$y \in R_{n+1} \subseteq R_+$. $y = \sum_{d_i \geq n+1} f_i a_i$, $a_i \in R$.

$$y = \sum f_i \, a_{i,\, n+1-d_i}$$

$n+1-d_i < n+1$

$\therefore \; a_{i,\, n+1-d_i} \in S$, by ind

Thus, $y \in S$.

($\Leftarrow$) Follows from Hilbert-Basis Theorem. ◪

The ideal $R_+ = \sum_{i \geq 1} R_i$ is called irrelevant ideal.

(Reasons due to projective geometry.)

R comm. ring.

$F = \{I_n\}_{n=0}^{\infty}$. $\quad R = I_0 \supset I_1 \supset I_2 \supset \cdots$ ideals

$$I_n I_m \subseteq I_{m+n}.$$

Let t be an indeterminate.

$$\mathcal{R}(F) := \bigoplus_{n=0}^{\infty} I_n t^n \subset R[t].$$

$\|$

Rees ring of F

The condition $I_n I_m \subseteq I_{n+m}$ gives $\mathcal{R}(F) = \bigoplus_{n \geq 0} I_n t^n$ is a graded ring.

$$\mathcal{R}(F)_0 = R, \quad \mathcal{R}(F)_1 = I_1 t, \quad \ldots$$

Let $I \subset R$ be an ideal. Then, we have the filtration

$$F : \quad R \supset I \supset I^2 \supset \cdots$$

$\mathcal{R}(F) =$ Rees ring of I.

$$= \bigoplus_{n \geq 0} I^n t^n = \left\{ \sum a_i t^i : a_i \in I^i \right\}.$$

Let M be an R-module. Let

$$M = M_0 \supset M_1 \supset \cdots$$ be a filtration of submodules.

Let $I \subseteq R$. The above filtration is called an I-filtration if

$$I M_n \subseteq M_{n+1} \quad \forall\, n$$

$\bigoplus_{n \geq 0} M_n t^n \subseteq M[t]$ is a graded $\mathcal{R}(I)$-module since

$$I^n M_m \subseteq I_{n+m} \quad \forall\, n, m.$$

$\bigoplus I^n t^n = \mathcal{R}(I)$

$\bigoplus I^n M t^n = \mathcal{R}_I(M)$

I-stable filtration. $\{M_n\}$ is called I-stable if

$$M_n = I M_{n-1} \quad \forall\, n \gg 0.$$

<u>Example</u> $\{I^n M\}_{n \geq 0}$ is an I-stable filtration.

Prop^n Suppose R is a Noetherian and M a f.g. R-module. Let $I \subsetneq R$ be an ideal and $\{M_n\}$ is an I-filtration of submodules of M. That is,

$$G: \quad M = M_0 \supset M_1 \supset M_2 \supset \cdots$$

with $I M_n \subset M_{n+1}$.

$\mathcal{R}(G) := \bigoplus M_n t^n$ = Rees-module of G.

Then, G is I-stable iff $\mathcal{R}(G)$ is a f.g. $\mathcal{R}(I)$-module.

$$\mathcal{R}(I) = \bigoplus_{n \geq 0} I^n t^n$$

Lecture 19 (26-03-2021)

26 March 2021 13:59

Preliminaries about I-stable filtrations

$\{I_n\}_{n=0}^{\infty}$ $\quad R = I_0 \supset I_1 \supset I_2 \supset \cdots$ ideals

$I_n I_m \subseteq I_{n+m} \quad \forall n, m \geq 0.$

Standard examples:

① $\{I^n\}_{n=0}^{\infty}$

② $p \to$ prime ideal

$p^{(n)} = p^n R_p \cap R$

$= p$-primary component of p^n if R is Noetherian.

$p^{(n)} p^{(m)} \subseteq p^{(n+m)} \quad \forall m, n \geq 0$

Rees ring of $F = \{I_n\}_{n=0}^{\infty}$

$$\mathcal{R}(F) = \left\{ \sum_{i=0}^{N} a_i t^i : a_i \in I_i \right\}$$

$$= \bigoplus_{n \geq 0} I_n t^n \subseteq R[t].$$

Let M be an R-module.

$G = \{M_n\}_{n=0}^{\infty}$: $\quad M = M_0 \supset M_1 \supset M_2 \supset \cdots$ submodules.

G is called F-compatible if $I_n M_m \subseteq I_{n+m} \quad \forall m, n \geq 0.$

Example. $\{I^n M\}_{n \geq 0}$ is $\{I^n\}_{n \geq 0}$-compatible.

Then, $\mathcal{R}(G) = \bigoplus_{n \geq 0} M_n t^n \subseteq M[t]$ is an $\mathcal{R}(F)$-graded module.

Q. When is $R(G)$ a f.g. $R(F)$ – module?

$G = \{M_n\}$ is stable I– stable if
$IM_n = M_{n+1} \quad \forall n \geq n_0.$

$M = M_0 \supset M_1 \supset \cdots \supset M_{n_0} \supset IM_{n_0} \supset I^2 M_{n_0} \supset \cdots$

$R(G) = M \oplus M_1 t \oplus \cdots \oplus M_{n_0} t^{n_0} \oplus IM_{n_0} t^{n_0+1} \oplus \cdots$

$F = \{I^n\}_{n \geq 0}.$

But $R(G)$ is an $R(I) = R(F)$ – module.
If R is Noe. and M f.g.

Then,
$R(I)\langle M \oplus M_1 t \oplus \cdots \oplus M_{n_0} t^{n_0} \rangle = R(G).$
$\therefore$ $R(G)$ is a f.g. $R(I)$ – module.

Note $R(I) = R \oplus \underbrace{It \oplus I^2 t^2}_{\text{generated by } (a_1 t, \ldots, a_r t)} \oplus \cdots$
where $I = (a_1, \ldots, a_r)$.

By our previous result, $R(I)$ is Noetherian.

Thm R– Noe, M– f.g., $G \to \{I^n\}$ -compatible
Then,
$R(G)$ is a f.g. $R(I)$ - module $\Leftrightarrow$ G is I– stable.

Proof. Above, we proved $(\Rightarrow)$

Conversely, let $R(G) = \bigoplus_{n \geq 0} M_n t^n$ be a f.g. $R(I)$ - module.

1. G is I-stable.

$$H_1 := M \oplus M_1 t \oplus \underbrace{I M_1}_{\subseteq M_2} t^2 \oplus \underbrace{I^2 M_1}_{\subseteq M_3} t^3 \oplus \cdots$$

$H_1 \subseteq R(G)$ is a submodule.

$$H_2 := M \oplus M_1 t \oplus M_2 t^2 \oplus I M_2 t^3 \oplus I^2 M_2 t^4 \oplus \cdots$$

Then, $H_1 \subseteq H_2 \subseteq R(G)$ are submodules. In fact, they are graded submodules.

Prop^n. (Generalised Artin Rees Lemma)

R - Noetherian, M - f.g.

$\{M_n\}_{n \geq 0}$ an I-stable filtration.

$N \leq M$ a submodule.

Then, $\{M_n \cap N\}$ is I-stable.

Proof. Let $H = \{M_n \cap N\}$. H is compatible with $\{I^n\}$-filtration since $\{M_n\}$ is.

$$R(G) = \bigoplus M_n t^n$$
$$\cup\!\!|$$
$$R(H) = \bigoplus (M_n \cap N)\, t^n$$

Both are $R(I)$-modules. G is I-stable.

Thus, $R(G)$ is f.g. $R(I)$-module and hence, Noe.

Hence, $R(H)$ is Noe. and in particular, f.g. $R(I)$-mod.

Hence, $R(H)$ is Noe. and in particular, f.g. $R(I)$-mod.

$\Rightarrow$ $H = \{M_n \cap N\}$ is I-stable. ∎

Cor. (Classical Artin-Rees Lemma)

$R \to$ Noe, M a f.g. R-module, $I \neq R$ ideal, $N \subset M$ submodule

Then, $\exists\, k \geq 0$ s.t. $\forall\, n \geq k$,

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

Proof. Take $G = \{I^n M\} \to$ I-stable

Then, $H = \{I^n M \cap N\} \to$ induced filtration.

$\Rightarrow$ H is I-stable

$\Rightarrow$ $\exists k$ s.t. $\forall n \geq k$:

$$I^{n+1} M \cap N = I(I^n M \cap N)$$

$$= I^2(I^{n-1} M \cap N) = \cdots = I^{n-k}(I^k M^n \cap N). ∎$$

Thm. (Krull Intersection Theorem)

R — Noetherian ring, $I \neq R$ ideal, M is f.g.

$\bigcap_{n=1}^{\infty} I^n M = N \leq M$ submodule

Then,

(a) $\exists\, a \in I$ s.t. $(1+a)N = 0$,

(b) If $I \subseteq Jac(R)$, then $N = \bigcap_{n=1}^{\infty} I^n M = 0$,

(c) If R is Noe. domain, then $\bigcap I^n = 0$,

(d) If $I \subsetneq R$, (R, m) local Noe. ring, then $\bigcap I^n M = 0$.

Proof. (a) $\Rightarrow$ (b) since $1+a \in Units(R)$.

(a) $\Rightarrow$ (c) since $1+a \neq 0$ is a n.z.d.

(b) $\Rightarrow$ (d) since $Jac(R) = m$.

Thus, it suffices to prove (a).

$G = \{I^n M\}$ is I-stable

Thus, $\mathcal{S}$ is $H = \{I^n M \cap N\}$.

Thus, $\underbrace{I^n M \cap N}_{=N} = I(\underbrace{I^{n-1} M \cap N}_{=N}) \quad \forall n \geq n_0$

$\Rightarrow N = IN$. Note that N is f.g. Thus, NAK gives (a). ☒

Example. KIT need not be true if non-Noetherian.

$R = C^\infty(\mathbb{R})$

$+$ and $\cdot$ pointwise. R is not Noetherian.

$$\varphi : R \longrightarrow \mathbb{R}$$
$$f \longmapsto f(0)$$

$$R/\ker\varphi \cong \mathbb{R}$$

Consider $x = id_{\mathbb{R}} \in R$.

Then, $\ker\varphi = (x) = m$ and $\bigcap m^n \neq 0$.

$$t \mapsto \begin{cases} e^{-1/t^2} & , t \neq 0 \\ 0 & ; t = 0 \end{cases}$$ is in $\bigcap m^n$.

Structure of graded primes and graded maximal ideals

$$R = \bigoplus_{n=0}^{\infty} R_n$$

...

$\cup\!|$
$I \to$ ideal (not necessarily homogeneous)

Recall. $I = \bigoplus (I \cap R_n) \iff I$ is gen'd by homogeneous elts.

$I^* := \bigoplus_{n \geq 0} (I \cap R_n)$.

Propⁿ. (1) If p is a prime in R, then p^* is also prime.
(2) maximal graded ideals $= \{ m \oplus R_1 \oplus R_2 \oplus \cdots \mid m \in \mathrm{mSpec}(R_0) \}$.

(3) R is Noe. graded ring, $M = \bigoplus_{n \geq 0} M_n$ graded.

Then, $p \in \mathrm{Ass}(M)$ is graded and $p = \mathrm{ann}(x)$ for x homogeneous.

Prop. (1) If non-zero homo elts of $R = \bigoplus R_n$ are non-zero-divisors, then R is a domain.

(2) Let $P \neq R$ be a graded ideal.
If $\forall$ homog. $a, b \in R$: $a, b \notin P \Rightarrow ab \notin P$,
then P is a prime ideal.

(3) p prime $\Rightarrow p^*$ prime.

(4) Any minimal prime of R is a graded ideal.

Proof. (1) Take $a, b \neq 0$ in R.

$a = \underset{\neq 0}{a_i} + a_{i+1} + \cdots + a_r$

$a_k, b_k \in R_k$

$b = \underset{\neq 0}{b_j} + b_{j+1} + \cdots + b_s$

higher degree, can't cancel

$ab = a_i b_j + (\cdots) \neq 0$.

$\neq 0$, by assumption

(2) We show R/p is an integral domain.

$R = \bigoplus_{n \geq 0} R_n$, $\quad p = \bigoplus_{n \geq 0} (p \cap R_n) = \bigoplus_{n \geq 0} p_n$.

$R/p \cong \bigoplus_{n \geq 0} R_n/p_n$ is a graded ring.

$0 \neq b + p_n \qquad b \in R_n \setminus p_n \Rightarrow b \notin p$

$0 \neq a + p_m \qquad a \in R_m \setminus p_m \Rightarrow a \notin p$

$\Rightarrow ab \notin p$, by assumption.

$\Rightarrow (a + p_n)(b + p_m) = ab + p_{n+m} \neq 0$.

$\Rightarrow R/p$ is an integral domain. $\therefore p$ is prime.

(c) Let $p \in \operatorname{Spec}(R)$.

$p^* \subset p$.

a, b homo., $ab \in p^* \subset p$ prime

$\Rightarrow a$ or $b \in p \Rightarrow a$ or $b \in p^*$.

since a, b homog.

(d) $p^* \subsetneq p \Rightarrow p^* = p$, by previous. ☒

Structure of maximal ideals that are graded ideals of $R = \bigoplus R_n$.

Obs. ① $R = \bigoplus_{n=0}^{\infty} R_n$. Suppose R is a field. $1 \in R_0$.

If $0 \neq x \in R_n$, $n \neq 0$, then $\exists y \neq 0$ s.t. $xy = 1$.

We get $x(\underbrace{y_0}_{} + y_1 + \cdots + y_m) = \underbrace{1}_{\deg 0}$, with $\deg > 0$.

Thus, $R_n = 0 \ \forall n \geq 1$ and R_0 is a field.

② Let M be a maximal ideal which is also graded.

$$M = \bigoplus_{n \geq 0} I_n .$$

Then, $R/M = \bigoplus \frac{R_n}{I_n}$ is a graded field.

Thus, $I_n = R_n \ \forall n \geq 1$ and I_0 is maximal.

(Converse clearly true.)

③ Let $I = \bigoplus I_n = \bigoplus I \cap R_n$ be a proper graded ideal.

$\Rightarrow R/I \neq 0.$ $\quad R/I = \frac{R_0}{I_0} \oplus \frac{R_1}{I_1} \oplus \cdots$

$1 \notin I \Rightarrow 1 \notin I_0 \Rightarrow \frac{R_0}{I_0} \neq 0 \Rightarrow I_0 \subsetneq R_0.$

$\Rightarrow \exists m \in \mathrm{mSpec}(R_0)$ s.t. $m \supseteq I_0.$

$m \oplus R_+ \supseteq I.$

Lecture 20 (30-03-2021)

30 March 2021 13:59

Dimension Theory of Finite Modules over Noetherian Local Rings

- Affine algebra $R = K[x_1, \dots, x_n]/I$. ← domain

  $\mathrm{trdeg}_K(Q(R)) = \dim(R)$ ← had seen

Notations:

$R \to$ Noetherian ring

$M \to$ finite R-module

$\mathrm{Supp}(M) = V(\mathrm{ann}(M)) \overset{\text{homeo.}}{\cong} \mathrm{Spec}(R/\mathrm{ann}(M))$

$= \{ \mathfrak{p} \in \mathrm{Spec}(R) \mid M_{\mathfrak{p}} \neq 0 \}$

Closed subset of $X = \mathrm{Spec}(R)$, in Zariski topology.

Topological def^n of dim

$= \sup \{ n \mid \exists$ a chain of irr. closed subsets of $\mathrm{supp}(M)$ of length $n \}$

Turns out to be same as ① Krull dim $(M) := \dim(R/\mathrm{ann}(M))$.

usual Krull dim.

Q. How to find $\dim(M)$?

Def^n. (Chevalley dimension of a module)

② $= \inf \{ n \mid \exists x_1, \dots, x_n \in R$ s.t. $\ell(M/(x_1, \dots, x_n)M) < \infty \}$.

(If $\ell(M) < \infty$, then the above is 0.)

Def^n (Using Hilbert polynomials)

③ Let $(R, \mathfrak{m})$ be a Noetherian local ring, M is a finite R-module.

$$\mathcal{F}: \quad R \supset \mathfrak{m} \supset \mathfrak{m}^2 \supset \mathfrak{m}^3 \supset \cdots$$

$\mathfrak{m}$-adic filtration of R.

$$\mathcal{R}(\mathcal{F}) = \bigoplus_{n=0}^{\infty} \mathfrak{m}^n t^n =: \mathcal{R}(\mathfrak{m}).$$

$\mathcal{F}$ is $\mathfrak{m}$-stable $\Rightarrow$ $\mathcal{R}(\mathfrak{m})$ is a Noetherian ring.

$$\mathcal{G}: \quad M \supset \mathfrak{m}M \supset \mathfrak{m}^2 M \supset \cdots. \qquad \mathcal{R}(\mathcal{G}) = \bigoplus_{n=0}^{\infty} \mathfrak{m}^n M t^n$$

$\mathcal{G}$ is $\mathfrak{m}$-stable $\Rightarrow$ $\mathcal{R}(\mathcal{G})$ is a f.g. graded module over $\mathcal{R}(\mathfrak{m})$.

$$\mathfrak{m}\mathcal{R}(\mathcal{F}) = \mathfrak{m} \oplus \mathfrak{m}^2 t \oplus \mathfrak{m}^3 t^2 \oplus \cdots$$

$$\frac{\mathcal{R}(\mathcal{F})}{\mathfrak{m}\mathcal{R}(\mathcal{F})} = \bigoplus_{n=0}^{\infty} \mathfrak{m}^n / \mathfrak{m}^{n+1} = gr_{\mathfrak{m}}(R)$$

$$\frac{\mathcal{R}(\mathcal{G})}{\mathfrak{m}\mathcal{R}(\mathcal{G})} = \bigoplus_{n=0}^{\infty} \frac{\mathfrak{m}^n M}{\mathfrak{m}^{n+1} M} = gr_{\mathfrak{m}}(M).$$

$gr_{\mathfrak{m}}(M)$ is a finite $gr_{\mathfrak{m}}(R)$-module.

(Recall: $\mathrm{Supp}(M/IM) = \mathrm{Supp}(M) \cap V(I)$.)

$$\frac{\mathfrak{m}^n M}{\mathfrak{m}^{n+1}} \subset \frac{M}{\mathfrak{m}^{n+1} M}$$

$$\mathrm{Supp}\left(\frac{\mathfrak{m}^n M}{\mathfrak{m}^{n+1} M}\right) \subset \mathrm{Supp}\left(M/\mathfrak{m}^{n+1}M\right)$$

$\uparrow$ v.space over $k = R/\mathfrak{m}$

$$= \mathrm{Supp}(M) \cap V(\mathfrak{m})$$
$$= \mathrm{Supp}(M) \cap \{\mathfrak{m}\}$$
$$= \{\mathfrak{m}\}$$

$$\Rightarrow \quad l\left(\mathfrak{m}^n M/\mathfrak{m}^{n+1}M\right) < \infty$$
$$\|$$
$$H_M(\mathfrak{m}, n) = \text{Hilbert function of } \mathrm{gr}_{\mathfrak{m}}(M).$$

We will show that

$$n \longmapsto \dim_k\left(\frac{\mathfrak{m}^n M}{\mathfrak{m}^{n+1} M}\right) \text{ is given}$$

by a polynomial $P_M(x)$ $\forall n \gg 0$.

That is,

$$P_M(n) = \dim_k\left(\frac{\mathfrak{m}^n M}{\mathfrak{m}^{n+1} M}\right) \quad \forall n \gg 0.$$

$\uparrow$ Hilbert poly. of M

Thm. $\dim(M) = 1 + \deg(P_M(x))$.

Thus, we have ①, ②, ③ which all capture the same dimension.

Prop^n. Let $R = \bigoplus_{n=0}^{\infty} R_n$ graded Noetherian ring.

$$= R_0[x_1, \dots, x_r]$$

R_0: Noe. $x_1, \dots, x_r$: homogeneous, degree d_i

(If all $d_i = 1$, we call R standard.)

Noe. ↓ homogeneous, degree d_i (we call R standard.)

$M = \bigoplus_{n \in \mathbb{Z}} M_n$ graded R-module f.g.

Then,

(1) $M_n = 0 \quad \forall \; n \ll 0$.

(2) Each M_n is a f.g. R_0-module.

(3) If R_0 is Artinian, then $\ell_{R_0}(M_n) < \infty \quad \forall n$.

Proof. Notation : $M_{\geq r} := \bigoplus_{n=r}^{\infty} M_n$. $M_{\geq r}$ is a graded R-submodule.

(1) $M_{\geq 0} \subseteq M_{\geq -1} \subseteq M_{\geq -2} \subseteq \cdots$

is an a.c. of submodules. Since M is Noe.,

$\exists \; p$ s.t. $M_{-p} = M_{-p-1} = M_{-p-2} = \cdots$.

$\Rightarrow M_n = 0 \quad \forall \; n \leq -(1+p)$.

(2) $M_{\geq n} = M_n \oplus M_{n+1} \oplus \cdots$

$M_{\geq n+1} = M_{n+1} \oplus \cdots$

$\Rightarrow \dfrac{M_{\geq n}}{M_{\geq n+1}} \cong M_n$.

OTOH, $M_{\geq n}$ is a f.g. R-submodule.

$\therefore M_n$ is a f.g. R-module

In this case, $R_+ \subseteq \operatorname{ann}(M_n)$. Thus,

M_n is a f.g. $R/R_+ \cong R_0$ - module.

(3) Let R_0 be Artinian. Then, M_n is f.g. R_0-module, by ②. Thus, R_0 is Art. + Noe.; thus, it has finite length. ∎

$H(M,\lambda)$ = Hilbert series of M

$$= \sum_{n\in\mathbb{Z}} \ell_{R_0}(M_n)\,\lambda^n.$$

We will show that $H(M,\lambda)$ is a rational function.

Example. $K[x_1,\dots,x_d] = R$

$\dim(R) = d.$

$$R = \bigoplus_{n=0} R_n. \qquad R_n = k\text{-vector space of homogeneous polynomials of degree } n.$$

basis: monomials of degree n (in d vars.)

$$H(R,\lambda) = \sum_{n=0}^{\infty} \dim_K(R_n)\,\lambda^n$$

(This dimension is $\binom{d-1+n}{n}$ but we don't assume that.)

Notation $M = \bigoplus_{n\in\mathbb{Z}} M_n$. $M(r)$ is defined as $M(r)_n = M_{r+n}$.

$M(r)$ is a graded R-algebra.

Claim. $$H(R,\lambda) = \frac{1}{(1-\lambda)^d}.$$

Proof. $d=1$: matches.

Assume for $d-1$.

$$0 \longrightarrow R(-1) \xrightarrow{x_d} R \longrightarrow R/x_dR = k[x_1,\dots,x_{d-1}]$$

Exact seq. of R-modules.

Def^n $M = \bigoplus M_n \xrightarrow{f} \bigoplus N_n = N$ is called a homomorphism of graded R-modules if $f(M_n) \subseteq N_n \ \forall n$.
(f is an R-module homomorphism to begin with.)

Thus,

$$0 \to R(-1)_n \to R_n \to (R/x_d R)_n \to 0$$

exact seq. of v. spaces.

Using rank-nullity, we get

$$\dim(R_n) = \dim(R(-1)_n) + \dim((R/x_d R)_n).$$

$$\Rightarrow H(R,\lambda) = H(R(-1),\lambda) + H(R/x_d R, \lambda)$$

$$= \sum_{n=0}^{\infty} \dim(R_{n-1})\lambda^n + H(K[x_1,\dots,x_{d-1}],\lambda)$$

$$= \lambda H(R,\lambda) + \frac{1}{(1-\lambda)^{d-1}}$$

$$\Rightarrow H(R,\lambda) = \frac{1}{(1-\lambda)^d}.$$ ∎

d is the order of the pole at 1.

Ex. $\dim_K(R_n) = \binom{d-1+n}{d-1} \quad \forall n.$

(Hilbert-Serre Theorem)

Thm. $$H(M,\lambda) = \sum_{n\in\mathbb{Z}} l_{R_0}(M_n)\lambda^n = \frac{f(\lambda,\lambda^{-1})}{\prod_{i=1}^{r}(1-\lambda^{d_i})}$$

where $R = R_0[x_1,\dots,x_r]$ (not necessarily indeterminates)

$\deg(x_i) = d_i \geq 1$.

$f(\lambda,\lambda^{-1}) \in \mathbb{Z}[\lambda,\lambda^{-1}]$. ($M$ f.g. over R. $R_0 \to$ Artinian.)

Proof. Induction on r.

$r = 0 \Rightarrow R = R_0$ Artinian ring

$M = \bigoplus_{n \in \mathbb{Z}} M_n$ f.g. R_0 - module.

$\Rightarrow l_{R_0}(M) < \infty \Rightarrow M$ has finitely many non-zero.
So we get a polynomial.

Assume for $r-1$.

$R = R_0[x_1, \dots, x_r]$; $d_r \geq 1$.

$$0 \to K \longrightarrow R(-d_r) \xrightarrow{\mu_{x_r}} R \to C \longrightarrow 0$$ exact

kernel cokernel

sequence of Noe. graded R-modules.

Note that $x_r K = 0$.
Thus, K is an $R_0[x_1, \dots, x_{r-1}]$ module.
Same for C.

$$H(K, \lambda) - H(R(-d_r), \lambda) + H(R, \lambda) - H(C, \lambda) = 0$$

$$H(R, \lambda)(1 - \lambda^{d_r}) = H(C, \lambda) - H(K, \lambda)$$

induction hypothesis

$$= \frac{f(\lambda, \lambda^{-1})}{(1 - \lambda^{d_1}) \cdots (1 - \lambda^{d_{r-1}})}$$

$$\Rightarrow H(R, \lambda) = \frac{f(\lambda, \lambda^{-1})}{(1 - \lambda^{d_1}) \cdots (1 - \lambda^{d_r})}$$ ☒

(We proved the above for R, the proof for a general M goes in the same way.)

Now, if $d_i = 1 \ \forall i$, then

$$H(M, \lambda) = \frac{f(\lambda, \lambda^{-1})}{(1 - \lambda)^r}$$

$$\sum_{n \in \mathbb{Z}} l_{R_0}(M_n) \lambda^n = f(\lambda, \lambda^{-1}) \sum_{n=0}^{\infty} \binom{r-1+n}{n} \lambda^n$$

Equate co-efficient of λ^n $\forall\ n \gg 0$.

$$l_{R_0}(M_n) = \text{co-eff of } \lambda^n \text{ in } \left(f_{-p}\lambda^{-p} + \dots f_q \lambda^q\right)\left(\sum_{n \geq 0} \binom{r-1+n}{n} \lambda^n\right)$$

$$= \binom{n-p+r-1}{n} f_{-p} + f_{-p+1} \binom{n-(p-1)+r-1}{n} + \dots f_q \left(\quad \right).$$

↳ Polynomial in n with rational co-efficients.

Lecture 21 (06-04-2021)

06 April 2021 13:59

Dimension Theorem for finite modules over local rings

(1) Krull dimension of M $= \dim(\mathrm{Supp}(M))$ ← topological dim
$= \dim(R/\mathrm{ann}\, M)$

(2) Chevalley dimension $= \inf\{ n \mid \exists\, x_1,\dots,x_n \in \mathfrak{m}$ and $\ell_R\left(M/(x_1,\dots,x_n)M\right) < \infty \}$
$= c(M)$

(3) Hilbert - Samuel polynomials

Let I be $\mathfrak{m}$-primary

$R \supset I \supset I^2 \supset \cdots$ $\quad R(I) = \bigoplus_{n=0}^{\infty} I^n t^n$

Noetherian graded ring

$R(I)_+$ = ideal generated by +ve degree
$= 0 \oplus It \oplus I^2t^2 \oplus \cdots$

$$\frac{R(I)}{I R(I)} = \frac{\bigoplus I^n t^n}{\bigoplus I^{n+1} t^n} \cong \bigoplus_{n=0}^{\infty} I^n/I^{n+1}$$
$$= gr_I(R)$$

I-stable filtration

$M \supset IM \supset I^2M \supset \cdots = \mathcal{F}$

$\bigoplus_{n=0}^{\infty} I^n M t^n = R(\mathcal{F})$ is a f.g $R(I)$-module

Ex $\bigoplus_{n=0}^{\infty} I^nM/I^{n+1}M = gr_I(M)$ is a f.g graded module

over $gr_I(R)$

In fact, if $M = Rm_1 + \cdots + Rm_r$, then put $n_1 = m_1 + IM$

Then, $n_1, \ldots, n_r$ generated $gr_I(M)$ over $gr_I(R)$

$gr_I(R)$ is a Noe. ring to begin with. Thus, $gr_I(M)$ is a Noe module

I is m-primary $\quad Supp\left(\frac{I^nM}{I^{n+1}M}\right) \subseteq Supp\left(\frac{M}{I^{n+1}M}\right)$

$$= Supp(M) \cap V(I^{n+1})$$

$$= Supp(M) \cap V(I) = \{m\}$$

$$\ell\left(I^nM / I^{n+1}M\right), \quad \ell(M/I^nM) < \infty$$

Hilbert-Samuel function of M w.r.t. I

$n \mapsto H_I(M, n) = \ell(M/I^nM) : \mathbb{N} \to \mathbb{N}$

is a polynomial for $n >> 0$

$P_I(M, n)$ = Hilbert-Samuel polynomial of M w.r.t. I

$\forall$ m-primary ideals I, J $\quad \deg P_I(M,n) = \deg P_J(M,n)$

Thus, the degree depends only on M, which we denote by $d(M)$

Thm (Dimension Theorem) $\quad \dim(M) = c(M) = d(M)$.

Preparation

Setup: (R, m) local, M f.g. R-module, $M \neq 0$

Prop^n Let I be an m-primary ideal.

Let $M = M_0 \supset M_1 \supset M_2 \supset \cdots$ be any I-good filtration on M. (That is, $IM_i \subseteq M_{i+1}$ $\forall i$, and $\exists p$ s.t. $I^nM_p = M_{p+n}$ $\forall n \geq 1$)

Let $f: \mathbb{N} \to \mathbb{N}$ be $f(n) = \ell(M/M_n)$

$H_I(M, n) = \ell(M/I^nM) \rightsquigarrow P_I(M, n)$

Then, $P_I(M, n) = f(n) + \overset{\text{polynomial}}{p(n)}$ $\forall\ n \gg 0$

$P_I(M, n)$ and $f(n)$ have same degree and leading co-efficients and hence, $\deg p(n) < \deg P_I(M, n)$

Moreover, $p(n)$ has +ve leading co-eff

Proof

$\mathcal{F} = \{M_n\}$ is I-stable

$gr(\mathcal{F}) = \bigoplus_{n=0}^{\infty} M_n/M_{n+1}$ is f.g over $gr_I(R)$

Hilbert-Serre theorem $\Rightarrow$ $\ell(M_n/M_{n+1})$ is a polynomial for $n \gg 0$

$\Downarrow$ Ex

$$\sum_{i=0}^{n} \ell(M_i/M_{i+1}) \text{ is also a polynomial, } n \gg 0$$

$$\parallel$$

$$\ell(M/M_{n+1})$$

$\Rightarrow$ $\underset{\underset{f(n)}{\parallel}}{\ell(M/M_n)}$ is a polynomial for $n \gg 0$

$\ell(M/I^nM) = P_I(M, n)$

$\{M_n\}$ is I-stable $\Rightarrow \exists$ $M = M_0 \supset M_1 \supset \cdots \supset M_p \supset IM_p \supset I^2M_p \supset \cdots$

$\Rightarrow$ $M_n = I^{n-p}M_p$ $\forall\ n \geq p$

$I^nM \subset M_n \subset I^{n-p}M \subset M$

$$\ell(M/I^nM) \geq \ell(M/M_n) \geq \ell(M/I^{n-p}M)$$

$$P_I(M,n) \geq f(n) \geq P_I(M, n-p)$$

All of these are polynomials (Again, Hilbert-Serre.)

By Sandwich Theorem for limits, it follows that $P_I(M, -)$ and f have same degree and leading co-efficients

The fact about the difference $p(n) = P_I(M,n) - f(n) \geq 0$ now follows ⊠

$$\sqrt{I} = \mathfrak{m} \Rightarrow \mathfrak{m}^r \subset I \subset \mathfrak{m}$$
$$\Rightarrow \mathfrak{m}^{rn} \subset I^n \subset \mathfrak{m}^n$$
$$\Rightarrow \mathfrak{m}^{rn} M \subset I^n M \subset \mathfrak{m}^n M$$

$$\begin{array}{ccccc} \ell(M/\mathfrak{m}^{rn}M) & \geq & \ell(M/I^nM) & \geq & \ell(M/\mathfrak{m}^n M) \\ \| & & \| & & \| \\ g_M(rn) & \geq & P_I(M,n) & \geq & g_M(n) \end{array}$$

Thus, the degree of $P_I(M, -)$ is that of g_M and hence, is independent of $\mathfrak{m}$-primary ideal chosen

---

Prop^n Let us consider the exact sequence

$$0 \to N \to M \to Q \to 0$$

of finite R-modules

Then, $d(M) = \max\{d(N), d(Q)\}$ ↳ Consequence of following

Thm Let I be any $\mathfrak{m}$-primary ideal

(a) $P_I(M,n) = P_I(N,n) + P_I(Q,n) - \ell(n)$,

where $\ell(n) \in \mathbb{Q}[n]$ and $\deg \ell(n) < \deg P_I(N,n)$

(b) $d(M) = \max\{d(N), d(Q)\}$

Clearly, (a) $\Rightarrow$ (b). We prove (a)

Proof.

M

$|$

$N + I^n M$

(Assume $N \hookrightarrow M$ and $Q = M/N$)

$P_I(M,n) \leftarrow H_I(M,n)$

$\|$

$\ell(M/I^nM)$

$$\begin{tikzcd}
 & N+I^nM \arrow[dl, dash] \arrow[dr, dash] & \\
N \arrow[dr, dash] & & I^nM \arrow[dl, dash] \\
 & N \cap I^n M \arrow[d, dash] & \\
 & I^n N &
\end{tikzcd}$$

$P_I(M,n) \leftsquigarrow H_I(M,n)$
$\quad\quad\quad\quad \shortparallel$
$\quad\quad\quad \ell(M/I^nM)$

$$\ell(M/I^nM) = \left[\ell\left(\frac{M}{N+I^nM}\right)\right] + \ell\left(\frac{N+I^nM}{I^nM}\right)$$

$$= \left[\ell\left(\frac{M/N}{I^n(M/N)}\right)\right] + \ell\left(\frac{N+I^nM}{I^nM}\right)$$

$$= \ell\left(\frac{Q}{I^nQ}\right) + \ell\left(\frac{N}{N\cap I^nM}\right) \quad \text{diamond iso}$$

$$= \ell\left(\frac{Q}{I^nQ}\right) + \ell\left(\frac{N}{I^nN}\right) - \ell\left(\underbrace{\frac{N\cap I^nM}{I^nN}}_{\ell(n)}\right)$$

$$P_I(M,n) = P_I(Q,n) + P_I(N,n) - \ell(n)$$

Note that $\{I^nN\}$ and $\underbrace{\{I^nM\cap N\}}_{\text{(By general Artin-Rees.)}}$ are both I-stable.

By the earlier theorem, (a) now follows $\boxtimes$

Thm Let R be Noetherian, local and M a finite R module.
Then, $\dim(M) = c(M) = d(M)$

Proof (1) $\dim(M) \le d(M)$ [In particular, $\dim(M) < \infty$ is also shown.]

(2) $d(M) \le c(M)$

(3) $c(M) \le \dim(M)$.

(1) TS. $\dim(M) \le d(M)$. Apply induction on $d(M)$.

Suppose $d(M) = 0$

Thus, $\deg P_m(M,n) = 0$

$H_m(M,n)$ is a constant for large n $\exists n_0 \in \mathbb{N}$ s.t

Thus, $H_m(M,n) = H(M,n+1) = \quad \forall n \ge n_0$

$\quad\quad\quad\quad \shortparallel \quad\quad\quad\quad\quad \shortparallel$

Thus, $H_m(M, n) = H(M, n+1) = \quad \forall n \geq n_0$
$\| \qquad \|$
$\ell(M/m^nM) \qquad \ell(M/m^{n+1}M)$

$$\left[\begin{array}{c} M \\ | \\ m^nM \\ | \\ m^{n+1}M \end{array}\right]$$

Thus, $m^nM = m^{n+1}M$.

By NAK, $m^n M = 0$ or $m^n \subseteq \mathrm{ann}(M) \subseteq m$

Thus, $\sqrt{\mathrm{ann}(M)} = m$. Thus, $V(\mathrm{ann}(M)) = \{m\}$
$\|$
$\mathrm{Supp}(M)$

$\mathrm{Supp}(M) = \{m\} \Rightarrow R/\mathrm{ann}(M)$ is an Artinian ring

$\Rightarrow \dim(R/\mathrm{ann}(M)) = 0$
$\|$
$\dim(M)$

$\therefore \dim(M) \leq d(M)$ when $d(M) = 0$

Now, assume $d(M) > 0$. If $\dim(M) = 0$, we are done

Suppose $\dim(M) \geq 1$. Thus, $\mathrm{Supp}(M)$ has a chain of primes of length ≥ 1

Let $p_0 \subsetneq p_1 \subsetneq \quad \subsetneq p_r$ be a chain, $(r \geq 1)$ $p_i \in \mathrm{Supp}(M)$

We may assume p_0 is minimal in support.

Thus, $p_0 \in \mathrm{Ass}_R(M)$ and hence, $R/p_0 \hookrightarrow M$.

$0 \to R/p_0 \to M$
$\cong \quad \cup$
N

Let $N \hookrightarrow M$ be iso to R/p_0

Pick $x \in p_1 \setminus p_0$. Then, x is a n.z.d on the int domain R/p_0

Thus, x is a n.z.d. on N

$0 \to N \xrightarrow{x} N \to N/xN \to 0$ is a ses

By the second technical result,

$$P_m(N, n) = P_m(N, n) + P_m(N/xN, n) - \ell(n)$$

where $\deg(\ell(n)) < \deg(P_m(N, n))$.

$\Rightarrow \quad P_m(N/xN, y) = \ell(n)$

$\Rightarrow \quad \underbrace{d(N/xN) < d(N)}_{\text{by above}} \quad \underbrace{\leq d(M)}_{\text{use } 0 \to N \to M \to M/N \to 0}$

Note $\quad \operatorname{Supp}(N/xN) = \operatorname{Supp}(N) \cap V(x)$

Note $p_1 \subset \cdots \subset p_r$ is a chain in the above

$p_1 \in \operatorname{Supp}(N)$ since $N \cong R/p_0$

and thus, $p_2, \ldots, p_r \in \operatorname{Supp}(N)$ $\quad x \in p_1 \subset \cdots \subset p_r$

$\Downarrow$

$p_1, \ldots, p_r \in V(x)$

Thus, $\quad r-1 \leq d(N/xN) \leq d(M) - 1$

$\Rightarrow \quad r \leq d(M) \quad \Rightarrow \quad \dim(M) \leq d(M)$. $\boxtimes$

r was length of arbit chain

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

Let $x_1, \ldots, x_r \in m$ and $\ell\left(M/(x_1, \ldots, x_r)M\right) < \infty$

We show $d(M) \leq r$ and thus,

$$d(M) \leq \underbrace{\inf\{r \mid \ell(M/(x_1, \ldots, x_r)M) < \infty\}}_{= c(M)}$$

Let $J = (x_1, \ldots, x_r) \quad \ell(M/JM) < \infty$.

$\Rightarrow \quad \operatorname{supp}(M/JM) = \{m\} = \operatorname{Supp}(M) \cap V(J)$

$\Rightarrow \quad \operatorname{supp}(M/J^nM) = \operatorname{supp}(M) \cap V(J^n) = \{m\}$

$H_J(M, n) = \ell(M / J^n M)$

$\bigoplus J^n M / J^{n+1} M$ is f g graded module over $\bigoplus J^n / J^{n+1} \simeq R/J [\bar{x}_1, \ , \bar{x}_r]$

$\bar{x}_1 = x_1 + J^2 \in J/J^2$

By Hilbert - Serre : $\deg \ell\left(J^n M / J^{n+1} M \right) \leq r-1$

$\Rightarrow \deg P_J(M, n) \leq r$

$\qquad \qquad \qquad \qquad \qquad \parallel$

$\qquad \qquad \qquad \qquad \quad d(M)$

Lecture 22 (09-04-2021)

09 April 2021 14:00

(3) TS: $c(M) \leq \dim(M)$

Let $d = \dim(M)$. We induct on d

- $d=0$. Then, $\dim(R/\mathrm{ann}(M)) = 0$. $R/\mathrm{ann}(M)$ was Noetherian to begin with $\therefore$ $R/\mathrm{ann}(M)$ is Artinian

  Now, M is Artinian (over $R/\mathrm{ann}(M)$ and hence, R)

  Thus, $c(M) = 0$

- Assume $d \geq 1$

  Let $P_0 \subsetneq \cdots \subsetneq P_d$ be a chain of primes

  Thus, P_0 is minimal prime in $\mathrm{Supp}(M)$

  $\Rightarrow P_0 \in \min(\mathrm{Ass}(M))$

  Pick $x \in \underbrace{P_1 \setminus \bigcup_{p \in \min(\mathrm{Ass}(M))} p}_{\text{non-empty, prime avoidance}}$ (P_1 is not min'l)

Claim $\dim(M/xM) = d-1$

Proof. $\mathrm{Supp}(M/xM) = \mathrm{Supp}(M) \cap V(x)$

By construction, $p_1, \ldots, p_d \in \mathrm{Supp}(M/xM)$

$\Rightarrow d-1 \leq \dim(M/xM)$

OTOH, if $q_0 \subsetneq \cdots \subsetneq q_d$ is a chain in $\mathrm{Supp}(M/xM)$, then pick a min'l prime p' contained in q_0 (from $\mathrm{Supp}(M)$)

$p' \neq q_0$ since $x \notin p'$

But $p' \subsetneq q_0 \subsetneq \cdots \subsetneq q_d$ $\longrightarrow$ $d+1$ primes in $\mathrm{Supp}(M)$. $\rightarrow\leftarrow$ ∎

Now, we show that $c(M/xM) \geq c(M) - 1$

Suppose $t = c(M/xM) \Rightarrow \exists\, y_1, \ldots, y_t \in \mathfrak{m}$ s.t.

$$\ell\left(\underbrace{\frac{M/xM}{(y_1, \ldots, y_t)\, M/xM}}\right) < \infty$$

$$\ell\left(\frac{\overbrace{\ldots}}{\underbrace{(y_1, \ldots, y_t) M/_{xM}}_{\cong \frac{M}{(x, y_1, \ldots, y_t)M}}}\right) < \infty$$

Thus, $t+1 \geq c(M) \Rightarrow c(M/xM) \geq c(M) - 1$

By ind^n, $\underset{\underset{c(M)-1}{\vee\!\mid}}{c(M/xM)} \leq \dim(M/xM) = \dim(M) - 1$ ∎

Krull's altitude theorem

Cor 1 Let $I = (a_1, \ldots, a_n)$ be an ideal of a Noetherian ring R

Let p be a minimal prime containing I

Then, $ht(P) \leq n$

Thus, any prime ideal has finite height and every desc chain of prime ideals stabilises

altitude of I = $\max\{ht(P) \quad p \in \min(Ass(R/I))\}$

$ht(I) = \min\{ht(P) \quad p \in \min(Ass(R/I))\}$

Proof

$$R \longrightarrow R_p$$

$$I \subset p \qquad \underbrace{IR_p \subset pR_p}_{\substack{\text{no prime in between} \\ pR_p \text{ is max'l}}}$$

Thus, $R_p/_{IR_p}$ is an Artinian local ring

$\therefore \quad \ell\left(\frac{R_p}{(a_1, \ldots, a_n)R_p}\right) < \infty$

$\Rightarrow \quad ht(P) = \dim(R_p) = c(R_p) \leq n$ ∎

Cor 2 Krull's Principal Ideal Theorem: $ht(aR) \leq 1$.

Cor 3. Let R be a Noetherian ring and x an indeterminate.

Then, $\dim(R[x]) = \dim(R) + 1$

In particular, if k is a field and $x_1, \ldots, x_n$ are indeterminates, then $\dim(k[x_1, \ldots, x_n]) = n$

Proof

$$\begin{array}{cccccccccc} R[x] & P_0[x] & \subsetneq & P_1[x] & \subsetneq & \cdots & \subsetneq & P_r[x] & \subsetneq & (P_r, x) \\ | & | & & & & & & & & \downarrow \text{prime} \\ R & P_0 & \subsetneq & P_1 & \subsetneq & \cdot & \subsetneq & P_r & & \end{array}$$

$\therefore \dim(R[x]) \geq \dim(R) + 1$. [Including if $\dim(R) = 1$.]

$R[x]$ is Noetherian. If M is a maximal ideal of $R[x]$, then $ht(M) < \infty$, by Altitude theorem.

$$\begin{array}{cccc} R[x] & M & MW^{-1}R[x] & \\ | & | & | & \\ R & N = R \cap M & NR_N & W = R \setminus N \end{array}$$

$ht(N) = ht(NR_N)$ we wish to show

$ht(MW^{-1}R[x]) \leq ht(NR_N)$

We may R is local

Let $\dim(R) = d$ By dim thm, $\exists x_1, \ldots, x_d \in N$ s.t

$N = \sqrt{(x_1, \ldots, x_d)}$.

Thus, $N^t \subseteq (x_1, \ldots, x_d)$.

(Chevalley dim $R/(x_1, \ldots, x_d)$ is Art. local $\Downarrow$ $(x_1, \ldots, x_d) \to$ only prime containing is N)

$$R[x] \longrightarrow \frac{R[x]}{N[x]} \supseteq \frac{M}{N[x]} = (\bar{f}(x))$$

$\frac{R[x]}{N[x]} \cong (R/N)[x] \supseteq$ PID $\quad$ field $\leftarrow R/N$

$\Rightarrow M = (N, f)$

$N^t \subseteq (x_1, \ldots, x_d)$.

$M = (N, f) \Rightarrow M^t \subset (N^t, f) \subset (x_1, \ldots, x_d, f)$

Suppose P is a prime ideal containing $\mathfrak{I}$

$M^t \subseteq (x_1, \ldots, x_d, f) \subset P \subset R[x]$

$\Rightarrow \quad m^t \subseteq P \Rightarrow m \subseteq P \Rightarrow m = P$

$(x_1, , x_d, f)$ is m-primary

$\Rightarrow ht(m) \leq d+1$ ☒

Def^n $c(M) = d$ Suppose $x_1, , x_d \in R$ are st

$$\ell\left(M \big/ (x_1, , x_d)M \right) < \infty$$

Such a set of elements is called a system of parameters for M

If $M = R$. $q = (x_1, , x_d) \subset m$ is m-primary

Any m-primary ideal requires at least d generators

Conversely, if $(x_1, , x_d)$ is m-primary, then $x_1, , x_d$ is a SOP for R.

Thm (R, m) local ring dim d

Let $x_1, . , x_d$ SOP for R.

$k \cong R/m$

$$\underbrace{k \hookrightarrow R \longrightarrow R/m}_{\text{isomorphs}}$$

Then, $x_1, , x_d$ are alg indep over k

Example $R = k[[x, y]]$ local

$I = (x^2, xy) = (x) \cap (x^2, y)$

$I \subseteq (x) \subseteq m = (x, y)$

$\dim(R/I) = 1$

$$(R/I)\big/(\bar{y})(R/I) = \frac{R}{(x^2, xy, y)} = \frac{R}{(x^2, y)} \quad \text{Artinian}$$

$\Rightarrow \bar{y}$ is a SOP in R/I

(Note $\bar{y}$ is a zero divisor on R/I.)

$k[\bar{y}]$ is polynomial ring however, by the thm

Before we prove the theorem, a lemma

Prop Let (R, m) be a d-dim Ne. local ring

$q = (x_1, \ , x_d)$, is m-primary. Let

$f(t_1, \ , t_d) \in R[\underbrace{t_1, \ , t_d}_{\text{indet}}]$ be

homogeneous of degree s and $f(x_1, \ , x_d) \in q^{s+1}$

Then, $f \in m[t_1, \ , t_d]$

Proof $\alpha \cdot R/q \ [t_1, \ , t_d] \longrightarrow \bigoplus_{n=0}^{\infty} q^n/q^{n+1} = gr_q(R)$

$\bar{f}(t_1, \ , t_d) \longmapsto \bar{f}(\bar{x}_1, \ , \bar{x}_d) \in q^s/q^{s+1}$

$\bar{x}_1 = x_1 + q^2$

But, we are given $f(x_1, .. , x_d) \in q^{s+1}$

Thus, $\bar{f}(t_1, \ , t_d) \in \ker \alpha$

deg s homogeneous

$$T = \frac{R/q \ [t_1, \ , t_d]}{\bar{f}(t_1, .. , t_d)} \xrightarrow{\bar{\alpha}} gr_q(R)$$

$\bar{\alpha}(T_n) = q^n/q^{n+1}$

$\ell(q^n/q^{n+1}) \leq \ell(T_n)$

$\underbrace{R/q}_{\text{Artin local}} \ [t_1, .. , t_d]$.

Let S be an Artinian local ring. $S[t_1, .., t_n]$
$\cup$
$f \to s$ homogeneous

$$l\left(\frac{S[t_1,..,t_d]}{(f)}\right)_n = \text{polynomial for } n \gg 0$$

$$0 \to T(-s) \xrightarrow{f} T \longrightarrow T/(f) \to 0$$

If some coeff of f is not in m_S then it is a unit $\Rightarrow f$ is a n.z.d.
$\Downarrow$
above is exact

$$l((T/f)_n) \le l(T_n) - l(T_{n-s}) \searrow \deg\ d-2$$
$$\qquad\qquad \| \qquad\qquad\qquad \|$$
$$\qquad\qquad l(S)\binom{d-1+n}{d-1} \qquad (\ )$$

$$l(q^n/q^{n+1}) \le \deg\ d-2 \text{ poly for } n \gg 0$$
$\to \leftarrow$

Proof of thm Let $f(T_1, .., T_d) \in k[T_1, .., T_d]$
$f(x_1, .., x_d) = 0$

$f = f_s + f_{s+1} + \quad$ f_i are homg, $f_s \neq 0$

$0 = (x_1, , x_d) = f_s(x_1, , x_d) + f_{s+1}(x_1, , x_d) +$

$\Rightarrow f_s(x_1, , x_d) = -[f_{s+1}(x_1, , x_d) + \ +] \in q^{s+1}$

$\Rightarrow f_s \in m[t_1, , t_d]$
$\Rightarrow f_s = 0$ in $k[T_1, , T_d]$
$\Rightarrow x_1, ., x_d$ are alg indep $/ k$