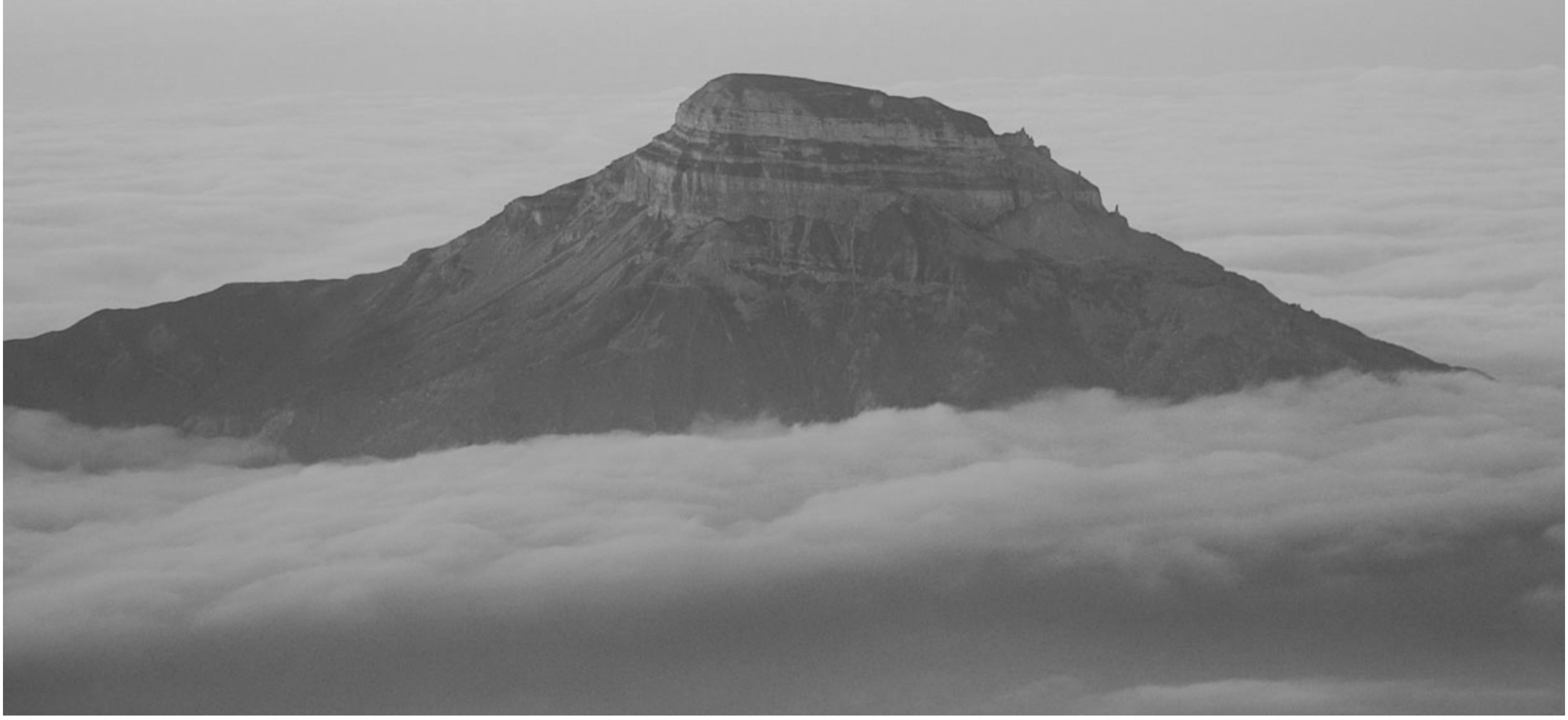
交代



日期: / §1.1 Preliminaries

§1.1.1. 常用的例子:

eg1. $\mathcal{U} \underset{open}{\subseteq} \mathbb{R}^n (/\mathbb{C}^n)$

$C^0(\mathcal{U}) = \{f: \mathcal{U} \to \mathbb{R} \mid f \text{ cont.}\}$.

$C^\infty(\mathcal{U}) = \{\text{smooth } f: \mathcal{U} \to \mathbb{R}\}$.

$\mathcal{O}(V) = \{\text{holomorphic } f: V \to \mathbb{C}\}$. (? 全纯函数.)

Core Thm1: (Hilbert Nulstellensats). (代数学基本定理的推广).

A maximal idea $I \subseteq \mathbb{C}[z_1, \cdots, z_n]$ is of the form:

$I = (z_1 - a_1, \cdots, z_n - a_n)$. for some $a_1, \cdots, a_n \in \mathbb{C}$.

注: 即 $\{\text{maximal ideals of } \mathbb{C}[z_1, \cdots, z_n]\} \xleftrightarrow{1:1} \mathbb{C}^n$.

$(z_1 - a_1, \cdots, z_n - a_n) \longleftrightarrow (a_1, \cdots, a_n)$

且此对应保持其结构.

eg.2. X compact Hausdorff space. Atiyah Ex26.

$X \xrightarrow{1:1} \{\text{maximal ideals of } C^0(X)\}$.

$x \in X \longmapsto \underset{max.\ ideal}{m_x = \{f \in C^0(X) \mid f(x) = 0\} \subseteq C^0(X)}$

§1.1.2. Ideal 的由来:

(理想 - 理想数)

日期:　　/

$\gcd(a,b)=d \iff$ ① $(a)\subseteq(d)$, $(b)\subseteq(d)$.

② $(a)\subseteq(c)$, $(b)\subseteq(c)$, $\Rightarrow (d)\subseteq(c)$.

$\iff$ (d) 是 min ideal s.t. $(a)\cup(b)\subseteq(d)$.

$\iff (a)+(b)=(d)$.

($I+J$ 是包含 $I\cup J$ 的最小理想) (当从代数整数环且非PID时,不存在gcd)

(注意. $\mathbb{Z}[\zeta_p]$ 大多非PID $\Rightarrow$ gcd 可能不存在)

* gcd在理想意义下总是存在. $\gcd(a,b)=(a)+(b)$.

$\Rightarrow$ "理想数", 认为 $(a)+(b)$ 也是一个"数", 将"数域""扩充".

$\Rightarrow$ 从而 gcd 等总是存在. 可以进行传统的数学操作.

理想的运算: ① $I+J$ ($\rightsquigarrow (a)+(b)=(\gcd(a,b))$).

② $I\cdot J \triangleq (\{ij \mid i\in I, j\in J\})$ ($\rightsquigarrow (a)\cdot(b)=(ab)$).

③ $I\cap J$ ($\rightsquigarrow (a)\cap(b)=(\mathrm{lcm}(a,b))$)

④ × ($\rightsquigarrow ?=(a+b)$) (理想是一种乘法性的工具)

(现代数论分为 $\begin{cases}\text{加法数论}\\ \text{乘法数论}\end{cases}$)

§1.1.3. $\mathbb{Z}$ 同余的推广:

① 素数　　④ 唯一因子分解.

② CRT

③ 二次互反律 $\rightarrow$?

日期: /

eg. CRT:

- Classical. If $a_1,\cdots,a_m\in\mathbb{Z}$ 两两互素, 则

$$\mathbb{Z}/a_1\cdots a_m\mathbb{Z}\cong(\mathbb{Z}/a_1\mathbb{Z})\times\cdots\times(\mathbb{Z}/a_m\mathbb{Z}).$$

- General: ideals $I_1,\cdots,I_m\subseteq R$. (def: I与J coprime: $I+J=R$).

$$\phi: R\to R/I_1\times\cdots\times R/I_m$$

thm: ① if $I_i+I_j=R$, $\forall i,j$. 则 $\prod_{i=1}^{n}I_i=\bigcap_{i=1}^{n}I_i$

② ϕ 满射 $\Leftrightarrow I_i+I_j=R,\ \forall i,j$.

③ $\mathrm{Ker}(\phi)=\bigcap_{i=1}^{n}I_i$.

§1.1.4. Core Thm2:

① $\mathbb{Z}[\zeta_p]$ 不是 UFD. if $p>19$. (但是∃ unique finite decomposition)

② [Kummer]. $\forall I\trianglelefteq\mathbb{Z}[\zeta_p]$ ideal. (此处的$\mathbb{Z}[\zeta_p]$可推广至Dedkind 环)

∃唯一分解 $I=\beta_1^{r_1}\cdots\beta_m^{r_m}$, where β_i 为 prime ideal.

(Rmk: If $I=(a)$ principle, $\beta_1,\cdots,\beta_m$ may not be 数.)

注意: 本课程中讨论的环 R, 不特别指出时即交换环.

日期: /

§1.2. Ideals & Solving Equations.

$f_1, f_2, \cdots, f_r \in \mathbb{Z}[x_1, \cdots, x_n]$, def $V_R(f_1, \cdots, f_r) = \{x \in R^n \mid f_1(x) = \cdots = f_r(x) = 0\}$. 丢番图方程.

Problem: what is $V(f_1, \cdots, f_r)$?

Fix $z \in R^n$, define $\varphi_z : \mathbb{Z}[x_1, \cdots, x_n] \longrightarrow R$. (即赋值映射).

$$x_i \longmapsto z_i.$$

则 $f(z) = 0 \iff f \in \ker(\varphi_z)$.

Cor: $f_1(z) = \cdots = f_r(z) = 0 \iff (f_1, \cdots, f_r) \subset \ker(\varphi_z)$.

Grothendieck:

解方程时要考虑所有域.

对 $R = k$ field: (证定义见后).

Fact1: $\ker(\varphi_z)$ is prime. (证良定义).

Fact2: let $\mathfrak{p} \subset \mathbb{Z}[x_1, \cdots, x_n]$ prime ideal. 则 $\exists$ field k 和

$z = (z_1, \cdots, z_n) \in k^n$ st $\ker(\varphi_z) = \mathfrak{p}$. (证满射).

def: Assume $k \overset{\phi}{\hookrightarrow} K$.

denote $(z_1, \cdots, z_n; k) \sim (w_1, \cdots, w_n; K)$.

if $\phi(z_i) = w_i$, $i = 1, \cdots, n$

$\Rightarrow$ 考虑不同域中同解的刻画 (证良定义).

$(\iff$

$$\begin{tikzcd} \mathbb{Z}[x_1, \cdots, x_n] \arrow[r, "\varphi_z"] \arrow[dr, "\varphi_w"'] & k \arrow[d, hook, "\phi"] \\ & K \end{tikzcd}$$

$\Rightarrow \ker(\varphi_z) = \ker(\varphi_w)$.)

Fact3: $(z_1, \cdots, z_n; k) \sim (w_1, \cdots, w_n; K) \iff \ker(\varphi_z) = \ker(\varphi_w)$. (证单射 & ~良定义)

日期: /

Fix $\mathbb{Z}[x_1,\cdots,x_n]$.

$$\bigcup_{k=\text{field}} k^n/\sim \xrightarrow{\Phi(1:1)} \{\text{primes in } \mathbb{Z}[x_1,\cdots,x_n]\}.$$

$$(z_1,\cdots,z_n;k) \longmapsto \operatorname{Ker}(\varphi_z)$$

Cor: $\rightsquigarrow \underbrace{\bigcup_k V_k(f_1,\cdots,f_n)/\sim}$ $\xrightarrow{1:1} \{\text{prime } p \text{ in } \mathbb{Z}[x_1,\cdots,x_n] \text{ s.t. } (f_1,\cdots,f_r)\subset p\}.$

$\downarrow 1:1$

$\underbrace{\{\text{prime } p \text{ in } \mathbb{Z}[x_1,\cdots,x_n]/(f_1,\cdots,f_r)\}}.$

Def: let R a ring. denote:

$\operatorname{Spec}(R)=\{\text{prime ideals of } R\}$. $\Rightarrow$ 反映了 $f_1,\cdots,f_r$ 所有可能的解.

Problem1: When is $\operatorname{Spec}(R)\neq\emptyset$. ?

Problem2: What is the structure of $\operatorname{Spec}(R)$?

Prop: $\forall$ ring $R\neq 0$ contains a maximal ideal. (Zorn 引理).

(特别地. $\operatorname{Spec}(R)\neq\emptyset$ if $R\neq 0$.)

Cor: Equations $f_1(x)=\cdots=f_r(x)=0$ 在某 field 中有解.

$\Leftrightarrow \operatorname{Spec}(\mathbb{Z}[x_1,\cdots,x_n]/(f_1,\cdots,f_r))\neq\emptyset$.

$\Leftrightarrow (f_1,\cdots,f_r)\neq\mathbb{Z}[x_1,\cdots,x_n]$.

Thm (Weak Hilbert Nullstenllensate). ☆

$k=\bar{k}$. let $f_1,\cdots,f_r\in k[x_1,\cdots,x_n]$.

日期: /

then $f_1(x)=\cdots=f_r(x)=0$ has solution in K.

$\Leftrightarrow (f_1,\cdots,f_r) \subsetneq k[x_1,\cdots,x_n]$.

Fix k, $z=(z_1,\cdots,z_n)\in k^n$. define $\varphi_z: k[x_1,\cdots,x_n]\to k$.

Prop: $\ker(\varphi_z)=(x_1-z_1,\cdots,x_n-z_n)$. is maximal.

pf: ① $(x_1-z_1,\cdots,x_n-z_n)\subseteq \ker(\varphi_z)\subsetneq (1)$.

② $k[x_1,\cdots,x_n]/(x_1-z_1,\cdots,x_n-z_n)\simeq k$. $\Rightarrow$ maximal.

③ ①② $\Rightarrow$ "=".

$$k^n \xrightarrow{\Phi} \{\text{maximal ideal in } k[x_1,\cdots,x_n]\}.$$

$$z=(z_1,\cdots,z_n) \longmapsto (x_1-z_1,\cdots,x_n-z_n)$$

Fact: let $f_1,\cdots,f_r\in k[x_1,\cdots,x_n]$. $z\in k^n$. then.

$f_1(z)=\cdots=f_r(z)=0 \Leftrightarrow f_1,\cdots,f_r\in \ker(\varphi_z)$.

$\Leftrightarrow (f_1,\cdots,f_r)\subset (x_1-z_1,\cdots,x_n-z_n)$

Thm (Weak Hilbert Nullstenllensate).

当 $k=\bar{k}$, 以下 1:1 成立.

$$\{z\in k^n \mid f_1(z)=\cdots=f_r(z)=0\} \xrightarrow{\Phi(1:1)} \{\text{maximal } m \text{ in } k[x_1,\cdots,x_n] \text{ s.t. } (f_1,\cdots,f_r)\subset m\}$$

$$\downarrow 1:1.$$

$$\{\text{maximal ideal in } k[x_1,\cdots,x_n]/(f_1,\cdots,f_r)\}.$$

日期: /

Rmk: $f: R\to S$ 为 ring. 同态.

① $p\subseteq S$ prime $\Rightarrow f^{-1}(p)\subseteq R$ prime

Pf: $R/f^{-1}(p) \hookrightarrow S/p$

$\mathbb{Z}. \Leftarrow \mathbb{Z}.$

② $m\subseteq$ maximal $\not\Rightarrow f^{-1}(p)$ maximal. (在 $k=\bar{k}$ 时成立.)

反eg. 取 $\mathbb{Z}\subseteq\mathbb{Q}$. $m=(0)$.

def: 极大理想谱.

$\mathrm{Specm}(R)=\{\text{maximal ideals in } R\}$.

ideals. solving equations

$k[x_1,\cdots,x_n]/(f_1,\cdots,f_r) \longleftrightarrow \{z \mid f_1(z)=\cdots=f_r(z)=0\}$

日期: /

§2: Modules

Def: Module:

① $(M,+)$ 为加法群.

② $R\times M\to M$. s.t. $\begin{cases} r\cdot(x+y)=rx+ry. \\ 1x=x. \\ (r+s)x=rx+sx. \\ r(sx)=(rs)x. \end{cases}$

Prop1: k is a field.

给定 $k[t]$ 模 M:

$\rightsquigarrow$ ① $k\times M\to M$. $\Rightarrow$ k-模.

② $\{t\}\times M\to M$ $\Rightarrow$ 线性算子.

反过来. 给定 $\begin{cases} M\in {}_k\mathrm{Vect} \ (k\text{上线性空间的集合}). & \Rightarrow k\text{-模} \\ \phi: M\to M.\ k\text{-线性}. & \Rightarrow \text{线性算子} \end{cases}$

$\rightsquigarrow$ Define: $k[t]\times M\to M$

$(f(t),x)\mapsto f(\phi)x.$

Ex: 若有多个线性算子 $\phi_1,\phi_2,\cdots,\phi_k$.

则 1° 它们可交换时, $\rightsquigarrow f[t_1,\cdots,t_k]$ 模.

2° 不可交换时, $\rightsquigarrow f\langle t_1,\cdots,t_k\rangle$ 模. (非交换多项式环).

记号: A=ring. A^{Mod} is cat of A-modules. (A-modules + A-linear maps).

Def: A 线性:

$M,N\in A^{\mathrm{Mod}}$ $\varphi: M\to N$ is A-linear map.

if: 1° $\varphi(x+y)=\varphi(x)+\varphi(y)$.

2° $\varphi(\lambda x)=\lambda\varphi(x)$. $\lambda\in A, x\in M$.

Morita's Thm:

A, B=ring. 则 $A\cong B$ iff $A^{\mathrm{Mod}}\cong B^{\mathrm{Mod}}$.

日期: /

启发: 环上的模可给出环上"所有"的性质.
$\Rightarrow$ 通过 Modules 和 linear maps 去研究 rings.

Q: How to construct A-modules?

① $I \subset A$ ideal, I 是 A-module. A/I 为 A-module.

② $M, N \in A^{Mod}$, $\rightsquigarrow M \oplus N$.

③ Submodules.

④ $\varphi: M \to N$ A-linear.
$\rightsquigarrow$ 1) $\ker(\varphi)$ is submodule.
2) $\operatorname{im}(\varphi)$ is submodule.
3) $\operatorname{coker}(\varphi) \triangleq N/\ker(\varphi)$.

Def: $M \in A^{Mod}$ is f.g. if $\exists S \subset M$, s.t.
1° $\#S < +\infty$. 2° $\langle S \rangle = M$

Ex: 对无限维线性空间,必须类似泛函分析,要引入赋范 $\Rightarrow C^*$ algebra.
$\hookrightarrow$ 研究 $C_0^\infty(X)$. (不可列无穷维).
交换代数中研究的大多为 f.g. Module.

Prop: M is f.g. iff M 是 $A^{\oplus n}$ 的商模.
$\hookrightarrow \bigoplus_{i=1}^{n} A$, f.g. free module.

Pf: $M = \langle x_1, \cdots, x_n \rangle$. Define:
$\varphi: A^{\oplus n} \to M$. $\Rightarrow M \cong A^{\oplus n}/\ker(\varphi)$.
$(a_1, \cdots, a_n) \mapsto \sum_{i=1}^{n} a_i x_i$

$\Leftarrow$ $\underset{i\text{th}}{(0, \cdots, 1, \cdots, 0)} \leftarrow x_i$

Thm (Cayley-Hamilton) (Prop 2.4 [Atiyah]).

日期: /

Let M be f.g. A-module. $I \subseteq A$ ideal.
let $\varphi: M \to M$ A-linear map s.t. $\varphi(M) \subseteq IM \subseteq M$.
$(=\{\sum_{\text{finite}} \lambda_i x_i \mid \lambda_i \in I, x_i \in M\})$.

Then $\exists f(\varphi) = \varphi^n + a_1\varphi^{n-1} + \cdots + a_n = 0$, for some $a_1, \cdots, a_n \in I$.

[M 不一定有基.(否则为 free module).].

Pf: $A = \langle x_1, \cdots, x_n \rangle$. 则 $\varphi(M) \subseteq IM$.

$\Rightarrow \varphi(x_i) = \sum_{j=1}^{n} a_{ij} x_i \ \forall i$. (可用矩阵描述,但 $\varphi(x) = \Gamma x$ 的 Γ 的意义依赖于 x). ⟵ (x 不能线性无关).

denote $\Gamma = (a_{ij})$. Then.
(不同生成元下的转移矩阵不相似. ⇒"特征多项式"与生成元选取有关)

$\Rightarrow A[t]^{n\times n} \ni (\varphi I - \Gamma)\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = 0$.

$\xrightarrow{\times (\varphi I - \Gamma)^*} \det(\varphi I - \Gamma)\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = 0$. (伴随阵不涉及除,对环 ✓).

$\rightsquigarrow \det(\varphi I - \Gamma) = 0$.
$\in I^{n\times n}$.

$\Rightarrow \varphi^n + a_1\varphi^{n-1} + \cdots + a_n = 0$.

(将 linear map 吸收入 module 中得到的好处.)

Props: Assume $I = A$. Define $N(\varphi) = \{ f \in A[t] \mid f(\varphi) = 0 \}$.

$\Rightarrow N(\varphi) \neq 0$ (C-H Thm.) 且 $N(\varphi) \subset A[t]$ 为 ideal.

case I: A = field $\Rightarrow N(\varphi)$ 是一个主理想 $\Rightarrow N(\varphi) = \langle f_{min} \rangle$.
($A[t]$ 为 PID).

case II: A = general. $\Rightarrow N(\varphi)$ 是主理想 iff $N(\varphi) = \langle f_{min} \rangle$.
($A[t]$ 不一定为 PID, $\rightsquigarrow$ 不一定总有 f_{min})

Q: When $N(\varphi)$ is f.g?

Hilbert Basis Thm: if A = Noeth. then $A[t]$ = noeth.
(Ex: 其商环也 noeth.).

$\rightsquigarrow$ 当A noeth, $N(\varphi)$ is f.g.

$\rightsquigarrow$ 没有 f_{min}, 但 $\exists$ 一组 $f_1, \cdots, f_k$ 可使 $\forall f(\varphi)=0 \Leftrightarrow f = a_1 f_1 + \cdots + a_k f_k$.

Lemma: (Nakayama's lemma) ☆☆

Assume A = local ring, m 是 A 的 maximal ideal. $M \in A^{Mod}$ f.g.

$$mM = M \Rightarrow M = 0$$

def: A is called a local ring, if A 只有一个 maximal ideal.

几何理解: • $U \subset \mathbb{R}^2$ open set

• $C^0(U)$ = ring of U 上连续函数.

Phylosiphy: $C^0(U)$ control U 的 geometry.

• maximal ideal $\rightsquigarrow$ point.

let $x \in U$. def $m_x = \{f \in C^0(U) \mid f(x) = 0\} \underset{maximal}{\subseteq} C^0(U)$.

且若 $x \neq y$, 则 $m_x \neq m_y$. (Horsdorff 分离性).

Pf:
$$\begin{tikzcd} C^0(U) \arrow[r, "ev_x"] \arrow[d] & \mathbb{R} \\ C^0(U)/m_x \arrow[ur, hook, "\simeq"'] & \end{tikzcd}$$

Cor1: $C^0(U)$ 有无穷个极大理想.

Cor2: Thm: [P_{14}. ex26].

$$\begin{aligned} U &\xrightarrow{\Phi} \{\text{maximal ideal of } C^0(U)\} \\ x &\longmapsto m_x \end{aligned}$$

Φ 为 $\cong$. (Φ is bijective 不平凡).

Q: $C^0(U)$ 如何得出 U 的基本群、同调群等?

日期:　　/

let $x\in U$. def: $f\sim_x g$ ($f,g\in C^0(U)$) if

$\exists$ 邻域 $W\ni x$, s.t. $f|_W=g|_W$.

def: $C_x^0 \triangleq C^0(U)/\sim$

Denote $[f]_x \triangleq f$ 在 $\sim_x$ 下的等价类 (as germ of f at x)

有 $[f]_x+[g]_x=[f+g]_x$. $[f]_x[g]_x=[fg]_x$.

Fact: $[f]_x$ 控制了 f 在 x 的 local 信息.

Fact: C_x^0 是个 local ring, 且其 maximal ideal $m_x=\{[f]_x\in C_x^0 \mid f(x)=0\}$.

Lemma: $m\subseteq A$ 是 unique maximal idea, 则 $\forall x\notin m$, $x\in A^*$.

Pf: $\Rightarrow$). 假设 $x\notin m$, $x\notin A^* \rightarrow \exists m'$ 为 maximal, $x\in m'$.

$\hookrightarrow m=m'$.

$\Leftarrow$). 假设 m' 为 maximal, $\Rightarrow m'\subset m$. (否则由条件矛盾) $\Rightarrow m'=m$.

Pf: let $[f]_x\notin m_x \Rightarrow f(x)\neq 0 \Rightarrow [f]_x\in C_x^0(U)^*$. 由 lemma, $C_x^0(U)$ 为 local ring.

启发: local ring 是个局部化的工具, 可研究 maximal idea 的局部性质.

Cor: $M\in A^{\mathrm{Mod}}$ f.g. $I\subset A$ ideal st. $IM=M$.

Then $\exists x\equiv 1 \pmod I$ s.t. $xM=0$.

Pf: let $\varphi=Id_M: M\to M$. then $\varphi(M)\subseteq IM=M$.

$\therefore$ 由 C-H Thm, $\exists a_1,\cdots,a_n\in I$ st. $\underbrace{(1+a_1+\cdots+a_n)}_{x}Id_M=0$.

$$\Rightarrow \begin{cases} x-1=0. \\ xM=0. \end{cases} \quad \#.$$

日期:　　/

Pf: (Nakayama's Lem.) 由 Cor, $\exists x\in A$, $x-1\in m$, s.t. $xm=0$.

$$\Rightarrow x\notin m \overset{\text{local}}{\Rightarrow} x\in A^*. \overset{xm=0}{\Rightarrow} m=0.$$

Cor: $M\in A^{\text{Mod}}$ f.g. $N\subseteq M$ 为 submodule. (A,m) is local.

则 $M=mM+N \Rightarrow M=N$.

Pf: $M/N=(mM+N)/N=mM/N$.

由 M f.g., M/N f.g. ∴由 Lem, $M/N=0$.

∴ $M=N$.

Props: (A,m) is Local, $M\in A^{\text{Mod}}$ f.g.

- A/m is a field (称作 剩余域, residue field). $=:k$. eg. $C_x^0(U)/m_x\cong\mathbb{R}$.
- M/mM is a k-vector space.

$$A/m\times M/mM\longrightarrow M/mM.$$

$$([a],[x])\longmapsto[ax].$$

[well-defined: $a-b\in m$, $x-y\in mM$ $\rightsquigarrow$ $ax-bx=(a-b)x\in mM$. $ax-ay=a(x-y)\in mM$.].

eg. $M=C_x^{0\oplus r}$. 则 $M\to M/mM$.

$([f_1]_x,\cdots,[f_r]_x)\mapsto(f_1(x),\cdots,f_r(x))$.

M/mM 也可视作某种取值.

Props: (A,m) is local, let $x_1,\cdots,x_n\in M$. s.t $[x_1],\cdots,[x_n]\in M/mM$ is a basis.

则 $\langle x_1,\cdots,x_n\rangle=M$.

日期:　　/

Pf: let $N=\langle x_1,\cdots,x_n\rangle \subset M$.

又 $N \twoheadrightarrow M/mM \Rightarrow N+mM=M$.

由Nakayama's Lem, $M=N$.

Why Nak Lem is important?

Problems of ring $\xrightarrow{\text{Localisation}}$ Problems for local ring.

$\Big\downarrow$ Nak lem

Problems for vector space.

eg. $$\underset{\substack{\text{IS} \\ (C_x^0)^{\oplus r}/m_x(C_x^0)^{\oplus r} \\ M/mM}}{\overset{A/m}{C_x^0/\oplus m_x}} \xrightarrow[\simeq]{ev_x} \overset{k}{\mathbb{R}^{\oplus r}}$$

日期:　　/

§. Magic of arrows(=homomorphism) （范畴论思想）.

Phylosophy: Elements 对 modules 不重要.

Classical math: Set + additional structure.

$\Downarrow$ ↓封装.

Morden math: $\boxed{\text{Object}}$ + Morphism. $\rightsquigarrow$ Category Theory.

eg.1. 用映射描述单射: $(M,N,K \in A^{Mod}, \varphi, \psi$ is A-linear$)$.

Classical: $\varphi: M \to N$ 单射 iff $\varphi(x)=0 \Leftrightarrow x=0$.

Universal: $\varphi: M \to N$ 单射 iff $\forall K \xrightarrow{\psi} M$, $\varphi\circ\psi=0 \Leftrightarrow \psi=0$.

eg.2. 满射:

Universal: $\varphi: M \to N$. 满射 iff $\forall N \xrightarrow{\psi} K$, $\psi\circ\varphi=0 \Leftrightarrow \psi=0$.

eg.3. $\ker(\varphi)$:

K is $\ker(\varphi)$ iff

$[$ ① $K \xrightarrow{l} M \xrightarrow{\varphi} N$: $\varphi\circ l=0$. $]$ → system. → 泛性质 Universal Property.

$[$ ② $\forall S \xrightarrow{\psi} M \xrightarrow{\varphi} N$ s.t. $\varphi\circ\psi=0$ 则 $\exists!$ $S \xrightarrow{g} K$ s.t. $\psi = l\circ g$ $]$ → largest object in the system. (Cat 意义下).

即

$$\begin{tikzcd} S \arrow[r, "\psi"] \arrow[dr, "\exists! g"'] & M \arrow[r, "\varphi"] & N \arrow[r] & 0 \\ & K \arrow[u] \arrow[u, phantom, "\circlearrowleft", shift left=3] & & \end{tikzcd}$$

Lemma: $\ker(\varphi)$ 在同构意义下唯一.

日期:　　　/

Pf:
$$\begin{tikzcd} K_1 \arrow[d, "\exists! g"'] \arrow[dr, "\iota_1"] \arrow[dd, bend left, "id_{K_1}"] \arrow[dd, bend right=80, "f\circ g"'] & & \\ K_2 \arrow[r, "\iota_2"] \arrow[d, "\exists! f"'] & M \arrow[r, "\varphi"] & N \\ K_1 \arrow[ur, "\iota_1"'] & & \end{tikzcd}$$

由图表交换, $f\circ g = id_{K_1}$. 相似地 $g\circ f = id_{K_2}$.

§. Exact Sequence.

$$\to M_{i-1} \xrightarrow{f_i} M_i \xrightarrow{f_{i+1}} M_{i+1} \to$$

① sequence is a complex if $f_{i+1}\circ f_i = 0$ $\forall i$.

② sequence is exact at M_i if $\mathrm{Im}(f_i) = \mathrm{Ker}(f_{i+1})$.

Rmk: ① $0 \to M \xrightarrow{f} N$. is exact at M $\Leftrightarrow$ f 单

② $M \xrightarrow{f} N \to 0$ is exact at N $\Leftrightarrow$ f 满

③ $0 \to M \to N \xrightarrow{f} K$ is exact $\Leftrightarrow$ $M \cong \ker(f)$.

$$\begin{tikzcd} 0 \arrow[r] & M \arrow[r] \arrow[d, "\cong"', "\exists!"] & N \arrow[r, "f"] & K \\ 0 \arrow[r] & \ker(f) \arrow[ur, hook] & & \end{tikzcd}$$

④ $M \to N \xrightarrow{f} K \to 0$ is exact $\Leftrightarrow$ $K \cong \mathrm{coker}(f)$.

$$\begin{tikzcd} M \arrow[r] & N \arrow[r, "f"] \arrow[d] & K \arrow[r] & 0 \\ & \mathrm{coker}(f) \arrow[ur, "\cong", "\exists!"'] \arrow[r] & 0 & \end{tikzcd}$$

§ Hom.

Def: let $M, N \in {}_A\mathrm{Mod}$, define an A-Module $\mathrm{Hom}_A(M,N)$:

日期:　　/

① as a set: $Hom_A(M,N)=\{f:M\to N \mid f \text{ is } A\text{-linear}\}$.

② 加法: $f,g\in Hom_A(M,N)$, $(f+g)(x)\triangleq f(x)+g(x)$.

③ 数乘: $f\in Hom_A(M,N)$, $\lambda\in A$, $(\lambda f)(x)\triangleq \lambda f(x)$.

Rmk: 一般, $f\cdot g\in Hom_A(M,N)$ 无法定义

2 cases $\begin{cases} ① \text{ def } f\cdot g(x)=f(x)g(x) \Leftarrow \text{ if } N \text{ is } A\text{-algebra, well-defined.} \\ ② \text{ def } f\cdot g(x)=g(f(x)) \Leftarrow \text{ if } M=N, \text{ well-defined. (对应矩阵乘法).} \end{cases}$

eg. let $V,W\in k^{vect}$.

① $Hom_k(V,V)=End_k(V)\simeq Mat^{n\times n}$ $(n=\dim V)$.

② $Hom_k(V,k)=V^*$.

eg let $R^{\oplus n}\in R^{Mod}$.

$Hom_R(R^{\oplus n},R^{\oplus n})\triangleq End_R(R^{\oplus n})\simeq Mat_R^{n\times n}$.

Prop: (函子性).

let $M_1,M_2,N\in R^{Mod}$. $\varphi:M_1\to M_2$. R-linear.

Then 2 maps: $Hom_R(M_2,N)\xrightarrow{\varphi^*}Hom_R(M_1,N)$. $\Rightarrow$ pull back.

$f \mapsto f\circ\varphi$.

$Hom_R(N,M_1)\xrightarrow{\varphi_*}Hom_R(N,M_2)$. $\Rightarrow$ push forward.

$g\mapsto \varphi\circ g$.

φ^*与φ_*均R-linear.

• If $M_1 \xrightarrow{\varphi} M_2 \xrightarrow{\psi} M_3$. 则 $(\psi\circ\varphi)^* = \varphi^*\circ\psi^*$. ⇒ 协变函子

$(\psi\circ\varphi)_* = \psi_*\circ\varphi_*$. ⇒ 反变函子

• Exactness of Hom.

Thm: ① $M_1 \xrightarrow{\varphi} M_2 \xrightarrow{\psi} M_3 \to 0$ is exact

$\Leftrightarrow$ $0 \to \mathrm{Hom}_R(M_3,N) \xrightarrow{\psi^*} \mathrm{Hom}_R(M_2,N) \xrightarrow{\varphi^*} \mathrm{Hom}_R(M_1,N)$ is exact.

Pf: (i) exact $\Leftrightarrow$ ψ^* 单 $\Leftrightarrow$

Universal

$\forall f: M_3 \to N$, 若 $f\circ\psi = 0$. 则 $f=0$. $\Leftrightarrow$ ψ 满

(ii) $\mathrm{Ker}(\varphi^*) = \mathrm{Im}(\psi^*)$

$f\in$

$$\begin{tikzcd}
 & N & \\
M_1 \arrow[ur, "0"] \arrow[r, "\varphi"] & M_2 \arrow[u, "f"] \arrow[r, "\psi"] & M_3 \arrow[ul, "\exists g"'] \arrow[r] & 0
\end{tikzcd}$$

?

Rmk: 由于只用了 universal property, 所以可以推广到其他情形.

⇝ Abel Cat: ($\ni$ Module, Representation of group / Lie algebra, sheaf).

• Snake Lem 也对 Abel Cat 成立 ⇝ (Homology algebra / Abelian Cat)

Grothendieck ⇒

反过来,

② $0 \to M_1 \xrightarrow{\varphi} M_2 \xrightarrow{\psi} M_3$ is exact

$\Leftrightarrow$ $0 \to \mathrm{Hom}_R(N,M_1) \xrightarrow{\varphi^*} \mathrm{Hom}_R(N,M_2) \xrightarrow{\psi^*} \mathrm{Hom}_R(N,M_3)$ is exact.

日期: /

§. ⊗ (Tenser Product).

eg. matrix: R ring. $R^{n\times n}=\{n\times n \text{ matrix with coff in } R\}\in R^{\mathrm{Mod}}$.

def: $A, B\in R^{n\times n}$, $A\cdot B$ satisfies.

① $(A+B)\cdot C=A\cdot C+B\cdot C$, $C(A+B)=CA+CB$.

② $(rA)\cdot B=r(AB)=A\cdot(rB)$, $r\in R$.

⟶ How to define $m\cdot n$? ($m\in M, n\in N$).

Where is $m\cdot n$ in?

Def: $M, N, L\in R^{\mathrm{Mod}}$, a map $M\times N\xrightarrow{\varphi}L$ is bilinear iff:

(可视为product的一种推广) ① $\varphi(m_1+m_2, n)=\varphi(m_1, n)+\varphi(m_2, n)$.

$\varphi(m, n_1+n_2)=\varphi(m, n_1)+\varphi(m, n_2)$.

② $\varphi(rm, n)=\varphi(m, rn)=r\varphi(m, n)$.

$\Leftrightarrow$ $\varphi(-, n): M\to L$ is linear.
$x\mapsto\varphi(x, n)$

且 $\varphi(m, -): N\to L$ is linear.
$y\mapsto\varphi(m, y)$.

⟹ 任意固定某元后linear.

Consider ALL bilinear map. $M\times N\to L$: ⟹ 即product 组成的集合.

def $\mathcal{S}_{M,N}=\{\varphi: M\times N\to L \text{ bilinear}\}$.

Fact1: $\mathcal{S}_{M,N}\neq\emptyset$ ($M\times N\to 0\in\mathcal{S}_{M,N}$, $\forall M, N$)

Fact2: 若 $M\times N\xrightarrow{\varphi}L\in\mathcal{S}_{M,N}$, $L\xrightarrow{\psi}L'$ (R-linear).

则 $M\times N\xrightarrow{\varphi}L\xrightarrow{\psi}L'\in\mathcal{S}_{M,N}$.

⇝ Q: 是否有"排队"于最前的map? (universal property).

⇝ Is there $M\times N \xrightarrow{\varphi_0} K \in \mathcal{S}_{M\times N}$ s.t.

$\forall\, (M\times N \xrightarrow{\varphi} L) \in \mathcal{S}_{M\times N}$ $\exists !\, \psi: K\to L$ (R-linear)

$$\begin{tikzcd} M\times N \arrow[r, "\varphi_0"] \arrow[dr, "\varphi"'] & K \arrow[d, "\exists!\psi"] \arrow[dl, phantom, "\circlearrowright"] \\ & L \end{tikzcd} \qquad (*)$$

定义 $M\otimes_R N := K$

存在性? 唯一性?

Uniqueness: (同构意义下). Assume $M\times N \xrightarrow{\varphi_i} K_i$ $i=1,2$. 都satisfy $(*)$.,

then

$$\begin{tikzcd} & K_2 \arrow[d, "\exists!a_1"] \arrow[dd, bend left=60, "id"] \\ M\times N \arrow[ur, "\varphi_2"] \arrow[r, "\varphi_1"] \arrow[dr, "\varphi_2"'] & K_1 \arrow[d, "\exists!a_2"] \\ & K_2 \end{tikzcd}$$

id使图交换. 则由 a_1, a_2 唯一性.

$a_1\circ a_2 = id_{K_2}$.

Existence: 形式上记 $m\otimes n$, 尝试构造.

Consider $R^{\oplus M\times N}$ (作为集合) $=\left\{\text{formal finite sum } \sum_{i=1}^{n} a_i m_i\otimes n_i,\ \begin{matrix} a_i\in R \\ m_i\in M \\ n_i\in N\end{matrix}\right\}$.

(形式上)

↓ free module.

Consider $M\times N \to R^{\oplus M\times N}$ 但是不满足 $\underbrace{(m_1+m_2)\otimes n}_{2项} \neq \underbrace{m_1\otimes n + m_2\otimes n}_{1项}$.

$(m,n) \mapsto m\otimes n$

Q: How to improve?

def $\sim$ as a submodule 生成 by

$$\left\{\begin{array}{l} (m_1+m_2)\otimes n - m_1\otimes n - m_2\otimes n, \\ m\otimes(n_1+n_2) - m\otimes n_1 - m\otimes n_2, \\ (rm)\otimes n - m\otimes(rn), \\ (rm)\otimes n - r\cdot(m\otimes n) \end{array} : \forall m,n \in M,N \right\}$$

则 def: $M\times N \xrightarrow{\varphi_0} R^{\oplus M\times N}/\sim$

由
$$\begin{tikzcd} M\times N \arrow[r] \arrow[dr, "\varphi"'] & R^{\oplus M\times N} \arrow[r] \arrow[d, "\varphi'"] & R^{\oplus M\times N}/\sim \arrow[dl, "\exists!\psi"] \\ & L & \end{tikzcd}$$

$(m,n) \mapsto \varphi(m,n)$

φ bilinear $\rightsquigarrow \varphi'(\sim)=0 \overset{\text{coker}}{\rightsquigarrow} \exists!\psi$

Def: 张量积 (Tensor): ① $M\otimes N := R^{\oplus M\times N}/\sim$

② $M\times N \to M\otimes_R N$ is unique bilinear map satisfy (*).

- Def ① is NOT useful. ($\sim$ 太过复杂).

Fact1: $\because M\otimes_R N$ is generated by $\{x\otimes y \mid x\in M, y\in N\}$.

- if $M=\langle x_1,\cdots,x_r\rangle$, $N=\langle y_1,\cdots,y_r\rangle$. 则 $M\otimes_R N=\{x_i\otimes y_j : \forall i,j\}$.

Cor: $M,N\in R^{\mathrm{Mod}}$ are f.g. 则 $M\otimes_R N$ is f.g.

Generalization:

Def: $M_1,\cdots,M_n\in R^{\mathrm{Mod}}$, a map $M_1\times\cdots\times M_n\to N$ is multilinear, if it is linear in each variable.

Thm-Def: $\exists K\in R^{\mathrm{Mod}}$ 及 multilinear map $M_1\times\cdots\times M_n \xrightarrow{\varphi_0} K$ st.

$$\begin{tikzcd} M_1\times\cdots\times M_n \arrow[r, "\varphi_0"] \arrow[dr, "\forall\varphi"'] & K \arrow[d, "\exists!\psi"] \\ & L \end{tikzcd}$$

日期:　　/

- $K = R^{\oplus M_1\times\cdots\times M_n}/\sim$

- $M_1\otimes_R\cdots\otimes_R M_n$ 在 iso 意义下 unique.

Prop1: $M,N,P\in {}_R\mathrm{Mod}$. Then

① $M\otimes_R N\simeq N\otimes_R M$.

② $(M\otimes_R N)\otimes_R P\simeq M\otimes_R(N\otimes_R P)\simeq M\otimes_R N\otimes_R P$.

③ $(M\oplus_R N)\otimes_R P\simeq(M\otimes_R P)\oplus(N\otimes_R P)$.

↓

④ $(\bigoplus_{i\in I}M_i)\otimes_R P\simeq\bigoplus_{i\in I}(M_i\otimes_R P)$, $M_i\in {}_R\mathrm{Mod}$.

⑤ $R\otimes_R M\simeq M$. (逆映射: $1\otimes x\leftarrow x$).

$\rightsquigarrow$ $\otimes$ is a "product" in ${}_R\mathrm{Mod}$, $\oplus$ is a "sum" in ${}_R\mathrm{Mod}$
(没有逆,半群加法).

补: ⑥ $0\oplus M\simeq M$.

⑦ $M\oplus N\simeq N\oplus M$.

⑧ $(M\oplus N)\oplus P\simeq M\oplus(N\oplus P)\simeq M\oplus N\oplus P$.

Pf-eg.: ① $M\otimes_R N\to N\otimes_R M$. 但未必 well-defined.
$m\otimes n\mapsto n\otimes m$.

$\rightsquigarrow$
$$\begin{tikzcd}
M\times N \arrow[r] \arrow[d, "\varphi_0"'] \arrow[dr, "\varphi"] & N\times M \arrow[d] \\
M\otimes_R N \arrow[r, "\exists!\psi"'] & N\otimes_R M
\end{tikzcd}$$
$(x,y)\mapsto(y,x)$, well-defined. $(y\otimes x)$.

φ bilinear
$\rightsquigarrow \exists!\psi$ s.t. $\psi(x\otimes y)=y\otimes x$

③
$$\begin{tikzcd}
M\otimes_R P \arrow[r, "\exists!"] & (M\oplus N)\otimes_R P \\
M\times P \arrow[u] \arrow[r] \arrow[ur] & (M\oplus N)\times P \arrow[u]
\end{tikzcd}$$
N同理.

Rmk: $(M\times P)\oplus(N\times P)\to(M\oplus N)\otimes_R P$ 不是 bilinear.

日期: /

Prop 2: let $f: M_1 \to M_2$. $g: N_1 \to N_1$. R-linear. ∃! R-linear map.

$$M_1 \otimes N_1 \xrightarrow{f \otimes g} M_2 \otimes N_2.$$
$$x \otimes y \longmapsto f(x) \otimes g(y).$$

well-defined?:

$$\begin{tikzcd} (x,y) \arrow[rrr, mapsto] \arrow[ddd, mapsto] & & & (f(x),g(x)) \arrow[ddd, mapsto] \\ & M_1 \times N_1 \arrow[r, "f \times g"] \arrow[d] \arrow[dr, bend left, "\varphi"] & M_2 \times N_2. \arrow[d] & \\ & M_1 \otimes N_1. \arrow[r, "\exists! \psi \triangleq f \otimes g"'] & M_2 \otimes N_2. & \\ x \otimes y. & & & f(x) \otimes g(x) \end{tikzcd}$$

φ = bilinear.

$\rightsquigarrow \exists! \psi = f \otimes g$

→即⊗是函子,即⊗与复合交换.

Prop 3: (函子性) $M_1 \xrightarrow{f_1} M_2 \xrightarrow{f_2} M_3$.

then $$\begin{tikzcd} M_1 \otimes N \arrow[r, "f_1 \otimes id_N"] \arrow[rr, bend right, "(f_2 \circ f_1) \otimes id_N"'] & M_2 \otimes N \arrow[r, "f_2 \otimes id_N"] & M_3 \otimes N. \end{tikzcd}$$,即 $(f_2 \circ f_1) \otimes id_N$
$= (f_2 \otimes id_N) \circ (f_1 \otimes id_N)$.

Cor: if $M_1 \to M_2$ is R-linear 同构.

则 $f \otimes id_N: M_1 \otimes N \to M_2 \otimes N$. 也是 R-linear 同构.

Pf: $$\begin{tikzcd} M_1 \otimes N \arrow[r, "f \otimes id_N"] \arrow[rr, bend right, "id_{M_1 \otimes N}"'] & M_2 \otimes N \arrow[r, "f^{-1} \otimes id_N"] & M_1 \otimes N. \end{tikzcd}$$

$\therefore (f^{-1} \otimes id_N) \circ (f \otimes id_N) = id_{M_1 \otimes N}$.

同理, $(f \otimes id_N) \circ (f^{-1} \otimes id_N) = id_{M_2 \otimes N}$.

$\therefore f \otimes id_N$ is iso.

(即⊗保持同构)

日期:　　/

Prop4: (Right exactness of $\otimes$)

$M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3 \to 0$ is exact. $N \in {}_R\mathrm{Mod}$. ($\rightsquigarrow M_3 \simeq \mathrm{coker}(f)$).

$M_1 \otimes N \xrightarrow{f\otimes id_N} M_2 \otimes N \xrightarrow{g\otimes id_N} M_3 \otimes N \to 0$. is exact.

Cor: ① if $M_2 \to M_3$ is surjective, then

$M_2 \otimes N \to M_3 \otimes N$ is also surjective.

② $M_3 \otimes N \simeq M_2 \otimes N / \mathrm{im}(f\otimes id_N)$. (即 $= \mathrm{coker}(f\otimes id_N)$).

Rmk: · $\otimes$保持满射.

· $\otimes$不保持单射. (injective 对应于 Ker, ×; 而$\otimes$对应 surjective, coker, $\oplus$).

Pf-Cor1: Consider: $0 \to \mathrm{Ker}(\varphi) \to M_2 \xrightarrow{\varphi} M_3 \to 0$. exact

$\downarrow$

$M_2 \otimes N \xrightarrow{\varphi\otimes id_N} M_3 \otimes N \to 0$ exact.

Cor-Pf. M, N f.g. 则 $M\otimes N$ f.g.:

Proof: $\exists$ surjective map: $R^{\oplus s} \xrightarrow{f} M$. $R^{\oplus r} \xrightarrow{g} N$.

$\rightsquigarrow$ $R^{\oplus s} \otimes R^{\oplus r} \xrightarrow{id_{R^{\oplus s}}\otimes g} R^{\oplus s} \otimes N \xrightarrow{f\otimes id_N} M \otimes N$.

$= (R\oplus \cdots \oplus R) \otimes R^{\oplus r}$.

$= R^{\oplus r} \oplus \cdots \oplus R^{\oplus r} = R^{\oplus rs}$.

Pf-Cor2: $0 \to N \to M \to M/N \to 0$.

$\downarrow \otimes P$

$N\otimes P \to M \otimes P \to (M/N) \otimes P \to 0$.

日期: /

* 不保injective：

eg. $\mathbb{Z} \longrightarrow \mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z}$ $\in \mathbb{Z}^{\mathrm{Mod}}$.

$x \longmapsto 2x$.

$$\mathbb{Z}/2\mathbb{Z} \simeq \mathbb{Z}\otimes_{\mathbb{Z}}\mathbb{Z}/2\mathbb{Z} \longrightarrow \mathbb{Z}\otimes_{\mathbb{Z}}\mathbb{Z}/2\mathbb{Z}$$

$$x\otimes_{\mathbb{Z}}[y] \longmapsto 2x\otimes_{\mathbb{Z}}[y] = x\otimes_{\mathbb{Z}}[2y] = 0.$$

$\rightsquigarrow$ Cor: ① If $N\subset M$ submodule. then.

$N\otimes_R P$ 不一定是 $M\otimes_R P$ 的 submodule.

② $\exists\, x\in N,\ y\in P$. $x\otimes y = 0$ in $M\otimes_R P$.

但不一定 $x\otimes y=0$ in $N\otimes_R P$.

$\rightsquigarrow$ 张量积中用的元素必须明确在哪个模上.

$\rightsquigarrow$ 最好不要用元素表达式.

* R is important in $M\otimes_R N$:

eg. $\mathbb{C}\in\mathbb{C}^{\mathrm{Mod}}$, $\mathbb{C}\simeq\mathbb{R}^{\oplus 2}\in\mathbb{R}^{\mathrm{Mod}}$.

- $\mathbb{C}\otimes_{\mathbb{C}}\mathbb{C}\simeq\mathbb{R}^{\oplus 2}$.
- $\mathbb{C}\otimes_{\mathbb{R}}\mathbb{C}\simeq\mathbb{R}^{\oplus 2}\otimes\mathbb{R}^{\oplus 2}\simeq\mathbb{R}^{\oplus 4}$.

照镜子 ($\otimes$ 最有用的性质).

$\boxed{\text{Lem:}}$ $\mathrm{Hom}_R(M\otimes_R N, P) \simeq \mathrm{Hom}_R(M, \mathrm{Hom}_R(N,P))$.

(Cat: $\otimes$ is left adjoint of Hom).

Pf: ① $\mathrm{Hom}_R(M\otimes_R N, P) \xrightarrow{\Phi} \mathrm{Bilinear}_R(M\times N, P)$.

$\qquad f \longmapsto f\circ\varphi$.

- Φ 为 R-linear.
- Φ is bijective. $\Longleftarrow$

$\Downarrow$ Φ = iso.

$$\begin{tikzcd} M\times N \arrow[r, "\varphi"] \arrow[dr, "\forall\text{bilinear}"'] & M\otimes N \arrow[d, "\exists!"] \\ & P \end{tikzcd}$$

② $\mathrm{Bilinear}_R(M\times N, P) \xrightarrow{\psi} \mathrm{Hom}_R(M, \mathrm{Hom}_R(N,P))$.

$\qquad (f: M\times N \to P) \longmapsto (x, f(x,-))$.

- ψ 为 R-linear.
- ψ 为 bijective.

$\Downarrow$ ψ = iso.

Prop4-Pf: $\quad M_1 \to M_2 \to M_3 \to 0$ exact.

$$\Downarrow \mathrm{Hom}_R(-, \mathrm{Hom}_R(N,P)).$$

$0 \to \mathrm{Hom}_R(M_3, \mathrm{Hom}_R(N,P)) \to \mathrm{Hom}_R(M_2, \mathrm{Hom}_R(N,P)) \to \mathrm{Hom}_R(M_1, \mathrm{Hom}_R(N,P))$ exact. $\forall P\in {}_R\mathrm{Mod}$.

$$\Downarrow \text{Lem}$$

$0 \to \mathrm{Hom}_R(M_3\otimes N, P) \to \mathrm{Hom}_R(M_2\otimes N, P) \to \mathrm{Hom}_R(M_1\otimes N, P)$. exact $\forall P\in {}_R\mathrm{Mod}$.

$$\Downarrow$$

$M_1\otimes N \to M_2\otimes N \to M_3\otimes N \to 0$. exact.

日期:

§ $\boxed{\text{Change of scallar}}$: ($\otimes$的应用).

Assume $M \in R^{\mathrm{Mod}}$ let $S \xrightarrow{\sigma} R$ a ring homo, then

$M \overset{\text{also}}{\in} S^{\mathrm{Mod}}$. with $\overset{\in S}{s} \circ \overset{\in M}{x} := \sigma(s)\circ x$.

$$S \times M \xrightarrow{\sigma\times id} R\times M \to M.$$

反过来，有 $M \in S^{\mathrm{Mod}}$, define $M \otimes_S R \in R^{\mathrm{Mod}}$ as:

$$(M\otimes_S R)\times R \to M \otimes_S R.$$

$$(x\otimes r).r' \mapsto x \otimes rr'.$$

well-defined?:

$$\begin{tikzcd}
M\otimes_S R \arrow[r, "\exists ! \psi_r"] & M\otimes_S R \\
M\times R \arrow[u] \arrow[r, "\times r"] \arrow[ur, "\text{bilinear}"] & M\times R \arrow[u]
\end{tikzcd}$$

$$(x, r') \longmapsto (x, rr').$$

?

$S \xrightarrow{\sigma} R$.
则 $R \in S^{\mathrm{Mod}}$
$(s.r = \sigma(s).r.)$

即 $M \in S^{\mathrm{Mod}}$
$\rightsquigarrow \otimes_S R$ (只要 $S \xrightarrow{\sigma} R$)
$M\otimes_S R \in R^{\mathrm{Mod}}$.

Prop: $M \xrightarrow{f} N$ is S-linear. then $M\otimes_S R \xrightarrow{f\otimes id_R} N \otimes_S R$ is R-linear.

Cor: $M \in R^{\mathrm{Mod}}$. $I \subseteq R$ ideal $R \to R/I$.

$$M \otimes_R R/I \in R/I^{\mathrm{Mod}}.$$

Rmk: 当取 I s.t. R/I 为域，则 $M \otimes_R R/I \in R/I^{\mathrm{Vect}}$.

Cor: ① $R^{\oplus n} \simeq R^{\oplus m} \Leftrightarrow n = m$.

(线代: if $\langle x_1, \cdots x_n\rangle = R^{\oplus m}$, 则 $n \geq m$)

② $f: R^{\oplus n} \to R^{\oplus m}$. is surjective $\Rightarrow n \geq m$.

③ $f: R^{\oplus n} \to R^{\oplus m}$ is injective $\Rightarrow n \leq m$.

(线代: 若 $x_1, \cdots, x_n \in R^{\oplus m}$ 线性无关, 则 $n \leq m$).

日期:　　/

Pf: ① 取 I s.t. R/I is a field.

$$R^{\oplus n} \simeq R^{\oplus m}$$

$$(R/I)^{\oplus n} \simeq \underbrace{R/I \otimes_R R^{\oplus n}}_{\boxed{\in (R/I)^{Mod}}} \simeq \underbrace{R/I \otimes_R R^{\oplus m}}_{\boxed{\in (R/I)^{Mod}}} \simeq (R/I)^{\oplus m}$$

$$= (R/I \otimes_R R)^{\oplus m}$$

$\Leftrightarrow$ $n = m$.

② $R^{\oplus n} \longrightarrow R^{\oplus m} \to 0$ exact.

$$\rightsquigarrow$$

$R^{\oplus n} \otimes R/I \to R^{\oplus m} \otimes R/I \to 0$ exact.

$\simeq (R/I)^{\oplus n}$ 　　 $\simeq (R/I)^{\oplus m}$.

$\Leftrightarrow$ $n \geq m$

③ Rmk: 不可类似推导

Def (flat module) R-module M is flat if

$\forall$ $N_1 \xrightarrow{f} N_2$ injective.

$\rightsquigarrow$ $M \otimes_R N_1 \xrightarrow{Id_M \otimes f} M \otimes_R N_2$ injective. (M可保$\otimes_R$的单射)

Rmk1: $R/I \in R^{Mod}$ is not flat.

Rmk2: R is integral. 则 $Frac(R)$ is flat.

---

if R = integral. 记 $K = Frac(R)$. $\rightsquigarrow$ K = flat

则

$0 \to R^{\oplus n} \to R^{\oplus m}$ exact

$$\rightsquigarrow$$

$0 \to \underbrace{R^{\oplus n} \otimes_R K}_{\boxed{\in K^{Mod}}} \to \underbrace{R^{\oplus m} \otimes_R K}_{\boxed{\in K^{Mod}}}$ exact

$\simeq K^{\oplus n}$. 　　 $\simeq K^{\oplus m}$

$\Leftrightarrow$ $n \leq m$.

日期: /

而对一般的环 R:

用 Cayley-Hamilton Thm 可证.

?

§. flat module 前瞻.

eg ① free module $R^{\oplus S}$ is flat.

$$\begin{array}{ccc} M\otimes_R R^{\oplus S} & \hookrightarrow & N\otimes_R R^{\oplus S} \\ \wr\wr & & \wr\wr \\ M^{\oplus S} & \hookrightarrow & N^{\oplus S} \end{array}$$

② $\mathbb{Q}$ is not free, but is flat.

③ Thm: A = Notherian. local. ring. $M \in {}_A\mathrm{Mod}$ f.g.

then M is flat $\Leftrightarrow$ M is free.

④ 分式模 $S^{-1}R \in {}_R\mathrm{Mod}$ 均为 flat module (提供 non-free 例子).

日期: / §3.1: Fractions of rings & modules.

Def: subset $S\subseteq A$ is "乘积封闭" if $\begin{cases} ① & 1_A\in S. \\ ② & S\cdot S\subseteq S. \end{cases}$ (Rmk: S为集合).

eg. D = domain, $D\setminus\{0\}$ 为 multiplicatively closed.

Def: A is ring. $S\subseteq A$ multiplicatively closed. define:

$$S^{-1}A=\{(x,s)\mid x\in A,\ s\in S\}/\sim$$

$\sim$: $(a,s)\sim(b,t) \Leftrightarrow (at-bs)u=0$. for some $u\in S$

因为A不一定是 domain

Claim 1: $\sim$ 为等价条件.

Pf: ① $(a,s)\sim(a,s)$ ✓ (取 $u=1_A\in S$ 即可).

② $(a,s)\sim(b,t) \Leftrightarrow (b,t)\sim(a,s)$. ✓.

③ $(a,s)\sim(b,t)$, $(b,t)\sim(c,w) \Rightarrow (a,s)\sim(c,w)$.

$(at-bs)v=0$ $(bw-ct)u=0$. $\Rightarrow (aw-cs)\underbrace{tvu}_{\in S}=0$.

Claim 2: $S^{-1}A$ is a ring.

def: $\frac{a}{s}+\frac{b}{t}=\frac{at+bs}{st}$. $\frac{a}{s}\cdot\frac{b}{t}=\frac{ab}{st}$

验证: ① $+,\cdot$ well defined

② $\frac{0}{1}\in S^{-1}A$ is "zero". $\frac{1}{1}\in S^{-1}A$ is "unit".

③ $A\to S^{-1}A$ is a ring hom.
$a\mapsto\frac{a}{1}$

eg.1. A = domain, $S=A\setminus\{0\}$. 则 $S^{-1}A\cong \mathrm{Frac}(A)$.

eg.2. $f\in A$. $S_f=\{f^n\}_{n\geq0}$. Denote $A_f:=S_f^{-1}A$.

Prop: (Universal Property).

日期: /

$\mathcal{S}_{A,S}=\{f:A\to B \mid f(S)\subseteq B^*\}$ 可验证 $f:A\to B\in \mathcal{S}_{A,S}$, $g:B\to C$ 则 $g\circ f\in \mathcal{S}_{A,S}$.

从而必有排在最前的

Given A, S. let $g:A\to B$. s.t. $g(S)\subseteq B^*$. 则 $\exists!\psi: S^{-1}A\to B$. s.t. 图表交换.

即
$$\begin{tikzcd} A \arrow[r, "\varphi"] \arrow[d, "g"'] & S^{-1}A \arrow[dl, "\exists!\psi"] \arrow[dl, phantom, shift right=4, "\circlearrowleft"] \\ B & \end{tikzcd}$$

Def: A is ring, $S\subseteq A$ ($1\in S$, $S\cdot S\subseteq S$). $M\in {}_A\mathrm{Mod}$. Define:

$S^{-1}M\in {}_{S^{-1}A}\mathrm{Mod}$ by:

$$S^{-1}M=\{(m,s)\mid m\in M, s\in S\}/\sim.$$

- $(m,s)\sim(m',s') \iff \exists t\in S$, s.t. $t(sm'-s'm)=0$.
- $\frac{m}{s}+\frac{n}{t}=\frac{tm+sn}{st}$. $\frac{m}{s}\cdot\frac{n}{t}=\frac{m\cdot n}{s\cdot t}$.

(Rmk: 也可看作一种换环.).

Prop1: (映射也可换环).

$f:M\to N$ A-linear. ($S\subseteq A$).

then, $S^{-1}f: S^{-1}M \longrightarrow S^{-1}N$. $\left\langle \begin{array}{l}\text{well-defined}\\ S^{-1}A \text{ linear.}\end{array}\right.$

$\frac{m}{s} \longmapsto \frac{f(m)}{s}$.

日期: /

Pf: well-defined: 假设 $\frac{m_1}{s_1}=\frac{m_2}{s_2} \Rightarrow t(s_2m_1-s_1m_2)=0.\ t\in S.$

$$\Downarrow f$$

$$t(s_2f(m_1)-s_1f(m_2))=0 \Rightarrow \frac{f(m_1)}{s_1}=\frac{f(m_2)}{s_2}.$$

Prop 2: 函子性:(可复合).

if $M\xrightarrow{f}N\xrightarrow{g}P$. A-linear, then $S^{-1}g\circ S^{-1}f=S^{-1}(g\circ f)$

☆ Prop3: 正合性.

Assume: $M\xrightarrow{f}N\xrightarrow{g}P$ is exact.

then $S^{-1}M\xrightarrow{S^{-1}f}S^{-1}N\xrightarrow{S^{-1}g}S^{-1}P$ is exact.

(Rmk: Hom函子左正合(保单不保满), ⊗函子右正合(保满不保单).

S^{-1}函子正合(保单又保满)).

Pf: ① $\mathrm{Im}(S^{-1}f)\subseteq\ker(S^{-1}g) \Leftarrow S^{-1}g\circ S^{-1}f=S^{-1}(g\circ f)=S^{-1}(0)=0.$

② $\ker(S^{-1}g)\subseteq\mathrm{Im}(S^{-1}f)$:

Assume $\frac{x}{s}\in\ker(S^{-1}g).,\ x\in N. \Rightarrow \frac{g(x)}{s}=0=\frac{0}{1}\in S^{-1}P \Rightarrow t\cdot g(x)=0.\ (\exists t\in S)$

$\xRightarrow{\text{A-linear}}\ tx\in\ker(g)=\mathrm{Im}(f)\Rightarrow tx=f(y),\ y\in M.$

$\Rightarrow \frac{x}{s}=\frac{tx}{ts}=\frac{f(y)}{ts}\in\mathrm{Im}(S^{-1}f).$ #

Cor: Assume $0\to M_1\to M_2\to M_3\to 0$. is exact, then

$$0\to S^{-1}M_1\to S^{-1}M_2\to S^{-1}M_3\to 0.$$

日期: /

Prop4: $M \in {}_A\mathrm{Mod}$. $S \subseteq A$ ($1 \in S$, $S\cdot S \subseteq S$). ∃一个自然的 $S^{-1}A$-module 同构:

$$S^{-1}A \otimes_A M \xrightarrow{\simeq} S^{-1}M.$$

$$\frac{a}{s} \otimes m \longmapsto \frac{am}{s}.$$

(Rmk: 分式化的换环 ⟺ 张量积上的换环: 提供分式化、张量积两种观点).

Pf: • $(\frac{a}{s}, m) \longmapsto (\frac{am}{s})$. ⇐ bilinear.

$$\begin{tikzcd} S^{-1}A \times M \arrow[r] \arrow[d] & S^{-1}M \\ S^{-1}A \otimes_A M \arrow[ur, "\exists ! \varphi"'] & \end{tikzcd}$$

⇒ φ 良定义.

• φ surjective: $\frac{m}{s} = \varphi(\frac{1}{s} \otimes m)$.

• φ injective:

lemma: ∀元素 $\in S^{-1}A \otimes_A M$ is $\frac{1}{s} \otimes m$ 的形式 (这在一般的⊗中不行, 为有限和).

记 $\xi \in S^{-1}A \otimes_A M$, 记 $\xi = \sum \frac{a_i}{s_i} \otimes m_i$ let $s = \prod s_i$.

$$= \sum \frac{\overset{\in A}{a_i t_i}}{s} \otimes m_i. \quad t_i = \prod_{j \neq i} s_j.$$

$$= \sum \frac{1}{s} \otimes a_i t_i m_i$$

$$= \frac{1}{s} \otimes (\sum a_i t_i m_i).$$

#

(Prop3 & Prop4).

Cor: $S^{-1}A$ is a flat A-module.

Cor: A = integral. then $\mathrm{Frac}(A) \in {}_A\mathrm{Mod}$ is flat.

日期: /

Prop 5: ($\otimes$与 S^{-1} 的交换性:)

$$S^{-1}M \otimes_{S^{-1}A} S^{-1}N \xrightarrow{\simeq} S^{-1}(M \otimes_A N).$$

Pf: $S^{-1}M \otimes_{S^{-1}A} S^{-1}N \simeq (M \otimes_A S^{-1}A) \otimes_{S^{-1}A} (S^{-1}A \otimes_A N)$

$\simeq M \otimes_A (S^{-1}A \otimes_{S^{-1}A} S^{-1}A) \otimes_A N$

$\simeq (M \otimes_A N) \otimes_A S^{-1}A$

$\simeq S^{-1}(M \otimes_A N).$ #

(Rmk: $A \to B$ ring hom. $N \subseteq M$ is submodule. 记 $i: N \hookrightarrow M$.

则 $i_B: B \otimes_A M \to B \otimes_A N$. injective.

而 $S^{-1}M \to S^{-1}N$ is injective.

即用$\otimes$换环,可能不保子模;但 S^{-1} 保子模 $\rightsquigarrow$ S^{-1} 保若类性质.).

Prop 6: $N_1, N_2 \subseteq M$ are submodule.

① $S^{-1}(N_1+N_2) = S^{-1}N_1 + S^{-1}N_2$.

② $S^{-1}(N_1 \cap N_2) = S^{-1}N_1 \cap S^{-1}N_2$.

③ $S^{-1}(M/N_1) \simeq S^{-1}M / S^{-1}N_1$.

Pf: ①: $\subseteq$:) $\forall \frac{n_1+n_2}{s} \in S^{-1}(N_1+N_2)$

$= \frac{n_1}{s} + \frac{n_2}{s} \in S^{-1}N_1 + S^{-1}N_2$.

$\supseteq$:) $\forall \frac{n_1}{s} \in S^{-1}N_1$, $\frac{n_2}{t} \in S^{-1}N_2$. then $\frac{tn_1+sn_2}{ts} \in S^{-1}(N_1+N_2)$.

日期: /

②: $\subseteq$: 显.

$\supseteq$: $\forall \frac{n_1}{s} = \frac{n_2}{t}$, 有 $u(tn_1 - sn_2) = 0$. 记 $w = utn_1 = usn_2 \in N_1 \cap N_2$.

$\therefore \quad \frac{n_1}{s} = \frac{w}{uts} \in S^{-1}(M_1 \cap N_2)$

③ $0 \to N_1 \to M \to M/N_1 \to 0$. exact

$\Downarrow S^{-1}$.

$0 \to S^{-1}N_1 \to S^{-1}M \to S^{-1}(M/N_1) \to 0$. exact

日期: /

§3.2. Localization.

Def: (Localization at $p \in \mathrm{Spec}(A)$). $\mathrm{Spec}(A)=\{\text{prime ideal of } A\}$.

def: $S_p = A \setminus p$.

Denote the localization of A at $p \in \mathrm{Spec}(A)$ by: $A_p := S_p^{-1}A$.

几何意义: $U \in \mathbb{R}^n$. $C^0(U)=\{f: U \to \mathbb{R} \text{ 连续}\}$ is a ring.

let $x \in U$. define $m_x = \{f \in C^0(U) \mid f(x)=0\}$. ($C^0(U)$ 的 maximal ideal)

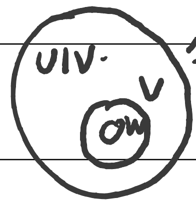
def $C^0(U)_x = \{f \in C^0(U)\}/\sim$. $f \sim g \Leftrightarrow \exists$ 邻域 $W \ni x$, s.t. $f|_W = g|_W$.

Prop 1: $C^0(U)_x \simeq C^0(U)_{m_x} := (\underbrace{C^0(U)\setminus m_x}_{:=S})^{-1} C^0(U)$.

Pf: $f \longmapsto f_x$. $\Leftarrow l_x(S) \subseteq C^0(U)_x^*$

$$\begin{tikzcd} C^0(U) \arrow[r, "l_x"] \arrow[d, "\varphi"'] & C^0(U)_x \\ C^0(U)_{m_x} \arrow[ur, "\exists!\psi"'] & \end{tikzcd}$$

$\Rightarrow \psi(\frac{f}{s}) = \frac{l_x(f)}{l_x(s)} = f_x (s_x)^{-1}$.



分离性.

Claim1: ψ 单射: $\psi(\frac{f}{s})=0 \Rightarrow f_x = 0$.

$\Rightarrow \exists \lambda \in C^0(U)$, s.t. $\lambda|_{U\setminus V}=0$. $\lambda|_W = 1$.

$\Rightarrow \lambda \cdot f = 0$ (且 $\lambda \in S$). $\Rightarrow \frac{f}{s} = 0 \in S^{-1}C^0(U)$.

Claim2: ψ 满射: l_x 满射 $\Rightarrow \psi$ 满射.

Prop 2: A_p is a local ring. 且 P_p is its unique maximal ideal.

Pf: ① $A_p / P_p \simeq (A/p)_p = (A\setminus p)^{-1} A/p = \mathrm{Frac}(A/p)$. is a field.

S^{-1} 与 / 交换. $A\setminus p \to (A/p)\setminus\{0\}$. integral.

$\Rightarrow P_p$ is maximal ideal

② P_p is the unique maximal $\Leftarrow \forall \frac{x}{s} \notin P_p$, 有 $\frac{x}{s} \in (A_p)^*$.

日期: /

Prop3: $M\in {}_A\mathrm{Mod}$, $x\in M$, then

(i) $x=0$

$\Leftrightarrow$ (ii) $\frac{x}{1}=0\in M_p$. $\forall p\in \mathrm{Spec}(A)$.

$\Leftrightarrow$ (iii) $\frac{x}{1}=0\in M_m$, $\forall$ maximal ideal m.

$\boxed{\text{Geometry}}$: $f=0\in C^0(U)$. $\Leftrightarrow$ $\underbrace{[f]_x}_{\text{germ}}=0\in C_x^0=C^0_{m_x}$ $\forall x\in U$

Pf: (i) $\Rightarrow$ (ii) $\Rightarrow$ (iii). 显.

(iii) $\Rightarrow$ (i): Assume $x\neq 0$. Consider $\underset{x的零化子}{\mathrm{Ann}(x)}:=\{a\in A, ax=0\}\leq A$.

$x\neq 0\Rightarrow 1\notin \mathrm{Ann}(x)\Rightarrow\exists$ maximal ideal $m\supseteq \mathrm{Ann}(x)$.

由 $\underbrace{\frac{x}{1}}_{=0}\in M_m=(A\setminus m)^{-1}M$.

$\Rightarrow$ $tx=0$. $t\in A\setminus m$.

而由 $t\in \mathrm{Ann}(x)\subseteq m$. 矛盾.

Cor1: $M\in {}_A\mathrm{Mod}$, then TFAE

(i) $M=0$. (ii) $M_p=0$. $\forall p\in \mathrm{Spec}(A)$. (iii) $M_m=0$ $\forall$ maximal $m\leq A$.

Cor2: $\varphi: M\to N$ (A-linear), then TFAE:

(i) φ injective (或 surjective).

(ii) $\varphi_p: M_p\to N_p$ injective (或 surjective).

(iii) $\varphi_m: M_m\to N_m$ injective (或 surjective).

日期:　　　/

$\boxed{\text{Geometry:}}$ 局部化保持任意局部的性质.

Pf: Consider $0 \to \ker(\varphi) \to M \xrightarrow{\varphi} N$. exact.

$\Downarrow$ 分式化.

$0 \to \ker(\varphi)_p \to M_p \xrightarrow{\varphi_p} N_p$ exact. $p \in \operatorname{Spec}(A)$.

$= \ker(\varphi_p)$.
(Prop3).

$\Downarrow$

$0 \to \ker(\varphi)_m \to M_m \xrightarrow{\varphi} N_m$ exact m = maximal. #.

$= \ker(\varphi_m)$:
(Prop3).

Cor 3: $M \in {}_A\text{Mod}$. TFAE.

(i) M = flat A-module

(ii) M_p = flat A_p-module.

(iii) M_m = flat A_m-module

(Rmk: flat 是局部性质).

Thm: A local Notherian ring, $M \in {}_A\text{Mod}$ f.g. then

M is flat $\Leftrightarrow$ M is free.

$\boxed{\text{Geometry:}}$ f.g. flat module 对应于向量丛.

Pf: (i)$\Rightarrow$(ii): $M_p = \underset{\text{flat}}{M} \otimes_A \underset{\text{flat}}{A_p}$. $\Rightarrow M_p$ flat.

(ii)$\Rightarrow$(iii): 显.

(iii)$\Rightarrow$(i): 由 $N \to P$ injective

日期: /

$\therefore N_m \to P_m$ injective. $\forall m$

$\overset{M_m \text{ flat}}{\Rightarrow}$ $M_m \otimes_{A_m} N_m \to M_m \otimes_{A_m} P_m$ injective. $\forall m$

$\Rightarrow (M\otimes_A N)_m \to (M\otimes_A P)_m$ injective. $\forall m$

$\Rightarrow M\otimes_A N \to M\otimes_A P$ injective.

Application:

in linear algebra: $V \in k^{\text{Vect}}$, $\dim V < +\infty$, $\varphi: V\to V$ k-linear.

φ is inj $\Leftrightarrow \varphi$ is surjective $\Leftrightarrow \varphi$ is iso.

Prop: A ring. $\varphi: A^{\oplus n} \to A^{\oplus n}$ (A-linear).

(i) φ is inj. $\not\Rightarrow \varphi$ is iso. (反eg. $\mathbb{Z} \xrightarrow{\times 2} \mathbb{Z}$.)

(ii) φ is surj $\Rightarrow \varphi$ is iso.

Pf: consider: $0 \to K \to A^{\oplus n} \xrightarrow{\varphi} A^{\oplus n} \to 0$. ($K := \ker\varphi$) exact

希望prove. $K=0$. $\Leftarrow$ $K=0$是局部性质.

$\Leftrightarrow K_p = 0.\ \forall p$.

$\downarrow \otimes_A A_p$.

$0 \to K_p \to A_p^{\oplus n} \to A_p^{\oplus n} \to 0$ exact.

非flat有时也可保inj. $\to$ $\downarrow \otimes_{A_p} F$. ($F := A_p/p_p$).

$0 \overset{?}{\to} K_p\otimes F \to F^{\oplus n} \xrightarrow{\psi} F^{\oplus n} \to 0$. $\in F^{\text{Vect}}$ exact.

$\Rightarrow \psi$ is iso $\Rightarrow K_p\otimes F \simeq K_p \otimes_{A_p} (A_p/p_p)$
Vect.

$\simeq K_p/p_pK_p \simeq 0$

$\uparrow$ 作商与$\otimes$的交换性.

·又由 P32. ex.12. K_p f.g.

∴由 Nakayama Lem: $\Rightarrow K_p=0. \Rightarrow K=0.$

(Rmk: 局部化思路: $\to$ exact $\to$ 局部化 $\to$ Vect $\to$ Nakayama $\to$ 局部化 $\to$ #).

$0\xrightarrow{?}$ 的proof:

Lemma: $0\to M_1\to M_2\to M_3\to 0\in A^{Mod}$ exact. M_3 is flat. then

$0\to M_1\otimes_A N\to M_2\otimes_A N\to M_3\otimes_A N\to 0$. is exact 对$\forall N\in A^{Mod}$成立.

(Rmk: 由此可得 $0\xrightarrow{?}$ 的正确性.)

Pf: Consider $0\to K\to \underbrace{A^{\oplus I}}_{:=F}\xrightarrow{\psi} N\to 0$. exact. (可取I为N的生成元, $K=\ker(\psi)$).

$$\Rightarrow \begin{tikzcd}
 & 0 & 0 & 0 & \\
\ar[r] & M_1\otimes N \ar[u] \ar[r, "\otimes\text{右正合}"] & M_2\otimes N \ar[u] \ar[r] & M_3\otimes N \ar[u] \ar[r] & 0 \\
0 \ar[r, "F\text{ flat}"] & M_1\otimes F \ar[u] \ar[r] & M_2\otimes F \ar[u, "\otimes\text{的右正合性}"'] \ar[r] & M_3\otimes F \ar[u] \ar[r] & 0 \\
 & M_1\otimes K \ar[u] \ar[r] & M_2\otimes K \ar[u] \ar[r] & M_3\otimes K \ar[u] \ar[r] & 0 \\
 & \ker \ar[u] \ar[r] & \ker \ar[u] \ar[r] & 0 \ar[u, "M_3\text{ flat}"'] \ar[r] & {}
\end{tikzcd}$$

$\overset{\text{snake}}{\Longrightarrow}$ $0\to M_1\otimes N\to M_2\otimes N$ exact #.

日期: /

§3.3. Select prime ideals.

Prop1: A ring. $I\subseteq A$ ideal. ∃一一对应:

① $\{p\in \mathrm{Spec}(A) \mid p\supseteq I\} \xleftrightarrow{1:1} \mathrm{Spec}(A/I)$.

② $\{p \text{ is maximal in } A\} \xleftrightarrow{1:1} \{p/I \text{ is maximal in } A/I\}$.

Prop2: A ring. $S\subseteq A$ $(1\in S, S\cdot S\subseteq S)$. def $\sigma: A\to S^{-1}A$, $a\mapsto \frac{a}{1}$. then ∃一一对应:

$\mathrm{Spec}(S^{-1}A) \xleftrightarrow{1:1} \{p\in \mathrm{Spec}(A) \mid p\cap S=\emptyset\}$.

$S^{-1}p \longleftarrow p$

(Rmk: ① 即当且仅当 $p\cap S=\emptyset$ 时, $S^{-1}p$ 为真理想

② 可导出: A_p is a local ring.

Pf: $\mathrm{Spec}(A_p) \xleftrightarrow{1:1} \{q\subseteq A \mid q\cap (A\setminus p)=\emptyset\}$.

P_p is unique maximal $\longleftarrow$ p is unique maximal.

③ $I\subseteq S^{-1}A$ is maximal $\not\Rightarrow$ $\sigma^{-1}(I)$ is maximal.)

Pf: ① S^{-1}, σ^{-1} is well-defined. ($S^{-1}: I\to S^{-1}I$ $\quad \sigma: A\to S^{-1}A$, $a\mapsto \frac{a}{1}$)

(即左→右, 右→左良定)

S^{-1}:) 欲证: $p\in \mathrm{Spec}(A) \Rightarrow \begin{cases} S^{-1}p=S^{-1}A, & S\cap p\neq\emptyset \\ S^{-1}p\in \mathrm{Spec}(S^{-1}A), & S\cap p=\emptyset \end{cases}$

consider $S^{-1}A/S^{-1}p \simeq S^{-1}(A/p) = \begin{cases} 0, & S\cap p\neq\emptyset \\ \bar{S}^{-1}(A/p), & S\cap p=\emptyset, \ \bar{S}\equiv S \pmod p \end{cases}$

σ^{-1}:) $p\in \mathrm{Spec}(S^{-1}A) \Rightarrow \sigma^{-1}(p)\in \mathrm{Spec}(A)$, 且 $\sigma^{-1}(p)\cap S=\emptyset$.

日期:　　　/

② (i) $S^{-1}\sigma^{-1}(J) = J$ for $\forall J \in S^{-1}A$ ideal. (要放宽点).

(ii) $\sigma^{-1}S^{-1}(p) = p$ for $\forall p \in Spec(A)$, 且 $p \cap S = \emptyset$.

pf: (i): $\forall \frac{a}{s} \in S^{-1}\sigma^{-1}(J) \Rightarrow a \in \sigma^{-1}(J) \Rightarrow \frac{a}{1} \in J$.

$\frac{a}{s} = \frac{1}{s} \cdot \frac{a}{1} \in J \Leftarrow$ 　　$\Rightarrow S^{-1}\sigma^{-1}(J) \subset J$.

$\forall \frac{a}{s} \in J \Rightarrow \sigma(a) = \frac{a}{s} \cdot s \in J \Rightarrow a \in \sigma^{-1}(J) \Rightarrow \frac{a}{s} \in S^{-1}\sigma^{-1}(J)$.

$\Rightarrow J \subset S^{-1}\sigma^{-1}(J)$.

(ii) $p \subseteq \sigma^{-1}S^{-1}(p) \Leftarrow \sigma(p) \subseteq S^{-1}(p)$. √.

$x \in \sigma^{-1}S^{-1}(p) \Rightarrow \frac{x}{1} = \frac{y}{s}$　$s \in S, y \in p$.

$\Rightarrow \exists t \in S,\ tsx = ty$. $\Rightarrow tsx \in p$

又 $t, s \in S$ .. $S \cap p = \emptyset$. $\Rightarrow x \in p$.

$\Rightarrow p \supset \sigma^{-1}S^{-1}(p)$.　#.

日期: /

§4.1 Notherian ring & module

(v.s. finite dimensional spaces).

Def: A ring. $M \in {}_A\mathrm{Mod}$. M is notherian if $\forall$ submodule is f.g.

A is a notherian ring if A as a module $\in {}_A\mathrm{Mod}$ is notherian.

Prop 1: (1)

$$\begin{tikzcd}
\text{域} \arrow[r] & \mathrm{ED} \arrow[r, Rightarrow] & \mathrm{PID} \arrow[r] \arrow[dl] \arrow[d] & \mathrm{UFD} \arrow[d] & \text{非整交换环} \\
 & \mathrm{Noeth} \arrow[r, dash] & \mathrm{Bezout} \arrow[u] \arrow[r] & \mathrm{GCD}\text{整环} \arrow[r] & \text{整环} \arrow[u]
\end{tikzcd}$$

(2) A notherian $\Rightarrow$ A/I, $S^{-1}A$ notherian. ($\forall I, S$). → 构造notherian 的方法

(3) (Hilbert's Basis Thm) A noetherian, B is f.g. A-algebra.

$\Rightarrow B$ notherian.

def: B is A-algebra: $A \to B \begin{cases} B \in {}_A\mathrm{Mod} \\ B \text{ is ring. (即:有乘法)} \end{cases}$

$\Rightarrow$ eg. if A notherian, then

$A[x_1, \cdots, x_n]$, $A[x_1, \cdots, x_n]/I$, $S^{-1}A[x_1, \cdots, x_n]$ 均 notherian.

补充: $E_\lambda := \mathbb{Q}[x, y]/(y^2 - x(x-1)(x-\lambda))$, $\lambda \neq 0, 1$. ← 椭圆曲线

1° knowledge of E_λ implys Fermat's Last Thm.

2° 千禧八大问题 BSD conjecture is about E_λ.

---

(4) a subring of notherian ring may not be Notherian.

eg. $A = k[x_1, \cdots, x_n, \cdots]$ is not f.g.

but $\mathrm{Frac}(A)$ is a field.

日期: /

eg. $\mathcal{O}_{\mathbb{C},0}$ = the ring of germs of holo functions at 0. (全纯函数环)

$= \{$收敛的形式幂级数 $\underbrace{\sum_{n=0}^{+\infty} a_n x^n}_{= z^k \cdot u}\}$.

$\rightsquigarrow$ PID.

更一般地, $\mathcal{O}_{\mathbb{C}^n,0}$ 也是 notherian ring. (is local ring).

$\Rightarrow$ 有关 notherian 的性质可以用在复几何中.

4') $\boxed{\text{(Hilbert Invariance Thm)}}$ (广义对称多项式的有限生成性)

Thm: Assume a f.g. subgroup $G \subseteq \mathrm{Aut}_k(\bigoplus_{i=1}^{n} kx_i)$ ← 即对 $x_1,\cdots,x_n$ 作线性变换.

then G acts on $k[x_1,\cdots,x_n]$ by:

$\rho: g(f(x)) = f(g^{-1}(x))$. $x = (x_1,\cdots,x_n)$.

• Symmetric polynomial: (对称多项式).

$f \in k[x_1,\cdots,x_n]$ is Symmetric poly. if $f(x) = f(\sigma(x))$. $\forall \sigma \in S_n$.

则 S_n act on $k[x_1,\cdots,x_n]$ by:

$\rho: \sigma(f(x)) = f(\sigma^{-1}(x))$.

则记 $k[x_1,\cdots,x_n]^{S_n} = \{f \mid \sigma f = f, \forall \sigma \in S_n\}$ = the ring of sym. poly.

$= k[s_0,\cdots,s_n]$ ($s_0 = x_1 + \cdots + x_n$, $s_n = x_1 \cdots x_n$. 即 $k[x_1,\cdots,x_n]^{S_n}$ f.g.).

$\rightsquigarrow$ Q: 如果将 S_n 替换, 是否还有限生成?

(Rmk: S_n 中元对应基本矩阵, 而 $\mathrm{Aut}_k(\bigoplus_{i=1}^{n} kx_i)$ 对应 $\forall n$ 阶矩阵).

记 $k[x_1,\cdots,x_n]^G = \{f \in k[x_1,\cdots,x_n] \mid \sigma f = f, \forall \sigma \in G\}$

日期: /

then, is finitely generated k-algebra. (从而是 Notherian).

Rmk: (Hilbert's 14's problem):

Q: what if $G \subseteq GL_n(k)$ is NOT f.g.?

- Nagata: NO.
- $k[x_1, \cdots, x_n]^G$ is finitely generated

  if $G \subseteq GL_n(k)$ is $\begin{cases} \text{reductive when } char(k)=0. \\ \text{geometry reductie when } char(k)>0. \end{cases}$

Noeth环的性质

Thm: $M \in A^{Mod}$. Notherian

$\Leftrightarrow$ every chain of submodules $0 \subseteq M_1 \subseteq \cdots \subseteq M_n \subseteq \cdots$,

$\exists m$, s.t $M_m = M_{m+1} = \cdots$

Prop: let $0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$. exact. then.

M is notherian $\Leftrightarrow$ M', M'' are notherian

Pf: $\Rightarrow$). ① $\forall$ chain in M', $\rightsquigarrow$ a chain in M.

② $\forall$ chain in M'': $0 \subseteq N_1 \subseteq N_2 \subseteq \cdots$

$$\downarrow g^{-1}$$

$0 \subseteq g^{-1}(N_1) \subseteq g^{-1}(N_2) \subseteq \cdots (\subseteq M)$ Stationary.

$$\downarrow g$$

$0 \subseteq N_1 \subseteq \cdots$ $(\subseteq M'')$ stationary.

$\Leftarrow$) let $0 \subseteq N_1 \subseteq \cdots$ be chain in M.

then $0 \subseteq \overset{\simeq M'\cap N_1}{f^{-1}(N_1)} \subseteq \cdots$ $(\subseteq M')$ stationary.

$0 \subseteq \overset{\simeq (N_1+M')/M'}{g(N_1)} \subseteq \cdots$ $(\subseteq M'')$ stationary.

$$\rightsquigarrow \begin{cases} M'\cap N_m = M'\cap N_{m+1} = \cdots \\ (N_m+M')/M' = (N_{m+1}+M')/M' = \cdots \end{cases}$$

$\rightsquigarrow N_m = N_{m+1} = \cdots \rightsquigarrow M$ notherian. #

Cor: If $M_1, \cdots, M_n \in A^{\mathrm{Mod}}$ is notherian $\Rightarrow \bigoplus_{i=1}^{n} M_i$ is notherian.

Rmk: $\oplus$ 保 Noeth 性.

Prop: A = notherian ring. $M \in A^{\mathrm{Mod}}$ f.g. $\Rightarrow M$ is notherian.

Pf: $M \simeq A^{\oplus n}/N$. ∴ 由 Cor, M is notherian.

Cor: A = notherian ring. $I \subseteq A \Rightarrow A/I$ is notherian. 商环仍 noeth.

Pf: $A/I \in A^{\mathrm{Mod}}$ is f.g.

$\Rightarrow A/I \in A^{\mathrm{Mod}}$ is notherian.

$\Rightarrow \forall\, 0 \subseteq J_1 \subseteq \cdots$ chain in A/I (ring)

自然地是 chain in A/I (module).

Cor: A notherian. $B \in A^{\mathrm{Mod}}$ is f.g. $\overset{\simeq A[x_1,\cdots,x_r]/\ker(\varphi)}{A\text{-algebra}}$. Then B is notherian as a ring.

Pf: $\forall$ ideal of B is an A sub-module. #

(Rmk: Assume B is f.g. by $y_1, \cdots, y_n$, 则 as a A-algebra $\Leftrightarrow \forall y \in B$ 为 $y_1, \cdots, y_n$ 的多项式; as a ring $\Leftrightarrow \forall y \in B$ 为 $y_1, \cdots, y_n$ 的线性组合)

日期: /

Prop: A = noeth. $S \subseteq A$ then, $S^{-1}A$ = noeth.

Pf: Fact: $A \xrightarrow{\sigma} S^{-1}A$ 有 $J = S^{-1}(\sigma^{-1}(J))$.

对 $S^{-1}A$ 上: $\forall\ 0 \subset J_1 \subset J_2 \subset \cdots$

$\Rightarrow A$ 上: $0 \subset \sigma^{-1}(J_1) \subset \sigma^{-1}(J_2) \subset \cdots$ stable ← A noeth.

$\Rightarrow S^{-1}A$ 上: $0 \subset \underbrace{S^{-1}\sigma^{-1}(J_1)}_{=J_1} \subset \underbrace{S^{-1}\sigma^{-1}(J_2)}_{=J_2} \subset \cdots$ Stable.

$\Rightarrow\ 0 \subset J_1 \subset J_2 \subset \cdots$ Stable. #

Cor: A noetherian. $p \in \operatorname{Spec}(A)$. $\Rightarrow A_p$ is notherian.

Thm (flat module 的刻画). (P29, P30, P39).

① A is local noetherian ring, $M \in A^{Mod}$ f.g., then

M flat $\Leftrightarrow$ M free.

② A is noetherian ring, $M \in A^{Mod}$ f.g. TFAE:

1) M is flat.

2) M_p is free A_p-module $\forall\ p \in \operatorname{Spec}(A)$.

(Rmk: f.g. flat module $\xrightarrow{\text{geometry}}$ 向量丛.)

Pf: ① let $m \subseteq A$ be A's maximal ideal. 记 $k := A/m$. $\to$ field

日期: /

由 m. f.g. $\therefore \exists x_1,\cdots,x_r \in M$. s.t. $x_1 \bmod mM, \cdots, x_r \bmod mM \in \underbrace{M/mM}_{} \in k^{Mod}$.

为 M/mM 的一组基. $= M\otimes_A A/m = M\otimes_A k$. $A\to k$. 换环.

By Nakayama Prop 2.8. $x_1,\cdots,x_r$ generate M.

def. $\varphi: A^{\oplus r} \to M$. 为满射
$e_i \mapsto x_i$.

Consider: $0 \to K \to A^{\oplus r} \to \overset{\text{flat}}{M} \to 0$.

$$\Rightarrow \quad 0 \to K\otimes_A k \to \underbrace{k\otimes_A A^{\oplus r}}_{= k^{\oplus r}} \xrightarrow{\cong} k\otimes_A M \to 0.$$

$\Uparrow$
$e_i \mapsto x_i \bmod mM$.

$\Rightarrow \quad K/mK \simeq K\otimes_A k = 0$.

By Nakayama Prop 2.6: $K=0$ if K f.g. $\Leftarrow$ A noethrian $\Rightarrow A^{\oplus r}$ noetherian $\Rightarrow K$ noetherian. #

② ①+P39. Cor3. #.

Thm: $\boxed{\text{(Hilbert's Basis Thm)}}$

A noetherian $\Rightarrow A[x]$ noetherian.

Pf: let $J \subseteq A[x]$ is ideal.

def $I = \{a_n \in A \mid f(x) = b_n x^n + b_{n-1}x^{n-1} + \cdots + b_0 \in J\} \subseteq A$.

A noetherian $\Rightarrow I = (a_1,\cdots,a_r)$.

由 I def. 令 $f_i = a_i x^{r_i} +$ lower terms $\in J$. 记 $J_0 = (f_1,\cdots,f_r)$.

*: 对 $\forall g \in J$, $g = g_m x^m + \cdots$

若 $m \geq \max\{r_i\}$. 由 $g_m = \sum_{i=1}^{r} a_i h_i$.

$\therefore g'(x) = g(x) - \sum_{i=1}^{r} h_i f_i(x) \cdot x^{m-r_i} \in J$. 且 $\deg(g') \leq m-1$.

$\Rightarrow \forall g \in J$, 有分解: $g = h + f$. $f \in J_0$, $\deg(h) < \max\{r_i\}$.

$\Rightarrow$ let $M = \bigoplus_{i=1}^{\max\{r_i\}} Ax^i \subseteq A[x]$.

则有, $J = \underset{\text{低次}}{(J \cap M)} + \underset{\text{高次}}{J_0}$.

A noetherian $\Rightarrow M$ notherian $\Rightarrow J \cap M$ f.g. $\Rightarrow J$ f.g.

Application: (零化多项式).

*: $V \in {}_k\text{Vect}$, $\dim V < +\infty$, let $\varphi \in \text{End}_k(V)$.

$I_\varphi = \{f(t) \in k[t] \mid f(\varphi) = 0\} \subseteq k[t]$ (is ideal)

- 由 Caylay-Hamilton: $I_\varphi \neq 0$.
- $k[t]$ is PID $\Rightarrow \exists f_{min} \in k[t]$, s.t. $I_\varphi = (f_{min})$.

Extension: A ring. $M \in A^{\text{Mod}}$. $\varphi \in \text{End}_A(M)$.

$I_\varphi = \{f \in A[x] \mid f(\varphi) = 0\} \subseteq A[x]$. (is ideal).

(Rmk: $A[x]$ may NOT be a PID if A is NOT a field)

- $\exists f_{min} \in A[x]$ s.t. $I_\varphi = (f_{min}) \Leftrightarrow I_\varphi$ is principal. (f_{min}存在的充要条件).
- I_φ is always f.g. if A is noetherian.

日期: /

Nullstellensatz

Thm (Strong Nullstellensatz). (SHN).

Let k be a field, E a f.g. k-algebra $(E\simeq k[x_1,\cdots,x_n]/I)$. if E is a field.

Then $[E:k]<+\infty$.

Lem: let $A\subseteq B\subseteq C$ be rings. s.t.

① A Noetherian.

② C is a f.g. A-algebra

③ C is a f.g. B-module.

$\Rightarrow B$ is a f.g. A-algebra.

Thm Pf: 由 E is a f.g. k-algebra.

∴ 不妨设 $E=k[x_1,\cdots,x_n]$. (x_i可能为代数元或超越元).

不妨 $\Rightarrow$ 分开. def $F=k(x_1,\cdots,x_r)$,

s.t. $F\subseteq E$ is algebraic & $k\subseteq F$ is transcendential.

Consider $k\subseteq F\subseteq E$. 满足Lem的3个条件.

$\Rightarrow F$ is f.g. k-algebra.

Aim: $F=k(x_1,\cdots,x_r)\overset{?}{=}k$.

if NOT, then 任取 f.g. k-algebra, $F=k[\frac{f_1}{g_1},\cdots,\frac{f_m}{g_m}]$, $f_i,g_i\in k[x_1,\cdots,x_r]$ (UFD).

choose a prime 因子 h of $g_1\cdots g_m+1$.

$\Rightarrow \frac{1}{h} \notin k[\frac{f_1}{g_1}, \cdots, \frac{f_m}{g_m}]$. 而 $h \in F$.

$\Rightarrow F' \subsetneq F$.

$\Rightarrow$ 这与 F 为 f.g. k-algebra 矛盾. $\therefore F = k$.

$\Rightarrow [E:k] = [E:F] < +\infty$. #

Lem Pf: Assume: C is f.g. by $x_1, \cdots, x_n \in C$ as A-algebra.

C is f.g. by $y_1, \cdots, y_m \in C$ as B-module.

$$\Rightarrow \begin{cases} x_i = \sum_j b_{ij} y_j. & ① \\ y_i y_j = \sum_k b_{ijk} y_k. & ② \end{cases}$$

let $B_0 = A[b_{ij}, b_{ijk}]$.

Consider $A \subseteq B_0 \subseteq B \subseteq C$.

由 $\forall\, \xi \in C$, $\xi = f(x_1, \cdots, x_n)$. (系数 $\in A$).

$\overset{①}{=} g(y_1, y_2, \cdots, y_m)$ (系数 $\in A[b_{ij}]$).

$\overset{②}{=} \sum_i b_i y_i$ (二次以上被化掉, 系数 $\in A[b_{ij}, b_{ijk}]$).

$\Rightarrow$ C is f.g. as B_0-module

又 $\because B_0$ is f.g. as A-algebra $\overset{HBT}{\Longrightarrow} B_0$ is notherian. ring.

$\Rightarrow C \in {}_{B_0}\mathrm{Mod}$ is Noetherian.

$\Rightarrow B \in {}_{B_0}\mathrm{Mod}$ is f.g. B-algebra

日期: /

又 B_0 f.g. is f.g. A-algebra.

$\Rightarrow B$ is f.g. A-algebra. #

Cor 1: ① k field. A f.g. k-algebra, $m \subseteq A$ maximal.

Then, $[A/m : k] < +\infty$.

② if $k = \bar{k}$, then $A/m \simeq k$.

Cor 2: (即代数学基本定理 FTA).

If $k = \bar{k}$, $A = k[x_1, \cdots, x_n]$. $m \subseteq A$ is maximal.

则 $\exists\, a_1, \cdots, a_n \in k$, s.t. $m = (x_1 - a_1, \cdots, x_n - a_n)$.

Pf: $A/m \simeq k$

$x_i \mapsto a_i = \varphi(x_i \bmod m)$.

$\Rightarrow x_i - a_i \bmod m \in \ker(\varphi)$.

$\Rightarrow x_i - a_i \in m$.

$\Rightarrow (x_1 - a_1, \cdots, x_n - a_n) \subseteq m$.

↳ maximal

$\Rightarrow (x_1 - a_1, \cdots, x_n - a_n) = m$.

Rmk: 即 $\exists\, k^n \xleftrightarrow{1:1} \{\text{maximal ideal of } k[x_1, \cdots, x_n]\}$.

Ext. to Alg. Set:

$\Sigma \subseteq k[x_1, \cdots, x_n]$, $S \subseteq k^n$.

① $V(\Sigma) = V((\Sigma)) = V(\underbrace{r(\Sigma)}_{\text{根式理想}})$.

(HBT)

- $\forall \Sigma$. (even $\#\Sigma = +\infty$), 有:

$$V(\Sigma) \overset{\text{无限}}{=} V(\langle\Sigma\rangle) \overset{\text{HBT.}}{=} V(\underbrace{f_1,\cdots,f_r}_{\text{有限}}).$$

② $V(I(V(\Sigma))) = V(\Sigma)$.

$r(J) \subseteq I(V(J))$.

(Nullstellensate)

- if $k=\bar{k}$, then

$r(J) = I(V(J))$.

In particular, $J = I(V(J))$ if $J = r(J)$. is radical.

Thm: if $k=\bar{k}$, Then $\exists$ 1:1 correspondence:
(HC).

$$\{\text{alg. set in } k^n\} \underset{V}{\overset{I}{\rightleftarrows}} \{\text{radical ideals of } k[x_1,\cdots,x_n]\}.$$

satisfy:

① $V(0) = k^n$, $V(k[x_1,\cdots,x_n]) = \emptyset$.

$\boxed{②}$ $I \subseteq J \iff V(I) \subseteq V(J)$. (radical ideal)($\Rightarrow$无须$k=\bar{k}$)

$\boxed{③}$ $V(I) = V(J) \iff r(I) = r(J)$. (ideal) ($\Leftarrow$无须$k=\bar{k}$).

④ $\cdot V(\sum I_i) = \cap V(I_i)$

$\cdot I(\cap V_i) = r(\sum I(V_i))$.

⑤ $V(IJ) = V(I \cap J) = V(I) \cup V(J)$.

$I(V_1 \cup V_2) = I(V_1) \cap I(V_2)$.

日期: /

⑥ · $V(I(S))=S$ iff $S=V(J)$. for some ideal

$\boxed{\cdot}$ $I(V(J))=J$. iff $J=r(J)$.

Cor: (Generalization of FTA) $k=\bar{k}$, 则.

$V(I)=\emptyset \iff r(I)=(1)$.

· Cor: $k=\bar{k}$, then $V(f_1,\cdots,f_r)=\emptyset \iff 1=\sum f_i g_i$. for some $g_1,\cdots,g_r\in k[x_1,\cdots,x_n]$.

Lem1: $J\subseteq A$ ideal, then $r(J)=\bigcap\limits_{\substack{J\subseteq p,\\ p\in Spec(A)}} p$.

(radical ideal) 的刻画.

pf: Consider: $\varphi: A\to A/J$.

then $\varphi^{-1}(r(0))=r(J)$.

Claim: $r(0)=\bigcap\limits_{p\in Spec(A)} p$.

pf: $\subseteq$:) $\forall x\in r(0)$. $x^n=0\in p \Rightarrow x\in p$.

$\supseteq$:) Assume $x\notin r(0)$.

let Σ be ideals J of A s.t. $x^n\notin J$. $(\exists n>0)$.

· $\Sigma\neq\emptyset$. $(0\in\Sigma)$ $\xRightarrow{\text{Zorn引理}}$ $\exists$ maximal object J_0 in Σ.

· J_0 is prime): let $a,b\notin J_0$, then $(a)+J_0, (b)+J_0\notin\Sigma$.

$\Rightarrow \exists m_a, m_b\geq 1$, s.t. $x^{m_a}\in(a)+J_0$, $x^{m_b}\in(b)+J_0$.

日期: /

$\Rightarrow x^{m_a+m_b} \in (ab)+J_0 \Rightarrow (ab)+J_0 \notin \Sigma$

$\Rightarrow ab \notin J_0$.

Cor: ideal $J \subseteq A$ is radical $\Leftrightarrow$ $J = \bigcap_{\substack{J \subseteq p \\ p \in Spec(A)}} p$.

Thm-Pf: • $r(J) \subseteq I(V(J))$. ✓

• $r(J) \supseteq I(V(J))$:)

$\Leftrightarrow \forall f \notin r(J) \Rightarrow f \notin I(V(J))$.

$\Leftrightarrow \exists a \in V(J)$, s.t. $f(a) \neq 0$

$\Leftrightarrow \exists$ maximal ideal m_a s.t. $J \subseteq m_a$ & $f \notin m_a$.

Lem 2: k field. A, B f.g. k-alg. $\varphi: A \to B$ hom.

$m \subseteq B$ maximal $\Rightarrow \varphi^{-1}(m) \subseteq A$ maximal.

Rmk: 对 prime ideal 的拉回是平凡的;

对maximal ideal 的拉回一般不成立,但在f.g. k-alg.上是成立的.

Consider $k \subseteq A/\varphi^{-1}(m) \subseteq B/m \begin{cases} \text{field} \\ \text{f.g. } k\text{-alg.} \end{cases} \Rightarrow [B/m : k] < +\infty$

$\Rightarrow A/\varphi^{-1}(m)$ is field $\Rightarrow \varphi^{-1}(m) \subseteq A$ is maximal ideal.

日期: /

Lem3: A f.g. k-alg, $I \subseteq A$ ideal, then

$$r(I) = \bigcap_{\substack{I \subseteq m \\ \text{maximal ideal}}} m$$

<= $r(J)$的刻画在 f.g. k-alg.上的加强.

Pf: Step 1: 设 $f \notin r(I) \Rightarrow$ ($r(I)$刻画) $\exists p \in Spec(A)$ s.t.

$I \subseteq p$ & $f \notin p$ ($\Leftrightarrow \{f^n\} \cap p = \emptyset$).

Step 2: Find maximal ideal m s.t.

$p \subseteq m$ & $f \notin m$.

Consider: $\varphi: A \to A/p$ ($\bar{f} = \varphi(f)$).

$\psi: A/p \to (A/p)_{(\bar{f})} := S^{-1}(A/p)$. ($S = \{\bar{f}^n\}$).

对 prime/maximal ideal 的筛选 (商/分式化)

又 $(A/p)_{(\bar{f})} = (A/p)[\frac{1}{\bar{f}}] \subseteq Frac(A/p)$. <= $(A/p)_{(\bar{f})}$即用于筛选极大理想ideal 所用的环.

$\Rightarrow$ $(A/p)_{(\bar{f})} \neq 0$. $\leftarrow$ A/p为domain.

A/p f.g. k-alg. $\Rightarrow (A/p)[\frac{1}{\bar{f}}]$ f.g. k-alg. $\Rightarrow (A/p)_{(\bar{f})}$ f.g. k-alg.

$\Rightarrow \exists$ maximal ideal $\bar{m} \subseteq (A/p)_{(\bar{f})}$.

$\uparrow \subseteq$ $\uparrow \notin$

由Lem2: $(\psi \circ \varphi)^{-1}(\bar{m})$ is maximal ideal in A.

$(A/p)_{(\bar{f})} \to$ s.t. $p \subseteq m$ & $f \notin m$.

由 $f \notin r(J) \Rightarrow \exists$ maximal ideal m_2 s.t. $J \subseteq m_2$ & $f \notin m_2$. #.

日期:
(Utilization.).

Thm (Ax-Grothendieck)

$\mathbb{C}^n \xrightarrow{P} \mathbb{C}^n$ polynomial map.

则 P injective $\Rightarrow P$ surjective.

Pf: Step1: ($\Rightarrow$ finite field).

$\mathbb{F}_q^n \xrightarrow{P} \mathbb{F}_q^n$ polynomial map,

P inj $\Rightarrow P$ surj.

Step2: $P=(P_1,\cdots,P_n)$. $P_i\in\mathbb{C}[x_1,\cdots,x_n]$.
(几何→代数)

① P inj. $\Leftrightarrow$ $P(x)=P(y)\Rightarrow x=y$.

$\Leftrightarrow V((P_1(x)-P_1(y),\cdots,P_n(x)-P_n(y))\subseteq V((x_1-y_1,\cdots,x_n-y_n))$.

$\overset{HC}{\Leftrightarrow}$ $(x_1-y_1,\cdots,x_n-y_n)\subseteq r(P_1(x)-P_1(y),\cdots,P_n(x)-P_n(y))$.

$\Leftrightarrow$ $(x_j-y_j)^{r_j}=\sum_{i=1}^{n}(P_i(x)-P_i(y))Q(x,y)$. (*).

② P不是 surj. $\Leftrightarrow \exists z\in\mathbb{C}^n$, s.t. $P^{-1}(z)=\emptyset$.

$\Leftrightarrow V(P_1(x)-z,\cdots,P_n(x)-z)=\emptyset$.

$\overset{HC}{\Leftrightarrow}$ $\sum_{i=1}^{n}(P_i(x)-z)R_i(x)=1$ (**).

$\boxed{\text{Step3: (mod } m).}$ ☆

let $S\subseteq\mathbb{C}$ generated by $\mathbb{Z}$ and all coefficience of P_i, Q_i, R_i

$\Rightarrow$ (*),(**) defined on S.

let $m \subseteq S$ maximal ideal

$\Rightarrow S/m$ is a field & is f.g. as a $\mathbb{Z}$-algebra.

Claim: $\mathbb{Z} \to S/m$ is NOT injective.

$\Rightarrow \ker \neq \emptyset$.

$\Rightarrow \exists$ prime $p \in \mathbb{Z}$, $\mathbb{Z}/p\mathbb{Z} \underset{SHN}{\overset{f.g.}{\subseteq}} S/m$.

$\Rightarrow S/m \simeq \mathbb{F}_{p^r}$.

$\overset{\text{对}(*),(**), P \bmod m}{\Longrightarrow}$ $P \pmod m: \mathbb{F}_{p^r} \to \mathbb{F}_{p^r}$ s.t. $(*)(**)$ hold.

$\Longrightarrow$ $P \pmod m$ inj. 但不 surj.

由Step 1 #.

Pf of Claim: If $\mathbb{Z} \to S/m$ is injective.

$\Rightarrow \mathbb{Q} \xrightarrow[f.g]{} S/m$.

$\overset{SHN}{\Rightarrow} [S/m : \mathbb{Q}] < +\infty$.

$\Rightarrow \exists e_1, \cdots, e_r \in S/m$, s.t. $S/m = \bigoplus_{i=1}^{r} \mathbb{Q} e_i$

设 $S/m = \mathbb{Z}[x_1, \cdots, x_n]$

$\overset{\text{通分}}{\Rightarrow} \exists q \in \mathbb{Z}$ s.t. $q x_i \in \bigoplus_{i=1}^{r} \mathbb{Z} e_i$

$\Rightarrow \bigoplus_{i=1}^{r} \mathbb{Q} e_i = S/m = \bigoplus_{i=1}^{r} \mathbb{Z}[\frac{1}{q}] e_i$. 矛盾.

日期: /

Rmk: · 几何 $\overset{HC}{\Longleftrightarrow}$ 代数 $\overset{\text{mod}\,m}{\Longrightarrow}$ 有限域.

· GHC:

* : {alg. subscheme in k^n} $\overset{I,V}{\longleftrightarrow}$ {ideals of $k[x_1,\cdots,x_n]$}.
(= alg. set with 重数).

* : {subscheme of $\mathrm{Spec}(A)$} $\overset{I,V}{\longleftrightarrow}$ {ideals of A}.

rmk: 几何行 ⇐ 去看图行.

日期: /

代數數論.

Leading Problem 1:

Fermat's Last Theorem:

$x^n+y^n=z^n$, $x,y,z\in\mathbb{Z}$, $n\geq 3$. $\Rightarrow xyz=0$.

We want to prove:

Thm (Kummer): $p\geq 5$ is a regular prime. Then,

$x^p+y^p=z^p$, $p\nmid xyz$ has no solution in $\mathbb{Z}$.

(Rmk: Kummer's proof也证明了$p\mid xyz$的情况,但是较复杂,这里不作证明)

Case $n=2$:

Step1: Assume x,y,z 互素且 $2\nmid z$.

在$\mathbb{C}$上分解 $\downarrow$

Step2: $\overset{分解}{\Longrightarrow}$ $(x+iy)(x-iy)=z^2$ in $\mathbb{Z}[i]=\{a+bi\mid a,b\in\mathbb{Z}\}$.

Fact: · $\mathbb{Z}[i]$ is UFD · $\mathbb{Z}[i]^*=\{\pm1,\pm i\}$ ⟵ 在$\mathbb{C}$上易刻画 <= 可逆元的刻画.

UFD $\downarrow$

Step3: $x+iy$, $x-iy$ coprime.

pf: if $\exists$ prime $\pi\in\mathbb{Z}[i]$ s.t. $\pi\mid x+iy$, $\pi\mid x-iy$.

$\Rightarrow \pi\mid z$, $\pi\mid 2x$ <= 唯一因子分解.

但 $\overset{\mathbb{Z}上}{(2x,z)=\mathbb{Z}}$ $\Rightarrow 2xf+zg=1 \Rightarrow \overset{\mathbb{C}上}{(2x,z)=}\mathbb{Z}[i]\supseteq(\pi)$. 矛盾.

Step4: $\overset{UFD}{\Longrightarrow}$ $x+iy=u\cdot a^2$ $u\in\mathbb{Z}[i]^*$, $\underset{=m+ni}{a}\in\mathbb{Z}[i]$.

$\Rightarrow (x,y,z)=(\pm(m^2-n^2), \pm 2mn, \pm(m^2+n^2))$

日期: /

一般地, $x^p+y^p=z^p$

[由于$(x+1)\cdots(x+\zeta^{p-1})=x^p+1$. (对$x$同样有$0,1,\cdots,\zeta^{p-1}$共$p$个根).
∴作为对y的方程有$0,1,\zeta,\cdots,\zeta^{p-1}$共$p$个根, 从而恒等]

$\overset{分解}{\Longrightarrow}$ $(x+y)(x+\zeta y)(x+\zeta^2 y)\cdots(x+\zeta^{p-1}y)=z^p$, $\zeta=e^{\frac{2\pi i}{p}}\in\mathbb{C}$.

- we should study: $\mathbb{Z}[\zeta]=\{a_0+a_1\zeta+\cdots+a_{p-1}\zeta^{p-1}\mid a_i\in\mathbb{Z}\}$.

Q1: Is $\mathbb{Z}[\zeta]$ UFD? Yes. iff $p\le 19$. (But, Kummer: 扩充到理想后有UF).

Q2: What is $\mathbb{Z}[\zeta]^*$? Kummer: $u\in\mathbb{Z}[\zeta]^*\Rightarrow\frac{u}{\bar{u}}=\zeta^k$ for some k.

Def: (理想数) [Kummer].

An ideal number I of $\underset{\text{Noeth.}}{\mathbb{Z}[\zeta_p]}$ is a subset

$I=\{\sum a_i\xi_i\mid a_1,\cdots,a_r\in\mathbb{Z}[\zeta_p]\}$ for some $\xi_1,\cdots,\xi_r\in\mathbb{Z}[\zeta_p]$.

(在 $\mathbb{Z}[\zeta_p]$上 $\Leftrightarrow$ ideal).

Thm: (Kummer).

$\forall p$, $I\subseteq\mathbb{Z}[\zeta_p]$ ideal. Then $\exists!$ $I=\beta_1^{r_1}\cdots\beta_s^{r_s}$. , $\beta_1,\cdots,\beta_s\in\mathrm{Spec}(\mathbb{Z}[\zeta_p])$.

Lemma: ① $[\mathbb{Q}(\zeta_p):\mathbb{Q}]=p-1$.

$\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})\simeq(\mathbb{Z}/p\mathbb{Z})^*$.

② $(1-\zeta)$ is a prime ideal in $\mathbb{Z}[\zeta_p]$. $(\zeta:=\zeta_p)$.

$(p)=(1-\zeta)^{p-1}$. $(p\in\mathbb{Z}$ prime$)$.

③ $(1-\zeta)=(1-\zeta^i)$ $i=1,\cdots,p-1$.

日期: /

$p\to$ 某次方为1.

④ 单位根 in $\mathbb{Z}[\zeta_p]$ are $\{\pm\zeta^k\}$ (即 $\forall a^m=1, a\in\mathbb{Z}[\zeta_p]$, $\exists l$, s.t $a=\zeta_p^l$)

Pf: ① $\sigma^{(k)}\in Gal(\mathbb{Q}(\zeta_p)/\mathbb{Q})$: $\mathbb{Q}(\zeta_p)\longrightarrow\mathbb{Q}(\zeta_p)$.

$$\zeta_p\longmapsto\zeta_p^k.$$

易有 $\sigma^{(i)}\sigma^{(j)}=\sigma^{(ij)}$. $\Rightarrow Gal(\mathbb{Q}(\zeta_p)/\mathbb{Q})\simeq(\mathbb{Z}/p\mathbb{Z})^*$

$\overset{\text{Galios}}{\Rightarrow}[\mathbb{Q}(\zeta_p):\mathbb{Q}]=p-1$.

③ $1-\zeta^i=(1-\zeta)(1+\zeta+\zeta^2+\cdots+\zeta^{i-1})\Rightarrow(1-\zeta^i)\subseteq(1-\zeta)$.

$(i,p)=1\Rightarrow ai+bp=1.\Rightarrow(\zeta^i)^a=\zeta.\overset{\text{类似地}}{\Longrightarrow}(1-\zeta)\subseteq(1-\zeta^i)$.

② 由 $\mathbb{Z}[\zeta]/(1-\zeta)\overset{\zeta\mapsto1}{\simeq}\mathbb{Z}$ integral. $\Rightarrow(1-\zeta)$ is prime.

又 $x^p-1=(x-1)(x-\zeta)\cdots(x-\zeta^{p-1})$.

$\Rightarrow(x-\zeta)\cdots(x-\zeta^{p-1})=x^{p-1}+\cdots+1$

$\overset{x=1}{\Rightarrow}(1-\zeta)\cdots(1-\zeta^{p-1})=p$.

$\Rightarrow(p)=(1-\zeta)^{p-1}$.

④ lem: $\zeta_m\in\mathbb{Q}(\zeta_n)$. $\Rightarrow m|n$ or $2\nmid n$ & $m|2n$. ($\Leftrightarrow\varphi(m)|\varphi(n)$).

$\Updownarrow$

pf: $\mathbb{Q}(\zeta_m)\subseteq\mathbb{Q}(\zeta_n)\subseteq\mathbb{Q}(\zeta_{mn})$.

$\Updownarrow$ Galios (rmk: ① 对合数m也是对的).

$Ker((\mathbb{Z}/mn\mathbb{Z})^*\to(\mathbb{Z}/n\mathbb{Z})^*)$

$\cap|$

$Ker((\mathbb{Z}/mn\mathbb{Z})^*\to(\mathbb{Z}/m\mathbb{Z})^*)$. $\boxed{((\mathbb{Z}/pq\mathbb{Z})^*\simeq(\mathbb{Z}/p\mathbb{Z})^*\times(\mathbb{Z}/q\mathbb{Z})^*)}$

$\Rightarrow$ By CRT, 可 Assume $m=q_1^{r_1}$, $n=q_2^{r_2}$, q_1,q_2 prime.

日期:　　　/

$$\Rightarrow \begin{tikzcd} (\mathbb{Z}/mn\mathbb{Z})^* \arrow[r] \arrow[d] & (\mathbb{Z}/n\mathbb{Z})^* \arrow[dl, dashed, "\exists!"] \\ (\mathbb{Z}/m\mathbb{Z})^* & \end{tikzcd}$$

子群 $\Rightarrow \varphi(m) \mid \varphi(n). \Leftrightarrow m \mid n$ or $2 \nmid n \,\&\, m \mid 2n.$ #.

Kummer's Lem:

$u \in \mathbb{Z}[\zeta_p]^*$. Then $\frac{u}{\bar{u}} = \zeta_p^k$ for some k.

Pf: let $f \in \mathbb{Z}[X]$ s.t. f 为 $\frac{u}{\bar{u}}$ 的定义多项式.

$\Rightarrow f(\frac{u}{\bar{u}}) = \prod (X - \sigma(\frac{u}{\bar{u}}))$. ? (Galios)

$\sigma \in Gal(\mathbb{Q}(\frac{u}{\bar{u}})/\mathbb{Q}) = Gal(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ (因为 $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ 为 Abel 扩张)

$\because$ $Gal(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ 可交换. $\therefore \forall \sigma, \left|\sigma(\frac{u}{\bar{u}})\right| = \left|\frac{\sigma(u)}{\overline{\sigma(u)}}\right| = 1.$

"共轭" $\in$ $\cong (\mathbb{Z}/p\mathbb{Z})^*$.

(σ 与"共轭"交换
且 σ 保除法).

$\Rightarrow$ 对 $\forall (\frac{u}{\bar{u}})^n$, 其定义多项式 g_n 有 $\begin{cases} \deg(g_n) \leq \deg(f). \\ g_n\text{'s 根模长为1}. \end{cases}$ ← Galios

由 $\exists$ finite $g \in \mathbb{Z}[X]$ s.t. $\begin{cases} \deg(g) \leq \deg(f) \Leftarrow \deg(g) \text{ 有一致上界} \\ \forall \text{ root of } g \text{ 模为1}. \Leftarrow g\text{'s 系数有一致上界}. \end{cases}$

$\Rightarrow \#\{(\frac{u}{\bar{u}})^n, n \in \mathbb{N}\} < +\infty$.

$\Rightarrow \exists t, (\frac{u}{\bar{u}})^t = 1$, 即 $\frac{u}{\bar{u}}$ = a root of unity.

$\Rightarrow \frac{u}{\bar{u}} = \pm \zeta^k$. #.

Def: (regular prime)

A prime number $p > 3$ is regular prime if:

$\forall I \subseteq \mathbb{Z}[\zeta_p]$ ideal. I^p is principal $\Rightarrow I$ is principal.

Thm: $x^p+y^p=z^p$, $(p\nmid xyz)$ has no solutions in $\mathbb{Z}$. for regular prime p.

Pf: Step1: $(x+y)(x+\zeta y)\cdots(x+\zeta^{p-1}y)=(z)^p$ (x,y,z 互素).

理想观点

Step2: $(x+\zeta^i y)$ 与 $(x+\zeta^j y)$ 互素.(即不$\exists \beta\in Spec(\mathbb{Z}[\zeta_p])$ s.t. $\begin{cases}(x+\zeta^i y)\subseteq\beta\\(x+\zeta^j y)\subseteq\beta\end{cases}$)

($\Leftrightarrow$ $(x+\zeta^i y,\ x+\zeta^j y)=(1)$).

If not, $\exists\beta\in Spec(\mathbb{Z}[\zeta_p])$. s.t $x+\zeta^i y,\ x+\zeta^j y\in\beta$

$\Rightarrow$ $(\zeta^i-\zeta^j)y\in\beta$

ζ^i可逆

$\Leftrightarrow$ $(1-\zeta^{j-i})y\in\beta$.

$(p)=(1-\zeta)^{p-1}$

$\Rightarrow$ $py\in\beta$

又 $z^p=(x+y)\cdots(x+\zeta^{p-1}y)\in\beta$. $\overset{\beta素}{\Rightarrow}$ $z\in\beta$.

这与 $(py,z)=1$ 矛盾.

Step3: By UFD of kummer $\Rightarrow$ $(x+\zeta^i y)=I^p$ for some ideal $\subseteq\mathbb{Z}[\zeta_p]$.

分解

$\overset{\text{regular prime}}{\Longrightarrow}$ $I=(\alpha)$ for some $\alpha\in\mathbb{Z}[\zeta_p]$.

回到元素

$\Longrightarrow$ $x+\zeta y=u\alpha^p$, $u,\alpha\in\mathbb{Z}[\zeta_p]$. (下面考虑 $i=1$).

Step4: Note that $\alpha=\sum_{i=0}^{p-1}a_i\zeta_p^i\in\mathbb{Z}[\zeta_p]$.

$\Rightarrow x\equiv y \pmod p$.

由 $\alpha^p\equiv(\sum_{i=0}^{p-1}a_i\zeta_p^i)^p\equiv\sum_{i=0}^{p-1}a_i^p \pmod p$.

$\Rightarrow$ $\alpha^p\equiv\bar{\alpha}^p \pmod p$.

$\Rightarrow$ $x+\bar{\zeta}y\equiv\bar{u}\alpha^p \pmod p$.

日期: /

$$\Rightarrow (x+\zeta y) \equiv \frac{u}{\bar{u}} \cdot (x+\zeta^{-1}y)$$

$$\equiv \zeta^k (x+\zeta^{-1}y) \equiv \zeta^k x + \zeta^{k-1} y \pmod p$$

$\mathbb{Z}[\zeta_p]/(p) \simeq \mathbb{Z}[\zeta_p]/(1-\zeta_p)^{p-1}$ is freely generated by $\zeta_p, \cdots, \zeta_p^{p-2}$ over $\mathbb{Z}/p\mathbb{Z}$. ($\in \mathbb{F}_p^{\mathrm{Vect}}$)

$$\xRightarrow[\text{系数相等}]{p \nmid xyz} k=1 \ \& \ x \equiv y \pmod p$$

Step 5: $\Rightarrow x^p + (-z)^p = (-y)^p$

$$\xRightarrow{\text{同上}} x \equiv -z \pmod p.$$

$$\Rightarrow 2x^p \equiv x^p + y^p \equiv z^p \equiv -x^p \pmod p.$$

$$\Rightarrow 3x^p \equiv 0 \pmod p. \xRightarrow{p>3} p \mid x. \text{ 矛盾. } \#.$$

Preview & Extension

the problem remained: decomposition, regular prime.

the object studied: $\mathbb{Z}[\zeta_p]$.

Thm: (Kummer's criterion) TFAE:

① p is a regular prime.

② $\forall m<0, 2 \nmid m, \ p \nmid \zeta(m) = -\frac{B_{1-m}}{1-m}$ $\left[\frac{t}{e^t-1} = \sum_{n \geq 0} B_n \frac{t^n}{n!}\right]$.

③ $p \nmid B_2, B_4, B_6, \cdots, B_{p-3}$.

日期:　　/

Rmk: * $2<p<100$, p is regular prime iff $p\neq 37,59,67$.

* 猜想: 1) $\#\{\text{regular prime}\}=+\infty$

2) $\lim\limits_{n\to+\infty}\frac{\#\{\text{regular prime}\leq n\}}{\#\{\text{prime}\leq n\}}\approx 0.6$.

Leading Problem2:

Pell Equation:

给定$N(\neq a^2)$, K, $x^2-Ny^2=K$ 在$\mathbb{Z}(\mathbb{Q})$上要么无解,要么有无穷组解.

Analysis: 考虑分解 $(x-\sqrt{N}y)(x+\sqrt{N}y)=K$., $x,y\in\mathbb{Z}$.

$x+\sqrt{N}y\in\mathbb{Z}[\sqrt{N}]$.

def norm N: $N(x+\sqrt{N}y)=(x+\sqrt{N}y)(x-\sqrt{N}y)=x^2-Ny^2\in\mathbb{Z}$.

↳ def为共轭.

Fact: $\alpha,\beta\in\mathbb{Z}[\sqrt{N}]$, $N(\alpha)N(\beta)=N(\alpha\beta)$.

Cor: $\alpha\in\mathbb{Z}[\sqrt{N}]^*\iff N(\alpha)=1$.

Pf: $N(\alpha)=1\Rightarrow\bar{\alpha}=\alpha^{-1}\Rightarrow\alpha\in\mathbb{Z}[\sqrt{N}]^*$

$\alpha\in\mathbb{Z}[\sqrt{N}]^*\Rightarrow\exists\beta$, $\alpha\beta=1\Rightarrow N(\alpha)N(\beta)=1\Rightarrow N(\alpha)=\pm1$.

? how to proof $N(\alpha)\neq-1$?

$\Rightarrow$ Pell equation $\iff N(\alpha)=K$. $\alpha=x+\sqrt{N}y\in\mathbb{Z}[\sqrt{N}]$.

let $N(\alpha_0)=K$, $\beta\in\mathbb{Z}[\sqrt{N}]^*\Rightarrow N(\alpha_0\beta)=1$.

$\Rightarrow$ Pell Thm $\iff\#\mathbb{Z}[\sqrt{N}]^*>+\infty$.

日期: /

the problem remained: $\#\mathbb{Z}[\sqrt{N}]^*$.

the object studied: $\mathbb{Z}[\sqrt{N}]$.

Def: (ring of algebraic numbers)

(rmk: $K\subseteq\mathbb{C}$, 因为 $\mathbb{C}=\overline{\mathbb{R}}$).

① a finite field extension $K/\mathbb{Q}$. (即 $[K:\mathbb{Q}]<+\infty$) is called a 代数域.

& An element $\xi\in K$ is called an algebraic number, if $\exists f(x)\in\mathbb{Q}[x]$ s.t. $f(\xi)=0$.

② $\xi\in\mathbb{C}$ is an algebraic integer if $\exists$ 首一 $f(x)\in\mathbb{Z}[x]$ s.t. $f(\xi)=0$.

③ $[K:\mathbb{Q}]<+\infty$, define $O_K=\{\xi\in K \mid \xi \text{ is an algebraic integer}\}$

eg1. $O_{\mathbb{Q}}=\mathbb{Z}$.

Pf: $\mathbb{Z}\subseteq\mathbb{Q}$ 且 $\forall n\in\mathbb{Z}$, 零化 $f(x)=x-n$. $\Rightarrow \mathbb{Z}\subseteq O_{\mathbb{Q}}$.

取 $\frac{r}{s}\in O_{\mathbb{Q}}\subseteq\mathbb{Q}$, 不妨 $(r,s)=1$. 则 $\exists a_i\in\mathbb{Z}$ s.t.

$$(\tfrac{r}{s})^n+a_1(\tfrac{r}{s})^{n-1}+\cdots+a_{n-1}=0.$$

$$\Leftrightarrow\quad r^n+a_1sr^{n-1}+\cdots+a_{n-1}s^n=0.$$

$$\Rightarrow s\mid r \overset{(s,r)=1}{\Longrightarrow} s=\pm1. \Rightarrow \mathbb{Z}\supseteq O_{\mathbb{Q}} \quad \#.$$

eg.2. $\begin{cases} K: & \mathbb{Q} \quad \mathbb{Q}(\sqrt{2}) \quad \mathbb{Q}(\sqrt{3}) \quad \mathbb{Q}(\sqrt{5}) \quad \cdots \\ O_K: & \mathbb{Z} \quad \mathbb{Z}[\sqrt{2}] \quad \mathbb{Z}[\sqrt{3}] \quad \mathbb{Z}[\frac{1+\sqrt{5}}{2}] \quad \cdots \end{cases}$

(Rmk: $\mathbb{Z}[\sqrt{N}]$ 不全是 $\mathbb{Q}(\sqrt{N})$ 的 O_K.)

日期: /

Main Problems: $\begin{cases} \text{UFD / unique finite decomposition.} \\ O_K^*. \end{cases}$

Main Result:

Thm1: $\forall$ ideal $I \subseteq O_K$ has a unique decomposition:

$$I = \mathfrak{p}_1^{r_1} \mathfrak{p}_2^{r_2} \cdots \mathfrak{p}_s^{r_s}. \quad \mathfrak{p}_1, \cdots, \mathfrak{p}_s \in \mathrm{Spec}(O_K).$$

Thm2: (Dirichlet's unit thm) $[K:\mathbb{Q}] < +\infty$.

$$O_K^* \simeq \mathbb{Z}^{\oplus r} \oplus \{\text{roots of unity}\}. \quad r = r_1 + r_2.$$

where $r_1 = \#\mathrm{Hom}(K, \mathbb{R})$, $r_2 = \#\mathrm{Hom}(K, \mathbb{C})/\mathrm{conj}$.

↳ "共轭", 即共轭只算一次.

Cor1: $r = 0 \Leftrightarrow r_1 = 0, r_2 = 1$

$\Leftrightarrow K = \mathbb{Q}[\sqrt{m}]$. $m \in \mathbb{Z}_{<0}$.

Cor2: $\mathbb{Z}[\sqrt{N}]^* > +\infty \Rightarrow x^2 - Ny^2 = K$ has either infinite solution in $\mathbb{Z}$.

or none solution in $\mathbb{Z}$.

Goal 3: Class Group.

Def: $[K:\mathbb{Q}] < +\infty$, we can associate a finite abelian group,

as $Cl(K)$ or $Cl(O_K)$ (class group of K). $h_K = \# Cl(O_K)$.

FACT: ① O_K is UFD $\Leftrightarrow Cl(K) = \{e\} \Leftrightarrow O_K$ is a PID. $\Leftrightarrow h_K = 1$.

② p is a regular prime $\Leftrightarrow p \nmid \# Cl(\mathbb{Q}(\zeta_p))$.

日期:　　/

Thm: let $k=\mathbb{Q}[\sqrt{m}]$ $m\in\mathbb{Z}_{<0}$. then,

O_k is UFD iff

$$k=\mathbb{Q}(\sqrt{-1}),\mathbb{Q}(\sqrt{-2}),\mathbb{Q}(\sqrt{-3}),\mathbb{Q}(\sqrt{-7}),\mathbb{Q}(\sqrt{-11}),$$

$$\mathbb{Q}(\sqrt{-19}),\mathbb{Q}(\sqrt{-43}),\mathbb{Q}(\sqrt{-67}),\mathbb{Q}(\sqrt{-163}).$$

Rmk: $\exists$ infinite $n\in\mathbb{Z}_{>0}$ s.t. $O_{\mathbb{Q}[\sqrt{n}]}$ is UFD.

Q: How to compute $Cl(k)$.?

• Dirichlet Zeta Fuction:

$\chi:(\mathbb{Z}/N\mathbb{Z})^*\to\mathbb{C}^*$. homomorphism of group.

$$L(s,\chi)=\sum_{n=0}^{+\infty}\frac{\chi(n)}{n^s}\quad,\quad \chi(n)=\begin{cases}\chi(n \bmod N) & \text{if } (n,N)=1.\\ 0 & \text{, otherwise.}\end{cases}$$

Thm:

① $L(s,\chi)$ have analytic continuation to $\mathbb{C}$. as meromorphism function.

② $L(s,\chi)$ is holomorphic in $\{s\neq1\}$. (即只可能有s=1这一个极点)

If $Im(\chi)\neq\{1\}$, then $L(s,\chi)$ is holomorphic on $\mathbb{C}$.

Thm: $k=\mathbb{Q}(\sqrt{m})$ $m\in\mathbb{Z}_{<0}$. $N=\begin{cases}|m| & , m\equiv1 \pmod 4.\\ |4m| & , m\equiv2,3 \pmod 4.\end{cases}$

$\exists!\ \chi:(\mathbb{Z}/N\mathbb{Z})^*\to\{\pm1\}\subseteq\mathbb{C}^*$. s.t. $(\frac{m}{p})=\chi(p \bmod N)$. $\forall$ prime $p\nmid N$.

then. $h_{O_k}=\#Cl(O_k)=\frac{\#O_k^*}{2}\cdot L(0,\chi)=\frac{\#O_k^*\sqrt{N}}{2\pi}L(1,\chi)$.

日期: /

Mindmap:

Primary decomposition of Notherian ring.

$\Downarrow$ $\Downarrow$

Simple dimension Theory $\Rightarrow$ Dedekind domain (Decomposition) Artin Ring.

$\Downarrow$ $\swarrow$

Decomposition in O_K $\Leftarrow$ discrete valuation ring (DVR).

---

§1: Integral.

Def: B ring, $A \subseteq B$ subring, $x \in B$ is integral over A,

iff $x^n + a_1 x^{n-1} + \cdots + a_n = 0$ for some $a_1, \cdots, a_n \in A$.

Rmk: A, B field, $A \subseteq B$. $x \in B$ is algebraic over A,

iff $a_0 x^n + a_1 x^{n-1} + \cdots + a_n = 0$ for some $a_0, \cdots, a_n \in A$.

(即 integral is algebraic's 推广. 重点是要求首一)

e.g. $A = \mathbb{Z}$, $B = K$, $[K:\mathbb{Q}] < +\infty$, $x \in K$ is integral over $\mathbb{Z}$

iff x is an algebraic integer.

e.g.: $\mathbb{Z} \subseteq \mathbb{Q}$. $r \in \mathbb{Q}$ is integral over $\mathbb{Z}$ iff $x \in \mathbb{Z}$.

即 $O_{\mathbb{Q}} = \mathbb{Z}$.

Prop: TFAE ($A \subseteq B$ subring).

① $x \in B$ is integral over A.

② $A[x]$ is f.g. as an A-module.

日期: /

③ $A[x] \subseteq C \subseteq B$ for a subring C which is f.g. as A-module.

④ $\exists$ faithful $A[x]$-module M which is f.g. as A-module.

Pf: ①⇒②: $x \in B$ integral $/A$.

$\Rightarrow x^{n+r} = -(a_1 x^{n+r-1} + \cdots + a_n x^r)$. $\forall r \geq 0$.

$\Rightarrow A[x]$ is f.g. as A-module by $1, x, \cdots, x^{n-1}$.

②⇒③: let $C = A[x]$.

③⇒④: let $M = C$.

④⇒①: Consider $\phi_x : M \to M$. s.t. $\phi_x(m) \triangleq xm$.

易验证 ϕ_x is A-linear. 由 Cayley-Hamilton

$\Rightarrow \exists\ \Phi \triangleq \phi_x^n + a_1 \phi_x^{n-1} + \cdots + a_n = 0$. $a_i \in A$

由 $\Phi(m) = (x^n + a_1 x^{n-1} + \cdots + a_n) \cdot m = 0$ $\forall m \in M$.

$\xRightarrow{\text{faithful}} x^n + \cdots + a_n = 0$. $\Rightarrow x$ is integral over A.

Cor 1: let $x_1, \cdots, x_n \in B$. integral$/A$. then.

$A[x_1, \cdots, x_n]$ is f.g. as A-module

Pf: $A \underset{f.g.}{\subseteq} A[x_1] \underset{f.g.}{\subseteq} A[x_1, x_2] \underset{f.g.}{\subseteq} \cdots \underset{f.g.}{\subseteq} A[x_1, \cdots, x_n]$.

Cor 2: let $C = \{b \in B \mid b$ integral$/A\}. \subseteq B$ is a subring.

Pf: $x, y \in C \Rightarrow A[x, y]$ is f.g. as A-module.

$\Rightarrow x\pm y,\ xy \in A[x,y] \subseteq B.$

$\Rightarrow x\pm y,\ xy \in C.$ □.

eg. $[k:\mathbb{Q}]<+\infty$. O_k is a subring.

(Rmk: $O_k \subseteq K$. $\Rightarrow$ K is a domain).

Def : $A\subseteq B$ subring. $C \triangleq \{b\in B \mid b \text{ is integral over } A\}$ is called integral closure (整闭包) of A in B.

def B is integral over A iff $B=C$.

def A is integrally closed iff $A=C$.

Prop :(传递性)

$A\subseteq B\subseteq C$. rings. B integral $/A$, C integral $/B$, then. C integral $/A$.

Pf: $\forall x\in C$. 由 C integral $/B$.

$\exists\ x^n+b_1x^{n-1}+\cdots+b_n=0.\ \ b_1,\cdots,b_n\in B.$

记 $B'=A[b_1,\cdots,b_n]\subseteq B$. $\Rightarrow$ B' is f.g. as A-module.

$\Rightarrow x$ integral $/B'$. $\Rightarrow$ $B'[x]$ is f.g. as B'-module.

$\Rightarrow B'[x]$ is f.g. as A-module. $\Rightarrow A[x]$ is f.g. as A-module.

$\Rightarrow x$ integral $/A$.

日期:　　/

Cor: $A\subseteq B$ rings. C is integral closure of A in B.

then C is integrally closed in B.

Pf: $x\in B$ integral$/C \xRightarrow{C \text{ integral}/A} x$ integral$/A \Rightarrow x\in C$.

eg. ($A=\mathbb{Z}$, $B=K$, $C=O_K$). O_K is integrally closed in K.

即 $\forall\ \xi\in K$. if $\xi^n+a_1\xi^{n-1}+\cdots+a_n=0$. $a_1,\cdots,a_n\in O_K$. $\Rightarrow \xi\in O_K$.

Def : domain A is integrally closed if A is integrally closed in $\mathrm{Frac}(A)$.

eg. $\mathbb{Z}$ is integrally closed.

Prop : $\mathrm{Frac}(O_K)=K$.

Pf: $\subseteq$: 显然.

$\supseteq$: 由 $[K:\mathbb{Q}]<+\infty$. $\therefore K$ is algebraic$/\mathbb{Z}$.

$\Rightarrow \forall x\in K$, $\exists\ a_0x^n+\cdots+a_n=0$. for some $a_1,\cdots,a_n\in\mathbb{Z}$.

$\Rightarrow (a_0x)^n+\cdots+a_na_0^{n-1}=0. \Rightarrow a_0x\in O_K$.

$\Rightarrow x\in\mathrm{Frac}(O_K)$.

Cor: O_K is integrally closed.

日期: /

Prop: (商,分式化保 integral). $A\subseteq B$ subring, B integral/A.

(i) $I\subseteq B$ ideal. then $A/A\cap I \hookrightarrow B/I$ is integral.

(ii) $S\subseteq A$ ($1\in S$, $SS\subseteq S$), $S^{-1}B$ is integral/$S^{-1}A$.

Pf: (i) $x\in B \Rightarrow x^n+a_1x^{n-1}+\cdots+a_n=0$ $(*)$, $a_i\in A$.

$* \bmod I \Rightarrow [x]^n+[a_1][x]^{n-1}+\cdots+[a_n]=0$. $[a_i]\in A/A\cap I$.

$\Rightarrow [x]\in B/I$ integral/$A/A\cap I$.

(ii) let $\frac{x}{s}\in S^{-1}B$ ($x\in B$, $s\in S$). then.

$\frac{(*)}{s^n} \Rightarrow (\frac{x}{s})^n+\frac{a_1}{s}(\frac{x}{s})^{n-1}+\cdots+\frac{a_n}{s}=0$. $\frac{a_i}{s}\in S^{-1}A$.

$\Rightarrow \frac{x}{s}$ integral/$S^{-1}A$.

(iii) (分式化保整闭包).

$A\subseteq C\subseteq B$, C is integral closure of A in B.

then, $S^{-1}C$ is integral closure of $S^{-1}A$ in $S^{-1}B$.

Pf: by (ii), $\Rightarrow S^{-1}C$ is integral/$S^{-1}A$.

Consider $\frac{b}{s}\in S^{-1}B$ is integral/$S^{-1}A$

有 $(\frac{b}{s})^n+\frac{a_1}{s_1}\cdot(\frac{b}{s})^{n-1}+\cdots+\frac{a_n}{s_n}=0$. $(*)$. $\frac{a_i}{s_i}\in S^{-1}A$.

let $t=s_1\cdots s_n$. then, $(*)\cdot(ts)^n \Rightarrow$

$$(tb)^n+\underbrace{a_1\cdot\frac{s}{s_1}\cdot t}_{\in A}\cdot(tb)^{n-1}+\cdots+\underbrace{a_n\cdot\frac{s}{s_n}\cdot s^{n-1}t^n}_{\in A}=0.$$

$\Rightarrow tb$ integral $/A \Rightarrow tb \in C$.

而 $t \in S$. $\Rightarrow b \in S^{-1}C$.

Thm: A. integrally closed. domain. $K = \mathrm{Frac}(A)$.

$K \leq L$ finite separable field extension.

B is the integral closure of A in L.

then $\exists$ basis $v_1, \cdots, v_n$ of $L \in {}_K\mathrm{Vect}$. s.t. $B \subseteq \sum_{i=1}^{n} A v_i$

(Cor: B is noetherian if A is noetherian).

Pf: Step 1: Consider $v \in L$. a is algebraic $/K$.

$\Rightarrow \exists\ a_0 v^r + \cdots + a_n = 0$. $a_i \in A$.

$\Rightarrow \exists\ (a_0 v)^r + \cdots + a_n a_0^{r-1} = 0$.

$\Rightarrow a_0 v \in B$.

$\Rightarrow$ let $v_1, \cdots, v_n \in L$ is a basis of $L \in {}_K\mathrm{Vect}$.

by above, we can have $a_i \in A$ s.t. $a_i v_i \in B$.

$\Rightarrow$ 不妨 assume $v_1, \cdots, v_n \in B$.

Step 2: Aim: $\forall\, b \in B$. $b = \sum_{i=1}^{n} a_i v_i$, $a_i \in A$.

Idea: 记 $v = \sum \lambda_i v_i \in V \in {}_K\mathrm{Vect}$.

(对偶空间).

考虑内积 $\langle \cdot, \cdot \rangle$. 及 dual basis $v_1', \cdots, v_n'$.

日期: /

即 $\langle v_i, v_j' \rangle = \begin{cases} 1, & i=j. \\ 0, & \text{otherwise}. \end{cases}$

$\Rightarrow \langle v, v_j' \rangle = \lambda_j.$

let $T: L \to K$ be the trace map:

$$\alpha \mapsto \sum_{\sigma \in Gal(L/K)} \sigma(\alpha) \quad \Leftarrow \text{seperable}.$$

① $T(B) \subseteq A$:

$\forall \alpha \in B$. 有首一poly. $f \in A[x] \subseteq K[x]$. s.t $f(\alpha)=0$.

$\because$ α与$\sigma(\alpha)$在K上有同一零化多项式. $\forall \sigma \in Gal(L/K)$.

又 $\sigma(\alpha) \in K$ 且 A integrally closed in K.

$\Rightarrow \sigma(\alpha) \in A$. $\Rightarrow \sum_{\sigma \in Gal(L/K)} \sigma(\alpha) \in A$.

$\downarrow$?

② $T(k\alpha) = kT(\alpha)$

$\forall k \in K$, $\forall \alpha \in B$. 有首一poly. $f \in A[x] \subseteq K[x]$. s.t $f(\alpha)=0$.

$\because$ α与$\sigma(\alpha)$在K上有同一零化多项式. $\forall \sigma \in Gal(L/K)$.

$\therefore$ $k\alpha$与$k\sigma(\alpha)$在K上有同一零化多项式. $\forall \sigma \in Gal(L/K)$.

$\Rightarrow T(k\alpha) = kT(\alpha)$.

$\forall b \in B$, assume $b = \sum_{i=1}^{n} \lambda_i v_i'$ $\quad \lambda_i \in K$, $v_i' \in L$.

$T(b) \in A$. $\quad T(\underline{\langle b, v_i \rangle}) = \lambda_i$ $\quad \langle \cdot,\cdot \rangle$: 保A. 与T交换.

$\langle A, A \rangle \subseteq A$.

$= \langle T(b), T(v_i) \rangle$

日期: /

An idea: 考虑 L 的对偶空间: L^*

其基为 $v_1^*, v_2^*, \cdots, v_n^*$

s.t. $v_i^*(v_i)=1$, $v_i^*(v_j)=0$. $j\neq i$

记 $f(\alpha,\beta)=\beta\alpha$, $\alpha\in L$, $\beta\in L^*$

↑? 则 $f(v, v_i^*)=\lambda_i$.

Cor: O_K is noetherian.

§2: Dimension.

Def: (Dedekind domain).

domain A is Dedekind if:

① A is noetherian.

② A is integrally closed.

③ $\dim A=1$.

Goal: 1) A Dedekind, $I\subseteq A$ ideal $\exists!$

$I=\mathfrak{p}_1^{r_1}\cdots\mathfrak{p}_s^{r_s}$, $\mathfrak{p}_1,\cdots\mathfrak{p}_s\in \mathrm{Spec}(A)$.

2) O_K is Dedekind.

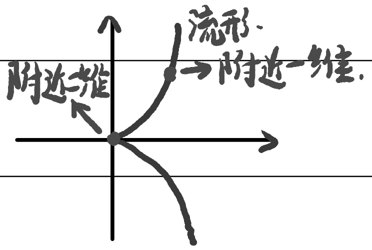
Q: How to define dim?

Geometric: Q1: let $S\subseteq k^n$ algebraic subset. What is $\dim S$?

eg. * $\{0\} \subseteq k$. $\dim\{0\} = 0$.

* $k^n = Z(0)$. $\dim k^n = n$.

* $X = \{x^2 - y^3 = 0\} \subseteq k^2$. $\dim X = 1$.



Fact: Let $S \subseteq \mathbb{C}^n$ be an algebraic subset, then

$$S_{reg} = \{x \in S \mid S \text{ is a mfd. near } x\} \subseteq S. \text{ is dense.}$$

is a mfd.

$\Rightarrow$ define $\dim S \triangleq \dim S_{reg}$ as mfd.

Geometric - Algebraic:

Q_2: How to define $\dim S$ algebraically? ($S \in k^n$ algebraic subset)

eg. k^2. Consider sequence: $\{0\} \subseteq \{x_1 = 0\} \subseteq k^2$. $(*)$.

$$\dim k^2 = \operatorname{len}(*) - 1.$$

k^n. 类似地有 $\dim k^n = \operatorname{len}(*) - 1$.

Problem: * length of sequence is not unique.

eg $\{0\} \subseteq k^2$. $\operatorname{len} = 2 \neq 3$.

* sequence may not be regular.

eg. $\{0\} \subseteq \{0,1\} \subseteq \{0,1,2\} \subseteq \cdots \subseteq \{0,1,2,\cdots,n\} \subseteq \cdots \subseteq \mathbb{R}$.

$\operatorname{len} = \infty \neq 2$.

日期: /

Def: * A sequence $S_0 \subseteq S_1 \subseteq \cdots \subseteq S_d = S$ is maximal if

不∃ algebraic subset Y s.t. $S_i \subsetneq Y \subsetneq S_{i+1}$ for some $i=0,1,\cdots,d-1$.

* An algebraic subset $S \subseteq k^n$ is irreducible if

$S = S_1 \cup S_2$ 且 S_1, S_2 are algebraic subsets $\Rightarrow S = S_1$ 或 $S = S_2$.

eg. Assume $\mathbb{C} = S_1 \cup S_2$. $S_1 \subsetneq \mathbb{C}, S_2 \subsetneq \mathbb{C} \Rightarrow \# S_1 < +\infty, \# S_2 < +\infty$.

$\Rightarrow \# \mathbb{C} < +\infty$. 矛盾

Def: (Krull Define)

$S \subseteq k^n$ algebraic subset, $(*)$ $S_0 \subsetneq S_1 \subsetneq \cdots \subsetneq S_d = S$ is a maximal sequence of irreducible algebraic subsets of S.

Denote $\dim_{Krull}(*) = d$.

Denote $\dim_{Krull} S = \max\limits_{(*)} \operatorname{len}(*)$.

Thm: ① $\dim_{Krull} S = \dim S_{reg}$.

② for ∀ maximal sequence of irr. alg. subsets $(*)$ of S.

Then, $\dim_{Krull}(*) = \dim_{Krull} S$.

Algebraic: Q3: R ring. How to define $\dim R$?

Lem: A ring. $I_1, \cdots, I_n \subseteq A$ ideals. $\mathfrak{p} \in \operatorname{Spec}(A)$. s.t. $\bigcap\limits_{i=1}^{n} I_i \subseteq \mathfrak{p}$.

then ∃ i, s.t. $I_i \subseteq \mathfrak{p}$.

Pf: suppose $I_1,\cdots,I_n \nsubseteq \mathfrak{p}$. $\Rightarrow \exists\, x_i \in I_i,\ x_i \notin \mathfrak{p}$.

$\Rightarrow x_1\cdots x_n \in \bigcap_{i=1}^n I_i \setminus \mathfrak{p} \Rightarrow \bigcap_{i=1}^n I_i \nsubseteq \mathfrak{p}$. 矛盾.

Cor: A ring. $I_1,\cdots,I_n \subseteq A$ ideals. $\mathfrak{p} \in \mathrm{Spec}(A)$. s.t. $\bigcap_{i=1}^n I_i = \mathfrak{p}$.

then $\exists\, i$, s.t. $I_i = \mathfrak{p}$.

Prop: $I \subseteq k[x_1,\cdots,x_n]$. $(k=\bar{k})$ then $Z(I)$ is irreducible $\Leftrightarrow$ I is prime.

Pf: $(\Leftarrow)$: I is prime. 若 $Z(I) = Z_1 \cup Z_2$. $\Rightarrow$ $I = I(Z_1) \cap I(Z_2)$. $\xRightarrow{\text{lem}}$ $I = I(Z_1)$ or $I = I(Z_2)$. $\Rightarrow$ $Z(I) = Z_1$ or Z_2.

$(\Rightarrow)$: 若 I 不为 prime. 则 $\exists\, I_1, I_2$, s.t. $I_1 \cap I_2 = I$ 且 $I_1 \nsubseteq I, I_2 \nsubseteq I$.

$\Rightarrow \exists\, Z_1, Z_2$ s.t. $Z_1 \cup Z_2 = Z(I)$ 且 $Z(I_1) \nsubseteq Z(I), Z(I_2) \nsubseteq Z(I)$.

Inspiration.

$S \subseteq k^n$ algebraic subset, $(*)$ $S_0 \subsetneq S_1 \subsetneq \cdots \subsetneq S_d = S$ maximal irr. alg. sets sequence

$\Downarrow I$ $\qquad\qquad \Downarrow I$

$I(S) \subsetneq I(S_{d-1}) \subsetneq \cdots \subsetneq I(S_0) \subseteq k[x_1,\cdots,x_n]$. maximal prime sequence.

Def: A ring. define the Krull dimension of A as:
(dim).

$\dim_{\text{Krull}} A = \max\{\text{length}(*)-1 \mid (*)\text{: a sequence of prime ideals of } A\}$.

Rmk: ① $S \subseteq k^n$ alg. set. $\dim S = \dim k[x_1,\cdots,x_n]/I(S)$.

② If A is local Noetherian, the $\dim A < +\infty$.

③ $A = k[x_1,\cdots,x_n,\cdots]$, $(x_1) \subsetneq (x_1,x_2) \subsetneq \cdots \subsetneq (x_1,\cdots,x_n) \subsetneq \cdots$

日期: /

$\dim A = +\infty$. (即 $\exists A$ s.t. $\dim A = +\infty$).

④ $\dim A[x] = \dim A + 1$.

Prop: ① * k field. $\dim k = 0$.

* $\dim A = 0 \overset{?}{\Rightarrow} A$ field.

No! eg. $\mathrm{Spec}\, k[t]/t^2 = \{(t)\}$. $\Rightarrow \dim k[t]/t^2 = 0$.

(可理解为,存在幂零元的).

Def: a noetherian ring A is Artin iff $\dim A = 0$.

② A domain. then A field $\Leftrightarrow \dim A = 0$.

Pf: $\Leftarrow$: $(0) \in \mathrm{Spec}(A)$.

$\overset{\dim A = 0}{\Rightarrow} (0)$ maximal

$\Rightarrow A$ field.

Cor: $\dim A = 1 \Leftrightarrow \forall\, 0 \neq I \subseteq A$ ideal is maximal.

Goal: Thm: $A \subseteq B$ domain. B integral$/A$.

$\dim A = 1 \Rightarrow \dim B = 1$.

Cor1: $A = \mathbb{Z}$, $B = O_K$. $\Rightarrow \dim O_K = 1$.

Cor2: O_K is Dedekind.

Lem1: $A \subseteq B$. domains. B integral/A. Then

B is a field $\Leftrightarrow$ A is a field.

Pf: ($\Leftarrow$): let $y \in B, y \neq 0$. $\exists\ y^n + a_1 y^{n-1} + \cdots + a_n = 0$. ($a_i \in A$, $\underset{\text{domain.}}{a_n \neq 0}$)

$\Rightarrow$. $y^{-1} = -\underbrace{a_n^{-1}}_{\in A}(\underbrace{y^{n-1} + a_1 y^{n-2} + \cdots + a_{n-1}}_{\in B}) \in B$. $\Rightarrow$ B field.

$\Rightarrow$): let $x \in A$, $x \neq 0$. $\xRightarrow[B\text{ field}]{}$ $x^{-1} \in B$.

$\Rightarrow \exists\ x^{-m} + a_1 x^{-m+1} + \cdots + a_m' = 0$. ($a_i' \in A$).

$\Rightarrow$ $x^{-1} = -(a_1' + a_2' x + \cdots + a_m' x^{m-1}) \in A$

$\Rightarrow$ A field.

Lem2: let $A \subseteq B$ rings. B integral/A. $q \in \mathrm{Spec}(B)$. $\mathfrak{p} = q \cap A \in \mathrm{Spec}(A)$.

Then, q is maximal $\Leftrightarrow$ $\mathfrak{p}$ is maximal.

(Rmk: 即 maximal 在 integral 条件下可拉回).

Pf: B/q. is integral $/A/q$. $\xRightarrow{\text{lem1}}$ q max. $\Leftrightarrow$ p max.

Lem3: let $A \subseteq B$ rings. B integral/A. $q_1, q_2 \in \mathrm{Spec}(B)$.

s.t. $q_1 \subseteq q_2$. 且 $q_1 \cap A = q_2 \cap A = \mathfrak{p} \in \mathrm{Spec}(A)$.

then $q_1 = q_2$.

Pf: Consider $A_\mathfrak{p} \subseteq B_\mathfrak{p}$ ($:= (A \setminus \mathfrak{p})^{-1} B$.)

从而 $q_1 B_\mathfrak{p} \subseteq q_2 B_\mathfrak{p}$.

日期: /

$$q_1 B_\beta \cap A_\beta = q_2 B_\beta \cap A_\beta = \beta A_\beta. \text{ maximal in } A_\beta.$$

$\xRightarrow[B_\beta \text{ integral}/A_\beta]{\text{lem2}} q_1 B_\beta, q_2 B_\beta$ maximal in B_β.

$\Rightarrow q_1 B_\beta = q_2 B_\beta$. $\qquad B \xrightarrow{\sigma} B_\beta$.

$\xRightarrow[\sigma^{-1}(q_1 B_\beta) = q_1]{\text{拉回}} q_1 = q_2$

Thm-Pf: Step 1: lem1 $\Rightarrow \dim B \geq 1$.

Step 2: Assume $\dim B \geq 2$.

$\exists\ (0) \subsetneq q_1 \subsetneq q_2 \in \mathrm{Spec}(B)$.

$\Downarrow \cap A$

$(0) \subsetneq q_1 \cap A \subsetneq q_2 \cap A \in \mathrm{Spec}(A)$.

$\xRightarrow{\dim A = 1} q_1 \cap A = q_2 \cap A \xRightarrow{\text{lem3}} q_1 = q_2. \Rightarrow$ 矛盾!

或 $(0) = q_1 \cap A \xRightarrow{\text{lem3}} q_1 = 0. \Rightarrow$

$\Rightarrow \dim B = 1$. $\square$

Now we will go into the decomposition theorem.

Consider $\mathbb{Z}$: $(n) = (p_1^{r_1}) \cdots (p_s^{r_s}) = (p_1)^{r_1} \cap \cdots \cap (p_s^{r_s})$.

$r(p_i^{r_i}) = (p_i) \in \mathrm{Spec}(\mathbb{Z})$.

Def (primary ideal) $I \subseteq A$. is a primary ideal iff:

$ab \in I,\ a \notin I \Rightarrow b^v \in I$ for some $v \geq 1$. (即 $b \in r(I)$).

Tools first.

§3. Associated Prime.

Def: A noetherian. $M \in {}_A\mathrm{Mod}$. f.g. $\mathfrak{p} \in \mathrm{Spec}(A)$.

$\mathfrak{p}$ is an associated prime of M iff: $\mathfrak{p} = \mathrm{ann}(x)$ for some $x \in M$.

记 $\mathrm{Ass}(M) = \{\text{associated prime of } M\}$.

(Rmk: $\mathrm{ann}(x) = \{a \in A \mid ax = 0\}$. $\mathrm{ann}(M) = \{a \in A \mid aM = 0\}$.)

Prop1: ① $\mathfrak{p} \in \mathrm{Ass}(M) \Longleftrightarrow \exists$ injective morphism $A/\mathfrak{p} \hookrightarrow M$.

② $\forall\, x \neq 0 \in A/\mathfrak{p}$. $\mathrm{ann}_A(x) = \mathfrak{p}$.

i.e. $\mathrm{Ass}_A(A/\mathfrak{p}) = \{\mathfrak{p}\}$.

Pf: ① $\Rightarrow$): $\mathfrak{p} \in \mathrm{Ass}(M) \Rightarrow \mathfrak{p} = \mathrm{ann}(x)$.

$$\Rightarrow \Phi: \ A/\mathrm{ann}(x) \xrightarrow{\times x} M. \qquad a \longmapsto ax.$$

易验证, Φ is injective.

$\Leftarrow$): 由 $\iota: A/\mathfrak{p} \hookrightarrow M$. 记 $x = \iota(1)$.

$\Rightarrow \mathfrak{p} = \mathrm{ann}(x)$.

② 由①显然.

Prop2: A Noetherian. $0 \neq M \in {}_A\mathrm{Mod}$. f.g.

① Every maximal element of $\{\mathrm{ann}(x) \mid x \neq 0 \in M\}$.

is an associated prime of M.

In particular, $\mathrm{Ass}_A(M)=\phi \Leftrightarrow M=0$.

② Define $\overset{\text{zero-divisor}}{ZD_A(M)}=\{a\in A \mid \exists x\neq 0\in M \text{ s.t. } ax=0\}$.

then $ZD_A(M)=\bigcup\limits_{\mathfrak{p}\in \mathrm{Ass}_A(M)}\mathfrak{p}$.

Pf: ① Aim: $\mathrm{ann}(x)$ is maximal (in $\mathrm{Ass}(M)$) $\Rightarrow$ $\mathrm{ann}(x)$ is prime.

$\underset{\hookrightarrow abx=0}{ab\in \mathrm{ann}(x)}$. $\underset{\hookrightarrow bx\neq 0}{b\notin \mathrm{ann}(x)}$ $\Rightarrow$ $\mathrm{ann}(x)\subseteq \mathrm{ann}(bx)$.

又 $\mathrm{ann}(x)$ maximal $\Rightarrow$ $\mathrm{ann}(x)=\mathrm{ann}(bx)$

又 $a\in \mathrm{ann}(bx)$. $\Rightarrow$ $a\in \mathrm{ann}(x)$.

$\Rightarrow$ $\mathrm{ann}(x)$ is prime.

② By definition: $\bigcup\limits_{\mathfrak{p}\in \mathrm{Ass}_A(M)}\mathfrak{p}\subseteq ZD_A(M)$.

$\supseteq$): $\forall a\in ZD_A(M)$, 有 $ax=0$, $x\neq 0$. ($a\in ZD_A(M)$).

$\overset{①}{\Rightarrow}$ $a\in \mathrm{ann}(x)\subseteq \mathfrak{p}$ for some $\mathfrak{p}\in \mathrm{Ass}_A(M)$.

Review: A ring. $S\subseteq A$. ($1\in S$, $S\cdot S\in S$) $\exists$ 1:1 correspondence:

$$\mathrm{Spec}(S^{-1}A)\rightleftarrows\{\mathfrak{p}\in \mathrm{Spec}(A)\mid \mathfrak{p}\cap S=\phi\}.$$

$$q\longmapsto \sigma^{-1}(q).$$

$$S^{-1}\mathfrak{p}\longleftarrow\!\shortmid\ \mathfrak{p}.$$

$\sigma: A\hookrightarrow S^{-1}A$.
$a\mapsto \frac{a}{1}$.

from this point: We always regard $\mathrm{Spec}(S^{-1}A)\hookrightarrow \mathrm{Spec}(A)$

as a subset of $\mathrm{Spec}(A)$.

日期: /

Thm: A Noetherian. $S\subseteq A$ ($1\in S$, $SS\subseteq S$). (分式化下的对应关系)

① $N\in {}_{S^{-1}A}\mathrm{Mod}$. Then $\mathrm{Ass}_{S^{-1}A}(N)=\sigma(\mathrm{Ass}_A(N))\cap \mathrm{Spec}(S^{-1}A)$

② $M\in {}_A\mathrm{Mod}$. Then $\mathrm{Ass}_{S^{-1}A}(S^{-1}M)=\sigma(\mathrm{Ass}_A(M))\cap \mathrm{Spec}(S^{-1}A)$.

Pf: ① $\subseteq$): let $P\in \mathrm{Ass}_{S^{-1}A}(N)$ s.t. $P=\mathrm{ann}_{S^{-1}A}(x)$, $x\in N$.

$\Rightarrow \sigma^{-1}(P)=\sigma^{-1}(\mathrm{ann}_{S^{-1}A}(x))=\mathrm{ann}_A(x)\in \mathrm{Ass}_A(N)$.

$\supseteq$): let $\mathfrak{p}\in \mathrm{Ass}_A(N)$ s.t. $\mathfrak{p}=\mathrm{ann}_A(x)$, $x\in N$.

若 $\mathfrak{p}\cap S\neq\phi$, 则 $S^{-1}\mathfrak{p}=S^{-1}A\notin \mathrm{Spec}(S^{-1}A)$.

$\Rightarrow \mathfrak{p}\cap S=\phi \Rightarrow S^{-1}\mathfrak{p}\in \mathrm{Spec}(S^{-1}A)$.

又 $S^{-1}\mathfrak{p}=S^{-1}\mathrm{ann}_A(x)=\mathrm{ann}_{S^{-1}A}(x)$.

↳易用元素验证.

② $\supseteq$): let $\mathfrak{p}\in \mathrm{Ass}_A(M)$ s.t. $\mathfrak{p}\cap M=\phi$. (否则类似上面)

$\Rightarrow \exists\ A/\mathfrak{p}\hookrightarrow M$.

$\overset{S^{-1}}{\Rightarrow}\ S^{-1}(A/\mathfrak{p})\cong S^{-1}A/S^{-1}\mathfrak{p}\hookrightarrow S^{-1}M$.

$\Rightarrow S^{-1}\mathfrak{p}\in \mathrm{Ass}_{S^{-1}A}(S^{-1}M)$.

$\subseteq$): let $P=\mathrm{ann}_{S^{-1}A}(x)\in \mathrm{Ass}_{S^{-1}A}(S^{-1}M)$ for some $x\in M$.

let $\mathfrak{p}=\sigma^{-1}(P)$.

Claim: $\mathfrak{p}=\mathrm{ann}_A(tx)$ for some $t\in S$.

$\Rightarrow \mathfrak{p}\in \mathrm{Ass}_A(M)$.

日期: /

Proof of Claim: Assume $\mathrm{ann}_A(x) \subsetneq \mathfrak{p}$. (否则取 $t=1$)

$\Rightarrow \exists\, b \in \mathfrak{p} \setminus \mathrm{ann}_A(x)$ s.t. $bx \neq 0 \in A$, $bx = 0 \in S^{-1}A$

$\Rightarrow bx \neq 0 \in A$, $bxs = 0 \in A$ for some $s \in S$.

$\Rightarrow \mathrm{ann}_A(x) \subsetneq \mathrm{ann}_A(sx) \subseteq \mathfrak{p}$.

$\xRightarrow[\text{Notherian}]{\text{induction}}$ Claim 得证 $\square$

Cor: A Noetherian. $M \in {}_A\mathrm{Mod}$ f.g. $\mathfrak{p} \in \mathrm{Spec}(A)$. Then,

$\mathfrak{p} \in \mathrm{Ass}_A(M) \Leftrightarrow \mathfrak{p}_\mathfrak{p} \in \mathrm{Ass}_{A_\mathfrak{p}}(M_\mathfrak{p})$.

Thm: (与 exact sequence 的关系)

A ring. $0 \to M' \to M \to M'' \to 0$. exact sequence of A-modules.

Then, $\mathrm{Ass}_A(M') \subseteq \mathrm{Ass}_A(M) \subseteq \mathrm{Ass}_A(M') \cup \mathrm{Ass}_A(M'')$.

Pf: let $\mathfrak{p} = \mathrm{ann}_A(x) \in \mathrm{Ass}_A(M')$. $x \in M' < M$. $\Rightarrow \mathfrak{p} \in \mathrm{Ass}_A(M)$.

let $\mathfrak{p} \in \mathrm{Ass}_A(M)$. $\Rightarrow A/\mathfrak{p} \hookrightarrow M$. 记 $A/\mathfrak{p} \simeq N \subseteq M$.

$$\begin{cases} N \cap M' \neq 0. \Rightarrow \exists x \in M' \text{ s.t. } 0 \neq x \in N \simeq A/\mathfrak{p}. \Rightarrow \mathrm{ann}_A(x) = \mathfrak{p}. \Rightarrow \mathfrak{p} \in \mathrm{Ass}_A(M'). \\ N \cap M' = 0 \Rightarrow A/\mathfrak{p} \hookrightarrow M \to M'' \simeq M/M'. \Rightarrow A/\mathfrak{p} \hookrightarrow M'' \Rightarrow \mathfrak{p} \in \mathrm{Ass}_A(M''). \end{cases}$$ $\square$

Thm: A Noetherian. $M \in {}_A\mathrm{Mod}$ f.g. (Noeth 环的链式分解)

① Then $\exists$ chain of submodules: $0 = M_0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_n = M$.

s.t. $M_i / M_{i-1} \simeq A/\mathfrak{p}_i$ for some $\mathfrak{p}_i \in \mathrm{Spec}(A)$.

② $Ass_A(M_i) \subseteq \{\mathfrak{p}_1, \cdots, \mathfrak{p}_i\}$.

Pf: ① · Aim: Find $M_1 \subseteq M$. s.t. $M_1 \simeq A/\mathfrak{p}_1$. for some $\mathfrak{p}_1 \in Spec(A)$.

$M \neq 0 \Rightarrow Ass_A(M) \neq \emptyset$.

let $\mathfrak{p}_1 \in Ass_A(M)$. $\Rightarrow A/\mathfrak{p}_1 \overset{\varphi_1}{\hookrightarrow} M$. let $M_1 = Im(\varphi_1) \simeq A/\mathfrak{p}_1$.

· Aim: Find $M_2 \subseteq M$. s.t. $M_2/M_1 \simeq A/\mathfrak{p}_2$. for some $\mathfrak{p}_2 \in Spec(A)$.

$M/M_1 \neq 0 \Rightarrow Ass_A(M/M_1) \neq \emptyset$. ($M/M_1 = 0$ 则分解结束).

Let $\mathfrak{p}_2 \in Ass_A(M/M_1) \Rightarrow A/\mathfrak{p}_2 \overset{\varphi_2}{\hookrightarrow} M/M_1$ let $M_2/M_1 = Im(\varphi_2) \simeq A/\mathfrak{p}_2$.

By Induction & Noetherian, □.

② Consider $0 \to M_{i-1} \to M_i \to M_i/M_{i-1} \to 0$.

$$\Rightarrow Ass_A(M_{i-1}) \subseteq Ass_A(M_i) \subseteq \underbrace{Ass_A(M_{i-1})}_{\overset{\text{induction}}{\cap\!|}\ \{\mathfrak{p}_1, \cdots, \mathfrak{p}_{i-1}\}} \cup \underbrace{Ass_A(M_i/M_{i-1})}_{= Ass_A(A/\mathfrak{p}_i) = \{\mathfrak{p}_i\}}$$

$$\subseteq \{\mathfrak{p}_1, \cdots, \mathfrak{p}_i\}.$$ □.

Cor: A Noetherian $M \in {}_A\mathrm{Mod}$ f.g. $\Rightarrow Ass_A(M)$ is a finite set.

§4: Supported Prime.

Def: A ring. $M \in {}_A\mathrm{Mod}$. let.

$$Supp_A(M) = \{\mathfrak{p} \in Spec(A) \mid M_\mathfrak{p} \neq 0\}.$$

日期: /

Lem: M f.g. Then $\mathrm{supp}_A(M)=\{\mathfrak{p}\in \mathrm{Spec}(A) \mid \mathrm{ann}_A(M)\subseteq \mathfrak{p}\}$

(计算手段) $\simeq \mathrm{Spec}(A/\mathrm{ann}_A(M))$.

Pf: M f.g. $\Rightarrow$ Assume $M=(x_1,\cdots,x_n)$.

then $M_{\mathfrak{p}}=0 \Leftrightarrow \frac{x_i}{1}=0\in M_{\mathfrak{p}}$.

$\Leftrightarrow \exists\, s_i\notin \mathfrak{p}$ st. $s_ix_i=0\in M$.

$\Leftrightarrow \exists\, s\notin \mathfrak{p}$ st. $sx_1=0,\cdots,sx_n=0$.

$\Leftrightarrow \exists\, s\notin \mathfrak{p}$ st. $s\in \mathrm{ann}_A(M)$.

$\Leftrightarrow \mathrm{ann}_A(M)\nsubseteq \mathfrak{p}$. $\square$.

Thm: A Noetherian. $M\in {}_A\mathrm{Mod}$ f.g. Then, (Ass & supp)

① $\mathrm{Ass}_A(M)\subset \mathrm{supp}_A(M)$.

② the minimal elements in $\mathrm{Ass}_A(M)$ and $\mathrm{supp}_A(M)$ is the same.

Pf: ① $\mathfrak{p}\in \mathrm{Ass}_A(M)\Rightarrow \exists\, A/\mathfrak{p}\hookrightarrow M$.

$\Rightarrow 0\neq (A/\mathfrak{p})_{\mathfrak{p}}\hookrightarrow M_{\mathfrak{p}}$.

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

$\Rightarrow \mathfrak{p}\in \mathrm{supp}_A(M)$.

② 若 $\mathfrak{p}$ is minimal in $\mathrm{supp}_A(M)$.

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

日期:　　/

$$\overset{\subseteq \sigma(\mathrm{Supp}_A(M))}{} \qquad \overset{\subseteq \sigma(\{q \mid q\in \mathrm{Spec}(A) \text{且} q\subset p\})}{}$$

$$\Leftrightarrow \phi \neq \mathrm{Ass}_{A_p}(M_p) = \sigma(\mathrm{Ass}_A(M)) \cap \mathrm{Spec}(A_p) \underset{\substack{\uparrow \\ \text{minimal}}}{\subseteq} \{p_p\}$$

$$\Rightarrow \mathrm{Ass}_{A_p}(M_p) = \{p_p\} \Rightarrow p \in \mathrm{Ass}_A(M).$$

又由 $\mathrm{Ass}_A(M) \subseteq \mathrm{supp}_A(M)$.

$\Rightarrow$ the minimal elements in $\mathrm{Ass}_A(M)$ and $\mathrm{supp}_A(M)$ is the same.

§5: Primary Submodule

Def: A ring. $N, M \in {}_A\mathrm{Mod}$ $N \subset M$.

N is primary iff $\forall a \in A, x \in M$.

$x \notin N$ & $ax \in N \Rightarrow a^v M \subseteq N$. for some $v>0$.

Rmk: ① 等价于: i) $[x] \neq 0 \in M/N$. $a[x] = 0 \in M/N \Rightarrow a^v \in \mathrm{ann}_A(M/N)$. for some $v>0$.

ii) $ZD_A(M/N) \subseteq r(\mathrm{ann}_A(M/N))$.

② 易验证, 该定义与 primary ideal 的定义相容.

Thm: A Noetherian $M \in {}_A\mathrm{Mod}$ f.g. Then
(刻画).

a submodule $N \subseteq M$ is primary iff $\# \mathrm{Ass}_A(M/N) = 1$

In this case, if $\mathrm{Ass}_A(M/N) = \{P\}$ then $r(\mathrm{ann}(M/N)) = P$. $\leftarrow$ 计算方法.

$= ZD_A(M/N)$.

lem: $r(I) = \bigcap\limits_{\substack{r(I)\subseteq p \\ p \in \mathrm{Spec}(A)}} p$. ($r(I)$ 的素理想分解 Thm)

日期: /

Pf: Assume N primary

$\Rightarrow \bigcup \mathrm{Ass}_A(M/N) = ZD_A(M/N) \subseteq r(\mathrm{ann}_A(M/N)) \overset{\text{lem}}{=} \bigcap \mathrm{supp}_A(M/N) \overset{\text{minimal}}{=} \bigcap \mathrm{Ass}_A(M/N)$

$\Rightarrow \mathrm{Ass}_A(M/N) = \{P\}$ & $ZD_A(M/N) = P$ & $r(\mathrm{ann}_A(M/N)) = P$.

Conversely 同理.

Def: N is P-primary if $\mathrm{Ass}_A(M/N) = \{P\}$.

Lem: N_1, N_2 are P-primary $\Rightarrow N_1 \cap N_2$ is P-primary.

Pf: Consider $M/N_1 \cap N_2 \hookrightarrow M/N_1 \oplus M/N_2$. (CRT).

$\phi \neq \mathrm{Ass}_A(\underset{}{M/N_1 \cap N_2}) \subseteq \mathrm{Ass}_A(M/N_1 \oplus M/N_2) = \{P\}$. ($M/N_1\cap N_2 \neq 0$)

$\Rightarrow \mathrm{Ass}_A(M/N_1 \cap N_2) = \{P\}$. $\Rightarrow N_1 \cap N_2$ is P-primary.

§6: Decomposition

Thm: M Noetherian. $\forall$ submodule $N \subseteq M$.

$\exists$ an irreducible decomp.

i.e. $N = N_1 \cap \cdots \cap N_n$. s.t. $\forall N_i$ satisfy: $N_i = N_{i1} \cap N_{i2} \Rightarrow N_i = N_{i1}$ or $N_i = N_{i2}$.

Pf: Let $\mathcal{S} = \{N \subseteq M$ submodule which does NOT admit irr. decomp.$\}$.

If $\mathcal{S} \neq \phi \underset{M \text{ Noeth}}{\Longrightarrow} \exists$ maximal $N \in \mathcal{S}$.

N is not irr. (否则 $N = N$ 即为 irr. decomp.)

$\Rightarrow N = N_1 \cap N_2$. $N_1, N_2 \supsetneq N \Rightarrow N_1, N_2 \notin \mathcal{S} \Rightarrow N \notin \mathcal{S}$. 矛盾.

日期: /

e.g. $A=k$, $M=k^n$. $V\subseteq k^n$ irreducible iff $\dim V=n-1$.

且 $\mathrm{Ass}_k(k^n/V)=\{0\}$. ← k 只有一个 prime ideal.

Def: (*) $N=N_1\cap\cdots\cap N_r$ is irredundant if.

$$N\neq\bigcap_{\substack{1\le i\le r,\\ i\neq j}} N_i \quad \text{for } \forall j.$$

(Noeth)

Thm: A Noetherian $M\in{}_A\mathrm{Mod}$. f.g.

① Any irreducible submodule is primary. (反过来不对).

② if $N=N_1\cap\cdots\cap N_r$. with $\mathrm{Ass}_A(M/N_i)=\{P_i\}$.

is irredundant primary decomp. Then, $\mathrm{Ass}_A(M/N)=\{P_1,\cdots,P_r\}$.

③ A Noetherian $M\in{}_A\mathrm{Mod}$. f.g.

$\forall$ submodule $N\subseteq M$ has a primary decomp.

④ $N=N_1\cap\cdots\cap N_r$ is an irredudant, primary decomp. which is minimal.

(i.e. $P_i\neq P_j$ $\forall i,j$. $\mathrm{Ass}(M/N_i)=\{P_i\}$. i.e. 不可再合并同类项.).

if P_i is minimal in $\mathrm{Ass}(M/N)$., then:

$$N_i=\varphi_{P_i}^{-1}(N_{P_i}) \quad \text{where } \varphi_{P_i}: M\hookrightarrow M_{P_i}.$$

In particular, N_i is uniquely determined by M, N.

日期:　　/

Pf: ① 不妨 Assume $N=0$. (by replace M by M/N).

Assume $N=0$ is not primary.

$\Rightarrow Ass_A(M) \ni P_1, P_2$.

$$\begin{tikzcd} A/p_1 \arrow[r, hook, "\varphi_1"] & M \\ A/p_2 \arrow[ur, hook, "\varphi_2"'] & \end{tikzcd}$$

Let $\underset{\neq 0}{N_1 = Im(\varphi_1)}$. $\underset{\neq 0}{N_2 = Im(\varphi_2)}$.

若 $N_1 \cap N_2 \neq 0$. then $\exists x \neq 0$, $x \in N_1 \Rightarrow ann(x) = P_1$.

$x \in N_2 \Rightarrow ann(x) = P_2$ 矛盾.

$\therefore N_1 \cap N_2 = 0 \Rightarrow 0$ is not irr.

② Assume $N=0$. 由 $0 = N_1 \cap \cdots \cap N_r$.

Then $M \hookrightarrow M/N_1 \oplus \cdots \oplus M/N_r$. (CRT).

$\Rightarrow Ass_A(M) \subseteq Ass_A(M/N_1 \oplus \cdots \oplus M/N_r) = \{P_1, \cdots, P_r\}$.

Conversely,

irredundant $\Rightarrow 0 \neq \bigcap_{i \neq 1} N_i \simeq \bigcap_{i\neq 1} N_i / N_1 \cap (\bigcap_{i \neq 1} N_i)$

$\simeq N_1 + \bigcap_{i \neq 1} N_i / N_1$

$\subseteq M/N_1$.

$\Rightarrow \phi \neq Ass(\bigcap_{i \neq 1} N_i) \subseteq Ass(M/N_1) = \{P_1\}$.

$\Rightarrow \mathrm{Ass}(\bigcap_{i\neq 1} N_i) = \{P_1\}$

$\bigcap_{i\neq 1} N_i \subseteq M$.

$\Rightarrow P_1 \in \mathrm{Ass}(M)$.

类似地

$\Rightarrow \{P_1, \cdots, P_r\} \subseteq \mathrm{Ass}(M)$

③ 由①与 irr. decomp. ,易得.

④ Step1: 不妨设 $P_i \in \mathrm{Ass}(M/N)$ is minimal.

$\forall j \neq i$, 有 $\mathrm{Ass}_A((M/N_j)_{P_i}) = \underbrace{\sigma(\mathrm{Ass}(M/N_j))}_{=\{(P_j)_{P_i}\}} \cap \underbrace{\mathrm{Spec}(A_{P_i})}_{=\{P_{P_i} \mid P \subseteq P_i\}} = \phi$.

P_i minimal. $\Rightarrow P_i \nsubseteq P_j$.

$\Rightarrow (M/N_j)_{P_i} = 0$.

$\Rightarrow M_{P_i} = (N_j)_{P_i}$.

$\Rightarrow N_{P_i} = (\bigcap_{j=1}^{r} N_j)_{P_i} = M_{P_i} \cap \cdots \cap M_{P_i} \cap (N_i)_{P_i} = (N_i)_{P_i}$.

Step2: $\mathrm{Ass}(M/N_i) = \{P_i\} \Rightarrow ZD(M/N_i) = P_i$.

$\Rightarrow \quad M/N_i \to (M/N_i)_{P_i}$ injective

($\because$ 若 $0 \neq x \longmapsto \frac{x}{1} = 0 \Rightarrow \exists s \notin P_i$, st $sx = 0$. 矛盾)

$$\Rightarrow \begin{tikzcd} M \arrow[r, "\varphi_{P_i}"] \arrow[rr, bend right, "\mathrm{Ker} = N_i"'] & M_{P_i} \arrow[r] & (M/N_i)_{P_i} \end{tikzcd}$$

$= \varphi_{P_i}^{-1}((N_i)_{P_i})$.

$\Rightarrow N_i = \varphi_{P_i}^{-1}((N_i)_{P_i}) = \varphi_{P_i}^{-1}(N_{P_i})$. $\square$

日期: /

eg. ① $A=M=\mathbb{Z}$.

$n\in\mathbb{Z}$, $n=p_1^{r_1}\cdots p_s^{r_s}$ $\Rightarrow (n)=(p_1^{r_1})\cdots(p_s^{r_s})$ $\left\{\begin{array}{l}\text{irredundant}\\ \text{minimal}\\ \text{primary}\\ \text{unique} \leftarrow (p_i)\ \text{minimal}.\end{array}\right.$

② A Noetherian. $I=r(I)$.

$I=\bigcap_{\substack{I\subseteq \mathfrak{p}\\ \mathfrak{p}\in\operatorname{Spec}(A)}}\mathfrak{p}=\mathfrak{p}_1\cap\cdots\cap\mathfrak{p}_r$, $\mathfrak{p}_i\in\{\mathfrak{p}\supseteq I,\mathfrak{p}\in\operatorname{Spec}(A)\}$ minimal.

Cor: A Noetherian. $\dim A=1$. then, $\forall\, I\subseteq A$ ideal.

admits a unique irredundant primary decomp. which is minimal:

$I=q_1\cap\cdots\cap q_r \underset{\uparrow}{=} q_1\cdots q_r$.

CRT $\leftarrow$ $q_i+q_j=(1)$ $\longleftarrow$ $r(q_i+q_j)=r(r(q_i)+r(q_j))=r(\mathfrak{p}_i+\mathfrak{p}_j)=r(1)=(1)$.

Lemma1: A Dedekind domain. q is p-primary $\Rightarrow$ $q=p^r$ for some $r>0$.

Lemma2: A Dedekind domain. $p\in\operatorname{Spec}(A)$. (Dedekind在局部化下保持)

$\Rightarrow A_p$ is a local Dedekind domain.

Pf:

$A_p\left\{\begin{array}{l}\text{Noetherian, domain} \Leftarrow A_p\subseteq \operatorname{Frac}(A). \ (\to\text{以上都是扩域.})\\ \dim A_p=1. \Leftarrow \operatorname{Spec}(A_p)=\{q_p \mid q\in\operatorname{Spec}(A)\text{且 } q\subseteq p\}=\{0,P\}\\ \text{integrally closed} \Leftarrow \text{分式化下保持}.\end{array}\right.$

日期: /

Thm: local Dedekind domain $\Leftrightarrow$ local DVR. (不证)

(等价刻画)

Lemma 3: A local DVR, m maximal ideal $\Rightarrow$ every ideal $I = m^r$ for some r (不证).

由 lemma 2,3 及 Thm, lemma 1 易证. $\square$.

(Dedekind decomp.)

Thm: A Dedekind domain. $I \overset{\exists!}{=} p_1^{r_1} \cdots p_s^{r_s}$. $p_i \in \operatorname{Spec}(A)$.

Cor: $[K:\mathbb{Q}] < +\infty$. $\forall I \subseteq \mathcal{O}_K$, $I \overset{\exists!}{=} p_1^{r_1} \cdots p_s^{r_s}$. $p_i \in \operatorname{Spec}(\mathcal{O}_K)$. $\square$

日期:　　　/