交换代数讲义电子版

TaD 整理

2024 年春季学期 (于世卓)

目录

交换代数（“神学”）的优势 **vii**

课程简介 **ix**

1 交换代数简介, 抽象代数复习 **1**

1.1 群作用 1

1.2 环论 5

2 交换代数简介 (UFD, Dedekind 整环及其在数论上应用) **7**

2.1 多项式的不变子环 7

2.2 理想与商环 9

2.2.1 素理想与极大理想 9

2.3 Euclidean, PID, UFD 与 Noether 环 11

2.4 UFD 的推广: Dedekind 整环 13

2.4.1 推广 1: 元素运算 $\underset{\text{推广}}{\rightsquigarrow}$ 理想的运算 13

2.4.2 推广 2: UFD$\rightsquigarrow$Dedekind 整环 13

2.5 代数数论中的应用 15

3 不变理论与 Hilbert 基定理 **17**

3.0.1 理想 vs 代数 18

3.1 多项式环上的群作用 19

3.1.1 方式 1: 由群表示诱导 19

3.1.2 群表示 vs 群作用 19

3.1.3 方式 2: 环自同构子群作用 20

4 Hilbert 基定理证明与 Gröbner 基 25

4.1 Noether 环与 Hilbert 基定理 25

4.1.1 Noether 环的等价定义 25

4.1.2 Hilbert 基定理 26

4.1.3 Hilbert 基定理的推论 28

4.2 Gröbner 基的存在性与域上的 Hilbert 基定理 29

4.2.1 Gröbner 基的优势 30

4.2.2 域上加强版的 Hilbert 基定理 30

5 Buchberger 算法, Noether 模 33

5.1 Hilbert 基定理的组合直观 33

5.1.1 $R[x]$ 情形 33

5.1.2 $R[x, y]$ 的情况 34

5.2 Buchberger 算法: Gröbner 的计算 35

5.3 Noether 环 $\rightsquigarrow$Noether 模 38

5.3.1 模的零化子 40

5.3.2 子模与理想 40

5.3.3 Noether 模等价定义 40

5.3.4 模上的 Hilbert 基定理 41

5.3.5 模同态与 PDE 的解 43

6 正合列, 模上的 Hilbert 基定理, 自由消解与 Syzygy 模 45

6.1 正合列 45

6.2 短正合列的性质 47

6.3 模上 Hilbert 基定理 49

6.4 Hilbert Syzygy 定理 50

7 Hilbert Syzygy 定理, 自由模的 Gröbner 基, Hilbert 多项式定理 53

7.1 Hilbert Syzygy 定理与 Gröbner 基 53

7.2 自由模上的 Gröbner 基 54
7.3 分次自由消解 58
7.4 多项式环的 Hilbert 多项式 59

8 Hilbert 多项式定理, Poincaré 级数 **61**
8.1 Hilbert 多项式定理 61
8.2 Hilbert 多项式性质 62
8.3 不变量理论中的 Poincaré 级数 65
8.4 同调代数简介 66
8.4.1 模张量积 66

9 同调代数简介 (张量积, 平坦模与 Tor) **69**
9.1 张量 69
9.1.1 张量的性质与计算 70
9.1.2 张量积, 正合列与 Hom 函子 72
9.2 平衡函子 Tor 75

10 环的扩张, 不变量理论与 Galois 理论 **79**
10.1 整环和整扩张 79
10.2 不变理论与环, 域扩张理论 (⊃Galois 理论) 82
10.3 Galois 扩张的构造 82

11 整扩张的应用 (Noether 正规化定理, Krull 维数) **85**
11.1 Noether 正规化定理 85
11.2 环的 Krull 维数与整扩张 86
11.3 Hilbert 零点定理 $\underset{\text{zero position theorem}}{\text{Nullstellensatz}}$ 89
11.3.1 弱零点定理 89

12 Hilbert 零点定理 **91**
12.1 强零点定理 93

13 局部化 **97**

13.1 环的局部化 . . . 97

13.2 模的局部化 . . . 100

13.3 局部环 . . . 102

14 Zariski 拓扑, 复方阵的 GIT 分类 **105**

14.1 Noether 环的局部化 . . . 105

14.2 Zariski 拓扑 . . . 106

14.3 课程思政: Zariski 拓扑的拓扑基 . . . 107

14.4 GIT 等价与复方阵的分类 . . . 109

14.5 素谱上的 Zariski 拓扑 . . . 110

14.6 拓扑基与开邻域 . . . 111

15 连续函数环, 素谱上的零点定理 **113**

15.1 Stone-Weierstrass 定理, 弱零点定理与 Zariski 拓扑的关系 . . . 113

15.2 素谱上的零点定理 . . . 115

15.3 环局部化的素谱 . . . 118

16 范畴与函子 **121**

16.1 高阶强零点定理 (Nagata,Zariski) . . . 121

16.2 范畴 . . . 122

16.3 函子 . . . 123

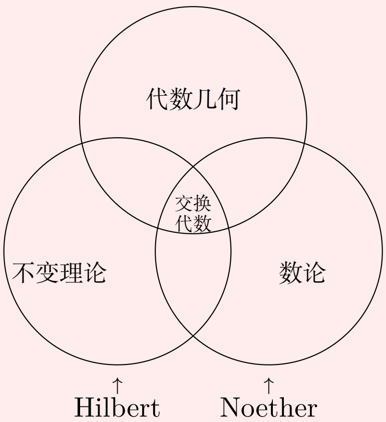
16.4 维数理论与离散赋值环 . . . 125

16.4.1 维数的局部性 . . . 125

16.4.2 离散赋值环 DVR . . . 125

交换代数（“神学”）的优势

注解 0.1



P. Gordon “King of Invariant Theory”
$\updownarrow$ 师生
Noether

P. Gordon:
1. 交换代数 (Hilbert 的方法) 不是数学, 而是 “神学”.
2. 我说服自己 “神学” 也有它的优势.

例 0.0.1: 不变理论: Hilbert 14 问题

群 G 作用在 $k[x_1, \cdots, x_n]$, k 是域, 则 $k[x_1, \cdots, x_n]$ 的不变子环是不是有限生成的 $k-$ 代数 $(k[\xi_1, \cdots, \xi_{\underset{\text{有限个}}{\underset{\downarrow}{m}}}])$?

$$\begin{array}{lcl} G: \text{有限群} & \surd & \text{Hilbert(Hilbert 基定理)\& Chern(陈类)} \\ G: \text{任意群} & \times & \text{有限生成} \iff G\text{是约化群 Nagata 永田雅宜} \end{array}$$

定理 0.0.1: 数论 + 代数几何: Fermat 大定理

$a^n + b^n = c^n, n \geq 3$ 无正整数解.

猜想 0.0.1: Frey 猜想

Fermat 方程有正整数解 $\Longrightarrow$ 椭圆曲线 $y^2 = x(x-a^n)(x+b^n)$(在 $\mathbb{Q}$ 上) 不是模曲线.

解决:

第 1 步: 证明 Frey 猜想 (by Ribet).

第 2 步: 任意椭圆曲线上模曲线 (by Wiles).

核心工具: 交换代数.

课程简介

注解 0.2: 主要内容

Hilbert 四大定理

基定理 $\searrow$ 零点定理 $\swarrow$

Noether 环/有限长度模理论 (PID 升级)

+ 整扩张 (域的代数扩张升级)

局部化 (分式域升级)

$\Downarrow$

“俯视” 抽象代数

Syzygy 定理 $\searrow$ 多项式定理 $\swarrow$

同调代数及其应用

+IT(不变理论)

$\Downarrow$

$\begin{cases} \text{表示论} \\ \text{Galois 理论} \end{cases}$

注解 0.3: 参考书

1. GTM 150 Eisenbud 交换代数 (1-4 章)
2. 丘赛考纲
3. Invariant theory (Neusel)
4. Atiyah.

注解 0.4: 目标

1. 对接 Eisenbud-Borcherds 体系 (UC Berkeley)
2. 丘赛.

注解 0.5: 考核

$$\begin{array}{cc} 50(\text{平时}) & 50(\text{考试}) \\ & 100:60+40 \\ \left\{\begin{array}{l} \text{作业}: 5\times 10 \\ \text{本科生论坛}: 25 \\ \text{丘赛}: 50 \end{array}\right. & \begin{array}{cc} \text{必答} & \underset{\text{(最多两题)}}{\text{选答}} \\ 4\times 15 & 4\times 20 \end{array} \\ & 100/140 \end{array}$$

Chapter 1

交换代数简介，抽象代数复习

1.1 群作用

定义 1.1.1: 群作用

$\sigma : G \times X \to X, (g, x) \mapsto g \cdot x$ 称为**群作用**, 如果满足:

1. $(gh) \cdot x = g \cdot (h \cdot x), \forall g, h \in G, x \in X$(左作用),

2. $e \cdot x = x, \forall x \in X$.

这样的 X 称为 $G-$ 集合.

定义 1.1.2: 群轨道

给定 $x \in X, G \cdot x = \{g \cdot x | g \in G\}$ 称为过 x 的轨道.

定义 1.1.3: 稳定化子

给定 $x \in X, G_x = \{g \in G | g \cdot x = x\}$ 称为 x 处的稳定化子.

性质 1.1.4

$\forall$ 给定 $x, y \in X$, 若 $G \cdot x \cap G \cdot y \neq \varnothing$, 则 $G \cdot x = G \cdot y (\Longleftrightarrow X$ 可以分解为不同轨道的不交并).

性质 1.1.5

$\forall x \in G, G \cdot x \to G/G_x, g \cdot x \mapsto gG_x$ 为双射 (轨道 $\iff$ 齐性空间).

注解 1.1

应用:

1. 解释其它数学概念,

2. 数论, 集合, 组合 $\cdots$

例 1.1.1

仿射空间: A 为点集, $\exists$ 相伴的向量空间 V, 满足: $A \times V \to A, (a, v) \mapsto a + v$,

$$\left.\begin{array}{l}1.a+0=a, \forall a \in A(x \cdot e = x) \\ 2.(a+v)+w=a+(v+w)((xg_1)g_2 = x(g_1g_2))\end{array}\right\} \text{群作用}$$

3.$\forall a \in A, V \to A: v \mapsto a + v$ 是双射 (**自由, 可迁**).

(单射 $\iff$ 自由: $xg = x \implies g = e$)"消去律"

(满射 $\iff$ 可迁: $x, y \in A \implies \exists g \in G$ 使得 $y = xg$)"轨道唯一"

作业 1.1

集合 A 是仿射空间 $\iff \exists$ 向量空间 V, 使得 V 在 A 上的加法群作用是自由且可迁的.

例 1.1.2

1. Lagrangian 定理,

2. Fermat 小定理,

3. Cauchy 定理.

定理 1.1.6: Lagrangian 定理

G 是有限群, H 是 G 的子群, 则 $|H|\,|\,|G|$.

考虑群作用 $H \times G \to G, (h,g) \mapsto hg$. 由性质1.1.4得 $G = \bigcup\limits_{g\in G} Hg, |G| = \sum\limits_{g\in G} |Hg|$, 且 $\forall g, g' \in G, |Hg| = |Hg'| \Longrightarrow |H|\,|\,|G|$.

定理 1.1.7: Fermat 小定理, Cauchy 定理

$p \nmid n, p$ 为素数, $n \in \mathbb{N}^*$, 则 $n^{p-1} \equiv 1 \pmod p$.

G 是 n 阶有限群, $p|n$, 则 G 中包含 (至少 $p-1$) 个 p 阶元素.

设 G 是 n 阶群, p 为素数. 令 $X = \{(x_0, \cdots, x_{p-1}) \in G^p : x_0 x_1 \cdots x_{p-1} = e\}$($X$不是$G^p$的子群). 考虑群作用:$\sigma : \mathbb{Z}/p\mathbb{Z} \times X \to X, ([i], (x_0, \cdots, x_{p-1})) \mapsto (x_i, \cdots, x_{p-1}, x_0, \cdots, x_{i-1})$. 由性质1.1.5得 $\forall x \in X$, 轨道 $\mathcal{O}_x$ 满足 $|\mathcal{O}_x|\,|p \Longrightarrow |\mathcal{O}_x| = 1$或$p$, 由性质 1.1.4 得 $n^{p-1} = |X| = \overset{\text{轨道的计数}}{\overset{\uparrow}{\#}}(|\mathcal{O}_x| = 1) + p \cdot \#(|\mathcal{O}_x| = p)$. 特别地 $|\mathcal{O}_x| = 1 \Longleftrightarrow \mathcal{O}_x\{(g, \cdots, g)|g^p = e\}$.

情况 1: $p \nmid n \Longrightarrow$Fermat 小定理.

只需证: $\#(|\mathcal{O}_x| = 1) = 1$. 由于, $\left|\mathcal{O}_{(e,e,\cdots,e)}\right| = 1$, 故 $\#(|\mathcal{O}_x| = 1) \geq 1$. 假设 $\#(|\mathcal{O}_x| = 1) > 1$, 则 $\exists q \neq e$ 使得 $g^p = e$. 由 Lagrangian 定理, g 生成的循环子群满足 $p = |\langle g \rangle|\,|n$, 矛盾.

情况 2: $p|n \Longrightarrow$Cauchy 定理

假设 G 中不存在 $a \neq e$ 使得 $a^p = e$, 则 $\#(|\mathcal{O}_x|) = 1$(即 $x = (e, \cdots, e)$). 故 $n^{p-1} = 1 + p \cdot (|\mathcal{O}_x| = p)$, 由于 $p|n^{p-1} =$ 左边, 但 $p \nmid$ 右边, 矛盾.

注解 1.2

若要避免此矛盾, 则需 $\#(|\mathcal{O}_x| = 1) = kp, k \in \mathbb{N}^* \Longrightarrow p$ 阶元素个数最少是 $p-1$ 个.

作业 1.2

求证上述证明中的 σ 是群作用, 要验证良定义, 即 $\mathrm{Im}\sigma \subset X$.

1.2 环论

注解 1.3

在本门课中, 如无特殊约定, 环指的是 $\overset{\substack{\text{多项式函数性质}\\ \text{代数}\leftrightarrow\text{几何}\\ \text{多项式函数环}\leftrightarrow\text{概形}\supset\text{簇}\\ \downarrow}}{\text{交换幺}}$ 环.

定义 1.2.1: 交换幺环:$R,+,\cdot$

$\left.\begin{array}{l} 1.(R,+)\text{是交换群} \\ 2.\cdot\text{ 满足结合律} \\ 3.\text{分配律} \end{array}\right\}$

4.交换律$ab = ba$

5.乘法单位元$1\cdot a = a = a\cdot 1$.

注解 1.4: 关于非幺环

没有 1 的环可以 "嵌入"(单同态) 到幺环, 但性质不一定保持不变.

定义 1.2.2: Dorrol 嵌入

设 R 是没有 1 的环, 考虑幺环 $\mathbb{Z}\times R, (n,a)+(m,b) \overset{\text{def}}{=} (m+n, a+b), (n,a)\cdot(m,b) \overset{\text{def}}{=} (mn, nb+ma+ab)$, 乘法单位元是$(1, 0_R)$.

注解 1.5: 关于非交换环 (李代数, 量子群, 非交换几何 $\cdots$)

1. 一些非交换环具有一定 "交换性", 亦可诱导交换环. 微分算子环 $A = \mathbb{R}[x_1,\cdots,x_n,\frac{\partial}{\partial x_1},\cdots,\frac{\partial}{\partial x_n}] \approx$ 交换环. $x_ix_j = x_jx_i, \frac{\partial}{\partial x_i}x_i = x_i\frac{\partial}{\partial x_i} + 1$(Leibniz 法则), $\underset{\substack{\downarrow\\ \text{交换子}}}{[\frac{\partial}{\partial x_i}, x_i]} = 1$.

(例如 $\frac{\partial}{\partial x_i}(x_i, f) = x_i\frac{\partial f}{\partial x_i} + f$.)

2. 非交换环交换化 $\longrightarrow$ 滤子.

$A_0 = \mathbb{R}[x_1,\cdots,x_n] \subset A_1 \subset \cdots \subset A, A_i \overset{\text{def}}{=} \{a\in A : [a,f] \overset{\text{def}}{=} a\cdot f - f\cdot a \in A_{i-1}, \forall f \in$

$A_0\}, A_C = A_0 \oplus A_1/A_0 \oplus A_2/A_1 \oplus \cdots$ 是交换环.

例 1.2.1

$A_1 = A$, 在 A_1/A_0 中 $[1] = [0] \Longrightarrow \dfrac{\partial}{\partial x_i} x_i = x_i \dfrac{\partial}{\partial x_i}, A_C = \mathbb{R}[x_1, \cdots, x_n][y_1, \cdots, y_n] \longrightarrow$ 环扩张.

Chapter 2

交换代数简介 (UFD, Dedekind 整环及其在数论上应用)

定义 2.0.1: 子环

交换幺环的子集且为幺环称为子环.

注解 2.1

理想不被视为子环.

2.1 多项式的不变子环

作业 2.1

设 G 是群, $S = k[x_1, \cdots, x_n], G \times S \to S$ 是群作用, $S^G \overset{\text{def}}{=} f \in S : g \cdot f = f, \forall g \in G$.

问题: S^G 是不是 S 的子环? 什么条件可以使得 S^G 是 S 的子环?

例 2.1.1

$G = S_n, V = k^n = \mathrm{Span}_k\{e_1, \cdots, e_n\}$, 群作用:

$$G \times V \to V \underset{\text{诱导}}{\rightsquigarrow} \qquad G \times V^* \to V^*(\text{对偶表示}) \qquad \underset{\text{诱导}}{\rightsquigarrow} G \times k[x_1, \cdots, x_n] \to k[x_1, \cdots, x_n]$$

$$(\sigma, (e_1, \cdots, e_n) \mapsto (e_{\sigma(1)}, \cdots, e_{\sigma(n)}))$$

$$\sigma(x_i)(e_1, \cdots, e_n) \overset{\text{def}}{=} x_i(\sigma^{-1}(e_1, \cdots, e_n)) = x_i(e_{\sigma^{-1}(1)}, \cdots, e_{\sigma^{-1}(n)}) = x_{\sigma^{-1}(i)}(e_1, \cdots, e_n)$$

$$\sigma\left(\sum_i \alpha_{i_1,\cdots,i_n} x_1^{i_1} \cdots x_n^{i_n}\right) \overset{\text{def}}{=} \sum_i \alpha_{i_1,\cdots,i_n} \sigma(x_1)^{i_1} \cdots \sigma(x_n)^{i_n} = \sum_i \alpha_{i_1,\cdots,i_n} x_{\sigma^{-1}(1)}^{i_1} \cdots x_{\sigma^{-1}(n)}^{i_n}$$

注解 2.2

第一列的式子 $\iff$ 群表示: $G \to GL(V), \sigma \mapsto ((e_1, \cdots, e_n) \mapsto (e_{\sigma(1)}, \cdots, e_{\sigma(n)}))$.

$S^G = k[s_1, \cdots, s_n], s_i$ 是 i 次对称多项式, 是 $k[x_1, \cdots, x_n]$ 的不变子环.

注解 2.3

s_i 代数无关.

定义 2.1.1: 环同态

R, S 是环 (交换幺环). $\varphi : R \to S$ 称为环同态, 若:

1.$\varphi(r + r') = \varphi(r) + \varphi(r')$

2.$\varphi(rr') = \varphi(r)\varphi(r')$

3.$\varphi(1) = 1.\star$

若 φ 为双射, 则称为环同构.

例 2.1.2

$\mathbb{Z} \to \mathbb{Z}, n \mapsto 0$ 不视为环同态.

定理 2.1.2: 环同态定理

$\varphi : R \to S$ 是环同态. $\ker\varphi = \{r \in R | \varphi(r) = 0\}$, 则 $R/\ker\varphi \cong \mathrm{Im}\varphi$.

例 2.1.3

$\mathbb{R}[x] \to \mathbb{C}, f(x) \mapsto f(i) \Longrightarrow \ker\varphi = g(x)(x^2+1) = (x^2+1), \mathbb{R}[x]/(x^2+1) \cong \mathbb{C}.$

2.2 理想与商环

定义 2.2.1: 理想

$I \triangleleft R$:

1.I 是 $(R,+)$ 的子群

2.$IR \subset I$(**乘法 "黑洞"**).

定义 2.2.2: 商环

$R/I \overset{\text{def}}{=} \{a+I : a \in R\} \Longleftrightarrow I$是$R$的理想.

2.2.1 素理想与极大理想

定义 2.2.3: 素元

$a \in$ 整环 $R^* \setminus \underset{\downarrow}{\overset{\text{可逆元}}{U}}$ $, a|xy \Longrightarrow a|x$ 或 $a|y$.

定义 2.2.4: 素理想

I 是环 R 理想 $(I \neq R)$, 若 $ab \in I \Longrightarrow a \in I$ 或 $b \in I$, 则称 I 是素理想.

注解 2.4

引理 1. a 是素元 $\Longrightarrow (a)$ 是素理想.

反之, (0) 是任何整环素理想, 但 0 不是素元.

定理 2.2.5

I 是 R 理想, I 是素理想 $\Longleftrightarrow R/I$ 是整环.

定义 2.2.6: 极大理想

I 是环 R 在真包含关系 (偏序) 下的极大理想.

定理 2.2.7

I 是 R 理想, I 是极大理想 $\Longleftrightarrow R/I$ 是域.

$\Longrightarrow$ 极大理想是素理想.

反之, (0) 是任意整环的素理想, 但不一定为极大理想.

例 2.2.1

环 R 素理想的集合称为素 $\underset{\text{(特征值)}}{\text{谱}}$, 记为 Spec$R$.

$R \rightsquigarrow$(Zariski) 拓扑空间 (几何), $p \in R \rightsquigarrow$ 点;

$R \rightsquigarrow$ 函数空间 (代数), $r \in R \rightsquigarrow$ 函数.

1. $R=\mathbb{Z}, \operatorname{Spec}R=\{(0),\underbrace{(2),(3),(5),\cdots}_{\text{素数}}\}$.

其中 $(0)\subset(p),(0)\longrightarrow$ “泛点”, $(p)\longrightarrow$ “闭点”.

2. $A: n\times n$ 复矩阵, $\lambda_1,\cdots,\lambda_i : A$ 的谱 (所有特征根).

$$\mathbb{C}[A] \overset{\text{def}}{=} \{p(A) : p\in\mathbb{C}[x]\} \cong \mathbb{C}[x]/(A\text{的}\underset{(x-\underset{\text{特征根}}{\lambda_1})^{\overset{\text{重数}}{n_i}}(x-\lambda_2)^{n_2}\cdots(x-\lambda_i)^{n_i}}{\text{极小多项式}})$$

考虑环同态 $\mathbb{C}[x]\xrightarrow{\varphi}\mathbb{C}[A], x\mapsto A,\rightsquigarrow$ 满同态, $\ker\varphi=\{f\in\mathbb{C}[x]:f(A)=0\}=$(极小多项式).

$\operatorname{Spec}\mathbb{C}[A]\cong\{(x-\underset{A\text{的谱}}{\lambda_1}),\cdots,(x-\underset{A\text{的谱}}{\lambda_i})\}$(幂零环,(0)$\notin\operatorname{Spec}\mathbb{C}[A]$).

作业 2.2

$R=\mathbb{C}[x,y]$, 写出 Spec$R$ 以及哪些素理想是极大理想?

2.3 Euclidean, PID, UFD 与 Noether 环

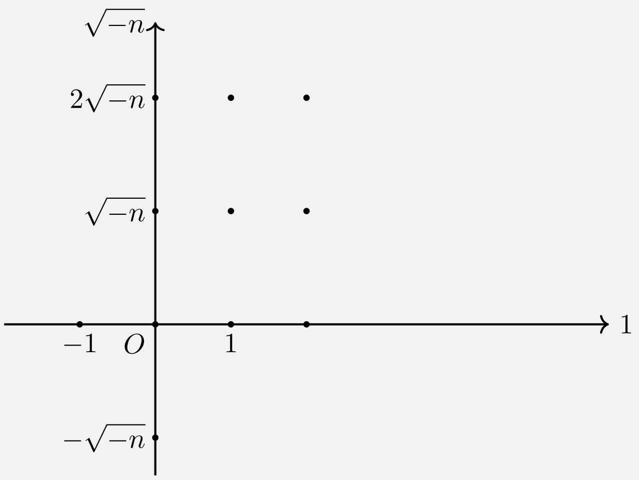
注解 2.5

	循环群 推广↓		Noether 环 ↓	
Euclidean	$\subset$ PID	$\subset$ UFD	$\subset$	整环
可做带余除法	所有理想为主理想	1. 不可约元为素元 $\boxed{\text{2. 主理想升链稳定}}$		
	↓推广	↓推广		
Noether 环:	所有理想有限生成	$\Longleftrightarrow$ 所有理想升链稳定		

例 2.3.1: Euclidean 整环与复平面开覆盖

给定一复平面格点.

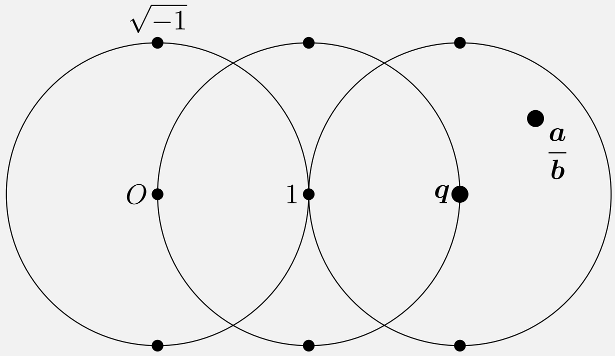
纲领: 复平面是否可以由格点为圆心的单位开圆盘覆盖? $\Longleftrightarrow$ $\mathbb{Z}[\sqrt{-n}]$ **是不是 Euclidean 整环?**



例 2.3.2

$\mathbb{Z}[\sqrt{-1}]$ 是 Euclidean 整环, 对 $\forall a, b \in \mathbb{Z}[\sqrt{-1}] \subset \mathbb{C}$, 令 $g'(a) = |a|^2$. 由于复平面可以被圆心为 $m + n\sqrt{-1}$ 的单位开圆盘覆盖.

$\exists q \in \mathbb{Z}[\sqrt{-1}]$, 使得 $\dfrac{a}{b} = q + \dfrac{r}{b}, \left|\dfrac{r}{b}\right|^2 < 1 \Longrightarrow a = bq + r$ 使得 $r \in \mathbb{Z}[\sqrt{-1}]$且 $|r|^2 < |b^2| \Longrightarrow \mathbb{Z}[\sqrt{-1}]$ 是 Euclidean.



作业 2.3

求证: $\mathbb{Z}[\sqrt{-2}], \mathbb{Z}\left[\dfrac{1+\sqrt{-3}}{2}\right]$ 是欧氏环, $\mathbb{Z}[\sqrt{-3}]$ 不是欧氏环.

例 2.3.3

性质 2.3.1

$\mathbb{Z}[\sqrt{-1}]$ 是 UFD$\Longrightarrow$Fermat 平方和定理 (若 $p=4k+1$ 为素数, 则 $p=m^2+n^2, m,n\in\mathbb{Z}$).

$(\mathbb{Z}/p\mathbb{Z})^* = \{\overline{1}, \overline{2}, \cdots, \overline{p-1}\}$ 关于乘法为循环群 $\langle g\rangle$, 阶数被 4 整除 $\Longrightarrow$ 存在阶数为 4 的元素 $\overline{a}=g^k \Longrightarrow \overline{a^2}$ 阶数为 2.

$$\overline{a^2}=\overline{p-1}\Longrightarrow a^2=-1+np\Longrightarrow a^2+1=np, (a+\sqrt{-1})(a-\sqrt{-1})=np$$

由于 $p|(a+\sqrt{-1})(a-\sqrt{-1})$ 但 $p\nmid a+\sqrt{-1}, a-\sqrt{-1}$, 故 p 不是素元. 由于 $\mathbb{Z}[\sqrt{-1}]$ 是 UFD, p 可约, 故存在不可约分解.

$$p=(x+y\sqrt{-1})(x-y\sqrt{-1})\underset{\text{单位}:\pm1,\pm\sqrt{-1}}{\underset{\downarrow}{u}}\Longrightarrow p=|p|=\left|x+y\sqrt{-1}\right|\left|x-y\sqrt{-1}\right|=x^2+y^2$$

2.4 UFD 的推广: Dedekind 整环

2.4.1 推广 1: 元素运算 $\underset{\text{推广}}{\rightsquigarrow}$ 理想的运算

注解 2.6

理想运算	直观	例:$\mathbb{Z}$
$I \cap J$	最小公倍	$4\mathbb{Z} \cap 6\mathbb{Z} = 12\mathbb{Z}$
$I + J \overset{\text{def}}{=} \{i + j : i \in I, j \in J\} = (I, J)$	最大公约	$4\mathbb{Z} + 6\mathbb{Z} = 2\mathbb{Z}$
$I \cdot J \overset{\text{def}}{=} (\{ij : i \in I, j \in J\}) \longrightarrow$ **生成**	乘法	$4\mathbb{Z} \cdot 6\mathbb{Z} = 24\mathbb{Z}$

定理 2.4.1: 中国剩余定理

若 $I + \underset{\text{满同态}}{\underset{\downarrow}{J}} = R$, 则 $R/I \cap J \cong R/I \times R/J$.

注解 2.7

若 $R = \mathbb{Z}$, 即为数论上的中国剩余定理.

$R \to R/I \times R/J, r \mapsto (r + I, r + J)$ 是满同态, $\ker = I \cap J \Longrightarrow R/I \cap J \cong R/I \times R$.

理想类固定整环 R, 理想 $I \sim J \overset{\text{def}}{\Longleftrightarrow} \exists \alpha, \rho \in R^*$, 使得 $\alpha I = \rho J$, R 中理想关于 $\sim$ 的等价类.

注解 2.8

若 R 是 PID, 则 R 的理想类唯一. $(2\mathbb{Z} \sim 3\mathbb{Z} \subset \mathbb{Z}.)$

2.4.2 推广 2: UFD$\rightsquigarrow$Dedekind 整环

定义 2.4.2: Dedekind 整环

整环 R 的任意非零理想都可以唯一分解为素理想的乘积.

例 2.4.1

$\mathbb{Z}[\sqrt{-5}]$ 不是 UFD: $6 = 2\times 3 = (1+\sqrt{-5})(1-\sqrt{-5})$, 但 $\forall I = \overset{p_1}{\overset{\parallel}{(2, 1+\sqrt{-5})}}{}^{m_1} = \overset{p_2}{\overset{\parallel}{(2, 1-\sqrt{-5})}}{}^{m_2}\, \overset{p_3}{\overset{\parallel}{(3, 1+\sqrt{-5})}}{}^{m_3}\, \overset{p_4}{\overset{\parallel}{(3, 1-\sqrt{-5})}}{}^{m_4}$.

特别地, $(2) = p_1p_2, (3) = p_3p_4, (1+\sqrt{-5}) = p_1p_3, (1-\sqrt{-5}) = p_2p_4$.

注解 2.9

UFD$\not\subset$Dedekind 整环, 例:$k[x,y]$.

$(x) \in \mathrm{Spec}R \subset (x,y)$.

UFD$\cap$Dedekind=PID.

结论 2.4.3: Dedekind 整环的重要性

1. 理想类关于乘法构成群.

例 2.4.2

$\mathbb{Z}[\sqrt{-5}]$ 只有 2 个理想类: $\underset{\uparrow}{\overset{\text{主理想}}{C_1}}$, $\underset{\downarrow}{\overset{\text{非主理想}}{C_2}}$. 乘法满足

$$\begin{array}{c|cc} \cdot & C_1 & C_2 \\ \hline C_1 & C_1 & C_2 \\ C_2 & C_2 & C_1 \end{array} \cong \mathbb{Z}/2\mathbb{Z}$$

注解 2.10

R 的理想类群平凡 $\Longleftrightarrow$ R 是 PID.

2. 对应光滑曲线.

代数等价定义: R 整环满足:

$$\begin{cases} 1.R: \text{Noether 环} \\ 2.\mathrm{Spec}R\text{中除}(0)\text{外都是极大理想} \quad \leftrightarrow \dim 1 \\ 3.R \leftrightarrow \underset{\text{分式域}}{\underset{\downarrow}{\mathrm{Frac}R}}\text{是整扩张} \quad \leftrightarrow \text{不光滑集:codim2} \end{cases}$$

$\updownarrow$

光滑曲线

2.5 代数数论中的应用

定理 2.5.1

$m^3 = n^2 + 5$ 不存在整数解.

基于 UFD 的错误证明:

在 $\mathbb{Z}[\sqrt{-5}]$ 中进行因式分解 $m^3 = (n-\sqrt{-5})(n+\sqrt{-5})$, 由于 $n-\sqrt{-5}$ 与 $n+\sqrt{-5}$ 互素, 若 $\mathbb{Z}[\sqrt{-5}]$ 是 UFD$\searrow$

$$\boxed{n-\sqrt{-5} = (d+e\sqrt{-5})^3 \Longrightarrow e^2 = \frac{4}{3}\text{或}2 \Longrightarrow \text{不存在整数解}}$$

用 Dedekind 整环的更正:

$(m)^3 = (n-\sqrt{-5})(n+\sqrt{-5}) \Longrightarrow (n-\sqrt{-5}) = I^3 \subset \mathbb{Z}[\sqrt{-5}]$, 考虑 $\mathbb{Z}[\sqrt{-5}]$ 理想类群乘法表

$$\begin{array}{r|cc} \cdot & C_1 & C_2 \\ \hline \text{主理想类} \longleftarrow C_1 & C_1 & C_2 \\ \text{非主理想类} \longleftarrow C_2 & C_2 & C_1 \end{array} \cong \mathbb{Z}/2\mathbb{Z}$$

1. I 是主理想 $\in C_1$, 则 $I = (d+e\sqrt{-5})$, 由同方法可得, 不存在整数解.
2. I 不是主理想 $\in C_2$, 则 $I^3 = I^2 \cdot I \in C_2$, 不是主理想, 而 $(n-\sqrt{-5}) \in C_1$, 矛盾.

Chapter 3

不变理论与 Hilbert 基定理

定义 3.0.1: 代数

$\varphi : R \to S$ 是环同态, S 称为 $R-$ 代数.

注解 3.1

一个 $R-$ 代数 S 自然满足:

存在群作用 $R \times S \hookrightarrow S, (r,s) \mapsto \varphi(r)s$ 使得, $r(s+s') = rs + rs', (r+r')s = rs + r's, (rr')s = r(r's), 1 \cdot s = s$.

定义 3.0.2: 代数的生成

若 $R-$ 代数 $S = R[s_1, s_2, s_3, \cdots], \overbrace{s_1, s_2, s_3, \cdots}^{\text{不一定有限}} \in S$, 则称 $s_1, s_2, \cdots$ 是 $R-$ 代数的生成元.

注解 3.2

同态 $\underset{\text{诱导}}{\rightsquigarrow}$ 群作用 $\underset{\text{复合 }+}{\rightsquigarrow}$ (直观上的) 多项式

例 3.0.1

1. 任意环 S 是 $\mathbb{Z}-$ 代数, $\varphi(n) = n \cdot 1_R$.
2. 任意环 S 是其子环 R 的 $R-$ 代数.
3. 多项式环 $R[x_1, \cdots, x_n]$ 是 $R-$ 代数, $\varphi(\alpha) = \alpha, \alpha \in R$.

定义 3.0.3: 代数同态

设 S, S' 是 $R-$ 代数, $\varphi : S \to S'$ 若满足 $\varphi(rs) = r\varphi(s), \forall r \in R, s \in S$, 则称 φ 为 $R-$ 代数同态.

3.0.1 理想 vs 代数

例 3.0.2

$\mathbb{F}[x, y]$ 是代数 ($\mathbb{F}$ 是域).

$$\begin{array}{ccccc}
y^4 & xy^4 & x^2y^4 & x^3y^4 & x^4y^4 \\
y^3 & xy^3 & x^2y^3 & x^3y^3 & x^4y^3 \\
y^2 & xy^2 & x^2y^2 & x^3y^2 & x^4y^2 \\
y & xy & x^2y & x^3y & x^4y \\
1 & x & x^2 & x^3 & x^4
\end{array}$$

凸集 (包含上方及右侧所有元素)(张成的向量空间)$\longrightarrow$ 理想

凸点 $\longrightarrow$ 极小元 (整除关系) $\longrightarrow$ 生成元

$\updownarrow$

理想升链极大元 (有限个, 由 Dickson 引理)

注解 3.3

有限生成理想 $\cup\mathbb{F}$ 是一个代数, 但不一定是有限生成代数.

$$(x) \underset{\mathbb{F}[x,y]}{\underset{\cap}{\bigcup}} \mathbb{F} = \underset{\mathbb{F}[x,y]}{\underset{\cap}{\mathbb{F}\left[x, xy, xy^2, xy^3, \cdots\right]}} \text{不是有限生成子代数}$$

3.1 多项式环上的群作用

3.1.1 方式 1: 由群表示诱导

定义 3.1.1: 群表示

设 G 为群, $GL(n,\mathbb{F}) \overset{\text{def}}{=} \{\mathbb{F}\text{上}n \times n\text{可逆矩阵}\}$, $\mathbb{F}$ 是域.($(GL(n,\mathbb{F}),\circ)$ 是一个群.) 群同态 $\rho : G \to GL(n,\mathbb{F})$ 称为 G 的一个表示. **若 ρ 为单射, 称为忠实表示.**

3.1.2 群表示 vs 群作用

注解 3.4

引理 1. $\forall g \in G$ 诱导了 $\mathbb{F}^n$ 上的线性变换, 即 $g : \mathbb{F}^n \to \mathbb{F}^n, v \mapsto g \cdot f \overset{def}{=} (\rho(g)v^t)^t, v = (v_1, \cdots, v_n) \in \mathbb{F}^n$.

引理 2. G 的表示诱导了 $\mathbb{F}^n$ 上的线性群作用, 即 $G \times \mathbb{F}^n \to \mathbb{F}^n, (g,v) \mapsto (\rho(g)v^t)^t, v = (v_1, \cdots, v_n) \in \mathbb{F}^n$.

$$
\begin{array}{ccc}
\text{非平凡群表示} \rightsquigarrow & \text{线性群作用} & \rightsquigarrow \text{非线性群作用} \\
\rho : G \to GL(n,\mathbb{F}) \rightsquigarrow & G \times \mathbb{F}^n \to \mathbb{F}^n \rightsquigarrow G \times (\mathbb{F}^n)^* \to (\mathbb{F}^n)^* & \rightsquigarrow G \times \mathbb{F}[x_1, \cdots, x_n] \to \mathbb{F}[x_1, \cdots, x_n] \\
g \mapsto \rho(g) & (g,v) \mapsto (\rho(g)v^t)^t \quad (g, x(v)) \mapsto x(g^{-1} \cdot v) & \left(g, \sum \alpha_{i_1,\cdots,i_n} x_1^{i_1} \cdots x_n^{i_n}\right) \mapsto \sum \alpha_{i_1,\cdots,i_n} (gx_1)^{i_1} \cdots (gx_n)^{i_n}
\end{array}
$$

性质 3.1.2

$\mathbb{F}[x_1, \cdots, x_n]^G \overset{\text{def}}{=} \{f \in \mathbb{F}[x_1, \cdots, x_n] : g \cdot f = f, \forall g \in G\}$ 是 $\mathbb{F}[x_1, \cdots, x_n]$ 的子环, 亦为 $\mathbb{F}-$ 代数, 称为**不变子环**.

$g \cdot 1 = g \cdot (1 \cdot 1) = (g \cdot 1)^2 \implies \deg(g \cdot 1) = 0, g \cdot 1 = \alpha \in \mathbb{F}, \alpha^2 = \alpha \overset{\text{非平凡}}{\implies} \alpha = 1, g \cdot k = k, \forall k \in \mathbb{F} \implies \mathbb{F} \subset \mathbb{F}[x_1, \cdots, x_n]^G$, 对 $\forall f_1, f_2 \in \mathbb{F}[x_1, \cdots, x_n]^G, g(f_1 - f_2) = g \cdot f_1 + g \cdot (-f_2) = f_1 - f_2 \in \mathbb{F}[x_1, \cdots, x_n]^G, g(f_1 f_2) = (g \cdot f_1)(g \cdot f_2) = f_1 f_2 \in \mathbb{F}[x_1, \cdots, x_n]^G \implies \mathbb{F}[x_1, \cdots, x_n]^G$ 是子环. 又 $\mathbb{F} \to \mathbb{F}[x_1, \cdots, x_n]^G, k \mapsto k$ 是环同态, $\mathbb{F}[x_1, \cdots, x_n]^G$ 是 $\mathbb{F}-$ 代数.

注解 3.5

由于 $\mathbb{F}[x_1,\cdots,x_n]^{G/\ker\rho}=\mathbb{F}[x_1,\cdots,x_n]^G$, 因此可以不妨设 ρ 是忠实表示.

作业 3.1

写清楚 $G/\ker\rho\times\mathbb{F}[x_1,x_2,\cdots,x_n]\to\mathbb{F}[x_1,x_2,\cdots,x_n]$, 并求证上述注解.

3.1.3 方式 2: 环自同构子群作用

定义 3.1.3

$\mathrm{Aut}(\mathbb{F}[x_1,\cdots,x_n])$: 多项式环自同构群.

性质 3.1.4

令 $G\subset\mathrm{Aut}(\mathbb{F}[x_1,\cdots,x_n])$, 群作用 $G\times\mathbb{F}[x_1,\cdots,x_n]\to\mathbb{F}[x_1,\cdots,x_n],(\varphi,f)\mapsto\varphi(f)$ 的不变子集 $\mathbb{F}[x_1,\cdots,x_n^G$ 是 $\mathbb{F}[x_1,\cdots,x_n]$ 的不变子环, 亦是 $\mathbb{F}-$ 代数.

$$\left.\begin{aligned}\varphi(kf)=\varphi(k)\varphi(f)=k\varphi(f)\\ \varphi(f_1+f_2)=\varphi(f_1)+\varphi(f_2)\end{aligned}\right\}\varphi\text{是线性作用}$$

$\forall f_1^G,f_2^G\in\mathbb{F}[x_1,\cdots,x_n]^G,\varphi(f_1^G-f_2^G)=\varphi(f_1^G)-\varphi(f_2^G)=f_1^G-f_2^G\in\mathbb{F}[x_1,\cdots,x_n]^G,\varphi(f_1^Gf_2^G)=\varphi(f_1^G)\varphi(f_2^G)=f_1^Gf_2^G\in\mathbb{F}[x_1,\cdots,x_n]^G$. $\mathbb{F}[x_1,\cdots,x_n]^G$ 是子环及 $\mathbb{F}-$ 子代数.

猜想 3.1.1: Hilbert 14 问题:

$\mathbb{F}[x_1,\cdots,x_n]^G$ 是不是有限生成 $\mathbb{F}-$ 代数?

例 3.1.1

$G=S_n\curvearrowright S=k[x_1,\cdots,x_n],S^G=k[s_1,\cdots,s_n],s_i$ 是对称多项式 (代数无关).

例 3.1.2

$G=A_n$(交错群: 偶置换构成子群)$\subset S_n \overset{\text{限制作用}}{\curvearrowright} A=\mathbb{F}[x_1,\cdots,x_n]$.

定理 3.1.5

A^G 是由 $s_1,\cdots,s_n$ 及 Vandermonde 行列式 $\nabla_n=\prod\limits_{i<j}(x_i-x_j)$ 生成. 特别地, 存在多项式 $p(s_1,\cdots,s_n)$ 使得 $\nabla_n-p(s_1,\cdots,s_n)=0$(当 $n=2$ 时, $\nabla_2^2=(x_1-x_2)^2=(x_1+x_2)^2-4x_1x_2=s_1^2-4s_2,\nabla_2^2-4e_1^2-4e_2=0$). 即存在关系 (syzygy).

例 3.1.3

$G=\mathbb{Z}/3\mathbb{Z}$ 作用在 $A=\mathbb{C}[x,y],1\cdot(x,y)=(\omega x,\omega y),\omega^3=1,\omega=\mathrm{e}^{\frac{2}{3}\pi\mathrm{i}},x^ay^b\in A^G\Longleftrightarrow 3|a+b$.

定理 3.1.6

A^G 是由 x^3,x^2y,xy^2,y^3 有限生成的 $\mathbb{C}-$ 代数.

令 $z_0=x^3,z_1=x^2y,z_2=xy^2,z_3=y^3$, $z_0,\cdots,z_3$ 蕴含关系

$$\begin{cases} z_0z_3-z_1z_2=0 \\ z_0z_2-z_1^2=0 \\ z_1z_3-z_2^2=0 \end{cases} \quad (3\text{ 个 }1\text{ 阶 syzygy}).$$

令 $\begin{array}{c} a_1=z_2^2-z_1z_3 \\ a_2=z_0z_3-z_1z_2 \\ a_3=z_1^2-z_0z_2 \end{array} \Longrightarrow a_1,a_2,a_3$ 蕴含关系: $\begin{cases} z_1a_1+z_2a_2+z_3a_3=0 \\ z_0a_1+z_1a_2+z_2a_3=0 \end{cases}$ (2 个 2 阶 syzygy).

例 3.1.4: 二项式的不变理论

$SL(2,\mathbb{C})=\left(\begin{array}{cc} m & n \\ p & q \end{array}:mq-pn=1,m,n,p,q\in\mathbb{C}\right),V_d=\mathbb{C}[x,y]_d$($d$阶齐次多项式 $\rightsquigarrow d+1$维向量空间$,\cong\mathbb{C}^{d+1}$).

定义 $SL(2,\mathbb{C})$ 在 $\mathbb{C}[x_0,\cdots,x_d]$ 上的群作用如下:

第一步:

$$\begin{aligned} SL(2,\mathbb{C})\times\mathbb{C}^2 &\to \mathbb{C}^2 \\ (A,v) &\mapsto Av \end{aligned} \underset{\text{诱导}}{\rightsquigarrow} SL(2,\mathbb{C}\times V_d \to V_d$$

第二步:

$$g\cdot f(v)=f(g^{-1}v), f\in V_d, v\in\mathbb{C}^2, g\in SL(2,\mathbb{C}) \underset{\text{诱导}}{\rightsquigarrow} SL(2,\mathbb{C})\times\mathbb{C}[x_0,\cdots,x_d]\to\mathbb{C}[x_0,\cdots,x_d]$$

向量空间 $\longrightarrow$ 多项式 ($\cong$ 向量空间)

第三步:

$$g\cdot j(f)=j(g^{-1}f)\forall j\in\mathbb{C}[x_0,\cdots,x_d]$$

当 $d=2, V_2=\{f=a_0x^2+2a_1xy+a_2y^2, a_i\in\mathbb{C}\}$, 验证:$j(f)=a_1^2-a_0a_2\in\mathbb{C}[a_0,a_1,a_2]$ 是不变的.

$$SL(2,\mathbb{C})\curvearrowright\mathbb{C}[a_0,a_1,a_2]$$

$$g=\begin{pmatrix} m & n \\ p & q\end{pmatrix}, mq-pn=1, g\cdot v=\begin{pmatrix} m & n \\ p & q\end{pmatrix}\begin{pmatrix} x \\ y\end{pmatrix}=\begin{pmatrix} mx+ny \\ px+qy\end{pmatrix}$$

$$\uparrow$$

$$\begin{pmatrix} x \\ y\end{pmatrix}$$

$$g^{-1}\cdot f(v)=f(g\cdot v)=a_0(mx+ny)^2+2a_1(mx+ny)(px+qy)+a_2(px+qy)^2$$

$$=(a_0m^2+2a_1mp+a_2p^2)x^2+2(a_0mn+a_1np+a_1mq+a_2pq)xy+(a_0n^2+2a_1nq+a_2q^2)y^2$$

$$j(g^{-1}f)=(a_0mn+a_1np+a_1mq+a_2pq)^2-(a_0m^2+2a_1mp+a_2p^2)(a_0n^2+2a_1mq+a_2q^2)$$

$$=(a_1^2-a_0a_2)(mq-np)^2=a_1^2-a_0a_2=j(f)$$

定理 3.1.7

$\mathbb{C}[a_0,a_1,a_2]^{SL(2,\mathbb{C})}=\mathbb{C}[a_1^2-2a_0a_2]$.

定理 3.1.8

d	生成元个数
3	1
4	2
5	4
6	5
7	30
8	9
9	92

(对 d 充分大的情形) 最少 d 个, 上界 $\leq d^6$(有限生成, Gordan$\longrightarrow$Hilbert).

定理 3.1.9: IT 基本定理

$\mathbb{F}$ 是特征 0 域, $S = \mathbb{F}[x_1, \cdots, x_n], G \subset \mathrm{Aut}(\mathbb{F}[x_1, \cdots, x_n])$ 是有限群, 则 S^G 有限生成.

关键点 1: 将环分次.

$$
\begin{array}{cccccl}
\mathbb{F}[x_1, \cdots, x_n] & = R_0 & \oplus R_1 & \oplus R_2 \cdots & & \\
\cup & {\scriptstyle 0\text{ 次}} \| & {\scriptstyle 1\text{ 次}} \cup & \cup {\scriptstyle 2\text{ 次}} & & \\
\mathbb{F}[V]^G & = I_0 & \oplus I_1 & \oplus I_2 \cdots & \searrow & \text{分次环} \\
 & \| & & & & \\
 & \mathbb{F} & & & &
\end{array}
$$

设 J 是 $\mathbb{F}[x_1, \cdots, x_n]$ 中由 $I_1, I_2, \cdots$ 生成的理想.

$$J = SI_1 + SI_2 + \cdots \subset \mathbb{F}[x_1, \cdots, x_n]$$

关键点 2: Hilbert 基定理: $\mathbb{F}[x_1, \cdots, x_n]$ 任意理想有限生成 (Noether 环).

由 Hilbert 基定理, 可设 $J = (a_1, \cdots, a_k)$. 下证: $S^G = \mathbb{F}[a_1, \cdots, a_k]$, 即对 $\forall f \in S^G, f \in \mathbb{F}[a_1, \cdots, a_k]$. 对 $\deg f$ 进行归纳证明:

1. 若 $\deg f = 0, f \in \mathbb{F} \subset \mathbb{F}[a_1, \cdots, a_k]$ 自然成立.

2. 假设若 $\deg f \leq m$, 都有 $f \in \mathbb{F}$, 对于 $\deg = m + 1 > 0$ 的 $f \in S^G$ 有

$$
\begin{aligned}
f &= f_{\deg=0} && + f_{\deg>0} \in J \\
&= c_0 && + a_1c_1 + a_2c_2 + \cdots + a_kc_k, c_k \in \mathbb{F}[x_1, \cdots, x_n]
\end{aligned}
$$

关键点 3: 应用平均 (缠结, Reynold) 算子, $\pi^G : S \to S^G, f \mapsto \frac{1}{|G|}\sum_{g\in G} g\cdot f$**.**

$$f = \pi^G(f) = \pi^G(a_1c_1) + \cdots + \pi^G(a_kc_k) + c_0 = \sum_i \frac{1}{|G|}\sum_{g\in G}(\overset{a_i}{\overset{\parallel}{g\cdot a_i}})(g\cdot c_i) + c_0$$

$$= a_1\pi^G(c_1) + \cdots + a_k\pi^G(c_k) + c_0$$

由于 $\pi^G \in S^G$, 且 $\deg \le m$, 根据归纳假设, $\pi^G(c_i) \in \mathbb{F}[a_1, \cdots, a_k], \forall i$. 因此 $f \in \mathbb{F}[a_1, \cdots, a_k]$.

注解 3.6

1. 若 G 非有限群的约化群, $\frac{1}{|G|}\sum_{g\in G} g\cdot f = \underset{\text{紧李群}(SU(n))}{\int_G} g\cdot f\mathrm{d}g$ (不变积分).
2. $\mathbb{F}$ 特征 p, 若 $p \nmid |G|$ 时, 亦成立.

Chapter 4

Hilbert 基定理证明与 Gröbner 基

4.1 Noether 环与 Hilbert 基定理

4.1.1 Noether 环的等价定义

性质 4.1.1

下列命题等价:

1.R 的任意理想是有限生成的,

2. 任意严格递理想升链 $I_1 \subset I_2 \subset I_3 \subset \cdots$ 的长度是有限的.

3. 设 $S = \{R\text{中的所有理想}\}, \subset$ 是序关系, S 的任意非空子集有极大元.

$1 \implies 2$

对于任意给定的严格理想升链, 由升链条件得, $I = \bigcup\limits_{i \in \mathbb{N}^*} I_i$ 是理想.

注解 4.1

一般地, 理想的并不是理想.

由 1 得, I 是有限生成的, 设生成元是 $a_1, \cdots, a_k$, 由于每一个 a_i 必属于某一个 I_j, 故 $\exists n \in \mathbb{N}^*$, 使得 I_n 包含所有 a_i, 故升链长度有限.

$2 \implies 1$

不妨设 I 为 R 的非零理想. 取 I 中的非零元 a_1, 若 $I \neq (a_1)$, 继续取 $a_2 \in I$ 使得 $a_2 \notin (a_1)$, 若 $I \neq (a_1, a_2)$, 继续取 $a_3 \in I$ 使得 $a_3 \notin (a_1, a_2)$, 以此类推, 则得到严格升链 $0 \subset (a_1) \subset (a_1, a_2) \subset \cdots$, 由2得长度有限, 故在某一个 a_k 终止. 故 $I = (a_1, \cdots, a_k)$ 为有限生成理想.

注解 4.2

$2 \Longleftrightarrow 3$ 与环结构无关, 适用于所有偏序集.

$2 \Longrightarrow 3$, 对 S 的任意非空子集 T, 取 $I_1 \in T$, 若 I_1 不是极大元, 则 $\exists I_2$ 使得 $I_1 \subset I_2$, 若 I_2 仍不是极大元, 则 $\exists I_3$ 使得 $I_1 \subset I_2 \subset I_3$, 假设没有极大元, 则得 ∞ 长度的升链, 矛盾.

$3 \Longrightarrow 2$, 考虑升链 $I_1 \subset I_2 \subset I_3 \subset \cdots$, 选取 $(\{I_k, \subset\})$ 中的极大元 $I_m \Longrightarrow$ 升链终止于 $I_m \Longrightarrow$ 长度有限.

注解 4.3

2中升链有限长 $\not\leftrightarrows$ 降链有限长 (Artin 环).

例 4.1.1

$\mathbb{Z}$ 是 Noether 环但 $(2) \supset (4) \supset (8) \cdots$ 是无穷降链.

4.1.2 Hilbert 基定理

注解 4.4: 动机

1. 不变理论:$S = k[x_1, \cdots, x_n]$, 证明 S^G 有限生成.

2. 设 X 是多项式集 $K \subset S$ 的公共零点集 $\overset{\text{称为}(K\text{的})\text{代数集}}{\overset{\downarrow}{V(K)}} \overset{\text{def}}{=} \{p \in \mathbb{F}^n : f(p) = 0, \forall f \in K\}$, 则 X 是有限个多项式 $\underset{(K)=(f_1,f_2,\cdots,f_m)}{\underset{\downarrow}{f_1, f_2, \cdots, f_m}}$ 的代数集.

定理 4.1.2

R 是 Noether 环 $\Longrightarrow R[x]$ 是 Noether 环 $\Longrightarrow R[x_1,\cdots,x_n]$ 是 Noether 环.

设 I 是 $R[x]$ 的理想, 分次: $I=\underset{0\text{ 次}}{I_0}+\underset{1\text{ 次}}{I_1}+\cdots+\underset{k\text{次}}{I_k}$.

$$J_0=\{\underset{(\text{即所有}f(x)=\boxed{a_0}\in I)}{I_0\text{首系数}}\}$$

$$J_1=\{\underset{(\text{即所有}f(x)=\boxed{a_1}x+a_0\in I)}{I_1\text{首系数}}\}\cup\{0\}$$

$$J_2=\{\underset{(\text{即所有}f(x)=\boxed{a_2}x^2+a_1x+a_0\in I)}{I_2\text{首系数}}\}\cup\{0\}$$

$$\cdots$$

$$J_k=\{I_k\text{首系数}\}\cup\{0\}$$

由 I 是 $R[x]$ 的理想得 J_k 是 R 的理想 $(RI\subset I)$, 且 $J_0\subset J_1\subset J_2\subset J_3\cdots(xI_k\subset I\Longrightarrow xI_k\subset I_{k+1}\Longrightarrow J_k\subset J_{k+1})$, 由 R 是 Noether 环得 J_k 有限生成且 $J_0\subset J_1\subset J_2\cdots\subset J_n$ 长度有限.

下面构造 I 的生成集. 令

$$S_0=\{J_0\text{生成元所对应的}I_0\text{中代表元}\}\subset I(\text{有限集})$$

$$S_1=\{J_1\text{生成元所对应的}I_1\text{中代表元}\}\subset I(\text{有限集})$$

$$(a_1\in J_1\Longrightarrow\text{任取 1 个代表元}a_1x+a_0\in I_1)$$

$$\vdots$$

$$S_{\underset{\text{长度有限}}{\underset{\downarrow}{n}}}=\{J_n\text{生成元所对应的}\underset{\text{有限集}}{\underset{\downarrow}{I_n}}\text{中代表元}\}\subset I(\text{有限集})$$

令 $S=\bigcup\limits_{k=0}^{n}S_k(\text{有限集})$, 下证 $I=(S)$. 对 $\forall f=a_mx^m+a_{m-1}x^{m-1}+\cdots+a_0\in I$. $\exists$ 多项式 $g\in(S)$ 使得 f 与 g 的首系数相同.

若 $m \leq n$, 则 $a_m \in J_m$, 令 $f_1 = g \in (S)$.

若 $m > n$, 令 $f_1 = gx^{m-n} \in (S)$.

则 $f - f_1$ 的最高次项被消去, 故 $\deg(f - f_1) < \deg f$. 由于 $f - f_1 \in I$, 依相同方法, 可继续降低次数, 并在最多 $\deg f$ 步内将次数降为 0.

故 $f - f_1 - f_2 - \cdots - f_k = 0 \Longrightarrow f = f_1 + f_2 \cdots + f_k \in (S) \Longrightarrow I \subset (S) \subset I = (S)$.

作业 4.1

设 R 是 Noether 环, 求证: R 的形式幂级数环 $R[[x]]$ 是 Noether 环.(提示: 考虑常数项生成的理想.)

4.1.3 Hilbert 基定理的推论

性质 4.1.3

若环 R 是 Noether 环, 则 R/I 为 Noether 环.

由于 R/I 的理想与 R 中包含的理想 $1-1$ 对应, 故 R/I 中的理想有限生成. $J + I \subset R/I \longleftrightarrow I + J \subset R$.

性质 4.1.4

Noether 环的同态像是 Noether 环.

$\varphi : R \to S, \mathrm{Im}\varphi \cong R/\ker\varphi$, 由性质4.1.3得证.

定理 4.1.5

设 R 为 Noether 环, 若 S 是一个有限生成的 $R-$ 代数, 则 S 是 Noether 环.

设 $S = R[s_1, \cdots, s_n], s_1, \cdots, s_n \in S$. 则 $\varphi : R[x_1, \cdots, x_n] \to R[s_1, \cdots, s_n], f \mapsto f(s_1, \cdots, s_n)$ 是环同态. 由同构定理 $S \cong R[s_1, \cdots, s_n]/\ker\varphi$. 由性质4.1.3, S 是 Noether 环.

4.2 Gröbner 基的存在性与域上的 Hilbert 基定理

定义 4.2.1: 字典序

考虑 $\mathbb{F}[x_1,\cdots,x_n]$ 中的单项式, $\overset{m_1}{\overset{\parallel}{Ax_1^{a_1}x_2^{a_2}\cdots x_n^{a_n}}} \underset{lex}{>} \overset{m_2}{\overset{\parallel}{Bx_1^{b_1}x_2^{b_2}\cdots x_n^{b_n}}} \overset{def}{\Longleftrightarrow} a_1 > b_1$或$a_1 = b_1$且$a_2 > b_2,\cdots$, 即第一个不同的$a_i \neq b_i$有$a_i > b_i$.

定义 4.2.2: 次数字典序

$\overset{m_1}{\overset{\parallel}{Ax_1^{a_1}x_2^{a_2}\cdots x_n^{a_n}}} \underset{grlex}{>} \overset{m_2}{\overset{\parallel}{Bx_1^{b_1}x_2^{b_2}\cdots x_n^{b_n}}} \overset{def}{\Longleftrightarrow} \deg m_1 > \deg m_2$或$\deg m_1 = \deg m_2$且$m_1 \underset{lex}{>} m_2$.

定义 4.2.3: 整除偏序

$m_1 \underset{div}{<} m_2 \Longleftrightarrow m_1|m_2$.

定义 4.2.4: 单项式序

单项式集合上的全序满足:

1. $m \geq 1, \forall m = Ax_1^{a_1}\cdots x_n^{a_n}$,
2. 若 $m_1 \geq m_2$, 则 $mm_1 \geq mm_2$ 对所有 m.

结论 4.2.5

字典序, 次数字典序都是单项式序, 整除偏序不是单项式序.

定义 4.2.6: Gröbner 基

设 $<$ 是 $\mathbb{F}[x_1,\cdots,x_n]$ 中单项式序, $f \in \mathbb{F}[x_1,\cdots,x_n] \longrightarrow \mathrm{LT}(f) \overset{\text{def}}{=} f$的首项, I 是 $\mathbb{F}[x_1,\cdots,x_n]$ 的理想 $\longrightarrow \mathrm{LT}(I)(\mathrm{LT}(f) : f \in I) \longrightarrow$ 生成理想.

$\{g_1,\cdots,g_n\}$ 称为 I 的 Gröbner 基, 若 $g_1,\cdots,g_n$ 生成 I 且 $\mathrm{LT}(g_1),\cdots,\mathrm{LT}(g_n)$ 生成 $\mathrm{LT}(I)$.

4.2.1 Gröbner 基的优势

例 4.2.1

令 I 是 $\mathbb{F}[x,y]$ 中由 $g_1 = xy + \underset{\text{非 Gröbner 基}}{1}, g_2 = x + y$ 生成的理想, 令 $f = x^2y + y$, 考虑 f 是否属于 I.

$$f = \boxed{x^2y} + y, g_1 = \boxed{xy} + 1, g_2 = \boxed{x} + y$$

$$f = x^2y = xg_1 \boxed{-x} + y = xg_1 - g_2 + 2y$$

$$\text{或} = xy(x+y) - \boxed{xy^2} + y = xyg_2 - yg_1 - 2y$$

$$f = f_I + r, f_I \in I, \boxed{r\text{与带余除法顺序选取有关}}$$

定理 4.2.7

固定 $\mathbb{F}[x_1, \cdots, x_n]$ 上的单项式和理想 I 的 Gröbner 基 $\{g_1, \cdots, g_m\}$, 则

1. 任意 $f \in R$ 可以唯一分解为 $f = f_I + r$, 其中 $f_I \in I$, 且对任意 $g_i, \mathrm{LT}(g_i) \nmid r$ 中任意单项式, 即 f_i 和 r 与带余除法中 g_i 顺序的选取无关.

2.$f \in I \iff r = 0$.

1. 对 $g_1, \cdots, g_m$ 做带余除法, $\exists$ 分解 $f = f_I + r = f_I' + r'$, 则 $\mathrm{LT}(r - r') \in \mathrm{LT}(I)$ 则单项式 $\mathrm{LT}(r - r') = m\mathrm{LT}(g_i), m$ 是单项式. 由于 $\mathrm{LT}(g_i) \nmid \mathrm{LT}(r)$, 且 $\mathrm{LT}(g_i) \nmid \mathrm{LT}(r')$. 同理, r 中各单项式都相同.

2.$\Longleftarrow$ 定义可得.

$\Longrightarrow f = f_I + 0$ 是唯一分解, $r = 0$.

4.2.2 域上加强版的 Hilbert 基定理

定理 4.2.8

对 $\forall$ 理想 $I \subset \mathbb{F}[x_1, \cdots, x_n], I$ 存在 Gröbner 基.

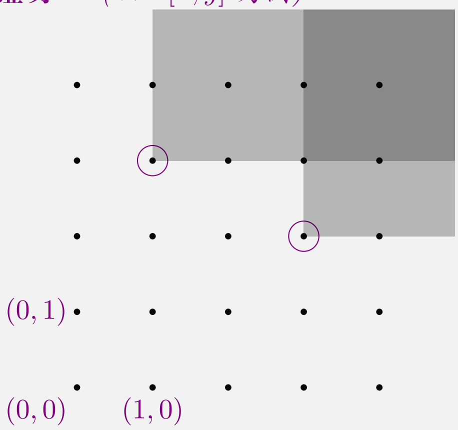
引理 1. *若 $g_1, \cdots, g_m \in I$ 满足 $(LT(g_1), \cdots, LT(g_m) = LT(I))$, 则 $I = (g_1, \cdots, g_m)$.*

证明 1. *对 $\forall f \in I$, 由带余除法 $f = c_1g_1 + \cdots + c_mg_m + r$, 则 $r \in I$, 且 $LT(r) \in$*

$LT(I) = (LT(g_1), \cdots, LT(g_m))$. 故 $\exists i, LT(g_i) | LT(r)$. 又由带余除法定义 $r = 0$, 故 $f \in (g_1, \cdots, g_m)$.

引理 2 (Dickson 引理)**.** *设 S 为 $\mathbb{F}$ 上的任意单项式集合, 则 S 在整除的偏序关系下只有有限个极小元.*

证明 2. *(以 $\mathbb{F}[x, y]$ 为例)*



1. 将 x, y 的次数在格点上作图.

2. 圈出 S 最左侧一列最下方的点 (k_1, m_1), 并划去 S 中 (k_1, m_1) 包含边界在内右上方的所有点 (即 $> x^{k_1}y^{m_1}$ 的所有点).

3. 圈出剩下点中最左侧一列最下方的点 (k_2, m_2) 并划去右上方的点.

4. 按相同方法继续选点, 由于 $m_1 > m_2 > m_3 \cdots$ 故有限步内 $m_n = 0$.

注解 4.5

对 n 元多项式只需在 n 维格点上用相同方法.

由 Dickson 引理, $\overset{\substack{\text{字典序}\\ \downarrow}}{\mathrm{LT}(I)}$ 由有限个 $\overset{\substack{\text{整除偏序}\\ \downarrow}}{\text{极小元}}$ $L_1, \cdots, L_m$ 生成. 由引理 1, 只需选取 $g_1, \cdots, g_m \in I$, 使得 $\mathrm{LT}(g_1) = L_1, \cdots, \mathrm{LT}(g_m) = L_m$, 自然满足:$I = (g_1, \cdots, g_m)$.

Chapter 5

Buchberger 算法, Noether 模

5.1 Hilbert 基定理的组合直观

5.1.1 $R[x]$ 情形

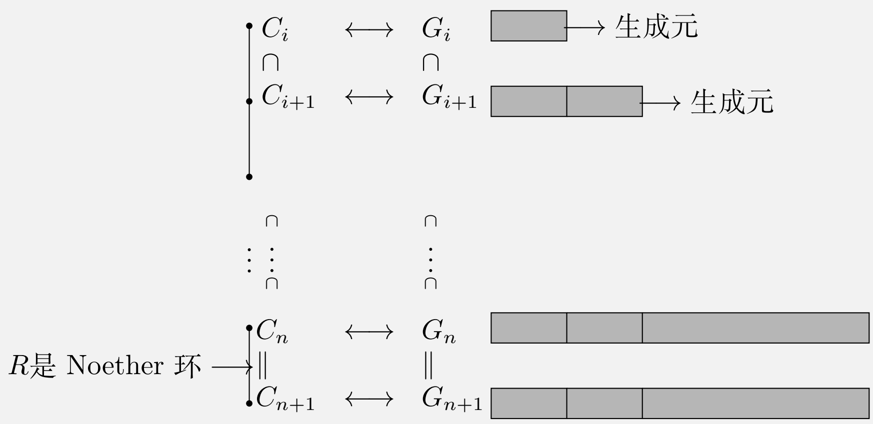
性质 5.1.1

$I \subset R[x], C_i = \{ \overset{\text{最高次系数}}{\overset{\uparrow}{\mathrm{LC}}}(f) : \deg f = i, f \in I\} \cup \{0\} \subset R.$

C_i 构成 1− 叉树, $C_i \bullet\!\!\longrightarrow\!\!\bullet\, C_{i+1} \Longleftrightarrow$

1. 线代表偏序关系, $x^n | x^{n+1}$ 且 $C_i \subsetneqq C_{i+1}$;

2. 每个点上被赋予了一个 $\underset{\substack{\downarrow \\ R\text{是 Noether 环}}}{\text{有限生成集}}$.



$\Longrightarrow C = (G_n), G_n$ 中每个元素 g 分别在 I 中找 1 个代表元 $i_g \in I$, 则 $I = (i_g : g \in G_n) \longrightarrow$ 有限生成集.

当 $R = \mathbb{F}$ 时 $C_i = C_{i+1} = \cdots = C_{n+1}, G_i = (1) = \mathbb{F}$.

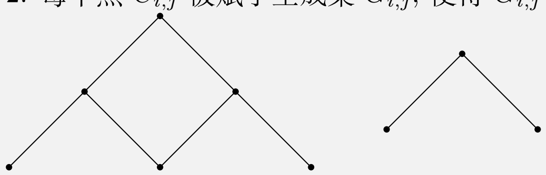
5.1.2 $R[x, y]$ 的情况

性质 5.1.2

$I \subset R[x, y], c_{i,j} = \{\mathrm{LC}(f) : f \in I, \mathrm{LT}(f) = \mathrm{LC}(f)x^i y^j\} \cup \{0\}$.

图中的线 $C_{i,j} \bullet\!\!-\!\!\!-\!\!\!-\!\!\bullet C_{i+1,j}(C_{i,j+1}) \Longleftrightarrow$

1. $x^i y^j | x^{i+1} y^j (x^i y^{j+1})$, 且 $C_{i,j} \subsetneqq C_{i+1,j}(C_{i,j+1})$;
2. 每个点 $C_{i,j}$ 被赋予生成集 $G_{i,j}$, 使得 $G_{i,j} \subsetneqq G_{i+1,j}(G_{i,j+1})$.



性质 5.1.3

R 是 Noether 环 $\Longrightarrow$

1. 每个极小元生成的 2− 叉树的节点有限;
2. 每个节点被赋予的 $G_{i,j}$ 是有限集.

性质 5.1.4

Dickson 引理 $\Longrightarrow$ 极小元只有有限个 $\Longrightarrow$ 所有 $G_{i,j}$ 的并是有限集, 设为 G. 在 G 中每个元素 g 分别找一个 I 中的代表元 i_g, 则 $\{i_g : g \in G\}$ 是 I 的有限生成集.

注解 5.1

$R = \mathbb{F} \Longrightarrow$ 树变为有限个孤立点.

注解 5.2

$R[x_1, \cdots, x_n]$: 将图中的 2− 叉树改为 $n-$ 叉树, 其他不变 $\Longrightarrow G$ 是有限集 $\Longrightarrow \{i_g\}$ 是 I 上的有限生成集.

命题 5.1.1

Noether 环上多项式环理想的 $n-$ 叉树结构?

5.2 Buchberger 算法: Gröbner 的计算

定义 5.2.1

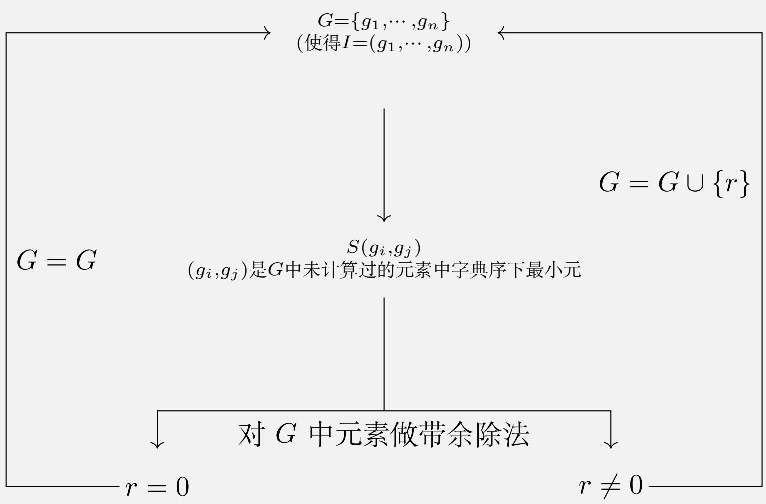
对 $f, g \in \mathbb{F}[x_1, \cdots, x_n]$, 定义: $S(f,g) = \dfrac{M}{\mathrm{LT}(f)} f - \dfrac{M}{\mathrm{LT}(g)} g$, 其中, M 是 $\mathrm{LT}(f), \mathrm{LT}(g)$ 首 1 的最小公倍单项式.

定理 5.2.2

对任意给定单项式序 $<$ 和理想 $I, G = \{g_1, \cdots, g_n\}$ 是 I 的生成元, G 是 Gröbner 基 $\Longleftrightarrow \forall i, j, S(g_i, g_j)$ 对 $g_1, \cdots, g_n$ 做带余除法, 余式为 0.

结论 5.2.3: Buchberger 算法

设 $S(g_1, g_2)$ 对 G 的余式为 r_{12}, 若 $r_{12} \neq 0$, 令 $g_3 = r_{12}$, g 中加入 g_3, 若 $r_{12} = 0$, G 不变. 设 $S(g_1, g_3)$ 对新 G 的余式为 r_{13}, 若 $r_{13} \neq 0$, 令 $g_4 = r_{13}$, G 中加入 g_4, 若 $r_{13} = 0$, G 不变. 按 (i, j) 的字典序, 持续对 $S(g_i, g_j)$ 做带余除法并扩充 G, 直至满足5.2.2中条件, 得到的 G 即为 Gröbner 基.



程序在有限步算完终止, 得到的 G 是 Gröbner 基, $G=\{g_1,\cdots,g_n,g_{n+1},\cdots,g_m\}$.

例 5.2.1

$\mathbb{F}[x,y],<$: 次数字典序, $I=(f,g), f=x^3-2xy, g=x^2y-2y^2+x$, $\mathrm{LT}(f)=x^3, \mathrm{LT}(g)=x^2y, M=x^3y, G=(f,g)$.

$S(f,g)=y(x^3-2xy)-x(x^2y-2y^2+x)=x^3y-2xy^2-x^3y+2xy^2-x^2=-x^2=0f+0g+(-x^2)$

$r_1 \overset{\text{def}}{=} -x^2$.

$$\Longrightarrow G(f,g,r_1), S(f,r_1)=(x^3-2xy)-(-x)(-x^2)=-2xy \overset{\text{def}}{=} r_2$$

$$\Longrightarrow G(f,g,r_1,r_2), S(f,r_2)=y(x^3-2xy)-(-\frac{1}{2})x^2(-2xy)=-2xy^2=yr_2$$

$$\text{又} S(g,r_1)=(x^2y-2y^2+x)-(-y)(-x^2)=-2y^2+x \overset{\text{def}}{=} r_3$$

$$\Longrightarrow G=(f,g,r_1,r_2,r_3), S(f,r_3)=-y^2(x^3-2xy)-(-\frac{1}{2}x^3)(x-2y^2)=2xy^3+\frac{1}{2}x^4=\frac{x}{2}f+x^2y+2xy^3=\frac{x}{2}f$$

$$S(g,r_2)=x^2y-2y^2+x+\frac{1}{2}x(-2xy)=-2y^2+x=r_3$$

$$S(g,r_3)=y(x^2y-2y^2+x)+\frac{1}{2}x^2(-2y^2+x)=-2y^3+xy+\frac{1}{2}x^3$$

$$S(r_1,r_2)=(-y)(-x^2)-(-\frac{1}{2}x)(-2xy)=x^2y-x^2y=0$$

$$S(r_1,r_3)=(-y^2)(-x^2)-(-\frac{1}{2}x^2)(-2y^2+x)=\frac{1}{2}x^3=-\frac{1}{2}xr_1$$

$$S(r_2,r_3)=(-\frac{1}{2}y)(-2xy)-(-\frac{1}{2}x)(-2y^2+x)=-\frac{1}{2}r_1$$

$\Longrightarrow G=(f,g,r_1,r_2,r_3)$ 是 Gröbner 基.

注解 5.3

I 的 Gröbner 基不唯一, 特别地, 若存在 $p\in G$ 使得 $\mathrm{LT}(p)\in(\mathrm{LT}(G-\{p\}))$, 则 $G-\{p\}$ 是 I 的 Gröbner 基.

定义 5.2.4: 极小的 Gröbner 基

若 I 的 Gröbner 基 G 满足:

1. $\forall p\in G$ 是首 1 多项式;
2. $\forall p\in G,\mathrm{LT}(p)\notin(\mathrm{LT}(G-\{p\}))$,

则称 G 是 $\underset{\text{基中元素数量}}{\underset{\downarrow}{\textbf{极小}}}$ **的 Gröbner 基**.

例 5.2.2

上例中, $f_1=x^3-2xy,f_2=x^2y-2y^2+x,f_3=-x^2,f_4=-2xy,f_5=-2y^2+x,\mathrm{LT}(f_1)=xf_3,\mathrm{LT}(f_2)=-yf_3\Longrightarrow\hat{f}_3=x^2,\hat{f}_4=xy,\hat{f}_5=y^2-\frac{1}{2}x$ 是极小的 Gröbner 基, 然而, 极小的 Gröbner 基亦不是唯一的. $\hat{f}_3=x^2+axy,a\in\mathbb{F},\hat{f}_4=xy,\hat{f}_5=y^2-\frac{1}{2}x$ 都是极小的.

5.3 Noether 环 $\rightsquigarrow$Noether 模

注解 5.4

$$\text{模:}\begin{cases}1.\text{环} \overset{\text{作用}}{\curvearrowright} \text{交换群} \\ 2.\ \underset{\text{自由 (线性无关) 生成元}}{\underset{\downarrow}{\text{向量空间}}} \text{的推广: 生成元} + \text{线性关系}\end{cases}$$

定义 5.3.1

$R-$ 模 M 是一个交换群 $(M,+)$ 上赋予环 R 的作用.

$R\times M\to M$, 使得

$$(r_1r_2)\cdot m=r_1\cdot(r_2\cdot m)\quad r\cdot(m_1+m_2)=r\cdot m_1+r\cdot m_2\quad (r_1+r_2)\cdot m=r_1\cdot m+r_2\cdot m\quad 1\cdot m=m$$

例 5.3.1

$$\begin{array}{cc}\text{交换群是}\mathbb{Z}-\text{模} & \mathbb{F}\text{向量空间是}\mathbb{F}-\text{模}(\mathbb{F}\text{是域}) \\ n\cdot g\overset{\text{def}}{=}\underbrace{g+g+\cdots+g}_{n\text{次}} & k\cdot e_i\overset{\text{def}}{=}ke_i\end{array}$$

$$\text{环}R\text{是}R-\text{模}: R\times R\to R\quad r\cdot r'=rr'$$

注解 5.5

环 R 亦是其子环 $S\subset R$ 的 $S-$ 模. $S\cdot r'=Sr'$.

例 5.3.2: 代数 vs 模

S,R 是环.

性质 5.3.2

S 是个 $R-$ 代数 $\Longleftrightarrow$ S 是个 $R-$ 模, 使得 $(r\cdot s_1)s_2 = s_1(r\cdot s_2) = r\cdot(s_1s_2)$.

$\Longrightarrow$ $r\cdot S \overset{\text{def}}{=} \varphi(r)S$, 即为 S 上满足条件的模结构.

$\Longleftarrow$ 只需验证: $R\to S, r\mapsto r\cdot 1_S$ 是环同态.

$$\varphi(r_1r_2) = (r_1r_2)\cdot 1_S = (r\cdot 1_S)(r_2\cdot 1_S) = \varphi(r_1)\varphi(r_2)$$

$$(r_1\cdot 1_S)(r_2\cdot 1_S) = 1_S(r_1\cdot(r_2\cdot 1_S)) = r_1\cdot(r_2\cdot 1_S) = (r_1r_2)\cdot 1_S$$

$$\varphi(r_1+r_2) = \varphi(r_1)+\varphi(r_2)$$

$$(r_1+r_2)\cdot 1_S = r_1\cdot 1_S + r_2\cdot 1_S$$

$$\varphi(1_R) = 1_R\cdot 1_S = 1_S$$

$$\boldsymbol{\varphi(r)S = (r\cdot 1_S)S = r\cdot S}$$

例 5.3.3

群环: 群 $\underset{\text{诱导}}{\rightsquigarrow}$ 环. $(G,\cdot)$: 交换群, $\mathbb{F}$: 域.

$\mathbb{F}G \overset{\text{def}}{=} \left\{\sum_{g\in G}\alpha_g g : \alpha_g\in\mathbb{F}\right\}$, 其中 $\sum_{g\in G}\alpha_g g$ 是形式和.$+$: 形式和, $\cdot$: 群乘法.

1. **给定群表示**

$\rho: G\to GL(V) \rightsquigarrow$ 表示空间 V 是一个 $\mathbb{F}G$ 模: $\mathbb{F}G\times V\to V$

$$\left(\sum_{g\in G}\alpha_g g\right)\cdot v \overset{\text{def}}{=} \sum_{g\in G}\alpha_g\rho(g)\cdot v$$

2. **给定 $\mathbb{F}G-$ 模**

$\mathbb{F}G\times V\to V, \left(\sum_{g\in G}\alpha_g g, v\right)\mapsto \sum_{g\in G}\alpha_g g\cdot v \rightsquigarrow$ 诱导表示: $G\to GL(V), g\mapsto (v\mapsto g\cdot v)$.

5.3.1 模的零化子

作业 5.1: 模的零化子

设 M 是 $R-$ 模, 定义 $\mathrm{Ann}_R M \overset{\text{def}}{=} \{r \in R | rm = 0, \forall m \in M\}$ 称为 M 的零化子. 若 $\mathrm{Ann}_R M = 0$, 则称 $R-$ 模 M 是**忠实的**.

1. 求证: $\mathrm{Ann}_R M$ 是 R 的理想且 M 是忠实的 $R/\mathrm{Ann}_R M-$ 模;
2. 表示 $\rho : G \to GL(n, \mathbb{F})$ 是忠实的, 是否等价于 $\mathbb{F}^n$ 是忠实的 $\mathbb{F}G-$ 模?

5.3.2 子模与理想

注解 5.6

$$\begin{array}{cc}
\text{子模}: R-\text{模}M\text{的子集}N,\text{且仍是}R-\text{模} & \text{理想}: I \subset R \\
\sigma|_N : R \times N \to N\text{使得} & 1.I\text{是}(R,+)\text{子群} \\
1.N\text{是}M\text{子群} & 2.RI \subset I \\
2.\sigma(M) \subset N & \\
\multicolumn{2}{c}{\textbf{把环R看成R-模, 理想I即为子R-模}} \\
M/N\text{为}\quad \underset{r\cdot m\cdot N \overset{\text{def}}{=} (rm)\cdot N}{\underset{\downarrow}{R-\text{模}}} \iff N\text{为子}R-\text{模} & R/I\text{为环} \iff I\text{是理想}
\end{array}$$

定义 5.3.3: 生成元

若 $M = \sum\limits_{i \in \underset{\text{指标集}}{\underset{\downarrow}{A}}} R \cdot m_i$, 则称 $\{m_i\}$ 是 M 的生成元.

若 $I = \sum\limits_{i \in A} R \cdot s_i$, 则称 $\{s_i\}$ 是 I 的生成元.

5.3.3 Noether 模等价定义

性质 5.3.4: Noether 模等价定义

1. $R-$ 模 M 的所有子模有限生成 (注: R 是 Noether 环 $\iff$ R 作为 $R-$ 模是 Noether 模);
2. M 的严格子模升链 $M_1 \subset M_2 \subset \cdots \subset M_n$ 长度有限.
3. S 是 M 子模构成的集合, S 的非空子集有极大元.

把理想替换成子模即可.

注解 5.7

升链长度有限 $\overset{\not\Rightarrow}{\not\Leftarrow}$ 降链长度有限 (Artin 模).

$\not\Rightarrow$ $\mathbb{Z}$ 作为 $\mathbb{Z}-$ 模

$$\not\Leftarrow \mathbb{Z}\left[\frac{1}{2}\right]/\mathbb{Z} \overset{\lim}{=} (\mathbb{Z}/\mathbb{Z} \subset \mathbb{Z}/2\mathbb{Z} \subset \mathbb{Z}/4\mathbb{Z} \subset \cdots)$$

$$\begin{array}{ccc} \downarrow & \downarrow & \downarrow \\ \mathbb{Z}[\frac{1}{2}]/\mathbb{Z} & \mathbb{Z}[\frac{1}{2}]/\mathbb{Z} & \mathbb{Z}[\frac{1}{2}]/\mathbb{Z} \end{array}$$

5.3.4 模上的 Hilbert 基定理

定理 5.3.5: 模上的 Hilbert 基定理

R 是 Noether 环, 则有限生成的 $R-$ 模.

模的两要素 + 正合列.

定义 5.3.6: 模同态

$M, N : R-$ 模, $\varphi : M \to N$ 称为 $R-$ **模同态**, 若 $\varphi(m+m') = \varphi(m)+\varphi(m'), \forall m, m' \in M$, 且 $\varphi(r \cdot m) = r\varphi(m), \forall r \in R, m \in M$.

例 5.3.4

1. $M : R-$ 模, 对 $\forall$ 给定 $m \in M, R \to M, r \mapsto r \cdot m$ 是模同态.
2. $R = \mathbb{R}\left[x_1, \cdots, x_n, \dfrac{\partial}{\partial x_1}, \cdots, \dfrac{\partial}{\partial x_n}\right], M = C^\infty(\mathbb{R}^n)$, 则 M 是 (左)$R-$ 模.

R 的理想 $I \longleftrightarrow$ PDE: $Lf = 0$, 所有 $L \in I$.

$\forall$ 给定 $f \in M, \varphi_f : {}^{R/I \to C^\infty(\mathbb{R}^n)}_{r+I \mapsto rf}$ 是 (左) 模同态.

例 5.3.5

作业 5.2

$\mathbb{F}$ 是特征 0 域, $R=\mathbb{F}[x_1,\cdots,x_n], G\subset \underset{\uparrow}{\overset{\text{代数自同态}}{\mathrm{Aut}}}\ R$ 是有限群, R^G 不变子环. 求证:

1. R 是 R^G- 模;
2. 平均算子 $\pi^G: R\to R, f\mapsto \frac{1}{|G|}\sum_{g\in G} g\cdot f$ 是 R^G- 模同态, 满足 $\mathrm{Im}\pi^G=R^G$ 且 $\pi^G|_{R^G}=\mathrm{Id}$.

定理 5.3.7: 模同构定理

1. $\mathrm{Im}\varphi\cong M/\ker\varphi$;
2. S,T 为 M 的子模, $(S+T)/T\cong S/S\cap T$.

结论 5.3.8: 模的 "两要素"

1. 生成元; 2. 关系.

定义 5.3.9: 模的直和

M_1,M_2 是 $R-$ 模, $M=M_1\oplus M_2$, 是模的直和, $r\cdot(m_1,m_2)\overset{\text{def}}{=\!=}(r\cdot m_1,r\cdot m_2)$.

定义 5.3.10: 自由模

$R-$ 模 M 模同构于若干个 R 的直和.

定理 5.3.11: 两要素定理

对 $\forall R-$ 模 M, M 同构于自由模的商模, 即 $M\cong \overset{\text{生成元}}{\underset{\uparrow}{\bigoplus_{i\in I}}}\Big/\overset{\text{关系}}{\underset{\uparrow}{\sim}}$.

设 $\{m_i, i \in I\}$ 是 M 的生成元, 则 $M = Rm_1 + Rm_2 + \cdots$, 考虑满同态 $\varphi : \bigoplus_{i\in I} R \to M, (r_1, r_2, \cdots) \mapsto r_1m_1 + r_2m_2 + \cdots$, 则 $M \cong \bigoplus_{i\in I} R / \ker\varphi \Longrightarrow \bigoplus_{i\in I} R$ 由自由的生成元决定, $\ker\varphi$ 由生成元的关系决定.

5.3.5 模同态与 PDE 的解

作业 5.3

设 M, N 是 $R-$ 模, $\hom_R(M, N)$ 是所有 $M \to N$ 上 $R-$ 模同态的集合. 令 $(\varphi_1 + \varphi_2)(m) \overset{\text{def}}{=} \varphi_1(m) + \varphi_2(m), \forall m \in M, (r, \varphi)(m) \overset{\text{def}}{=} \varphi(r \cdot m), \forall r \in R, m \in M$. 求证: $\hom_R(M, N)$ 是 $R-$ 模.

作业 5.4

$R = \left[x_1, \cdots, x_n, \dfrac{\partial}{\partial x_1}, \cdots, \dfrac{\partial}{\partial x_n}\right]$, I 是 R 的理想, 探究 $\mathbb{R}^n$ 中 PDE 的解与 $\underset{(\text{右}R-\text{模})}{\boxed{\hom_R(R/I, C^\infty(\mathbb{R}^n))}}$ 的关系.

Chapter 6

正合列, 模上的 Hilbert 基定理, 自由消解与 Syzygy 模

6.1 正合列

定义 6.1.1

设 M 是 $R-$ 模, 考虑模同态链

$$M_1 \xrightarrow{f_1} M_2 \xrightarrow{f_2} M_3 \xrightarrow{f_3} \cdots \xrightarrow{f_{n-1}} M_n$$

若 $\mathrm{Im} f_k = \ker f_{k+1}$, 则称模同态链为正合列.

例 6.1.1

$$0 \to A \underset{a\mapsto(a,0)}{\to} A \oplus B \underset{(a,b)\mapsto b}{\to} B \to 0 \text{是正合列}$$

例 6.1.2

设 B 是 A 子模,

$$0 \to A \underset{b\mapsto b}{\to} A \oplus B \underset{a\mapsto a+B}{\to} B \to 0 \text{是正合列}$$

推论 6.1.2

R^n 是自由模, $\varphi: R^n \to M$ 是模同态, $0 \to \ker\varphi \to R \to M \to 0$ 是正合列.

例 6.1.3

M_1, M_2 是 M 的子模, 则

$$0 \to M_1 \cap M_2 \underset{m \mapsto (m,m)}{\to} M_1 \oplus M_2 \underset{(m_1,m_2) \mapsto m_1 - m_2}{\to} M_1 + M_2 \to 0 \text{是正合列}$$

例 6.1.4

设 $M = (m) = R_m$, 使得 $r_1 m = r_2 m = \cdots = r_n m = 0, r_1, \cdots, r_n \in R$,

$$R^n \underset{(0,\cdots,\underset{\text{第}i\text{个}}{1},\cdots,0) \mapsto r_i}{\to} R \underset{r \mapsto r_m}{\to} M \to 0 \text{是正合列}$$

例 6.1.5

M 两要素:

1. 生成元是 $\{m_\alpha\}_{\alpha \in A} \Longrightarrow$ 同态: $R^A \xrightarrow{\varphi} M, (r_1, r_2, \cdots) \mapsto r_1 m_1 + r_2 m_2 + \cdots$,
2. $M \cong R^A / \ker\varphi \Longrightarrow$ 关系 $\longleftrightarrow$ 理想 $\ker\varphi \subset R$ 的生成元 $\{r_\rho\}_{\rho \in B}$.

则

$$R^B \underset{(0,\cdots,\underset{\text{第}\rho\text{个}}{1},\cdots,0) \mapsto r_i}{\to} R^A \underset{(0,\cdots,\underset{\text{第}\alpha\text{个}}{1},\cdots,0) \mapsto r_i}{\to} M \to 0 \text{是正合列}$$

例 6.1.6

$G = \mathbb{Z}/3\mathbb{Z} \curvearrowright R = \mathbb{C}[x,y], \sigma(x,y) = (\omega x, \omega y), \omega = \mathrm{e}^{\frac{2}{3}\pi \mathrm{i}}, \mathbb{C}[x,y]^G = \mathbb{C}[\underset{z_0(x,y)}{\underset{\parallel}{x^3}}, \underset{z_1(x,y)}{\underset{\parallel}{x^2 y}}, \underset{z_2(x,y)}{\underset{\parallel}{xy^2}}, \underset{z_3(x,y)}{\underset{\parallel}{y^3}}]$ 是有限生成的 $\underset{R}{\overset{\text{def}}{\parallel}}$ $\mathbb{C}[x^3, x^2, xy^2, y^3] -$ 模.

定义 $z_i \cdot z_j(x,y) = z_i(x,y) z_j(x,y)$.

$$z_0 \cdot y^3 = x^3 y^3, z_1 \cdot xy^2 = x^2 yxy^2 = x^3 y^3, \cdots$$

3 个 1 阶 syzygy(关系)

$$z_0z_3 - z_1z_2 = 0, z_1^2 - z_0z_2 = 0, z_2^2 - z_1z_3 = 0(\text{关于}x, y)$$

令 $a_1 = z_2^2 - z_1z_3, a_2 = z_0z_3 - z_1z_2, a_3 = z_1^2 - z_0z_2$, 2 个 2 阶 syzygy

$$z_0a_1 + z_1a_2 + z_2a_3 = 0, z_1a_2 + z_2a_2 + z_3a_3 = 0$$

令 $b_1 = z_0a_1 + z_1a_2 + z_2a_3, b_2 = z_1a_1 + z_2a_2 + z_3a_3$, b_1, b_2 $R-$ 线性无关.
得到 $R-$ 模正合列

$$0 \to \underset{\text{基底}\nwarrow\ \boxed{\begin{matrix} b_1 \\ b_2 \end{matrix}}}{R^2} \begin{array}{c} \xrightarrow{\varphi_2} \\ \begin{matrix} \mapsto & z_0a_1 + z_1a_2 + z_2a_3 \\ \mapsto & z_1a_1 + z_2a_2 + z_3a_3 \end{matrix} \\ \scriptstyle \mathrm{Im}(b_1),\mathrm{Im}(b_2)\ R-\text{线性无关} \end{array} \Big\} R^3\text{中元素} \quad \underset{\text{基底}\nwarrow\ \boxed{\begin{matrix} a_1 \\ a_2 \\ a_3 \end{matrix}}}{R^3} \begin{array}{c} \xrightarrow{\varphi_1} \\ \begin{matrix} \mapsto & z_2^2 - z_1z_3 \\ \mapsto & z_0z_3 - z_1z_2 \\ \mapsto & z_1^2 - z_0z_2 \end{matrix} \\ \scriptstyle \mathrm{Im}(a_1),\mathrm{Im}(a_2),\mathrm{Im}(a_3)\ R-\text{线性无关} \end{array} \overset{\mathbb{C}[z_0,z_1,z_2,z_3]}{\overset{\|}{R}} \begin{array}{c} \xrightarrow{\varphi_0} \\ \begin{matrix} z_0 & \mapsto & x^3 \\ z_1 & \mapsto & x^2y \\ z_2 & \mapsto & xy^2 \\ z_3 & \mapsto & y^3 \end{matrix} \end{array} \mathbb{C}[x, y]^G \to 0$$

$$\mathrm{Im}\varphi_1 \overset{\text{def}}{=} 1\text{阶 syzygy 模}$$

$$\mathrm{Im}\varphi_2 \overset{\text{def}}{=} 2\text{阶 syzygy 模}$$

k 阶 syzygy 模有限生成.

6.2 短正合列的性质

定义 6.2.1: 短正合列

正合列 $0 \to A \xrightarrow{\alpha} B \xrightarrow{\rho} C \to 0$ 称为短正合列.

$\Longleftrightarrow \alpha$ 单射, ρ 满射且 $\mathrm{Im}\alpha = \ker \rho$.

定义 6.2.2: 分裂

若 $\exists$ 模同态 $\tau : C \to B$ 使得 $\rho \circ \tau = \mathrm{Id}$, 则称该短正合列是分裂的.

$\Longleftrightarrow \exists$ 模同态 $\sigma : B \to A$, 使得 $\sigma \circ \alpha = \mathrm{Id}$.

注解 6.1

引理 1. 短正合列 $0 \to A \to B \to C \to 0$ 同构意义下与 $0 \to A \to B \to B/A \to 0$ 相同.

证明 1. α 单射 $\Longrightarrow A$ 是 $B-$ 子模, ρ 是满射 $\Longrightarrow C \cong B/\ker\rho \cong B/A$.

引理 2. 对分裂正合列 $0 \to A \to B \to C \to 0$, 同构意义下有 $B = A \oplus C$.

证明 2. 由 $\ker\rho = \mathrm{Im}\alpha, \rho \circ \tau = Id \Longrightarrow \mathrm{Im}\tau \cap \mathrm{Im}\alpha = \{0\}$.

性质 6.2.3

设 $0 \to A \to B \to C \to 0$ 是短正合列, B 是 Noether 模 $\Longleftrightarrow A, C$ 都是 Noether 模.

$\Longrightarrow$

$0 \to A \xrightarrow{i} B \xrightarrow{\rho} B/A \to 0, A \subset B$, A 的子模升链是 B 的子模升链 $\Longrightarrow A$ 是 Noether 模. 考虑 B/A 的子模升链为 $\{(B_i+A)/A\}$, 由于 $\{B_i+A\}$ 长度有限 $\Longrightarrow \{(B_i+A)/A\}$ 长度有限.

$\Longleftarrow$

设 $\{B_i\}$ 是 B 的子模升链, 则 $\{i^{-1}(B_i)\} = \{A \cap B_i\}$ 是 A 的子模升链, 长度有限. 即 $\exists n \in \mathbb{N}^*$ 使得 $B_m/A \cap B_m = B_{m+1}/A \cap B_{m+1} \cdots \Longrightarrow$ 不妨设 $m \leq n$, 则 $B_n/Q = B_{n+1}/Q = \cdots \Longrightarrow$ 假设 $\exists x \in B_{n+1}$ 且 $x \notin B_n \Longrightarrow x \in Q = A \cap B_{n+1} \subset B_{n+1}$, 矛盾. $\Longrightarrow B_n = B_{n+1}$, 同理 $B_{n+1} = B_{n+2} \cdots \Longrightarrow B$ 是 Noether 模.

推论 6.2.4

若 A, B 是 Noether 模, 则 $A \oplus B$ 是 Noether 模.

推论 6.2.5

若 R 是 Noether 环, 则 R^n 是 Noether $R-$ 模.

6.3 模上 Hilbert 基定理

定理 6.3.1: 模上 Hilbert 基定理

R 是 Noether 环, M 是有限生成 $R-$ 模, 则 M 是 Noether 模.

M 是有限生成 $R-$ 模 $\Longrightarrow M \cong R^n / \ker\varphi, \varphi : R^n \to M$, 得到正合列

$$0 \to \ker\varphi \to R^n \xrightarrow{\varphi} M \to 0$$

.

R 是 Noether 环 $\Longrightarrow R^n$ 是 Noether $R-$ 模, 故 M 和 $\ker\varphi$ 都是 Noether $R-$ 模.

结论 6.3.2: PID 自由模定理

PID 的自由模 D^n 的子模必为自由模 $D^m, m \leq n$.

设 M 是 D^n 子模, 由于 D 是 Noether 环, 故 D^n 是 Noether 模. M 是有限生成, 生成元记为 $f_1, \cdots, f_k$, 则

$$\begin{pmatrix} f_1 \\ \vdots \\ f_k \end{pmatrix} = \underset{\overset{\parallel}{A}}{\begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{k1} & \cdots & a_{kn} \end{pmatrix}} \begin{pmatrix} e_1 \\ \vdots \\ e_n \end{pmatrix} \longrightarrow D^n\text{基底}$$

D 是 PID, $\exists$ 可逆矩阵 $P_{k\times k}$ 和 $Q_{n\times n}$ 使得

$$PAQ = \begin{pmatrix} d_1 & & & & 0 \\ & \ddots & & & \\ & & d_m & & \\ & & & \ddots & \\ 0 & & & & 0 \end{pmatrix}, (d_1) \supset (d_2) \supset \cdots \supset (d_m), d_i \neq 0 \quad \text{([抽象代数, 邓少强]定理3.2.5)}$$

令 $\begin{pmatrix} f_1' \\ \vdots \\ f_k' \end{pmatrix} = P^{-1} \begin{pmatrix} f_1 \\ \vdots \\ f_k \end{pmatrix}, \begin{pmatrix} e_1' \\ \vdots \\ e_k' \end{pmatrix} = Q \begin{pmatrix} e_1 \\ \vdots \\ e_k \end{pmatrix} \Longrightarrow f_i' = d_i e_i', 1 \leq i \leq m, f_i' = 0, i > m$. 则 $\{f_i\}_{i \leq i \leq m}$ 是 M 生成元, 令 $\sum \alpha_i d_i e_i' = 0, \alpha_i \in D, 1 \leq i \leq m$, 则 $\alpha_i d_i = 0, 1 \leq i \leq m \overset{\text{PID}}{\Longrightarrow} \alpha_i = 0, 1 \leq i \leq m$, 故 $M \cong D^M$, 基底为 $f_1', \cdots, f_m'$.

结论 6.3.3: 不变理论: Syzygy 模有限生成

G : 有限群, k: 域, $G \to A = \mathbb{F}[x_1, \cdots, x_n]$ 得到正合列

$$\cdots \to R^{n_2} \underset{\substack{h_k \overset{k=1,\cdots,n_2}{\mapsto} r_k g_k \\ \text{使得} \sum r_k g_k = 0}}{\xrightarrow{\varphi_2}} R^{n_1} \underset{\substack{g_k \overset{k=1,\cdots,n_2}{\mapsto} f_k(z_i) \\ \text{使得} f_k(a_i)=0}}{\xrightarrow{\varphi_1}} \overset{\substack{R \\ \|}}{k[z_1, \cdots, z_n]} \underset{z_i \mapsto a_i}{\xrightarrow{\varphi_0}} \overset{\substack{z_i \cdot a_j = a_i \cdot a_j \\ \mathbb{C}[a_1, \cdots, a_n] \\ \|}}{A^G} \to 0$$

定义 6.3.4

$R-$ 模 $\mathrm{Im}\varphi_k$, 称为 A^G **的** k **阶 syzygy 模**.

定理 6.3.5

对 $\forall k, k$ 阶 syzygy 模有限生成.

$\mathrm{Im}\varphi_1$ 是 Noether 模 R(Hilbert 基定理) 的子模.
$\Longrightarrow \mathrm{Im}\varphi_1$ 有限生成 $\Longrightarrow R^{n_1}$ 是有限生成 (n_1 有限)$\Longrightarrow R_{n_1}$ 是 Noether 模 $\Longrightarrow$ 子模 $\mathrm{Im}\varphi_2$ 有限生成 $\Longrightarrow R^{n_2}$ 是 Noether 模 (n_2 有限)$\cdots \Longrightarrow R^{n_{k-1}}$ 是 Noether 模 $\Longrightarrow \mathrm{Im}\varphi_k$ 有限生成.

命题 6.3.1

对 $\forall A^G$, 正合列长度有限?$\rightsquigarrow$Hilbert Syzygy 定理.

6.4 Hilbert Syzygy 定理

定义 6.4.1: 自由消解

设 M 是 $R-$ 模, F_i 是自由 R 模正合列,

$$g \overset{\text{def}}{=} \cdots \to F_n \xrightarrow{\varphi_n} \cdots F_1 \xrightarrow{\varphi_1} F_0 \to M \to 0$$

称为模 M 的一个自由消解.

模 $\mathrm{Im}\varphi_i$ 称为 M 的 i 阶 **syzygy 模**.

$F_1 \to F_0 \to M \to 0$ 称为模 M 的一个**表现** (presentation).

若 $F_{n+1} = 0$ 且 $F_i \neq 0, 1 \leq i \leq n$, 称自由消解的**长度**为 n.

例 6.4.1

设 M 是有限生成 $R-$ 模, 生成元 $(m_1, \cdots, m_s)$, 1 阶 syzygy 模为 $\{(a_1, \cdots, a_s) \in R^s : a_1 m_1 + \cdots + a_s m_s = 0\} \subset R^s, M = R = \mathbb{Q}[x, y], I = (xy, x^2), \mathrm{Syz}(xy, x^2) = (x, y) \in R^2$.

$$0 \to R \underset{b_1 \mapsto y a_1 + x a_2}{\longrightarrow} R^2 \underset{\substack{a_1 \mapsto x^2 \\ a_2 \mapsto xy}}{\longrightarrow} I \to 0$$

注解 6.2

对有限消解 $0 \to F_n \xrightarrow{\varphi_n} F_{n-1} \xrightarrow{\varphi_{n-1}} F_{n-2} \to \cdots \to F_0 \to M \to 0$, $\ker \varphi_{n-1} = \mathrm{Im} \varphi_n \cong F_n$ 是自由模.

定理 6.4.2: Hilbert Syzygy 定理

设 $R = \mathbb{F}[x_1, \cdots, x_n]$, 则有限生成的 $R-$ 模 M, 存在长度 $\leq n$ 的自由消解.

推论 6.4.3

不变子环 S^G 存在自由消解, 长度 $\leq$syzygy 生成元个数 $\longrightarrow$ 命题6.3.1.

作业 6.1

找不变子环 S^G 自由消解的具体例子.

Chapter 7

Hilbert Syzygy 定理, 自由模的 Gröbner 基, Hilbert 多项式定理

7.1 Hilbert Syzygy 定理与 Gröbner 基

定义 7.1.1: Gröbner 基

多项式环 $\mathbb{F}[x_1, \cdots, x_n], <$ (单项式序), 对 $\forall$ 理想 I, $\exists G = \{f_1, \cdots, f_m\}$ 满足, $I = (f_1, \cdots, f_m), \mathrm{LT} I = (\mathrm{LT} f_1, \cdots, \mathrm{LT} f_m)$, 称 G 是 I 的 Gröbner 基.

性质 7.1.2

对 $\forall f \in \mathbb{F}[x_1, \cdots, x_n]$, f 对 Gröbner 基 G 做带余除法, 余式 r 与 G 中次序选取无关.

定义 7.1.3: 约化的 Gröbner 基

若 I 的 Gröbner 基 G 满足:

1. $\forall p \in G$ 是首 1 多项式.
2. $\forall p \in G$, p 中任意单项式都不在 $(\mathrm{LT}(G\ \{p\}))$ 中, 则称 G 是约化的 Gröbner 基.

定理 7.1.4

I 的约化的 Gröbner 基是唯一的.

例 7.1.1

$\mathbb{F}[x,y], <$: 次数字典序, $I=(f_1,f_2), f_1=x^3-2xy, f_2=x^2y-2y^2+x$. 由 Buchberger 算法得, $f_3=x^2\boxed{+axy}, f_4=xy, f_5=y^2-\frac{1}{2}x$, 都是极小 Gröbner 基, 而 f_1,f_2,x^2,f^4,f_5 是约化 Gröbner 基.

注解 7.1

子模 $\longleftrightarrow$ **理想**.

7.2 自由模上的 Gröbner 基

定义 7.2.1

我们考虑多项式环 $R=\mathbb{F}[x_1,\cdots,x_n]$ 上的自由模 $R^s, s\in\mathbb{N}^*$, 设 $(e_1,\cdots,e_s)$ 是 R^s 的基底;

R^s **的中的多项式**定义为: $m=cx^\alpha e_i, c\in\mathbb{F}, \alpha\in\mathbb{Z}^s, x^\alpha$ 是 R 中首 1 多项式.

$$m_1=c_1x^\alpha e_i, m_2=c_2x^\beta e_j, \underset{\text{最小公倍式}}{\mathrm{LCM}}(m_1,m_2)\overset{\text{def}}{=}\begin{cases}0, i\neq j\\ \mathrm{LCM}(\underset{R\text{中单项式}}{\underset{\uparrow}{x^\alpha}}, x^\beta)e_i, i=j\end{cases}.$$

定理 7.2.2

$M\subset R^q$ 是由 R^q 上单项式 $\{m_1,\cdots,m_s\}$ 生成的子模, 设 $e_1,\cdots,e_s$ 是 R^s 的基底, 令 $m_{i,j}=\mathrm{LCM}(m_i,m_j)$, 则 M 的 (1 阶)syzygy 模: $\mathrm{Syz}(m_1e_1+\cdots+m_se_s)\overset{\text{def}}{=}\{a_1e_1+\cdots+a_se_s: a_1m_1+\cdots+a_sm_s=0\}\subset R^s$. 由 $\{\sigma_{i,j}=\frac{m_{i,j}}{m_i}e_i-\frac{m_{i,j}}{m_j}e_j, 1\leq i<j\leq s\}$ 生成, 其中 $m_{i,j}=\mathrm{LCM}(m_i,m_j)$, 且令 $\frac{e_k}{e_k}=1$.

定义 7.2.3: R^t 上的单项式序

定义同 R 上单项式序, 令 $>$ 是 R 上单项式序.

例 7.2.1

$>_{TOP}$: $x^\alpha e_i >_{TOP} \overset{\text{def}}{\Longleftrightarrow} x^\alpha > x^\beta$, 或 $\alpha=\beta$ 且 $i<j$.

$>_{POT}$: $x^\alpha e_i >_{POT} \overset{\text{def}}{\Longleftrightarrow} i<j$ 或 $i=j$ 且 $x^\alpha > x^\beta$.

定义 7.2.4: Gröbner 基

有限集 $\{g_1,\cdots,g_s\}\subset M\subset R^t$ 称为 $(M,>)$ 的 Gröbner 基, 若 $(\mathrm{LT}(M)) = (\mathrm{LT}(g_1),\cdots,\mathrm{LT}(g_s))$. 若 Gröbner 基 $G=\{g_1,\cdots,g_s\}$ 满足

1. g_i 是首 1 多项式.
2. g_i 中任意单项式都不在 $(\mathrm{LT}(G\backslash\{g_i\}))$ 中, 则称 G 为约化的 Gröbner 基.

定理 7.2.5

$(M\subset R^t,>)$ 存在 Gröbner 基且约化 Gröbner 基唯一.

结论 7.2.6: Buchberger 算法

$(R^t. \ >), f,g\in R^t$, $S-$ 向量: $S(f,g)=\dfrac{m}{\mathrm{LT}(f)}f-\dfrac{m}{\mathrm{LT}(g)}g$, 其中, $m=\mathrm{LCM}(\mathrm{LT}(f),\mathrm{LT}(g))$.

定理 7.2.7

1. $G=\{g_1,\cdots,g_s\}\subset R^t$ 是 Gröbner 基 $\Longleftrightarrow$ $S(g_i,g_j)$ 对 G 做带余除法的余式为 0, $\forall 1\le i,j\le s$.

2. G 可以依下列算法扩充为 Gröbner 基.

起始:$G=\{g_1,\cdots,g_n\}\subset R^t, C\overset{\text{def}}{=}\{(g_i,g_j)|1\le i,j\le n\}$

运行: 任取$(g_i,g_j)\in C$, 检测$S(g_i,g_j)$对G 做带余除法的余数r

$r\overset{\text{def}}{=}\overline{S(g_i,g_j)}^{G}$ $\begin{cases} r=0, G=G, C=C\backslash\{(g_i,g_j)\} \\ r\ne 0, G=G\cup\{r\}, C=C\cup\{(g_i,r)\}\backslash\{(g_i,g_j)\}\end{cases}$

终止: $C=\varnothing$, 此时的 G 为 I 生成元扩充的 Gröbner 基.

例 7.2.2

$M\subset R^3, R=\mathbb{R}[x_1,x_2,x_3,x_4], >$ 是 R^3 上 TOP 次数字典序.

设 M 是由 $\underset{=g_1}{\begin{pmatrix} x_1+x_2 \\ x_3 \\ \boxed{x_1x_3}-x_4\end{pmatrix}}, \underset{=g_2}{\begin{pmatrix} \boxed{x_1x_2x_3}-x_4 \\ x_2x_3 \\ x_1x_4\end{pmatrix}}, \underset{=g_3}{\begin{pmatrix} \boxed{x_1^2} \\ x_2^2 \\ x_3^2-x_4\end{pmatrix}}\in R^3$ 生成的子模,

则 $\{g_1,g_2,g_3,g_4\}$ 是 M 的约化 Gröbner 基, $g_4=\begin{pmatrix} x_1x_4^2 \\ \boxed{x_2^3x_3}-x_1x_2x_3 \\ x_2x_3^3-x_1^2x_4-x_2x_3x_4\end{pmatrix}$.

定理 7.2.8: Hilbert Syzygy 定理

设 $R=\mathbb{F}[x_1,\cdots,x_n]$, 则有限生成的 $R-$ 模 M 存在长度 $\le n$ 的自由消解.

$$0\to F_n\xrightarrow{\varphi_n}F_{n-1}\xrightarrow{\varphi_{n-1}}\cdots F_1\xrightarrow{\varphi_1}F_0\xrightarrow{\varphi_0}M\to 0$$

注解 7.2

任意有 n 个生成元的有限生成 $\mathbb{F}-$ 代数都是有限生成 $R-$ 模. $x_i\cdot g_j\overset{\text{def}}{=}g_ig_j(g_i,g_j$生成元).

思路:

1. i 阶 Syzygy 模 Gröbner 基 $\underset{\text{诱导}}{\rightsquigarrow}$ $i+1$ 阶 syzygy 模的 Gröbner 基.

考虑 M 的表现 $\underset{s\text{表现生成元关系}}{\underset{\downarrow}{R^s}} \xrightarrow{\varphi_1} \underset{t\text{表现生成元个数}}{\underset{\downarrow}{R^t}} \xrightarrow{\varphi_0} M \to 0$, $\mathrm{Im}\varphi_1 = \ker\varphi_0$ 有限生成 (R^t 为 Noether 模), 设 $>$ 是 R^t 上的 TOP 字典序. 令 $(\mathrm{Im}\varphi_1, >)$ 的 Gröbner 基为 $G = \{g_1, \cdots, g_r\}$, 则 $(R^t, >)$ 在 R^s 上诱导了 "换元序"$>_1$: $x^\alpha e_i \overset{\text{(单项式序)}}{\overset{\uparrow}{>_1}} x^\beta e_j \overset{\text{def}}{\Longleftrightarrow}$ $\mathrm{LT}_>(x^\alpha \underset{\text{换元}}{g_i}) > \mathrm{LT}_>(x^\beta \underset{\text{换元}}{g_j})$.

将 $S(g_i, g_j)$ 展开, $S(g_i, g_j) = \sum_{k=1}^{s} a_{ijk}\boxed{g_k}, a_{ijk} \in R$, 令 $m_{i,j} \overset{\text{def}}{=} \mathrm{LCM}(\mathrm{LT}(g_i), \mathrm{LT}(g_j)).a_{i,j} = \sum_{k=1}^{s} a_{ijk}\boxed{e_k} \in R^s$ 及 $S_{i,j} = \frac{m_{i,j}}{\mathrm{LT}(g_i)}e_i - \frac{m_{i,j}}{\mathrm{LT}(g_j)}e_j - a_{i,j} \in R^s$, 则 $\{S_{i,j} : S_{i,j} \neq 0\}$ 是 M 的 2 阶 syzygy 模在 $>_1$ 的 Gröbner 基 **(Schreger 定理)**.

高阶 Gröbner 基中出现的不定元越来越少.

$$\text{不妨设 } \mathrm{LT}\underset{\{g_i\}\text{重排}}{\underset{\downarrow}{g_i}} = c_i x_m^a y_i e_k, \mathrm{LT}g_j = c_j x_m^b y_j e_k$$

其中 $c_i \in R, x_m$ 是字典序最高项, y_i, y_j 是字典序低阶项, $i < j$ 且 $a > b$.$\star$

则 $\mathrm{LT}(S_{i,j}) = \frac{m_{i,j}}{\mathrm{LT}(S_{i,j})}e_i = c_{i,j}\frac{\boxed{x_m^a}\mathrm{LCM}(y_i, y_j)}{\boxed{x_m^a}y_i}e_i = c_{ij}\frac{\mathrm{LCM}(y_i, y_j)}{y_i}e_i \Longrightarrow x_m$ 不再出现 $\Longrightarrow$ 每做一步消解, Gröbner 基中 $\mathrm{LT}(S_{i,j})$ 少一个不定元 x_k, 进而 $\exists$ 长度 $r \leq n$ 的自由消解 $0 \to \underset{\leq n-r}{R^{S_r}} \xrightarrow{\varphi_r} R^{S_{r-1}} \cdots \underset{\leq n-1\text{个}}{R^{S_1}} \xrightarrow{\varphi_1} \underset{n\text{个}}{R^t} \to M \to 0$.

定义 7.2.9: 分次环

环 R 称为分次环, 如果 $R = R_0 \oplus R_1 \oplus R_2 \cdots$ (群直和), 使得 $R_i \cdot R_j \subset R_{i+j}, \forall i, j \geq 0$.

例 7.2.3

$\mathbb{F}[x_1, \cdots, x_n] = \bigoplus_{\deg} \underset{\deg = k}{\mathbb{F}[x_1, \cdots, x_n]}$ 是分次环.

定义 7.2.10: 分次模

设 $R=\bigoplus\limits_{n=0} R_n$ 是分次环, $R-$ 模 M 若满足

1. $M=\bigoplus\limits_{k\in I} M_k$(交换群)
2. $R_nM_k\subset M_{n+k}$

则称 M 是分次模.

定义 7.2.11: 分次模的平移

$M(d)_e \overset{\text{def}}{=} M_{d+e} \longrightarrow M(d)\cong M.$

7.3 分次自由消解

定义 7.3.1: $R-$ 模分次同态

设 $R=\bigoplus\limits_{n=v}^{\infty} R_n$ 为分次环, $M=\bigoplus\limits_{-\infty}^{+\infty} M_m, N=\bigoplus\limits_{-\infty}^{+\infty} N_m$ 为分次 $R-$ 模. 若 $M\to N$ 的同态 f 满足 $\forall n\in\mathbb{N}^*, f(M_n)\subset N_n$, 则称 f 是 $R-$ 模分次同态.

定义 7.3.2: 分次自由消解

设 R 是分次环, $\mathcal{F}:\cdots F_n\xrightarrow{\varphi_n}\cdots F_1\xrightarrow{\varphi_1}F_0\to M\to 0$ 是 $R-$ 模 M 的自由消解, 若每个 F_i 是分次 $R-$ 模且 φ_k 都是 $R-$ 模分次同态, 则称 $\mathcal{F}$ 为分次自由消解.

定理 7.3.3: Hilbert Syzygy 定理 (分次)

设 $R=\mathbb{F}[x_1,\cdots,x_n]$, 有限生成的分次 $R-$ 模都存在长度有限 $(\leq n)$ 的分次自由消解, 且任意 F_i 都是有限生成的.

$\Longrightarrow$Hilbert 多项式定理: 分次模的维数增长规律.

定义 7.3.4

设 $R=\mathbb{F}[x_1,\cdots,x_n]$, M 是有限生成的分次 $R-$ 模, $M=\bigoplus\limits_{-\infty}^{+\infty}M_s, H_M(s)=\dim_{\mathbb{F}}M_s$(将 M_s 看成向量 $\mathbb{F}-$ 向量空间) 称为 M 的 Hilbert 函数.

注解 7.3

$\dim_{\mathbb{F}}M_s$ 必有限, 否则子模 $\bigoplus\limits_{s}^{\infty}M_s$ 不是有限生成, 与 M 是 Noether 模矛盾.

定理 7.3.5: Hilbert 多项式定理

设 M 是有限生成的分次 $R-$ 模, $R=\mathbb{F}[x_1,\cdots,x_n]$, 则存在 $r\in\mathbb{Z}$, 使得 Hilbert 函数 $\underset{\dim_{\mathbb{F}}M_s}{\underset{\downarrow}{H_M(s)}}, s\geq r$, 恰为次数 $\leq n$ 的多项式, 该多项式称为 Hilbert 多项式.

7.4 多项式环的 Hilbert 多项式

性质 7.4.1

$\mathbb{F}$: 向量空间, $M=R=\mathbb{F}[x_1,\cdots,x_n], R=\bigoplus\limits_{i=0}^{\infty}R_i, R_i$ 为 i 阶齐次多项式构成的

$$H_M(s)=\dim_{\mathbb{F}}R_s\underset{\downarrow}{=}C_{n+s-1}^{s-1}$$

$$\begin{aligned}
\text{计数}\longleftarrow&\#\{x_1^{k_1}x_2^{k_2}\cdots x_n^{k_n}:k_i\geq 0,\sum k_i=s\}\\
=&\#\{x_1^{k_1}\cdots x_n^{k_n}:k_i\geq 1,\sum k_i=n+s\}\\
=&\#\{\cdots|\cdots|\cdots:s+n\text{个点分为}n\text{组}\}=\overset{\text{组合多项式}}{\overset{\uparrow}{C_{n+s-1}^{n-1}}}=C_{n+s-1}^{s}
\end{aligned}$$

推论 7.4.2

$H_{M(d)}(s)\overset{\text{def}}{=}H_M(s+d)=C_{s+d+n-1}^{n-1}=C_{n+s+d-1}^{s+d}.$

Chapter 8

Hilbert 多项式定理, Poincaré 级数

8.1 Hilbert 多项式定理

注解 8.1: Hilbert 多项式定理证明

M 存在有限的分次自由消解

$$\mathcal{F}: 0 \to F_n \xrightarrow{\varphi_n} \cdots \xrightarrow{\varphi_1} F_0 \xrightarrow{\varphi_0} M \to 0$$

由多项式环 Hilbert 多项式得, $H_{F_i}(s) = \dim(F_i)_s$ 为组合多项式且次数 $\leq n$.

$$\begin{aligned} H_M(s) &= \dim(F_i)_s - \dim(\ker\varphi_0) \\ &= \dim(F_0)_s - \dim(F_1)_s + \dim(\ker\varphi_1) \quad \boxed{\dim(\ker\varphi_n)_s = \dim(F_n)_s} \\ &= \cdots = \sum_{i=0}^{n}(-1)^i H_{F_i}(s) \end{aligned}$$

为次数 $\leq n$ 的多项式.

例 8.1.1

$R^G=\mathbb{C}[x^3,x^2y,xy^2,y^3]\subset\mathbb{C}[x,y], R=\mathbb{C}[z_0,z_1,z_2,z_3]$, 自由消解:

$$0\to R^2\underset{\begin{pmatrix}1,0\\0,1\end{pmatrix}\begin{pmatrix}b_1\\b_2\end{pmatrix}\mapsto\begin{pmatrix}z_0a_1+z_1a_2+z_2a_3\\z_1a_1+z_2a_2+z_3a_3\end{pmatrix}}{\to} R^3\underset{\begin{pmatrix}1,0,0\\0,1,0\\0,0,1\end{pmatrix}\begin{pmatrix}a_1\\a_2\\a_3\end{pmatrix}\mapsto\begin{pmatrix}z_2^2-z_1z_3\\z_0z_3-z_1z_2\\z_1^2-z_0z_2\end{pmatrix}}{\xrightarrow{\varphi_1}} R\underset{\begin{matrix}\begin{pmatrix}z_0\\z_1\\z_2\\z_3\end{pmatrix}\mapsto\begin{pmatrix}x^3\\x^2y\\xy^2\\y^3\end{pmatrix}\\ \begin{pmatrix}\overset{\longleftrightarrow}{\downarrow} & 1\mapsto 1\\ \text{模同态} & z_0\cdot 1\mapsto z_0=x^3\end{pmatrix}\end{matrix}}{\to} R^G\to 0$$

分次消解:

$$0\to R^2(\overset{\nearrow}{-3})\underset{\begin{matrix}\begin{pmatrix}z_0,z_1,z_2\\z_1,z_2,z_3\end{pmatrix}\\(1,0)\leftarrow b_1\mapsto(z_0,z_1,z_2)\\(0,1)\leftarrow b_2\mapsto(z_1,z_2,z_3)z_1a_1+z_2a_2+z_3a_3\end{matrix}}{\overset{\begin{matrix}\text{分次模}M\\\text{有}n\text{次元}\\\text{在}M(d)\text{中}\\\text{变为}n-d\text{次元}\end{matrix}}{\to}} R^3(\overset{\nwarrow}{-2})\underset{\begin{matrix}\begin{pmatrix}z_2^2-z_1z_3\\z_0z_3-z_1z_2\\z_1^2-z_0z_2\end{pmatrix}\\(1,0,0)\leftarrow a_1\mapsto z_2^2-z_1z_3\\(0,1,0)\leftarrow a_2\mapsto z_0z_3-z_1z_2\\(0,0,1)\leftarrow a_3\mapsto z_1^2-z_0z_2\end{matrix}}{\to} R\underset{\substack{(1)\\1\mapsto 1}}{\to} R^G\to 0$$

R^G 的 Hilbert 多项式为 $H_{R^G}(s)=H_R(s)-3H_{R(-2)}(s)+2H_{R(-3)}(s)\overset{n=4}{\equiv}C_{s+3}^3-3C_{s+1}^3+2C_s^3=3s+1,s\geq 0$.

8.2 Hilbert 多项式性质

性质 8.2.1: 整性

Hilbert 多项式 $\subset$ 整值多项式 $(f(n)\in\mathbb{Z})\supsetneqq$ 整系数多项式, 任意整值一元多项式是组合多项式 $C_n^0,C_n^1,C_n^2,\cdots$ 的 $\mathbb{Z}-$ 线性组合.

$$\begin{matrix}C_n^0 & C_n^1 & C_n^2 & C_n^3 & \cdots & & n=0\\ 1 & 0 & 0 & 0 & & & n=1\\ * & 1 & 0 & 0 & & \text{多项式中取} & n=2\\ * & * & 1 & 0 & & & n=3\\ * & * & * & 1 & & & \cdots\end{matrix}.$$

设 f 是 k 此整值一元多项式, 用下面逼近方法:

$$\begin{array}{ll}
f(0) = m_0 \Longrightarrow m_0 C_n^0 + \overset{\text{尾项}}{\underset{\uparrow}{0}} & 0\text{次} \\
f(1) = m_1 \Longrightarrow m_0 C_n^0 + m_1 C_n^1 + 0 & 1\text{次} \\
\vdots & \\
f(k) = m_k \Longrightarrow m_0 C_n^0 + \cdots + m_k C_n^k + 0 & k\text{次}
\end{array}$$

$\Longrightarrow f(n) = m_0 C_n^0 + \cdots + m_k C_n^k$.

性质 8.2.2: 短正合列可加性

对于 $\mathbb{F}[x_1, \cdots, x_n]-$ 分次模同态的短正合列

$$0 \to A \to B \to C \to 0$$

有 $H_A(s) + H_C(s) = H_B(s)$.

$\dim_{\mathbb{F}} A_s + \dim_{\mathbb{F}} C_s = \dim_{\mathbb{F}} B_s \Longrightarrow H_A(s) + H_C(s) = H_B(s)$.

定义 8.2.3: Poincaré 级数

$P(M,t) \overset{\text{def}}{=} \sum\limits_{n\geq 0}^{\infty} \dim_{\mathbb{F}} M_s t^s$(与模的分次有关).

例 8.2.1

$M = \mathbb{F}[x_1, \cdots, x_n], P = (M,t) = \sum\limits_{s=0}^{\infty} C_{n+s-1}^s t^s = \left(\sum\limits_{s=0}^{\infty} t^s\right)^n = \left(\frac{1}{1-t}\right)^n = \frac{1}{(1-t)^n}$.

例 8.2.2

$M = \mathbb{C}[x^3, x^2y, xy^2, y^3] \subset \mathbb{C}[x,y], P(M,t) = \sum\limits_{s=0}^{\infty} (3s+1)t^s = \sum\limits_{s=0}^{\infty} t^s + 3t \sum\limits_{s=0}^{\infty} st^{s-1} =$

$$\frac{1}{1-t}+\frac{3t}{(1-t)^2}=\frac{2t+1}{(1-t)^2}.$$

注解 8.2

对于 $\mathbb{F}[x_1,\cdots,x_n]-$ 模 (不一定分次) 有时也可以看成分次 $\mathbb{F}-$ 模 (向量空间) 来推广 Poincaré 级数的定义.

定义 8.2.4

设 $M=\mathbb{F}[h_1,\cdots,h_k]\subset\mathbb{F}[x_1,\cdots,x_n], h_i$ 齐次多项式 (按多项式次数分次是分次 $\mathbb{F}-$ 向量空间), 可以定义 Poincaré 级数 $P(M,t)=\sum\limits_{-\infty}^{\infty}\dim_{\mathbb{F}}M_{(d)}t^d$.

作业 8.1

求证:

1. $\mathbb{C}[x^3,y^3,xy]$ 的 Poincaré 级数是 $\dfrac{1+t^2+t^4}{(1-t^3)^2}$.
2. Poincaré 级数对分次模同态短正合列具有可加性, 即对 $0\to M_A\to M_B\to M_C\to 0$, 有 $P(M_A,t)+P(M_C,t)=P(M_B,t)$.

定理 8.2.5: Hilbert Serre 定理

$M=\mathbb{F}[h_1,\cdots,h_n]\subset\mathbb{F}[x_1,\cdots,x_m], m_i$ 是齐次多项式, Poincaré 级数 $P(t)$ 是 t 的有理函数, $P(t)=\dfrac{f(t)}{(1-t^{k_1})(1-t^{k_2})\cdots(1-t^{k_n})}$, 其中 $k_1,\cdots,k_n$ 是 $x_1,\cdots,x_n$ 在 R 中的次数 (不一定为 1).

对 n 归纳.

1. $n=0$, M 是 $\mathbb{F}-$ 向量空间, $M_n=0, n>\dim M$, $P(t)$ 是多项式.
2. 不定元个数 $\le n-1$ 成立, 令 $\mathcal{M}:M\to M, m\mapsto x_n\cdot m$, 考虑正合列

$$0\to\ker\mu\to M\to\mu/\ker\mu\to 0$$

及

$$0 \to \mathrm{Im}\mu \to M \to \mu/\mathrm{Im}\mu \to 0$$

由 Hilbert 多项式可加性得

$$\left.\begin{aligned} P(M,t) &= P(\ker\mu,t) + P(\mu/\ker\mu,t) \\ P(M,t) &= P(\mathrm{Im}\mu,t) + P(M/\mathrm{Im}\mu,t) \end{aligned}\right\} \text{联立}$$

由 $M/\ker(M) \cong \mathrm{Im}\mu$ 得 $(M/\ker\mu)_{(i)} \cong (\mathrm{Im}\mu)_{i+k_n} \implies P(M/\ker\mu,t) = t^{-k_n}P(\mathrm{Im}\mu,t)$.

因此 $\begin{cases} P(M,t) = P(\ker\mu,t) + t^{-k_n}P(\mathrm{Im}\mu,t) \\ P(M,t) = P(\mathrm{Im}\mu,t) + P(M/\mathrm{Im}\mu,t) \end{cases} \implies P(M,t) = \dfrac{-t^{k_n}}{1-t^{k_n}}P(\ker\mu,t) + \dfrac{1}{1-t^{k_n}}P(M/\mathrm{Im}\mu,t)$, 又由定义, $x_n \in \mathrm{Ann}(\ker\mu)$ 且 $x_n \in \mathrm{Ann}(M/\mathrm{Im}\mu)$, 故 $\ker\mu$ 和 $M/\mathrm{Im}\mu$ 是 $\mathbb{F}[x_1,\cdots,x_n]-$ 模, 由归纳假设, 定理成立.

8.3 不变量理论中的 Poincaré 级数

定理 8.3.1: Molien 定理

G : 有限群, $R = \mathbb{F}[x_1,\cdots,x_n], \rho : G \hookrightarrow GL(n,\mathbb{F}), R^G$: 不变子环.

R^G 的 Poincaré 级数为 $P(R^G,t) = \dfrac{1}{|G|}\displaystyle\sum_{g\in G}\dfrac{1}{\det(I-\rho(g)^{-1}t)}$.

注解 8.3

1. P 中 $M_{(n)}t^n$ 的 n 定义为齐次多项式次数.
2. Poincaré 级数由表示的特征多项式确定.

注解 8.4

$$P(R^G,t) = \frac{1}{|G|}\sum_{g\in G}\frac{1}{\det(I-\rho(g)^{-1}t)} = \frac{1}{|G|}\sum_{g\in G}\frac{\det(-\rho(g))}{\underbrace{\det(tI-\rho(g))}_{\text{特征多项式}}}.$$

例 8.3.1

$\mathbb{Z}/3\mathbb{Z} \to \mathbb{C}[x,y], 1\cdot(x,y) \stackrel{\text{def}}{=} (\omega x, \omega y). \omega = e^{\frac{2}{3}\pi i}$, 表示: $0 \mapsto I, 1 \mapsto \begin{pmatrix} \omega & \\ & \omega \end{pmatrix}, 2 \mapsto \begin{pmatrix} \omega^2 & \\ & \omega^2 \end{pmatrix}, R^G = \mathbb{C}[x^3, x^2y, xy^2, y^3]$. 由 Molien 定理, Poincaré 级数为 $\frac{1}{3}\left(\frac{1}{(1-t)^2} + \frac{1}{(1-\omega t)^2} + \frac{1}{(1-\omega^2 t)^2}\right) = \frac{2t^3+1}{(1-t^3)^2}$.

vs $\frac{2t+1}{(1-t)^2}, t \longleftrightarrow t^3$, 原因: 分次的定义不同.

推论 8.3.2

R^G 的 Poincaré 级数在 $t=1$ 处的奇点阶数为 n.

8.4 同调代数简介

注解 8.5

自由消解 $\rightsquigarrow$Tor 平衡函子.

命题 8.4.1: 问题引入

模张量积是否保持短正合列? $\rightsquigarrow$ 平坦模, Tor;

即若 $0 \to A \to B \to C \to 0$ 是 $R-$ 模正合列, M 是 $R-$ 模, $0 \to A\otimes M \to B \otimes M \to C \otimes M \to 0$ 是不是正合列?

8.4.1 模张量积

例 8.4.1

对于多项式 $R[x], R[y], R$ 是环,

$$R[x] \underset{\downarrow}{\oplus} R[y] \neq R[x,y], \text{基底:} R[x] \overset{\text{以}R\text{为系}\overset{\uparrow}{\text{数}}\longrightarrow\text{基底}}{\otimes_R} R[y]$$

$$\begin{array}{c} \text{基底}\{x^i, y^j, i,j \geq 0\} \\ \{x^i\} \cup \{y^j\} \neq \{x^i\}\cdot\{y^j\} \end{array} \rightsquigarrow \underset{\substack{(\text{基底乘积/笛卡尔积}) \\ \downarrow\text{直观}}}{\text{张量积}} = \mathrm{Span}_R\{x^i y^j, i,j \geq 0\}$$

注解 8.6: 动机

将双线性映射线性化(**将两个 $R-$ 模乘积上的双线性映射用一个 $R-$ 模的线性映射替代**), $M,N:R-$ 模, 对 $\forall$ 双线性映射 $M\times N\to P$, 使得存在唯一的线性映射满足

图表
$$\begin{tikzcd}
M\times N \arrow[r, "\text{定义}", "\text{双线性}"'] \arrow[dr, "\text{双线性}"'] & M\otimes_R N \arrow[d, "\text{线性}"] \\
 & P
\end{tikzcd}$$
可交换 (泛性质).

Chapter 9

同调代数简介 (张量积, 平坦模与 Tor)

9.1 张量

注解 9.1: 构造

"两要素": 生成元 +"关系".

定义 9.1.1

$M \otimes_R N$ 定义为:

1. 生成元 $\overset{\mathcal{B}_M \times \mathcal{B}_N(\text{基的笛卡尔积})\boxtimes M\times N}{\overset{\downarrow}{\{(m_i, n_j)\}}}$, $\{m_i\}_{i\in I}$ 为 M 生成元, $\{n_j\}_{j\in J}$ 为 N 生成元, 生成自由模 $C(\cong R^{I\times J})$.

2. "关系"$\longleftrightarrow$ 商掉的子模.(定义)$\star$

定义 9.1.2: 双线性关系

$$\begin{array}{lcl} r(m\otimes n) = (rm)\otimes n & \longleftrightarrow & \boxed{\begin{array}{l} r(m,n)-(rm,n) \\ r(m,n)-(m,rn) \\ (m_1+m_2,n)-(m_1,n)-(m_2,n) \\ (m,n_1+n_2)-(m,n_1)-(m,n_2) \end{array}} \\ r(m\otimes n) = m\otimes(rn) & \longleftrightarrow & \\ m\otimes(n_1+n_2) = m\otimes n_1 + m\otimes n_2 & \longleftrightarrow & \\ (m_1+m_2)\otimes n = m_1\otimes n + m_2\otimes n & \longleftrightarrow & \end{array} \quad \begin{array}{c}\text{生}\\\text{成}\\\text{子}\\\text{模}\\ D \\ \cap \\ R^{I\times J}\end{array}$$

$M \otimes_R N \overset{\text{def}}{=} C/D, (m,n)$ 在 C/D 中像记为 $m\otimes n$.

$$\begin{array}{ccccccccc} 0\to & \ker\varphi & \to & R^{I\times J} & \xrightarrow{\varphi} & M\otimes_R N & \to & 0 \\ & \overset{\text{def}\|}{D} & & \begin{pmatrix} 0 & 0 & \cdots \\ & 1\to(i,j) & \\ 0 & 0 & \cdots \end{pmatrix} & \overset{\text{def}}{\mapsto} & m_i\otimes n_j & \cong & (m_i,n_j)\in \mathcal{B}_M\times\mathcal{B}_N \end{array}$$

9.1.1 张量的性质与计算

性质 9.1.3

$(M_1 \oplus M_2)\otimes_R N \cong M_1\otimes_R N \oplus M_2 \otimes_R N$.

基底 $(\overline{\{\alpha_i, \beta_j\}, \gamma_k}), \{(\overline{\alpha_i,\gamma_k})\cup(\overline{\beta_j,\gamma_k})\} = \{(\overline{\alpha_i,\gamma_k}), (\overline{\beta_j,\gamma_k})\}$.

$(M_1\oplus M_2)\times N \to A$ 的双线性映射 (φ_1,φ_2) 与 $M_1\times N \xrightarrow{\varphi_1} A, M_2\times N \xrightarrow{\varphi_2} A$ 的一堆双线性映射 $1-1$ 对应.

性质 9.1.4

$R \otimes_R M \cong M$.

(基底 $\{\overline{(1, \alpha_i)}\}$, 基底 $\overline{\alpha_i}$.)

$R \times M \xrightarrow{\varphi} A$ 的双线性映射与 $M \to A$ 的双线性映射 $1-1$ 对应.($\varphi_r, \forall$ 给定 $r \in R$.)

例 9.1.1

k 是域, $k^m \otimes_R k^n \cong k^{mn}$, 由性质9.1.3, 性质9.1.4得 $k^m \otimes_R k^n = (\underbrace{k \oplus \cdots \oplus k}_{m\text{个}}) \otimes_R k^n = \underbrace{k^n \oplus k^n \cdots \oplus k^n}_{m\text{个}} = k^{mn}$.

例 9.1.2

$\mathbb{Z}/m\mathbb{Z} \otimes_R \mathbb{Z}/n\mathbb{Z} = 0, \gcd(m, n) = 1$.

基底 $(1, 1)$, 由 $\gcd(m, n) = 1$, $\exists k, r, km + rn = 1, (1, 1) = (km + rn, 1) = (rn, 1) = (r, n) = 0$.

作业 9.1

R 是环, I, J 是 $R-$ 理想. 求证:

$R/I \otimes_R R/J = R/(I, J)$ $\Longrightarrow \mathbb{Z}/m\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/\gcd(m, n)\mathbb{Z}$

作业 9.2

求证:

$R/I \otimes_R M = M/IM$

性质 9.1.5: $\otimes$ 与 $\varinjlim$ 可换

正向极限: direct limit,$\varinjlim$.

$A_1 \xrightarrow{f_{12}} A_2 \xrightarrow{f_{23}} A_3 \xrightarrow{f_{34}} \cdots$ 是 $R-$ 同态序列, 使得 $f_{ij} = f_{ik} \circ f_{kj}, \forall i < k < j$,

$\varinjlim A_j = \bigsqcup_{\text{不交并} \subset A_1 \times A_2 \times A_3 \cdots} A_i / \sim, x_i \sim x_j \overset{\text{def}}{\Longleftrightarrow} \exists k \geq i$且$k \geq j, f_{ik}(x_i) = f_{jk}(x_j)$.

例 9.1.3

$\mathbb{Q} \times_{\mathbb{Z}} \mathbb{Q} = \mathbb{Q}$.

(基底: $\left(\frac{q_1}{p_1}, \frac{q_2}{p_2}\right) = \left(\frac{q_1}{p_1}, \frac{p_1 q_2}{p_1 p_2}\right) = \left(1, \frac{q_1 q_2}{p_1 p_2}\right)$.)

考虑: $\mathbb{Z} \xrightarrow{\times 2} \mathbb{Z} \xrightarrow{\times 3} \mathbb{Z} \xrightarrow{\times 4} \mathbb{Z} \cdots$

$$(\mathbb{Z}, 0, 0, \cdots) \underset{(n,\cdots) \mapsto (0,2n,\cdots)}{\xrightarrow{\times 2}} (0, \mathbb{Z}, 0, \cdots) \underset{(0,m,\cdots) \mapsto (0,0,3m,\cdots)}{\xrightarrow{\times 3}} (0, 0, \mathbb{Z}, \cdots) \cdots$$

$$\varinjlim\{\mathbb{Z}\} = \bigsqcup_k (0, \cdots, \underset{\text{第}k\text{个}}{\underset{\uparrow}{\mathbb{Z}}})/\sim \cong \mathbb{Z} \cup \frac{\mathbb{Z}}{2} \cup \frac{\mathbb{Z}}{3} \cdots = \mathbb{Q}$$

$$\mathbb{Q} \times_{\mathbb{Z}} \mathbb{Q} = (\varinjlim\{\mathbb{Z}\}) \otimes_{\mathbb{Z}} \mathbb{Q} = \varinjlim\{(\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Q})\} \underset{\downarrow}{=} \mathbb{Q}$$

$$\varinjlim \mathbb{Q} \xrightarrow{\times 2} \mathbb{Q} \xrightarrow{\times 3} \mathbb{Q} \to \cdots = \mathbb{Q} \cup \frac{\mathbb{Q}}{2} \cup \frac{\mathbb{Q}}{3} \cdots = \mathbb{Q}$$

例 9.1.4

$\mathbb{Q} \otimes_{\mathbb{Z}} (\mathbb{Z}/2\mathbb{Z})((r,1), \forall 0 \leq r \leq 1, (r,1)\left(\frac{2p}{2q}, 1\right) = \left(\frac{1}{2q}, 0\right) = (0,0))$.

$$\begin{aligned}
&\mathbb{Q} \otimes_{\mathbb{Z}} (\mathbb{Z}/2\mathbb{Z}) \\
=&\varinjlim(\mathbb{Z} \xrightarrow{\times 2} \mathbb{Z} \xrightarrow{\times 3} \cdots) \otimes_{\mathbb{Z}} (\mathbb{Z}/2\mathbb{Z}) \\
=&\varinjlim(\mathbb{Z} \otimes \mathbb{Z}/2\mathbb{Z} \xrightarrow{\times 2} \mathbb{Z} \otimes \mathbb{Z}/2\mathbb{Z} \xrightarrow{\times 3} \cdots) \\
=&\varinjlim(\mathbb{Z}/2\mathbb{Z} \xrightarrow{\times 0} \mathbb{Z}/2\mathbb{Z} \xrightarrow{\times 1} \cdots) \\
=&0
\end{aligned}$$

9.1.2 张量积, 正合列与 Hom 函子

性质 9.1.6

$0 \to A \xrightarrow{f_A} B \xrightarrow{f_B} \to C \to 0$ 是正合列, 则 $\twoheadrightarrow$ $M \otimes_R A \underset{m \otimes a \mapsto m \otimes f_A(a)}{\to} M \otimes_R B \underset{m \otimes b \mapsto m \otimes f_B(b)}{\to} M \otimes_R C \to 0$ 是正合列.

注解 9.2

R 是域, $B = A \oplus C$, 张量积保短正合列.

例 9.1.5: Universal counterexample ⋆

$R = \mathbb{Z} \otimes \mathbb{Z}/2\mathbb{Z}$,

$$0 \to \mathbb{Z} \xrightarrow{\times 2} \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \to 0$$

$$\underset{\substack{\| \\ \mathbb{Z}/2\mathbb{Z}}}{\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z}} \underset{\substack{n \mapsto 0 \\ \downarrow \\ \text{非单射} \\ \downarrow \\ \text{不保短正合列}}}{\to} \underset{\substack{\| \\ \mathbb{Z}/2\mathbb{Z}}}{\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z}} \to \mathbb{Z}/2\mathbb{Z} \otimes \mathbb{Z}/2\mathbb{Z} \to 0$$

定义 9.1.7: 平坦模

对短正合列 $0 \to A \to B \to C \to 0$, 若模 M 满足: $0 \to M \otimes A \to M \otimes B \to M \otimes C \to 0$ 是正合列, 则称 M 是平坦模.

例 9.1.6

$\mathbb{Z}\left[\frac{1}{2}\right] = \left\{\frac{m}{2^n}, m, n \in \mathbb{Z}\right\}$ 是平坦 $\mathbb{Z}-$ 模.

$\hom(A, B) \overset{\text{def}}{=} \{A \to B\text{上模同态}\}$ 构成 $R-$ 模, $(r\varphi)(a) \overset{\text{def}}{=} r(\varphi(a)) = \varphi(r(a))$.

性质 9.1.8

$\hom(M, \hom(B, X)) \cong \hom(M \otimes B, X)$.

性质 9.1.9

$0 \to A \to B \to C \to 0$ 是正合列, 则

$$0 \to \hom(M, A) \to \hom(M, B) \to \underset{\substack{\downarrow \\ \text{协变函子}}}{\hom(M, C)} \not\twoheadrightarrow 0$$

$$0 \not\twoheadleftarrow \hom(A, M) \leftarrow \hom(B, M) \leftarrow \underset{\substack{\downarrow \\ \text{反变函子}}}{\hom(C, M)} \leftarrow 0$$

例 9.1.7: Universal counterexample ⋆

$$R=\mathbb{Z}, 0\to\mathbb{Z}\xrightarrow{\times 2}\mathbb{Z}\to\mathbb{Z}/2\mathbb{Z}\to 0$$

$M=\mathbb{Z}/2\mathbb{Z}, \hom(\mathbb{Z}/2\mathbb{Z},\cdot)$:

$$0\to\underset{\substack{\| \\ 0 \\ 2\varphi(1)=0 \\ \varphi(1)=0}}{\hom(\mathbb{Z}/2\mathbb{Z},\mathbb{Z})}\to\underset{\substack{\| \\ 0}}{\hom(\mathbb{Z}/2\mathbb{Z},\mathbb{Z})}\ \underset{\substack{\downarrow \\ \text{不是满射}}}{\to}\ \underset{\substack{\| \\ \mathbb{Z}/2\mathbb{Z}}}{\hom(\mathbb{Z}/2\mathbb{Z},\mathbb{Z}/2\mathbb{Z})}$$

$\hom(\cdot,\mathbb{Z}/2\mathbb{Z})$:

$$\underset{\substack{\| \\ \mathbb{Z}/2\mathbb{Z}}}{\mathbb{Z},\mathbb{Z}/2\mathbb{Z}}\ \underset{\substack{\times 2 \\ \downarrow \\ \text{不是满射}}}{\longleftarrow}\ \underset{\substack{\| \\ \mathbb{Z}/2\mathbb{Z}}}{\mathbb{Z}/2\mathbb{Z},\mathbb{Z}/2\mathbb{Z}}\leftarrow\underset{\substack{\| \\ \mathbb{Z}/2\mathbb{Z}}}{\mathbb{Z}/2\mathbb{Z},\mathbb{Z}/2\mathbb{Z}}$$

定义 9.1.10: 投射模

$R-$ 模 P 称为投射模, 若对 $\forall R-$ 模满同态 $M\xrightarrow{\psi}N$, 都有 $\begin{array}{c}\hom(P,M)\to\hom(P,N)\\ (p\mapsto m)\mapsto(p\mapsto\psi(m))\end{array}$ 是满同态.

$\iff$ 对 $\forall$ 满同态 $\alpha: M\twoheadrightarrow N$ 和同态 $\beta: P\to N$, $\exists$ 同态 $\gamma: P\dashrightarrow M$, 使得 $\beta=\alpha\gamma$.

$$\begin{tikzcd} & P \arrow[dl, dashed, "\exists\gamma"'] \arrow[d, "\beta"] \\ M \arrow[r, two heads, "\alpha"'] & N \end{tikzcd}$$

定义 9.1.11: 投射消解

$\exists P_n\to\cdots P_2\to P_1\to P_0\to M\to 0$, 其中 P_i 是投射模.

定义 9.1.12: 入射模

$R-$ 模 Q 称为入射模, 若对 $\forall R-$ 模单同态 $M\hookrightarrow N$, 都有 $\begin{array}{c}\hom(M,Q)\leftarrow\hom(N,Q)\\ \psi^*(f)\hookleftarrow f\end{array}$ 是单同态, $\psi^*(f)(m)\overset{\text{def}}{=}f(\varphi(m))\iff$ 对 $\forall$ 单同态 $M\overset{\alpha}{\hookrightarrow}$ 和同态 $M\xrightarrow{\rho}Q$, 都 $\exists$ 同态 $\gamma: N\to Q$ 使得 $\rho=\rho\circ\alpha$.

定义 9.1.13: 入射消解

对 M, $\exists 0 \to M \to Q_0 \to Q_1 \to \cdots, Q_i$ 是内射模.

$$\begin{tikzcd} M \arrow[r, hook, "\alpha"'] \arrow[d, "\beta"'] & N \arrow[dl, dashed, "\gamma"] \\ Q & \end{tikzcd}$$

例 9.1.8

$\mathbb{Z}$ 的入射消解: $0 \to \mathbb{Z} \hookrightarrow \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$.

9.2 平衡函子 Tor

定义 9.2.1

$A, B : R-$ 模, 设 $\cdots \to R_{n_2} \to R_{n_1} \to R_{n_0} \to A \to 0$ 是 A 的一个自由消解, $\otimes B$ 得到 $B^{n_2} \xrightarrow{\varphi_1} B^{n_1} \xrightarrow{\varphi_0} B^{n_0} \to 0$.

$$\mathrm{Tor}_i^R(A, B) \overset{\text{def}}{=} \frac{\ker(B^{n_i \to B^{n_{i-1}}})}{\mathrm{Im}(B^{n_{i+1}} \to B^{n_i})} \underset{i\text{阶同调群}}{\longleftarrow} \textbf{链复形}(\varphi_i \circ \varphi_{i-1} = 0)$$

注解 9.3

自由消解可以替换为投影消解.

性质 9.2.2

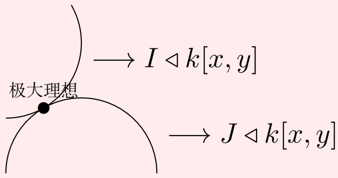
1. $\mathrm{Tor}_i^R(A, B) = \mathrm{Tor}_i^R(B, A)$,
2. $\mathrm{Tor}_0^R(A, B) = A \otimes_R B$,
3. 若 A 或 B 平坦, 则 $\mathrm{Tor}_i(A, B) = 0, i \geq 1$, 若 $\mathrm{Tor}_1^R(A, B) = 0$ 对 $\forall B$, 则 A 是平坦模,
4. 若 $0 \to A \to B \to C \to 0$ 是短正合列, M 是 $R-$ 模, 则

$$\cdots \to \mathrm{Tor}_2^R(C, M) \to \mathrm{Tor}_1^R(A, M) \to \mathrm{Tor}_1^R(B, M) \to \mathrm{Tor}_1^R(C, M) \to \underset{\mathrm{Tor}_0^R(A,M)}{A \otimes_R M} \to \underset{\mathrm{Tor}_0^R(B,M)}{B \otimes_R M} \to \underset{\mathrm{Tor}_0^R(C,M)}{C \otimes_R M} \to 0$$

是正合列.

注解 9.4: 应用

1. 代数几何: $R = k[x,y], m$ 为其极大理想, 相交数 $\dim_k\left(\sum_i (-1)^i \mathrm{Tor}_i^R(R/I, R/J)\right)$.



2. 表示论: G : 有限群, M : $G-$ 模 $\longleftrightarrow \varphi : G \to GL(n,\mathbb{Z}), H_i(G,M) \overset{\text{def}}{=} \mathrm{Tor}_i^{\mathbb{Z}[G]}(\mathbb{Z}, M)$.

李代数: $g : k$ 上李代数, $M : y$ 模 $H_\star(g,M) = \mathrm{Tor}_\star^{U(g)}(k,M), U(y)$: 泛包络代数 $\underset{k\oplus y\oplus y\otimes y\oplus\cdots}{\underset{\|}{T(y)}} \ /(a\otimes b - b\otimes a - [a,b])$.

例 9.2.1

$R = k[x]/(x^2), M = R/(x), \mathrm{Tor}_i^R(M,M)$, 基底 : $1, x \to$ 基底 : 1, 关系 $x \cdot 1 = 0\star$.

M 自由消解 (无限长) 为

$$
\begin{array}{cccccccccccc}
\cdots \to & R & \underset{1\mapsto x}{\to} & R & \underset{1\mapsto x}{\to} & R & \underset{1\mapsto x}{\to} & R & \underset{1\mapsto 1}{\to} & R/(x) & \cong k \to 0 \\
\otimes M & M & \underset{0}{\to} & M & \underset{0}{\to} & M & \underset{0}{\to} & M & \to & 0 & \\
H_\star & k & & k & & k & & k & & & \\
 & \uparrow & & \uparrow & & \uparrow & & \uparrow & & & \\
 & \mathrm{Tor}_3 & & \mathrm{Tor}_2 & & \mathrm{Tor}_1 & & \mathrm{Tor}_0^R & (M,M) & &
\end{array}
$$

例 9.2.2

$R = k[x,y], M_{(0,0)} = \underset{\downarrow}{R/(x,y)}, M_{(0,1)} = R/(x, y-1)$,

$$
\begin{array}{c|c|cc}
 & y^2 & xy^2 & x^2y^2 \\
 & y & xy & x^2y \\
\hline
 & 1 & x & x^2 \\
\end{array}
$$

$M_{(0,0)}$ 生成元: 1, 关系: $x\cdot 1=0, y\cdot 1=0$, 有限自由消解为

$$0\to R \xrightarrow[1\mapsto(y,-x)]{} R\oplus R \xrightarrow[\substack{(1,0)\mapsto x\\(0,1)\mapsto y}]{} R \xrightarrow[1\mapsto 1]{} M_{(0,0)}\to 0$$

$$
\begin{array}{cccccccc}
\otimes_{M_{(0,0)}} & 0\to & M_{(0,0)} & \xrightarrow{0} & M_{(0,0)}^2 & \xrightarrow{0} & M_{(0,0)} & \to 0 \\
1-1_\star & & k & & k^2 & & k & \\
 & & \uparrow & & \uparrow & & \uparrow & \\
 & & \mathrm{Tor}_2^R & & \mathrm{Tor}_1^R & & \mathrm{Tor}_0^R & (M_{(0,0),M_{(0,0)}}) \\
\otimes_{M_{(0,1)}} & M_{(0,1)} & \xrightarrow[1\mapsto(1,0)]{} & M_{(0,1)}^2 & \xrightarrow[\substack{(1,0)\mapsto 0\\(0,1)\mapsto 1}]{} & M_{(0,1)} & & \to 0 \\
H_\star & 0 & & 0 & & 0 & & \\
 & & & & & \downarrow & & \\
 & & & & & \mathrm{Tor}_0^R(M_{(0,0)},M_{(0,1)}) & & \\
\end{array}
$$

例 9.2.3

$H_i(\overset{\overset{G}{\parallel}}{\mathbb{Z}/n\mathbb{Z}}) \overset{\text{def}}{=} \mathrm{Tor}_i^{\mathbb{Z}[G]}(\mathbb{Z},\mathbb{Z})$. $\mathbb{Z}[G]$: 基底 $1,g,g^2,..,g^{n-1}(g^n=1), \mathbb{Z}\cong\mathbb{Z}[G]/(1-g)\longrightarrow g=\bar{1}$. $\mathbb{Z}$ 的自由消解为 $\cdots\mathbb{Z}[G] \xrightarrow[1\mapsto 1+g+\cdots+g^{n-1}]{} \mathbb{Z}[G] \xrightarrow[1\to 1-g]{} \mathbb{Z}[G] \xrightarrow[1\mapsto 1]{} \mathbb{Z}\to 0$.

$$
\begin{array}{cccccccccc}
\otimes_{\mathbb{Z}} & \mathbb{Z} & \xrightarrow{0} & \mathbb{Z} & \xrightarrow{n} & \mathbb{Z} & \xrightarrow{0} & \mathbb{Z} & \to 0 \\
H_\star & \mathbb{Z}/n\mathbb{Z} & & 0 & & \mathbb{Z}/n\mathbb{Z} & & \mathbb{Z} & \\
 & \mathrm{Tor}_3 & & \mathrm{Tor}_2 & & \mathrm{Tor}_1 & & \mathrm{Tor}_0 & \\
\end{array}
$$

定义 9.2.3: $\mathrm{Ext}_R^i(X,A)$

1. 取 A 的入射消解: $0\to A\to I_0\to I_1\to I_2\to\cdots$,
2. 作用 $\hom(X,\cdot)$ 得到 $0\to\hom(I_0,A)\xrightarrow{\varphi_0}\hom(I_1,A)\xrightarrow{\varphi_1}\cdots$,

3. $H_\star : \mathrm{Ext}^i_R(X,A) = \dfrac{\ker\varphi_i}{\mathrm{Im}\varphi_{i-1}}$.

例 9.2.4

1.

$$\begin{array}{cccccc}
\mathrm{Ext}(\mathbb{Z},\mathbb{Z}) & 0\to & \mathbb{Z}\to & \mathbb{Q} & \to & \mathbb{Q}/\mathbb{Z} & \to 0 \\
\hom(\mathbb{Z},\cdot) & & 0\to & \mathbb{Q} & \to & \mathbb{Q}/\mathbb{Z} & \to 0 \\
H_\star & & & \mathbb{Z} & & 0 & \\
 & & & \mathrm{Ext}^0(\mathbb{Z}/\mathbb{Z}) & & \mathrm{Ext}^1(\mathbb{Z}/\mathbb{Z}) &
\end{array}$$

2..

$$\begin{array}{ccccccc}
\mathrm{Ext}(\mathbb{Z}/n\mathbb{Z},\mathbb{Z}/m\mathbb{Z}) & 0\to & \mathbb{Z}/m\mathbb{Z}\to & \mathbb{Q}/\mathbb{Z} & \xrightarrow{\times m} & \mathbb{Q}/\mathbb{Z} & \to 0 \\
\hom(\mathbb{Z}/n\mathbb{Z},\cdot) & & 0\to & \mathbb{Z}/n\mathbb{Z} & \xrightarrow{\times m} & \mathbb{Z}/n\mathbb{Z} & \to 0 \\
H_\star & & & \mathbb{Z}/\gcd(m,n)\mathbb{Z} & & \mathbb{Z}/\gcd(m,n)\mathbb{Z} & \\
 & & & \uparrow & & \uparrow & \\
 & & & \mathrm{Ext}^0 & & \mathrm{Ext}^1 &
\end{array}$$

性质 9.2.4

Ext $\stackrel{\text{def}}{=}$ (extensions) : $0\to A\to B\to C\to 0$ 是短正合列, 则

$$0\to \hom(C,A)\to\hom(C,B)\to\hom(C,C)\to\mathrm{Ext}^1(C,A)\to\mathrm{Ext}^1(C,B)\to\mathrm{Ext}^1(C,C)\to\cdots$$

是长正合列.

Chapter 10

环的扩张, 不变量理论与 Galois 理论

10.1 整环和整扩张

定义 10.1.1: 域的扩张

若 $\exists$ 域的单同态 $\varphi : K \hookrightarrow L$, 则称 L 是 K 的域扩张.

定义 10.1.2: 代数元

$\lambda \in L$ 称为 K 的代数元, 若 $\exists$ 非 0 多项式 $p(x) \in K[x]$, 使得 $p(\lambda) = 0$.

定义 10.1.3: 代数扩张

若 L 中的元素均为 K 的代表元, 则称 L 是 K 的代数扩张.

例 10.1.1

$\mathbb{R} \hookrightarrow \mathbb{C}$ 是代数扩张, $\mathbb{R}(x^2) \hookrightarrow \mathbb{R}(x)$ 是代数扩张.

定义 10.1.4: 整元和整扩张 (代数元和代数扩张的推广)

R 是环，S 是 R 的子环.

1. $r \in R$ 称为子环 S 的**整元**，若 $\exists S$ 的首 1 多项式 $p(x) = x^k + s_{k-1}x^{k-1} + \cdots + s_1 x + s_0 \in S[x]$ 使得 $p(r) = 0$.
2. 若环的扩张 $S \hookrightarrow R$ 称为**整扩张**，若 R 中的元素均为 S 的整元.

性质 10.1.5

$R = \mathbb{F}[x_1, \cdots, x_n].R^G \hookrightarrow R$ 是整扩张.

对 $\forall$ 给定 $f \in R$，考虑多项式 $\Phi_f(t) \overset{\text{def}}{=} \prod_{g \in G}(t - gf) \in R[t]$，其中 t 是新增不定元. 由于 t 的所有系数是关于 $g_1 f, g_2 f, \cdots, g_n f$ 的对称多项式，故在 G 的作用下不变 $\Longrightarrow \Phi_f(t) \subset R^G[t]$，而 f 是 Φ_f 的根，故 $R^G \hookrightarrow R$ 是整扩张.

定义 10.1.6: 域的有限扩张

对域扩张 $K \hookrightarrow L$，若 L 是 K 的有限维向量空间，则称 L 是 K 的有限扩张，记 $|L : K| = \dim_k L$.

例 10.1.2

$$|\mathbb{C} : \mathbb{R}| = 2, \left|\mathbb{R}(x) : \mathbb{R}(x^2)\right| = 2, |\overset{\overset{\text{超越扩张}}{\uparrow}}{\mathbb{R}(x)} : \mathbb{R}| = \infty.$$

定理 10.1.7

1. $K \hookrightarrow L$ 是有限扩张 $\Longleftrightarrow \exists K$ 的代数元 $\lambda \in L$ 使得 $L = K(\lambda)$.
2. $|L : K| = \deg m_\lambda(x)$，其中 $m_\lambda(x) \in K[x]$ 是 λ 的极小多项式 (首 1 不可约多项式 $m \in K[x]$ 使得 $m(\lambda) = 0$).

定义 10.1.8: 环的有限扩张

若 R 是 $S \subset R$ 的有限生成 $S-$ 模，则称 R 是 S 的有限扩张.

定理 10.1.9: “多项式的线性化条件”

R 是 S 的有限扩张 $\iff R=S[a_1,\cdots,a_k],a_1,\cdots,a_k$ 是 S 的整元 (环的有限扩张定理).

设 $S\hookrightarrow R$ 是环扩张.

引理 1. $r\in R$ 是整元 $\iff S[r]$ 是有限生成 $S-$ 模.

引理 2. $r\in R$ 是整元 $\iff \exists$ 忠实的 $S[r]-$ 模 $M\subset R$, 使得 M 是有限生成的 $S-$ 模.

证明 2. $\Longrightarrow$ r 是整元, $\exists f(r)=r^k+s_{k-1}r^{k-1}+\cdots+s_1r+s_0$ 使得 $f(r)=0\Longrightarrow r^k=-s_{k-1}r^{k-1}-\cdots-s_1r-s_0\in S+Sr+\cdots+Sr^{k-1}$, 进而 $r^{k+i}=-s_{k-1}r^{k-1+i}-\cdots-s_1r^{i+1}-s_0r^i\in S+Sr+\cdots+Sr^{k-1}$, 因此, $S[r]$ 是由 $1,r,r^2,\cdots,r^{k-1}$ 有限生成的 $S-$ 模.

$\Longleftarrow$ 不妨设 $1,r,\cdots,r^n$ 是 $S-$ 模 $S[r]$ 的有限生成元 *(首 1 齐次替换)*. 因此, $r^{n+1}=\sum\limits_{i=0}^{n}s_ir^i,\exists s_i\in S\Longrightarrow r^{n+1}-\sum\limits_{i=0}^{n}s_ir^i=0.$

证明 2. $\Longrightarrow$ 令 $M=S[r]$, 即为有限生成 $S-$ 模, 由于 $1\in S[r]$, 故 $S[r]$ 是忠实的.

$\Longleftarrow$ 设 M 是有限生成 S 模, 生成元为 $e_1,\cdots,e_n$ 使得 $rM\subset M$ 且 M 是忠实 $S[r]-$ 模. 对 $\forall i$, 由 M 有限生成, $re_i=\sum s_{ij}e_j,s_{ij}\in S$. 进而, 得到线性方程组 (关于 e_i)

$$\begin{cases}(r-s_{11})e_1-s_{12}e_2-s_{13}e_3-\cdots=0\\ -s_{21}e_1+(r-s_{22})e_2-s_{23}e_3-\cdots=0\\ \vdots\\ -s_{n1}e_1+\cdots+(r-s_{nn})e_n=0\end{cases}$$

设 C 为线性方程组的系数矩阵, $C\begin{pmatrix}e_1\\ \vdots\\ e_n\end{pmatrix}=0,C^*C\begin{pmatrix}e_1\\ \vdots\\ e_n\end{pmatrix}=0\Longrightarrow \det Ce_i=0,\forall i$. 又由于 M 是忠实的, 且 $(e_1,\cdots,e_n)$ 生成 $M\Longrightarrow\det(C)=0$, 将 $\det(C)$ 展开, 即得到关于 r 的方程 $r^n+c_1r^{n-1}+\cdots+c_n=0,c_i\in S\Longrightarrow r$ 是整元.

由引理 “$\Longleftarrow$” 自然成立. “$\Longrightarrow$” 由于 R 是有限生成 $S-$ 模, 生成元为 $a_1,\cdots,a_k\in R$, 故 $R=S+Sa_1+Sa_2+\cdots+Sa_k\subset S[a_1,\cdots,a_k]=R$. 下证生成元是整元. 对 $\forall a_i\in R$, 由于 $1\in R$, R 是忠实的 $S[a_i]-$ 模, 由引理得 a_i 都是整元.

10.2 不变理论与环, 域扩张理论 ($\supset$Galois 理论)

定理 10.2.1: Noether

对 $\boxed{\text{特征任意}}$ 的域 $\mathbb{F}$, G 是有限群, R^G 有限生成.

令 S 为 $\Phi_{x_i}\overset{\text{def}}{=}\prod\limits_g(x-gx_i)\in R[x]$ 中所有系数生成的 $\mathbb{F}-$ 代数.

$$\underset{\substack{\text{第 1 步:}S\text{是有限生成的}\\ \mathbb{F}-\text{代数(系数有限项}\leq n|G|)\\ S\text{是 Noether 环}}}{S}\quad\subseteq\quad\underset{\substack{\text{第 3 步:}R^G\subset R\text{是有限生成}S-\text{模}\\ \xRightarrow{\text{第 1 步}}R^G\text{是有限生成的}\mathbb{F}-\text{代数}}}{R^G}\quad\subseteq\quad\underset{\substack{\text{第 2 步: 由于}x_i\text{是}\Phi_{x_i}\text{的根}\\ \Longrightarrow x_i\text{是}S\text{的整元}\\ R\text{是有限生成的}S-\text{模}\\ \Longrightarrow R\text{是 Noether}S-\text{模}}}{R}$$

$$r\in R^G=k_1\underset{\substack{\downarrow\\ k_1\sum_{\text{有限}}\mathbb{F}-\text{多项式}}}{S_1}+\cdots+k_n\underset{\substack{\downarrow\\ k_n\sum_{\text{有限}}\mathbb{F}-\text{多项式}}}{S_n}$$

10.3 Galois 扩张的构造

定义 10.3.1: Galois 群

设 $K\hookrightarrow L$ 是域扩张, $\mathrm{Gal}(L/K)=\{\varphi\in\mathrm{Aut}(L):\varphi(K)=K,\forall K\in K\}$.

注解 10.1

$K\subset L^{\mathrm{Gal(L/K)}}$ 且对有限扩张 $K\hookrightarrow L$, 下列命题等价:

1. $K\hookrightarrow L$ 是 Galois 扩张 ($\Longleftrightarrow\exists p\in K[x]$ 使得 p 无重根且 L 是 p 对分裂域 ($L=K(\lambda_1,\cdots,\lambda_n),\lambda_1\neq\lambda_2\neq\cdots\neq\lambda_n\in L$ 是 p 对根))
2. $K=L^{\mathrm{Gal}(L/K)}$
3. $|\mathrm{Gal}(L/K)|=|L:K|$

注解 10.2

不变量理论 $\underset{构造}{\rightsquigarrow}$ 以有限群 G 的 Galois 群的正规域扩张.

第 1 步: 有限群 $\exists$ 忠诚表示 $\longrightarrow G\times\mathbb{C}[x_1,\cdots,x_n]\to\mathbb{C}[x_1,\cdots,x_n]$.

第 2 步: 分式域 $\underset{\mathbb{C}(V)^G}{\underset{\|\mathrm{def}}{\mathrm{Frac}(\mathbb{C}[x_1,\cdots,x_n]^G)}}\hookrightarrow\underset{\mathbb{C}(V)}{\underset{\|\mathrm{def}}{\mathrm{Frac}(\mathbb{C}[x_1,\cdots,x_n])}}$ 是域的扩张.

定理 10.3.2

$\mathbb{C}(V)^G\hookrightarrow\mathbb{C}(V)$ 是 Galois 扩张, Galois 群为 G.

考虑多项式 $f(t)=\prod_{i=1}^{n}\prod_{g\in G}(t-gx_i)\in K[t],x_1,\cdots,x_n$ 为 $f(t)$ 的根 $\Longrightarrow\mathbb{C}(V)$ 是 f 的分裂域 $\Longrightarrow\mathbb{C}(V)$ 是 $\mathbb{C}(V)^G$ 正规扩张 $\xRightarrow{特征\ 0}\mathbb{C}(V)^G\hookrightarrow\mathbb{C}(V)$ 是 Galois 扩张, 设其 Galois 群为 H, 则有 $\mathbb{C}(V)^H=\mathbb{C}(V)^G\Longrightarrow H=G$.

定理 10.3.3: Galois 基本定理

$K\hookrightarrow L$ 是 Galois 扩张, Galois 群为 G

$$\{K\subset 域\subset L\}\underset{1-1}{\longleftrightarrow}\{\{e\}\subset 有限群\subset G\}$$

$$M\mapsto\mathrm{Galois}(L/M)$$

$$L^H\leftarrow\!\shortmid H$$

作业 10.1

对 $\forall\mathbb{C}(V)^G\hookrightarrow K\hookrightarrow\mathbb{C}(V)$, $\exists G$ 的子群 H 使得 $K=C(V)^H$.

作业 10.2

设 $S\hookrightarrow R\subset\mathbb{F}[x_1,\cdots,x_n]$ 是有限生成分次 $\mathbb{F}-$ 代数且扩张为整扩张, 则 R,SPoincaré 级数在 $t=1$ 奇点的阶数相同.

Chapter 11

整扩张的应用 (Noether 正规化定理, Krull 维数)

11.1 Noether 正规化定理

定理 11.1.1: Noether 正规化定理

域 $\mathbb{F}$ 上的有限生成代数 A, $\exists$ 代数无关的元素 $y_1, \cdots, y_r$ 使得 A 是 $\mathbb{F}[y_1, \cdots, y_r]$ 的有限扩张.

下面对 A 生成元个数的最小值进行归纳:

1. $k = 0$, 即 $A = \mathbb{F}$ 自然成立.

2. 假设 $k \leq n-1$ 时, $A = \mathbb{F}[x_1, \cdots, x_k]$ 是 $\mathbb{F}[y_1, \cdots, y_r]$ 的整扩张. 当 $k = n, A = \mathbb{F}[x_1, \cdots, x_n], x_i \in A$.

(a) 若 $x_1, \cdots, x_n$ 代数无关, 自然成立.

(b) 若 $x_1, \cdots, x_n$ 代数相关, $\exists$ 非常数多项式 $f(T_1, \cdots, T_n)$ 使得 $f(x_1, \cdots ., x_n) = 0(*)$, 不妨设 T_1 在 f 中出现, 令 $f = c_0 T_1^N + c_1 T_1^{N-1} + \cdots + c_N, c_0 \neq 0, c_i \in \mathbb{F}[T_2, \cdots, T_n]$.

(i) 若 $c_0 \in \mathbb{F}$, 由 $(*)$ 得, $x_1 \in A$ 是 $\mathbb{F}[x_2, \cdots, x_n]$ 的整元. 由归纳假设, $\exists$ 代数无关的 $y_1, \cdots, y_r \in A$, 使得 $\mathbb{F}[x_1, \cdots, x_n]$ 是 $\mathbb{F}[y_1, \cdots, y_r]$ 的有限扩张. 由有限扩张定理 A

是 $\mathbb{F}[y_1,\cdots,y_r]$ 的有限扩张.

(ii) 若 $c_0 \notin \mathbb{F}$, 令 $m \in \mathbb{N}^*, y_1 = x_1, y_2 = x_2 - x_1^{m^2}, \cdots, y_r = x_r - x_1^{m^r}$, 其它 $y_i = x_i, r+1 \le i \le n$. 由于 $y_i \in \mathbb{F}[x_1,\cdots,x_n]$ 且 $x_i \in \mathbb{F}[x_1,y_2,\cdots,y_n] = \mathbb{F}[y_1,\cdots,y_n]$. 故 $A = \mathbb{F}[x_1,\cdots,x_n] = \mathbb{F}[y_1,\cdots,y_n]$. 因此, 由 $(*)$ 得, $\exists$ 多项式 $g(T_1,\cdots,T_n) = f(T_1, T_2 + T_1^{m^2}, T_r + T_1^{m^r}, T_{r+1},\cdots,T_n) \in \mathbb{F}[T_1,\cdots,T_n]$ 使得 $g(y_1,\cdots,y_n) = 0$. 下面只需证以下命题.

命题 11.1.1

当 m 足够大, $g(T_1,\cdots,T_n) = c_0' T_1^N + c_1' T_1^{N-1} + \cdots + c_N'$ 满足 $c_0' \neq 0, c_i' \in \mathbb{F}[T_2,\cdots,T_r]$ 且 $c_0' \in \mathbb{F}$.

令 $f(T_1,\cdots,T_n) = \sum c_{j_1,\cdots,j_n} T_1^{j_1}\cdots T_n^{j_n}$ (直和意义). 取足够大的 m 使得对所有 $c_{j_1,\cdots,j_r} \neq 0$, T_1 的次数 $j_1 + m^2 j_2 + \cdots + m^r j_r$ 互不相同, 则 $g(T_1,\cdots,T_n) = \sum c_{j_1,\cdots,j_r} T_1^{j_1}(T_2 + T_1^{m^2})^{j_2}\cdots(T_r + T_1^{m^r})^{j_r}\cdots T_n^{j_n}$ 在字典序下首项不会相消.

11.2 环的 Krull 维数与整扩张

定义 11.2.1

设 R 设环, $p_i \in \mathrm{Spec}R$, R 的 Krull 维数定义为 $\dim R \overset{\text{def}}{=} \sup\{n : p_0 \subsetneqq p_1 \subsetneqq \cdots \subsetneqq p_n \subset R\}$, 对 $p \in \mathrm{Spec}R$, $ht(p) \overset{\text{def}}{=} \sup\{n : p_0 \subsetneqq p_1 \subsetneqq \cdots \subsetneqq p_n \subset p\}$ 称为 p 的商 (或余维数). 对任意理想 I, $ht(I) \overset{\text{def}}{=} \{ht(p) : I \subset p\}$ 称为 I 的商.

注解 11.1: 目的

1. $k[x_1,\cdots,x_n]$ 的 Krull 维数是 $n \longleftrightarrow k^n$ 的向量空间维数.
2. 不变理论, G 是有限群, $G \curvearrowright R = k[x_1,\cdots,x_n], \dim R^G = n$.

定理 11.2.2

1. 设 $S \subset R$ 是环的整扩张, 则有 $\dim S = \dim R$,
2. $\dim k[x_1, \cdots, x_n] = n, k$ 是域.

1. 先证 $\dim S \leq \dim R$.

定理 11.2.3: Lying-over 定理

$S \subset R$ 是整扩张, 对 $\forall p \in \mathrm{Spec} S, \exists p' \in \mathrm{Spec} R$ 使得 $p = p' \cap S$.

由 Lying-over 定理, 对 $p_0 \subset S, \exists p_0' \in \mathrm{Spec} R$ 使得 $p_0' \cap S = p_0$.

定理 11.2.4: Going-up 定理

$S \subset R$ 是整扩张, $p, q \in \mathrm{Spec} S$ 使得 $p \subset q$, 设 $p' \in \mathrm{Spec} R$ 使得 $p = p' \cap S$, 则 $\exists q' \in \mathrm{Spec} R$ 使得 $q' \supset p'$ 且 $q = q' \cap S$, $p' \subset \boxed{q'} \subset R, p \subset q \subset S$.

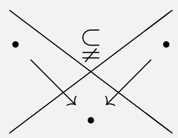
由 Going-up 定理, 对$\forall$ $\begin{array}{ccccccc} p_0 & \subsetneq & p_1 & \subsetneq \cdots \subsetneq & p_n & \subset & S \\ \uparrow \text{lying over} & & \uparrow \text{over} & & \uparrow \text{over} & & \uparrow \text{over} \\ p_0' & \subsetneq & p_1' & \subsetneq \cdots \subsetneq & p_n' & \subset & R \end{array}$ $\Longrightarrow \dim S \leq \dim R$.

$\exists p_1', \cdots, p_n'$使得

$\dim S \geq \dim R$:

定理 11.2.5: 不相容定理

设 $S \subset R$ 是整扩张, $p \subset q \in \mathrm{Spec} R$, 且 $p \cap S = q \cap S$ 且 $p = q$.



对 $\forall R$ 中素理想严格升链 $q_0 \subsetneq \cdots \subsetneq q_n \subset R$, 由于素理想限制在 S 上仍是素理想 $\Longrightarrow q_0 \cap S \subset \cdots \subset q_n \cap S \subset S$, 由不相容定理, 升链为严格升链 $(q_0 \cap S \subsetneq \cdots \subsetneq q_n \cap S \subsetneq S)$. 因此 $\dim R \leq \dim S$.

2. 对向量空间 k^n 对维数归纳.

(1) $\dim = 0$, k 唯一的素理想是 $(0) \Longrightarrow \dim k = 0$.

(2) 假设 $\dim k[x_1, \cdots, x_{n-1}] = n-1$, 对 $R = k[x_1, \cdots ., x_n]$ 有素理想升链 $\{0\} \subsetneq$

$(x_1) \subsetneqq (x_1,x_2) \subsetneqq \cdots \subsetneqq (x_1,\cdots,x_n) \subset k[x_1,\cdots,x_n]$, 因此, $\dim R \geq n$. 取 R 中的任意一个极大素理想升链 $\{0\} \subsetneqq p_1 \subsetneqq p_2 \subsetneqq \cdots \subsetneqq p_m$, 下证 $m \leq n$.

引理 1. *Noether 整环是 UFD$\Longleftrightarrow$ 商为 1 的理想为主理想.*

由于 R 是 Noether 整环, 故 $p_1 = (f), f$ 是 R 中首一不可约多项式. 令 $\pi: f \in S[x_n], S = k[x_1,\cdots,x_{n-1}] \Longrightarrow x_n$ 是 $S \longleftrightarrow R/(f)$ 的整元 $\Longrightarrow R/(f)$ 是 S 的整扩张 $\Longrightarrow \dim R/(f) = \dim S = n-1$, 考虑 $\{0\} = \underset{\substack{\| \\ p_1}}{p_1/(f)} \subsetneqq \underset{\substack{\| \\ p_1}}{p_2/(f)} \subsetneqq \cdots \subsetneqq \underset{\substack{\| \\ p_1}}{p_m/(f)} \Longrightarrow m-1 \leq n-1 \Longrightarrow m \leq n$.

注解 11.2

对于整扩张 $S \subset R$, Going-down 性质不一定成立.

性质 11.2.6: Going-down

$$\begin{array}{c} p' \subset q' \subset R \\ \downarrow \substack{\text{lying} \\ \text{over}} \downarrow \\ p \subset q \subset S \end{array}$$
$, p,q \in \mathrm{Spec}S, q' \in \mathrm{Spec}R$ 使得 $q' = q \cap S, \exists p' \in \mathrm{Spec}R$ 使得 $p' \cap S = R$.

定理 11.2.7: Going-down

若 S, R 还是整环且 S 是整闭的 ($S \hookrightarrow \mathrm{Frac}S$ 是整扩张), 则 Going-down 条件成立.

例 11.2.1

不变理论中 $R^G \hookrightarrow R = k[x_1,\cdots,x_n]$ 满足 lying-over, going-up, going-down 条件.

11.3 Hilbert 零点定理 Nullstellensatz
zero position theorem

注解 11.3

$$\text{Hilbert 基定理} \Longrightarrow \text{弱零点定理} \Longleftrightarrow \text{强零点定理}$$
$$\searrow \quad \swarrow$$
$$\text{正规化} + \text{局部化}$$

11.3.1 弱零点定理

注解 11.4

考虑 $R = k[x_1, \cdots, x_n]$ 中极大理想的分类, k 为域. 自然地, $\underset{k^n \text{中的点}(a_1,\cdots,a_n)\in k^n}{\overset{\Updownarrow 1-1}{(x_1 - a_1, x_2 - a_2, \cdots, x_n - a_n)}}$ 是一类极大理想.

猜想 11.3.1

$(x_1 - a_1, x_2 - a_2, \cdots, x_n - a_n)$ 是不是 R 所有极大理想的形式?

例 11.3.1

$k = \mathbb{R}, \mathbb{R}[x], (x^2 + 1)$ 是极大理想 $\neq (x - a_1)$, $(\mathbb{R}[x]/(x^2 + 1) \cong \mathbb{C})$, 故上述猜想错误.

但当 k 是代数闭域, 有以下定理:

定理 11.3.1: 弱零点定理

k : 代数闭域, $(x_1 - a_1, x_2 - a_2, \cdots, x_n - a_n)$ 是 $k[x_1, \cdots, x_n]$ 的所有极大理想. (几何含义: k^n 中的点 $\overset{1-1}{\longleftrightarrow}$ $k[x_1, \cdots, x_n]$ 中的极大理想).

当 $k = \mathbb{C}$ 时的证明:(基于集合论和域扩张)

设 m 是 $\mathbb{C}[x_1, \cdots, x_n]$ 极大理想. $K \overset{\text{def}}{=} \mathbb{C}[x_1, \cdots, x_n]/m$ 是 $\mathbb{C}$ 的有限生成代数且为 $\mathbb{C}$ 的域扩张 $\Longrightarrow \mathbb{C}[x_1, \cdots, x_n]/m$ 是 $\mathbb{C}$ 的 (至多) 可数维向量空间.

假设 $\exists a$ 是 K 的超越元 $\overset{\text{定义}}{\Longrightarrow} \dfrac{1}{a - \alpha}, \alpha \in \mathbb{C}$ 是 K 的超越元 $\longleftarrow$(局部化思想).

$$\Longrightarrow L = \mathbb{C}\left(\underset{\alpha\in\mathbb{C}}{\frac{1}{a - \alpha}}, \cdots\right) \longrightarrow \text{基底不可数, 矛盾.}$$

$\Longrightarrow K$ 是 $\mathbb{C}$ 的代数扩张, 由于 $\mathbb{C}$ 是代数闭域 $\Longrightarrow K = \mathbb{C}$

$\Longrightarrow$ 对 $\forall x_i \in K, \exists c_i \in \mathbb{C}$ 使得 $x_i = c_i \in K$

$\Longrightarrow x_i - c_i \in m \Longrightarrow m = (x_i - c_i, 1 \leq i \leq n)$.

Chapter 12

Hilbert 零点定理

定理 12.0.1: 弱零点定理

k : 代数闭域, $(x_1-a_1, x_2-a_2, \cdots, x_n-a_n)$ 是 $k[x_1,\cdots,x_n]$ 的所有极大理想. (几何含义: k^n 中的点 $\xleftrightarrow{1-1}$ $k[x_1,\cdots,x_n]$ 中的极大理想).

一般代数闭域上的证明: $\boxed{\textbf{Zariski 引理}}$

设域 K 是域 k 的有限生成的 $k-$ 代数, 则 k 是有限生成的 $k-$ 模. 由 Noether 正规化定理, 令 $K=k[\underbrace{x_1,\cdots,x_m}_{\text{代数无关}},\underbrace{x_{m+1},\cdots,x_n}_{\text{代数（整）扩张}}]$, 使得 n 最小, 下用反证法证 $m=0$. 设 $m\geq 1, F \overset{\text{def}}{=} k(x_1,\cdots,x_m)$ 是 k 的扩张, 则 K 是有限生成的 $F-$ 模.

$$\begin{array}{c} K \subset F \subset K \\ F \text{ 是 } k- \text{ 代数} \end{array} \quad \text{使 得} \quad \begin{cases} 1.\ k\text{是 Noether 环} \\ 2.\ K\text{是有限生成}k-\text{代数} \\ 3.\ K\text{是有限生成}F-\text{模} \end{cases} \xRightarrow[\text{定理}]{\text{Artin-Tale}}$$

F是有限生成的$k-$代数.

由 2,3 设 $K = k[x_1, \cdots ., x_n] = Fy_1 + \cdots + Fy_k$, 则 $x_i = \sum\limits_j f_{ij}y_j, f_{ij} \in F$. 且

由 2 得 $y_iy_j \in K$, 故 $y_iy_j = \sum\limits_k f_{ijk}y_k, f_{ijk} \in F$.

$\xrightarrow{\sum f_iy_i, f_i \in k[x_1,\cdots,x_n], \text{系数通过}x_ix_j\text{变为}F_1\text{中系数}}$ 设 F_1 是由所有 f_{ij}, f_{ijk} 生成的 $k-$ 代数 (有限生成), 则 K 是有限生成 F_1- 模, 由 Hilbert 基定理:

1. F_1 是 Noether 环,
2. K 是 Noether F_1- 模.

$\Longrightarrow$ 子模 F 是有限生成 F_1- 模, 又 F_1 是有限生成 $k-$ 代数. 故 F 是有限生成 $k-$ 代数.

令 $F = k[z_1, \cdots, z_n], z_i = \dfrac{f_i}{g_i}, f_ig_i \in k[x_1, \cdots, x_n]$. 取不可约多项式 $h = g_1 \cdots g_s + 1, (h, g_i) = 1$, 则 $\underbrace{\frac{1}{n} \underset{\Uparrow}{\notin} k[z_1, \cdots, z_s] = F}_{((g_1\cdots g_m, h=1), f(z_1,\cdots,z_s)\text{分母为}g_i\text{倒数}, i\in\mathbb{N}^*)}$, 与 F 是域矛盾.

注解 12.1: Zariski 引理 $\Longrightarrow$ 弱零点定理

设 m 是 $k[x_1, \cdots, x_n]$ 极大理想, 则 $k[x_1, \cdots, x_n]/m$ 既是域又是有限生成 $k-$ 代数. 由 Zariski 引理, $k[x_1, \cdots, x_n]/m$ 是有限生成 $k-$ 模. $\Longrightarrow k[x_1, \cdots, x_n]/m$ 是 k 的代数扩张 $\Longrightarrow k[x_1, \cdots, x_n]/m \cong k$($k$ 代数闭)$\Longrightarrow x_i + m = a_i + m, a_i \in k \Longrightarrow m = (x_1 - a_1, \cdots, x_n - a_n)$.

12.1 强零点定理

定义 12.1.1: 代数集

设 I 是 $k[x_1, \cdots, x_n]$ 的理想, I 中 $\underset{\substack{\Updownarrow \\ \text{所有生成元的共同零点}}}{\text{所有多项式共同零点}}$ 称为 I 的代数集, 记为 $V(I)$.

命题 12.1.1

假设 $V(I) \neq \varnothing, k[x_1, \cdots, x_n]$ 中在 $V(I)$ 上取值为 0 的多项式所生成的理想 $J(V)$ 与 I 的关系.

例 12.1.1

$k[x], I = (x^2), V(I) = 0 \in k, J(V) = (x) \neq I, x^2 \in I$, 但 $x \notin I, J \neq I$.

定义 12.1.2

设 I 是环 R 的理想, $\sqrt{I} \overset{\text{def}}{=} \{f \in R : f^m \in I, \exists m \in \mathbb{N}\}$ 称为**理想 I 的根**. 若 $\sqrt{I} = I$, 称 I 是**根理想**.

注解 12.2

(1) $I \subset \sqrt{I}$.

(2) 理想的根是根理想, 即 $\sqrt{\sqrt{I}} = \sqrt{I}$. 考虑 J 与 $\sqrt{I}$ 的关系: 若 $f^n(V(I)) = 0 \in k \Longrightarrow f(V) = 0 \Longrightarrow f \in J \Longrightarrow \sqrt{I} \subset J$.

注解 12.3

强零点定理: 当 k 是代数闭域, $\sqrt{I} = J$.(代数集 $\overset{1-1}{\longleftrightarrow}$ 根理想)

若 k 不说代数闭域, $J(V_{\bar{k}}(I)) = \sqrt{I} \subset k[x_1, \cdots, x_n]$. 域 $\bar{k}$ 是 k 的闭包, 其中 $J(V_{\bar{k}}(I)) \overset{\text{def}}{=} \{f \in k[x_1, \cdots, x_n : f(x) = 0]\}$.

例 12.1.2

$X=\begin{pmatrix} a & b \\ c & d \end{pmatrix}, X^2=\begin{pmatrix} a^2+bc & (a+d)b \\ (a+d)c & d^2+bc \end{pmatrix}$, 考虑 $\mathbb{C}[a,b,c,d]$ 的理想 $I=(a^2+bc,(a+d)b,(a+d)c,d^2+bc), V(I)=\left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix}\text{幂零矩阵}, a,b,c,d\in\mathbb{C}\right\}\subset\mathbb{C}^4$.

注解 12.4

1. 2 阶幂零矩阵 X 使得 $X^2=0$.
2. $V(I)$ 不是 $\mathbb{C}^4$ 子空间.

对 $\forall$ 幂零矩阵 $x\in V(I), \mathrm{tr}=0, \det=0$. 由 Hilbert 强零点定理, $(\mathrm{tr},\det)\subset I(V(I))=\sqrt{I}$, 即 $(a+d,ad-bc)\subset\sqrt{I}$.

反之, 假设 $\exists x\notin(a+d,ad-bc)$ 使得 $x^n\in I$, 考虑商环 $\mathbb{C}[a,b,c,d]/(a+d,ad-bc)\underset{a=-d}{\cong}\mathbb{C}[a,b,c]/(a^2+bc)$, 则 $[x^n]\in\underset{I}{(a^2+bc,(a+d)b,(a+d)c,d^2+bc)}+(a+d,ad-bc)\underset{a=-d}{\cong}0+(a^2+bc)\Longrightarrow x$是零因子.

而由 a^2+bc 不可约 $\Longrightarrow(a^2+bc)$ 是素理想 $\Longrightarrow\mathbb{C}[a,b,c]/(a^2+bc)$ 为整环, 与 x 是零因子矛盾. 故 $\sqrt{I}\subset(a+d,ad-bc)\Longrightarrow\sqrt{I}=(a+d,ad-bc)$.

性质 12.1.3: 一般情形

令 $X=(x_{ij})_{1\le i,j\le n}$ 是不定元构成的 n 阶方阵. 设 $I\subset\mathbb{C}[x_{11},\cdots,x_{nn}]$ 是 x^n 中所有元素生成的理想. $V(I)=\{\text{幂零矩阵}\}$, 由于幂零矩阵的特征多项式 $\det(\lambda I_{n\times n}-X)=\lambda^n$, 则 $\det(\lambda I_{n\times n}-X)$ 所有 $\lambda^k, k\le n-1$ 的系数都是幂零矩阵的零化多项式, 因此 $(\lambda^k, k\le n-1\text{的系数})\subset I(V(I))=\sqrt{I}$.

定理 12.1.4

$\sqrt{I}=(\det(\lambda I_{n\times n}-X)\text{中}k\le n-1\text{的系数})$.

命题 12.1.2

$X=(x_{ij})_{n\times n}, Y=(y_{ij})_{n\times n}, I=([X,Y]\overset{\text{def}}{=}\underset{\mathbb{C}[x_{11},\cdots,x_{nn},y_{11},\cdots,y_{nn}]}{\overset{\cup}{XY-YX}}\text{中元素}), V(I)\cong$

$\{(A,B) \in M_{n\times n} \times M_{n\times n} \cong \mathbb{C}^{2n^2} : AB = BA\}, J(V(I)) = \sqrt{I}, \left((X+Y)^n - \sum_i C_n^i X^i Y^{n-i}\right) \in \sqrt{I}, \forall n \in \mathbb{N}^*$.

1. $\sqrt{I} = I$?
2. $\mathbb{C}[x_{11}, \cdots, x_{nn}, y_{11}, \cdots, y_{nn}]/I$ 有没有幂零元?

作业 12.1

求证:

1. $I \subset \sqrt{I}$.
2. 若 $I \subset J$, 则 $\sqrt{I} \subset \sqrt{J}$.
3. $\sqrt{\sqrt{I}} = \sqrt{I}$.
4. $\sqrt{I+J} = \sqrt{\sqrt{I} + \sqrt{J}}$.
5. $\sqrt{IJ} = \sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$.
6. $I = (1) \Longleftrightarrow \sqrt{I} = (1)$.

性质 12.1.5

弱零点定理 $\Longrightarrow$ 强零点定理 (Rabinowitch 技巧 $\Longrightarrow$ 局部化)

对 $\forall f \in J(V(I))$, I 是 $k[x_1, \cdots, x_n]$ 的理想. 考虑理想 $(I, 1 - \underbrace{1 - x_0 f}_{\frac{1}{f}}) \in k[x_0, x_1, \cdots, x_n]$, I 中多项式与 $1 - x_0 f$ 没有公共根.

由弱零点定理, 该理想不包含在任一极大理想中 $\Longrightarrow (I, 1 - x_0 f) = k[x_0, \cdots, x_n] \Longrightarrow 1 = \sum_{i=1}^{k} a_i b_i + a(1 - x_0 f), a, a_i \in k[\boxed{x_0}, \cdots, x_n], b_i \in I$. 取 $x_0 = \dfrac{1}{f}$, 得 $1 = \sum_{i=1}^{m} a_i b_i$, 其中, $a_i \in k\left[x_1, \cdots, x_n, \boxed{\dfrac{1}{f}}\right]$. 故 $a_i = \dfrac{c_i}{f^m}, c_i \in k[x_1, \cdots, x_n]$(可让 m 足够大是的 a_i 分母相同). 则 $1 = \sum \dfrac{c_i}{f^m} b_i \Longrightarrow f^m = \sum c_i b_i \in I$.

性质 12.1.6

强零点定理 $\Longrightarrow$ 弱零点定理

弱零点定理 $\Longleftrightarrow V(I)=\varnothing$ 当且仅当 $I=k[x_1,\cdots,x_n]=(1)$.

"$\Longrightarrow$" 极大理想 $V(m)$ 必非空, $\exists(a_1,\cdots,a_n)\in V(m)$, 则 $J(V(m))=\sqrt{m}=m\subset(x_1-a_1,\cdots,x_n-a_n)$, 故 $m=(x_1-a_1,\cdots,x_n-a_n)$.

若 $I=(1), V(I)=\varnothing$ 自然成立. 若强定理成立, 当 $V(I)=\varnothing$ 时, $J(V(I))=k[x_1,\cdots,x_n]=\sqrt{I}\Longrightarrow 1\in\sqrt{I}\Longrightarrow 1=1^n\in I\Longrightarrow I=k[x_1,\cdots,x_n]$.

Chapter 13

局部化

13.1 环的局部化

命题 13.1.1: 局部化

设 R 是环, S 是 R 的子集.

目标: 构造 R 的扩张 $R[S^{-1}]$, 使得 S 中所有元素都可逆.

方法 1: Rabinowitsch 技巧.

$$R[S^{-1}] = R[t_1, t_2, \cdots]/(s_1 \underset{\substack{\downarrow \\ s_1\text{的逆}}}{t_1} -1, s_2 \underset{\substack{\downarrow \\ s_2\text{的逆}}}{t_2} -1, \cdots)$$

注解 ***13.1***

$R[S^{-1}]$ 满足泛性质: 对 $\forall$ 环同态 φ, 满足 $\varphi(S)$ 在 T 中可逆, 则 $\exists$ 唯一环同态 ψ, 使得图表可换:

$$\begin{tikzcd} & R[S^{-1}] \arrow[d, dashed, "\psi"] \\ R \arrow[ur, "i"] \arrow[r, "\varphi"'] & T \end{tikzcd} \qquad \varphi = \psi \circ i.$$

可令 $\psi(r) = \varphi(r) \in T, \psi(t_i) = (\varphi(s_i))^{-1} \in T$.

方法 2: 分式域方法

不妨设 S 乘法封闭 $(1 \in S, \forall s_1, s_2 \in S \Longrightarrow s_1 s_2 \in S)$ 且不含 0. ***(若 S 不封闭, 可通***

过乘法生成封闭子集.)

1. 若 S 没有零因子, 则可以照搬分式域方法.

构造 $R[S^{-1}]$, 取 $(r,s)\in R\times S$, 记为 $\frac{r}{s}$, 在 $R\times S$ 上定义等价关系 $\frac{r_1}{s_1}\sim\frac{r_2}{s_2}\iff r_1s_2=r_2s_1$. 定义运算 $\frac{r_1}{s_1}+\frac{r_2}{s_2}\overset{def}{=}\frac{r_1s_2+r_2s_1}{s_1s_2}$, $\frac{r_1}{s_1}\cdot\frac{r_2}{s_2}=\frac{r_1r_2}{s_1s_2}$, $0\overset{def}{=}\frac{0}{1}, 1=\frac{1}{1}$.

需验证: (1) $\sim$ 是等价关系, (2) $\cdot,+$ 是良定义的, (3) $(R[S^{-1}],+,\cdot)$ 构成环.

注解 13.2

验证中要点: 传递性 (用到 S 不含零因子条件).

$$\begin{array}{ccccc}
\frac{r_1}{s_1}\sim\frac{r_2}{s_2} & , & \frac{r_2}{s_2}\sim\frac{r_3}{s_3} & \Longrightarrow & \frac{r_1}{s_1}\sim\frac{r_3}{s_3}\\
\updownarrow & & \updownarrow & & \updownarrow\\
r_1s_2=r_2s_1 & & r_2s_3=r_3s_2 & \Longrightarrow & r_1s_3=r_3s_1\\
\downarrow\times s_3 & & \swarrow\times s_1 & & \\
r_1s_2s_3 & = & r_2s_1s_3=r_3s_1s_2 & \Longrightarrow & \underset{s_2\text{不是零因子}}{\boxed{s_2}(r_1s_3-r_3s_1)=0}
\end{array}$$

$\Longrightarrow r_1s_3-r_3s_1=0$.

2. 若 S 含有零因子.

思路: 考虑 $I=\{r\in R: rs=0,\exists s\in S\}$ 及 $p:R\to R/I$.

(i) I 是理想. $\left(r_1s_1=0, r_2s_2=0\Longrightarrow\begin{cases}(r_1+r_2)\overset{\subset S}{\boxed{s_1s_2}}=0 & \Longrightarrow r_1+r_2\in I\\ rr_1s_1=0 & \Longrightarrow rr_1\in I\end{cases}\right)$.

(ii) $p(S)$ 没有零因子, 故可以构造 $R[S^{-1}]\overset{def}{=}(R/I)[S^{-1}]$.

定义 13.1.1

在 $R\times S$ 中定义等价类: $(r_1,s_1)\sim(r_2,s_2)\overset{def}{\iff}\exists s\in S$, $R[S^{-1}]\overset{def}{=}R\times S$ 中关于 $\sim$ 的等价类, 使得 $s(r_1s_2-r_2s_1)=0$. 记为 $R[S^{-1}]\overset{def}{=}\left\{\frac{a}{s}:a\in R,s\in S\right\}$, $+,\cdot$ 定义同情形 1.

验证中要点:

(1) 传递性: $\frac{a}{s}\sim\frac{a'}{s'}, \frac{a'}{s'}\sim\frac{a''}{b''}$. $\exists u,v\in S, u(as'-a's)=v(a's''-a''s')=0\Longrightarrow$

$$\underset{S}{\boxed{s'uv}}^{\uparrow S\text{封闭}}(as''-a''s)=vs'u(as'-a's)+usv(a's''-a''s')\Longrightarrow\frac{a}{s}\sim\frac{a''}{s''}.$$

(2) $+,\cdot$ 良定义: 即若 $\frac{a}{s}\sim\frac{a'}{s'}$, 则 $\frac{as'+a's}{ss'}\sim\frac{a''s'+a's''}{s''s'}(i)$ 且 $\frac{aa'}{ss'}=\frac{a'a''}{s's''}(ii)$.

$$\left(\begin{array}{l}\text{验证: }\frac{a}{s}\sim\frac{a''}{s''}\overset{def}{\Longleftrightarrow}\exists u\in S\text{使得}u(as''-a''s)=0\\ \Longrightarrow u((as'+a's)(s''s)-(a''s'+a's'')(ss'))=(s')^2u(as'-a''s)=0\Longleftrightarrow(i)\\ \text{且}u((aa')(s''s')-(a''a')(ss'))=a's'u(a''-a''s)=0\Longleftrightarrow(ii)\end{array}\right)$$

注解 13.3

当 R 是整环, $S=R\backslash\{0\},R[S^{-1}]$ 即是 R 的分式域.

例 13.1.1

$R=\mathbb{Z}$,

1. $S=\mathbb{Z}\backslash\{0\},R[S^{-1}]=\mathbb{Q}(\text{分式域})$,
2. $S=\{2\}(\Longleftrightarrow 2\text{生成的子群})$

$$\begin{aligned}R[S^{-1}]\underset{\text{方法 2}}{=}\left\{\frac{a}{2^n}\right\}&\overset{\text{方法 1}}{\underset{\nearrow}{\equiv}}\mathbb{Z}[x]/(2x-1)\\ \varphi:\mathbb{Z}[x]\to\left\{\frac{a}{2^n}\right\}&,\ker\varphi=(2x-1)\\ f\mapsto f\left(\frac{1}{2}\right)&\end{aligned}$$

3. $S=\text{奇素数}$, $R[S^{-1}]=\left(\frac{a}{b},b\text{是奇数}\right)$.

例 13.1.2

$R=\mathbb{C}[x]$,

1. $S=R\backslash\{x\}$, $R[S^{-1}]=\left\{\text{有理函数}\frac{p(x)}{q(x)},q\neq 0\right\}$

2. $S=\{x\}$, $R[S^{-1}] \overset{\text{方法 }1}{=} \left\{ \underset{\underset{\text{Laurent 多项式}}{\downarrow}}{\dfrac{p(x)}{x^n}} \right\}$

$$\underset{\Uparrow}{\overset{\text{方法 }2}{=}} \mathbb{C}[x,y]/(1-xy)$$

$$\varphi:\mathbb{C}[x,y]\to\left\{\frac{p(x)}{x^n}\right\}$$

$$f(x,y)\mapsto f\left(x,\frac{1}{x}\right),\ker\varphi-(1-xy)$$

3. $S=\{x\alpha,\alpha\in\mathbb{C}^*\}, R[S^{-1}]=\left\{\dfrac{p(x)}{q(x)}:q(0)\neq 0\right\}=0$ 点良定义的有理数.

例 13.1.3

$R=\mathbb{C}[x,y]/(xy), S=\{x+(xy)\}, R[S^{-1}] \overset{\text{方法 }1}{=} \mathbb{C}[x,y,z]/(xy,1-xz) \overset{\text{方法 }2}{\cong} \left\{\dfrac{f(x,y)}{x^n}:xy=0\right\} \underset{\left(\frac{y}{x^n}=\frac{xy}{x^{n+1}}=0\right)}{\underset{\downarrow}{=}}$

$$\varphi:\mathbb{C}[x,y,z]/(xy)\to\mathbb{C}\left[x,\frac{1}{x}\right]$$

$$f(x,z)+g(y,z)\mapsto f\left(x,\frac{1}{x}\right),\ker\varphi=(1-xz)$$

13.2 模的局部化

定义 13.2.1: 模的局部化

设 S 是 R 的可乘集, $M[S^{-1}]=\left\{\dfrac{m}{s},m\in M,s\in S\right\}$, $\dfrac{m}{s}=\dfrac{m'}{s'}\overset{\text{def}}{\Longleftrightarrow}\exists s\in S$ 使得 $\underset{\text{零因子}}{s(s'm-sm')}=0$, $r\cdot\dfrac{m}{s}\overset{\text{def}}{=}\dfrac{rm}{s}$, $\dfrac{m}{s}+\dfrac{m'}{s'}\overset{\text{def}}{=}\dfrac{s'm+sm'}{ss'}$ 称为模 M 的局部化.

例 13.2.1

$p \in \mathrm{Spec}R, M_{(p)} \overset{\text{def}}{=} M[(R\backslash p)^{-1}]$ 是一个 $R(p)$ 模, $R_{(p)} = R[(R\backslash P)^{-1}]$, 称为 M 在 p 的局部模.

性质 13.2.2

$A, B, C : R-$ 模, $S \subset R$, $0 \to A \xrightarrow{f_A} B \xrightarrow{f_B} C \to 0$ 是正合列, 则 $0 \to A[S^{-1}] \xrightarrow{g_A} B[S^{-1}] \xrightarrow{g_B} C[S^{-1}] \to 0$ 是正合列.

设 $\frac{b}{s} \in B[S^{-1}]$ 使得 $g_B\left(\frac{b}{s}\right) = 0$, 只需证: $\frac{b}{s} \in \mathrm{Im}g_A$. 令 $c = f_B(c) \in S$ 使得 $g_B\left(\frac{b}{s}\right) \overset{\text{def}}{=} \frac{c}{s'} = 0$, 即 $\exists s_0 \in S$ 使得 $cs_0 = 0$. 令 $s_1 \in f_B^{-1}$, 则 $f_B(bs_1) = cs_0 = 0$, 由正合性, $bs_1 \in \mathrm{Im}f_A$, 设 $f_A(0) = bs_1$, 则 $\frac{b}{s} = \frac{bs_1}{ss_1} = \frac{f_A(a)}{ss_1} \in \mathrm{Im}g_A$.

注解 13.4

由于 $M[S^{-1}] \cong M \otimes_R R[S^{-1}], R[S^{-1}]$ 是平坦 $R-$ 模.

注解 13.5

应用: 模的局部性

1. $M = 0 \iff$ 对所有 $p \in \mathrm{Spec}R$(或 $m \in \mathrm{Spec}_m R$), $M_{(p)} = 0 (M_{(m)} = 0)$.
2. $0 \to A \to B \to C \to 0$ 是正合列

$$\begin{aligned} &\iff 0 \to A_{(p)} \to B_{(p)} \to C_{(p)} \to 0 \text{是正合列}, \forall p \in \mathrm{Spec}R \\ &(\text{或} \iff 0 \to A_{(m)} \to B_{(m)} \to C_{(m)} \to 0 \text{是正合列}, \forall m \in \mathrm{Spec}_m R) \end{aligned}$$

3. M 是平坦 $R-$ 模 $\iff M_{(p)}$ 平坦, $\forall p \in \mathrm{Spec}R$.

13.3 局部环

性质 13.3.1: 局部环的等价条件

环 R 称为**局部环**, 若满足下列等价条件:

1. R 有唯一的极大理想,
2. $\forall r \in R$, r 或 $1-r$ 至少有一个为可逆元,
3. $m = \{r \in R : r\text{不是可逆元}\}$ 是 R 的 (极大) 理想.($\star$)

$3 \Longrightarrow 1$ R 的 $\forall$ 非零真理想 I 满足 $I \subset m$, 否则 $\exists$ 可逆元 $u \in I \Longrightarrow I = R$, 矛盾, 故 R 有唯一极大理想 m.

$1 \Longrightarrow 3$ 对 $\forall x \notin m$, 若 x 不可逆, 则 $(x) \subset$ 另一个极大理想, 矛盾.

$3 \Longrightarrow 2$ 由 $3 \Longrightarrow 1$ 得唯一极大理想为 3 中 m, 假设 $r, 1-r$ 都不是可逆元, 则 $r, 1-r \in m \Longrightarrow 1 \in m, m = R$, 矛盾.

$2 \Longrightarrow 3$ 对 $\forall x \in m$, 假设 $\exists r \in R$ 使得 rm 是可逆元, 即 $rx \notin m$, 即 $\exists y \in R$, 使得 $yrx = 1 \Longrightarrow x$ 是可逆元, 矛盾, 故 $rx \in m$. 对 $x_1, x_2 \in m$, 假设 $x_1 + x_2 \notin m$, 即 $\exists y \in R$, 使得 $y(x_1 + x_2) = 1$, 则 $yx_1 = 1 - yx_2$, 由于 $yx_1 \in m, yx_2 \in m \Longrightarrow yx_1$ 不可逆, 且 yx_2 不可逆 $\Longrightarrow 1 - yx_2$ 可逆, 矛盾.

例 13.3.1

1. 域是局部环, $m = \{0\}$,
2. $\mathbb{Z}$ 不说局部环, $m = (2), (3), (5), \cdots$

例 13.3.2

设 p 是 R 的素理想, $S = R \backslash p$(注意 S 封闭). 定义 $R_{(p)} = R[S^{-1}]$, $R_{(p)}$ 是局部环 (称为 R 是 p 处的局部环), 极大理想为 $m = \left\{\dfrac{a}{s} : a \in p, s \notin p\right\}$.

结论 13.3.2: 局部环与维数

1. 维数的局部性: R 任意环, $\dim R = \sup \dim R_{(m)}, m \in \mathrm{Spec}_m R$.
2. 局部 Noether 环的维数, R : 局部 Noether 环, m 是 R 唯一极大理想.

方法 1: Hilbert 多项式.

性质 13.3.3

$\dim_{R/m} R/m^n$ 是关于 n 的多项式 $H(n)$, n 足够大 (称为局部 Noether 环的 Hilbert 多项式) 且满足 $\dim R = \deg(H(n))$.

方法 2: $m-$ 准素理想的最小生成元.

定义 13.3.4: 准素理想

$j \subset R$ 是理想, $xy \in J \Longrightarrow x \in J$ 或 $y^n \in J, \exists n \in \mathbb{N}^*$.

定义 13.3.5: $m-$ 准素理想

设 R 是 Noether 环, $m \in \mathrm{Spec}_m R$, $\forall$ 理想 $m \supset I \supset m^n (\forall n \in \mathbb{N}^*)$ 都是准素理想, 称为 $m-$ 准素理想.

性质 13.3.6

$\dim R = \inf\{m - \text{准素理想生成元个数}\}$.

Chapter 14

Zariski 拓扑, 复方阵的 GIT 分类

14.1 Noether 环的局部化

命题 14.1.1

Noether 环的局部化是不是 Noether 环?

工具: 理想的扩张与局限.

定义 14.1.1: 理想的扩张与局限

考虑 $f: R \to R[S^{-1}], r \mapsto \frac{r}{1}$.

理想扩张 I^e**:** $I \to (f(I))$(理想同态像不一定是理想, $\mathbb{Z} \hookrightarrow \mathbb{Q}, I = (2)$).

$f^{-1}(J) \leftarrow J$(同态原像是理想): J^c : **理想局限**.

性质 14.1.2

设 J 是 $R[S^{-1}]$ 理想, $J = (J^c)^e$.

$f(f^{-1}(J)) \subset J \Longrightarrow (J^c)^e \subset J$. 下证: $J \subset (J^c)^e$.

对 $\forall x = \frac{r}{s} \in J$, 有 $\frac{r}{1} = \frac{r}{s} \cdot s \in J \Longrightarrow r \in f^{-1}(J) \Longrightarrow \frac{r}{1} \in f(f^{-1}(J))$. 由于 $\frac{1}{s} \in R[S^{-1}]$, 故 $\frac{r}{s} = \frac{r}{1} \cdot \frac{1}{s} \in (f(f^{-1}(J))) \Longrightarrow J \subset (J^c)^e$.

性质 14.1.3

$$\begin{aligned}\{R[S^{-1}]\text{中的理想}\} &\to \{R\text{中的理想}\}\\ J &\mapsto J^c = f^{-1}(J)\end{aligned}$$ 是单射.

若 $J^c = (J')^c$, 由性质14.1.2, $\underset{J}{\underset{\|}{(J^c)^e}} = \underset{J'}{\underset{\|}{(J'^c)^e}} \Longrightarrow$ 单射.

定理 14.1.4

若 R 是 Noether 环, 则 $R[S^{-1}]$ 是 Noether 环.

$$\begin{array}{ccccccccc} I_1 & \subset & I_2 & \subset\cdots\subset & I_n & \subset & I_{n+1} & R[S^{-1}]\text{中升链} \\ c\downarrow & & c\downarrow & & c\downarrow & & \downarrow c & \\ f^{-1}(I_1) & \subset & f^{-1}(I_2) & \subset\cdots\subset & f^{-1}(I_n) & \underset{\text{Noether 环}}{\overset{}{\underset{\uparrow}{=}}} & f^{-1}(I_{n+1}) & R\text{中升链} \end{array}$$

由于理想局限是单射, 且 $I_n^c = I_{n+1}^c \Longrightarrow I_n = I_{n+1} \Longrightarrow R[S^{-1}]$ 是 Noether 环.

作业 14.1

设 p 是 R 的素理想, S 是封闭的且 $p \cap S = \varnothing$, $(p^e)^c = p$.

作业 14.2

对一般理想 $I \subset R, (I^e)^c = I$ 是否成立?

14.2 Zariski 拓扑

注解 14.1

主要内容:

1. 代数集, 素谱, 极大谱上的 Zariski 拓扑,

2. 紧 Hausdorff 空间的任意拓扑结构可由 Zariski 拓扑诱导.

学科交叉: 交换代数, 拓扑学, 泛函分析.

课程思政: Zariski 拓扑的拓扑基

公理 14.2.1: 闭集公理

拓扑空间 (X,τ), X : 集合, τ : X 子集族.

1. $\varnothing, X \in \tau$,

2. τ 中元素任意交封闭,

3. τ 中元素有限并封闭.

τ 中的元素称为闭集.

定义 14.2.2: Zariski 拓扑

令 $\tau = \{C_i\}$, C_i 是 k^n 中代数集 $\longleftrightarrow$ 多项式 $\{p_i\}$ 共同零点.

1. 任意交 $\begin{array}{ccc} \bigcap\limits_{i\in A} C_i & \longleftrightarrow & \bigcup\limits_{i\in A} V(p_i) \\ \searrow & & \swarrow \\ & \text{方程联立} & \end{array}$,

2. 有限并 $\begin{array}{ccc} C_1\cup C_2\cup\cdots\cup C_n & \longleftrightarrow & V(p_1\cdots p_n) \\ \searrow & & \swarrow \\ & \text{多项式乘法} & \end{array}$

$\Longrightarrow$ 任意交, 有限并封闭.

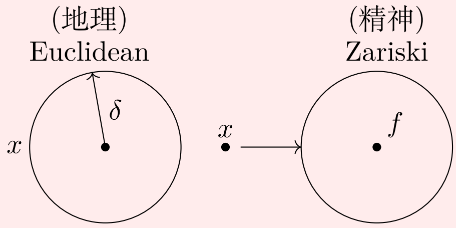
又 $\varnothing = Z((1)), k^n = Z((0))$ 是代数集 $\Longrightarrow \tau$ 满足闭集公理, 称为 Zariski 拓扑.

14.3 课程思政: Zariski 拓扑的拓扑基

注解 14.2

$\forall$ 开集 $U = \bigcup\limits_{b\in\mathcal{B}} b$, $\forall$ 给定 $\boxed{f} \in k[x_1,\cdots,x_n], U_f = \{x\in k^n : f(x)\boxed{\neq 0}\}$ 是 Zariski 拓扑基, 且 $\forall$ 开集 $U\subset k^n$ 是 U_f 的 $\underset{\text{Hilbert 基定理}}{\underset{\updownarrow}{\text{有限并}}}$.

$$\text{“}\overset{\uparrow}{\boxed{\text{德}}}\overset{\nearrow}{\boxed{\text{不孤}}}\text{, 必有}\boxed{\text{邻}}\text{”} \longleftrightarrow \boxed{\text{开邻域}}$$

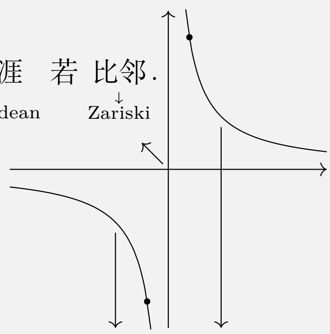


$$\left.\begin{array}{r}\text{给定}x \xrightarrow{\text{找}} f \in k[x_1, \cdots, x_n]\text{使得}f(x) \neq 0 \\ \Longrightarrow U_f\text{是}x\text{开邻域}\end{array}\right\} \text{借助“函数”构造开邻域}$$

例 14.3.1

$\mathbb{R}^2$ 中的集合 $\{(x, y) \in \mathbb{R}^2 : xy = 1\}$ 是 Zariski 拓扑下的闭集, 且是 $\underset{\substack{\Downarrow \\ \neq\text{真闭}\cup\text{真闭} \\ \neq\text{真闭}\sqcup\text{真闭}}}{\text{不可约}}$ 的 $\Longrightarrow$ 连通的.

海内存知己, $\underset{\substack{\downarrow \\ \text{Euclidean}}}{\text{天涯}}$ 若 $\underset{\substack{\downarrow \\ \text{Zariski}}}{\text{比邻}}$.



Zariski 下同一个连通分支

例 14.3.2

设 $A^{mn} = \{\text{线性变换} : k^m \to k^n\} = \{m \times n\text{矩阵}\} \cong k^{mn}$, $\{\text{非满秩矩阵}\}$ 是闭集 (所有 $i+1$ 阶子式为 0), $\{\text{满秩矩阵}\}$ 是开集.

14.4 GIT 等价与复方阵的分类

定义 14.4.1

Zariski 闭包: $X \subset \mathbb{A}^n, J(X) = \{f \in l[x_1, \cdots, x_n] : f(x) = 0, x \in X\} = (f_1, \cdots, f_m)$,
则 $\overline{X} = \bigcap V(f_i)$.

考虑群作用 $X \times G \to X$, X 是集合.

$x_1 \sim x_2 \overset{\text{def}}{\iff} x_1 G = x_2 G \iff x_1 G \cap x_2 G \neq \varnothing$

$X/G \overset{\text{def}}{=} X/\sim$

$x_1 \underset{\text{GIT}}{\sim} x_2 \overset{\text{def}}{\iff} \overline{x_1 G} \cap \overline{x_2 G} \neq \varnothing$

$X//G \overset{\text{def}}{=} X/\underset{\text{GIT}}{\sim}$

例 14.4.1: Jordan 标准形

$X = M_{n\times n} : n$ 阶复矩阵, $G = GL(n, \mathbb{C})$: 可逆复矩阵.

$$M_{n\times n} \times GL(n, \mathbb{C}) \to M_{n\times n}, (A, g) \mapsto g^{-1}Ag$$

$$X/G = \{M_{n\times n}\text{的所有 Jordan 标准形}\}, X//G = \{M_{n\times n}\text{所有对角矩阵}\}$$

当 $n = 2$, 比较 $\begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix} \cdot G \neq \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} \cdot G \in X/G$, 特征多项式均为 $(x-\lambda)^2$, 但极小多项式 $(x-\lambda)^2 \neq (x-\lambda) \Longrightarrow \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} \in \overline{\begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}}$.

$\Longrightarrow \begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix} \cdot G \subset X$ 不是闭子集, 且 $\overline{\begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} \cdot G} \cap \overline{\begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix} \cdot G} \neq \varnothing$

$\Longrightarrow \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} \cdot G = \begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix} \cdot G \in X//G$.

总结: 所有复矩阵在 GIT 等价意义下可由对角矩阵分类.

14.5 素谱上的 Zariski 拓扑

定理 14.5.1

R 是环, Spec$R = \{$素理想$\}$. 定义闭集: $\exists I \underset{\text{子集}}{\subset} R, Z(I) = \{p \in \text{Spec}R : p \supset I\}$ 构成闭集. 则 $(\text{Spec}R, \tau = \{Z(I) : I \subset R\})$ 构成拓扑空间, 称为 **Zariski 拓扑**.

注解 14.3

I 可不妨设为根理想, 即 $Z(I) \underset{1}{=} Z((I)) \underset{2}{=} Z(\sqrt{(I)})$.

$\overset{1}{\subset}, \overset{1}{\supset}, \overset{2}{\supset}$: 直接验证.

$\overset{2}{\subset}$: 对 $\forall p \supset I$, 满足 $\forall x \in \sqrt{(I)} \implies (I) \subset p \xrightarrow{\text{素理想}} x \in p \implies p \supset \sqrt{(I)} \implies Z(\sqrt{(I)}) \supset Z(I)$.

1. $\varnothing, \text{Spec}R \in I$. 验证: $Z(R) = \varnothing, Z(0) = \text{Spec}R$.
2. $\bigcap_{\alpha\in A} Z(I_\alpha) = Z\left(\sum_{\alpha\in A}(I_\alpha)\right)$, A 是指标集. 验证: $\forall p \in \bigcap_{\alpha\in A} Z(I_\alpha) \implies I_\alpha \subset p, \forall\alpha \in A \implies \sum_{\alpha\in A} \subset p \implies \bigcap_{\alpha\in A} Z(I_\alpha) \subset Z\left(\sum_{\alpha\in A} I_\alpha\right)$. $\forall p \in Z\left(\sum_{\alpha\in A} I_\alpha\right) \implies \forall\alpha \in A, I_\alpha \subset \sum_{\alpha\in A} I_\alpha \in p \implies p \in \bigcap_{\alpha\in A} Z(I_\alpha) \implies Z\left(\sum_{\alpha\in A} I_\alpha\right) \subset \bigcap_{\alpha\in A} Z(I_\alpha)$.
3. $\forall p \in Z(I_1) \cup Z(I_2)$, 不妨设 $p \in Z(I_1) \implies I_1 \subset p \implies I_1I_2 \subset p \implies Z(I_1) \cup Z(I_2) \subset Z(I_1I_2)$. $\forall p \in Z(I_1I_2), I_1I_2 \subset p \xrightarrow{\text{素理想}} I_1 \subset p$ 或 $I_2 \subset p \implies Z(I_1I_2) \subset Z(I_1) \cup Z(I_2)$.

注解 14.4

极大谱 $\text{Spec}_m R = \{R$中极大理想$\}$, 闭集: $\forall$ 给定 $I \subset R, V(I) = \{m : m \supset I$极大理想$\}$.

定理 14.5.2

令 $k = \underline{k}, R = k[x_1, \cdots, x_n]/I$, I 是根理想.

$$(\text{Spec}_m R, I_{\text{Zariski}}) \cong (V(I), I_{\text{Zariski}})$$
$$m = (x_1 - a_1, \cdots, x_n - a_n) \mapsto (a_1, \cdots, a_n)$$

14.6 拓扑基与开邻域

注解 14.5

$\star$ **借助“函数”找一点开邻域:**

$p \in \mathrm{Spec}R$ 的邻域: 找函数 $f \in R$ 使得 $f \notin p$,$p(f)$ 是 p 的一个邻域.

$\mathrm{Spec}R$ 上拓扑基: $\forall$ 给定 $f \in R$, $D(f) = \{p : f \notin p\}$.

Chapter 15

连续函数环, 素谱上的零点定理

15.1 Stone-Weierstrass 定理, 弱零点定理与 Zariski 拓扑的关系

定理 15.1.1: Stone-Weierstrass 定理

设 (K,τ_k) 是紧 Hausdorff 空间, $C(K,\mathbb{R})$ 是 K 上实连续函数构成的代数.

注解 15.1

$C(K,\mathbb{R})$ 是 Banach 空间, $\|f\|_\infty \overset{\text{def}}{=} \sup\limits_{x\in K}|f(x)|$.

设 $\mathcal{A}$ 是 $C(K,\mathbb{R})$ 的子代数, 若:

1. $\mathcal{A}$ 在 K 上是可分点的 (若 $x\neq y\in K, \exists f\in\mathcal{A}$ 使得 $f(x)\neq f(y)$).
2. 对 $\forall x\in K, \exists f\in\mathcal{A}$ 使得 $f(x)\neq 0$.

则 $\mathcal{A}$ 是 $C(K,\mathbb{R})$ 稠密的.

定理 15.1.2

设 I 是 $C(K)$ 的极大理想, $\exists$ 唯一 $x_0\in K$ 使得 $I=I_{x_0}$, 其中, $I_{x_0}\overset{\text{def}}{=}\underbrace{\{f\in C(K): f(x_0)=0\}}_{\text{极大理想}}$.

注解 15.2

该定理可以看作交换代数中 Stone-Weierstrass 定理, 亦可以看做 $C(K)$ 上的弱零点定理.

假设不存在 $x_0 \in K$ 使得 $\forall f \in I, f(x_0) = 0$, 令 $\mathcal{A} = I \cup \{1\}$, $\mathcal{A}$ 满足Stone-Weierstrass 条件 2, 下证: $\mathcal{A}$ 满足Stone-Weierstrass 条件 1. 假设 $I \subset \mathcal{A}$ 不可分点, 即 $i(x) = i(y), \forall x, y \in K$, 由 Urysohn 引理:
$\exists f \in C(K)$ 使得 $f(x) \neq f(y)$ 对 $\forall x \neq y \in K \Longrightarrow f \notin I$.

定理 15.1.3: Urysohn 引理

设 X 是 $T_4(\supset$ 紧 Hausdorff 空间) 拓扑空间, C, D 是 X 不交闭集, 则 $\exists$ 连续函数 $f : X \to R$, 使得 $f(x) \subset [0,1], f(C) = 0, f(D) = 1$.

由于 I 是理想, $f, i \in I \Longrightarrow f(x)i(x) = f(y)i(y) \Longrightarrow i(x) = i(y) = 0, \forall x, y \Longrightarrow I \subset I_{x,y} \stackrel{\text{def}}{=} \{g \in C(K) : g(x) = g(y) = 0\} \subsetneqq I_x$或$I_y$, 与 I 是极大理想矛盾. 故 $\mathcal{A}$ 可满足Stone-Weierstrass 条件 1.
由 Stone-Weierstrass 定理, $I \subset I \cup \{1\}$ 在 $C(K)$ 中稠密的, 则对 $\forall \varepsilon > 0, \exists f \in I$, 使得 $\|f - \underset{\text{常函数}}{\underset{\uparrow}{1}}\|_\infty < \varepsilon$. 取 $\varepsilon = \frac{1}{2}$, 则 f 没有零点 $\Longrightarrow \frac{1}{f} \in C(K)$, 则 $1 = \frac{1}{f} \cdot f \in I \Longrightarrow I = C(K)$, 矛盾.
最后证唯一性: 由Stone-Weierstrass 条件 1得 $\forall x_1 \neq x_2$, 有 $Ix_1 \neq Ix_2$.

注解 15.3

$K \underset{x \leftrightarrow I_x}{\overset{1-1}{\longleftrightarrow}} \mathrm{Spec}_m C(K) \Longrightarrow \mathrm{Spec}_m C(K)$ 上的 Zariski 拓扑结构可以通过双射在 K 上诱导拓扑结构 τ_m.

定理 15.1.4

$\tau_m = \tau_K$, 即 (K, τ_K) 与 $(\mathrm{Spec}_m C(K), \tau_{\text{Zariski}})$ 同胚.

取 K,τ_K 中开集 W, 证明 W 是 (K,τ_m) 拓扑基的开覆盖. 由 Urysohn 引理, $\forall x \in W, \exists f_x(x)=1$.

只需证 $W=\bigcup\limits_{x\in W} U(f_x)$ 开覆盖, 其中 $U(f)=\{x\in K: f(x)\neq 0\}=\{x\in K: f\notin I_x\}(\star)$

对 $\forall x\in W, x\in U(f_x)\Longrightarrow W\subset \bigcup\limits_{x\in W} U(f_x)$. 对 $y\in U(f_x)$, 假设 $y\notin W$, 则 $f_x(y)=0$, 矛盾. $y\in W$, $\bigcup\limits_{x\in W} U_f\subset W$.

15.2 素谱上的零点定理

定义 15.2.1: 素谱上的函数

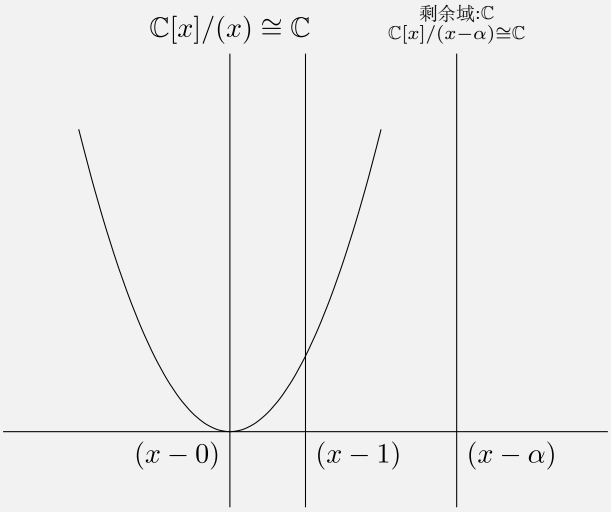
取值的域随 $p\in \mathrm{Spec}R$ 的变化而变化, 邻点取值的域为 $\mathrm{Frac}(R/p)$.⇝"移动靶"

$R\to R/p\to \mathrm{Frac}(R/p)$

$f\mapsto f+p\hookrightarrow f+p$

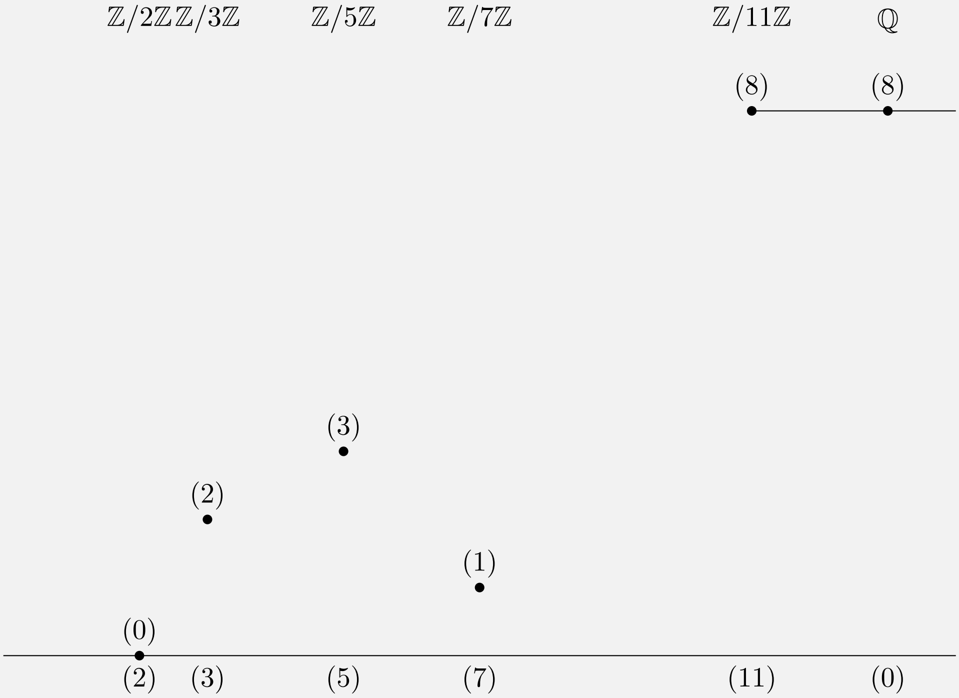
例 15.2.1

$R=\mathbb{C}[x], f=x^2\in R, f((x))=x^2+(x)=0, f((x-1))=x^2-1+1+(x-1)=1, f((x-\alpha))=x^2-\alpha^2+\alpha^2+(x-\alpha)=\alpha^2$.



例 15.2.2

$R=\mathbb{Z}, f=8, f((2))=0, f((3))=2, f((5))=3, f((7))=1, f((p))=8, p\geq 11, f((0))=8.$



定义 15.2.2: 零函数

考虑 "零函数": $\forall p\in \mathrm{Spec}R$, 若 $f\in R$, 使得 $f(p)=0$, 则称 f 是 $\mathrm{Spec}R$ 的零函数.

注解 15.4

对 $\forall p\in \mathrm{Spec}R, f(p)=0 \Longleftrightarrow f\in p, \forall p\in \mathrm{Spec}R \Longleftrightarrow f\in \bigcap\limits_{p\in \mathrm{Spec}R} p.$

结论 15.2.3: 素谱的零点定理

$\mathrm{Spec}R$ 的零函数为 R 的幂零根基, 即 $\sqrt{0}=\bigcap\limits_{p\in \mathrm{Spec}R} p$.($R$ 的幂零根基 $=\mathrm{Spec}R$ 的零函数.)

注解 15.5

$\underset{\{r\in R:\exists n\in\mathbb{N}^*,r^n=0\}}{\overset{\uparrow}{\text{幂零根基}}}$ 不一定是 $\underset{I\subset R,\exists n\in\mathbb{N}\text{使得}I^n=0}{\overset{\uparrow}{\text{幂零理想}}}$ (R 不是 Noether 环).

$R=k[x_1,x_2,\cdots,\underset{\text{可数}}{\infty}]/(x_1,x_2^2,x_3^3,\cdots)$, $\sqrt{0}=(x_1,x_2,x_3,\cdots)$, 然而 $(\sqrt{0})^n\neq 0,\forall n$(交叉项无法清零).

引理 1. 若 R 是 Noether 环, 理想 $I\subset R$, 则 $\exists n\in\mathbb{N}$ 使得 $(\sqrt{I})^n\subset I$.

证明 1. 由 R 是 Noether 环, $\sqrt{I}$ 有限生成, 设生成元为 $(a_1,\cdots,a_m)$, 则 $\exists k_i\geq 1$ 使得 $a_i^{k_i}\in I$. 令 $k=\max\{k_i\}$, 则对所有 i, $a_i^k\in I$. $\forall x\in\sqrt{I},x=\sum_{i=1}^m r_ia_i,r_i\in R,a_i\in\sqrt{I}$, 则 $x^{\underset{\text{足够大}}{\boxed{mk}}}\in(a_1^{i_1},\cdots,a_m^{i_m}:i_j\geq 0,i_1+i_2+\cdots+i_m=mk)\subset(a_1,\cdots,a_m^k)\subset I$.

性质 15.2.4

若 R 是 Noether 环, $\sqrt{0}$ 是幂零理想.

取 $I=0$ 得 $\exists n,(\sqrt{0})^n\subset 0\Longrightarrow(\sqrt{0})^n=0$.

定理 15.2.5: 素谱的零点定理

Spec$R$ 的零函数为 R 的幂零根基, 即 $\sqrt{0}=\bigcap_{p\in\mathrm{Spec}R}p$.($R$ 的幂零根基 =Spec$R$ 的零函数.)

引理 1. 设 S 是 R 的可乘子集, I 是 R 的理想使得 $I\cap S=\varnothing$, 则 $\exists$ 素理想 $p\supset I$ 使得 $p\cap S=\varnothing$.

证明 1. 设 p 是在包含关系下, 包含 I 且与 S 不交的极大元 (Zorn 引理保证极大元存在性). 下证 p 是素理想.

若 $ab\in p$, 则 $(p+(a))\cap\neq\varnothing$ 与 $(p+(b))\cap S\neq\varnothing$ 不可能同时成立 (否则由 S 可乘性, $p\cap S\neq\varnothing$). 不妨设 $(p+(a))\cap S=\varnothing$, 且 $I\subset p+(a)$. 由 p 的极大性得, $p=p+(a)\Longrightarrow a\in p$.

"$\sqrt{0}\subset\bigcap_{p\in\mathrm{Spec}R}p$":

对 $\forall p \in \mathrm{Spec}R$, 若 $a^n = a^{n-1} \cdot a = 0 \in p$, 则 $a \in p$ 或 $a^{n-1} \in p$, 以此类推可得 $a \in p$, 故 $\sqrt{0} \subset \bigcap\limits_{p \in \mathrm{Spec}R} p$.

"$\sqrt{0} \supset \bigcap\limits_{p \in \mathrm{Spec}R} p$"

假设 $\exists a \in \bigcap\limits_{p \in \mathrm{Spec}R} p$ 使得 $a \notin \sqrt{0}$. 令 $S = \{1, a, a^2, \cdots\}, I = \{0\}$, 则 $S \cap I = \varnothing$, 故 $\exists p \supset I$, 使得 $p \cap S = \varnothing \Longrightarrow a \notin p$, 矛盾. 因此, 对 $\forall a \in \bigcap\limits_{p \in \mathrm{Spec}R} p$ 有 $a \notin \sqrt{0}$.

作业 15.1

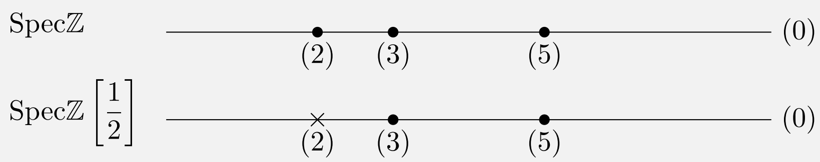
对 $\forall$ 理想 I, $\sqrt{I} = \bigcap\limits_{素理想 p \supset I} p.(0 \longleftrightarrow I)$

15.3 环局部化的素谱

性质 15.3.1

$\mathrm{Spec}R[S^{-1}] \cong \{p \in \mathrm{Spec}R : p \cap S = \varnothing\}$.

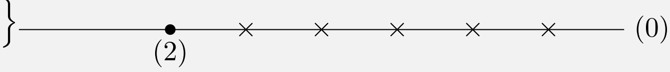
例 15.3.1



例 15.3.2

局部环 $R_{(p)} \overset{\text{def}}{=} R[(R \backslash p)^{-1}]$.

$\mathrm{Spec}\mathbb{Z}_{(2)} = \left\{\frac{a}{b} : b \in 奇数, a \in \mathbb{Z}\right\}$



注解 15.6: $R_{(p)}$ **vs** R/p

性质 15.3.2

$$\mathrm{Spec} R/p \longleftrightarrow \{p' \in \mathrm{Spec} R : p' \supset p\} \left(\overset{\text{def}}{=} \overline{\{p'\}}^{\overset{\text{Zariski}}{\uparrow}} \right)$$

(当 $p = (0)$, $\mathrm{Spec} R/(0) \cong \mathrm{Spec} R = \overline{(0)}$)

$\mathrm{Spec} R_{(p)} \longleftrightarrow \{p' \in \mathrm{Spec} R : p' \subset p\}$

(当 p 是极大理想 $\longleftrightarrow$ 孤立点 $\cup$ 泛点)

Chapter 16

范畴与函子

16.1 高阶强零点定理 (Nagata,Zariski)

定义 16.1.1

$x = V(p)$ 是代数簇, p 是素理想. $p^{\langle n \rangle} \overset{\text{def}}{=} \{f \in k[x_1, \cdots, x_m] : \dfrac{\partial^{n-1}}{\partial x_{i_1} \cdots \partial x_{i_{n-1}}}(x) = 0, 所有 x \in X, i_1, \cdots, i_{n-1} \in \{1, 2, \cdots, m\}\}$.

注解 16.1

$n = 1, p^{\langle 1 \rangle} : I(X)$ 是**素理想**.

命题 16.1.1

如何等价描述 $p^{\langle n \rangle} \rightsquigarrow$ 符号幂.

定义 16.1.2

$p : k[x_1, \cdots, x_n]$ 的素理想, $p^{(n)} \overset{\text{def}}{=} \{x \in k[x_1, \cdots, x_m] : \exists y \notin p, 使得 xy \in p^n\}$ 称为 p 的 n 次符号幂.

定理 16.1.3: Nagata-Zariski 定理

设 k 是代数闭域, $p^{\langle n\rangle}=p^{(n)}$.

定理 16.1.4: 有效零点定理

设 $I(F_1,\cdots,F_r),F_i$ 阶数为 d_i, 由 Hilbert 强零点定理, $\forall g\in I(V(I))=\sqrt{I}$, $\exists$ 最小 $n\in\mathbb{N}^*$ 使得 $g^n\in I$.

命题 16.1.2: 公开问题

n 能否由 d_i 控制?

定理 16.1.5: JAMS,1988

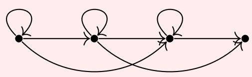
若 $d_1=d_2=\cdots=d_r\geq 2$, 则 $n\leq d_1\cdots d_r$.

16.2 范畴

注解 16.2: 范畴

范畴 C 的三要素

1. 对象类: ObC, • • • • • • •

2. 态射类: $\hom(C)$, 态射 $f\in\hom C\overset{\text{def}}{\Longleftrightarrow}$ 存在唯一源对象 $a\in\mathrm{Ob}C$ 和靶对象 $b\in\mathrm{Ob}C$, 使得 $f:a\to b$.($\hom C=\bigcup\limits_{a,b\in\mathrm{Ob}C}\underset{(\text{二元运算})}{\hom(a,b)}$)  3. 合成: 对 $\forall a,b,c\in\mathrm{Ob}C$, $\begin{array}{c}\hom(a,b)\times\hom(b,c)\to\hom(c,a)\\(f,g)\mapsto g\circ f\end{array}$, 满足结合律 $f\in\hom(a,b),g\in\hom(b,c),h\in\hom(c,d)$, 则 $h\circ(g\circ f)=(h\circ g)\circ f$. $\exists\mathrm{id}_a\in\hom(a,a)$ 使得 $\forall f\in\hom(b,a),g\in\hom(a,c)$ 有 $\mathrm{id}_a\circ f=f,g\circ\mathrm{id}_a=g$.

例 16.2.1

群范畴: 对象: 半群, 态射: 群同态

环范畴: 对象: 环, 态射: 环同态 (有交换环中同态定义 $(1\to 1)$ 保证了环同态是态射)

模范畴: 对象: 模, 态射: 模同态

向量空间范畴: 对象: 向量空间态射: 线性映射

例 16.2.2

代数集: $\underset{\star\text{几何}}{X \subset k^n} \xleftrightarrow{1-1}$ 根理想 $I \subset k[x_1, \cdots, x_n] \xleftrightarrow{1-1} \mathcal{A} = \underset{\star\text{代数}\to\text{函数环}}{k[x_1, \cdots, x_n]/I}$

代数集范畴 $\longleftrightarrow \sqrt{0} = 0$且有限生成代数范畴

$\updownarrow$

对象	代数集	约化仿射代数
态射	正则映射 $\overset{\text{def}}{=} X \to Y \subset k^m$ 使得 每一个分量投影 $X \to k$ 都是多项式函数	代数同态
合成	正则映射的复合	代数同态的复合

16.3 函子

定义 16.3.1: 反变函子

C, D 是范畴, $\mathcal{F} : C \to D$ 称为反变函子, 如果 $\mathcal{F}$ 满足:

1. $\mathcal{F}$ 是对象类之间良定义的映射 (即对 $a \in \mathrm{Ob}C$, $\exists$ 唯一的 $\mathcal{F}(a) \in \mathrm{Ob}D$)

2. 对 $f \in \hom(a, b)(a, b \in \mathrm{Ob}C)$, 存在唯一 $\mathcal{F}(f) \in \hom(\mathcal{F}(b), \mathcal{F}(a))$(源靶对调) 使得

(a) 对 $\forall a \in \mathrm{Ob}C$, $\mathcal{F}(\mathrm{id}_a) = \mathrm{id}_{G(a)}$,

(b) 对 $f \in \hom(a, b), g \in \hom(b, c)$, $(g \circ f) = \mathcal{F}(f) \circ \mathcal{F}(g)$(反变)

$$\begin{tikzcd} A \arrow[r, "g\circ f"] \arrow[d, "f"'] & C \\ B \arrow[ur, "g"'] & \end{tikzcd} \qquad \begin{tikzcd} \mathcal{F}(A) & \mathcal{F}(C) \arrow[l, "\mathcal{F}(g\circ f)"'] \arrow[dl, "\mathcal{F}(g)"] \\ \mathcal{F}(B) \arrow[u, "\mathcal{F}(f)"] & \end{tikzcd}$$

注解 16.3

1. C(代数集)$\to C$(约化仿射代数)

$\mathcal{F}: \quad X \mapsto k[x_1, \cdots, x_n]/I(X)$

$\qquad \varphi \mapsto \varphi^*$是反变函子

$\downarrow$

定义 16.3.2: 拉回映射

X, Y : 定义域, k : 值域
$k[X] \overset{\text{def}}{=} \{f : X \to k\}$
$k[Y] \overset{\text{def}}{=} \{f : Y \to k\}$
$\varphi : X \to Y \underset{\text{诱导}}{\rightsquigarrow} \overset{\varphi^* : \mathcal{Y} \to \mathcal{F}(X)}{(\varphi^*(f))(x) \overset{\text{def}}{=} f(\varphi(x))}$, 称为$\varphi$的拉回.

令 X, Y 是代数集, k 是代数闭域, $k[X] = k[x_1, \cdots, x_n]/I(X), k[Y] = k[y_1, \cdots, y_n]/I(Y), \varphi : X \to Y \rightsquigarrow \varphi^* : k[X] \to k[Y]$.

2.

定义 16.3.3: 协变函子

若定义中 $\mathcal{F}(f) \in \hom(\mathcal{F}(a), \mathcal{F}(b))$(不对调), $\mathcal{F}(g \circ f) = \mathcal{F}(g) \circ \mathcal{F}(f)$, 即

$$\begin{tikzcd} A \arrow[r, "g \circ f"] \arrow[d, "f"'] & C \\ B \arrow[ur, "g"'] & \end{tikzcd} \qquad \begin{tikzcd} \mathcal{F}(A) \arrow[r, "\mathcal{F}(g \circ f)"] \arrow[d, "\mathcal{F}(f)"'] & \mathcal{F}(C) \\ \mathcal{F}(B) \arrow[ur, "\mathcal{F}(g)"'] & \end{tikzcd}$$

则称 $\mathcal{F} : C \to D$ 为协变函子.

例 16.3.1

C(拓扑空间基点)	C(群)
$\text{Ob}C : (X, X_0)$	$\text{Ob}C : G$
$\hom_C$: 连续映射$\varphi : X \to Y$使得$\varphi(x_0) = y_0$	$\hom_C$: 群同态$G \to H$

$\mathcal{F} : \begin{array}{c} (X, x_0) \mapsto \pi_1(X, x_0) \\ \varphi : \varphi_* \end{array}$ 是协变函子.

$(x_0$ 的环路 $\underset{\varphi}{\rightsquigarrow} y_0$ 的环路 $\underset{\text{同伦等价类}}{\rightsquigarrow} \varphi_*(\pi_1(X, x_0)) \subset \pi_1(Y, y_0))$

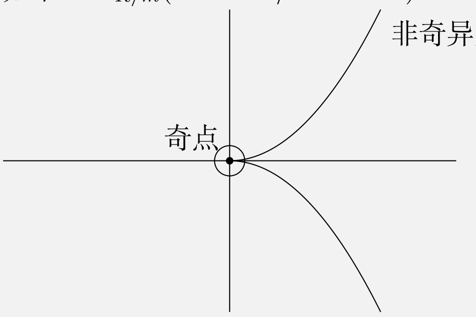
16.4 维数理论与离散赋值环

16.4.1 维数的局部性

定义 16.4.1: 正则局部环与奇点

R 任意环, $\dim R = \sup \dim R_{(m)}, m \in \mathrm{Spec}_m R$. Noether 局部环 (R, m) 称为正则的,

如果 $\dim_{R/m}(\overset{\text{Hilbert 零点}m\text{处余切空间}p}{\overset{\uparrow}{m/m^2}}) = \dim R$.



注解 16.4

1. 对一般 Noether 局部环, $\dim R \leq \dim_{R/m}(m/m^2)$(Nakayama),
2. 代数集 R 中点 m 是奇点 $\Longleftrightarrow$ $(R_{(m)}, \tilde{m})$ 是局部正则环, $\tilde{m} = \left\{\dfrac{r}{s} : r \in m, s \notin m\right\} \subset R_{(m)} \cong m$.

例 16.4.1

$k[x,y]/(y^2 - x^3)$, 考虑 $(0,0)$ 处局部环, $R = k[x,y]_{\underset{\text{奇点}}{\underset{\uparrow}{(x,y)}}}/(y^2 - x^3)$, $m = (x,y), \dim_k m/m^2 = 2, \dim R = 1$.

16.4.2 离散赋值环 DVR

定义 16.4.2

非域整环 R 称为 **DVR**, 若满足下面等价条件

(R, m) 是 Noether, 且 m 是主理想 (t)

$\Longleftrightarrow$ $\exists$ 不可约元 $t \in R$, 使得 $\forall$ 非零 $z \in R$ 可以写成 $z = ut^n$, u 是单位, $n \in \mathbb{N}$(z 的赋值), t 称为 R 的单值化参数.

注解 16.5

$$v : \mathrm{Frac} R \to \mathbb{Z} \cup \{\infty\} : \begin{cases} v(0) = \infty \\ v(ut^n) = n \end{cases} \quad \text{称为赋值映射.}$$

定理 16.4.3: DVR 几何意义

$k = \bar{k}$, 不可约曲线 $f \in k[x, y]$ 在点 $\underset{m}{\overset{k[x,y]/(f)\text{极大理想}}{\Updownarrow}}$ 光滑 $\Longleftrightarrow k[x, y]_{(m)}/(f)$.

参考文献

[抽象代数, 邓少强] 邓少强, 朱富海编著. 抽象代数 [M]. 北京：科学出版社, 2017.06.