



代数学笔记

作者：吕浩哲 (Lucas Shen)

时间：January 7, 2024

封面：<https://www.pixiv.net/artworks/100631860>

悟已往之不谏，知来者之可追。——陶渊明

目录

第 1 章	Galois 理论	1
1.1	分裂域	1
1.1.1	同构延拓定理	1
1.1.2	嵌入理论	2
1.2	可分扩张与正规扩张	3
1.2.1	可分扩张	3
1.2.2	正规扩张	4
1.3	Galois 扩张与 Galois 基本定理	5
1.3.1	Galois 基本定理	5
1.3.2	三次方程求根公式	7
1.4	Galois 理论的一些应用	8
1.4.1	单扩张	8
1.5	迹和范数	9
1.5.1	基本定义	9
1.5.2	Hilbert 90 定理	11
第 2 章	模论	13
2.1	基本概念	13
2.1.1	模的定义	13
2.1.2	单模与合成列	14
2.1.3	直和与直积	16
2.2	正合列	17
2.3	自由模、投射模与内射模	21
2.3.1	自由模	21
2.3.2	投射模 (projective)	22
2.3.3	内射模 (injective)	23
2.4	张量积	26
2.4.1	张量积的定义和性质	26
2.4.2	张量函子与平坦模	27
2.4.3	基变换	29
2.5	PID 上有限生成模的结构	30
2.5.1	矩阵的标准形理论	32
第 3 章	交换代数初步	34
3.1	Noether 环与 Artin 环	34
3.1.1	Noether 环与 Noether 模	34
3.1.2	Artin 环与 Artin 模	35
3.2	局部化	36
3.2.1	环的局部化	36
3.2.2	模的局部化	37
3.2.3	理想的局部化	38
3.2.4	局部环	39

3.3	整扩张	41
3.3.1	整性与有限	41
3.3.2	正规扩张	42
3.3.3	有限性定理	42
3.4	Noether 正规化定理	43
第 4 章	有限群表示论	45
4.1	群的表示	45
4.1.1	群同态语言下的群表示	45
4.1.2	$F[G]$ -模语言下的群表示	47
4.2	半单代数	49
4.2.1	半单代数	49
4.2.2	可除代数	50
4.2.3	群表示语言下的应用与重述	52
4.3	表示的提升与分解	53
4.4	特征标理论	54
4.4.1	特征标的定义及性质	54
4.4.2	正交关系	55
4.4.3	特征标表的计算	57
4.4.4	特征标表的其它应用	59
4.5	Burnside 定理	61
4.5.1	代数整数的一些结论	61
4.5.2	Burnside 定理	62
4.6	诱导表示	62
4.6.1	诱导表示与诱导特征	62
4.6.2	借助诱导表示计算特征标表	65
附录 A	补充内容	66
A.1	Galois 下降	66
A.2	交换代数前置补充	66

第1章 Galois 理论

1.1 分裂域

定义 1.1 (分裂域)

设 $E/F, f(x) \in F[x]$, 若 f 在 E 中的不可约因子均为一次多项式, 则称 $f(x)$ 在 E 中分裂; 若 $f(x)$ 在任何 E, F 的中间域中都不能分裂, 则称 E 为 f 的分裂域.



换句话说, E 为 $f \in F[x]$ 的分裂域说明其包含了 f 全部的根, 因此若设 f 在代数闭域 $\bar{F}$ 中的根为 $\alpha_1, \dots, \alpha_n$, 则 $F(\alpha_1, \dots, \alpha_n)$ 就是其代数闭域. 下面给出分裂域存在性的另一个证明.

定理 1.1

设 F 为域, $f(x) \in F[x]$ 为非常值多项式, 则 f 存在分裂域, 并且它们在同构意义下唯一.



证明 存在性: 对 f 的次数归纳, $\deg f = 1$ 的情形是平凡的. 设命题对所有 $\deg f < d$ 的 f 成立, 则对 $\deg f = d$, 存在域 B 使得 f 在 B 中有根 α_1 , 即 f 在 B 有分解 $f(x) = (x - \alpha_1)g(x)$, 这里 $\deg g = d - 1$, 根据归纳假设, g (关于 B) 存在分裂域 E_1 , 且在 E_1 中有分解

$$g(x) = (x - \alpha_2) \cdots (x - \alpha_k), \quad (1.1)$$

即 f 在 $B(\alpha_2, \dots, \alpha_k)$ 中分裂, 并且不能在更小的域中分裂 (否则与 E_1 的极小性矛盾), 故

$$B(\alpha_2, \dots, \alpha_k) = F(\alpha_1, \dots, \alpha_k) \quad (1.2)$$

为 f 的分裂域, 得证.

唯一性的证明需要一些引理, 这里先考虑一些分裂域的性质.

命题 1.1

1. 设 E 为 $f(x) \in F[x]$ 的分裂域, 则 E/F 为有限扩张, 从而是代数扩张.
2. 设 $f(x) \in F[x]$ 非常值, E 为其分裂域, $\deg f = d$, 则 $[E : F] \leq d!$, 特别当 f 不可约时, $d \mid [E : F]$.



1.1.1 同构延拓定理

代数中的同构往往表示两个外表不同的对象具有相同的结构, 它们实际上只是相同的模型贴上了不同的标签, 在此基础上, 同构延拓定理表明两个同构域上在对应标签的衍生结构 (如扩域) 也具有同构关系.

引理 1.1 (向单扩张域延拓)

设 $\sigma_0 : F_1 \rightarrow F_2$ 为域同构, $f_1(x) \in F_1[x]$ 不可约, $f_2(x) = \sigma_0(f_1(x)) \in F_2[x]$, 且 α_1, α_2 分别是 f_1, f_2 的一个根, 则 σ_0 可以延拓为 (或者说唯一诱导出) 域同构 $\sigma : F_1(\alpha_1) \rightarrow F_2(\alpha_2)$ 的域同构, 使得 $\sigma(\alpha_1) = \alpha_2$.



推论 1.1

设 $f(x) \in F[x]$ 不可约, α_1, α_2 为 f 的两个根, $E_i = F(\alpha_i)$, 则存在唯一同构 $\sigma : E_1 \rightarrow E_2$ 使得 $\sigma(\alpha_1) = \alpha_2, \sigma|_F = \text{Id}$.



定理 1.2 (向分裂域延拓)

设 $\sigma_0 : F_1 \rightarrow F_2$ 为一个域同构, $f_1(x) \in F_1[x]$ 不可约, $f_2(x) = \sigma_0(f_1(x)) \in F_2[x]$, E_1, E_2 分别为 f_1, f_2 的分裂域, 则 σ_0 可以延拓为域同构 $\sigma : E_1 \rightarrow E_2$.



证明 设 f_1 在 $F_1[x]$ 中分解为 k 个不可约因子之积, 令 $d_F(f_1) = \deg f_1 - k$, , 当 $d_F(f_1) = 0$ 时结论显然成立 (这时 $E_i = F_i, \sigma = \sigma_0$), 若 $d_F(f_1) > 0$, 则其存在次数大于 1 的不可约因子 $g_1(x)$, 设 α_1, α_2 分别为 g_1, g_2 在 E_1, E_2 中的根, 则根据延拓定理, σ_0 可以先延拓为域同构

$$\sigma_1 : F_1(\alpha_1) \rightarrow F_2(\alpha_2), \sigma_1(\alpha_1) = \alpha_2, \quad (1.3)$$

设 $B_i = F_i(\alpha_i)$, 则 $f_1(x) \in F[x] \subset B[x]$, 这时 $d_B(f_1) < d_F(f_1)$, E_i 可以看作 $B_i[x]$ 上 f 的分裂域, 因此由归纳假设, σ_1 可以延拓为域同构 $\sigma : E_1 \rightarrow E_2$, 得证.

上述延拓定理可以通过下图理解

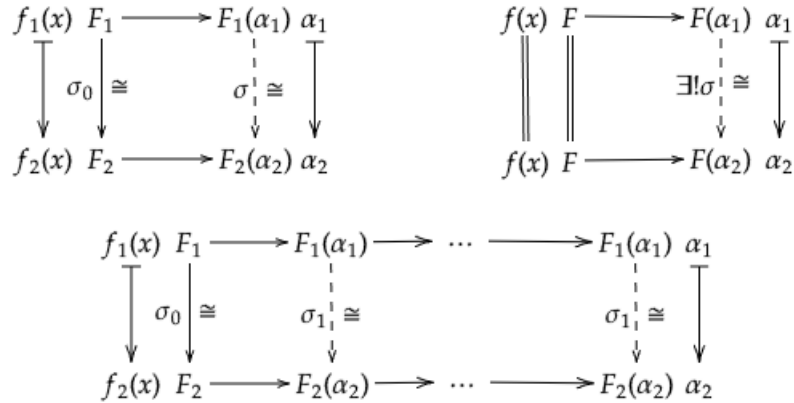


图 1.1: 同构延拓

借助延拓定理易证分裂域唯一性.

推论 1.2 (分裂域的同构唯一性)

设 $f(x) \in F[x]$, 则 f 的任何分裂域均相互同构.



1.1.2 嵌入理论

定义 1.2 (F -嵌入)

设 E/F 为域, $\bar{F}$ 为其代数闭域, 若单同态 $\sigma : E \rightarrow \bar{K}$ 满足 $\sigma|_F = \text{Id}$, 则称 σ 为 E 到 $\bar{F}$ 的一个 F -嵌入, 并且称 $\sigma(E)$ 与 E 共轭.



首先考虑单扩张的情形, 设 $E = F(\alpha), \alpha \in \bar{F}$, 那么任一 F -嵌入 $\sigma : E \rightarrow \bar{F}$, 必定将 α 映为 m_α 的另一个根; 反之根据延拓定理, 对 m_α 的两个根 α, α' , 存在唯一同构使得 $F(\alpha) \cong F(\alpha')$, 因此可得有如下引理

引理 1.2

设 $E = F(\alpha)$ 为单扩张, 则 E 到 $\bar{F}$ 的 F -嵌入的个数等于 m_α 在 $\bar{F}$ 中不同根的个数, 因此小于 $\deg m_\alpha = [E : F]$, 等号成立当且仅当 E/F 为可分扩张 (或者说 u 为可分元, 可分的概念在后面给出).



该引理可以归纳推广到有限扩张的情形

推论 1.3 (有限扩张的 F -嵌入)

设 E/F 为有限扩张, 则 E 到 $\bar{F}$ 的 F -嵌入的个数小于 $[E : F]$, 等号成立当且仅当 E/F 为可分扩张.



根据上面定理的取等条件, 可以引出可分的概念.

定义 1.3 (可分性)

1. 称 $f(x) \in F[x]$ 为可分多项式, 若其任意不可约因子都没有重根.
2. 设 E/F 为代数扩张, 称 $\alpha \in E$ 为可分元, 若其在 F 中的极小多项式 $m_\alpha(x)$ 可分.
3. 称代数扩张 E/F 为可分扩张, 若任何 $\alpha \in E$ 都是可分元.



注 由于极小多项式本身不可约, 因此 α 为可分元当且仅当 m_α 无重根.

1.2 可分扩张与正规扩张

1.2.1 可分扩张

引理 1.3

设 $E/F, f(x) \in F[x], \alpha \in E$ 使得 $f(\alpha) = 0$, 则 α 为 f 的单根当且仅当 $f(\alpha) = 0, f'(\alpha) \neq 0$.



证明 设 $f(x) = (x-\alpha)g(x)$, 则 $f'(x) = (x-\alpha)g'(x) + g(x) \Rightarrow f'(\alpha) = g(\alpha)$. 若 α 为 f 的单根, 则 $f'(\alpha) = g(\alpha) \neq 0$; 反之若 $f'(\alpha) \neq 0$ 则 $g(\alpha) \neq 0$, 因此 $x - \alpha \nmid g(x)$, 即 α 为 f 的单根.

命题 1.2

设 $f(x) \in F[x]$ 不可约, 若 $f'(x) \neq 0$, 则 $f(x)$ 可分. 进一步有

1. 若 $\text{char } F = 0, f(x) \in F[x]$ 不可约且 $f'(x) \neq 0$, 则 f 可分.
2. 若 $\text{char } F = p, f(x) \in F[x]$ 不可约, 则 f 可分 ($f'(x) \neq 0$) 或存在 $g(x) \in F[x]$ 使得 $f(x) = g(x^p)$.



证明 设 E 为 f 的分裂域, $\alpha \in E$ 为 f 的根, 则 f 不可约说明 $f(x) = m_\alpha(x)$, 并且 $f'(\alpha) \neq 0$ (否则与极小性矛盾), 故 α 为 f 的单根, 因此 f 可分. $\text{char } F = p$ 的情形也是显然的.

称 E/F 为可分扩张当且仅当对任意 $\alpha \in E, m_\alpha(x) \in F[x]$ 均可分, 借助上面的命题可得

推论 1.4 (零特征域上的代数扩张可分)

若 $\text{char } F = 0$, 则 F 的任何代数扩张均可分.



证明 设 E/F 为代数扩张, 则对任意 $\alpha \in E, m_\alpha(x) \in F[x]$ 无重根, 因此 E/F 可分.

定义 1.4 (完全域 (perfect field))

称域 F 为完全域, 若其任何代数扩张均为可分扩张.



注 前述推论说明任何零特征域均为完全域.

下面给出一个 p 特征域的完全性判别法, 首先考虑一个引理.

引理 1.4

设 $\text{char } F = p, a \in F, a \notin F^p$, 则对任意 $t \geq 1, f(x) = x^{p^t} - a \in F[x]$ 不可约.



证明 作不可约分解 $f(x) = g_1(x) \cdots g_k(x) \in F[x]$, 设 $g_1(\alpha) = 0, E = F(\alpha)$, 则 $g_1 = m_\alpha$, 进一步

$$f(x) = x^{p^t} - a = (x - \alpha)^{p^t} \in E[x], \quad (1.4)$$

由于每个 $g_i \mid f$, 因此 g_i 均为 $x - \alpha$ 的幂, 故 $g_1 \mid g_i$, 将上面的讨论对 $g_2, \dots, g_k$ 进行, 可得 $g_1 = \cdots = g_k = g$, 即 $f(x) = g(x)^k$, 因此

$$f(x) = (x - \alpha)^{p^t} = (x - \alpha)^{jk}, \quad (1.5)$$

设 $j = p^s, k = p^{t-s}$, 若 $t - s \neq 0$ 则

$$g(x) = (x - \alpha)^{p^s} \in F[x] \Rightarrow g(x)^{p^{t-s-1}} = (x - \alpha)^{p^{t-1}} = x^{p^{t-1}} - \alpha^{p^{t-1}} \in F[x], \quad (1.6)$$

因此 $b = \alpha^{p^{t-1}} \in F$, 此时 $b^p = \alpha^{p^t} = a$, 与 $a \notin F^p$ 矛盾, 因此 $t = s, k = 1$, 即 $f = g$ 不可约.

定理 1.3

F 为完全域当且仅当 $\text{char } F = 0$ 或 $\text{char } F = p$ 且 $F = F^p = \{a^p : a \in F\}$.



证明 设 E/F 为代数扩张, 若 $\text{char } F = p, F = F^p$, 则对任意 $\alpha \in E, m_\alpha(x) \in F[x]$, 若 $m'_\alpha \neq 0$, 则 m_α 可分; 若 $m'_\alpha = 0$ 则设 $m_\alpha(x) = \sum_{i=0}^k c_i x^{ip}$, 由于 $F = F^p$, 存在 $d_i^p = c_i$, 即

$$m_\alpha(x) = \sum_{i=0}^k c_i x^{ip} = \sum_{i=0}^k (d_i x^i)^p = \left(\sum_{i=0}^k d_i x^i \right)^p, \quad (1.7)$$

这与 m_α 的不可约性矛盾, 故 E/F 可分.

反之设 F 为完全域, $\text{char } F = p$, 假设存在 $a \in F, a \notin F^p$, 则考虑 $f(x) = x^p - a \in F[x]$, 由引理得 $f(x)$ 不可约, 设 α 为 f 的根, 则 $f(x) = (x - \alpha)^p$, 它有重根, 与 $F(\alpha)/F$ 的可分性矛盾.

推论 1.5

任何有限域都是完全域.



证明 设 F 为有限域, $\text{char } F = p$, 考虑 Frobenius 自同态 $\Phi : F \rightarrow F, \Phi(a) = a^p$, 则 $\text{Im } \Phi = F^p \leq F$, 对任意 $a, b \in F, a \neq b$ 说明 $\Phi(a) - \Phi(b) = \Phi(a - b) \neq 0$, 故 Φ 为单射, 即 $|\text{Im } \Phi| = |F|, F^p = F$, 即 F 为完全域.

1.2.2 正规扩张

定义 1.5 (正规扩张)

称代数扩张 E/F 为正规扩张, 若任何在 E 中有根的多项式 $f(x) \in F[x]$ 都在 E 中分裂.



注 容易验证正规扩张的等价定义: 任意 $\alpha \in E$ 在 F 中的极小多项式 $m_\alpha(x)$ 在 E 中分裂.

显然, 借助分裂域进行的扩张必然正规. 下面的定理给出了有限正规扩张的具体刻画.

定理 1.4

设 E/F 为有限代数扩张, 则下述命题等价:

1. E/F 为正规扩张.
2. E 为某个 $f(x) \in F[x]$ 的分裂域.
3. E/F 是共轭封闭的, 即对 $\bar{F}$ 中任意 F -嵌入 $\sigma : E \rightarrow \bar{K}$ 都有 $\sigma(E) = E$.



证明 $1 \Rightarrow 2$: 设 $E = F(\alpha_1, \dots, \alpha_n)$, 则 $f(x) = m_{\alpha_1}(x) \cdots m_{\alpha_n}(x)$ 在 E 中分裂 (每个 $m_{\alpha_i} \in F[x]$), 并且不存在更小的中间域 E' 使之分裂 (否则 E' 须包含 $\alpha_1, \dots, \alpha_n$), 即得.

$2 \Rightarrow 3$: 设 f 的根为 $\alpha_1, \dots, \alpha_n$, 则 $E = F(\alpha_1, \dots, \alpha_n)$, 其分裂域性质说明 σ 将每个根 α_i 映为另一个根 α_j , 因此 $\sigma(E) = E$.

$3 \Rightarrow 1$: 若不然, 则存在 $\alpha \in E$ 使得 $m_\alpha \in F[x]$ 存在一个不在 E 中的根 α' , 根据延拓定理有下图成立

其中 E' 与 E 同构, 但 E/F 的共轭封闭性说明 $\sigma(E) = E' = E$, 因此 $\alpha' \in E$, 矛盾.

从上面的共轭封闭性可以理解“正规”的来源, 一个群的正规子群只有其自身一个共轭类, 正规扩张也说明其只有其一个共轭类.

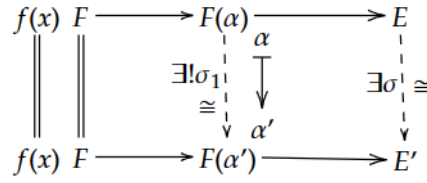


图 1.2: 同构延拓

1.3 Galois 扩张与 Galois 基本定理

1.3.1 Galois 基本定理

定义 1.6 (Galois 群)

设 E/F , 定义 $\text{Gal}(E/F) = \{\sigma \in \text{Aut}(E) : \forall x \in F, \sigma(x) = x\}$, 即 E 上的 F -自同构.

定义 1.7 (固定子域)

设 $S \subset \text{Aut}(E)$, 定义 $\text{Fix}(S) = \{a \in E : \forall \sigma \in S, \sigma(a) = a\}$.

容易验证 Galois 群确实是一个群, 固定子域也确实是一个域. 另外由定义可以看出, Galois 群与固定子域存在互逆关系, 易证它们有如下性质

命题 1.3

设 $F, F_1, F_2 \leq E; G, G_1, G_2 \leq \text{Aut}(E)$, 则

1. 若 $G_1 \leq G_2$ 则 $\text{Fix}(G_1) \geq \text{Fix}(G_2)$; 若 $F_1 \leq F_2$ 则 $\text{Gal}(E/F_1) \geq \text{Gal}(E/F_2)$.
2. $F \leq \text{Fix}(\text{Gal}(E/F))$, $G \leq \text{Gal}(E/\text{Fix}(G))$.
3. $\text{Gal}(E/\text{Fix}(\text{Gal}(E/F))) = \text{Gal}(E/F)$, $\text{Fix}(\text{Gal}(E/\text{Fix}(E/F))) = \text{Fix}(E/F)$.

证明

1. 这是显然的.
2. 这是显然的.
3. 令 $G = \text{Gal}(E/F)$, 由 2 直接得到

$$\text{Gal}(E/F) \leq \text{Gal}(E/\text{Fix}(\text{Gal}(E/F))), \quad (1.8)$$

另一方面

$$F \leq \text{Fix}(\text{Gal}(E/F)) \Rightarrow \text{Gal}(E/F) \geq \text{Gal}(E/\text{Fix}(\text{Gal}(E/F))), \quad (1.9)$$

故 $\text{Gal}(E/\text{Fix}(\text{Gal}(E/F))) = \text{Gal}(E/F)$, 另一个同理.

下面定义 Galois 扩张, 首先考虑定理

定理 1.5 (Galois 判定定理)

设 E/F 为有限扩张, $G = \text{Gal}(E/F)$, 则如下等价:

1. $\text{Fix}(G) = F$.
2. $|G| = [E : F]$.
3. E/F 为正规可分扩张.

注 注意到 E/F 为正规可分扩张当且仅当 E 为 F 上某个可分多项式的分裂域.

证明 $1 \Rightarrow 2$: 显然 $|G| \leq [E : F]$ (G 中元素都是 E 上的 F -嵌入), 反方向由 Artin 引理可得;

2 $\Rightarrow$ 1: 显然 $F \leq \text{Fix}(G)$, 再加上 $[E : F] = |G| = [E : \text{Fix}(G)]$ (也就是 Artin 引理) 即得.

2 $\Leftrightarrow$ 3: 回顾: E/F 可分当且仅当 E 到 $\bar{F}$ 的 K -嵌入有 $[E : F]$ 个; E/F 正规当且仅当 E 到 $\bar{F}$ 的 F -嵌入 σ , 都有 $\sigma(L) = L$, 即 $\sigma \in \text{Gal}(L/K)$.

引理 1.5 (Artin)

设 $G = \{\sigma_1 = \text{Id}, \dots, \sigma_n\} \leq \text{Aut}(E)$, $F = \text{Fix}(G)$, 则 $[E : F] = n$, 也即 $[E : \text{Fix}(G)] \leq |G|$.

注 显然有 $|G| \leq |\text{Gal}(E/\text{Fix}(G))| \leq [E : \text{Fix}(G)]$ (这里不需要 G 的群结构), 因此 Artin 引理等价于一边的不等号.

证明 若 $[E : F] = r > n = |G|$, 则存在 F -线性无关元 $e_1, \dots, e_r \in E$, 考虑矩阵

$$(\sigma_i(e_j))_{n \times r} = \begin{pmatrix} \sigma_1(e_1) & \sigma_1(e_2) & \cdots & \sigma_1(e_r) \\ \vdots & \vdots & & \vdots \\ \sigma_n(e_1) & \sigma_n(e_2) & \cdots & \sigma_n(e_r) \end{pmatrix} = (x_1, x_2, \dots, x_r), \quad (1.10)$$

不妨设 $x_1, \dots, x_k$ 恰好 E -线性相关, 即存在唯一 $a_2, \dots, a_k \in E$ 使得

$$x_1 = a_2 x_2 + \cdots + a_k x_k \Rightarrow e_1 = a_2 e_2 + \cdots + a_k e_k, \quad (1.11)$$

下证 $a_i \in F$, 任取 $\sigma \in G$, σ 作用在上述矩阵上可视为行变换 $(\sigma_i(e_j)) \mapsto (\sigma \sigma_i(e_j))$, 它不改变线性相关关系, 故

$$\sigma(x_1) = a_2 \sigma(x_2) + \cdots + a_k \sigma(x_k), \quad (1.12)$$

另一方面直接用 σ 作用可得

$$\sigma(x_1) = \sigma(a_2) \sigma(x_2) + \cdots + \sigma(a_k) \sigma(x_k), \quad (1.13)$$

根据唯一性可知 $a_i \in F$, 与 F -线性无关矛盾.

定义 1.8 (Galois 扩张)

称代数扩张 E/F 为 Galois 扩张, 若其满足上述定理的任一条.

引理 1.6

1. 若有限群 $G \leq \text{Aut}(E)$, 则 $\text{Gal}(E/\text{Fix}(G)) = G$.
2. 设 $G_1, G_2 \leq \text{Aut}(E)$ 且不相同, 则 $\text{Fix}(G_1), \text{Fix}(G_2)$ 也不相同.
3. 设 $H \leq G \leq \text{Aut}(E)$, $\sigma \in G$, 则 $\sigma(\text{Fix}(H)) = \text{Fix}(\sigma H \sigma^{-1})$.

证明

1. 根据定义显然有 $G \leq \text{Gal}(E/\text{Fix}(G))$, 反之假设存在 $\sigma \in \text{Gal}(E/\text{Fix}(G)), \sigma \notin G$, 则根据前面的定理 (一边实际上不需要 G 是群) 可得矛盾:

$$n = |G| = [E : \text{Fix}(G)] \geq [E : \text{Fix}(G \cup \{\sigma\})] \geq |G \cup \{\sigma\}| = n + 1, \quad (1.14)$$

2. 注意到 $G_i = \text{Gal}(E/\text{Fix}(G_i))$, 因此

$$\text{Fix}(G_1) = \text{Fix}(G_2) \Leftrightarrow \text{Gal}(E/\text{Fix}(G_1)) = \text{Gal}(E/\text{Fix}(G_2)) \Leftrightarrow G_1 = G_2. \quad (1.15)$$

3. 显然 $\sigma(\text{Fix}(H)) \leq \text{Fix}(\sigma H \sigma^{-1})$, 而对任意 $a \in \text{Fix}(\sigma H \sigma^{-1}), h \in H$, 都有

$$\sigma h \sigma^{-1}(a) = a \Leftrightarrow h(\sigma^{-1}(a)) = \sigma^{-1}(a) \quad (1.16)$$

故 $\sigma^{-1}(a) \in \text{Fix}(H), a \in \sigma(\text{Fix}(H)), \text{Fix}(\sigma H \sigma^{-1}) \subset \sigma(\text{Fix}(H))$, 得证.

定理 1.6 (Galois 基本定理)

设 E/F 为有限 Galois 扩张, $G = \text{Gal}(E/F)$, 则

1. E/F 的中间域 B 与 G 的子群 G_B 之间存在一一对应: $B = \text{Fix}(G_B), G_B = \text{Gal}(E/B)$.
2. 设 $E \supset B \supset F$, 则 B/F 为正规扩张当且仅当 $G_B \triangleleft G$, 并且此时 B/F 为 Galois 扩张, $\text{Gal}(B/F) \cong G/G_B = \text{Gal}(E/F)/\text{Gal}(E/B)$.
3. 对每个中间域 B , $[B:F] = [G:G_B]$ 且 $[E:B] = |G_B|$.

**证明**

1. 对任意 $H \leq G$, Fix 给出了一个映射

$$\Gamma: \{G \text{ 的子群} \} \longrightarrow \{E/F \text{ 中间域} \} \quad (1.17)$$

$$H \longmapsto \text{Fix}(H) \quad (1.18)$$

引理说明 $\text{Fix}(H_1) = \text{Fix}(H_2) \Leftrightarrow H_1 = H_2$, 因此 Γ 为单射, 另外对任意中间域 B , $\text{Gal}(E/B) \leq G$, 而 E/F 为 Galois 扩张说明 E/B 为 Galois 扩张, 因此 $B = \text{Fix}(\text{Gal}(E/B))$, 故 Γ 为满射.

2. 若 $G_B \triangleleft G$, 由引理可得 $\forall \sigma \in G$

$$\sigma(B) = \text{Fix}(\sigma G_B \sigma^{-1}) = \text{Fix}(G_B) = B, \quad (1.19)$$

即 B 对共轭封闭, 可得 B/F 正规. 进一步, $\sigma(B) = B$ 实际上诱导出了一个良定的群同态

$$\mathcal{R}: \text{Gal}(E/F) \longrightarrow \text{Gal}(B/F) \quad (1.20)$$

$$\sigma \longmapsto \sigma|_B \quad (1.21)$$

显然 $\mathcal{R}$ 为满射, 并且

$$\text{Ker } \mathcal{R} = \{\sigma: \sigma|_B = \text{Id}_B\} = \text{Gal}(E/B) = G_B, \quad (1.22)$$

根据同态基本定理可得

$$G/G_B = \text{Gal}(E/F)/\text{Gal}(E/B) \cong \text{Gal}(B/F). \quad (1.23)$$

反之若 B/F 为 Galois 扩张, 则 B 必然为某个可分多项式 $f(x) \in F[x]$ 的分裂域, 设 $\beta_1, \dots, \beta_r$ 为 f 的根, 则 $B = F(\beta_1, \dots, \beta_r)$. $f \in F[x]$ 说明对任意 $\sigma \in G$ 有 $\sigma(f(x)) = f(x)$, 因此 σ 作了这 r 个根的置换, 这也说明了 $\sigma(B) = B$, 根据上一条引理有 $\text{Fix}(\sigma G_B \sigma^{-1}) = \text{Fix}(G_B)$, 因此 $G_B = \sigma G_B \sigma^{-1}$, 即 $G_B \triangleleft G$.

3. E/F 为 Galois 扩张说明 E/B 为 Galois 扩张, 因此

$$B = \text{Fix}(\text{Gal}(E/B)) \Rightarrow [E:B] = |\text{Gal}(E/B)| = |G_B|, \quad (1.24)$$

而另一方面 $[E:F] = [E:B][B:F]$, $|G| = |G_B|[G:G_B]$, 因此 $[B:F] = [G:G_B]$.

1.3.2 三次方程求根公式**定义 1.9 (多项式的 Galois 群)**

设 E 为 $f(x) = (x - r_1) \cdots (x - r_n) \in F[x]$ 的分裂域, 则称 $\text{Gal}(E/F)$ 为多项式 f 的 Galois 群.



注 由于 $G = \text{Gal}(E/F)$ 的元素给出了根的置换 (即根集合上的作用), 因此 G 可以嵌入到 S_n 中, 可不妨设 $G \leq S_n$. 特别当 f 不可约时, 这样的作用是 **可迁的** (transitive).

定义 1.10 (判别式)

记号如上, 设 $\text{char } F \neq 2$, 称 $\Delta = \prod_{i < j} (r_i - r_j)$ 为 f 的判别式.



注 显然 $\Delta^2 \in F$, 并且 $G \leq A_n$ 当且仅当 $\Delta \in F$ (根据置换的奇偶性可得).

定义 1.11 (循环扩张)

称 E/F 为循环扩张, 若 $\text{Gal}(E/F)$ 为循环群.

**定理 1.7 (循环扩张的刻画)**

设 p 为素数, $\text{char } F \neq p$, F 包含所有 p 次单位根, E/F 为 p 次循环扩张, 则存在 $c \in F$ 使得 E 为 $x^p - c \in F[x]$ 的分裂域.



考虑 F 中的三次方程 $x^3 + px + q = 0$, 要求 $\text{char } F \neq 2, 3$, 其判别式 $D^2 = -4p^3 - 27q^2 \in F$ (根据齐次性, 待定系数可得), 因此其 Galois 群 $G \leq A_3$ (不妨设 $G = S_3$), 根据 Galois 对应可得

$$G \triangleright A_3 \triangleright \{1\} \quad (1.25)$$

$$F \subset F(D) \subset E \quad (1.26)$$

设 $E = K(D)(\sqrt[3]{c})$, 则 $\sigma(\sqrt[3]{c}) = \omega \sqrt[3]{c}$, 设

$$\beta = r_1 + \omega \sigma(r_1) + \omega^2 \sigma^2(r_1) \quad (1.27)$$

$$\Rightarrow \sigma(\beta) = \omega^2 \beta \quad (1.28)$$

$$\Rightarrow \sigma(\beta^3) = \beta^3 \quad (1.29)$$

因此 $\beta^3 \in F(D)$. 事实上 $\beta^3 = 27 - 3(4 - \omega)D$

1.4 Galois 理论的一些应用

1.4.1 单扩张

定义 1.12 (单扩张)

设 E/F 为代数扩张且存在 $\alpha \in E$ 使得 $E = F(\alpha)$, 则称 E 为 F 的单扩张.

**定理 1.8**

设 E/F 为有限扩张, 则 E/F 为单扩张当且仅当存在有限多个中间域 $F \subset B \subset E$.



证明 若 F 为有限域, 则 E/F 为有限扩张说明 E 为有限域, 因此其中间域个数也是有限的, E^* 为循环群, 因此存在 $\alpha \in E$ 使得 $E = F(\alpha)$.

对于 F 无限的情况, 若 $E = F(\alpha)$ 为单扩张, 考虑 $m_\alpha(x) \in F[x]$, 对任意中间域 $F \subset B \subset E$, 可以考虑 $\tilde{m}_\alpha(x) \in B[x]$, 则显然有

$$\tilde{m}_\alpha | m_\alpha, \quad E = B(\alpha), \quad \deg \tilde{m}_\alpha = [E : B], \quad (1.30)$$

设在 F 中添加 $\tilde{m}_\alpha$ 的系数得到的域为 D , 则 $F \subset D \subset B \subset E = D(\alpha)$, $\tilde{m}_\alpha(x) \in D[x]$, 此时 $\tilde{m}_\alpha$ 必然为 α 在 D 中的极小多项式, 因此 $[E : D] = \deg \tilde{m}_\alpha = [E : B]$, 这说明 $B = D$, 也即中间域 B 与极小多项式 m_α 的因子一一对应, 这样的因子只有有限个 (相当于根的组合), 故中间域也只有有限多个.

反之设 E/F 的中间域仅有限多个, 只需证明对任意 $\alpha, \beta \in E$, 存在 $\gamma_1 \in E$ 使得 $F(\alpha, \beta) = F(\gamma_1)$. 对于 $a \in F$, 考虑扩域 $F(\alpha + a\beta)$, 由于中间域仅有限多个, 因此必然存在 $a_1 \neq a_2 \in F$ 使得 $F(\alpha + a_1\beta) = F(\alpha + a_2\beta)$, 令 $\gamma_i = \alpha + a_i\beta$, 则 $F(\gamma_1) = F(\gamma_2)$, 即 $\gamma_1, \gamma_2 \in F(\gamma_1)$, $\gamma_2 - \gamma_1 = (a_2 - a_1)\beta \in F(\gamma_1)$, 这说明

$$F(\gamma_1) \subset F(\alpha, \beta) \subset F(\gamma_1) \Rightarrow F(\gamma_1) = F(\alpha, \beta). \quad (1.31)$$

借助 Galois 理论, 很容易得出如下结论.

推论 1.6

若 E/F 为有限可分扩张, 则 E/F 为单扩张.



证明 设 $E = F(\alpha_1, \dots, \alpha_k)$, 则每个极小多项式 $m_{\alpha_i}(x) \in F[x]$ 都可分, 因此 $f(x) = m_{\alpha_1}(x) \cdots m_{\alpha_k}(x)$ 也可分, 设 $E' \supset E$ 为 f 的分裂域, 则 E'/F 为 Galois 扩张, 根据 Galois 对应可知 E'/F 只有有限多个中间域, 因此 E/F 也只有有限多个中间域, 即 E/F 为单扩张.

引理 1.7

设 E/F 为有限 Galois 扩张, $\alpha \in E$, 则 $E = F(\alpha)$ 当且仅当对任意 $\sigma \in \text{Gal}(E/F)$, $\sigma \neq \text{Id}$ 有 $\sigma(\alpha) \neq \alpha$.



证明 【证法 1】设

$$d = [F(\alpha) : F] = \deg m_\alpha(x), \quad n = [E : F] = |\text{Gal}(E/F)|, \quad (1.32)$$

则 $E = F(\alpha)$ 当且仅当 $n = d$, 设 $m_\alpha(x) = (x - \alpha_1) \cdots (x - \alpha_d)$, 这里的根为 $\alpha_1 = \alpha$ 的 Galois 共轭元, 故 $E = F(\alpha)$ 当且仅当 α 有 n 个共轭元, 即每个 $\sigma \in \text{Gal}(E/F)$ 对应了一个共轭元 (Id 对应自身).

【证法 2】设 $B = F(\alpha)$, 则由 FTGT, 存在 $H \leq \text{Gal}(E/F)$ 使得 $B = \text{Fix}(H)$, 事实上这里

$$H = \{\sigma \in \text{Gal}(E/F) : \sigma|_B = \text{Id}\} = \{\sigma \in \text{Gal}(E/F) : \sigma(\alpha) = \alpha\}, \quad (1.33)$$

因此 $E = B = \text{Fix}(H) \Leftrightarrow H = \{\text{Id}\}$, 得证.

上面的结果也可以不依赖 Galois 理论独立给出.

引理 1.8

设 E/F 为有限可分扩张, $\alpha \in E$, 则 $E = F(\alpha)$ 当且仅当对任意不为 Id_E 的 F -嵌入 $\sigma : E \rightarrow \bar{F}$ 都有 $\sigma(\alpha) \neq \alpha$.



证明 E/F 有限可分说明 $E/F(\alpha)$ 有限可分, 而 $[E : F(\alpha)] = |\text{Hom}_{F(\alpha)}(E, \bar{F})|$, 因此 $E = F(\alpha)$ 当且仅当 $|\text{Hom}_{F(\alpha)}(E, \bar{F})| = 1$, 即仅有 Id_E 保持 α 不变.

证明 【可分扩张为单扩张】只需考虑无限域情形, 设 $E = F(\alpha, \beta)$ 为可分扩张, $m_\alpha, m_\beta \in F[x]$ 的根分别为 $\alpha_1 = \alpha, \dots, \alpha_m; \beta_1 = \beta, \dots, \beta_n$, $|F| = \infty$ 说明存在 $c \in F$, 只要 $(i, j) \neq (1, 1)$ 就有 $\alpha + c\beta \neq \alpha_i + c\beta_j$ (因为 $(\alpha - \alpha_j)/(\beta_j - \beta)$ 仅有限个), 令 $\gamma = \alpha + c\beta$, 则由上述引理可知 $E = F(\gamma)$ (因为 F -嵌入必然将 α, β 映为某个 α_i, β_j).

1.5 迹和范数

1.5.1 基本定义

对于有限扩张 E/F 以及非零元 $u \in E$, 可以诱导一个线性变换 $T_u \in \text{Hom}_F(E, E)$, $T_u(x) = ux$, 由此定义

定义 1.13 (迹与范数)

设 E/F 为有限扩张, 对任意 $u \in E$, 定义

$$\text{Tr}_{E/F}(u) = \text{tr}(T_u), \quad N_{E/F}(u) = \det(T_u). \quad (1.34)$$



注 根据定义可得 trace 和 norm 都在 F 中 (考虑对应变换的矩阵).

例 1.1

- 设 $E/F = \mathbb{Q}(\sqrt[3]{5}, \omega)/\mathbb{Q}$, $\alpha = \sqrt[3]{5}$, 则其一组基为 $1, \alpha, \alpha^2, \omega, \omega\alpha, \omega\alpha^2$, 易验证

$$\text{Tr}_{E/F}(\alpha) = 0 = 0 \cdot [E : F(\alpha)], \quad N_{E/F}(\alpha) = 5^{[E:F(\alpha)]}. \quad (1.35)$$

- 设 $E = F(\alpha)$, $m_\alpha(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$, 则 $\text{Tr}_{E/F}(\alpha) = -a_{n-1}$, $N_{E/F}(\alpha) = (-1)^n a_0$, 这一观察是因为 T_α 的极小多项式与 α 的极小多项式相同, 根据维数可知 T_α 的特征多项式等于极小多项式. 对于 Galois 扩张, 其范数与迹有如下等价定义

引理 1.9 (Galois 扩张的范数/迹)

设 E/F 为有限 Galois 扩张, $G = \text{Gal}(E/F)$, 对于 $u \in E$ 有

$$\text{Tr}_{E/F}(u) = \sum_{\sigma \in G} \sigma(u), \quad N_{E/F}(u) = \prod_{\sigma \in G} \sigma(u). \quad (1.36)$$



证明 设 $B = F(u)$, $[B:F] = m$, $[E:F] = n$, 则 $1, u, \dots, u^{m-1}$ 是 B/F 的一组基, 设 $v_1, \dots, v_{n/m}$ 为 E/B 的一组基, 则

$$1, u, \dots, u^{m-1}, v_1, v_1 u, \dots, v_1 u^{m-1}, \dots, v_{n/m}, \dots, v_{n/m} u^{m-1} \quad (1.37)$$

是 E/F 的一组基, 设 $m_u(x) = x^m + a_{m-1}x^{m-1} + \cdots + a_0$, 则这也是 T_u 的极小多项式, 其友方阵为

$$C_u = \begin{pmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & \cdots & 0 & -a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -a_{n-1} \end{pmatrix}, \quad (1.38)$$

进一步可得 T_u 在上述基下的矩阵为 $\text{diag}(C_u, C_u, \dots, C_u)$, 因此

$$\text{Tr}_{E/F}(u) = n/m(-a_{n-1}), \quad N_{E/F}(u) = (-1)^n a_0^{n/m}, \quad (1.39)$$

设 m_u 的所有根为 $u_1 = u, u_2, \dots, u_m$, 则根据延拓定理, 对于每个 u_i , 恰好存在 $[E:B] = n/m$ 个 $\text{Gal}(E/F)$ 中的自同构 σ 使得 $\sigma(u) = u_i$, 因此

$$\text{Tr}_{E/F}(u) = n/m(-a_{n-1}) = n/m \sum_{i=1}^m u_i = \sum_{\sigma \in G} \sigma(u), \quad (1.40)$$

$$N_{E/F}(u) = (-1)^n a_0^{n/m} = \left(\prod_{i=1}^m u_i \right)^{n/m} = \prod_{\sigma \in G} \sigma(u). \quad (1.41)$$

命题 1.4

设 E/F 为 n 次 Galois 扩张, 设 B 为中间域 (故 E/F 为 Galois 扩张) 且 B/F 为 Galois 扩张, 则对任意 $a \in F, \alpha, \beta \in E$ 有

1. $N_{E/F}(a) = a^n$, $\text{Tr}_{E/F} = na$.
2. $N_{E/F}(\alpha\beta) = N_{E/F}(\alpha)N_{E/F}(\beta)$, $\text{Tr}_{E/F}(\alpha + \beta) = \text{Tr}_{E/F}(\alpha) + \text{Tr}_{E/F}(\beta)$.
3. $N_{E/F}(\alpha) = N_{B/F}(N_{E/B}(\alpha))$, $\text{Tr}_{E/F}(\alpha) = \text{Tr}_{B/F}(\text{Tr}_{E/B}(\alpha))$



定理 1.9

设 E/F 有限可分, 则

$$\text{Tr} : E \times E \longrightarrow F \quad (1.42)$$

$$(x, y) \longmapsto \text{Tr}(xy) \quad (1.43)$$

为一个非退化双线性函数 (即其对应度量矩阵可逆) .



证明 双线性函数是显然的. 由于有限可分扩张必为单扩张, 因此可设 $E = F(u)$, 令 $u_1 = u, \dots, u_n$ 为 u 的共轭元 (在代数闭包 $\bar{F}$ 中考虑), 即 $m_u(x) = (x - u_1) \cdots (x - u_n)$, 取 E/F 的基 $1, u, \dots, u^{n-1}$, 记该基下的度量阵

为 A , 则 $a_{ij} = \text{Tr}(u^{i+j-2}) = \sum_{k=1}^n u_k^{i+j-2}$, 由此可得

$$A = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ u_1 & u_2 & \cdots & u_n \\ \vdots & \vdots & \cdots & \vdots \\ u_1^{n-1} & u_2^{n-1} & \cdots & u_n^{n-1} \end{pmatrix} \begin{pmatrix} 1 & u_1 & \cdots & u_1^{n-1} \\ 1 & u_2 & \cdots & u_2^{n-1} \\ \vdots & \vdots & \cdots & \vdots \\ 1 & u_n & \cdots & u_n^{n-1} \end{pmatrix}, \quad (1.44)$$

故其非退化.

1.5.2 Hilbert 90 定理

定理 1.10 (Dedekind)

设 E/F 为 Galois 扩张, $G = \text{Gal}(E/F) = \{\sigma, \dots, \sigma_n\}$, 则 $\sigma_1, \dots, \sigma_n$ 是 F -线性无关的.

证明 不妨设 $\sigma_1 = a_2\sigma_2 + \cdots + a_m\sigma_m$, 并且 a_i 唯一 (即取极大线性无关组), 则对任意 $u, v \in E$ 有

$$\sigma_1(u) = a_2\sigma_2(u) + \cdots + a_m\sigma_m(u) \quad (1.45)$$

$$\sigma_1(vu) = a_2\sigma_2(vu) + \cdots + a_m\sigma_m(vu), \quad (1.46)$$

不妨取 $v \in L$ 使得 $\sigma_1(v) \neq \sigma_2(v)$ 则

$$\sigma_1(u) = a_2 \frac{\sigma_2(v)}{\sigma_1(v)} \sigma_2(u) + \cdots + a_m \frac{\sigma_m(v)}{\sigma_1(v)} \sigma_m(u), \quad (1.47)$$

矛盾.

引理 1.10

设 E/F 有限, $G = \text{Gal}(E/F)$, $f: G \rightarrow E$ 满足 $f(\sigma\tau) = f(\sigma) + \sigma(f(\tau))$ (cocycle 条件), 则存在 $v \in E$, 对任意 $\sigma \in G$ 有 $f(\sigma) = v - \sigma(v)$.

证明 不妨设 $f \neq 0$. 根据 Dedekind 定理, 存在 $u \in E$ 使得 $w = \sum_{\sigma \in G} f(\sigma)\sigma(u) \neq 0$ 且 $\sum_{\sigma \in G} \sigma(u) \neq 0$, 取 $\eta \in G$, 则

$$\eta(w) = \sum_{\sigma \in G} \eta(f(\sigma)\sigma(u)) = \sum_{\sigma \in G} \eta(f(\sigma))\eta(\sigma(u)) \quad (1.48)$$

$$= \sum_{\sigma \in G} (f(\eta\sigma)(\eta\sigma)(u) - f(\eta)(\eta\sigma)(u)) \quad (1.49)$$

$$= w - f(\eta)\text{Tr}(u) \quad (1.50)$$

$$\Rightarrow f(\eta) = \frac{w - \eta(w)}{\text{Tr}(u)}, \quad (1.51)$$

令 $v = w/\text{Tr}(u)$ 即得.

引理 1.11

设 E/F 有限, $G = \text{Gal}(E/F)$, $f: G \rightarrow E$ 满足 $f(\sigma\tau) = f(\sigma)\sigma(f(\tau))$, 则存在 $v \in E$, 对任意 $\sigma \in G$ 有 $f(\sigma) = v/\sigma(v)$.

证明 不妨设 $f \neq 0$. 根据 Dedekind 定理, 存在 $u \in E$ 使得 $w = \sum_{\sigma \in G} f(\sigma)\sigma(u) \neq 0$, 取 $\eta \in G$, 则

$$\eta(w) = \sum_{\sigma \in G} \eta(f(\sigma)\sigma(u)) = \sum_{\sigma \in G} \eta(f(\sigma))\eta(\sigma(u)) \quad (1.52)$$

$$= \sum_{\sigma \in G} (f(\eta\sigma)(\eta\sigma)(u))/f(\eta) \quad (1.53)$$

$$= w/f(\eta) \quad (1.54)$$

$$\Rightarrow f(\eta) = \frac{w}{\eta(w)}, \quad (1.55)$$

令 $v = w$ 即得.

定理 1.11 (Hilbert 90)

设 E/F 为有限循环 Galois 扩张, $\text{Gal}(E/F) = \langle \sigma \rangle$, 设 $u \in E$ 则

1. 若 $\text{Tr}_{E/F}(u) = 0$, 则存在 $v \in E$ 使得 $u = v - \sigma(v)$.
2. 若 $N_{E/F}(u) = 1$, 则存在 $v \in E$ 使得 $u = v/\sigma(v)$.



证明

1. 令 $f: G \rightarrow L$ 使得

$$f(1) = 0, f(\sigma) = u, f(\sigma^2) = u + \sigma(u), f(\sigma^i) = u + \sigma(u) + \cdots + \sigma^{i-1}(u), \quad (1.56)$$

$\text{Tr}(u) = 0$ 说明 f 是良定的. 由于

$$f(\sigma^i \sigma^j)(u) = u + \cdots + \sigma^{i-1}(u) + \sigma^i(u) + \cdots + \sigma^{i+j-1}(u) \quad (1.57)$$

$$= [f(\sigma^i) + \sigma^i(f(\sigma^j))](u), \quad (1.58)$$

故 f 满足 cocycle 条件, 根据引理可知存在 $v \in E$ 使得 $u = f(\sigma) = v - \sigma(v)$.

2. 令 $f: G \rightarrow L$ 使得

$$f(1) = 0, f(\sigma) = u, f(\sigma^2) = u\sigma(u), f(\sigma^i) = u\sigma(u) \cdots \sigma^{i-1}(u), \quad (1.59)$$

$N(u) = 1$ 说明 f 是良定的. 由于

$$f(\sigma^i \sigma^j)(u) = u \cdots \sigma^{i-1}(u) \sigma^i(u) \cdots \sigma^{i+j-1}(u) \quad (1.60)$$

$$= [f(\sigma^i) \sigma^i(f(\sigma^j))](u), \quad (1.61)$$

故 f 满足引理条件, 即存在 $v \in E$ 使得 $u = f(\sigma) = v/\sigma(v)$.

考虑 Hilbert 90 的应用.

定理 1.12 (循环扩张)

设 p 为素数, E/F 为 p 次循环 Galois 扩张, F 包含本原 p 次单位根, 则

1. 若 $\text{char } F \neq p$, 则存在 $a \in K$ 使得 $L \cong K[x]/(x^p - a)$.
2. 若 $\text{char } F = p$, 则 (注意此时 p 次单位根只有 1) 存在 $c \in K$ 使得 $L \cong K[x]/(x^p - x + c)$.



证明

1. 设 ζ 为 p 次本原单位根, 则 $N_{E/F}(\zeta) = 1$, 因此存在 $v \in L$ 使得 $\zeta = v/\sigma(v)$, 即 $\sigma(v) = \zeta^{-1}v$, 观察得到 $v \notin F, v^p \in F$, 因此 $m_v(x) = x^p - v^p$, 得证.
2. 此时 $\text{Tr}_{E/F}(1) = 0$, 因此存在 $v \in E$ 使得 $1 = v - \sigma(v)$, 也即 $\sigma(v) = v - 1$, 易验证 $m_v(x) = x^p - x + c$.

第2章 模论

2.1 基本概念

2.1.1 模的定义

定义 2.1 (模)

设 R 为幺环, $(M, +)$ 为群, 若存在二元运算 $R \times M \rightarrow M, r \cdot x = rx$ (或者说数乘), 满足

- $1 \cdot x = x$.
- $(r_1 r_2)x = r_1(r_2 x)$.
- $r_1(x_1 + x_2) = r_1 x_1 + r_1 x_2$.
- $(r_1 + r_2)x = r_1 x + r_2 x$.

则称 M 为 (左) R -模,



注 右模的定义也是类似的, 只是第二条变为 $x(r_1 r_2) = (xr_1)r_2$, 有时也会将右模的作用写在左边, 二者的区分在于结合顺序的先后. 特别当 R 为交换环时, 左模与右模等价.

例 2.1

- 设 k 为域, V/k 为线性空间, 则 V 为 k -模.
- $\mathbb{Z}$ -模等价于 Abel 群.
- 设 k 为域, $R = M_n(k)$, $V = k^n$ 为列向量几何, 则 V 是一个左 R -模, 考虑行向量可得右模.
- 设 V/k 为线性空间, $T \in \text{Hom}(V, V)$, $R = k[x]$, 则令 $f(x) \cdot T = f(T)$ 可以给出一个 R -模, 记为 V^T .

定义 2.2 (子模)

设 M 为 R -模, 称子群 $N \leq M$ 为其子 R -模, N 也是一个 R -模.



注 容易验证, $N \leq M$ 为子模当且仅当其满足封闭性, 即 $RN \subset N$.

例 2.2 设 R 为幺环, 则 R 可视为 R -模, 并且其子模为其理想.

命题 2.1

设 $N_1, N_2 \leq M$, 则 $N_1 \cap N_2, N_1 + N_2 = \{z_1 + z_2 : z_i \in N_i\} \leq M$.



定义 2.3 (生成的模)

设 M 为 R -模, 对于 $S \subset M$, 定义 S 生成的模为 M 中的包含 S 的最小的子模, 记为 (S) .



定义 2.4 (商模)

设 M 为 R -模, N 为其子模, 则可定义商模 $M/N = \{a + N : a \in M\}$, 有数乘 $r \cdot (x + N) = rx + N$.



定义 2.5 (模同态)

称映射 $f : M \rightarrow N$ 为模同态, 若它是 R -线性的加法群同态.



例 2.3

- 设 M 为 R -模, 取定 $x \in M$, 设 $\varphi_x : R \rightarrow M, r \mapsto rx$, 则容易验证 φ_x 是一个模同态, 并且 $\text{Im } \varphi_x = Rx$.
- 设 $V = k^2, T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, R = k[x]$, 则 V^T 是一个 R -模, 取 $e_1 = (1, 0)^T, e_2 = (0, 1)^T$, 考虑 $\varphi_{e_1}, \varphi_{e_2} : R \rightarrow V$,

则容易验证

$$\operatorname{Im} \varphi_{e_1} = ke_1, \quad \operatorname{Im} \varphi_{e_2} = V. \quad (2.1)$$

- 设 R 为交换环, 取 $a \in R$, 设 $\psi_a: M \rightarrow M, x \mapsto ax$, 则容易验证 ψ_x 是一个模同态 (若非交换, 则无模结构).
- 设 R 为交换环, M, N 为 R -模, 考虑 $\operatorname{Hom}_R(M, N)$, 它在加法、数乘下构成一个 R -模.

定理 2.1 (同态基本定理)

1. 设 $f: M \rightarrow N$ 为 R -模同态, 则 $M/\operatorname{Ker} f \cong \operatorname{Im} f$.
2. 设 $N_1, N_2 \leq M$, 则 $N_1/N_1 \cap N_2 \cong (N_1 + N_2)/N_2$.
3. 设 $K \leq N \leq M$, 则 $M/N \cong (M/K)/(N/K)$.
4. 设 $N \leq M$, 则 M/N 的子模与 M 的包含 N 的子模存在一一对应.



例 2.4 延续上例记号, 则 $\operatorname{Ker} \varphi_{e_1} = (x-1) \leq k[x] = R$, 因此 $k[x]/(x-1) \cong Re_1 = ke_1$. 另一方面由于 $k[x] = k[x-1]$, 因此 $\operatorname{Ker} \varphi_{e_2} = ((x-1)^2)$, 故 $k[x]/((x-1)^2) \cong Re_2 = V^T$.

2.1.2 单模与合成列

定义 2.6 (单模)

称 R -模 M 为单模, 若其无非平凡子模.



例 2.5

- 设 R 为交换环, 将其视为 R -模, 则 R 为单模当且仅当其无非平凡理想, 即它是域.
- k^n 作为 $R = M_n(k)$ 模是单模, 也就是说对任意非零向量 $v \in k^n$, $Rv = k^n$.

易知 M 为单模当且仅当任何 $0 \neq x \in M$ 都有 $Rx = M$, 也即 $M = (x)$, 此时存在满同态 $f: R \rightarrow M, f(r) = rm$, 根据同态基本定理可得

$$M \cong R/\operatorname{Ker} f, \quad (2.2)$$

根据理想的对应关系可知 $\mathfrak{m}$ 为极大理想, 因此可得推论

推论 2.1

R -模 M 为单模当且仅当存在极大理想 $\mathfrak{m} \triangleleft R$ 使得 $M \cong R/\mathfrak{m}$.



定义 2.7 (合成列)

设 M 为 R -模, 若有子模列 $M = M_0 \supsetneq M_1 \supsetneq \cdots \supsetneq M_n = \{0\}$ 使得 M_i/M_{i+1} 为单模, 则称 M 有一个长度为 n 的合成列.



例 2.6

- 视 $\mathbb{Z}$ 为 $\mathbb{Z}$ 模, 则其不存在有限长度的合成列, 因为其中单模为 $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$ (p 为素数).
- 考虑 $\mathbb{Z}/12\mathbb{Z}$, 则其有合成列 $\mathbb{Z}/12\mathbb{Z} \supsetneq 3\mathbb{Z}/12\mathbb{Z} \supsetneq 6\mathbb{Z}/12\mathbb{Z} \supsetneq \{0\}$, 相邻商模为 $\mathbb{Z}_3, \mathbb{Z}_2, \mathbb{Z}_2$. 事实上它还有其它合成列, 不过相邻商模是相同的 (可能次序不同).

定理 2.2

设 M 为 R -模, 假设其有长度为 n 的合成列, 则

1. M 的任意子模 N 也有合成列.
2. Jordan-Holder 引理: M 的任意两个合成列长度相同, 并且因子 $M_0/M_1, \dots, M_{n-1}/M_n$ 在同构意义下唯一.



证明

1. 令 $N_i = N \cap M_i$, 则易验证 $N_i/N_{i+1} = (N \cap M_i)/(N \cap M_{i+1}) \leq M_i/M_{i+1}$, 因此通过去掉一些元素即可得到 N 的合成列.
2. 对长度 n 归纳, 当 $n = 1$ 时显然成立, 假设命题对不超过 $n - 1$ 的情形成立 (即若模存在一个长度不超过 $n - 1$ 的合成列, 则其所有合成列长度相同且同构). 设 M 有两个合成列

$$M = N_0 \supsetneq \cdots \supsetneq N_m = \{0\}, \quad M = M_0 \supsetneq \cdots \supsetneq M_n = \{0\}, \quad (2.3)$$

不妨设 $N_1 \neq M_1$, 考虑下图

$$\begin{array}{ccccccc}
 & M_1 & \supsetneq & M_2 & \supsetneq & \cdots & \supsetneq & M_n = \{0\} \\
 & \nearrow & & \searrow & & & & \\
 M & & & & & & & \\
 & \nwarrow & & \nearrow & & & & \\
 & N_1 & \supsetneq & N_2 & \supsetneq & \cdots & \supsetneq & N_m = \{0\}
 \end{array}
 \quad
 \begin{array}{ccccccc}
 M_1 \cap N_1 & \supsetneq & M_2 \cap N_1 & \supsetneq & \cdots & \supsetneq & M_n \cap N_1 = \{0\}
 \end{array}$$

根据归纳假设, 上图中 M_1, N_1 所具有的两个合成列彼此同构, 故 $m = n$, 显然 $M = M_1 + N_1$, 根据同态定理有

$$M/M_1 \cong N_1/(M_1 \cap N_1), \quad M/N_1 \cong M_1/(M_1 \cap N_1), \quad (2.4)$$

因此 M 的两个合成列彼此同构, 长度相同, 得证.

将群论中的 Zassenhaus 引理推广, 可以给出一个直接证明 (与群的合成列类似)

引理 2.1 (Zassenhaus butterfly lemma)

设 M 为 R -模, $A^* \leq A \leq M, B^* \leq B \leq M$, 则有同构

$$\frac{A^* + (A \cap B)}{A^* + (A \cap B^*)} \cong \frac{A \cap B}{(A \cap B^*) + (A^* \cap B)} \cong \frac{(A \cap B) + B^*}{(A^* \cap B) + B^*}. \quad (2.5)$$



证明 根据对称性, 只需证明左半边. 设 $D = (A \cap B^*) + (A^* \cap B)$, 考虑映射

$$f: A^* + (A \cap B) \longrightarrow (A \cap B)/D \quad (2.6)$$

$$a + m \longmapsto m + D \quad (2.7)$$

显然 f 为满射, 首先证明其良定性, 设 $a_1 + m_1 = a_2 + m_2$, 则

$$m_1 - m_2 = a_2 - a_1 \in A^* \cap A \cap B = A^* \cap B \subset D, \quad (2.8)$$

因此

$$f(a_1 + m_1) = m_1 + D = m_2 + D = f(a_2 + m_2). \quad (2.9)$$

再证 f 为同态:

$$f((a_1 + m_1) - (a_2 + m_2)) = (m_1 - m_2) + D = (m_1 + D) - (m_2 + D) = f(a_1 + m_1) - f(a_2 + m_2), \quad (2.10)$$

显然

$$\text{Ker } f = A^* + (A \cap B^*) + (A^* \cap B) = A^* + (A \cap B^*), \quad (2.11)$$

故由同态基本定理得证.

定理 2.3 (Jordan-Holder-Schreier)

若 R -模 M 存在合成列, 则其合成列在同构意义下唯一.



证明 设 $M = M_0 \supsetneq \cdots \supsetneq M_n = \{0\}, M = N_0 \supsetneq \cdots \supsetneq N_m = \{0\}$ 为 M 的两个合成列, 则对任意 $0 \leq i \leq n - 1$

有

$$M_i = M_{i+1} + (M_i \cap N_0) \supset M_{i+1} + (M_i \cap N_1) \supset \cdots \supset M_{i+1} + (M_i \cap N_{m-1}) \supset M_{i+1} + (M_i \cap N_m) = M_{i+1}, \quad (2.12)$$

如此添加若干因子后, 得到新列 (未必是合成列), 长度为 $(n+1) + (n+1)*m = (n+1)(m+1)$, 对另一个合成列也可以作如此操作, 根据 Zassenhaus 引理可得

$$\frac{M_{i+1} + (M_i \cap N_j)}{M_{i+1} + (M_i \cap N_{j+1})} \cong \frac{(M_i \cap N_j) + N_{j+1}}{(M_{i+1} \cap N_j) + N_{j+1}}, \quad (2.13)$$

因此新列中的因子存在通过对应关系, 这时抛去平凡因子后可以得到等价的合成列, 而一开始的列本身就是合成列, 即得两合成列等价.

2.1.3 直和与直积

定义 2.8 (直和)

设 $\{M_i : i \in I\}$ 为一族 R -模, 令 $\bigoplus_{i \in I} M_i = \{(x_i)_{i \in I} : x_i \in M_i, \text{ 仅有限个 } x_i \neq 0\}$, 可赋模结构 $r(x_i)_{i \in I} = (rx_i)_{i \in I}$, 称 $\bigoplus_{i \in I} M_i$ 为这一族 R -模的直和.

命题 2.2 (直和的泛性质)

设 $\{M_i : i \in I\}$ 为一族 R -模, 设 $\{f_i \in \text{Hom}_R(M_i, N) : i \in I\}$ 为一组模同态, 则存在唯一模同态 $F : \bigoplus_{i \in I} M_i \rightarrow N$ 使得对任意 $f_i = F \circ \iota_i$, 这里 ι_i 为自然嵌入.

$$\begin{array}{ccc} \bigoplus_{i \in I} M_i & \xleftarrow{\iota_i} & M_i \\ & \searrow \exists! F & \downarrow f_i \\ & & N \end{array}$$

定义 2.9 (直积)

设 $\{M_i : i \in I\}$ 为一族 R -模, 令 $\prod_{i \in I} M_i = \{(x_i)_{i \in I} : x_i \in M_i\}$, 可赋模结构 $r(x_i)_{i \in I} = (rx_i)_{i \in I}$, 称 $\prod_{i \in I} M_i$ 为这一族 R -模的直积.

命题 2.3 (直积的泛性质)

设 $\{M_i : i \in I\}$ 为一族 R -模, 设 $\{f_i \in \text{Hom}_R(N, M_i) : i \in I\}$ 为一组模同态, 则存在唯一模同态 $F : N \rightarrow \prod_{i \in I} M_i$ 使得 $f_i = \pi_i \circ F$, 这里 π_i 为自然投影.

$$\begin{array}{ccc} \prod_{i \in I} M_i & \xrightarrow{\pi_i} & M_i \\ & \nwarrow \exists! F & \uparrow f_i \\ & & N \end{array}$$

定义 2.10 (构成直和)

设 $K, N \leq M$, 则有自然同态 $K \oplus N \rightarrow M, (x, y) \mapsto x + y$, 若该同态为单同态, 则称 K, N 在 M 中构成直和, 可记 $K \oplus N \leq M$ (对任意有限情形类似).

命题 2.4

设 $M_1, \dots, M_n \leq M$, 则它们构成直和等价于对每个 i , $M_i \cap (M_1 + \cdots + M_{i-1}) = \{0\}$.

2.2 正合列

定义 2.11 (正合与正合列)

设 $M_1 \xrightarrow{\varphi} M_2 \xrightarrow{\psi} M_3$ 为 R -模同态复合, 称此序列在 M_2 处正合, 若 $\text{Ker } \psi = \text{Im } \varphi$. 称一系列同态复合是正合列, 若其处处正合.

例 2.7

- 左正合列: $0 \rightarrow K \xrightarrow{\varphi} M$, 其中 φ 为单同态.
- 右正合列: $M \xrightarrow{\psi} N \rightarrow 0$, 其中 ψ 为满同态.
- 短正合列: $0 \rightarrow K \xrightarrow{\varphi} M \xrightarrow{\psi} N \rightarrow 0$, 其中 φ 为单同态, ψ 为满同态且 $\text{Ker } \psi = \text{Im } \varphi$.
- 若 $K \leq M$, 则 $0 \rightarrow K \xrightarrow{\iota} M \xrightarrow{\pi} M/K \rightarrow 0$ 为正合列.
- $0 \rightarrow K \rightarrow K \oplus N \rightarrow N \rightarrow 0$ 为正合列.

称两个正合列同构, 若存在如下交换图

$$\begin{array}{ccccc} K_1 & \longrightarrow & M_1 & \longrightarrow & N_1 \\ \cong \downarrow & & \cong \downarrow & & \cong \downarrow \\ K_2 & \longrightarrow & M_2 & \longrightarrow & N_2 \end{array}$$

定理 2.4 (短五引理)

设有如下交换图, 其中行正合

$$\begin{array}{ccccccc} 0 & \longrightarrow & K & \xrightarrow{\phi_1} & M & \xrightarrow{\phi_2} & N \longrightarrow 0 \\ & & \downarrow g & & \downarrow f & & \downarrow h \\ 0 & \longrightarrow & K' & \xrightarrow{\psi_1} & M' & \xrightarrow{\psi_2} & N' \longrightarrow 0 \end{array}$$

则

1. g, h 为满同态 $\Rightarrow f$ 为满同态.
2. g, h 为单同态 $\Rightarrow f$ 为单同态.
3. g, h 为同构 $\Rightarrow f$ 为同构.

证明

1. 设 $m' \in M'$, 此时存在 $n \in N$ 使得 $h(n) = \psi_2(m')$, ϕ_2 满说明存在 $m \in M$ 使得 $\phi_2(m) = n$, 因此

$$\psi_2(m') = h(\phi_2(m)) = \psi_2(f(m)) \Rightarrow m_0 = f(m) - m' \in \text{Ker } \psi_2 = \text{Im } \psi_1, \quad (2.14)$$

故存在 $k' \in K'$ 使得 $m_0 = \psi_1(k')$, g 满说明存在 $k \in K$ 使得 $k' = g(k)$, 因此

$$m_0 = \psi_1(g(k)) = f(\phi_1(k)) \Rightarrow m' = f(m - \phi_1(k)) = f(\tilde{m}), \quad (2.15)$$

故 f 为满射.

2. 设 $m \in M$ 使得 $f(m) = 0$, 则

$$f(m) = 0 \Rightarrow 0 = \psi_2(f(m)) = h(\phi_2(m)) \Rightarrow \phi_2(m) = 0, m \in \text{Ker } \phi_2 = \text{Im } \phi_1, \quad (2.16)$$

因此存在 $k \in K$ 使得 $m = \phi_1(k)$, 并且

$$0 = f(\phi_1(k)) = \psi_1(g(k)) \Rightarrow g(k) = 0 \Rightarrow k = 0, m = f(k) = 0, \quad (2.17)$$

故 f 为单同态.

3. 由 1,2 显然.

定理 2.5 (五引理)

设有如下正合列的交换图

$$\begin{array}{ccccccccc}
 M_1 & \xrightarrow{g_1} & M_2 & \xrightarrow{g_2} & M_3 & \xrightarrow{g_3} & M_4 & \xrightarrow{g_4} & M_5 \\
 \downarrow f_1 & & \downarrow f_2 & & \downarrow f_3 & & \downarrow f_4 & & \downarrow f_5 \\
 N_1 & \xrightarrow{h_1} & N_2 & \xrightarrow{h_2} & N_3 & \xrightarrow{h_3} & N_4 & \xrightarrow{h_4} & N_5
 \end{array}$$

则

1. 若 f_1 满, f_2, f_4 单, 则 f_3 单.
2. 若 f_5 单, f_2, f_4 满, 则 f_3 满.

**证明**

1. 设 $m_3 \in M_3, f(m_3) = 0$, 则

$$0 = h_3(f_3(m_3)) = f_4(g_3(m_3)) \Rightarrow g_3(m_3) = 0, m_3 \in \text{Ker } g_3 = \text{Im } g_2, \quad (2.18)$$

因此存在 $m_2 \in M_2$ 使得 $m_3 = g_2(m_2)$, 并且

$$0 = f_3(g_2(m_2)) = h_2(f_2(m_2)) \Rightarrow f_2(m_2) \in \text{Ker } h_2 = \text{Im } h_1, \quad (2.19)$$

因此存在 $m_1 \in N_1$ 使得 $f_2(m_2) = h_1(n_1)$, f_1 满说明存在 $m_1 \in M_1$ 使得 $n_1 = f_1(m_1)$, 因此

$$f_2(m_2) = h_1(f_1(m_1)) = f_2(g_1(m_1)) \Rightarrow m_2 = g_1(m_1), \quad (2.20)$$

因此 $m_3 = g_2(m_2) = g_2(g_1(m_1)) = 0$, 即 f_3 为单同态.

2. 设 $n_3 \in N_3$, f_4 满说明存在 $m_4 \in M_4$ 使得 $f_4(m_4) = h_3(n_3)$, 并且

$$0 = h_4(h_3(n_3)) = h_4(f_4(m_4)) = f_5(g_4(m_4)) \Rightarrow g_4(m_4) = 0, m_4 \in \text{Ker } g_4 = \text{Im } g_3, \quad (2.21)$$

因此存在 $m_3 \in M_3$ 使得 $m_4 = g_3(m_3)$, 并且

$$h_3(n_3) = f_4(m_4) = f_4(g_3(m_3)) = h_3(f_3(m_3)) \Rightarrow n' = n_3 - f_3(m_3) \in \text{Ker } h_3 = \text{Im } h_2, \quad (2.22)$$

因此存在 $n_2 \in N_2$ 使得 $n' = h_2(n_2)$, f_2 满说明存在 $m_2 \in M_2$ 使得 $n_2 = f_2(m_2)$, 因此

$$n' = h_2(f_2(m_2)) = f_3(g_2(m_2)) \Rightarrow n_3 = f_3(m_3 + g_2(m_2)) \in \text{Im } f_3, \quad (2.23)$$

故 f_3 满.

定理 2.6 (蛇形引理)

设有如下交换图, 其中两行三列正合

$$\begin{array}{ccccccc}
 & 0 & & 0 & & 0 & \\
 & \downarrow & & \downarrow & & \downarrow & \\
 & R & & S & & T & \\
 & \downarrow & & \downarrow & & \downarrow & \\
 & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow 0 \\
 & \downarrow & & \downarrow & & \downarrow & \\
 0 & \longrightarrow & A' & \longrightarrow & B' & \longrightarrow & C' \\
 & \downarrow & & \downarrow & & \downarrow & \\
 & U & & V & & W & \\
 & \downarrow & & \downarrow & & \downarrow & \\
 & 0 & & 0 & & 0 &
 \end{array}$$

$$\begin{array}{ccccccc}
 & 0 & & 0 & & 0 & \\
 & \downarrow & & \downarrow & & \downarrow & \\
 & R & \xrightarrow{\varphi_1} & S & \xrightarrow{\varphi_2} & T & \\
 & \downarrow \alpha_1 & & \downarrow \alpha_2 & & \downarrow \alpha_3 & \\
 & A & \xrightarrow{f} & B & \xrightarrow{g} & C & \longrightarrow 0 \\
 & \downarrow \beta_1 & & \downarrow \beta_2 & & \downarrow \beta_3 & \\
 0 & \longrightarrow & A' & \xrightarrow{f'} & B' & \xrightarrow{g'} & C' \\
 & \downarrow \gamma_1 & & \downarrow \gamma_2 & & \downarrow \gamma_3 & \\
 & U & \xrightarrow{\psi_1} & V & \xrightarrow{\psi_2} & W & \\
 & \downarrow & & \downarrow & & \downarrow & \\
 & 0 & & 0 & & 0 &
 \end{array}$$

则有正合列

$$R \xrightarrow{\varphi_1} S \xrightarrow{\varphi_2} T \xrightarrow{\rho} U \xrightarrow{\psi_1} V \xrightarrow{\psi_2} W$$



证明 STEP 1. 定义满足交换图的同态 $\varphi_1, \varphi_2, \psi_1, \psi_2$.

直接定义

$$\varphi_1 = \alpha_2^{-1} \circ f \circ \alpha_1, \quad \varphi_2 = \alpha_3^{-1} \circ g \circ \alpha_2, \quad (2.24)$$

由于 α_2 是单同态, 因此验证 φ_1 的良好性只需证明 $\text{Im } f \circ \alpha_1 \subset \text{Im } \alpha_2 = \text{Ker } \beta_2$ (φ_2 同理), 而这是因为

$$\beta_2 \circ (f \circ \alpha_1) = f' \circ (\beta_1 \circ \alpha_1) = 0. \quad (2.25)$$

同样直接定义

$$\psi_1 = \gamma_2 \circ f' \circ \gamma_1^{-1}, \quad \psi_2 = \gamma_3 \circ g' \circ \gamma_2^{-1}, \quad (2.26)$$

由于 γ_1 为满同态, 因此验证 ψ_1 的良好性只需证明 $\text{Ker } \gamma_1 = \text{Im } \beta_1 \subset \text{Ker } \gamma_2 \circ f'$ (ψ_2 同理), 而这是因为

$$(\gamma_2 \circ f') \circ \beta_1 = (\gamma_2 \circ \beta_2) \circ f = 0. \quad (2.27)$$

STEP 2. 定义满足交换图的同态 $\rho \in \text{Hom}_R(T, U)$.

直接定义

$$\rho = \gamma_1 \circ f'^{-1} \circ \beta_2 \circ g^{-1} \circ \alpha_3, \quad (2.28)$$

首先 g 满说明 $\text{Im } \alpha_3$ 中的元素在其中有原像, 为说明 ρ 在 g^{-1} 以及 f'^{-1} 位置的良好性, 只需分别证明

- $\text{Im } \beta_2 \circ g^{-1} \circ \alpha_3 \subset \text{Im } f' = \text{Ker } g'.$
- $\text{Ker } g = \text{Im } f \subset \text{Ker } \gamma_1 \circ f'^{-1} \circ \beta_2.$

第一点是因为 (注意 g 满)

$$g' \circ (\beta_2 \circ g^{-1} \circ \alpha_3) = \beta_3 \circ (g \circ g^{-1}) \circ \alpha_3 = \beta_3 \circ \alpha_3 = 0. \quad (2.29)$$

第二点是因为 (注意 f' 单)

$$(\gamma_1 \circ f'^{-1} \circ \beta_2) \circ f = \gamma_1 \circ (f'^{-1} \circ f') \circ \beta_1 = \gamma_1 \circ \beta_1 = 0 \quad (2.30)$$

STEP 3. 证明正合性.

1. $R \xrightarrow{\varphi_1} S \xrightarrow{\varphi_2} T$. 显然 $\varphi_2 \circ \varphi_1 = 0 \Rightarrow \text{Im } \varphi_1 \subset \text{Ker } \varphi_2$, 设 $s \in \text{Ker } \varphi_2$, 则

$$\varphi_2(s) = 0 \Leftrightarrow g(\alpha_2(s)) = 0 \Leftrightarrow \alpha_2(s) = f(a) \in \text{Ker } g = \text{Im } f, \quad (2.31)$$

进一步

$$0 = \beta_2(\alpha_2(s)) = \beta_2(f(a)) = f'(\beta_1(a)) \Rightarrow \beta_1(a) = 0, a \in \text{Ker } \beta_1 = \text{Im } \alpha_1, \quad (2.32)$$

即存在 $r \in R$ 使得 $a = \alpha_1(r)$, 因此 $s = \alpha_2^{-1}(f(\alpha_1(r))) = \varphi_1(s)$, 即得 $\text{Ker } \varphi_2 \subset \text{Im } \varphi_1$.

2. $S \xrightarrow{\varphi_2} T \xrightarrow{\rho} U$. 显然 $\rho \circ \varphi_2 = 0 \Rightarrow \text{Im } \varphi_2 \subset \text{Ker } \rho$, 设 $t \in \text{Ker } \rho$, 则

$$\rho(t) = 0 \Leftrightarrow \gamma_1 \circ f'^{-1} \circ \beta_2(g^{-1}(\alpha_3(t))) = 0 \Rightarrow f'^{-1}(\beta_2(g^{-1}(\alpha_3(t)))) = \beta_1(a) \in \text{Ker } \gamma_1 = \text{Im } \beta_1, \quad (2.33)$$

因此 $\beta_2(g^{-1}(t)) = f'(\beta_1(a)) = \beta_2(f(a))$, 说明 $g^{-1}(\alpha_3(t)) - f(a) = \alpha_2(s) \in \text{Ker } \beta_2 = \text{Im } \alpha_2$, 因此

$$t = \alpha_3^{-1} \circ g(f(a) + \alpha_2(s)) = \alpha_3^{-1}(g(\alpha_2(s))) \in \text{Im } \varphi_2, \quad (2.34)$$

即得 $\text{Ker } \rho \subset \text{Im } \varphi_2$.

3. $T \xrightarrow{\rho} U \xrightarrow{\psi_1} V$. 显然 $\psi_1 \circ \rho = 0 \Rightarrow \text{Im } \rho \subset \text{Ker } \psi_1$, 设 $u \in \text{Ker } \psi_1$, 则

$$0 = \psi_1(u) = \gamma_2(f'(\gamma_1^{-1}(u))) \Rightarrow f'(\gamma_1^{-1}(u)) = \beta_2(b) \in \text{Ker } \gamma_2 = \text{Im } \beta_2, \quad (2.35)$$

而

$$\beta_3(g(b)) = g'(\beta_2(b)) = g'(f'(\alpha_1^{-1}(u))) = 0 \Rightarrow g(b) = \alpha_3(t) \in \text{Ker } \beta_3 = \text{Im } \alpha_3, \quad (2.36)$$

因此

$$\rho(t) = \gamma_1(f'^{-1}(\beta_2(g^{-1}(\alpha_3(t)))) = \gamma_1 \circ f'^{-1}(\beta_2(b)) = \gamma_1 \circ f'^{-1} \circ f' \circ \gamma_1^{-1}(u) = u, \quad (2.37)$$

即得 $\text{Ker } \psi_1 \subset \text{Im } \rho$.

4. $U \xrightarrow{\psi_1} V \xrightarrow{\psi_2} W$. 显然 $\psi_2 \circ \psi_1 = 0 \Rightarrow \text{Im } \psi_2 \subset \text{Ker } \psi_1$, 设 $v \in \text{Ker } \psi_2$, 则

$$0 = \psi_2(v) = \gamma_3(g'(\gamma_2^{-1}(v))) \Rightarrow g'(\gamma_2^{-1}(v)) = \beta_3(c) \in \text{Ker } \gamma_3 = \text{Im } \beta_3, \quad (2.38)$$

g 满说明存在 $b \in B$ 使得 $c = g(b)$, 因此

$$g'(\beta_2(b)) = \beta_3(g(b)) = g'(\gamma_2^{-1}(v)) \Rightarrow \gamma_2^{-1}(v) - \beta_2(b) = f'(a') \in \text{Ker } g' = \text{Im } f', \quad (2.39)$$

故

$$\psi_1(\gamma_1(a)) = \gamma_2(f'(a)) = \gamma_2(\gamma_2^{-1}(v) - \beta_2(b)) = v \in \text{Im } \psi_1, \quad (2.40)$$

即得 $\text{Ker } \psi_2 \subset \text{Im } \psi_1$.

命题 2.5 (左正合函子)

若 $0 \rightarrow K \rightarrow M \rightarrow N \rightarrow 0$ 为正合列, 则对任意 R -模 X , 函子 $\text{Hom}_R(X, -), \text{Hom}_R(-, X)$ 是左正合的, 即有正合列

$$\begin{aligned} 0 &\longrightarrow \text{Hom}_R(X, K) \longrightarrow \text{Hom}_R(X, M) \longrightarrow \text{Hom}_R(X, N) \\ 0 &\longrightarrow \text{Hom}_R(N, X) \longrightarrow \text{Hom}_R(M, X) \longrightarrow \text{Hom}_R(K, X) \end{aligned}$$

注 称函子左正合, 若其在一个短正合列上的作用可以得到一个左正合列, 反之可定义右正合. 同时左、右正合的函子称为正合函子.

正合函子有一个等价定义

命题 2.6 (正合函子)

函子 F 正合 (不妨设它协变) 当且仅当它在正合列 $K \rightarrow M \rightarrow N$ 的作用 $F(K) \rightarrow F(M) \rightarrow F(N)$ 也是正合的.

证明 只需证明同时左右正合的函子满足上述性质. 设有正合列 $K \xrightarrow{f} M \xrightarrow{g} N$, 将其分裂可得短正合列 (注意 $\text{Im } f = \text{Ker } g$, 因此 $\text{Im } g \cong M/\text{Ker } g = M/\text{Im } f$)

$$0 \longrightarrow \text{Im } f \longrightarrow M \longrightarrow \text{Im } g \longrightarrow 0$$

特别地有左、右正合列 $0 \rightarrow \text{Im } g \rightarrow N, K \rightarrow \text{Im } f \rightarrow 0$, 并且 F 在其上的作用也可得左、右正合列, 即有下图

$$\begin{array}{ccccccc} & & 0 & & 0 & & \\ & & \uparrow & & \downarrow & & \\ 0 & \longrightarrow & F(\text{Im } f) & \longrightarrow & F(M) & \longrightarrow & F(\text{Im } g) \longrightarrow 0 \\ & & \uparrow & & \parallel & & \downarrow \\ & & F(K) & \xrightarrow{F(f)} & F(M) & \xrightarrow{F(g)} & F(N) \end{array}$$

由此可得 $\text{Im } F(f) = F(\text{Im } f), \text{Ker } F(g) = F(\text{Ker } g)$ (注意 $\text{Im } g \cong M/\text{Ker } g$), 故 $\text{Im } F(f) = \text{Ker } F(g)$.

定义 2.12 (可裂)

称短正合列 $0 \rightarrow K \rightarrow M \rightarrow N \rightarrow 0$ 可裂, 若它同构于 $0 \rightarrow K \rightarrow K \oplus N \rightarrow N \rightarrow 0$.

定理 2.7

正合列 $0 \rightarrow K \xrightarrow{\varphi} M \xrightarrow{\psi} N \rightarrow 0$ 可裂当且仅当其满足以下条件之一：

1. 存在 $\pi : M \rightarrow K$ 使得 $\pi \circ \varphi = \text{Id}_K$.
2. 存在 $j : N \rightarrow M$ 使得 $\psi \circ j = \text{Id}_N$.

$$0 \longrightarrow K \xrightarrow{\varphi} M \xrightarrow{\psi} N \longrightarrow 0$$

$\swarrow \pi$ $\nwarrow j$
 $\quad \quad \quad \quad \quad$

证明 可裂的正合列显然具有这一性质，只需证明另一边.

1. 此时定义同态

$$f : M \longrightarrow K \oplus N \quad (2.41)$$

$$m \longmapsto (\pi(m), \psi(m)) \quad (2.42)$$

则容易验证它满足如下交换图

$$\begin{array}{ccccccc} 0 & \longrightarrow & K & \xrightarrow{\varphi} & M & \xrightarrow{\psi} & N \longrightarrow 0 \\ & & \parallel & & \downarrow f & & \parallel \\ 0 & \longrightarrow & K & \longrightarrow & K \oplus N & \longrightarrow & N \longrightarrow 0 \end{array}$$

$\swarrow \pi$ $\nwarrow j$
 $\quad \quad \quad \quad \quad$

由短五引理得证.

2. 此时定义同态

$$g : K \oplus N \longrightarrow M \quad (2.43)$$

$$(k, n) \longmapsto \varphi(k) + j(n) \quad (2.44)$$

容易验证它满足如下交换图

$$\begin{array}{ccccccc} 0 & \longrightarrow & K & \longrightarrow & K \oplus N & \longrightarrow & N \longrightarrow 0 \\ & & \parallel & & \downarrow g & & \parallel \\ 0 & \longrightarrow & K & \xrightarrow{\varphi} & M & \xrightarrow{\psi} & N \longrightarrow 0 \end{array}$$

$\swarrow \pi$ $\nwarrow j$
 $\quad \quad \quad \quad \quad$

由短五引理得证.

2.3 自由模、投射模与内射模

本节默认 R 为交换幺环.

2.3.1 自由模

定义 2.13 (自由模)

设 M 为 R -模，若存在 $\{e_i : i \in I\}$ 使得对任意 $x \in M$ ，存在唯一 $a_i \in R, \forall i \in I$ (且只有有限个非 0) 使得 $x = \sum_i a_i e_i$ ，则称 M 为自由模， $\{e_i : i \in I\}$ 为 M 的一组基.

根据定义，若 $\{e_i : i \in I\}$ 为自由模 M 的一组基，则有 $M \cong \bigoplus_{i \in I} R e_i \cong \bigoplus_{i \in I} R$.

命题 2.7

自由模基集的势不依赖于基的选取.

证明 取 R 的极大理想 $\mathfrak{m}$, 则 $\mathfrak{m}M = \{\sum_i c_i e_i : c_i \in \mathfrak{m}\}$ 是 M 的子模, 并且

$$M/\mathfrak{m}M \cong \frac{\bigoplus_{i \in I} R}{\bigoplus_{i \in I} \mathfrak{m}} \cong \bigoplus_{i \in I} R/\mathfrak{m}, \quad (2.45)$$

因此由线性空间的情形即得.

命题 2.8 (自由模的泛性质)

设 N 为 R -模, M 为自由模, 基为 $\{e_i : i \in I\}$, 给定映射 $f : \{e_i : i \in I\} \rightarrow N$, 则存在唯一 R -模同态 $F : M \rightarrow N$ 使得 $F(e_i) = f(e_i)$.

$$\begin{array}{ccc} \{e_i : i \in I\} & \xrightarrow{f} & N \\ \downarrow \iota & \nearrow \exists! F & \\ M & & \end{array}$$

命题 2.9

任何 R -模都同构于某个自由模的商模.

证明 设 N 为 R -模, $\{y_i : i \in I\}$ 为 N 的生成元, 设 $\{e_i : i \in I\}$ 为 $\bigoplus_{i \in I} R$ 的标准基, 令 $f : \{e_i : i \in I\} \rightarrow N, e_i \mapsto y_i$, 则存在满同态 $F : \bigoplus_{i \in I} R \rightarrow N$, 由同态定理可知 $N \cong (\bigoplus_{i \in I} R)/\text{Ker } F$.

2.3.2 投射模 (projective)

定义 2.14 (投射模)

设 P 为 R -模, 称 P 为投射模, 若任给满同态 $u \in \text{Hom}_R(M, N)$, 以及 $f \in \text{Hom}_R(P, N)$, 存在提升 $F \in \text{Hom}_R(P, M)$ 使得 $f = u \circ F$.

$$\begin{array}{ccccc} M & \xrightarrow{u} & N & \longrightarrow & 0 \\ & \nwarrow \exists F & \uparrow f & & \\ & & P & & \end{array}$$

例 2.8 非投射模 考虑 $\mathbb{Z}$ -模 $\mathbb{Z}_6$, 则不存在提升 F , 因为这样的 F 必须满足 $0 = F(\bar{6}) = 6F(\bar{1})$.

$$\begin{array}{ccccc} \mathbb{Z} & \xrightarrow{u} & \mathbb{Z}_6 & \longrightarrow & 0 \\ & \nwarrow + & \uparrow \text{Id} & & \\ & & \mathbb{Z}_6 & & \end{array}$$

例 2.9 自由模是投射模 设 $\{e_i : i \in I\}$ 为自由模的基, 对任意 $i \in I$, 取 $x_i \in u^{-1}(f(e_i))$, 令 $F' : e_i \mapsto x_i$, 则根据自由模的泛性质可知存在唯一同态 F 使得 $F \circ \iota = F'$, 容易验证 $u \circ F = f$.

$$\begin{array}{ccccc} M & \xrightarrow{u} & N & \longrightarrow & 0 \\ & \nwarrow F & \uparrow f & & \\ & & \bigoplus_{i \in I} Re_i & & \\ & \nearrow F' & \uparrow \iota & & \\ & & \{e_i : i \in I\} & & \end{array}$$

例 2.10 投射模不一定是自由模 设 $\text{char } k \neq 2$, $R = k[x, y]/(x^2 + y^2 - 1)$, 则 $P = I = (x, y - 1)$ 是投射模, 但不是自由模.

$$\begin{array}{ccccc} M & \xrightarrow{u} & N & \longrightarrow & 0 \\ & \nwarrow F & \uparrow f & & \\ & & I & & \end{array}$$

对于同态 $f: I \rightarrow N$, 设 $n_1 = f(x), n_2 = f(y-1)$, 取 $m_1 \in u^{-1}(n_1), m_2 \in u^{-1}(n_2)$, 令 $F: I \rightarrow M, rx + s(y-1) = rm_1 + sm_2$, 则 F 是一个同态, 并且

$$u(F(rx + s(y-1))) = u(rm_1 + sm_2) = rn_1 + sn_2 = f(rx + s(y-1)), \quad (2.46)$$

故 I 为投射模.

下述命题说明给出了投射模的等价刻画, 并且说明自由模与投射模很相近 (相差一个直和项), 后面将证明 PID 上的投射模都是自由模.

命题 2.10 (投射模的等价刻画)

下述等价:

1. P 为投射 R -模.
2. 函子 $\text{Hom}_R(P, -)$ 正合.
3. 短正合列 $0 \rightarrow K \rightarrow M \rightarrow P \rightarrow 0$ 可裂.
4. P 为自由模的直和项, 即存在 P' 使得 $P \oplus P' \cong \bigoplus R$.

证明 $1 \Leftrightarrow 2$: 设有正合列 $0 \rightarrow K \xrightarrow{f} M \xrightarrow{g} N \rightarrow 0$, 函子 $\text{Hom}_R(P, -)$ 正合当且仅当有正合列

$$0 \longrightarrow \text{Hom}_R(P, K) \xrightarrow{f_L} \text{Hom}_R(P, M) \xrightarrow{g_L} \text{Hom}_R(P, N) \longrightarrow 0$$

而这当且仅当 g_L 为满同态 (因为它本身是左正合的), 即对任意 $u \in \text{Hom}_R(P, N)$, 存在 $v \in \text{Hom}_R(P, M)$ 使得 $u = g_L(v) = g \circ v$, 这实际上就是投射模性质的等价表述.

$1 \Rightarrow 3$: 根据投射模的定义, 存在 $j: P \rightarrow M$ 使得 $\psi \circ j = \text{Id}$, 故短正合列可裂.

$$\begin{array}{ccccccc} 0 & \longrightarrow & K & \xrightarrow{\varphi} & M & \xrightarrow{\psi} & P \longrightarrow 0 \\ & & & & & \nwarrow \exists j & \uparrow \text{Id} \\ & & & & & & P \end{array}$$

$3 \Rightarrow 4$: 由于任何 R 模都是自由模的商模, 因此首先存在右正合列 $\bigoplus_{i \in I} R \xrightarrow{\varphi} P \rightarrow 0$, 记 $P' = \text{Ker } \varphi$ 则有正合列

$$0 \longrightarrow P' \longrightarrow \bigoplus_{i \in I} R \xrightarrow{\varphi} P \longrightarrow 0$$

由可裂性得到 $\bigoplus_{i \in I} R \cong P \oplus P'$.

$4 \Rightarrow 1$: 设 π, ι 分别为 $\bigoplus R$ 到 P 的投影以及反过来的嵌入, 由于自由模是投射模, 因此存在 $F: \bigoplus R \rightarrow M$ 使得 $u \circ F = f \circ \pi$, 因此

$$u \circ (F \circ \iota) = f \circ (\pi \circ \iota) = f, \quad (2.47)$$

即 $F \circ \iota: P \rightarrow M$ 满足投射模的条件.

$$\begin{array}{ccccc} M & \xrightarrow{u} & N & \longrightarrow & 0 \\ \uparrow F & \nearrow f \circ \pi & \uparrow f & & \\ \bigoplus R & \xleftarrow{\iota} & P & \xrightarrow{\pi} & \end{array}$$

2.3.3 内射模 (injective)

定义 2.15 (内射模)

设 E 为 R -模, 称 E 为内射模, 若任给单同态 $v \in \text{Hom}_R(K, M)$, 以及 $f \in \text{Hom}_R(k, E)$, 存在 $\tilde{f} \in \text{Hom}_R(M, E)$ 使得 $f = \tilde{f} \circ v$.

$$\begin{array}{ccccc}
 0 & \longrightarrow & K & \xrightarrow{v} & M \\
 & & \downarrow f & \swarrow \exists \tilde{f} & \\
 & & E & &
 \end{array}$$

例 2.11 $\mathbb{Z}$ 作为 $\mathbb{Z}$ -模不是内射模，因为它是 PID 且不是可除的（这里提前使用了后面的 Baer 判别法）。

命题 2.11 (内射模的等价刻画)

下述等价：

1. E 为内射模.
2. $\text{Hom}_R(-, E)$ 正合.
3. 短正合列 $0 \rightarrow E \rightarrow M \rightarrow N \rightarrow 0$ 分裂.

证明 $1 \Leftrightarrow 2$: 设有正合列 $0 \rightarrow K \xrightarrow{f} M \xrightarrow{g} N \rightarrow 0$, 函子 $\text{Hom}_R(-, E)$ 正合当且仅当有正合列

$$0 \longrightarrow \text{Hom}_R(M, E) \xrightarrow{g^R} \text{Hom}_R(N, E) \xrightarrow{f^R} \text{Hom}_R(K, E) \longrightarrow 0$$

而这当且仅当 f^R 为满同态（因为函子本身左正合），即对任意 $u \in \text{Hom}_R(K, E)$, 存在 $v \in \text{Hom}_R(N, E)$ 使得 $u = f^R(v) = v \circ f$, 这实际上就是投射模性质的等价表述.

$1 \Rightarrow 3$: 根据内射模的定义, 存在 $\pi: M \rightarrow E$ 使得 $\pi \circ \varphi = \text{Id}$, 故短正合列可裂.

$$\begin{array}{ccccccc}
 0 & \longrightarrow & E & \xrightarrow{\varphi} & M & \xrightarrow{\psi} & N \longrightarrow 0 \\
 & & \downarrow \text{Id} & \swarrow \exists \pi & & & \\
 & & E & & & &
 \end{array}$$

$3 \Rightarrow 1$: 此时存在 $\pi: M \rightarrow E$ 使得 $\pi \circ f = \text{Id}$, 因此可定义 $\varphi: L \rightarrow M$ 为 $\varphi(x) = f(u(h^{-1}(x)))$, 若 $h^{-1}(x)$ 为空则令 $\varphi(x) = 0$, 则这是一个良定的同态（因为 h 单），并且

$$\varphi \circ h = f \circ u \Rightarrow (\pi \circ \varphi) \circ h = (\pi \circ f) \circ u = \text{Id} \circ u = u, \quad (2.48)$$

故 E 为内射模.

$$\begin{array}{ccccccc}
 0 & \longrightarrow & K & \xrightarrow{h} & L & & \\
 & & \downarrow u & \swarrow \pi \circ \varphi & \downarrow \varphi & & \\
 0 & \longrightarrow & E & \xrightarrow{f} & M & \xrightarrow{g} & N \longrightarrow 0 \\
 & & & \swarrow \exists \pi & & &
 \end{array}$$

命题 2.12

- 内射模的直积是内射模，但直和不是.
- 投射模的直和是内射模，但直积不是.

证明 考虑下图即可

$$\begin{array}{ccccc}
 0 & \longrightarrow & K & \longrightarrow & M \\
 & & \downarrow & \swarrow & \downarrow \\
 & & E_i & \swarrow & \\
 & & \uparrow & \swarrow & \\
 & & \prod_{i \in I} E_i & &
 \end{array}
 \qquad
 \begin{array}{ccccc}
 M & \longrightarrow & N & \longrightarrow & 0 \\
 \swarrow & & \uparrow & \swarrow & \\
 & & P_i & \swarrow & \\
 & & \downarrow & \swarrow & \\
 & & \bigoplus_{i \in I} P_i & &
 \end{array}$$

对于内射模，有一个非常有用的判别法.

定理 2.8 (Baer 判别法)

设 E 为 R -模, 则 E 为内射模当且仅当对任意 R 的理想 I 以及同态 $g \in \text{Hom}_R(I, E)$, 有如下交换图:

$$\begin{array}{ccccc} 0 & \longrightarrow & I & \hookrightarrow & R \\ & & \downarrow g & \swarrow \exists \bar{g} & \\ & & E & & \end{array}$$

证明 一边是显然的 (理想可视为 R -模), 假设满足定理条件,

$$\begin{array}{ccccc} 0 & \longrightarrow & K & \longrightarrow & M \\ & & \downarrow f & & \\ & & E & & \end{array}$$

基本思路是依次添加元素 (用到 Zorn 引理). 对于 $K \leq N \leq M$, 对任意 $x \in M$, 有满同态 $R \rightarrow (x), r \mapsto rx$, 因此存在 R 的理想 J 使得 $R/J \cong (x)$ (设同构为 ϕ), 这自然诱导一个理想同态 $(x) \cong I/J \triangleleft R/J$, 考虑如下交换图

$$\begin{array}{ccccc} 0 & \longrightarrow & I & \longrightarrow & R \\ & & \downarrow & & \downarrow \\ 0 & \longrightarrow & I/J & \longrightarrow & R/J \\ & & \cong \downarrow & & \cong \downarrow \\ 0 & \longrightarrow & (x) \cap N & \longrightarrow & (x) \\ & & \downarrow & \swarrow \exists F' & \swarrow \exists F \\ & & E & & \end{array}$$

根据假设存在 $F \in \text{Hom}_R(R, E)$, 这可以诱导出 F' (因为 F 将 J 映为 0, 这是良定的), 这可以诱导如下交换图 (相当于将 F' 和 h 粘起来得到 $\tilde{h}$, 上面证明了它们在 $N \cap (x)$ 是相等的).

$$\begin{array}{ccccc} 0 & \longrightarrow & N & \longrightarrow & N + (x) \\ & & \downarrow h & \swarrow \tilde{h} & \\ & & E & & \end{array}$$

下面用 Zorn 引理完成证明, 令 $\mathcal{X} = \{(N, h) : K \leq N \leq M, h \in \text{Hom}_R(N, E)\}$, $h|_K = f$ (上面的讨论保证了该集合非空), 定义其中的偏序关系为

$$(N_1, h_1) \leq (N_2, h_2) \Leftrightarrow N_1 \leq N_2, h_2|_{N_1} = h_1, \quad (2.49)$$

则对其中任意链, $\{(N_i, h_i) : i \in I\}$, 令 $N = \bigcup_{i \in I} N_i$ (显然 N 依然为子模), $h = \bigcup_{i \in I} h_i$, 这里 $h(x) = h_i(x), x \in N_i$, 则 (N, h) 是一个上界, 并且任何 $m \in M$ 都包含在 N 中, 即 $N = M$, h 满足交换图.

$$\begin{array}{ccccc} 0 & \longrightarrow & K & \longrightarrow & M \\ & & \downarrow f & \swarrow h & \\ & & E & & \end{array}$$

定义 2.16 (可除模)

设 E 为 R -模, 若对任意 $x \in E, 0 \neq r \in R$, 存在 $y \in E$ 使得 $x = ry$, 则称 E 为可除模.

定理 2.9

设 R 为 PID, E 为 R -模, 则 E 为内射模当且仅当它可除.

证明 $\Rightarrow$: 对任意 $x \in E, 0 \neq r \in R$ 以及同态 $f: (r) \rightarrow E, f(ar) = ax$, 有如下交换图

$$\begin{array}{ccccc} 0 & \longrightarrow & (r) & \hookrightarrow & R \\ & & f \downarrow & \swarrow \exists F & \\ & & E & & \end{array}$$

由于 $f(r) = x = F(r) = rF(1)$, 因此令 $y = F(1) \in X$ 可得 $x = ry$, 即 E 可除.

$\Leftarrow$: 若 E 可除, 设 $0 \neq I = (r) \triangleleft R$, 则对任意同态 $f: (r) \rightarrow E$, 设 $f(r) = x$, 则存在 $y \in E$ 使得 $x = ry$, 令 $F: R \rightarrow E, F(r) = ry$ 则有如下交换图成立, 由 Baer 判别法可得 E 为内射模.

$$\begin{array}{ccccc} 0 & \longrightarrow & (r) & \hookrightarrow & R \\ & & f \downarrow & \swarrow F & \\ & & E & & \end{array}$$

2.4 张量积

本节设 R 为交换幺环.

2.4.1 张量积的定义和性质

定义 2.17 (模的张量积)

设 M, N 为 R -模, 定义 M, N 的张量积为 $M \otimes_R N = U/Z$, 其中

$$U = \bigoplus_{(x,y) \in M \times N} R \cdot (x,y) \cong \bigoplus_{(x,y) \in M \times N} R, \quad (2.50)$$

是自由模, $Z \leq U$ 由所有形如

$$(x_1 + x_2, y) - (x_1, y) - (x_2, y), r(x, y) - (rx, y), \quad (2.51)$$

$$(x, y_1 + y_2) - (x, y_1) - (x, y_2), r(x, y) - (x, ry) \quad (2.52)$$

的元素生成. 记 U/Z 中元素 $\overline{(x,y)}$ 为 $x \otimes y \in M \otimes_R N$.

例 2.12 设 k 为域, V, W 为 k -线性空间, 有一组基 $e_1, \dots, e_n; f_1, \dots, f_m$, 则线性空间的张量积为 $V \otimes_k W$, 它也是一个线性空间, 有一组生成元 $e_i \otimes f_j$.

可以看出, 张量积实际上是一种带有双线性结构的“积”. 由于 $M \times N$ 为 U 的一组基, 因此对一个双线性映射 $F: M \times N \rightarrow K$, 有交换图

$$\begin{array}{ccc} M \times N & \xrightarrow{F} & K \\ \downarrow & \nearrow \tilde{F} & \\ U & & \end{array}$$

而 F 的双线性性说明 $Z \subset \text{Ker } \tilde{F}$, 特别地, 映射 $\theta: (x,y) \mapsto x \otimes y$ 也是双线性映射, 并且该映射的核恰好为 Z , 由此可以给出张量积的泛性质.

定理 2.10 (张量积的泛性质)

$(M \otimes_R N, \theta: M \times N \rightarrow M \otimes_R N)$ 满足对任意双线性映射 $F: M \times N \rightarrow K$, 存在唯一同态 $f: M \otimes_R N \rightarrow K$ 使得 $F = f \circ \theta$.

$$\begin{array}{ccc} M \times N & \xrightarrow{F} & K \\ \downarrow \theta & \nearrow \exists! f & \\ M \otimes_R N & & \end{array}$$

事实上, 泛性质可以唯一确定张量积, 若 (T, θ') 也满足上述泛性质, 考虑下图即可

$$\begin{array}{ccc} M \times N & \xrightarrow{\theta'} & T \\ \downarrow \theta & \swarrow \exists! f & \uparrow \exists! g \\ \text{Id} \circ M \otimes_R N & & \end{array}$$

回到一开始的例子, 下面证明 $e_i \otimes f_j$ 确实是 $V \otimes_k W$ 的一组基 (即线性无关). 令 $T = \bigoplus_{i,j} k\alpha_{ij}$ (某种自由线性空间), 构造双线性映射

$$F: V \times W \longrightarrow T \quad (2.53)$$

$$\left(\sum_i a_i e_i, \sum_j b_j f_j\right) \mapsto \sum_{i,j} a_i b_j \alpha_{ij} \quad (2.54)$$

则有以下图

$$\begin{array}{ccc} V \times W & \xrightarrow{F} & T \\ \downarrow \theta & \nearrow \exists! f & \\ V \otimes_k W & & \end{array}$$

由于 f 将 $e_i \otimes f_j$ 映为 α_{ij} , 像的线性无关性保证了 $e_i \otimes f_j$ 的线性无关性.

命题 2.13

1. $R \otimes_R M \cong M$.
2. $M \otimes_R N \cong N \otimes_R M$.
3. $(\bigoplus_{i \in I} M_i) \otimes_R N \cong \bigoplus_{i \in I} (M_i \otimes_R N)$.

证明 依次验证泛性质即可.

2.4.2 张量函子与平坦模

R -模范畴中的函子 $- \otimes_R N$ 将对象 M 映为 $M \otimes_R N$, 同时将 $\varphi \in \text{Hom}_R(M, M')$ 映为 $\varphi_* \in \text{Hom}_R(M \otimes_R N, M' \otimes_R N)$, $\varphi_*(x \otimes y) = \varphi(x) \otimes y$, 即满足如下交换图

$$\begin{array}{ccc} M \times N & \xrightarrow{\varphi \times \text{Id}_N} & M' \times N \\ \downarrow \theta & & \downarrow \theta' \\ M \otimes_R N & \xrightarrow{\varphi_*} & M' \otimes_R N \end{array}$$

定理 2.11 (张量函子的右正合性)

张量函子是右正合协变函子, 即对于短正合列 $0 \rightarrow M' \xrightarrow{i} M \xrightarrow{p} M'' \rightarrow 0$, 有

$$M' \otimes_R N \xrightarrow{i_*} M \otimes_R N \xrightarrow{p_*} M'' \otimes_R N \longrightarrow 0$$

证明 首先显然 p_* 为满射, 并且 $p_* \circ i_* = 0$ (说明 $\text{Im } i_* \subset \text{Ker } p_*$), 这就诱导同态 (并且是满的)

$$q: \frac{M \otimes_R N}{\text{Im } i_*} \longrightarrow M'' \otimes_R N, \quad (2.55)$$

注意到事实：双线性映射 $F: M \times N \rightarrow K$ 可以延拓到 $M'' \times N$ 上当且仅当 $F|_{M' \times N} = 0$ ，而由下图

$$\begin{array}{ccccc}
 M' \times N & \xrightarrow{\bar{i}} & M \times N & \xrightarrow{\bar{p}} & M'' \times N \\
 \downarrow \theta' & & \downarrow \theta & & \downarrow \\
 M' \otimes_R N & & M \otimes_R N & \xrightarrow{\exists F} & M'' \otimes_R N \\
 & \searrow \bar{i}_* & \downarrow & \swarrow \exists! \bar{q} & \\
 & & \frac{M \otimes_R N}{\text{Im } \bar{i}_*} & &
 \end{array}$$

首先由 $M' \otimes_R N$ 的泛性质诱导出 $\bar{i}_*$ 满足左边的交换图，显然左路映射将 $M' \times N$ 映为 0，根据上面的事实可知中间的双线性映射存在延拓 F ，而 $M'' \otimes_R N$ 的泛性质又诱导出 $\bar{q}$ ，容易验证它是 q 的逆，这就说明 $\text{Im } \bar{i}_* = \text{Ker } p_*$ 。

定义 2.18 (平坦模)

称 R -模 F 为平坦模，若函子 $- \otimes_R F$ 是正合的。

例 2.13

- R -模 R 就是平坦模，因为 $R \otimes_R M \cong M$ 。
- $\mathbb{Z}$ -模 $\mathbb{Z}_n$ 不是平坦的，考虑 $0 \rightarrow \mathbb{Z} \xrightarrow{\times n} \mathbb{Z}$ ，则 $0 \rightarrow \mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}_n \rightarrow \mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}_n$ 不是正合的。
- 平坦模的直和、直和项都是平坦的。
- 投射模是平坦模（它是自由模的直和项，自由模是 R 的直和）。

定理 2.12

设 F 为 R -模，则 F 平坦当且仅当对任意理想 $I \triangleleft R$ ，有正合列

$$0 \longrightarrow I \otimes_R F \longrightarrow R \otimes_R F \cong F$$

证明 一个方向显然；假设 F 满足上述性质，只需证明对任意正合列 $0 \rightarrow M' \rightarrow M$ ，有正合列 $0 \rightarrow M' \otimes_R F \rightarrow M \otimes_R F$ ，相当于证明张量函子将单同态映为单同态。事实上，问题可约化到 M, M' 为有限生成的情形（假设张量函子作用后的列不正合，则存在非零元 $\sum_i x_i \otimes y_i \mapsto 0$ ，也即在 U 中

$$\sum_i (x_i, y_i) = \sum_j r_j [(x_j^1 + x_j^2, z_j) - (x_j^1, z_j) - (x_j^2, z_j)] + \sum_j r'_j [(rx'_j, z'_j) - r(x'_j, z'_j)] + \cdots, \quad (2.56)$$

因此可以将 M' 替换为 $(\{x_i\})$ ， M 替换为 $(\{x_j^1, x_j^2, z_j, z'_j, \text{etc}\})$ 。

设 $M = (x_1, \cdots, x_n)$ ，对 n 归纳，当 $n = 1$ 时 $M = (x_1) \cong R/J$ ，因此直接不妨设 $M = R/J, M' = I/J$ ，将张量函子作用可得下图：

$$\begin{array}{ccccccc}
 & & 0 & & 0 & & 0 & & \text{Ker} \\
 & & \downarrow & & \downarrow & & \downarrow & & \downarrow \\
 0 & \longrightarrow & J & \longrightarrow & I & \longrightarrow & I/J & \longrightarrow & 0 \\
 & & \parallel & & \downarrow & & \downarrow & & \\
 0 & \longrightarrow & J & \longrightarrow & R & \longrightarrow & R/J & \longrightarrow & 0
 \end{array}
 \quad
 \begin{array}{ccccccc}
 & & 0 & & 0 & & 0 & & \text{Ker} \\
 & & \downarrow & & \downarrow & & \downarrow & & \downarrow \\
 0 & \longrightarrow & J \otimes F & \longrightarrow & I \otimes F & \longrightarrow & I/J \otimes F & \longrightarrow & 0 \\
 & & \parallel & & \downarrow & & \downarrow & & \\
 0 & \longrightarrow & J \otimes F & \longrightarrow & R \otimes F & \longrightarrow & R/J \otimes F & \longrightarrow & 0
 \end{array}$$

由蛇形引理可得正合列 $0 \rightarrow \text{Ker} \rightarrow 0$ ，因此 $\text{Ker} = 0$ ，说明 F 平坦。

假设命题对 $n - 1$ 成立，设

$$M = (x_1, \cdots, x_n), M_{n-1} = (x_1, \cdots, x_{n-1}), M'_{n-1} = M' \cap M_{n-1}, \quad (2.57)$$

同样用张量函子作用可得（注意 $M/M_{n-1} \cong (\overline{x_n})$ ）

同理考虑 $\mathbb{Z} \rightarrow \mathbb{Q}$ 可得 $M \otimes_{\mathbb{Z}} \mathbb{Q} \cong (\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Q}) \oplus (\mathbb{Z}_4 \otimes_{\mathbb{Z}} \mathbb{Q}) \cong \mathbb{Q}$.

- 考虑 $k[x] \rightarrow k(x)$, 则 $k[x, y] \otimes_{k[x]} k(x) \cong k(x)[y]$.

命题 2.14

设 $i: R \rightarrow S$ 为环同态, M 为 R -模, N 为 S -模, 则

- $M \otimes_R N$ 有一个 S -模结构.
- $M_S \otimes_S N = (M \otimes_R S) \otimes_S N \cong M \otimes_R N$ (作为 S -模).

证明

- 定义数乘 $(s, x \otimes y) \mapsto x \otimes (sy)$ (良定易证), 则赋予它一个 S -模结构.
- 直接考虑映射 $(x \otimes s) \otimes y \mapsto x \otimes (sy)$ 以及 $x \otimes y \mapsto (x \otimes 1) \otimes y$ 即可, 下图说明良定性

$$\begin{array}{ccc}
 (M \otimes_R S) \otimes_S N & \xrightarrow{f} & M \otimes_R N \\
 \uparrow & \nearrow F & \\
 (M \otimes_R S) \times N & & \\
 \uparrow & \nearrow \tilde{F} & \\
 (M \times S) \times N & &
 \end{array}
 \qquad
 \begin{array}{ccc}
 (M \otimes_R S) \otimes_S N & \longleftarrow & M \otimes_R N \\
 \nwarrow & & \uparrow \\
 & & M \times N
 \end{array}$$

推论 2.2

- 若 M 为平坦 R -模, 则 M_S 为平坦 S -模.
- 若 S 为平坦 R -模, N 为平坦 S -模, 则 N 为平坦 R -模.

证明 若 $N' \leq N$ 为 S 模, 则由下图易得.

$$\begin{array}{ccccc}
 0 & \longrightarrow & M_S \otimes_S N' & \longrightarrow & M_S \otimes_S N \\
 & & \parallel & & \parallel \\
 0 & \longrightarrow & M \otimes_R N' & \longrightarrow & M \otimes_R N
 \end{array}$$

2.5 PID 上有限生成模的结构

本节的主要目标是证明如下定理:

定理 2.13

设 R 为 PID, M 为有限生成 R -模, 则 $M \cong F \oplus M_t$, 其中 $F \cong R^r$ 为自由模, $M_t \leq M$ 为 M 的挠子模. 更准确来说, 存在 $d_1 | d_2 | \cdots | d_s \in R$ 使得 $M_t \cong R/(d_1) \oplus \cdots \oplus R/(d_s)$, 这里 r 唯一, 称为 M 的秩, $d_1, \dots, d_s$ 为非平凡因子, 在相伴意义下唯一, 称为不变因子 (借助唯一分解可得初等因子, 二者能相互决定).

定义 2.20 (挠元/扭元 (torsion))

设 R 为交换幺环, M 为 R -模, 取 $x \in M$, 定义 $\text{ann}(x) = \{r \in R : rx = 0\}$, 称为 x 的零化子. 若 $x \neq 0$ 且 $\text{ann}(x) \neq (0)$, 则称 x 为挠元.

注 也就是说挠元只是有非平凡零因子的元素.

命题 2.15

若 R 为整环, 设 $M_t = \{M \text{ 中的挠元} \} \cup \{0\}$, 则 $M_t \leq M$, 称为 M 的挠模.

例 2.15 设 $M = \mathbb{Z} \oplus \mathbb{Z}_4$, 则 $M_t = \mathbb{Z}_4$. 并且

$$\mathbb{Z}^2 / (\mathbb{Z} \begin{pmatrix} 2 \\ 0 \end{pmatrix}) = \frac{\mathbb{Z} \oplus \mathbb{Z}}{2\mathbb{Z} \oplus 0} \cong \mathbb{Z}_2 \oplus \mathbb{Z}, \quad (2.59)$$

$$\mathbb{Z}^2 / (\mathbb{Z} \begin{pmatrix} 2 \\ 2 \end{pmatrix}) = \frac{\mathbb{Z} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \oplus \mathbb{Z} \begin{pmatrix} 1 \\ 0 \end{pmatrix}}{\mathbb{Z} \begin{pmatrix} 2 \\ 2 \end{pmatrix}} \cong \mathbb{Z}_2 \oplus \mathbb{Z}. \quad (2.60)$$

定理 2.14

设 $K \leq R^n$, R^n 为自由模 (R 为 PID), 则 K 为自由模且 $\text{rk}(K) \leq n$.



证明 对 n 归纳, 当 $n=1$ 时 $K = (a) \triangleleft R$ (R 为 PID), 故为自由模 (整环蕴含某种单性, 保证了 a 为基). 假设命题对 $n-1$ 成立, 则 $R^n = R^{n-1} \oplus R$, 记 $K_{n-1} = K \cap R^{n-1} \cong R^k$ (归纳假设), 则有如下交换图

$$\begin{array}{ccccccc} & & 0 & & 0 & & 0 \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & K_{n-1} & \longrightarrow & K & \longrightarrow & K/K_{n-1} \longrightarrow 0 \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & R^{n-1} & \longrightarrow & R^{n-1} \oplus R & \longrightarrow & R \longrightarrow 0 \end{array}$$

其中同态 $K/K_{n-1} \rightarrow R \cong \frac{R^{n-1} \oplus R}{R^{n-1}}$ 可以自然诱导 (因为 $K_{n-1} \cong R^k \leq R^{n-1}$), 直接看出同态 $K \rightarrow R^n \rightarrow R$ 的核为 $K \cap R^{n-1} = K_{n-1}$, 诱导单同态 $K/K_{n-1} \rightarrow R$, 因此 $K/K_{n-1} \cong R$, R 为投射模说明

$$0 \longrightarrow R^k \longrightarrow K \longrightarrow R \longrightarrow 0$$

可裂, 因此 K 为自由模.

定理 2.15

设 $F = R^n, K \leq F$, 则存在 F 的基 $f_1, \dots, f_n$ 以及 $d_1 | d_2 | \dots | d_s$ 使得 $K = \bigoplus_{i=1}^s \langle d_i f_i \rangle$.



证明 由前述定理可得 $K = (x_1, \dots, x_n)$, 设 $e_1, \dots, e_n$ 为标准基, 并且设转移矩阵为 A , 即

$$(x_1, \dots, x_n) = (e_1, \dots, e_n)A, \quad (2.61)$$

则命题等价于将矩阵 A 相抵到 $\text{diag}(d_1, \dots, d_s, 0, \dots, 0)$.

STEP 1. 通过初等变换使得第一行、第一列只有 11 位置非零.

首先可作列变换使得第一列变为 $(s_1, 0, \dots, 0)^T$, 其中 s_1 为第一列的最大公因子, 进一步可通过行变换使得第一行变为 $(s_2, 0, \dots, 0)$, 其中 s_2 为经过第一次变换后的第一行的最大公因子, 因此 $s_2 | s_1, (s_1) \subset (s_2)$, 以此类推可得理想升链 $(s_1) \subset (s_2) \subset \dots$, 由 PID 的 Noether 性可知必有终止, 因此在某一步之后 11 位置的元素整除第一行列的所有元素, 即达到目标.

STEP 2.a. 若 s_1 整除矩阵中的所有元素, 则归纳即可.

STEP 2.b. 若 s_1 不整除某个 a_{ij} , 则将其复制到第一行, 重复前面的操作即可.

推论 2.3 (结构定理 (存在性))

设 $M = (x_1, \dots, x_n)$, 则 $M \cong R^n/K$, 并且存在 R^n 的基 $f_1, \dots, f_n$ 使得 $K \cong \bigoplus_{i=1}^s \langle d_i f_i \rangle$, 从而

$$M \cong \frac{Rf_1 \oplus \dots \oplus Rf_n}{R(d_1 f_1) \oplus \dots \oplus R(d_s f_s)} \cong \bigoplus_{i=1}^s R/(d_i) \oplus R^{n-s} = M_t \oplus F. \quad (2.62)$$



注 由此也可以看出, M 的扭子模必然是 M_t 部分的子模.

下面证明唯一性

证明 【唯一性的证明】首先证明秩的唯一性，与 $K = \text{Frac}(R)$ 张量可得（注意扭模张量分式域得到零模）

$$M \otimes_R K \cong (R^r \otimes_R K) \oplus \bigoplus_{i=1}^s (R/(d_i) \otimes_R K) \cong K^r, \quad (2.63)$$

即得秩是唯一性的。

再证不变因子的唯一性，由于不变因子与初等因子相互决定，设 $d_i = u_i p_1^{n_{i1}} \cdots p_k^{n_{ik}}$ ，则由中国剩余定理可得分解

$$M_t \cong \bigoplus_{i=1}^s R/(d_i) \cong \bigoplus_{i=1}^s \bigoplus_{j=1}^k R/(p_j^{n_{ij}}), \quad (2.64)$$

因此只需证明初等因子的唯一性，断言（回忆 $M \otimes R/I \cong M/MI$ ，这对 $0 \rightarrow I \rightarrow R \rightarrow R/I$ 张量积 M 即得），

$$R/(c) \otimes_R R/(d) \cong R/((c) + (d)) = R/(\gcd(c, d)), \quad (2.65)$$

借此可以通过张量 $R/(p_i^n)$, $n \geq n_{mi}$ 提取出含有 p_i 的项（称为 M 的 p_i -准素部分），记为

$$M_{p_i} = \bigoplus_{j=1}^s R/(p_i^{n_{ji}}) := N, \quad (2.66)$$

则依次考虑

$$\frac{N}{pN} = N \otimes R/(p), \frac{pN}{p^2N}, \dots, \frac{p^{n-1}N}{p^nN}, p^nN \quad (2.67)$$

即得。

2.5.1 矩阵的标准形理论

设 k 为域， $V = k^n$, $A \in M_n(k)$ ，则 V 可视为 $R = k[x]$ -模 V^A ，可以看出 V^A 为有限生成模，并且是扭模。设 $e_1, \dots, e_n$ 为 V 的标准基（线性空间基），考虑满同态

$$\eta: R^n \rightarrow V^A, \quad (r_1, \dots, r_n) \mapsto r_1 e_1 + \dots + r_n e_n, \quad (2.68)$$

设 $K = \text{Ker } \eta$ ，有正合列

$$0 \longrightarrow \text{Ker} \longrightarrow R^n \longrightarrow V^A \longrightarrow 0$$

则 $K = \text{Ker}$ 也是秩为 n 的自由模。事实上 K 有一组基

$$(\alpha_1, \dots, \alpha_n) = (e_1, \dots, e_n) \begin{pmatrix} x - a_{11} & -a_{12} & \cdots & -a_{1n} \\ -a_{21} & x - a_{22} & \cdots & -a_{2n} \\ \vdots & \vdots & \cdots & \vdots \\ -a_{n1} & -a_{n2} & \cdots & x - a_{nn} \end{pmatrix}, \quad (2.69)$$

设 K' 为 $xI - A$ 的列向量生成的子模，则 $xe_i \equiv a_{i1}e_1 + \dots + a_{in}e_n \pmod{K'}$ ，因此任意 $\text{Ker} \ni \beta = \sum_{i=1}^n g(x)e_i \equiv \sum_{i=1}^n b_i e_i \pmod{K'}$ ，根据基的线性无关性可得 $\beta \equiv 0$, $K' = \text{Ker}$ 。

由于 $(\alpha_1, \dots, \alpha_n) = (e_1, \dots, e_n)(xI - A)$ 为 Ker 的基，因此存在 $S, T \in GL_n(\mathbb{R})$ 使得

$$S(xI - A)T = \text{diag}(d_1(x), \dots, d_n(x)), \quad d_1 | \cdots | d_n, \quad (2.70)$$

因此

$$V^A \cong R^n / \text{Ker } \eta \cong R/(d_1(x)) \oplus \cdots \oplus R/(d_n(x)), \quad (2.71)$$

此即 Lambda 矩阵导出的有理标准型的原理。

例 2.16 设 $k = \mathbb{Q}$, $V \cong k^6$, A 为 V 上的线性变换，假设

$$V^A \cong \frac{\mathbb{Q}[x]}{(x^2 + 1)} \oplus \frac{\mathbb{Q}[x]}{(x^2 + 1)(x - 1)^2}, \quad (2.72)$$

则 $V^A = Rv_1 \oplus Rv_2$ ，并且 A 在 V^A 中向量上的作用相当于 x 在右边多项式商环上的乘法，因此断言 V^A 的基为

$(v_1, xv_1, v_2, xv_2, x^2v_2, x^3v_2)$, 并且

$$x(v_1, xv_1, v_2, xv_2, x^2v_2, x^3v_2) = (v_1, xv_1, v_2, xv_2, x^2v_2, x^3v_2)\text{diag}(C_1, C_2), \quad (2.73)$$

其中 C_1, C_2 分别为两个多项式的友方阵.

第3章 交换代数初步

本章设 R 为交换幺环.

3.1 Noether 环与 Artin 环

3.1.1 Noether 环与 Noether 模

定义 3.1 (Noether 环)

若交换环 R 满足 Noether 条件 (即理想升链必有终止), 则称之为 Noether 环.

例 3.1

- PID 和域都是 Noether 环.
- $\mathbb{R}$ 上的连续函数环不是 Noether 环.

命题 3.1 (Noether 环的等价刻画)

R 为 Noether 环当且仅当其所有理想均是有限生成的.

注 容易看出, R 为 Noether 环也可以用“任意理想集都有极大元”刻画.

定理 3.1 (Hilbert basis theorem)

若 R 为 Noether 环, 则其多项式环 $R[x]$ 也是 Noether 环.

注 这说明多元多项式环也是 Noether 环.

证明 设 $I \triangleleft R[x]$, $J_n = \{f \in I \text{ 的 } n \text{ 次项系数}\}$, 则 $J_n \triangleleft R$ 且有升链

$$J_0 \subset J_1 \subset J_2 \subset \cdots, \quad (3.1)$$

设 $J_n = J_{n+1} = (c_1, \cdots, c_m)$ (Noether), 则对任意 $f(x) = \sum_{i=0}^n a_i x^i \in I$, 其任意系数都在 J_n 中, 设 $a_i = r_{i1}c_1 + \cdots + r_{im}c_m$, 则

$$f(x) = \sum_{i=0}^n a_i x^i = \sum_{i=0}^n \sum_{j=1}^m r_{ij} c_j x^i = \sum_{j=1}^m c_j \sum_{i=0}^n r_{ij} x^i := \sum_{j=1}^m c_j g_j(x) \in R[x]J_n, \quad (3.2)$$

因此 I 是有限生成的, $R[x]$ 是 Noether 环.

注 一方面由于 $R[x, y] = R[x][y]$, 因此对应多元多项式环也是 Noether 环, 另一方面上面的证明可以直接推广到形式幂级数环中, 因此 Noether 环 R 上的 $R[[x]]$ 也是 Noether 环.

定义 3.2 (Noether 模)

设 M 为 R -模, 若 M 满足 Noether 性质, 则称它为 Noether 模.

注 M 为 Noether 模当且仅当其任意子模是有限生成的.

命题 3.2

- Noether 模的子模、商模都是 Noether 模.
- 设有正合列 $0 \rightarrow K \rightarrow M \rightarrow N \rightarrow 0$, 若 K, N 为 Noether 模, 则 M 是 Noether 模.
- 有限个 Noether 模的直和也是 Noether 模.
- 若 R 为 Noether 环, M 为有限生成 R -模, 则 M 是 Noether 模.

证明

1. 显然.
2. 取 $M' \leq M$, 则短五引理保证下图成立

$$\begin{array}{ccccccc} 0 & \longrightarrow & M' \cap K & \longrightarrow & M' & \longrightarrow & \frac{M'}{M' \cap K} \longrightarrow 0 \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & K & \longrightarrow & M & \longrightarrow & N \longrightarrow 0 \end{array}$$

因此 $M' \cap K, M'/M' \cap K$ 都是有限生成的, 即得 M' 是有限生成的 (同样考虑短五引理, 则 M' 是某个 R^{m+n} 的满同态像, 因此是有限生成的).

3. 由 2 得.
4. 若 $M = (x_1, \dots, x_n)$, 则 $M \cong R^n/K$, 由 1 可得 M 是 Noether 模.

3.1.2 Artin 环与 Artin 模

定义 3.3 (Artin 环与 Artin 模)

- 称 R 为 Artin 环, 若其中任意理想降链都有终止.
- 称 R -模 M 为 Artin 模, 若其中任意子模降链都有终止.



注 Artin 环也可以用“任意理想集都有极小元”刻画.

命题 3.3

与 Noether 环类似, 对于正合列 $0 \rightarrow M' \rightarrow M \rightarrow M'' \rightarrow 0$, M 是 Artin 模当且仅当 M', M'' 是 Artin 模.



例 3.2

- $\mathbb{Z}_n$ 是 Artin 环.
- $k[x]/(x^2(x-1)), \mathbb{Q}[x]/(x^2+1)$ 也是 Artin 环.
- $k[x, y]/(x^2, y^2)$ 是 Artin 环.

命题 3.4

设 R 为 Artin 环, 则

1. R 的素理想都是极大理想.
2. R 只有有限多个极大理想 (设为 $\mathfrak{m}_1, \dots, \mathfrak{m}_n$).
3. 设 $J = \mathfrak{m}_1 \cap \dots \cap \mathfrak{m}_n$, 则存在 $r > 0$ 使得 $J^r = 0$.
4. $R \cong \prod_{i=1}^n R/\mathfrak{m}_i^r$ (同时作为环同构与 R -模同构).
5. R 为 Noether 环.



证明

1. 设 $\mathfrak{p} \triangleleft R$ 为素理想, 则只需证明 Artin 整环 $R/\mathfrak{p}$ 是域. 任取 $0 \neq \bar{x} \in R/\mathfrak{p}$, 考虑降链 $(\bar{x}) \supset (\bar{x}^2) \supset \dots$, 则必然存在 N 使得 $(\bar{x}^N) = (\bar{x}^{N+1})$, 即存在 $\bar{y}$ 使得 (整环的消去律)

$$\bar{x}^N = \bar{x}^{N+1}\bar{y} \Rightarrow \bar{x}\bar{y} = \bar{1}. \quad (3.3)$$

2. 假设 R 有无穷多个极大理想, 取可数个 $\mathfrak{m}_1, \dots, \mathfrak{m}_n, \dots$, 则有降链

$$\mathfrak{m}_1 \supset \mathfrak{m}_1 \cap \mathfrak{m}_2 \supset \dots, \quad (3.4)$$

设有终止 $\mathfrak{m}_1 \cap \dots \cap \mathfrak{m}_{N-1} = \mathfrak{m}_1 \cap \dots \cap \mathfrak{m}_N$, 则 $\mathfrak{m}_1 \cap \dots \cap \mathfrak{m}_{N-1} \subset \mathfrak{m}_N$, 则必然存在某个 $\mathfrak{m}_i \subset \mathfrak{m}_N$ (这是一个关于素理想的命题, 见附录), 与极大性矛盾.

3. J 即为 Jacobson 根, 考虑理想降链 $J \supset J^2 \supset \dots$, 则可取 $r > 0$ 使得 $J^r = J^{r+1}$, 考虑理想集 $\mathcal{J} = \{I \subset J^r : IJ^r \neq 0\}$ (不妨设其非空), 由 Artin 性可知 $\mathcal{J}$ 有极小元 I_0 , 因此存在 $x \in I_0$ 使得 $xJ^r \neq 0$, 极小性保证 $I_0 = (x)$. 而 $xJ^r = xJ^{r+1} = (xJ)J^r$, 再由极小性可知 $I_0 = (x) = xJ$, 因此存在 $a \in J$ 使得

$$x = xa, (1-a)x = 0, x = 0.$$

4. 由于 $\mathfrak{m}_1^r \cdots \mathfrak{m}_n^r \subset \mathfrak{m}_1^r \cap \cdots \cap \mathfrak{m}_n^r \subset (\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_n)^r = J^r = 0$, 因此由中国剩余定理可得

$$R \cong R/J^r = \frac{R}{\mathfrak{m}_1^r \cap \cdots \cap \mathfrak{m}_n^r} \cong \prod_{i=1}^n R/\mathfrak{m}_i^r, \quad (3.5)$$

5. 只需证明对任意 $r > 0$, $R/\mathfrak{m}^r$ 是 Noether 模. $r = 1$ 时平凡 (域为 Noether 模), 假设 $r > 1$, $R/\mathfrak{m}^{r-1}$ 是 Noether 模, 考虑正合列

$$0 \longrightarrow \mathfrak{m}^{r-1}/\mathfrak{m}^r \longrightarrow R/\mathfrak{m}^r \longrightarrow R/\mathfrak{m}^{r-1} \longrightarrow 0$$

并且 $\mathfrak{m}^{r-1}/\mathfrak{m}^r$ 是 $k = R/\mathfrak{m}$ -线性空间, 因此它是 Artin k -模 (域上 Artin 模与 Noether 模等价), 因此它是有限维的, 从而是 Noether 模, 故 $R/\mathfrak{m}^r$ 是 Noether 模.

注 Artin 环作为 R -模有长度有限的合成列.

命题 3.5

模 M 长度有限当且仅当它既是 Noether 模, 也是 Artin 模.

证明 一边显然, 反之设 M 同时是 Noether Artin 模, $\mathcal{X}$ 为 M 的长度有限的子模集合, 则它有极大元 N (Noether 性质), 若 $N \neq M$, 则设 $\mathcal{Y}$ 为 M 的真包含 N 的子模的集合, 它有极小元 N_0 (Artin 性质), 并且 N_0/N 为单模, 但 N_0 与 N 的极大性矛盾.

3.2 局部化

3.2.1 环的局部化

定义 3.4 (乘性子集)

交换环 R 中的乘法么半群 S 称为乘性子集.

借助乘性子集, 可按照以下步骤构造环 $S^{-1}R$, 称为 R 关于 S 的局部化.

1. $S^{-1}R = S \times R / \sim$, 其中 $(s_1, r_1) \sim (s_2, r_2)$ 当且仅当存在 $s \in S$ 使得 $s(s_1 r_2 - s_2 r_1) = 0$, 并记 $\overline{(r, s)} \in S^{-1}R$ 为 $\frac{r}{s}$, 则它可以对 S 中元素约分.
2. 定义加法与乘法为

$$\frac{r_1}{s_1} + \frac{r_2}{s_2} = \frac{s_2 r_1 + s_1 r_2}{s_1 s_2}, \quad \frac{r_1}{s_1} \cdot \frac{r_2}{s_2} = \frac{r_1 r_2}{s_1 s_2}. \quad (3.6)$$

则在该运算下 $S^{-1}R$ 为交换么环.

例 3.3

- 若 R 为整环, $S = R \setminus \{0\}$, 则 $S^{-1}R = \text{Frac}(R)$.
- 若 $R = \mathbb{Z}, S = \{1, 2, 2^2, \dots\}$, 则 $S^{-1}\mathbb{Z} = \{\frac{a}{2^n} : n \geq 0, a \in \mathbb{Z}\}$.
- 取非幂零元 $x \in R$ 以及 $S = \{1, x, x^2, \dots\}$, 则 $S^{-1}R = \{\frac{a}{x^n} : a \in R, n \in \mathbb{Z}\} := R_x$.
- $k[x]_x = \{\frac{f(x)}{x^m} : m \geq 0, f \in k[x]\}$.
- 设 $\mathfrak{p}$ 为 R 的素理想, 则 $S = R \setminus \mathfrak{p}$ 为乘性子集, $S^{-1}R = R_{\mathfrak{p}}$ 是一个局部环 (后证).
- 若 $S = U(R)$, 则 $S^{-1}R \cong R$.

对于环 R 和局部化环 $S^{-1}R$, 显然有嵌入 $\iota: R \hookrightarrow S^{-1}R, r \mapsto \frac{r}{1}$, 并且 $\iota(S) \subset U(S^{-1}R)$, $\text{Ker } \iota = \{r \in R : sr = 0, \exists s \in S\}$.

定理 3.2 (局部化环的泛性质)

若有环同态 $\varphi: R \rightarrow R'$ 且 $\varphi(S) \subset U(R')$, 则它可以唯一延拓为 $\tilde{\varphi}: S^{-1}R \rightarrow R'$, 即下图成立

$$\begin{array}{ccc} R & \xrightarrow{\varphi} & R' \\ \downarrow \iota & \nearrow \exists! \tilde{\varphi} & \\ S^{-1}R & & \end{array}$$

注 $\tilde{\varphi}(\frac{r}{s}) = \frac{\varphi(r)}{\varphi(s)}$.

3.2.2 模的局部化**定义 3.5 (模的局部化)**

设 M 为 R -模, $S \subset R$ 为乘性子集, 定义 $S^{-1}M = S \times M / \sim$, 其中

$$(s_1, x_1) \sim (s_2, x_2) \Leftrightarrow \exists s \in S, s(s_1x_2 - s_2x_1) = 0, \quad (3.7)$$

记 $\overline{(s, x)} \in S^{-1}M$ 为 $\frac{x}{s}$, 则 $S^{-1}M$ 是一个 $S^{-1}R$ 模, 称为 M 关于 S 的局部化模.

注 $S^{-1}R$ 模- $S^{-1}M$ 中的加法和数乘定义为

$$\frac{x_1}{s_1} + \frac{x_2}{s_2} = \frac{s_2x_1 + s_1x_2}{s_1s_2}, \quad \frac{r}{s} \cdot \frac{x}{s'} = \frac{rx}{ss'}. \quad (3.8)$$

对于模 M 和局部化模 $S^{-1}M$, 显然有嵌入 $\iota: M \hookrightarrow S^{-1}M, x \mapsto \frac{x}{1}$, 并且根据等价关系的定义, $\text{Ker } \iota = \{m \in M : sm = 0, \exists s \in S\}$.

定理 3.3 (局部化模的泛性质)

设 N 为 $S^{-1}R$ -模, 若有 R -模同态 $\psi: M \rightarrow N$, 则它可以唯一延拓为 $\tilde{\psi}: S^{-1}M \rightarrow N$, 即下图成立

$$\begin{array}{ccc} M & \xrightarrow{\psi} & N \\ \downarrow \iota & \nearrow \exists! \tilde{\psi} & \\ S^{-1}M & & \end{array}$$

注 $\tilde{\psi}(\frac{x}{s}) = \frac{1}{s}\psi(x)$.

命题 3.6

- $S^{-1}M \cong S^{-1}R \otimes_R M$.
- 若有 $0 \rightarrow M' \rightarrow M$, 则 $0 \rightarrow S^{-1}M' \rightarrow S^{-1}M$.
- $S^{-1}: \mathcal{M}_R \rightarrow \mathcal{M}_{S^{-1}R}$ 是正合函子.

注 对任意 R -模 M , $S^{-1}R \otimes_R M$ 具有 $S^{-1}R$ -模结构 (类比基变换).

证明

1. 首先有 R -模同态

$$f: M \rightarrow S^{-1}R \otimes_R M, \quad x \mapsto 1 \otimes x, \quad (3.9)$$

f 可由局部化模的泛性质唯一延拓为 $S^{-1}R$ -模同态

$$\tilde{f}: S^{-1}M \rightarrow S^{-1}R \otimes_R M, \quad \frac{x}{s} \mapsto \frac{1}{s} \otimes x \quad (3.10)$$

另一方面考虑 R -双线性映射

$$g: S^{-1}R \times M \rightarrow S^{-1}M, \quad \left(\frac{r}{s}, x\right) \mapsto \frac{rx}{s}, \quad (3.11)$$

g 可由张量积的泛性质延拓为 R -模同态

$$\tilde{g} : S^{-1}R \otimes_R M \rightarrow S^{-1}M, \quad \frac{r}{s} \otimes x \mapsto \frac{rx}{s} \quad (3.12)$$

并且 $\tilde{g}$ 实际上是 $S^{-1}R$ 模同态, 容易验证 $\tilde{f} \circ \tilde{g} = \text{Id}, \tilde{g} \circ \tilde{f} = \text{Id}$, 得证.

$$\begin{array}{ccc} M & \xrightarrow{f} & S^{-1}R \otimes_R M \\ \downarrow & \nearrow \exists! \tilde{f} & \\ S^{-1}M & & \end{array} \quad \begin{array}{ccc} S^{-1}R \times M & \xrightarrow{g} & S^{-1}M \\ \downarrow & \nearrow \exists! \tilde{g} & \\ S^{-1}R \otimes_R M & & \end{array}$$

2. 设 $f : M' \rightarrow M$ 为单同态, $f_* : S^{-1}M' \rightarrow S^{-1}M$, 则 $f_*(\frac{x'}{s}) = \frac{f(x')}{s} = 0$ 当且仅当存在 $a \in S$ 使得 $af(x') = f(ax') = 0$, f 单说明 $ax' = 0$, 因此 $\frac{x'}{s} = 0$, 故 $f_* = S^{-1}f$ 为单同态.
3. 2 说明局部化函子左正合, 根据 1 以及张量函子右正合可知局部化函子右正合.

推论 3.1

- $S^{-1}R$ 为平坦 R -模.
- $S^{-1}(M \oplus N) \cong S^{-1}M \oplus S^{-1}(N)$.
- $S^{-1}(M \otimes_R N) \cong S^{-1}M \otimes_{S^{-1}R} S^{-1}N$.
- $S^{-1}(M/L) \cong S^{-1}M/S^{-1}L, S^{-1}(M \cap N) \cong S^{-1}M \cap S^{-1}N$.

证明

1. S^{-1} 正合说明 $S^{-1}R$ 诱导的张量函子正合.
2. 同样转化到张量函子.
3. 使用基变换的一个结论: 若 $R \rightarrow S, M, N$ 分别为 R, S 模, 则 $M_S \otimes_S N \cong M \otimes_R N$; 这里有 $R \rightarrow S^{-1}R$, 并且 $N, S^{-1}M$ 分别为 $R, S^{-1}R$ 模, 因此

$$S^{-1}(M \otimes_R N) \cong S^{-1}R \otimes_R (M \otimes_R N) \cong S^{-1}M \otimes_R N \cong S^{-1}M \otimes_{S^{-1}R} S^{-1}N. \quad (3.13)$$

例 3.4 设 $R = \mathbb{R}[x, y], S = \{1, x, x^2, \dots\}$, 则 $S^{-1}R = \{\frac{f(x, y)}{x^n} : f \in R, n \in \mathbb{N}\}$, 考虑 R -模

$$M = \frac{\mathbb{R}[x, y]}{(xy, x(x-1))} \cong \frac{\mathbb{R}[x, y]}{(x)} \oplus \frac{\mathbb{R}[x, y]}{(y, x-1)}, \quad (3.14)$$

作局部化得到

$$M_x = S^{-1}R \otimes_R \frac{\mathbb{R}[x, y]}{(xy, x(x-1))} = S^{-1}R \otimes_R \left(\frac{\mathbb{R}[x, y]}{(x)} \oplus \frac{\mathbb{R}[x, y]}{(y, x-1)} \right) \cong \{0\} \oplus \mathbb{R}. \quad (3.15)$$

上面的 R 中元素可看作平面上的二元多项式函数, 其局部化环 $S^{-1}R$ 中的元素可看作定义在 y 轴之外的二元有理函数, 而模 M 中的元素则为定义在 y 轴以及 $(1, 0)$ 点处的二元多项式函数, 对模 M 作局部化后的模 M_x 可以看作定义在 $\{x \neq 0\} \cap \{(0, y), (1, 0)\} = \{(1, 0)\}$ 的多项式函数 (可理解为限制在一个开集上), 而这显然与 $\mathbb{R}$ 同构.

3.2.3 理想的局部化

定义 3.6 (理想的扩充与收缩)

- 设 $I \leq R$ (视为 R -子模), $S \subset R$ 为乘性子集, 则 $I^e := S^{-1}I \leq S^{-1}R$, 称为 I 的扩充.
- 设 $\iota : R \hookrightarrow S^{-1}R$ 为嵌入, 则对任意理想 $J \leq S^{-1}R$, 称 $J^c := \iota^{-1}(J) \leq R$ 为 J 的收缩.

记 $\mathcal{I}_R, \mathcal{I}_{S^{-1}R}$ 为二者理想的全体, 则扩充与限制可以视为二者之间的映射, 并且 $\iota^{-1} : \mathcal{I}_{S^{-1}R} \rightarrow \mathcal{I}_R$ 为单射.

命题 3.7

- 对任意 $J \in \mathcal{I}_{S^{-1}R}$ 有 $S^{-1}J^c = J$.
- 对任意 $I \in \mathcal{I}_R$ 有 $(S^{-1}I)^c \supset I$.

证明

1. 对任意 $\frac{r}{s} \in S^{-1}J^c \subset S^{-1}R, r \in J^c$ 有

$$\iota(r) \in J \Rightarrow \frac{r}{s} = \frac{1}{s}\iota(r) \in J, \quad (3.16)$$

反之设 $\frac{r}{s} \in J \subset S^{-1}R$, 则 $\psi(r) = \frac{r}{1} = s\frac{r}{s} \in J$, 因此 $r \in J^c, \frac{r}{s} \in S^{-1}J^c$.

2. 对任意 $r \in I$ 有 $\iota(r) \in S^{-1}I$, 因此 $r \in \iota^{-1}(S^{-1}I) = (S^{-1}I)^c$.

下例说明上面的包含关系未必取等.

例 3.5 设 $R = \mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}, I = (\bar{2}), S = (\bar{1}, \bar{3})$, 则 $S^{-1}R = \mathbb{Z}/2\mathbb{Z} = S^{-1}I$, 因此

$$(S^{-1}I)^c = \iota^{-1}(S^{-1}I) = \iota^{-1}(S^{-1}R) = R \supsetneq I. \quad (3.17)$$

记 $\text{Spec}(R)$ 为 R 的非平凡素理想集, $\text{Max}(R)$ 为 R 的极大理想集, 则 $\iota^{-1}: \mathcal{I}_{S^{-1}R} \rightarrow \mathcal{I}_R$ 诱导单射

$$\text{Spec}(S^{-1}R) \longrightarrow \text{Spec}(R), \quad (3.18)$$

因为对于 $Q \in \text{Spec}(S^{-1}R)$, 若 $ab \in Q^c$ 则 $\iota(ab) = \iota(a)\iota(b) \in Q$, 因此有 $\iota(a) \in Q$ 或 $\iota(b) \in Q$, 即 $a \in Q^c$ 或 $b \in Q^c$.

命题 3.8

$\text{Spec}(S^{-1}R)$ 中理想与 $\{\mathfrak{p} \in \text{Spec}(R) : \mathfrak{p} \cap S = \emptyset\}$ 一一对应.

证明 设 $Q \in \text{Spec}(S^{-1}R)$, 假设存在 $s \in Q^c \cap S$, 则 $1 = \frac{s}{s} \in Q$, 与素理想矛盾, 故 $Q^c \in RHS$, 并且对任意 $ab \in Q^c$ 有 $\iota(ab) = \iota(a)\iota(b) \in Q$, 因此有 $\iota(a) \in Q$ 或 $\iota(b) \in Q$, 即 $a \in Q^c$ 或 $b \in Q^c$, 即 Q^c 为素理想.

反之对于 $P \in RHS$, 任意 $\frac{x_1}{s_1} \cdot \frac{x_2}{s_2} = \frac{x_1x_2}{s_1s_2} \in P^e$, 存在 $s \in S$ 使得 $sx_1x_2 \in P$, 因此 $x_1x_2 \in P$, 必有 $x_1 \in P$ 或 $x_2 \in P$, 即 $\frac{x_1}{s_1} \in P^e$ 或 $\frac{x_2}{s_2} \in P^e$.

3.2.4 局部环

定义 3.7 (局部环)

称 $(R, \mathfrak{m})$ 为局部环, 若 R 为环且 $\mathfrak{m}$ 为 R 的唯一极大理想, 并且称 $R/\mathfrak{m}$ 为留数域.

注 $\mathfrak{m}$ 为 R 的唯一极大理想当且仅当 $U(R) = R \setminus \mathfrak{m}$.

例 3.6

- 设 $0 \in \mathbb{R}$, R 为 0 附近的光滑函数的全体, $\mathfrak{m} = \{f(x) \in R : f(0) = 0\}$ 为 R 的唯一极大理想, 因此 $(R, \mathfrak{m})$ 为局部环.
- 设 $R = k[x], P = (x) = xR, S = R \setminus P$, 则 $R_{(x)} = \{\frac{g(x)}{f(x)} : g \in k[x], f(0) \neq 0\}$, $P_{(x)} = \{\frac{xh(x)}{f(x)} : h \in k[x], f(0) \neq 0\}$, 则 $(R_{(x)}, P_{(x)})$ 是局部环.
- 设 $M = k[x]/(x(x-1))$, 则 $M_{(x)} = k[x]/(x), (x-1)_{(x)} = R_{(x)}$.

定理 3.4 (局部化得到局部环)

设 $\mathfrak{p} \in \text{Spec}(R)$, 则

1. $(R_{\mathfrak{p}}, \mathfrak{p}R_{\mathfrak{p}})$ 为局部环.
2. $R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}} \cong \text{Frac}(R/\mathfrak{p})$.

注 该命题说明, 关于素理想作局部化可得局部环, 特别的, 极大理想都是素理想, 因此关于极大理想局部化也可得局部环.

证明

1. $\frac{a}{b} \in R_{\mathfrak{p}} \setminus \mathfrak{p}R_{\mathfrak{p}}$ 当且仅当则 $a, b \notin \mathfrak{p}$, 因此 $\frac{b}{a} \in R_{\mathfrak{p}}$, 即得 $U(R_{\mathfrak{p}}) = R_{\mathfrak{p}} \setminus \mathfrak{p}R_{\mathfrak{p}}$.
2. 设 $\iota: R \rightarrow R_{\mathfrak{p}}$, 由于 $\iota(\mathfrak{p}) \subset \mathfrak{p}R_{\mathfrak{p}}$, 因此可诱导单同态 $\bar{\iota}: R/\mathfrak{p} \rightarrow R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}}$, 根据分式域的泛性质, 它诱导同态 $\tilde{\iota}: \text{Frac}(R/\mathfrak{p}) \rightarrow R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}}$, 易验证这是同构.

例 3.7

- 设 $R = k[x, y], P = (x), R_P = \left\{ \frac{g(x, y)}{f(x, y)} : x \nmid f(x, y) \right\}$, 则 $R_P / PR_P \cong k(\dots) = k(y)$.
- 若 $\mathfrak{m}$ 为极大理想, 则 $R_{\mathfrak{m}} / \mathfrak{m}R_{\mathfrak{m}} \cong R / \mathfrak{m}$ (极大理想必定是素理想).

命题 3.9

设 M 为 R -模, 则如下等价

1. $M = 0$.
2. 对任意 $\mathfrak{p} \in \text{Spec}(R)$, $M_{\mathfrak{p}} = 0$.
3. 对任意 $\mathfrak{m} \in \text{Max}(R)$, $M_{\mathfrak{m}} = 0$.

证明 只证 $3 \Rightarrow 1$: 若不然, 则取 $0 \neq x \in M$, $\text{ann}(x) = \{r \in R : rx = 0\} < R$, 取包含 $\text{ann}(x)$ 的极大理想 $\mathfrak{m}$, 则在 $M_{\mathfrak{m}}$ 中 $\frac{x}{1} = 0$, 因此存在 $s \in R \setminus \mathfrak{m}$ 使得 $sx = 0 \Rightarrow s \in \text{ann}(x) \subset \mathfrak{m}$, 矛盾.

推论 3.2

设 M, N 为 R -模, 则 $M \rightarrow N \rightarrow 0$ 当且仅当对任意 $\mathfrak{m} \in \text{Max}(R)$ 有 $M_{\mathfrak{m}} \rightarrow N_{\mathfrak{m}} \rightarrow 0$.

证明 $\Leftarrow$: 设 $M \rightarrow N \rightarrow \text{coker}$, 对任意极大理想 $\mathfrak{m}$, 根据张量函子的右正合性可得 $M_{\mathfrak{m}} \rightarrow N_{\mathfrak{m}} \rightarrow \text{coker}_{\mathfrak{m}}$, 因此 $\text{coker}_{\mathfrak{m}} = 0, \forall \mathfrak{m}$, 因此 $\text{coker} = 0$.

命题 3.10

设 $(R, \mathfrak{m})$ 为局部环, M 是有限生成 R -模, 则

1. $M = 0$ 当且仅当 $M/\mathfrak{m}M = 0$.
2. $M \rightarrow N \rightarrow 0$ 当且仅当 $M/\mathfrak{m}M \rightarrow N/\mathfrak{m}N \rightarrow 0$.

注 回忆 $M/\mathfrak{m}M \cong R/\mathfrak{m} \otimes M$.

证明

1. $\Leftarrow$: 此时 $\mathfrak{R} = \mathfrak{m}$, 因此当 $\mathfrak{m}M = \mathfrak{R}M = M$ 时, 根据 Nakayama 引理可知 $M = 0$.
2. 考虑 coker , 由 1 可得 (后者相当于前者被张量函子作用).

推论 3.3

设 R 为 Noether 环, M 为有限生成 R -模, 则 $M \rightarrow N \rightarrow 0$ 当且仅当对任意 $\mathfrak{m} \in \text{Max}(R)$ 有 $M/\mathfrak{m}M \rightarrow N/\mathfrak{m}N \rightarrow 0$.

证明 设 $M \rightarrow N \rightarrow \text{coker}$, 则 $\text{coker} = 0$ 当且仅当对任意 $\mathfrak{m} \in \text{Max}(R)$ 有 $\text{coker}_{\mathfrak{m}} = 0$, 而 $(R_{\mathfrak{m}}, \mathfrak{m}R_{\mathfrak{m}})$ 是局部环, $\text{coker}_{\mathfrak{m}}$ 是有限生成 $R_{\mathfrak{m}}$ 模, 因此 $\text{coker}_{\mathfrak{m}} = 0$ 当且仅当 $\text{coker}_{\mathfrak{m}}/\mathfrak{m}\text{coker}_{\mathfrak{m}} = 0$, 即

$$0 = R_{\mathfrak{m}}/\mathfrak{m}R_{\mathfrak{m}} \otimes_{R_{\mathfrak{m}}} \text{coker}_{\mathfrak{m}} \cong S^{-1}(R/\mathfrak{m} \otimes_R \text{coker}) \cong S^{-1}(\text{coker}/\mathfrak{m}\text{coker}) \Leftrightarrow \text{coker}/\mathfrak{m}\text{coker} = 0. \quad (3.19)$$

上面的定理表明, 判定模的满射等价于判定商每个极大理想模的满射, 而后者是 $R/\mathfrak{m}$ 线性空间, 因此往往更容易些.

定理 3.5

设 R 为整环, 则对任意乘性子集 S , 可视 $R \subset S^{-1}R \subset \text{Frac}(R)$, 则

$$R = \bigcap_{\mathfrak{m} \in \text{Max}(R)} R_{\mathfrak{m}}. \quad (3.20)$$

证明 任取 $\alpha \in \bigcap_{\mathfrak{m} \in \text{Max}(R)} R_{\mathfrak{m}}$, 则对任意 $\mathfrak{m} \in \text{Max}(R)$, 存在 $s_{\mathfrak{m}} \notin \mathfrak{m}, r_{\mathfrak{m}} \in R$ 使得 $\alpha = \frac{r_{\mathfrak{m}}}{s_{\mathfrak{m}}} \in R_{\mathfrak{m}}$. 断言 $(s_{\mathfrak{m}} : \mathfrak{m} \in \text{Max}(R)) = R$, 否则存在 $\mathfrak{m}_0 \supset (s_{\mathfrak{m}} : \mathfrak{m} \in \text{Max}(R))$, 但 $s_{\mathfrak{m}_0} \notin \mathfrak{m}_0$, 矛盾. 由于 $1 \in (s_{\mathfrak{m}} : \mathfrak{m} \in \text{Max}(R))$,

因此存在 $s_{m_1}, \dots, s_{m_n}, u_1, \dots, u_n$ 使得

$$1 = u_1 s_{m_1} + \dots + u_n s_{m_n} \Rightarrow \alpha = u_1 r_{m_1} + \dots + u_n r_{m_n} \in R. \quad (3.21)$$

3.3 整扩张

3.3.1 整性与有限

定义 3.8 (整性)

设 $R \subset S$ 为子环 (也称 S 为 R 的扩张) .

1. 设 $s \in S$, 称 s 在 R 上整, 若存在首一多项式 $f(x) \in R[x]$ 使得 $f(s) = 0$.
2. 若任意 $s \in S$ 都在 R 上整, 则称 S/R 为整扩张.



例 3.8 $\frac{\sqrt{2}}{2}$ 在 $\mathbb{Z}$ 上非整, 因为它的极小多项式为 $2x^2 - 1$, 但 $\sqrt{2}$ 在 $\mathbb{Z}$ 上整, 因为有首一零化多项式 $x^2 - 2$.

定理 3.6

设 $R \subset S, s \in S$, 则如下等价

1. s 在 R 上整.
2. $R[s]$ 为有限生成 R -模 (此时称 $R[s]/R$ 为有限扩张) .
3. 存在子扩张 $T, R \subset T \subset S$, 使得 $s \in T$ 且 T/S 有限.



证明 $1 \Rightarrow 2$: 设 $s^n + a_{n-1}s^{n-1} + \dots + a_0 = 0$, 则

$$s^n = -a_{n-1}s^{n-1} - \dots - a_0 \Rightarrow R[s] = R + Rs + \dots + Rs^{n-1}. \quad (3.22)$$

$2 \Rightarrow 3$: 取 $T = R[s]$ 即可.

$3 \Rightarrow 1$: 设 $T = (1 = t_1, \dots, t_n) = Rt_1 + \dots + Rt_n$, 则 $s \in T$ 诱导了 R -模同态 $m_s: T \rightarrow T, t \mapsto st$, 因此存在该同态在基 $(t_1, \dots, t_n)$ 下的矩阵 $A \in M_n(R)$, 则 s 是 A 的特征值, 也为特征多项式 $\varphi_A(x) \in R[x]$ 的根, φ_A 首一说明 $s \in S$ 整.

推论 3.4

设 $R \subset S$.

- 若 $s_1, s_2 \in S$ 在 R 上整, 则 $s_1 \pm s_2, s_1 s_2$ 在 R 上整.
- 若 S 为有限生成 R -代数, 即 $S = R[s_1, \dots, s_n] = R[x_1, \dots, x_n]/I$, 则 S/R 整当且仅当 S/R 有限.
- 若 $T/R, S/T$ 为整扩张, 则 S/R 为整扩张.



证明

1. 由于 $R[s_1]/R$ 有限, $R[s_1, s_2]/R[s_1]$ 有限, 因此 $R[s_1, s_2]/R$ 有限, 因此 $s_1 \pm s_2, s_1 s_2 \in R[s_1, s_2]$ 在 R 上整.
2. $\Rightarrow$: $s_1, \dots, s_n$ 在 R 上整说明 $R[s_1, \dots, s_n]/R$ 有限.
 $\Leftarrow$: 上一条定理.
3. 仿照域扩张中“代数扩张的复合是代数扩张”可证.

3.3.2 正规扩张

定义 3.9 (正规扩张)

设 S/R 为整扩张.

1. 称环 $\bar{R} = \{s \in S : s \text{ 在 } R \text{ 上整}\}$ 为 R 在 S 中的整闭包.
2. 设 R 为整环, R 在 $\text{Frac}(R)$ 中的整闭包 R^ν 称为 R 的正规化.
3. 若 $R = R^\nu$, 则称 R 正规.



注 容易验证 $(R^\nu)^\nu = R^\nu$.

例 3.9 设 k 为域, $R = k[x^2, x^3] \subset k[x]$ 不是正规的, 因为 $\text{Frac}(R) = \text{Frac}(k[x]) = k(x)$, $x = \frac{x^3}{x^2}$ 在 R 上整, 但 $x \notin R$.

命题 3.11

UFD 是正规的.



证明 设 R 为 UFD, 假设存在 $\alpha = \frac{u}{v} \in \text{Frac}(R)$, 它在 R 上整但 $\alpha \notin R$, 不妨设 $\gcd(u, v) \sim 1$, 取 v 的非平凡素因子 $p|v, p \nmid u$ ($\alpha \notin R$ 说明这可以做到), 则存在 $a_0, \dots, a_{n-1} \in R$ 使得

$$\left(\frac{u}{v}\right)^n + a_{n-1}\left(\frac{u}{v}\right)^{n-1} + \dots + a_0 = 0 \Rightarrow u^n + a_{n-1}u^{n-1}v + \dots + a_1uv^{n-1} + a_0v^n = 0, \quad (3.23)$$

与 $p|v, p \nmid u$ 矛盾.

例 3.10 $k[x_1, \dots, x_n], \mathbb{Z}, k[x, y, z]/(z^2 - xy)$ 都是正规的.

定理 3.7 (正规性是局部概念)

设 R 为整环, S 为其乘性子集.

1. 若 R 正规, 则 $S^{-1}R$ 正规.
2. 若对任意 $\mathfrak{m} \in \text{Max}(R)$, $R_{\mathfrak{m}}$ 正规, 则 R 正规.



证明

1. 由于 $\text{Frac}(S^{-1}R) = \text{Frac}(R)$, 取 $\alpha \in \text{Frac}(R)$, 若 α 在 $S^{-1}R$ 上整, 则存在 $\frac{a_0}{s_0}, \dots, \frac{a_{n-1}}{s_{n-1}} \in S^{-1}R$ 使得

$$\alpha^n + \frac{a_{n-1}}{s_{n-1}}\alpha^{n-1} + \dots + \frac{a_0}{s_0} = 0, \quad (3.24)$$

由于 R 正规, 因此只需证明存在 $s \in S$ 使得 $s\alpha$ 在 R 上整, 取 $s = s_0 \cdots s_{n-1}$ 则

$$(s\alpha)^n + \left(\frac{s}{s_{n-1}}a_{n-1}\right)(s\alpha)^{n-1} + \dots + \frac{s^n}{s}a_0 = 0 \Rightarrow s\alpha \in R^\nu = R \Rightarrow \alpha \in S^{-1}R, \quad (3.25)$$

得证.

2. 显然 $R \subset R^\nu$, 反过来有

$$R^\nu = \left(\bigcap_{\mathfrak{m} \in \text{Max}(R)} R_{\mathfrak{m}} \right)^\nu \subset \bigcap_{\mathfrak{m} \in \text{Max}(R)} R_{\mathfrak{m}}^\nu = \bigcap_{\mathfrak{m} \in \text{Max}(R)} R_{\mathfrak{m}} = R, \quad (3.26)$$

因此 R 正规.

3.3.3 有限性定理

定理 3.8 (有限性定理)

设 R 为正规整环, $K = \text{Frac}(R)$, L/K 为有限可分 (域) 扩张, 记 S 为 R 在 L 上的整闭包, 则存在 L/K 的基 $v_1, \dots, v_n$ 使得 $S \subset Rv_1 \oplus \dots \oplus Rv_n \subset L$.



注 若 R 为 Noether 环, 则 S/R 有限 (Noether 环上的有限生成模是 Noether 模, Noether 模的子模是有限生成的)

引理 3.1

设 R 为整环, $K = \text{Frac}(R) \subset L$ (代数扩张), 取 $\alpha \in L$, 若 α 在 R 上整, 设其在 K 上的极小多项式为 $x^n + \cdots + c_1x + c_0 \in K[x]$, 则 c_i 在 R 上整.



注 若 R 正规, 则 $c_i \in R$.

证明 设 $\alpha_1, \dots, \alpha_n$ 为 α 在 $\overline{K}$ 中的共轭元, 则 $\alpha_1, \dots, \alpha_n$ 在 R 上整 (因为它们都是 α 在 L 中极小多项式的根), 由 Vieta 定理可知 c_i 都在 R 上整.

证明 【有限性定理的证明】取 L/K 的基 $u_1, \dots, u_n$, 则可以通过乘一个 R 中的元素使得它们在 R 上整 (上节某定理证明). 由 $\text{Tr}: L \times L \rightarrow K$ 非退化可知存在 L/K 的基 $v_1, \dots, v_n$ 使得 $\text{Tr}(u_i v_j) = \delta_{ij}$, 任取 $\alpha \in S$ (在 R 上整), 令 $b_i = \text{Tr}(\alpha u_i) \in R$ (引理), 则 $\alpha = b_1 v_1 + \cdots + b_n v_n$, 因此 $S \subset Rv_1 \oplus \cdots \oplus Rv_n \subset L$.

代数整数

定义 3.10 (代数整数)

- 设 $\overline{\mathbb{Q}}$ 为 $\mathbb{Q}$ 的代数闭包, 对任意 $\alpha \in \overline{\mathbb{Q}}$, 若 α 在 $\mathbb{Z}$ 上整, 则称之为代数整数.
- 对于 $K/\mathbb{Q} \subset \overline{\mathbb{Q}}/\mathbb{Q}$, 记环 $\mathcal{O}_K = \{\alpha \in K : \alpha \text{ 在 } \mathbb{Z} \text{ 上整}\}$ 为 $\mathbb{Z}$ 在 K 上的整闭包.



例 3.11 若 $K = \mathbb{Q}(\sqrt{2})/\mathbb{Q}$, 则 $\mathcal{O}_K = \mathbb{Z} \oplus \mathbb{Z}\sqrt{2}$.

定理 3.9

设 $K/\mathbb{Q}$ 为 n 次扩张, 则 $\mathcal{O}_K$ 为秩 n 的自由 $\mathbb{Z}$ -模, 即存在 $\alpha_1, \dots, \alpha_n \in \mathcal{O}_K$ 使得 $\mathcal{O}_K = \mathbb{Z}\alpha_1 \oplus \cdots \oplus \mathbb{Z}\alpha_n$.



证明 根据有限性定理, 存在 $\alpha_1, \dots, \alpha_n$ 使得 $\mathcal{O}_K \subset \mathbb{Z}\alpha_1 \oplus \cdots \oplus \mathbb{Z}\alpha_n \subset K$, 因此 $\mathcal{O}_K$ 为秩不超过 n 的自由 $\mathbb{Z}$ -模, 进一步

$$\mathcal{O}_K \otimes_{\mathbb{Z}} \mathbb{Q} \subset K \otimes_{\mathbb{Z}} \mathbb{Q} = K, \quad (3.27)$$

由于对任意 $\alpha \in K$, 存在 $0 \neq m \in \mathbb{Z}$ 使得 $m\alpha$ 在 $\mathbb{Z}$ 上整, 因此上面可以取等, 说明 $\text{rk}(\mathcal{O}_K) = \text{rk}(K)$ (根据 PID 上有限生成模的结论, 与分式域张量积得到的结果不改变秩).

命题 3.12

设 $\epsilon_1, \dots, \epsilon_n$ 为 n 个单位根, 令 $\gamma = \frac{1}{n}(\epsilon_1 + \cdots + \epsilon_n) \neq 0$, 则 γ 为代数整数当且仅当 $\epsilon_1 = \cdots = \epsilon_n$, 即 $|\gamma| = 1$.



证明 注意到 γ 的共轭元也是单位根的平均值, 设 $\gamma_1, \dots, \gamma_t$ 为 γ 的共轭元, $\gamma_i = \frac{\sigma_i(\epsilon_1) + \cdots + \sigma_i(\epsilon_n)}{n}$, 则 $|\gamma| \leq 1$, 取等当且仅当 $\epsilon_1 = \cdots = \epsilon_n = 1$.

$\Rightarrow$: 此时 $\gamma_1, \dots, \gamma_t$ 均为代数整数, 因此 $\gamma_1 \cdots \gamma_t \in \mathbb{Z}$ (它在 Galois 变换下不变, 且为代数元), 从而 $|\gamma| = 1$, 得证.

3.4 Noether 正规化定理

定理 3.10 (Noether 正规化定理)

设 k 为域, A 为有限生成 k -代数, 则存在 $t_1, \dots, t_n \in A$ 使得

1. $t_1, \dots, t_n$ 在 k 上代数无关.
2. $k[t_1, \dots, t_n] \hookrightarrow A$ 为有限扩张.



证明 设 k 为无限域, $A = k[X, Y]/I = k[x, y]$, 不妨设 $I \neq (0)$, 取 $0 \neq f(X, Y) \in I, f(x, y) = 0$.

1. 若 $f(X, Y)$ 关于 Y 首一 (即 $f(X, Y) = Y^n + a_{n-1}(X)Y^{n-1} + \cdots + a_0(X)$), 则

$$y^n + a_{n-1}(x)y^{n-1} + \cdots + a_0(x) = 0, \quad (3.28)$$

则 $k[x] \hookrightarrow A$ 为有限扩张 (因为 $A = k[x] + k[x]y + \cdots + k[x]y^{n-1}$), 若 x 在 k 中不是代数元, 则 $k[x]$ 满足要求, 否则 $k \hookrightarrow A$ 满足要求.

2. 若 $f(X, Y)$ 关于 X, Y 都不首一, 则存在 $a, b, c, d \in k$ 使得 $ad - bc \neq 0$ 且做变量代换

$$\begin{cases} x = ax' + by', \\ y = cx' + dy', \end{cases} \quad (3.29)$$

后 f 关于 x', y' 的 y' 最高次项系数在 k 中, 因此可化为首一多项式, 重复上一条即可.

推论 3.5 (Hilbert 零点定理)

设 k 为代数闭域, $\mathfrak{m}$ 为多项式环 $k[x_1, \cdots, x_n]$ 的极大理想, 则存在 $a_1, \cdots, a_n \in k$ 使得 $\mathfrak{m} = (x_1 - a_1, \cdots, x_n - a_n)$.



证明 $A = k[x_1, \cdots, x_m]/\mathfrak{m}$ 为有限生成 k -代数, 由 Noether 正规化定理, 存在 $t_1, \cdots, t_r \in A$ 使得 $k[t_1, \cdots, t_r] \hookrightarrow A$ 有限, 而 A 为域, $k[t_1, \cdots, t_r]$ 为整环, 因此有限性蕴含 $k[t_1, \cdots, t_r]$ 为域, 但多项式环必然不是域, 因此 $r = 0$, $k \hookrightarrow A$ 为有限扩张, 但是 k 为代数闭域, 因此 $k \cong A$, 记同构为 φ , 令 $\bar{x}_i = \varphi(a_i)$, 则 $\bar{x}_i - \bar{a}_i = 0 \Rightarrow x_i - a_i \in \mathfrak{m}$, 因此 $(x_1 - a_1, \cdots, x_m - a_m) = \mathfrak{m}$.

推论 3.6

设 k 为代数闭域, $I \subsetneq k[x_1, \cdots, x_n]$, 则存在 $a = (a_1, \cdots, a_n) \in k^n$ 使得对任意 $f \in I$ 有 $f(a) = 0$.



因此存在 $k[x_1, \cdots, x_n]$ 中理想与 k^n 子集的对应:

$$J \mapsto V(J) = \{a \in k^n : f(a) = 0, \forall f \in J\}, \quad (3.30)$$

$$Z \mapsto I(Z) = \{f \in k[x_1, \cdots, x_n] : f(a) = 0, \forall a \in Z\}. \quad (3.31)$$

定理 3.11 (Hilbert 零点定理 (强形式))

设 k 为代数闭域, 理想 $J \subset k[x_1, \cdots, x_n]$, 则 $I(V(J)) = \sqrt{J}$.



证明 显然 $I(V(J)) \supset \sqrt{J}$, 反之设 $f \in I(V(J))$, 则 $f|_{V(J)} = 0$, 设考虑 $k[x_1, \cdots, x_n, y]/(J + (yf - 1))$, 设其极大理想 (对应到多项式环中) 为 $\mathfrak{m} = (x_1 - a_1, \cdots, x_n - a_n, y - b)$, 且 $\mathfrak{m} \supset J, \mathfrak{m} \supset yf - 1$, 则 $a = (a_1, \cdots, a_n) \in V(J)$, 并且 $bf(a) - 1 = 0$, 矛盾, 故该环无极大理想, 为零环.....

定理 3.12

设 R 为整环, $K = \text{Frac}(R)$, K_1/K 为有限扩张, R_1 为 R 在 K_1 中的整闭包, 则在以下两种情形之一, $R \hookrightarrow R_1$ 为有限扩张.

1. R 整闭且 Noether, K_1/K 可分.
2. R 为域 k 上的有限生成代数.



证明

1. 已证.
2. 不妨设 $R = k[t_1, \cdots, t_n]$ 为 k 上的 n 元多项式环,

第4章 有限群表示论

本章默认 $|G| < \infty$, $V/\mathbb{C}$.

4.1 群的代表

直接理解, 群的代表实际上可以看作一种线性作用.

定义 4.1 (线性作用)

设 G 为有限群, V 为 F -线性空间, 则 G 在 V 上的群作用称为线性作用, 若对任意 $v, w \in V, g \in G, \lambda \in F$ 有

$$g(v + w) = gv + gw, \quad g(\lambda v) = \lambda gv. \quad (4.1)$$

4.1.1 群同态语言下的群代表

定义 4.2 (线性表示)

设 G 为群, F 为域, 称 $(V/F, \rho)$ 为 G 的 F -线性表示, 指 V 配有群同态 $\rho: G \rightarrow GL(V)$, 表示次数定义为空间的维数 $\deg \varphi = \dim_F V$.

注 有时也会直接称 V 为 G 的 F -表示.

例 4.1

- $\rho: G \rightarrow GL(V), g \mapsto \text{Id}_V$ 称为平凡表示 (或主表示).
- 设 $G = \mathbb{Z}/n\mathbb{Z}, F = \mathbb{C}$, 则它的一维表示为

$$\rho: G \rightarrow \mathbb{C}^*, \quad \rho(k) = e^{2\pi kmi/n}, 0 \leq m \leq n-1. \quad (4.2)$$

- 设 G 置换作用于集合 S 上, 可以定义 $|S|$ 维 F -线性空间

$$F[S] = \left\{ \sum_{s \in S} a_s s : a_s \in F, s \in S \right\}, \quad (4.3)$$

则 G 在 S 上的作用对应了 G 在 $F[S]/F$ 上的线性作用

$$g \left(\sum_{s \in S} a_s s \right) = \sum_{s \in S} a_s (gs) = \sum_{s \in S} a_{g^{-1}s} s. \quad (4.4)$$

这称为群 G 的置换表示.

定义 4.3 (表示的等价)

称群 G 的两个表示 $\varphi: G \rightarrow GL(V), \psi: G \rightarrow GL(W)$ 是等价的, 若存在 (线性空间) 同构 $T: V \rightarrow W$ 使得对任意 $g \in G$ 有 $T\varphi_g = \psi_g T$, 记作 $\varphi \sim \psi$.

$$\begin{array}{ccc} V & \xrightarrow{\varphi_g} & V \\ \downarrow T & & \downarrow T \\ W & \xrightarrow{\psi_g} & W \end{array}$$

注 表示之间态射的全体记为 $\text{Hom}(\varphi, \psi)$, 它是 $\text{Hom}(V, W)$ 的子空间, 对任意 $g \in G$ 有 $T\varphi_g = \psi_g T$.

定义 4.4 (表示的直和)

设有表示 $\varphi^{(1)} : G \rightarrow GL(V_1), \varphi^{(2)} : G \rightarrow GL(V_2)$, 定义其直和为

$$\varphi^{(1)} \oplus \varphi^{(2)} : G \longrightarrow GL(V_1 \oplus V_2) \quad (4.5)$$

$$(v_1, v_2) \longmapsto (\varphi_g^{(1)}(v_1), \varphi_g^{(2)}(v_2)). \quad (4.6)$$

定义 4.5 (子表示)

设有表示 $\varphi : G \rightarrow GL(V)$, 若子空间 $W \leq V$ 是 G -不变的 (即对任意 g 有 $\varphi_g(W) \subset W$), 则称 $\varphi|_W : G \rightarrow GL(W)$ 为 V 的子表示.

定义 4.6 (不可约表示)

称表示 $\varphi : G \rightarrow GL(V)$ 是不可约的, 若其无非平凡子表示 (或者说 G -不变子空间只有 $\{0\}$ 和 V).

注 特别地, 所有一次表示都是不可约的.

定义 4.7 (完全可约)

称表示 $\varphi : G \rightarrow GL(V)$ 是完全可约的, 若存在分解 $V = V_1 \oplus \cdots \oplus V_n$, 这里每个 $V_n \leq V$ 都是 G -不变子空间, 并且 $\varphi|_{V_i}$ 都不可约.

注 根据定义, 不可约表示是完全可约的, 并且表示完全可约当且仅当 $\varphi(G)$ 可通过同一矩阵分块对角化.

定义 4.8 (表示的分解)

称表示 $\varphi : G \rightarrow GL(V)$ 是可分解的, 若存在 G -不变子空间 V_1, V_2 使得 $V = V_1 \oplus V_2$.

命题 4.1

可分解性、不可约性、完全可约性都是表示的等价不变量.

关于表示的分解, 有如下定理:

定理 4.1 (Maschke)

设域 F 特征为 0 或与群 G 的阶互素, 则对 V 的任意真子表示 U , 存在子表示 W 使得 $V = U \oplus W$, 即 G 的任何 F -表示的子表示均是直和项.

证明 设投影 $\pi : V \rightarrow U$, 令

$$\pi' : V \rightarrow V, \quad v \mapsto \frac{1}{|G|} \sum_{g \in G} g\pi(g^{-1}v), \quad (4.7)$$

则容易验证 $\pi'|_U = \text{Id}_U, \text{Im } \pi' = U$, 因此有直和 $V = \text{Im } \pi' \oplus \text{Ker } \pi' = U \oplus W$, 下证 W 为 V 的子表示, 只需证明对任意 $w \in W, x \in G$ 有 $gx \in W$, 注意到对任意 $x \in G, v \in V$ 有

$$\pi'(xv) = \frac{1}{|G|} \sum_{g \in G} g\pi(g^{-1}xv) = \frac{1}{|G|} x \left(\sum_{g \in G} (x^{-1}g)\pi(g^{-1}xv) \right) \quad (4.8)$$

$$= x \left(\frac{1}{|G|} \sum_{h \in G} h\pi(h^{-1}v) \right) \quad (4.9)$$

$$= x\pi'(v), \quad (4.10)$$

故得证.

对偶表示

设 U, V 都是 G 的 F -表示, 则 $\text{Hom}_F(U, V), U \otimes_F V$ 都是 F -线性空间, 可以定义 G 在 $\text{Hom}_F(U, V)$ 上的线性作用为

$$\Phi: G \rightarrow GL(\text{Hom}(U, V)), \quad \Phi_g(f) = g \circ f \circ g^{-1}, \quad (4.11)$$

对于张量积, 考虑双线性映射 $(u, v) \mapsto (gu) \otimes (gv)$, 则它诱导 F -线性映射

$$U \otimes_F V \rightarrow U \otimes_F V, \quad u \otimes v \mapsto (gu) \otimes (gv). \quad (4.12)$$

定义 4.9 (对偶表示/逆步表示)

设 $\varphi: G \rightarrow GL(V)$ 为 G 的表示, $V^* = \text{Hom}_F(U, F)$ 为对偶空间, 则称 $\varphi^*: G \rightarrow GL(V^*)$ 为其对偶表示, 其中 $\varphi_g^*(f) = f \circ \varphi_{g^{-1}}$.

注 若考虑一组基与其对偶基, 则 φ_g^* 在对偶基下的矩阵与 $\varphi_{g^{-1}}$ 在该基下的矩阵相差转置逆. 容易验证

$$\varphi_g^* \varphi_h^*(f) = f \circ \varphi_{h^{-1}} \circ \varphi_{g^{-1}} = f \circ \varphi_{(gh)^{-1}} = \varphi_{gh}^*(f). \quad (4.13)$$

命题 4.2

设 U, V 为 G 的 F -表示, 则有表示间的同构

$$\Gamma: U^* \otimes_F V \rightarrow \text{Hom}_F(U, V), \quad \varphi \otimes v \mapsto (u \mapsto \varphi(u)v). \quad (4.14)$$

置换表示与正则表示

若 G 作用于有限集 X 上, 则可视 $F[X]$ 为 $F[G]$ -模, 它是一个 G 的 F -表示, 即

$$g \left(\sum_{x \in X} a_x x \right) = \sum_{x \in X} a_x (gx) = \sum_{x \in X} a_{g^{-1}x} x, \quad (4.15)$$

这称为 G 的置换表示.

若上面 $X = G$, G 左乘作用于自身, 即 $F[G]$ 视为 G 的 F -表示, 称为 G 的正则表示.

4.1.2 $F[G]$ -模语言下的群表示

定义 4.10 (群环/群代数)

设 G 为有限群, F 为域, 定义群环 $F[G]$, 其中元素形如

$$\sum_{g \in G} a_g g, \quad a_g \in F, g \in G, \quad (4.16)$$

注

1. 它同时是一个 F -线性空间以及一个幺环, 因此是一个 F -代数.
2. 容易验证 $\dim_F F[G] = |G|$, 并且 F 为交换环当且仅当 G 为交换群.

若设 $\varphi: G \rightarrow GL(V)$ 为一个表示, 则 φ_g 可以视为 $g \in G$ 在 V 上的作用, 即 F -表示与 G 线性作用存在对应, 进一步用群环的语言, 这种线性作用实际上可以赋予 V 一个 $F[G]$ -模结构, 即

$$\left(\sum_{g \in G} a_g g \right) \cdot v = \sum_{g \in G} a_g (gv), \quad (4.17)$$

并且它是有限生成的. 可总结为如下命题, 它给出了看待有限群表示的三种视角:

命题 4.3 (F -表示 $\iff G$ 线性作用 $\iff$ 有限生成 $F[G]$ -模)

设 G 为有限群, F 为域, 则下列集合存在自然双射:

- G 的有限维 F -表示的全体.
- 配有 G 线性作用的有限维 F -线性空间的全体,
- 有限生成 $F[G]$ -模的全体.



注 有时直接称一个线性空间 V 为 G 的 F -表示, 实际上是将它视为 $F[G]$ -模.

在模的视角下, 许多定义有等价形式.

定义 4.11 (子表示 & 不可约表示)

- 称 W 为 V 的子表示, 若 W 为 V 的 $F[G]$ -子模, 或者说 G 在 V 上的线性作用对 W 封闭, 也可以说 W 是 G 的全不变子空间.
- 称 V 为不可约表示, 若 V 作为 $F[G]$ -模是单模.

**定义 4.12** (表示的直和)

设 V_1, V_2 为 G 的 F -表示, 则它们作为表示的直和实际上是作为 $F[G]$ -模的直和.

**定义 4.13** (半单模)

若模 M 为单模的直和, 则称 M 为半单模.



注 显然单模是半单模.

定义 4.14 (完全可约)

表示 V 的完全可约实际上是指它是半单 $F[G]$ -模.



在模的语言下, Maschke 定理有如下形式:

定理 4.2 (Maschke 定理)

设域 F 特征为 0 或与群 G 的阶互素, 则有限群 G 的非零 F -表示都是不可约表示的直和, 即任意有限生成非零 $F[G]$ -模是半单模.

**例 4.2** Maschke 定理的两个反例

- 无限群: 设 $G = (\mathbb{R}, +), V = \mathbb{R}^2$, 考虑

$$\varphi: G \rightarrow GL(\mathbb{R}^2), \quad r \mapsto \begin{pmatrix} 1 & r \\ 0 & 1 \end{pmatrix}, \quad (4.18)$$

则它是一个表示, 但不可对角化, 故不是完全可约的.

- $\text{char } F$ 与 $|G|$ 不互素: 设 $G = \mathbb{Z}/p\mathbb{Z}$, p 为素数 (注意 G 同时是一个域), 考虑

$$\varphi: G \rightarrow GL(M_2(\mathbb{Z}/p\mathbb{Z})) = GL_2(\mathbb{Z}/p\mathbb{Z}), \quad \bar{n} \mapsto \begin{pmatrix} \bar{1} & \bar{n} \\ 0 & \bar{1} \end{pmatrix}, \quad (4.19)$$

容易验证它是 G 在 $M_2(\mathbb{Z}/p\mathbb{Z})$ 上的一个 $\mathbb{Z}/p\mathbb{Z}$ -表示 (或者说是域 $\mathbb{Z}/p\mathbb{Z}$ 上的二次矩阵表示), 但 $\varphi(1)$ 的极小多项式为 $d(x) = (x - \bar{1})^2$, 说明它不可对角化, 但由 $(\bar{1}, 0)^T$ 生成的子空间是 G -不变子空间, 说明 φ 不是完全可约的.

一个单模的结论

定理 4.3 (Schur)

单模间的任意非零同态都是同构, 换句话说 $\text{Hom}_R(M, N)$ 为除环.



证明 设 $f: M \rightarrow N$ 为单模间的非零同态, 则一方面 $\text{Ker } f \leq M$ 说明 $\text{Ker } f = \{0\}$, 另一方面 $\text{Im } f \leq N$ 说明 $\text{Im } f = N$, 因此 $f: M \rightarrow N$ 为同构.

推论 4.1

若 M 为单 R -模, 则自同态环 $\text{End}_R(M)$ 是可除环.



证明 $\text{End}_R(M)$ 中元素为单模之间的同态, 因此或为平凡同态, 或为同构.

4.2 半单代数

本节中任意模都是有限生成的.

4.2.1 半单代数

引理 4.1

设 F 为域, A 为有限维 F -代数, M 为 A -模, 则下述等价

1. M 的任意子模都是 M 的直和项.
2. M 为半单模.
3. M 为单子模之和.



证明 $1 \Rightarrow 2 \Rightarrow 3$ 是显然的, 下证 $3 \Rightarrow 1$.

设 $N \leq M$, $V \leq M$ 是与 N 之交平凡的所有子模的极大元, 下证 $M = N + V = N \oplus V$, 若不然则由于 M 为单子模之和, 存在单模 $S \not\subseteq N + V$. S 为单模说明 $S \cap (N + V) = \{0\}$, 因此 $N \cap (V + S) = \{0\}$, 与 V 的极大性矛盾.

引理 4.2

半单模的子模、商模是半单模.



证明 设 N 为半单模 M 的子模, 则 $M = N \oplus W$, 因此 $N \cong M/W$ 为 M 的商模, 因此只需证明半单模的商模是半单模.

设 $M = S_1 + \cdots + S_n$ 为半单模, 其中 S_i 为单模, 考虑满同态 $\pi: M \rightarrow M/N$, 则 $\pi(S_i) = S_i N/N \cong S_i/S_i \cap N$, 因此 $\pi(S_i) \cong S_i$ 或 $\pi(S_i) = 0$, 说明 $M/N = \pi(S_1) + \cdots + \pi(S_n)$, 即 M/N 为半单模.

定义 4.15 (半单代数)

若代数 A 的非零 A -模都是半单模, 则称 A 为半单代数.



注 Maschke 定理实际是说群环 $F[G]$ 为半单 F -代数.

定理 4.4 (半单代数的等价刻画)

A 为半单代数当且仅当它自身是半单 A -模.



证明 若 A 是半单代数, 则由定义可得 A 是半单 A -模. 反之若 A 为半单 A -模, 则任意自由模 A^n 也是半单模, 而任意有限生成 A -模是自由模的商模, 故 A 也是半单模.

命题 4.4

设 A 为半单代数, 有 A -模同构 $A \cong S_1 \oplus \cdots \oplus S_r$, 其中 S_i 为单模, 则任意单 A -模必然同构于某个 S_i . 

证明 设 S 为单 A -模, $0 \neq s \in S$, 令 $\varphi: A \rightarrow S, a \mapsto as$, 则 φ 必然为满同态, 考虑 $\varphi_i = \varphi|_{S_i}: S_i \rightarrow S$, 则它们必然不全为零, 由 Schur 引理可知不为 0 的 φ_i 为同构.

推论 4.2

设 $\{S_1, \dots, S_r\}$ 为半单代数 A 的所有互不同构的单模, 则对于 A -模 M , 若 $M \cong n_1 S_1 \oplus \cdots \oplus n_r S_r$, 则 $\{n_1, \dots, n_r\}$ 是唯一确定的. 

证明 设 $\varphi: n_1 S_1 \oplus \cdots \oplus n_r S_r \cong m_1 S_1 \oplus \cdots \oplus m_r S_r$, 记 $\varphi_i = \varphi|_{n_i S_i}, \pi_j: M \rightarrow m_j S_j$, 考虑

$$\varphi_{ij} = \pi_j \circ \varphi \circ \varphi_i: n_i S_i \rightarrow m_j S_j, \quad (4.20)$$

若 $i \neq j$, 则 $\varphi_{ij} = 0$, 因此 $\varphi = \bigoplus_{i=1}^r \varphi_{ii}$, φ 为同构说明 $\varphi_{ii}: n_i S_i \rightarrow m_i S_i$ 为同构, 因此 $n_i = m_i$.

4.2.2 可除代数**定义 4.16 (可除代数)**

若可除环 D 是 F -代数, 则称之为 F -可除代数. 

例 4.3 若 D 为可除代数, 则 n 阶矩阵环 $M_n(D)$ 也是 F -代数, 通过矩阵乘法可知 D^n 为 $M_n(D)$ -模.

定理 4.5

设 D 为可除代数, 则环 $M_n(D)$ 是半单代数, 其单模均同构于 D^n , $M_n(D)$ 作为 $M_n(D)$ -模同构于 nD^n . 

证明 先证 D^n 为单 $M_n(D)$ -模. 设 N 为 D^n 的非零子模, 若 $0 \neq v = (v_1, \dots, v_n)^T \in N$, 不妨设 $v_j \neq 0$, 则 $(v_j^{-1} E_{ij}) \cdot v = e_j \in N$, 再由 $P_{ij} e_j = e_i \in N$ 可知 $N = D^n$, 得证.

设 C_k 为 $M_n(D)$ 中在第 k 列外均为零的矩阵集合, 则 $C_k \leq M_n(D)$ 并且 $C_k \cong D^n$, 即得 $M_n(D) \cong \bigoplus_{k=1}^n C_k \cong nD^n$, 故 $M_n(D)$ 为半单代数, D^n 为其唯一的单 $M_n(D)$ -模.

定义 4.17 (单代数)

若代数 A 只有平凡双边理想, 或者说它作为环是单环, 则称 A 为单代数. 

引理 4.3

单代数都是半单代数. 

证明 设 A 为单代数, Σ 为 A 的所有单子模之和. 若 S 为 A 的单子模, 则对任意 $a \in A$, $\varphi: S \rightarrow Sa, s \mapsto sa$ 有 $\text{Ker } \varphi = 0$ 或 $\text{Ker } \varphi = S$, 即 $Sa = 0$ 或 $Sa \cong S$, 因此 $Sa \subset \Sigma$, 说明 Σ 为 A 的双边理想, 因此 $\Sigma = A$, 即 A 是半单 A -模, 即为半单代数.

定理 4.6

设 D 为可除代数, 则 $M_n(D)$ 为单代数. 

证明 只需证明任意 $0 \neq M \in M_n(D)$, $(M) = J = M_n(D)$. 设 $M = (m_{ij})$ 且 $m_{rs} = a \neq 0$, 则

$$E_{ss} = (a^{-1} E_{sr}) M E_{ss} \in J, E_{ij} = P_{is} E_{ss} P_{sj} \in J, \quad (4.21)$$

得证.

定义 4.18 (反环/反代数)

对于环 R (或代数 A), 定义其反环 R^{op} (或反代数 A^{op}) 上的乘法为 $r_1 \circ r_2 = r_2 r_1$.

**引理 4.4**

- 代数 A 的反代数 A^{op} 与其自同态代数 $\text{End}_A(A) = \text{Hom}(A, A)$ 同构.
- $M_n(A)^{op} \cong M_n(A^{op})$.

**证明**

1. 设 $\varphi \in \text{End}_A(A)$, $a = \varphi(1)$, 则 $\varphi(b) = b\varphi(1) = ba$, 若设 $\rho_a : b \mapsto ba$, 则 $\text{End}_A(A) = \{\rho_a : a \in A\}$, 容易验证 $\rho : A^{op} \rightarrow \text{End}_A(A)$, $a \mapsto \rho_a$ 为代数同构.
2. 考虑转置.

引理 4.5

- 设 S 为单模, 则 $D = \text{End}_A(S)$ 为可除代数且有代数同态 $\text{End}_A(nS) \cong M_n(D)$.
- 设 $S_1, \dots, S_r$ 为互不同构的单模, $U_i = n_i S_i$, $D_i = \text{End}_A(S_i)$, 则

$$\text{End}_A(U_1 \oplus \dots \oplus U_r) \cong M_{n_1}(D_1) \oplus \dots \oplus M_{n_r}(D_r). \quad (4.22)$$

**证明**

1. 由 Schur 引理可得 D 为可除代数, 将 nS 视为列向量空间 S^n , 则显然有代数同态 $\Gamma : M_n(D) \rightarrow \text{End}_A(nS)$ (考虑直接作用), 若 $\Gamma(\Phi) = 0$, 设 $\Phi = (\varphi_{ij})$, 则取 $(0, \dots, s_i, \dots, 0)^T \in S^n$,

$$\Gamma(\Phi)(0, \dots, s_i, \dots, 0)^T = (\varphi_{1i}(s_i), \dots, \varphi_{ni}(s_i))^T = 0, \quad (4.23)$$

根据 s_i, i 的任意性可知 $\Phi = 0$, 即 Γ 为单射; 另一方面设 $\Psi \in \text{End}_A(nS)$, 对任意 $1 \leq i \leq n$, 令

$$\Psi(0, \dots, s_i, \dots, 0)^T = (\psi_{1i}(s_i), \dots, \psi_{ni}(s_i)), \quad (4.24)$$

则 $\psi_{ij} \in \text{End}_A(S)$, 并且 $\Gamma((\psi_{ij})) = \Psi$ 说明 Γ 为满射, 得证.

2. 设 $U = \bigoplus_{i=1}^r U_i$, 对任意 $\varphi \in \text{End}_A(U)$, 令

$$\varphi_{ij} = \pi_j \circ \varphi \circ \varphi_i : U_i \rightarrow U_j \quad (4.25)$$

可知对任意 $i \neq j$ 有 $\varphi_{ij} = 0$, 因此 $\varphi = \bigoplus_{i=1}^r \varphi_{ii}$, 由 1 得证.

命题 4.5

若 F 为代数闭域, S 为单模, 则 $\text{End}_A(S) \cong F$.



证明 设 $\varphi \in \text{End}_A(S)$, $\lambda \in F$ 为 φ 的一个特征值, 则 $\varphi - \lambda I \in \text{End}_A(S)$ 并且它不可逆, 因此只有 $\varphi = \lambda I$, 这说明 $\text{End}_A(S)$ 中的元素均为标量数乘, 即 $\lambda \mapsto \lambda I$ 给出了这一同构.

定理 4.7 (Wedderburn)

代数 A 半单当且仅当 $A \cong \bigoplus_{i=1}^r M_{n_i}(D_i)$, 其中 D_i 为可除代数.



证明 $\Leftarrow$: 显然.

$\Rightarrow$: 若 $A \cong U_1 \oplus \dots \oplus U_r = n_1 S_1 \oplus \dots \oplus n_r S_r$ 为半单模分解, 则

$$A^{op} \cong \text{End}_A(A) \cong \bigoplus_{i=1}^r M_{n_i}(\text{End}_A(S_i)), \quad (4.26)$$

$$A = (A^{op})^{op} \cong \bigoplus_{i=1}^r M_{n_i}(\text{End}_A(S_i)^{op}). \quad (4.27)$$

推论 4.3 (维数公式)

延续上述定理的记号, 两边作为 F -线性空间有

$$\dim_F A = n_1^2 + \cdots + n_r^2. \quad (4.28)$$

4.2.3 群表示语言下的应用与重述

对于有限群 G , $\mathbb{C}[G]$ 为半单模 (Maschke 定理), $\dim_{\mathbb{C}} \mathbb{C}[G] = |G|$, $\mathbb{C}$ 为代数闭域说明对任意单 $\mathbb{C}[G]$ -模 S 都有 $\text{End}_A(S) \cong \mathbb{C}$, 因此

推论 4.4

设 G 为有限群, 则 $\mathbb{C}[G] = \bigoplus_{i=1}^r M_{n_i}(\mathbb{C})$, $|G| = \sum_{i=1}^r n_i^2$.

定理 4.8 (Schur)

设 $(U, \varphi), (V, \rho)$ 为有限群 G 的两个不可约复表示, $T \in \text{Hom}(\varphi, \rho)$, 则必有 $T = 0$ 或 T 可逆, 也就是说

- 若 $\varphi \not\sim \rho$, 则 $\text{Hom}(\varphi, \rho) = 0$.
- 若 $\varphi \sim \rho$, 则存在 $\lambda \in \mathbb{C}$ 使得 $T = \lambda I$ (或者说 $\text{Hom}(\varphi, \varphi) \cong \mathbb{C}$).

注 Schur 定理也表述为: $\text{Hom}(\varphi, \rho)$ 为除环.

证明 $\mathbb{C}[G]$ 为半单代数说明 U, V 为单模, 由 Schur 引理可知当 $(U, \varphi) \not\sim (V, \rho)$ 时 $\text{Hom}(\varphi, \rho) \cong \text{Hom}_{\mathbb{C}[G]}(U, V) = \{0\}$, 当 $(U, \varphi) \sim (V, \rho)$ (不妨设二者相等) 时 $\text{Hom}(\varphi, \varphi) \cong \text{End}_{\mathbb{C}[G]}(U) \cong \mathbb{C}$.

推论 4.5

设 G 为 Abel 群, $\varphi: G \rightarrow GL(V)$ 不可约, 则 $\deg \varphi = \dim V = 1$.

注 事实上逆命题也成立, 因为单 $F[G]$ -模的种类有限, 并且由这些单模可以确定所有半单模, 即所有 F -表示.

证明 对任意 $g, h \in G$ 有 $\varphi_h \varphi_g = \varphi_{hg} = \varphi_{gh} = \varphi_g \varphi_h$, 因此 $\varphi(G) \subset \text{Hom}(\varphi, \varphi)$, 由 Schur 引理可知对任意 $g \in G$, 存在 $0 \neq \lambda_g \in \mathbb{C}$ 使得 $\varphi_g = \lambda_g I$, 再根据 φ 的不可约性得 $\dim V = 1$ (否则存在真 G -不变子空间), 得证.

推论 4.6

设 G 为有限 Abel 群, $\varphi: G \rightarrow GL(V)$ 为复表示, 则存在矩阵 T 使得对任意 $g \in G$, $T^{-1} \varphi_g T$ 为对角阵.

注 注意这里的 T 不依赖 g 的选取, 即 φ_g 可以同时对角化.

除了维数公式, 还可以借助群的中心得到不可约表示的个数.

定理 4.9 (不可约表示的个数)

设 G 的共轭类为 $C_1, \dots, C_s$, 则 G 的不可约表示的个数等于 s .

证明 设 $\mathbb{C}[G] = \bigoplus_{i=1}^r M_{n_i}(\mathbb{C})$, 则

$$Z(\mathbb{C}[G]) = \bigoplus_{i=1}^r Z(M_{n_i}(\mathbb{C})) \cong \mathbb{C}^r \Rightarrow \dim_F Z(\mathbb{C}[G]) = r, \quad (4.29)$$

而对任意 $x = \sum_{g \in G} a_g g \in Z(\mathbb{C}[G])$, $h \in G$ 都有 $x = h x h^{-1}$, 因此有 $a_g = a_{h g h^{-1}}$, 这说明系数在同一共轭类下取值相同, 因此

$$Z(\mathbb{C}[G]) = a_{C_1} \sum_{g \in C_1} g + \cdots + a_{C_r} \sum_{g \in C_r} g \Rightarrow \dim_F Z(\mathbb{C}[G]) = s, \quad (4.30)$$

即得 $r = s$.

4.3 表示的提升与分解

借助已有表示, 可以构造新的表示.

定义 4.19 (表示的提升)

设 (V, ρ) 为 G 的 F -表示, $T: H \rightarrow G$ 为同态, 设 $\rho^T = \rho \circ T: H \rightarrow GL(V)$, 则 (V, ρ^T) 为 H 的 F 表示, 称为 (V, ρ) 的提升.

$$\begin{array}{ccc} & & G \\ & \nearrow T & \downarrow \rho \\ H & \xrightarrow{\rho^T} & GL(V) \end{array}$$

命题 4.6 (表示与提升的不可约性)

记号如上, 则

- ρ^T 不可约 $\Rightarrow \rho$ 不可约.
- 若 T 为满射, 则 ρ 不可约 $\Rightarrow \rho^T$ 不可约.

证明

1. 假设 ρ 可约, 则存在 V 的 G -不变真子空间 W , 它同时是 H -不变的 ($\rho_h^T(W) = \rho_{T(h)}(W) \subset W$), 与 ρ^T 的不可约性矛盾.
2. 假设 ρ^T 可约, 则存在 V 的 H -不变子空间 W , 对任意 $g \in G$, 设 $h \in T^{-1}(g)$ 则 $\rho_g(W) = \rho_h^T(W) \subset W$, 即 W 也是 G -不变的, 矛盾.

例 4.4 设 $N \triangleleft G$, 则有典范同态 $\pi: G \rightarrow G/N$, 借此可将 G/N 的表示提升为 G 的表示.

定义 4.20 (表示的分解)

设 (V, φ) 为 G 的表示, $N \triangleleft G$ 且 $N \subset \text{Ker } \varphi$, $\pi: G \rightarrow G/N$ 为典范映射, 设

$$\bar{\varphi}: G/N \rightarrow GL(V), \quad gN \mapsto \varphi(g), \quad (4.31)$$

则 $(V, \bar{\varphi})$ 为 G/N 的表示, 这称为 (V, φ) 的分解.

注 $N \subset \text{Ker } \varphi$ 说明 $\bar{\varphi}$ 是良定的.

这里 φ 可视为 $\bar{\varphi}$ 的提升, π 为满射说明

命题 4.7 (表示与分解的不可约性)

记号如上, 则 φ 不可约当且仅当 $\bar{\varphi}$ 不可约.

命题 4.8 (提升与分解的一一对应)

设 $N \triangleleft G$, $\Omega_{G/N}$ 为群 G/N 的 F -表示的全体, Ω_G 为 G 的核包含 N 的 F -表示的全体, 则有双射

$$\sigma: \Omega_{G/N} \rightarrow \Omega_G, \quad \bar{\varphi} \mapsto \varphi = \bar{\varphi} \circ \pi, \quad (4.32)$$

并且 $\bar{\varphi}$ 不可约当且仅当 φ 不可约.

注意到表示的提升与分解不改变表示的次数 (即空间的维数), 因此从 G/N 的所有一次 F -表示可提升得到 G 的所有核包含 N 的一次表示. 特别当 G/N 为 Abel 群时, 其所有表示都是一次的, 因此可提升得到 G 的所有核包含 N 的表示 (并且均为一次). 考虑 G 的导群 G' , 易知 G/N 交换当且仅当 $N \supset G'$, 容易证明:

命题 4.9 (一次表示的对应)

群 G 的所有一次 F -表示构成的集合与 G/G' 的所有 (一次) F -表示的集合之间存在一一对应.

证明 设 φ 为 G 的一次表示, 则对任意 $g, h \in G$ 有

$$\varphi([g, h]) = [\varphi(g), \varphi(h)] = 1, \quad (4.33)$$

因此 $G' \subset \text{Ker } \varphi$, 同样考虑 $\sigma: \Omega_{G/G'} \rightarrow \Omega_G, \bar{\varphi} \mapsto \varphi$ 即得.

上述命题给出了求群 G 所有一次表示的方法.

例 4.5 置换群 $S_n (n \geq 3)$ 的一次表示 一方面 $[S_n : A_n] = 2$ 说明 S_n/A_n 交换, 因此 $S'_n \subset A_n$, 而 A_n 由 3-轮换生成, 注意到

$$(ijk) = (ik)(ij) = (jk)(ij)(jk)^{-1}(ij)^{-1} \in S'_n \Rightarrow S'_n = A_n, \quad (4.34)$$

因此 S_n 的一次复表示恰好与 $S_n/A_n \cong \mathbb{Z}/2\mathbb{Z}$ 的一次复表示对应, 而 S_n/A_n 有两个一次复表示 $\bar{\varphi}_0, \bar{\varphi}_1$, 其中 $\bar{\varphi}_0$ 为主表示 $\bar{\varphi}_1(\bar{1}) = -1$, 因此其提升 φ_0 为主表示, φ_1 满足

$$\varphi_1(\sigma) = \bar{\varphi}_1(\sigma A_n) = \begin{cases} 1, & \sigma \text{ 为偶置换} \\ -1, & \sigma \text{ 为奇置换} \end{cases} \quad (4.35)$$

由于 $|S_3| = 6$, 它有两个一次表示, 因此根据维数公式可知它还有一个二次不可约表示 φ_2 , 可以考虑它作用于一个三角形上, 此时存在 $\sigma \in S_3$ 使得 $\varphi_2(\sigma)$ 阶为 3, 故 φ_2 是不可约的.

4.4 特征标理论

4.4.1 特征标的定义及性质

定义 4.21 (特征标)

对于表示 $\varphi: G \rightarrow GL(V)$, 定义其特征标 $\chi_\varphi: G \rightarrow \mathbb{C}^*, \chi_\varphi(g) = \text{tr}(\varphi_g)$. 不可约表示的特征标称为不可约特征标.



注

1. 特征标是一个线性函数, 容易看出 $\chi_\varphi(1) = \deg \varphi$, 对于一次表示有 $\chi_\varphi = \varphi$. 有时也可记 $\chi_\varphi = \chi_V$.
2. 平凡表示的特征也称主特征, 一次表示的特征称为线性特征.

例 4.6 正则表示的特征 设 φ 为 G 的正则表示, 则

$$\chi_\varphi(g) = \begin{cases} |G|, & g = 1, \\ 0, & g \neq 1. \end{cases} \quad (4.36)$$

设 $G = \{g_1, \dots, g_n\}$, $[\varphi_g]$ 为 φ_g 在这一组基下的矩阵, 则

$$[\varphi_g]_{ij} = \begin{cases} 1, & g_i = gg_j \\ 0, & \text{else} \end{cases} = \begin{cases} 1, & g = g_i g_j^{-1} \\ 0, & \text{else} \end{cases} \quad (4.37)$$

特别有 $[\varphi_g]_{ii} = \delta_{g1}$, 即得.

命题 4.10

- $\chi_\varphi(g^{-1}) = \overline{\chi_\varphi(g)}$.
- 对任意表示 $(V, \varphi), g \in G$, $\chi_\varphi(g)$ 为 $\deg \varphi$ 个 $\text{ord } g$ 次单位根之和, 进而 $|\chi_\varphi(g)| \leq n$.
- $\chi_\varphi(g) = n$ 当且仅当 $\varphi(g) = I$, 因此 $\text{Ker } \varphi = \{g \in G : \chi_\varphi(g) = n\}$.
- $|\chi_\varphi(g)| = n$ 当且仅当 $\varphi(g) = cI$, 这里 c 为 $\deg \varphi$ 次单位根.



命题 4.11

- $\chi_{\varphi^1 \oplus \varphi^2} = \chi_{\varphi^1} + \chi_{\varphi^2}$.
- $\chi_{\varphi^1 \otimes \varphi^2} = \chi_{\varphi^1} \cdot \chi_{\varphi^2}$.
- $\chi_{U^*} = \overline{\chi_U}$, 其中 U^* 为 U 的对偶表示.
- $\chi_{\text{Hom}(U, V)} = \chi_{U^* \otimes V} = \overline{\chi_U} \cdot \chi_V$.



注 若表示有不可约分解 $\varphi \sim n_1 \varphi^1 \oplus \cdots \oplus n_s \varphi^s$, 则 $\chi_\varphi = n_1 \chi_{\varphi^1} + \cdots + n_s \chi_{\varphi^s}$.

命题 4.12 (特征标的共轭不变性)

- 若 $\varphi \sim \rho$, 则 $\chi_\varphi = \chi_\rho$.
- 对任意 $g, h \in G$ 有 $\chi_\varphi(h) = \chi_\varphi(ghg^{-1})$.



将特征标的共轭不变性提取出来, 可得类函数的定义.

定义 4.22 (类函数)

称函数 $f: G \rightarrow \mathbb{C}$ 为类函数, 若对任意 $g, h \in G$ 有 $f(h) = f(ghg^{-1})$.



注 若记 $L(G)$ 为所有 G 到 $\mathbb{C}$ 的函数的全体, 则类函数的全体可记为 $Z(L(G))$. 后面可知, 在给环 $L(G)$ 赋予乘法结构后, 类函数确实是它的中心. 有时类函数全体也记为 Cl .

定义 4.23 (特征标表)

设 G 的不可约特征为 $\chi_1, \cdots, \chi_s$, 共轭类为 $C_1, \cdots, C_s$, 则称矩阵 $X = (\chi_i(C_j))_{s \times s}$ 为 G 的特征标表.

**4.4.2 正交关系**

首先定义内积

定义 4.24 ($L(G)$ 中的内积结构)

设 $\varphi, \psi \in L(G)$, 定义其内积为

$$\langle \varphi, \psi \rangle = \frac{1}{|G|} \sum_{g \in G} \varphi(g) \overline{\psi(g)}. \quad (4.38)$$

**引理 4.6**

设 V 为 G 的复表示, $V^G = \{v \in V : gv = v, \forall g \in G\}$, 则

$$\dim V^G = \frac{1}{|G|} \sum_{g \in G} \chi_V(g). \quad (4.39)$$



证明 设 $a = \frac{1}{|G|} \sum_{g \in G} g \in \mathbb{C}[G]$, 显然 $a \in V^G$, 因此 $a^2 = a$, 考虑线性映射 $\rho_a: V \rightarrow V, v \mapsto av$, 则 $x^2 - x$ 是它的零化多项式, 说明 ρ_a 的特征值只有 0 和 1 且能对角化, 设分解 $V = V_1 \oplus V_0$, 若 $v \in V_1$, 则 $av = v$, 对任意 $g \in G$ 有

$$gv = gav = av = v \Rightarrow v \in V^G, \quad (4.40)$$

反之若 $v \in V^G$ 则显然 $av = v, v \in V_1$, 因此 $V_1 = V^G$, 故

$$\dim V^G = \text{tr}(\rho_a) = \frac{1}{|G|} \sum_{g \in G} \chi_V(g). \quad (4.41)$$

定理 4.10

设 U, V 为 G 的复表示, 则

$$\langle \chi_U, \chi_V \rangle = \dim_{\mathbb{C}} \operatorname{Hom}_{\mathbb{C}[G]}(U, V). \quad (4.42)$$



注 这里 $\operatorname{Hom}_{\mathbb{C}[G]}(U, V)$ 上的模结构是由 U, V 得到的, 即 $\Phi_g(f) = gfg^{-1}$.

证明 若视 $\operatorname{Hom}_{\mathbb{C}[G]}(U, V)$ 为 $\operatorname{Hom}_{\mathbb{C}}(U, V)$ 的子空间, 则对任意 $g \in G, \varphi \in \operatorname{Hom}_{\mathbb{C}[G]}(U, V)$ 有

$$(g\varphi)(u) = g\varphi(g^{-1}(u)) = \varphi(u) \Rightarrow \varphi \in (\operatorname{Hom}_{\mathbb{C}}(U, V))^G, \quad (4.43)$$

反过来显然, 因此 $\operatorname{Hom}_{\mathbb{C}[G]}(U, V) = (\operatorname{Hom}_{\mathbb{C}}(U, V))^G$, 由此可得

$$\dim_{\mathbb{C}} \operatorname{Hom}_{\mathbb{C}[G]}(U, V) = \dim_{\mathbb{C}} (\operatorname{Hom}_{\mathbb{C}}(U, V))^G \quad (4.44)$$

$$= \frac{1}{|G|} \sum_{g \in G} \chi_{\operatorname{Hom}(U, V)}(g) \quad (4.45)$$

$$= \frac{1}{|G|} \sum_{g \in G} \overline{\chi_U(g)} \chi_V(g) \quad (4.46)$$

$$= \langle \chi_V, \chi_U \rangle = \langle \chi_U, \chi_V \rangle, \quad (4.47)$$

最后的等号成立是因为结果为实数.

定理 4.11 (不可约特征的正交关系)

设 $\chi_1, \dots, \chi_r$ 为 G 的不可约特征, 则 $\langle \chi_i, \chi_j \rangle = \delta_{ij}$.



证明 由 Schur 引理即得.

推论 4.7

设 $\chi_1, \dots, \chi_r$ 为 G 的不可约特征, 则它们构成 Cl 的一组标准正交基, 因此每个 χ_V 写成 $\chi_1, \dots, \chi_r$ 的 $\mathbb{N}$ 线性组合方式唯一, 进而表示 V 由特征 χ_V 唯一决定.



在特征标表中, 每行对应一个不可约特征在共轭类上的取值, 因此

定理 4.12 (特征标表的行正交关系)

设 $\chi_1, \dots, \chi_r$ 为 G 的不可约特征, $C_1, \dots, C_r$ 为其共轭类, 则

$$\sum_{g \in G} \chi_i(g) \overline{\chi_j(g)} = \sum_{k=1}^r |C_k| \chi_i(C_k) \overline{\chi_j(C_k)} = \delta_{ij} |G|. \quad (4.48)$$



注 行正交关系并非指行向量正交.

事实上, 特征标表的列也有正交关系

定理 4.13 (列正交关系)

设 $\chi_1, \dots, \chi_r$ 为 G 的不可约特征, $C_1, \dots, C_r$ 为其共轭类, 则

$$\sum_{i=1}^r \chi_i(C_k) \overline{\chi_i(C_l)} = \delta_{kl} \frac{|G|}{|C_k|}. \quad (4.49)$$



证明 根据行正交关系可得

$$X \begin{pmatrix} \frac{|C_1|}{|G|} & & \\ & \ddots & \\ & & \frac{|C_r|}{|G|} \end{pmatrix} X^* = I_r \Rightarrow \begin{pmatrix} \frac{|C_1|}{|G|} & & \\ & \ddots & \\ & & \frac{|C_r|}{|G|} \end{pmatrix} X^* X = I_r, \quad (4.50)$$

其中 X^* 表示共轭转置.

4.4.3 特征标表的计算

由于任何表示的特征标都是不可约表示的线性组合, 因此在得到特征标表后, 可以得到任意表示的特征标. 在计算特征标表时, 主要有如下结论:

- $|G| = \sum_{i=1}^r |\chi_i(1)|^2$.
- G/G' 的不可约表示可一一提升为 G 的所有一维表示.
- 借助 G 在某个空间或集合中的作用构造表示.
- 通过已知表示构造新表示 (张量积、诱导表示等).

命题 4.13

设 α 为线性特征, χ 为不可约特征, 则 $\alpha\chi$ 也是不可约特征.

二面体群的特征标表

二面体群

$$D_n = \langle a, b | a^2 = b^n = e, aba^{-1} = b^{-1} \rangle. \quad (4.51)$$

例 4.7 D_3 的特征标表 根据 D_3 的共轭类可知它有 3 个不可约特征, 并且 $D'_3 = \langle b | b^3 = e \rangle, |D_3| = 6$ 说明 D_3 有两个一次不可约表示和一个二次不可约表示, 后者可通过作用在正三角形上得到.

D_3	$\{e\}$	$\{b, b^2\}$	$\{a, ab, ab^2\}$
χ_1	1	1	1
χ_2	1	1	-1
χ_3	2	-1	0

表 4.1: D_3 的特征标表

例 4.8 D_4 的特征标表 根据 D_4 的共轭类可知它有 5 个不可约特征, 并且 $D'_4 = \{e, b^2\}, |D_4| = 8$ 说明 D_4 有四个一次不可约表示和一个二次不可约表示, 前者由 $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ 的不可约表示提升得到, 后者可通过作用在正方形上得到.

D_4	$\{e\}$	$\{b, b^3\}$	$\{b^2\}$	$\{ab, ab^3\}$	$\{a, ab^2\}$
χ_1	1	1	1	1	1
χ_2	1	1	1	-1	-1
χ_3	1	-1	1	-1	1
χ_4	1	-1	1	1	-1
χ_5	2	0	-2	0	0

表 4.2: D_4 的特征标表

例 4.9 D_5 的特征标表 根据 D_5 的共轭类可知它有 4 个不可约特征, 并且 $D'_5 = \langle b | b^5 = e \rangle, |D_5| = 10$ 说明 D_5 有两个一次不可约表示和两个二次不可约表示, 后者可通过作用在正五边形上得到.

D_5	$\{e\}$	$\{b, b^3\}$	$\{b^2, b^3\}$	$\{ab, ab^2, ab^3, ab^4\}$
χ_1	1	1	1	1
χ_2	1	1	1	-1
χ_3	2	$\zeta_5^1 + \zeta_5^4$	$\zeta_5^2 + \zeta_5^3$	0
χ_4	2	$-(\zeta_5^1 + \zeta_5^4)$	$-(\zeta_5^2 + \zeta_5^3)$	0

表 4.3: D_5 的特征标表

¶ 置换群的特征标表

置换群的共轭类可以根据型来划分, 非常明确, 并且前面证明过, $S_n (n \geq 3)$ 的一次表示只有两个. 下面讨论几个例子.

例 4.10 S_3 的特征标表 由于 $S_3 \cong D_3$, 因此它们的特征标表相同.

S_3	(1)	(123)	(12)
χ_1	1	1	1
χ_2	1	1	-1
χ_3	2	-1	0

表 4.4: S_3 的特征标表

例 4.11 S_4 的特征标表 一方面借助共轭类以及数论知识可知 S_4 有一个二次表示, 两个三次表示. 由于 $\chi_2\chi_3$ 仍为二次表示, 因此 $\chi_2\chi_3 = \chi_3$, 因此 $\chi_3((12)) = \chi_3((1234)) = 0$, 设 $\chi_3((123)) = a, \chi_3((12)(34)) = b$, 则由行列正交关系可得

$$2 + 8a + 3b = 0, \quad 4 + 8a^2 + 3b^2 = |S_4| = 24 \Rightarrow a = -1, b = 2 \quad (4.52)$$

对于剩余两列, 首先有 $\chi_2\chi_4 = \chi_5$, 若设 χ_4 行为 a, b, c, d , 则 χ_5 行为 $-a, b, -c, d$, 第二四列、三五列作内积可得

$$ac = -1, \quad bd = 0, \quad (4.53)$$

因此可不妨设 $a = 1, c = -1$ (后两列对称性), 根据 χ_4 行正交性可得

$$9 + 6a^2 + 6c^2 + 3 + 3d^2 = 24 \Rightarrow b = 0, |d| = 1, \quad (4.54)$$

最后第一四行作内积可得

$$3 + 6a + 6c + 3d = 0 \Rightarrow d = -1. \quad (4.55)$$

S_4	(1)	(12)	(123)	(1234)	(12)(34)
χ_1	1	1	1	1	1
χ_2	1	-1	1	-1	1
χ_3	2	0	-1	0	2
χ_4	3	1	0	-1	-1
χ_5	3	-1	0	1	-1

表 4.5: S_4 的特征标表

¶ 其它例子

例 4.12 Q_8 的特征标表 对于四元数群 $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$, 它恰好有五个共轭类 $\{1\}, \{-1\}, \{\pm i\}, \{\pm j\}, \{\pm k\}$, 显然 $Q'_8 = \{\pm 1\}$, $Q_8/Q'_8 \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, 因此 Q_8 有四个一次表示和一个二次表示, 前者均由 $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ 的表示提升, 根据正交关系可以计算 χ_5 . 由上表可以看出, Q_8 与 D_4 的特征标表相同, 但它们并不同构 (后者无

D_4	$\{1\}$	$\{\pm i\}$	$\{-1\}$	$\{\pm j\}$	$\{\pm k\}$
χ_1	1	1	1	1	1
χ_2	1	1	1	-1	-1
χ_3	1	-1	1	-1	1
χ_4	1	-1	1	1	-1
χ_5	2	0	-2	0	0

表 4.6: Q_8 的特征标表

四阶元), 因此不同群可能给出同一特征标表.

例 4.13 A_5 的特征标表 首先 A_5 在 S_5 中有 4 个共轭类, 代表元为 $(1), (12)(34), (123), (12345)$, 个数分别为 1, 15, 20, 24, 并且显然前三个依然是 A_5 中的共轭类 (存在奇置换与它们交换), 对于最后一个, 它在 A_5 中恰好被分为两个共轭类, 分别以 $(12345), (12)(12345)(12) = (13452)$ 为代表元, 各 12 个元素.

由于 A_5 是单群, 因此其导群为自身, 不可约表示只有主表示, 借助一些数论知识可得它有两个三次表示, 一个四次表示和一个五次表示.

令 A_5 置换作用于 $X = \{1, 2, 3, 4, 5\}$ 上, $V = \mathbb{C}[X]$ 为五次表示, 则

$$\chi_V(g) = \#\{x \in X : gx = x\} = \begin{cases} 5, & g = 1, \\ 1, & g = (12)(34), \\ 2, & g = (123), \\ 0, & g = (12345), \\ 0, & g = (13452), \end{cases} \quad (4.56)$$

由于 $\langle \chi_V, \chi_V \rangle = 2, \langle \chi_V, \chi_1 \rangle = 1$, 因此 $\chi_V = \chi_1 + \chi_4$.

再令 A_5 置换作用于 $Y = \{\{i, j\} : \{i, j\} \subset X\}$ 上, $U = \mathbb{C}[Y]$ 为十次表示, 则

$$\chi_U(g) = \#\{y \in Y : gy = y\} = \begin{cases} 10, & g = 1, \\ 2, & g = (12)(34), \\ 1, & g = (123), \\ 0, & g = (12345), \\ 0, & g = (13452), \end{cases} \quad (4.57)$$

由于 $\langle \chi_U, \chi_U \rangle = 3, \langle \chi_U, \chi_1 \rangle = 1$, 故 $\chi_U = \chi_1 + \chi_4 + \chi_5$.

设 χ_2 行为 a, b, c, d , 则分别与第一列内积可得 χ_3 行为 $-a, -2-b, 1-c, 1-d$, 此时考虑二四、三四列内积可得

$$a(2c+1) = (b+1)(2c+1) = 0 \Rightarrow a=0, b=-1, \quad (4.58)$$

由三四列内积可得 $cd = -1$, 由 χ_4 列自身可得 $c+d=1$, 解方程可得

$$c, d = \frac{1 \pm \sqrt{5}}{2}. \quad (4.59)$$

A_5	$\{(1)\}$	$\{(123)\}$	$\{(12)(34)\}$	$\{(12345)\}$	$\{(13452)\}$
χ_1	1	1	1	1	1
χ_2	3	0	-1	$\frac{1+\sqrt{5}}{2}$	$\frac{1-\sqrt{5}}{2}$
χ_3	3	0	-1	$\frac{1-\sqrt{5}}{2}$	$\frac{1+\sqrt{5}}{2}$
χ_4	4	1	0	-1	-1
χ_5	5	-1	1	0	0

表 4.7: A_5 的特征标表

4.4.4 特征标表的其它应用

定义 4.25 (特征的核)

设 ρ 为 G 的表示, $\chi = \chi_\rho$, 称 $N_\chi = \{x \in G : \chi(x) = \chi(1)\} = \text{Ker } \rho$ 为特征的核.



注

1. 由于特征的取值均为单位根的和, 因此 $\chi(x) = \chi(1)$ 当且仅当 $\varphi(x) = \text{Id}$.
2. 正则表示的核平凡, 并且 $N_i = G$ 当且仅当 $i = 1$, 即 χ 为主特征.

命题 4.14

设 $N \leq G$, 则 $N \triangleleft G$ 当且仅当存在 $I \subset \{1, \dots, r\}$ 使得 $N = \bigcap_{i \in I} N_i$.



证明 $\Leftarrow$: 显然.

$\Rightarrow$: 令 $U = \mathbb{C}[G/N]$, ψ, χ 分别为 U 作为 G/N -表示、 G -表示的特征, 则 $\chi = \psi \circ \pi$. 由于正则表示的核平凡, 因此 $N_\psi = \{1\}$, 说明 $\chi(g) = \chi(1)$ 当且仅当 $gN = N, g \in N$, 因此 $N = N_\chi$. 设 $\chi = \sum_{i \in I} a_i \chi_i$, 则

$$|\chi(g)| \leq \sum_{i \in I} a_i |\chi_i(g)| \leq \sum_{i \in I} a_i \chi_i(1) = \chi(1), \quad (4.60)$$

因此 $g \in N_\chi$ 当且仅当对任意 $i \in I$ 都有 $\chi_i(g) = \chi_i(1)$, 即 $g \in N_i$, 因此 $N = N_\chi = \bigcap_{i \in I} N_i$.

借助上述命题, 可以用特征刻画单群.

推论 4.8

下述等价:

1. G 是单群.
2. 对 $i > 1$ 有 $N_i = \{1\}$.
3. 若存在 $g \neq 1$ 使某个 $\chi_i(g) = \chi_i(1)$, 则 $i = 1$.

**定义 4.26**

设 χ 为 G 的特征, 定义 $Z_\chi = \{x \in G : |\chi(x)| = \chi(1)\}$.



注 显然 $N_i \subset Z_i$.

引理 4.7

1. $Z_\chi \leq G$, $N_\chi \triangleleft Z_\chi$.
2. 若 $\chi = \chi_i$ 不可约, 则 $Z_i/N_i = Z(G/N_i)$, 即 G/N_i 的中心.
3. 特别地, 若 G 为非 Abel 单群, 则对 $i > 1$ 有 $Z_i = \{1\}$.



证明

1. $g, h \in Z_\chi$ 当且仅当 $\rho(g) = \lambda_g I, \rho(h) = \lambda_h I$, 其中 λ_g, λ_h 均为单位根, 因此 $\rho(gh^{-1}) = \lambda_g \lambda_h^{-1} I$, 说明 $gh^{-1} \in Z_\chi$. 另一方面若 $h \in N_\chi$, 则对任意 $g \in Z_\chi$ 都有

$$\chi(ghg^{-1}) = \chi(h) = \chi(1) \Rightarrow ghg^{-1} \in N_\chi, \quad (4.61)$$

因此 $N_\chi \triangleleft Z_\chi$.

2. 设 $h \in Z_i, g \in G$, 则 $\chi(ghg^{-1}h^{-1}) = \chi(1)$ (注意 $|\chi(h)| = \chi(1)$ 蕴含可交换性), 因此 $hN_i \in Z(G/N_i)$, 即 $Z_i/N_i \subset Z(G/N_i)$.

反之设 $gN_i \in Z(G/N_i)$, 则对任意 $x \in G$ 有 $\rho(g)\rho(x) = \rho(x)\rho(g)$ (这里 ρ 为左乘 $\mathbb{C}$ -同态), 故 $\rho(g) : V \rightarrow V, v \mapsto gv$ 是 $\mathbb{C}[G]$ -模同态, 但 Schur 引理保证 $\text{End}_{\mathbb{C}[G]}(V) \cong \mathbb{C}$, 因此 $\rho(g) = \mu \text{Id}_V$, 故 $g \in Z_i$, 即得 $Z(G/N_i) \subset Z_i/N_i$.

3. 此时对 $i > 1$ 有 $N_i = 1$, 因此 $Z_i = Z_i/N_i = Z(G/N_i)$ 也只能是 $\{1\}$.

命题 4.15

群 G 的中心为 $Z(G) = \bigcap_{i=1}^r Z_i$.



证明 一方面显然 $Z(G)N_i/N_i \leq Z(G/N_i) = Z_i/N_i$, 因此对所有 i 有 $Z(G) \leq Z_i$, 因此 $Z(G) \leq \bigcap_{i=1}^r Z_i$.

另一方面若 $g \in \bigcap_{i=1}^r Z_i$, 则由 $Z_i/N_i = Z(G/N_i)$ 可得对任意 $x \in G$ 有 $[g, x] \in N_i$, 因此 $[g, x] \in \bigcap_{i=1}^r N_i = \{1\}$, 即 $g \in Z(G)$.

引理 4.8

设 $N \triangleleft G$, 则 G/N 的不可约特征由 G 的不可约特征决定.



证明 根据表示的提升与分解可得, G/N 的不可约表示与 G 的核包含 N 的不可约表示一一对应, 而存在 $I \subset \{1, \dots, r\}$ 使得 $N = \bigcap_{i \in I} N_i$, 因此 G/N 的不可约表示与 $N_i, i \in I$ 一一对应.

推论 4.9

G 的特征标表可以决定 G 是否为幂零群.



证明 设有上中心序列 $\{1\} \triangleleft G_1 \triangleleft G_2 \triangleleft \dots$, 其中 $G_1 = Z(G), G_i/G_{i-1} \cong Z(G/G_{i-1})$, 首先由特征标表可决定 $G_1 = \bigcap_{i=1}^r Z_i$, 由引理可决定 G/G_1 的不可约特征, 进而可决定 $Z(G/Z(G)) = G_2$, 以此类推可决定所有 G_i , 即决定 G 是否幂零.

4.5 Burnside 定理

借助表示论, 可以反过来证明群论中的 Burnside 定理.

4.5.1 代数整数的一些结论

命题 4.16 (有理代数整数平凡)

若 $r \in \mathbb{Q}$ 为代数整数, 则 $r \in \mathbb{Z}$, 即有理代数数只有整数.

**命题 4.17**

- 设 χ 为 G 的特征标, 则对任意 $g \in G, \chi(g)$ 为代数整数.
- 设 (V, φ) 为 G 的不可约表示, C 为 G 的共轭类, 则 $\frac{|C|\chi_\varphi(C)}{\chi_\varphi(1)}$ 为代数整数.



证明

1. 不可约特征的取值为单位根之和, 因此 $\chi(g)$ 为单位根对整数的线性组合, 因此仍为代数整数.
2. 设 $\alpha = \sum_{x \in C} x$, 则对任意 $h \in G$ 有 $h\alpha h^{-1} = \alpha$, 考虑线性映射 $T_\alpha: V \rightarrow V, v \mapsto \alpha v$, 则对任意 $h \in G$ 有

$$\varphi(hv) = \alpha hv = h\alpha v = h\varphi(v) \Rightarrow \varphi \in \text{End}_{\mathbb{C}[G]}(V) \cong \mathbb{C}, \quad (4.62)$$

即存在 $\lambda \in \mathbb{C}$ 使得 $\varphi(v) = \alpha v = \lambda v$. 再考虑线性映射 $\tau: \mathbb{C}[G] \rightarrow \mathbb{C}[G], z \mapsto z\alpha$, 则 $\tau \in \text{End}_{\mathbb{C}[G]} \mathbb{C}[G]$, 视 V 为 $\mathbb{C}[G]$ 子模, 则对任意 $v \in V$ 有 $\tau(v) = v\alpha = \alpha v = \lambda v$, 即 λ 是 τ 的特征值, 令 A 为 τ 在基 G 下的矩阵, 则 $\det(\lambda I - A) = 0$, 并且 $f(x) = \det(xI - A)$ 为首一整系数多项式, 说明 λ 是代数整数, 而

$$\lambda \chi(1) = \text{tr}(T_\alpha) = \sum_{x \in C} \text{tr}(\varphi(x)) = \sum_{x \in C} \chi(x) = |C|\chi(C) \Rightarrow \lambda = \frac{|C|\chi(C)}{\chi(1)}, \quad (4.63)$$

得证.

推论 4.10

设 φ 为 G 的不可约表示, 则 $\chi_\varphi(1) \mid |G|$.



证明 设 $C_1, \dots, C_r$ 为 G 的共轭类, 则根据行正交关系可得

$$1 = \langle \chi_\varphi, \chi_\varphi \rangle = \frac{1}{|G|} \sum_{i=1}^r |C_i| \chi_\varphi(C_i) \overline{\chi_\varphi(C_i)} \Rightarrow \frac{|G|}{\chi_\varphi(1)} = \sum_{i=1}^r \left(\frac{|C_i| \chi_\varphi(C_i)}{\chi_\varphi(1)} \right) \overline{\chi_\varphi(C_i)}, \quad (4.64)$$

代数整数之和是代数整数, 有理代数整数就是整数, 故 $\chi_\varphi(1) \mid |G|$.

引理 4.9

设 $\epsilon_1, \dots, \epsilon_n$ 为单位根, 若

$$\gamma = \frac{\epsilon_1 + \dots + \epsilon_n}{n} \quad (4.65)$$

为代数整数, 则 $\epsilon_1 = \dots = \epsilon_n = \gamma$.

**4.5.2 Burnside 定理****引理 4.10**

若群 G 存在元素个数为素数正幂次的共轭类, 则 G 不是单群.



证明 设 G 的共轭类 C 大小为 $p^n, n \geq 1$, 则由列正交关系可得

$$0 = \sum_{i=1}^r \chi_i(C) \chi_i(1) \Rightarrow -\frac{1}{p} = \sum_{i=2}^r \chi_i(C) \cdot \frac{\chi_i(1)}{p}, \quad (4.66)$$

因此必然存在某个 i 使得 $\chi_i(C) \cdot \frac{\chi_i(1)}{p}$ 不是代数整数, 因此 $p \nmid \chi_i(1)$ 且 $\chi_i(g) \neq 0$, 因此 $|C| = p^n$ 与 $\chi_i(1)$ 互素, 由 Bezout 定理, 存在 $a, b \in \mathbb{Z}$ 使得 $ap^n + b\chi_i(1) = 1$, 因此有代数整数

$$\frac{\chi_i(C)}{\chi_i(1)} = a \frac{|C|\chi_i(C)}{\chi_i(1)} + b\chi_i(C), \quad (4.67)$$

由上节引理可得 $|\chi_i(C)| = \chi_i(1)$, 说明 $Z_i \neq \{1\}$, 因此 G 不是单群.

定理 4.14 (Burnside)

设 $|G| = p^a q^b$, 则 G 为可解群.



Burnside 定理有如下等价形式:

定理 4.15 (Burnside)

设 $|G| = p^a q^b$, p, q 为素数, 则它是不是单群, 除非它是素数阶循环群.



证明 设 G 非交换, $a, b \geq 1$, 根据 Sylow 定理可知 G 有 q^b 阶子群 H (且 H 非单群), 因此可取 $1 \neq g \in Z(H)$, 则 $H \leq N_G(g)$, 并且 $N_G(g) < G$ (因为 G 非交换), 因此

$$p^a = [G : H] = [G : N_G(g)][N_G(g) : H] \Rightarrow [G : N_G(g)] = p^t, t \geq 1, \quad (4.68)$$

这恰好是 g 所在共轭类的大小, 说明 G 不是单群.

4.6 诱导表示**4.6.1 诱导表示与诱导特征**

设 $H \leq G$, T 为左陪集代表元集, 则有分解 $G = \bigsqcup_{t \in T} tH$. 对于 H 的 F -表示 V , $F[G] \otimes_F V$ 是 F -线性空间 (这里 $F[G]$ 为 $(F[G], F[H])$ -双模, V 为左 $F[H]$ -模), 维数为 $|G| \cdot \dim_F V$, 则 $F[G] \otimes_F V$ 有 $F[G]$ -模结构

$$g(x \otimes v) = gx \otimes v. \quad (4.69)$$

令 Y 为 $F[G] \otimes_F V$ 的 F -子空间, 由

$$\{gh \otimes v - g \otimes hv : g \in G, h \in H, v \in V\} \quad (4.70)$$

生成, 则它是 $F[G] \otimes_F V$ 的子 $F[G]$ -模, 这是因为

$$x(gh \otimes v - g \otimes hv) = (xg)h \otimes v - (xg) \otimes (hv) \in Y. \quad (4.71)$$

定义 4.27 (诱导表示)

设 V 为 H 的 F -表示, 称 $(F[G] \otimes_F V)/Y$ 为其到 G 上的诱导表示, 记为 $\text{Ind}_H^G V$.



注 $\text{Ind}_H^G V$ 也可以认为是 $F[G] \otimes_{F[H]} V$.

引理 4.11

作为 G 的 F -表示, $\dim_F \text{Ind}_H^G V = [G : H] \dim_F V$, 并且若 $\{e_1, \dots, e_n\}$ 为 V 的一组 F -基, 则 $\{t \otimes e_i : t \in T, i = 1, \dots, n\}$ 是 $\text{Ind}_H^G V$ 的一组基.



证明 设 $\{e_1, \dots, e_n\}$ 为 V 的一组基, 则 Y 由

$$\{th \otimes e_i - t \otimes he_i : t \in T, 1 \neq h \in H, i = 1, \dots, n\} \quad (4.72)$$

生成, 故 $\dim_F Y \leq [G : H] \cdot (|H| - 1) \dim_F V$, 即得

$$\dim_F \text{Ind}_H^G V = \dim_F F[G] \otimes_F V - \dim_F Y \geq [G : H] \dim_F V, \quad (4.73)$$

另一方面, 若 $g = th$, 则在 $\text{Ind}_H^G V$ 中 $g \otimes v = th \otimes v = t \otimes (hv)$, 这是 $t \otimes e_i$ 的线性组合, 故

$$\dim_F \text{Ind}_H^G V \leq [G : H] \dim_F V, \quad (4.74)$$

得证.

注 除了上面的方法, 可以直接分解得到

$$F[G] \otimes_{F[H]} V = \left(\bigoplus_{g \in T} gF[H] \right) \otimes_{F[H]} V \cong \bigoplus_{g \in T} (gF[H] \otimes_{F[H]} V) \cong \bigoplus_{g \in T} (g \otimes_{F[H]} V). \quad (4.75)$$

命题 4.18 (诱导表示的传递性)

设 $H \leq L \leq G$, V 为 H 的表示, 则 $\text{Ind}_H^G V \cong \text{Ind}_L^G \text{Ind}_H^L V$.



证明 考虑基.

与诱导表示相反, 大群的表示可以限制为子群的表示.

定义 4.28 (限制表示)

设 U 为 G 的 F -表示 (即 $F[G]$ -模), 则它可以视为 $F[H]$ -模, 记为 $\text{Res}_H^G U$, 称为 U 在 H 上的限制表示.

**定理 4.16 (Frobenius reciprocity)**

设 H 为 G 的子群, U 为 $F[G]$ -模, V 为 $F[H]$ -模, 则有 F -线性空间同构

$$\text{Hom}_{F[H]}(V, \text{Res}_H^G U) \cong \text{Hom}_{F[G]}(\text{Ind}_H^G V, U). \quad (4.76)$$



注 从范畴角度而言, 诱导是限制的左伴随.

证明 设 $\varphi \in \text{Hom}_{F[H]}(V, \text{Res}_H^G U)$, 考虑 F -双线性映射

$$f_\varphi : F[G] \times V \rightarrow U, \quad (g, v) \mapsto g\varphi(v), \quad (4.77)$$

它诱导 F -线性映射

$$\tilde{f}_\varphi : F[G] \otimes_F V \rightarrow U, \quad g \otimes v \mapsto g\varphi(v), \quad (4.78)$$

φ 是模 $F[H]$ -同态说明 $Y \subset \text{Ker } \tilde{f}_\varphi$, 因此诱导映射

$$\Gamma(\varphi) : \text{Ind}_H^G V \rightarrow U, \quad g \otimes v \mapsto g\varphi(v), \quad (4.79)$$

显然它保持 $F[G]$ -模结构, 因此有 F -线性映射

$$\Gamma : \text{Hom}_{F[H]}(V, \text{Res}_H^G U) \rightarrow \text{Hom}_{F[G]}(\text{Ind}_H^G V, U), \quad \varphi \mapsto \Gamma(\varphi), \quad (4.80)$$

并且容易验证 Γ 为单射, 对任意 $\theta \in \text{Hom}_{F[G]}(\text{Ind}_H^G V, U)$, 令

$$\varphi : V \rightarrow \text{Res}_H^G U, \quad v \mapsto \theta(1 \otimes v), \quad (4.81)$$

则 $\varphi \in \text{Hom}_{F[H]}(V, \text{Res}_H^G U)$ 并且 $\Gamma(\varphi) = \theta$, 即 Γ 为满射.

定义 4.29 (诱导特征/限制特征)

- 若 V 作为 $\mathbb{C}[H]$ -模的特征为 φ , 记 φ^G 为 $\mathbb{C}[G]$ -模 $\text{Ind}_H^G V$ 的特征, 称为 φ 的诱导特征.
- 若 χ 是 $\mathbb{C}[G]$ -模 U 的特征, 记 $\chi|_H$ 为 $\mathbb{C}[H]$ -模 $\text{Res}_H^G U$ 的特征, 称为 χ 在 H 上的限制特征.

定理 4.17

设 $H \leq G$, φ 为 $\mathbb{C}[H]$ -模 V 的特征, χ 是 $\mathbb{C}[G]$ -模 U 的特征, 则

$$\langle \varphi, \chi|_H \rangle_H = \langle \varphi^G, \chi \rangle_G. \quad (4.82)$$

证明 根据 Frobenius 互反律可得

$$\langle \varphi, \chi|_H \rangle_H = \dim_{\mathbb{C}} \text{Hom}_{\mathbb{C}[H]}(V, \text{Res}_H^G U) = \dim_{\mathbb{C}} \text{Hom}_{\mathbb{C}[G]}(\text{Ind}_H^G V, U) = \langle \varphi^G, \chi \rangle_G. \quad (4.83)$$

命题 4.19 (诱导特征的计算)

设 $H \leq G$, T 为 H 的左陪集代表元系, $\mathbb{C}[H]$ -模 V 的特征为 χ , 则

$$\chi^G(g) = \sum_{t \in T, t^{-1}gt \in H} \chi(t^{-1}gt) = \frac{1}{|H|} \sum_{x \in G, x^{-1}gx \in H} \chi(x^{-1}gx). \quad (4.84)$$

证明 设 $\{e_i : i \in I\}$ 为 V 的一组基, 则 $\{t \otimes e_i : t \in T, i \in I\}$ 是 $\text{Ind}_H^G V$ 的一组基, 设

$$\rho^G(g) : \text{Ind}_H^G V \rightarrow \text{Ind}_H^G V, \quad t \otimes v \mapsto gt \otimes v, \quad (4.85)$$

则 $\chi^G(g) = \text{tr}(\rho^G(g))$, 对于 $t \in T, g \in G$, 设 $gt = sh$, 其中 $s \in T, h \in H$, 则

$$\rho^G(g)(t \otimes V) = s \otimes hV \subset s \otimes V, \quad (4.86)$$

因此当 $s \neq t$ 时 $t^{-1}gt \notin H$, $\rho^G(g)(t \otimes V)$ 不贡献 $\chi^G(g)$; 而当 $s = t$ 时 $t^{-1}gt \in H$, 此时

$$\rho^G(g)(t \otimes v) = gt \otimes v = t \otimes (t^{-1}gt)v, \quad (4.87)$$

因此它的贡献为 $\chi(t^{-1}gt)$, 得证.

进一步若设 $x = th, t \in T, h \in H$, 则 $x^{-1}gx = h^{-1}(t^{-1}gt)h$, 因此 $x^{-1}gx$ 当且仅当 $t^{-1}gt \in H$, 故

$$\chi^G(g) = \sum_{t \in T, t^{-1}gt \in H} \chi(t^{-1}gt) = \sum_{t \in T, t^{-1}gt \in H} \frac{1}{|H|} \sum_{x \in tH} \chi(x^{-1}gx) = \frac{1}{|H|} \sum_{x \in G, x^{-1}gx \in H} \chi(x^{-1}gx). \quad (4.88)$$

命题 4.20

设 χ 为 $H \leq G$ 的特征, 对于 $g \in G$, 令 s 为 g 所在 G 共轭类中 H 共轭类的个数, l 为 g 所在 G 共轭类中的元素个数, 则

1. 若 $s = 0$, 则 $\chi^G(g) = 0$.
2. 若 $s > 0$, $h_1, \dots, h_s$ 为这 s 个 H 共轭类的代表元, $k_1, \dots, k_s$ 为这些 (在 g 所在 G 共轭类中的) H 共轭类中元素个数, 则

$$\chi^G(g) = \sum_{i=1}^s \frac{|Z_G(g)|}{|Z_H(h_i)|} \chi(h_i) = [G : H] \sum_{i=1}^s \frac{k_i}{l} \chi(h_i). \quad (4.89)$$

注 对于一个 $h \in H$, 它所在的 H 共轭类为 $\{k^{-1}hk : k \in H\}$.

证明

1. 若 $s = 0$ 则不存在 $x \in G$ 使得 $x^{-1}gx \in H$, 因此 $\chi^G(g) = 0$.

2. 若 $s > 0$, 则由前述命题可得

$$\chi^G(g) = \frac{1}{|H|} \sum_{x \in G, x^{-1}gx \in H} \chi(x^{-1}gx) = \frac{1}{|H|} \sum_{i=1}^s \sum_{x \in G, x^{-1}gx \in C_H(h_i)} \chi(x^{-1}gx) = \frac{1}{|H|} \sum_{i=1}^s |X_i| \chi(h_i), \quad (4.90)$$

其中 $X_i = \{x \in G : x^{-1}gx \in C_H(h_i)\}$, 实际上

$$l = |C_G(g)|, k_i = |C_G(g) \cap C_H(h_i)|, \quad (4.91)$$

因此 Double Double Counting 可得

$$\frac{|X_i|}{|C_G(g) \cap C_H(h_i)|} = \frac{|G|}{|C_G(g)|} = \{y \in G : y^{-1}gy = g\} = Z_{\{g\}}, \quad (4.92)$$

代入即得.

4.6.2 借助诱导表示计算特征标表

例 4.14 S_3 的特征标表

S_3	(1)	(123)	(12)
χ_1	1	1	1
χ_2	1	1	-1
χ_3	2	-1	0

表 4.8: S_3 的特征标表

S_4	(1)	(12)	(123)	(1234)	(12)(34)
χ_1	1	1	1	1	1
χ_2	1	-1	1	-1	1
χ_3	2	0	-1	0	2
χ_4	3	1	0	-1	-1
χ_5	3	-1	0	1	-1

表 4.9: S_4 的特征标表

例 4.15 S_5 的特征标表

S_5	(1)	(12)	(123)	(1234)	(12)(34)		
χ_1	1	1	1	1	1		
χ_2	1						
χ_3							
χ_4							
χ_5							
χ_6							
χ_7							

表 4.10: S_5 的特征标表

附录 A 补充内容

A.1 Galois 下降

A.2 交换代数前置补充

命题 A.1 (素理想与极大理想的比较)

设 R 为非零交换幺环

- $\mathfrak{p} \triangleleft R$ 为素理想当且仅当 $R/\mathfrak{p}$ 为整环.
- R 中极大理想存在, 且任意非单位元素 (或者任意真理想) 都包含在一个极大理想中.
- R 中极大理想都是素理想.
- $\mathfrak{m} \triangleleft R$ 为极大理想当且仅当 $R/\mathfrak{m}$ 为域.

定义 A.1 (局部环)

若 R 只有一个极大理想, 则称 R 为局部环.

命题 A.2 (局部环与极大理想)

- 设 $(1) \neq \mathfrak{m} \triangleleft R$ 且 $R \setminus \mathfrak{m} \subset U(R)$, 则 R 为局部环且 $\mathfrak{m}$ 为极大理想.
- 若 $\mathfrak{m} \triangleleft R$ 为极大理想且 $1 + \mathfrak{m} \subset U(R)$, 则 R 为局部环.

证明

1. $R \setminus \mathfrak{m} \subset U(R)$ 说明 $\mathfrak{m}$ 极大, 进而任意非单位元素都在 $\mathfrak{m}$ 中, 因此 $\mathfrak{m}$ 为唯一极大理想, R 为局部环.
2. 任取 $x \in R \setminus \mathfrak{m}$, 则 $(x) + \mathfrak{m} = R$ 说明存在 $r \in R, m \in \mathfrak{m}$ 使得 $rx + m = 1, rx \in U(R)$, 因此 $(x) = R$, 因此 $R \setminus \mathfrak{m} \subset U(R)$, 由 1 可得.

定义 A.2 (幂零根 & Jacobson 根)

- 称 R 中所有素理想的交 $\mathfrak{N}$ 为幂零根.
- 称 R 中所有极大理想的交 $\mathfrak{R}$ 为 Jacobson 根.

注 由于极大理想都是素理想, 因此 $\mathfrak{N} \subset \mathfrak{R}$.

命题 A.3 (两种理想的刻画)

- $\mathfrak{N}$ 实际上是 R 中所有幂零元素的全体.
- $x \in \mathfrak{R}$ 当且仅当对任意 $r \in R$ 有 $1 - rx \in U(R)$.

证明

1. 若 $r \in R$ 幂零, 设 $r^n = 0$, 则对任意素理想 $\mathfrak{p}$ 有 $r^n \in \mathfrak{p}$, 因此 $r \in \mathfrak{p}$, 说明 $r \in \mathfrak{N}$; 反之若 $r \in R$ 不幂零, 设 Σ 为 $R \setminus \{r^n : n \in \mathbb{N}\}$ 中 R 的理想的集合, 则由 Zorn 引理易取其极大元 $\mathfrak{p}$, 下证 $\mathfrak{p}$ 为素理想. 根据其极大性, 对任意 $x, y \notin \mathfrak{p}$, 存在 m, n 使得

$$r^m \in (x) + \mathfrak{p}, r^n \in (y) + \mathfrak{p} \Rightarrow r^{m+n} \in (xy) + \mathfrak{p}, \quad (\text{A.1})$$

因此 $xy \notin \mathfrak{p}$, $\mathfrak{p}$ 为不包含 r 的素理想, 即得 $r \notin \mathfrak{N}$.

2. $\Rightarrow$: 假设存在 $r \in R, x \in \mathfrak{R}$ 使得 $1 - rx \notin U(R)$, 则存在包含 $1 - rx$ 的极大理想 $\mathfrak{m}$, $x \in \mathfrak{R} \subset \mathfrak{m}$ 说明 $1 \in \mathfrak{m}$, 与极大性矛盾.
 $\Leftarrow$: 假设存在 x 满足条件但不在某个 $\mathfrak{m}$ 中, 则 $(x) + \mathfrak{m} = R$, 即存在 $r \in R, m \in \mathfrak{m}$ 使得 $m + rx = 1, m =$

$1 - rx \in U(R)$, 矛盾.

推论 A.1 (Nakayama 引理)

设 M 为有限生成 R -模, $\mathfrak{R}$ 为 R 的 Jacobson 理想, 若 $\mathfrak{R}M = M$, 则 $M = 0$.



证明 设 $M = (x_1, \dots, x_n)$, 则 $\mathfrak{R}M = M$ 说明存在 $\mathfrak{R}$ 中的矩阵 J 使得

$$(x_1, \dots, x_n) = (x_1, \dots, x_n)J \Rightarrow (x_1, \dots, x_n)(I - J) = 0, \quad (\text{A.2})$$

设 $y = \det(I - J)$, 由于 $I - J$ 的对角线元素在 $1 + \mathfrak{R}$ 中, 其余元素在 $\mathfrak{R}$ 中, 因此 $y \in 1 + \mathfrak{R}$ 可逆, 说明 $(x_1, \dots, x_n) = 0$.

命题 A.4 (互素)

若交换幺环 R 的理想 $I_1, \dots, I_n$ 两两互素, 则

- $I_1 \cap \dots \cap I_n = I_1 I_2 \dots I_n$.
- $R/(I_1 \cap \dots \cap I_n) \cong R/I_1 \times \dots \times R/I_n$.



命题 A.5

- 设 $\mathfrak{p}_1, \dots, \mathfrak{p}_n \triangleleft R$ 为素理想且 $I \subset \bigcup_{i=1}^n \mathfrak{p}_i$, 则 I 包含在某个 $\mathfrak{p}_k$ 中.
- 设 $I_1, \dots, I_n \triangleleft R$ 且 $\mathfrak{p} \supset \bigcap_{i=1}^n I_i$ 为素理想, 则 $\mathfrak{p}$ 必然包含某个 I_k , 若前面的等号成立则后面的等号成立.



证明

1. 对 n 归纳, 证明 “若每个 $\mathfrak{p}_k$ 都不包含 I , 则 $I \not\subset \bigcup_{i=1}^n \mathfrak{p}_i$ ”, 从而导出矛盾. $n = 1$ 是平凡的, 假设命题对 $n - 1$ 成立, 则对任意 $1 \leq i \leq n$, 存在 $a_i \in I$ 使得 $a_i \notin \bigcup_{j \neq i} \mathfrak{p}_j$, 假设某个 $a_i \notin \mathfrak{p}_i$ 则得证, 否则考虑

$$y = \sum_{i=1}^n a_1 a_2 \dots \widehat{a_i} \dots a_n, \quad (\text{A.3})$$

则 $y \in I$ 但 $y \notin \bigcup_{i=1}^n \mathfrak{p}_i$, 得证.

2. 若不然则对任意 $1 \leq i \leq n$, 存在 $a_i \in I_i, a_i \notin \mathfrak{p}$, 因此 $a_1 \dots a_n \in I_1 \dots I_n \subset \bigcap_{i=1}^n I_i \subset \mathfrak{p}$, 说明必有某个 $a_i \in \mathfrak{p}$, 矛盾.